Cisco IOS XE Denali 16.3.x（Catalyst 3850 スイッチ）ソフトウェア コンフィギュレーション ガイド

初版：2016 年 8 月 3 日

最終更新：2017 年 3 月 3 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

© 2016 Cisco Systems, Inc. All rights reserved.

目 次

第 I 部 : オーディオ ビデオ ブリッジング 137

第 1 章 オーディオ ビデオ ブリッジング 1

機能情報の確認 1

オーディオ ビデオ ブリッジング ネットワークの概要 1

オーディオ ビデオ ブリッジング（AVB）について 1

AVB をサポートするライセンス 2

AVB の利点 2

AVB ネットワークのコンポーネント 2

AVB でサポートされる SKU 4

Generalized Precision Time Protocol（gPTP）について 4

Multiple Stream Reservation Protocol（MSRP）について 5

MSRP の機能 5

QoSHQoS について 6

マルチ VLAN 登録プロトコル（MVRP）について 7

AVB ネットワークの設定 8

AVB の設定 8

スイッチでの AVB のイネーブル化 8

デバイスでの AVB の設定 9

gPTP の設定 10

gPTP の有効化 10

PTP クロックの値の設定 11

HQoS の設定 12

HQoS のイネーブル化 12

フラットなポリシー形式から階層型ポリシー形式への移行：注意事項と制約事項 12
階層型 QoS ポリシーの形式 13
MVRP の設定 14
MVRP のイネーブル化 15
スイッチ インターフェイスでの MVRP の設定 16
AVB ネットワークのモニタリング 17
AVB のモニタリング 17
gPTP のモニタリング 17
MSRP のモニタリング 18
HQoS のモニタリング 18
MVRP のモニタリング 19
AVB 設定とモニタリングの例 19
AVB の例 19
gPTP の例 22
MSRP の例 25
HQoS の例 28
MVRP の例 38

第 II 部： キャンパス ファブリック 41

第 2 章 キャンパス ファブリック 43
キャンパス ファブリック 43
キャンパス ファブリックの概要 43
ファブリック ドメイン要素について 43
キャンパス ファブリック設定時の注意事項 45
ファブリック オーバーレイの設定方法 45
ファブリック エッジ デバイスの設定 45
ファブリック コントロール プレーン デバイスの設定 49
ファブリック境界デバイスの設定 50
キャンパス ファブリックでのセキュリティ グループ タグとポリシーの適用 51
キャンパス ファブリック オーバーレイを使用したマルチキャスト 52

キャンパス ファブリックのマルチキャスト PIM スパース モードの設定 52
キャンパス ファブリックのマルチキャスト PIM SSM の設定 54
キャンパス ファブリックのデータ プレーン セキュリティ 55
エッジ デバイスのデータ プレーン セキュリティの設定 55
コントロール プレーン デバイスのデータ プレーン セキュリティの設定 57
境界デバイスのデータ プレーン セキュリティの設定 58
キャンパス ファブリック設定の例 59

第 III 部： **CleanAir** 63

第 3 章 **Cisco CleanAir の設定** 65
機能情報の確認 65
CleanAir の前提条件 65
CleanAir の制約事項 66
CleanAir について 67
Cisco CleanAir のコンポーネント 68
Cisco CleanAir で使用される用語 69
Cisco CleanAir で検出できる干渉の種類 70
干渉デバイスのマージ 71
永続的デバイス 72
永続的デバイスの検出 72
永続的デバイスの回避 72
EDRRM および AQR の更新モード 72
CleanAir ハイ アベイラビリティ 73
CleanAir の設定方法 73
2.4 GHz 帯域の CleanAir のイネーブル化 73
2.4 GHz での電波品質とデバイスの CleanAir アラームの設定 74
2.4 GHz デバイスの干渉レポートの設定 75
5 GHz 帯域の CleanAir のイネーブル化 77
5 GHz での電波品質とデバイスの CleanAir アラームの設定 77
5 GHz デバイスの干渉レポートの設定 79

CleanAir-Events の EDRRM の設定 80
永続的デバイスの回避の設定 81
コントローラの GUI を使用した Cisco CleanAir の設定 82
Cisco Spectrum Expert の設定 82
Spectrum Expert の設定（CLI） 82
CleanAir パラメータのモニタリング 83
干渉デバイスのモニタリング 86
CleanAir の設定例 87
CleanAir に関する FAQ 88
その他の参考資料 90

第 4 章 **Bluetooth Low Energy の設定** 93
Bluetooth Low Energy について 93
Bluetooth Low Energy ビーコンのイネーブル化 94

第 IV 部： **インターフェイスおよびハードウェア コンポーネント** 97

第 5 章 **インターフェイス特性の設定** 99
インターフェイス特性の設定に関する情報 99
インターフェイス タイプ 99
ポートベースの VLAN 99
スイッチ ポート 100
ルーテッド ポート 101
スイッチ仮想インターフェイス 102
EtherChannel ポート グループ 103
10 ギガビット イーサネット インターフェイス 104
マルチギガビット イーサネット 104
Power over Ethernet（PoE）ポート 105
スイッチの USB ポートの使用 105
USB ミニタイプ B コンソール ポート 105
USB タイプ A ポート 106

インターフェイスの接続 106
インターフェイス コンフィギュレーション モード 107
イーサネット インターフェイスのデフォルト設定 109
インターフェイス速度およびデュプレックス モード 110
速度とデュプレックス モードの設定時の注意事項 111
IEEE 802.3x フロー制御 111
レイヤ 3 インターフェイス 112
Digital Optical Monitoring 113
インターフェイスの特性の設定方法 114
インターフェイスの設定 114
インターフェイスに関する記述の追加 115
インターフェイス範囲の設定 116
インターフェイス レンジ マクロの設定および使用方法 118
イーサネット インターフェイスの設定 120
インターフェイス速度およびデュプレックス パラメータの設定 120
マルチギガビット イーサネット パラメータの設定 122
IEEE 802.3x フロー制御の設定 123
レイヤ 3 インターフェイスの設定 124
論理レイヤ 3 GRE トンネル インターフェイスの設定 125
SVI 自動ステート除外の設定 127
インターフェイスのシャットダウンおよび再起動 128
コンソール メディア タイプの設定 129
USB 無活動タイムアウトの設定 130
Digital Optical Monitoring の有効化 131
インターフェイス特性のモニタ 132
インターフェイス ステータスの監視 132
インターフェイスおよびカウンタのクリアとリセット 133
インターフェイス特性の設定例 134
インターフェイスの説明の追加：例 134
インターフェイスのダウンシフト ステータスの表示：例 134
インターフェイス範囲の設定：例 135

インターフェイス レンジ マクロの設定および使用方法：例 135
インターフェイス速度およびデュプレックス モードの設定：例 136
レイヤ 3 インターフェイスの設定：例 136
コンソール メディア タイプの設定：例 137
USB 無活動タイムアウトの設定：例 137
インターフェイス特性機能の追加情報 138
インターフェイス特性の設定の機能履歴と情報 139

第 6 章 **Auto-MDIX の設定** 141
Auto-MDIX の前提条件 141
Auto-MDIX の制約事項 141
Auto-MDIX の設定に関する情報 142
インターフェイスでの Auto-MDIX 142
Auto-MDIX の設定方法 142
インターフェイスでの Auto-MDIX の設定 142
Auto-MDIX の設定例 143
その他の参考資料 144
Auto-MDIX の機能履歴と情報 145

第 7 章 **イーサネット管理ポートの設定** 147
機能情報の確認 147
イーサネット管理ポートの前提条件 147
イーサネット管理ポートに関する情報 147
デバイスへのイーサネット管理ポートの直接接続 148
ハブを使用したスタック デバイスへのイーサネット管理ポートの接続 148
イーサネット管理ポートおよびルーティング 149
サポートされるイーサネット管理ポートの機能 149
イーサネット管理ポートの設定方法 150
イーサネット管理ポートのディセーブル化およびイネーブル化 150
その他の参考資料 151
イーサネット管理ポートの機能情報 152

第 8 章 **LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定** 153

機能情報の確認 153

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要 154

LLDP 154

LLDP でサポートされる TLV 154

LLDP および Cisco デバイス のスタック 154

LLDP-MED 155

LLDP-MED でサポートされる TLV 155

ワイヤード ロケーション サービス 156

デフォルトの LLDP 設定 158

LLDP に関する制約事項 158

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定方法 159

LLDP のイネーブル化 159

LLDP 特性の設定 160

LLDP-MED TLV の設定 162

Network-Policy TLV の設定 163

ロケーション TLV およびワイヤード ロケーション サービスの設定 166

デバイス上でのワイヤード ロケーション サービスのイネーブル化 169

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定例 170

Network-Policy TLV の設定：例 170

LLDP、LLDP-MED、ワイヤード ロケーション サービスのモニタリングとメンテナンス 170

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの追加情報 172

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの機能情報 173

第 9 章 **システム MTU の設定** 175

機能情報の確認 175

MTU に関する情報 176

システム MTU の制約事項 176

システム MTU 値の適用 176

MTU サイズの設定方法 177

システム MTU の設定 177
Protocol-Specific MTU の設定 178
システム MTU の設定例 179
システム MTU の設定例 179
例：プロトコル固有 MTU の設定 179
例：システム MTU の設定 179
システム MTU に関する追加情報 179
システム MTU の機能情報 180
機能情報の確認 180
MTU に関する情報 180
システム MTU の制約事項 180
システム MTU 値の適用 181
MTU サイズの設定方法 181
システム MTU の設定 181
Protocol-Specific MTU の設定 182
システム MTU の設定例 184
システム MTU の設定例 184
例：プロトコル固有 MTU の設定 184
例：システム MTU の設定 184
システム MTU に関する追加情報 184
システム MTU の機能情報 185

第 10 章 内部電源装置の設定 187
内部電源装置に関する情報 187
内部電源装置の設定方法 187
内部電源装置の設定 187
内部電源装置のモニタ 188
内部電源装置の設定例 188
その他の参考資料 189
内部電源装置の機能履歴と情報 190

第 11 章 **PoE の設定** 191

機能情報の確認 191

PoE について 191

Power over Ethernet（PoE）ポート 191

サポート対象のプロトコルおよび標準 192

受電装置の検出および初期電力割り当て 192

電力管理モード 194

Cisco Universal Power Over Ethernet 197

PoE の設定方法 198

PoE ポートの電力管理モードの設定 198

シグナル/スペア ペアの電力のイネーブル化 200

電力ポリシングの設定 201

電力ステータスのモニタ 203

その他の参考資料 204

PoE の機能情報 204

第 12 章 **Cisco eXpandable Power System（XPS）2200 の設定** 207

XPS 2200 の設定に関する制約事項 207

XPS 2200 の設定について 207

Cisco eXpandable Power System（XPS）2200 の概要 207

XPS 2200 電源モード 208

RPS モード 209

スタック電源モード 209

混在モード 211

XPS 2200 システムのデフォルト 211

XPS 2200 を設定する方法 212

システム名の設定 212

XPS ポートの設定 213

XPS 電源装置の設定 215

XPS 2200 のモニタリングおよびメンテナンス 216

その他の参考資料 216
XPS 2200 の機能履歴と情報 217
関連資料 217
標準 217
MIB 217
RFC 217
シスコのテクニカル サポート 218

第 13 章 **EEE の設定 219**
EEE について 219
EEE の概要 219
デフォルトの EEE 設定 219
EEE の制約事項 219
EEE の設定方法 220
EEE のイネーブル化またはディセーブル化 220
EEE の監視 221
EEE の設定例 222
その他の参考資料 222
EEE 設定の機能履歴と情報 223

第 V 部： **IPv6 225**

第 14 章 **MLD スヌーピングの設定 227**
機能情報の確認 227
IPv6 MLD スヌーピングの設定に関する情報 227
MLD スヌーピングの概要 228
MLD メッセージ 229
MLD クエリー 229
マルチキャスト クライアント エージングの堅牢性 230
マルチキャスト ルータ検出 230
MLD レポート 231

MLD Done メッセージおよび即時脱退 231
トポロジ変更通知処理 232
IPv6 MLD スヌーピングの設定方法 232
MLD スヌーピングのデフォルト設定 232
MLD スヌーピング設定時の注意事項 233
スイッチでの MLD スヌーピングのイネーブル化またはディセーブル化（CLI） 234
VLAN での MLD スヌーピングのイネーブル化またはディセーブル化（CLI） 235
スタティック マルチキャスト グループの設定（CLI） 236
マルチキャスト ルータ ポートの設定（CLI） 237
MLD 即時脱退のイネーブル化（CLI） 238
MLD スヌーピング クエリーの設定（CLI） 239
MLD リスナー メッセージ抑制のディセーブル化（CLI） 241
MLD スヌーピング情報の表示 242
MLD スヌーピングの設定例 243
スタティックなマルチキャスト グループの設定：例 243
マルチキャスト ルータ ポートの設定：例 243
MLD 即時脱退のイネーブル化：例 243
MLD スヌーピング クエリーの設定：例 243

第 15 章 **IPv6 ユニキャスト ルーティングの設定 245**
機能情報の確認 245
IPv6 ユニキャスト ルーティングの設定について 245
IPv6 の概要 246
IPv6 Addresses 246
サポート対象の IPv6 ユニキャスト ルーティング機能 247
サポートされていない IPv6 ユニキャスト ルーティング機能 253
IPv6 機能の制限 253
IPv6 とスイッチ スタック 253
IPv6 のデフォルト設定 254
IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化（CLI） 255
IPv4 および IPv6 プロトコル スタックの設定（CLI） 258

デフォルト ルータ プリファレンスの設定（CLI） 261
IPv6 ICMP レート制限の設定（CLI） 262
IPv6 の CEF および dCEF の設定 263
IPv6 のスタティック ルーティングの設定（CLI） 263
RIP for IPv6 の設定（CLI） 266
OSPF for IPv6 の設定（CLI） 269
IPv6 の EIGRP の設定 271
IPv6 ユニキャスト リバース パス転送の設定 272
IPv6 の表示 272
DHCP for IPv6 アドレス割り当ての設定 274
DHCPv6 アドレス割り当てのデフォルト設定 274
DHCPv6 アドレス割り当ての設定時の注意事項 274
DHCPv6 サーバ機能のイネーブル化（CLI） 274
DHCPv6 クライアント機能のイネーブル化（CLI） 278
IPv6 ユニキャスト ルーティングの設定例 279
IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化：例 279
デフォルト ルータ プリファレンスの設定：例 279
IPv4 および IPv6 プロトコル スタックの設定：例 280
DHCPv6 サーバ機能のイネーブル化：例 280
DHCPv6 クライアント機能のイネーブル化：例 280
IPv6 ICMP レート制限の設定：例 281
IPv6 のスタティック ルーティングの設定：例 281
IPv6 の RIP の設定：例 281
IPv6 の表示：例 281

第 16 章
IPv6 マルチキャストの実装 283
機能情報の確認 283
IPv6 マルチキャスト ルーティングの実装に関する情報 283
IPv6 マルチキャストの概要 283
IPv6 マルチキャスト ルーティングの実装 284
IPv6 マルチキャスト リスナー ディスカバリ プロトコル 285

マルチキャスト クエリアとマルチキャスト ホスト 285
MLD アクセス グループ 285
受信側の明示的トラッキング 285
Protocol Independent Multicast 286
PIM スパース モード 286
IPv6 BSR：RP マッピングの設定 287
PIM-Source Specific Multicast (PIM-SSM) 287
ルーティング可能アドレスの hello オプション 288
PIM IPv6 スタブ ルーティング 288
スタティック mroute 289
MRIB 290
MFIB 290
MFIB 290
IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング 291
IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 292
IPv6 マルチキャストの実装 293
IPv6 マルチキャスト ルーティングのイネーブル化 293
MLD プロトコルのカスタマイズおよび確認 293
インターフェイスでの MLD のカスタマイズおよび確認 293
MLD グループ制限の実装 295
受信側の明示的トラッキングによってホストの動作を追跡するための設定 297
MLD トラフィック カウンタのリセット 297
MLD インターフェイス カウンタのクリア 298
PIM の設定 298
PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示 298
PIM オプションの設定 299
PIM トラフィック カウンタのリセット 301
PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット 301
PIM IPv6 スタブ ルーティングの設定 303
PIM IPv6 スタブ ルーティングの設定時の注意事項 303
IPv6 PIM ルーティングのデフォルト設定 304
IPv6 PIM スタブ ルーティングのイネーブル化 304

IPv6 PIM スタブ ルーティングのモニタ 306
BSR の設定 307
BSR の設定および BSR 情報の確認 307
BSR への PIM RP アドバタイズメントの送信 308
限定スコープ ゾーン内で BSR を使用できるようにするための設定 308
BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定 309
SSM マッピングの設定 310
スタティック mroute の設定 311
IPv6 マルチキャストでの MFIB の使用 312
IPv6 マルチキャストでの MFIB の動作の確認 312
MFIB トラフィック カウンタのリセット 313

第 17 章 **IPv6 クライアント IP アドレス ラーニングの設定 315**
IPv6 クライアント アドレス ラーニングの前提条件 315
IPv6 クライアント アドレス ラーニングについて 316
SLAAC アドレス割り当て 316
ステートフル DHCPv6 アドレス割り当て 317
静的 IP アドレス割り当て 319
ルータ要求 319
ルータ アドバタイズメント 319
ネイバー探索 319
ネイバー探索抑制 320
RA ガード 320
RA スロットリング 321
IPv6 ユニキャストの設定（CLI） 322
RA ガード ポリシーの設定（CLI） 322
RA ガード ポリシーの適用（CLI） 323
RA スロットル ポリシーの設定（CLI） 324
VLAN への RA スロットル ポリシーの適用（CLI） 325
IPv6 ネイバー プロービングの設定方法 326
IPv6 スヌーピングの設定（CLI） 330

IPv6 ND 抑制ポリシーの設定（CLI） 330
VLAN/PortChannel での IPv6 スヌーピングの設定 331
Switch での IPv6 の設定（CLI） 332
DHCP プールの設定（CLI） 333
DHCP を使用しないステートレス自動アドレス設定の設定（CLI） 334
DHCP によるステートレス自動アドレス設定の設定（CLI） 335
ステートフル DHCP のローカル設定（CLI） 336
ステートフル DHCP の外部的設定（CLI） 338
IPv6 アドレス ラーニング設定の確認 339
その他の参考資料 340
IPv6 クライアント アドレス ラーニングの機能情報 341

第 18 章 **IPv6 WLAN セキュリティの設定** 343
IPv6 WLAN セキュリティの前提条件 343
IPv6 WLAN セキュリティの制限 343
IPv6 WLAN セキュリティについて 344
IPv6 WLAN セキュリティの設定方法 347
ローカル認証の設定 347
ローカル ユーザの作成 347
クライアント VLAN とインターフェイスの作成 347
EAP プロファイルの設定 349
ローカル認証モデルの作成 351
クライアント WLAN の作成 352
WPA2+AES でのローカル認証の設定 354
外部 RADIUS サーバの設定 357
RADIUS 認証サーバ ホストの設定 357
RADIUS 認証サーバ グループの設定 358
クライアント VLAN の作成 359
外部 RADIUS サーバを使用した 802.1x WLAN の作成 361
その他の参考資料 362
IPv6 WLAN セキュリティの機能情報 363

第 19 章 **IPv6 ACL の設定** 365

IPv6 ACL の前提条件 365

IPv6 ACL の制限 365

IPv6 ACL について 366

IPv6 ACL の概要 366

ACL のタイプ 368

ユーザあたりの IPv6 ACL 368

フィルタ ID IPv6 ACL 368

ダウンロード可能 IPv6 ACL 368

IPv6 ACL とスイッチ スタック 368

IPv6 ACL の設定 369

IPv6 ACL のデフォルト設定 369

他の機能およびスイッチとの相互作用 369

IPv6 ACL の設定方法 370

IPv6 ACL の作成 370

インターフェイスへの IPv6 の適用 375

WLAN IPv6 ACL の作成 376

IPv6 ACL の確認 377

IPv6 ACL の表示 377

IPv6 ACL の設定例 378

例：IPv6 ACL の作成 378

例：IPv6 ACL の適用 378

例：IPv6 ACL の表示 378

例：RA スロットリングと NS 抑制の設定 379

例：RA ガード ポリシーの設定 380

例：IPv6 ネイバー バインディングの設定 381

その他の参考資料 382

IPv6 ACL の機能情報 383

第 20 章 **IPv6 Web 認証の設定** 385

IPv6 Web 認証の前提条件 385
IPv6 Web 認証の制限 385
IPv6 Web 認証について 386
Web 認証プロセス 386
IPv6 Web 認証の設定方法 387
WPA のディセーブル化 387
WLAN のセキュリティのイネーブル化 388
WLAN のパラメータ マップのイネーブル化 389
WLAN の認証リストのイネーブル化 389
グローバル Web 認証 WLAN パラメータ マップの設定 390
WLAN の設定 390
グローバル コンフィギュレーション モードの IPv6 のイネーブル化 392
IPv6 Web 認証の確認 392
パラメータ マップの確認 392
認証リストの確認 393
その他の参考資料 394
IPv6 Web 認証の機能情報 395

第 21 章 **IPv6 クライアント モビリティの設定** 397
IPv6 クライアント モビリティの前提条件 397
IPv6 クライアント モビリティの制限 397
IPv6 クライアント モビリティについて 398
ルータ アドバタイズメントの使用 399
RA スロットリングと NS 抑制 400
IPv6 アドレス ラーニング 400
複数の IP アドレスの処理 401
IPv6 Configuration 401
ハイ アベイラビリティ 401
IPv6 クライアント モビリティの確認 402
IPv6 クライアント モビリティのモニタリング 402
その他の参考資料 403

IPv6 クライアント モビリティの機能情報 404

第 22 章 IPv6 モビリティの設定 405

IPv6 モビリティの前提条件 405

IPv6 モビリティについて 405

コントローラ間ローミング 406

スティッキ アンカリングでのサブネット内ローミング、およびサブネット間ローミング 406

IPv6 モビリティの設定方法 406

IPv6 モビリティのモニタリング 406

その他の参考資料 409

IPv6 モビリティの機能情報 410

第 VI 部： IP 411

第 23 章 『Configuring HSRP』 413

HSRP の設定 413

機能情報の確認 413

HSRP の設定に関する情報 413

HSRP の概要 413

HSRP のバージョン 415

MHSRP 416

SSO HSRP 417

HSRP およびスイッチ スタック 417

IPv6 の HSRP の設定 417

HSRP の設定方法 418

HSRP のデフォルト設定 418

HSRP 設定時の注意事項 419

HSRP のイネーブル化 419

HSRP のプライオリティの設定 421

MHSRP の設定 424

HSRP 認証およびタイマーの設定 433

ICMP リダイレクト メッセージの HSRP サポートのイネーブル化 435
HSRP グループおよびクラスタリングの設定 435
HSRP の確認 435
HSRP コンフィギュレーションの確認 435
HSRP の設定例 436
HSRP のイネーブル化：例 436
HSRP のプライオリティの設定：例 436
MHSRP の設定：例 436
HSRP 認証およびタイマーの設定：例 437
HSRP グループおよびクラスタリングの設定：例 437
HSRP の設定に関する追加情報 438
HSRP の設定に関する機能情報 439

第 24 章 **NHRP の設定** 441
機能情報の確認 441
NHRP の設定に関する情報 442
NHRP および NBMA のネットワークの相互作用 442
ダイナミックに構築されたハブアンドスポーク ネットワーク 443
NHRP の設定方法 443
インターフェイス上での NHRP のイネーブル化 443
マルチポイント動作のための GRE トンネルの設定 444
NHRP の設定例 447
論理 NBMA の物理ネットワーク設計の例 447
例：マルチポイント動作のための GRE トンネル 449
NHRP の設定に関する追加情報 450
NHRP 設定の機能情報 451

第 25 章 **VRRPv3 プロトコルのサポート** 453
VRRPv3 プロトコルのサポート 453
機能情報の確認 453
VRRPv3 プロトコルのサポートの制限事項 454

VRRPv3 プロトコル サポートについて 454
VRRPv3 の利点 454
VRRP デバイスのプライオリティおよびプリエンプション 456
VRRP のアドバタイズメント 456
VRRPv3 プロトコル サポートについて 457
VRRPv3 の利点 457
VRRP デバイスのプライオリティおよびプリエンプション 458
VRRP のアドバタイズメント 459
VRRPv3 プロトコル サポートの設定方法 460
GLBP のイネーブル化と確認 460
VRRP グループの作成とカスタマイズ 462
FHRP クライアントの初期化前の遅延時間の設定 464
VRRPv3 プロトコル サポートの設定例 465
例：デバイス上の VRRPv3 のイネーブル化 465
例：VRRP グループの作成とカスタマイズ 465
例：FHRP クライアントの初期化前の遅延時間の設定 466
例：VRRP ステータス、設定、および統計情報の詳細 466
その他の参考資料 467
VRRPv3 プロトコルのサポートの機能情報 468
用語集 468

第 26 章
GLBP の設定 471
『Configuring GLBP』 471
機能情報の確認 471
GLBP の制限事項 471
GLBP の前提条件 471
GLBP に関する情報 472
GLBP の概要 472
GLBP アクティブ仮想ゲートウェイ 472
GLBP 仮想 MAC アドレスの割り当て 473
GLBP 仮想ゲートウェイの冗長性 474

GLBP 仮想フォワーダの冗長性 474
GLBP ゲートウェイのプライオリティ 474
GLBP ゲートウェイの重み付けとトラッキング 475
GLBP MD5 認証 475
ISSU-GLBP 476
GLBP SSO 476
GLBP の利点 477
GLBP の設定方法 477
GLBP のカスタマイズ 477
キー ストリングを使用した GLBP MD5 認証の設定 481
キー チェーンを使用した GLBP MD5 認証の設定 482
GLBP テキスト認証の設定 484
GLBP の重み付けの値とオブジェクト トラッキング 486
GLBP のトラブルシューティング 488
GLBP の設定例 489
例：GLBP 設定のカスタマイズ 489
例：キー ストリングを使用した GLBP MD5 認証の設定 490
例：キー チェーンを使用した GLBP MD5 認証の設定 490
例：GLBP テキスト認証の設定 490
例：GLBP 重み付けの設定 490
例：GLBP 設定のイネーブル化 491
GLBP に関する追加情報 491
GLBP の機能情報 492
用語集 493

第 VII 部： IP マルチキャスト ルーティング 495

第 27 章 IP マルチキャスト ルーティング テクノロジーの概要 497
機能情報の確認 497
IP マルチキャスト テクノロジーに関する情報 497
情報配信における IP マルチキャストの役割 497

IP マルチキャスト ルーティング プロトコル 498
マルチキャスト グループ伝送方式 499
IP マルチキャスト境界 501
IP マルチキャスト グループ アドレッシング 502
IP クラス D アドレス 502
IP マルチキャスト アドレスのスコーピング 502
レイヤ 2 マルチキャスト アドレス 504
IP マルチキャスト配信モード 505
Source Specific Multicast 505

第 28 章 **IGMP の設定** 507
機能情報の確認 507
IGMP および IGMP スヌーピングの前提条件 507
IGMP のの前提条件 507
IGMP スヌーピングの前提条件 508
IGMP および IGMP スヌーピングの制約事項 508
IGMP 設定の制約事項 508
IGMP スヌーピングの制約事項 509
IGMP に関する情報 510
Internet Group Management Protocol の役割 510
IGMP マルチキャスト アドレス 510
IGMP のバージョン 511
IGMPv1 511
IGMPv2 511
IGMP バージョン 3 512
IGMPv3 ホスト シグナリング 512
IGMP のバージョンの違い 512
IGMP の加入および脱退処理 515
IGMP の加入処理 515
IGMP の脱退処理 515
IGMP スヌーピング 516

マルチキャスト グループへの加入 517
マルチキャスト グループからの脱退 519
即時脱退 519
IGMP 設定可能脱退タイマー 520
IGMP レポート抑制 520
IGMP スヌーピングとデバイス スタック 521
IGMP フィルタリングおよびスロットリング 521
IGMP のデフォルト設定 522
IGMP スヌーピングのデフォルト設定 522
IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定 523
IGMP の設定方法 523
グループのメンバとしてのデバイスの設定（CLI） 523
IP マルチキャスト グループへのアクセスの制御（CLI） 526
IGMP バージョンの変更（CLI） 528
IGMP ホストクエリー メッセージ インターバルの変更（CLI） 529
IGMPv2 の IGMP クエリー タイムアウトの変更（CLI） 531
IGMPv2 の最大クエリー応答時間の変更（CLI） 533
静的に接続されたメンバとしてのデバイスの設定（CLI） 535
IGMP プロファイルの設定（CLI） 537
IGMP プロファイルの適用（CLI） 539
IGMP グループの最大数の設定（CLI） 541
IGMP スロットリング アクションの設定（CLI） 542
直接接続の IGMP ホストがない場合にマルチキャスト トラフィックが転送されるようにデバイスを設定する方法 544
IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御する方法 546
IGMP スヌーピングを設定する方法 549
IGMP スヌーピングのイネーブル化 549
VLAN インターフェイスでの IGMP スヌーピングのイネーブル化またはディセーブル化（CLI） 550
スヌーピング方法の設定（CLI） 551
マルチキャスト ルータ ポートの設定（CLI） 552

グループに加入するホストの静的な設定（CLI） 554
IGMP 即時脱退のイネーブル化（CLI） 555
IGMP 脱退タイマーの設定（CLI） 556
IGMP 堅牢性変数の設定（CLI） 558
IGMP 最終メンバー クエリ回数の設定（CLI） 559
TCN 関連コマンドの設定 561
IGMP スヌーピング クエリアの設定（CLI） 565
IGMP レポート抑制のディセーブル化（CLI） 567
IGMP のモニタリング 568
IGMP スヌーピング情報の監視 569
IGMP フィルタリングおよび IGMP スロットリングの設定のモニタリング 571
IGMP の設定例 571
例：マルチキャスト グループのメンバとしてのデバイスの設定 571
例：マルチキャスト グループへのアクセスの制御 572
例：IGMP スヌーピングの設定 572
例：IGMP プロファイルの設定 573
例：IGMP プロファイルの適用 573
例：IGMP グループの最大数の設定 574
例：ルーテッド ポートとしてのインターフェイス設定 574
例：SVI としてのインターフェイスの設定 574
例：直接接続された IGMP ホストがない場合に、マルチキャスト トラフィックを転送するようにデバイスを設定 575
IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御する方法 575
例：グループ G のすべての状態を拒否 576
例：ソース S のすべての状態を拒否 576
例：グループ G のすべての状態を許可 576
例：ソース S のすべての状態を許可 576
例：グループ G のソース S をフィルタリング 577
その他の参考資料 577
IGMP の機能履歴と情報 578

第 29 章 IGMP プロキシの設定 579
機能情報の確認 579
IGMP プロキシの前提条件 579
IGMP プロキシの情報 580
IGMP プロキシ 580
IGMP プロキシの設定方法 582
IGMP UDLR に対するアップストリーム UDL デバイスの設定 582
IGMP プロキシ サポート付きの IGMP UDLR に対するダウンストリーム UDL デバイスの設定 583
IGMP プロキシの設定例 587
例：IGMP プロキシ設定 587
その他の参考資料 588
IGMP プロキシの機能履歴と情報 589

第 30 章 スイッチド イーサネットでの IP マルチキャストの抑制 591
機能情報の確認 591
スイッチド イーサネット ネットワークで IP マルチキャストを抑制するための前提条件 592
スイッチド イーサネット ネットワークでの IP マルチキャストについての情報 592
IP マルチキャスト トラフィックとレイヤ 2 スイッチ 592
IP マルチキャスト用の Catalyst スイッチの CGMP 592
IGMP スヌーピング 593
Router-Port Group Management Protocol（RGMP） 594
スイッチド イーサネット ネットワークでマルチキャストを抑制する例 594
IP マルチキャスト用のスイッチの設定 594
IGMP スヌーピングの設定 595
CGMP のイネーブル化 595
レイヤ 2 スイッチド イーサネット ネットワークでの IP マルチキャストの設定 596
スイッチド イーサネット ネットワークで IP マルチキャストを抑制する設定例 597
例：CGMP の設定 597
RGMP の設定例 598

その他の参考資料 598

スイッチドイーサネット ネットワークでの IP マルチキャストの抑制に関する機能履歴と情報 599

第 31 章

PIM の設定 601

機能情報の確認 601

PIM の前提条件 601

PIM に関する制約事項 602

PIMv1 および PIMv2 の相互運用性 602

PIM スタブ ルーティングの設定に関する制約事項 603

Auto-RP および BSR の設定に関する制約事項 604

Auto-RP 拡張の制約事項 605

PIM に関する情報 606

Protocol Independent Multicast の概要 606

PIM デンス モード（PIM-DM） 606

PIM スパース モード（PIM-SM） 607

Multicast Source Discovery Protocol（MSDP） 608

スパース-デンス モード 608

PIM のバージョン 609

PIM スタブ ルーティング 610

IGMP ヘルパー 611

ランデブー ポイント 611

Auto-RP 612

PIM ネットワークでの Auto-RP の役割 613

マルチキャスト境界 614

Auto-RP のスパース - デンス モード 615

Auto-RP の利点 616

PIMv2 ブートストラップ ルータ 616

PIM ドメイン境界 617

マルチキャスト転送 617

マルチキャスト配信のソース ツリー 618

マルチキャスト配信の共有ツリー 618
ソース ツリーの利点 619
共有ツリーの利点 620
PIM 共有ツリーおよびソース ツリー 620
Reverse Path Forwarding 622
RPF チェック 623
PIM ルーティングのデフォルト設定 624
PIM の設定方法 625
PIM スタブ ルーティングのイネーブル化（CLI） 625
ランデブー ポイントの設定 627
マルチキャスト グループへの RP の手動割り当て（CLI） 628
新規インターネットワークでの Auto-RP の設定（CLI） 631
既存のスパース モード クラウドへの Auto-RP の追加（CLI） 634
問題のある RP への Join メッセージの送信禁止（CLI） 638
着信 RP アナウンスメント メッセージのフィルタリング（CLI） 638
PIMv2 BSR の設定 640
PIM ドメイン境界の定義（CLI） 641
IP マルチキャスト境界の定義（CLI） 643
候補 BSR の設定（CLI） 645
候補 RP の設定（CLI） 647
Auto-RP によるスパース モードの設定（CLI） 649
PIM 最短パス ツリーの使用の延期（CLI） 655
PIM ルータクエリー メッセージ間隔の変更（CLI） 657
PIM の動作の確認 659
PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト動作の確認 659
ファースト ホップ ルータでの IP マルチキャストの確認 659
SPT 上のルータでの IP マルチキャストの確認 661
ラスト ホップ ルータでの IP マルチキャスト動作の確認 663
PIM 対応ルータを使用した IP マルチキャストの到達可能性のテスト 667
マルチキャスト ping に応答するルータの設定 667

マルチキャスト ping に応答するように設定されたルータへの ping 669
PIM のモニタリングとトラブルシューティング 669
PIM 情報のモニタリング 669
RP マッピングおよび BSR 情報のモニタリング 670
PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング 671
PIM の設定例 671
例：PIM スタブ ルーティングのイネーブル化 671
例：PIM スタブ ルーティングの確認 672
例：マルチキャスト グループへの RP の手動割り当て 672
例：Auto-RP の設定 673
例：Auto-RP でのスパース モード 673
例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義 673
例：着信 RP アナウンスメント メッセージのフィルタリング 674
例：問題のある RP への Join メッセージの送信禁止 674
例：候補 BSR の設定 674
例：候補 RP の設定 675
その他の参考資料 675
PIM の機能履歴と情報 677

第 32 章 **IP マルチキャストに対する PIM MIB 拡張の設定** 679
機能情報の確認 679
IP マルチキャストに対する PIM MIB 拡張について 679
IP マルチキャストに対する SNMP トラップの PIM MIB 拡張 679
PIM MIB 拡張の利点 680
IP マルチキャストに対する PIM MIB 拡張の設定方法 680
IP マルチキャストに対する PIM MIB 拡張のイネーブル化 680
PIM MIB 拡張の設定例 682
IP マルチキャストに対する PIM MIB 拡張のイネーブル化の例 682
その他の参考資料 682

第 33 章 **MSDP の設定** 685

機能情報の確認 685
685
MSDP を使用して複数の PIM-SM ドメインを相互接続するための情報 685
MSDP を使用した複数の PIM-SM ドメインの相互接続の利点 685
686
MSDP メッセージ タイプ 688
SA メッセージ 688
SA 要求メッセージ 689
SA 応答メッセージ 689
キープアライブ メッセージ 689
SA メッセージの発信、受信および処理 689
SA メッセージの発信 689
SA メッセージの受信 690
SA メッセージの処理 693
MSDP ピア 693
MSDP MD5 パスワード認証 693
MSDP MD5 パスワード認証の動作 694
MSDP MD5 パスワード認証の利点 694
SA メッセージの制限 694
MSDP キープアライブ インターバルおよび保留時間インターバル 694
MSDP 接続再試行インターバル 695
デフォルト MSDP ピア 695
MSDP メッシュ グループ 697
MSDP メッシュ グループの利点 697
SA 発信フィルタ 697
MSDP での発信フィルタ リストの使用 698
MSDP での着信フィルタ リストの使用 699
MSDP の TTL しきい値 700
SA 要求メッセージ 700
SA 要求フィルタ 701
MSDP を使用して複数の PIM-SM ドメインを相互接続する方法 701

MSDP ピアの設定 701
MSDP ピアのシャットダウン 703
MSDP ピア間の MSDP MD5 パスワード認証の設定 704
トラブルシューティングのヒント 705
SA キャッシュ内で許可される特定の MSDP ピアからの SA メッセージ数の制限によるサービス拒絶（DoS）攻撃の防止 706
MSDP キープアライブ インターバルおよび保留時間インターバルの調整 707
MSDP 接続再試行インターバルの調整 708
デフォルトの MSDP ピアの設定 709
MSDP メッシュ グループの設定 710
ローカル ソースの RP によって発信された SA メッセージの制御 711
発信フィルタ リストを使用した SA メッセージの MSDP ピアへの転送の制御 712
着信フィルタ リストを使用した MSDP ピアからの SA メッセージの受信の制御 713
TTL しきい値を使用した SA メッセージで送信されたマルチキャスト データの制限 714
MSDP ピアへの送信元情報の要求 715
SA 要求フィルタを使用した MSDP ピアからの発信 SA 要求メッセージに対する応答の制御 716
境界 PIM デンス モード領域の MSDP への包含 717
RP アドレス以外の発信元アドレスの設定 718
MSDP のモニタリング 719
MSDP 接続統計情報および SA キャッシュ エントリの消去 721
MSDP の簡易ネットワーク管理プロトコル（SNMP）モニタリングのイネーブル化 722
トラブルシューティングのヒント 723
MSDP を使用して複数の PIM-SM ドメインを相互接続する設定例 724
例：MSDP ピアの設定 724
例：MSDP MD5 パスワード認証の設定 724
例：デフォルト MSDP ピアの設定 725
例：MSDP メッシュ グループの設定 727
その他の参考資料 727
Multicast Source Discovery Protocol の機能履歴と情報 728

第 34 章 ワイヤレス マルチキャストの設定 729

機能情報の確認 729

ワイヤレス マルチキャスト設定の前提条件 729

ワイヤレス マルチキャスト設定の制約事項 730

IPv6 スヌーピングの制限 730

IPv6 RA ガードの制限 730

ワイヤレス マルチキャストに関する情報 731

マルチキャスト最適化について 732

IPv6 グローバル ポリシー 732

IPv6 RA ガード 732

IPv6 スヌーピングに関する情報 733

IPv6 ネイバー ディスカバリ ネイバー インスペクション 733

ワイヤレス マルチキャストの設定方法 736

ワイヤレス マルチキャスト MCMC モードの設定（CLI） 736

ワイヤレス マルチキャスト MCUC モードの設定（CLI） 736

IPv6 スヌーピングの設定（CLI） 737

IPv6 スヌーピング ポリシーの設定（CLI） 738

マルチキャスト ルータ ポートとしてのレイヤ 2 ポートの設定（CLI） 738

IPv6 RA ガードの設定（CLI） 739

非 IP ワイヤレス マルチキャストの設定（CLI） 740

ワイヤレス ブロードキャストの設定（CLI） 741

WLAN の IP マルチキャスト VLAN の設定（CLI） 742

ワイヤレス マルチキャストのモニタリング 743

ワイヤレス マルチキャストの次の作業 743

第 35 章 SSM の設定 745

機能情報の確認 745

SSM の設定の前提条件 745

SSM 設定の制約事項 746

SSM に関する情報 747

SSM コンポーネントの概要 748
SSM および Internet Standard Multicast（ISM） 748
SSM IP アドレスの範囲 748
SSM の動作 749
SSM マッピング 749
スタティック SSM マッピング 750
DNS ベースの SSM マッピング 750
SSM の設定方法 752
SSM の設定（CLI） 752
Source-Specific Multicast（SSM）マッピングの設定 754
スタティック SSM マッピングの設定（CLI） 754
DNS ベースの SSM マッピングの設定（CLI） 756
SSM マッピングを使用したスタティック トラフィック転送の設定（CLI） 758
SSM のモニタリング 760
SSM マッピングのモニタリング 761
SSM の次の作業 761
その他の参考資料 761
SSM の機能履歴と情報 763

第 36 章 GRE トンネルを介するマルチキャスト ルーティングの設定 765
機能情報の確認 765
GRE トンネルを介するマルチキャスト ルーティングの設定の前提条件 765
GRE トンネルを介するマルチキャスト ルーティングの設定の制約事項 766
GRE トンネルを介するマルチキャスト ルーティングについて 766
GRE トンネルを介するマルチキャスト ルーティングの設定方法 767
非 IP マルチキャスト エリアを接続する GRE トンネルの設定 767
非 IP マルチキャスト エリアを接続するトンネリングの例 768

第 37 章 サービス検出ゲートウェイの設定 771
機能情報の確認 771
サービス検出ゲートウェイの設定に関する制約事項 771

サービス検出ゲートウェイおよび mDNS に関する情報 772
mDNS 772
mDNS-SD 773
サービス検出ゲートウェイ 773
mDNS ゲートウェイとサブネット 774
フィルタリング 775
サービス検出ゲートウェイの設定方法 776
サービス リストの設定（CLI） 776
mDNS ゲートウェイの有効化とサービスの再配布（CLI） 779
サービス検出ゲートウェイのモニタリング 782
設定例 783
例：発信 mDNS パケットに対する代替送信元インターフェイスの指定 783
例：サービス アナウンスメントの再配布 783
例：ワイヤレス クライアントに対する mDNS パケットのブリッジングの無効化 783
例：サービス リストの作成、フィルタの適用およびパラメータの設定 784
例：mDNS ゲートウェイの有効化とサービスの再配布 784
例：グローバル mDNS 設定 784
例：インターフェイス mDNS 設定 785
サービス検出ゲートウェイの設定の次の作業 785
その他の参考資料 786
サービス検出ゲートウェイの機能履歴と情報 787

第 38 章 **IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパース モードの最適化** 789
機能情報の確認 789
大規模な IP マルチキャスト展開での PIM スパース モードの最適化の前提条件 790
大規模な IP マルチキャスト展開での PIM スパース モードの最適化について 790
PIM 登録プロセス 790
PIM バージョン 1 の互換性 791
PIM 指定ルータ 791
PIM スパース モード登録メッセージ 792

メモリ要件を減らすために最短パス ツリーの使用を回避する 792
PIM 共有ツリーおよびソース ツリー（最短パス ツリー） 792
最短パスツリーの使用を回避または延期する利点 793
大規模な IP マルチキャスト展開で PIM スパース モードを最適化する方法 794
大規模な展開での PIM スパース モードの最適化 794
大規模なマルチキャスト展開での PIM スパース モードの最適化の設定例 796
大規模な IP マルチキャスト展開での PIM スパース モードの最適化の例 796
その他の参考資料 797
大規模な IP マルチキャスト展開での PIM スパース モードの最適化の機能履歴と情報 798

第 39 章 **IP マルチキャストの最適化：マルチキャスト サブセカンド コンバージェンス** 799
機能情報の確認 799
マルチキャスト サブセカンド コンバージェンスの前提条件 799
マルチキャスト サブセカンド コンバージェンスの制約事項 800
マルチキャスト サブセカンド コンバージェンスについて 800
マルチキャスト サブセカンド コンバージェンスの利点 800
マルチキャスト サブセカンド コンバージェンス スケーラビリティ拡張機能 800
PIM ルータ クエリ メッセージ 801
Reverse Path Forwarding 801
RPF チェック 801
トリガード RPF チェック 802
RPF フェールオーバー 802
トポロジの変更とマルチキャスト ルーティングのリカバリ 802
マルチキャスト サブセカンド コンバージェンスの設定方法 803
定期的な RPF チェック間隔の変更 803
PIM RPF フェールオーバー間隔の設定 804
PIM ルータ クエリ メッセージ間隔の変更 804
マルチキャスト サブセカンド コンバージェンス設定の確認 805
マルチキャスト サブセカンド コンバージェンスの設定例 806
定期的な RPF チェック間隔の変更例 806
PIM RPF フェールオーバー間隔の設定例 807

PIM ルータ クエリ メッセージ インターバルの変更例 807
その他の参考資料 807
マルチキャスト サブセカンド コンバージェンスの機能履歴と情報 808

第 40 章 IP マルチキャストの最適化：等コスト パス間での IP マルチキャスト ロード スプリッティング 809
機能情報の確認 809
等コスト パス間での IP マルチキャスト ロード スプリットの前提条件 810
等コスト パス間での IP マルチキャスト ロード スプリッティングについて 810
ロード スプリットとロード バランシング 810
複数の等コスト パスが存在する場合の IP マルチキャストのデフォルト動作 810
IP マルチキャスト トラフィックをロード スプリットする方法 813
ECMP マルチキャスト ロード スプリットの概要 813
S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード スプリット 813
基本 S-G ハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリット 814
S ハッシュおよび基本 S-G ハッシュ アルゴリズムを使用した場合の副産物としての予測可能性 814
S ハッシュおよび基本 S-G ハッシュ アルゴリズムを使用した場合の副産物としての局在化 815
ソース グループとネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリッティング 816
RPF パス選択のための PIM ネイバー クエリおよびハロー メッセージへの ECMP マルチキャスト ロード スプリットの影響 817
PIM-DM および Bidir-PIM での DF 選定でのアサート処理に対する ECMP マルチキャスト ロード スプリットの影響 818
PIM-SM および PIM-SSM での PIM アサート処理に対する ECMP マルチキャスト ロード スプリットの影響 819
ユニキャスト ルーティングが変わった場合の ECMP マルチキャスト ロード スプリットと再コンバージェンス 820
ECMP マルチキャスト ロード スプリットでの BGP の使用 821
スタティック mroute での ECMP マルチキャスト ロード スプリットの使用 821

IP マルチキャスト トラフィックのロード スプリッティングの代替方法 822
ECMP を介して IP マルチキャスト トラフィックをロード スプリットする方法 822
ECMP マルチキャスト ロード スプリットのイネーブル化 822
IP マルチキャスト ロード スプリットの前提条件：ECMP 823
機能制限 823
ソース アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 824
ソース アドレスおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 827
ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 829
ECMP を介した IP マルチキャスト トラフィックのロード スプリットの設定例 831
例：ソース アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 831
ソース アドレスおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化の例 831
ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化の例 832
その他の参考資料 832
ECMP を介した IP マルチキャスト トラフィックのロード スプリットの機能履歴と情報 833

第 41 章

IP マルチキャストの最適化：マルチキャスト向け SSM チャネル ベース フィルタリング 835
機能情報の確認 835
マルチキャスト境界向け SSM チャネル ベース フィルタリングの前提条件 836
マルチキャスト境界向け SSM チャネル ベース フィルタリング機能について 836
マルチキャスト境界のルール 836
マルチキャスト境界向け SSM チャネル ベース フィルタリングの利点 837
マルチキャスト境界向け SSM チャネル ベース フィルタリングの設定方法 837
マルチキャスト境界の設定 837
マルチキャスト境界向け SSM チャネル ベース フィルタリングの設定例 838
トラフィックを許可および拒否するマルチキャスト境界の設定例 838
トラフィックを許可するマルチキャスト境界の設定例 839
トラフィックを拒否するマルチキャスト境界の設定例 839

その他の参考資料 840
マルチキャスト境界向け SSM チャネル ベース フィルタリングの機能履歴と情報 841

第 42 章 IP マルチキャストの最適化：PIM デンス モード ステート リフレッシュ 843
機能情報の確認 843
PIM デンス モード ステート リフレッシュの前提条件 843
PIM デンス モード ステート リフレッシュの制約事項 844
PIM デンス モード ステート リフレッシュについて 844
PIM デンス モード ステート リフレッシュの概要 844
PIM デンス モード ステート リフレッシュの利点 845
PIM デンス モード ステート リフレッシュの設定方法 845
PIM デンス モード ステート リフレッシュの設定 845
PIM デンス モード ステート リフレッシュの設定 846
PIM DM ステート リフレッシュのモニタリングと維持 846
PIM デンス モード ステート リフレッシュの設定例 847
PIM デンス モード ステート リフレッシュ制御メッセージの発信、処理、および転送の例 847
PIM デンス モード ステート リフレッシュ制御メッセージの処理および転送の例 848
その他の参考資料 848
PIM デンス モード ステート リフレッシュの機能履歴と情報 849

第 43 章 IP マルチキャストの最適化：IGMP ステート制限 851
機能情報の確認 851
IGMP ステート制限の前提条件 851
IGMP ステート制限の制約事項 852
IGMP ステート制限に関する情報 852
IGMP ステート制限 852
IGMP ステート制限機能の設計 852
IGMP ステート リミッタのメカニズム 853
IGMP ステート制限の設定方法 853
IGMP ステート リミッタの設定 853

グローバルな IGMP ステート リミッタの設定 854
インターフェイスごとの IGMP ステート リミッタの設定 854
IGMP ステート制限の設定例 856
IGMP ステート リミッタの設定例 856
その他の参考資料 857
IGMP ステート制限の機能履歴と情報 858

第 VIII 部： レイヤ 2/3 859

第 44 章 スパニングツリー プロトコルの設定 861
機能情報の確認 861
STP の制約事項 861
スパニング ツリー プロトコルに関する情報 862
スパニングツリー プロトコル 862
スパニングツリー トポロジと BPDU 863
ブリッジ ID、デバイス プライオリティ、および拡張システム ID 865
ポート プライオリティとパス コスト 866
スパニングツリー インターフェイス ステート 867
デバイス またはポートがルート デバイスまたはルート ポートになる仕組み 870
スパニングツリーおよび冗長接続 871
スパニングツリー アドレスの管理 871
接続を維持するためのエージング タイムの短縮 872
スパニングツリー モードおよびプロトコル 872
サポートされるスパニングツリー インスタンス 873
スパニングツリーの相互運用性と下位互換性 873
STP および IEEE 802.1Q トランク 874
VLAN ブリッジ スパニングツリー 874
スパニング ツリーとデバイス スタック 874
スパニングツリー機能のデフォルト設定 875
スパニングツリー機能の設定方法 876
スパニングツリー モードの変更（CLI） 876

スパニング ツリーのディセーブル化（CLI） 878
ルート デバイスの設定（CLI） 879
セカンダリ ルート デバイスの設定（CLI） 880
ポート プライオリティの設定（CLI） 882
パス コストの設定（CLI） 883
VLAN のデバイス プライオリティの設定（CLI） 885
hello タイムの設定（CLI） 886
VLAN の転送遅延時間の設定（CLI） 887
VLAN の最大エージング タイムの設定（CLI） 888
転送保留カウントの設定（CLI） 889
スパニングツリー ステータスのモニタリング 890
スパニング ツリー プロトコルに関する追加情報 891
STP の機能情報 892

第 45 章 複数のスパニング ツリー プロトコルの設定 893
機能情報の確認 893
MSTP の前提条件 893
MSTP の制約事項 894
MSTP について 895
MSTP の設定 895
MSTP 設定時の注意事項 896
ルート スイッチ 897
MST リージョン 898
IST、CIST、CST 898
MST リージョン内の動作 899
MST リージョン間の動作 900
IEEE 802.1s の用語 900
MST リージョンの図 901
ホップ カウント 902
境界ポート 903
IEEE 802.1s の実装 904

ポートの役割名の変更 904
レガシーおよび規格デバイスの相互運用 904
単一方向リンク障害の検出 905
MSTP およびデバイス スタック 905
IEEE 802.1D STP との相互運用性 906
RSTP 概要 906
ポートの役割およびアクティブ トポロジ 906
高速コンバージェンス 908
ポート ロールの同期 909
ブリッジ プロトコル データ ユニットの形式および処理 910
トポロジの変更 911
プロトコル移行プロセス 912
MSTP のデフォルト設定 913
MSTP 機能の設定方法 913
MST リージョン設定の指定と MSTP のイネーブル化（CLI） 913
ルート デバイスの設定（CLI） 916
セカンダリ ルート デバイスの設定（CLI） 917
ポート プライオリティの設定（CLI） 919
パス コストの設定（CLI） 920
デバイス プライオリティの設定（CLI） 922
hello タイムの設定（CLI） 924
転送遅延時間の設定（CLI） 925
最大エージング タイムの設定（CLI） 926
最大ホップ カウントの設定（CLI） 926
高速移行を確実にするためのリンク タイプの指定（CLI） 927
ネイバー タイプの設定（CLI） 929
プロトコルの移行プロセスの再開（CLI） 930
MSTP に関する追加情報 931
MSTP の機能情報 932

第 46 章 オプションのスパニングツリー機能の設定 933

オプションのスパニングツリー機能について 933
PortFast 933
BPDU ガード 934
BPDU フィルタリング 934
UplinkFast 935
クロススタック UplinkFast 937
クロススタック UplinkFast の動作 937
高速コンバージェンスを発生させるイベント 939
BackboneFast 940
EtherChannel ガード 942
ルート ガード 943
ループ ガード 944
オプションのスパニングツリー機能の設定方法 944
PortFast のイネーブル化（CLI） 944
BPDU ガードのイネーブル化（CLI） 946
BPDU フィルタリングのイネーブル化（CLI） 948
冗長リンクで使用するための UplinkFast のイネーブル化（CLI） 949
UplinkFast のディセーブル化（CLI） 951
BackboneFast をイネーブル化（CLI） 952
EtherChannel ガードのイネーブル化（CLI） 953
ルート ガードのイネーブル化（CLI） 954
ループ ガードのイネーブル化（CLI） 955
スパニングツリー ステータスのモニタリング 956
オプションのスパニング ツリー機能に関する追加情報 957
オプションのスパニングツリー機能の機能情報 958

第 47 章 **EtherChannel の設定** 959
機能情報の確認 959
EtherChannel の制約事項 959
EtherChannel について 960
EtherChannel の概要 960

EtherChannel のモード 961
デバイス上の EtherChannel 961
EtherChannel リンクのフェールオーバー 962
チャネル グループおよびポートチャネル インターフェイス 963
Port Aggregation Protocol; ポート集約プロトコル 964
PAgP モード 965
PAgP 学習方式およびプライオリティ 966
PAgP と他の機能との相互作用 967
Link Aggregation Control Protocol 967
LACP モード 968
LACP とリンクの冗長性 969
LACP と他の機能との相互作用 969
EtherChannel の On モード 969
ロードバランシングおよび転送方式 970
MAC アドレス転送 970
IP アドレス転送 971
ロードバランシングの利点 972
EtherChannel およびデバイス スタック 973
デバイス スタックおよび PAgP 973
デバイス スタックおよび LACP 973
EtherChannel のデフォルト設定 973
EtherChannel 設定時の注意事項 975
レイヤ 2 EtherChannel 設定時の注意事項 976
レイヤ 3 EtherChannel 設定時の注意事項 977
Auto-LAG 977
Auto-LAG 設定時の注意事項 978
EtherChannel の設定方法 979
レイヤ 2 EtherChannel の設定 （CLI） 979
レイヤ 3 EtherChannel の設定 （CLI） 982
EtherChannel ロードバランシングの設定（CLI） 985
EtherChannel 拡張ロードバランシングの設定（CLI） 987

PAgP 学習方式およびプライオリティの設定 （CLI） 988
LACP ホット スタンバイ ポートの設定 989
LACP 最大バンドル機能の設定（CLI） 990
LACP ポートチャネル スタンドアロン ディセーブルの設定 991
LACP ポート チャネルの最小リンク機能の設定（CLI） 991
LACP システム プライオリティの設定（CLI） 992
LACP ポート プライオリティの設定（CLI） 993
LACP 高速レート タイマーの設定 995
グローバルな Auto-LAG の設定 996
ポート インターフェイスでの Auto-LAG の設定 997
Auto-LAG での持続性の設定 998
EtherChannel、PAgP、および LACP ステータスのモニタ 999
EtherChannel の設定例 1000
レイヤ 2 EtherChannel の設定：例 1000
レイヤ 3 EtherChannel の設定：例 1001
LACP ホット スタンバイ ポートの設定：例 1001
Auto-LAG の設定：例 1002
EtherChannels の追加リファレンス 1003
EtherChannels の機能情報 1004

第 48 章 **Resilient Ethernet Protocol の設定** 1005
機能情報の確認 1005
REP の概要 1005
リンク完全性 1008
短時間でのコンバージェンス 1008
VLAN ロード バランシング 1009
スパニングツリー インタラクション 1011
REP ポート 1011
REP の設定方法 1011
REP のデフォルト設定 1012
REP 設定時の注意事項 1012

REP 管理 VLAN の設定 1014
REP インターフェイスの設定 1015
VLAN ロード バランシングの手動によるプリエンプションの設定 1020
REP の SNMP トラップ設定 1021
REP のモニタリング 1022

第 49 章 単方向リンク検出の設定 1023
機能情報の確認 1023
UDLD 設定の制約事項 1023
UDLD について 1024
動作モード 1024
通常モード 1024
アグレッシブ モード 1025
単一方向の検出方法 1026
ネイバー データベース メンテナンス 1026
イベントドリブン検出およびエコー 1026
UDLD リセット オプション 1027
UDLD のデフォルト設定 1027
UDLD の設定方法 1028
UDLD のグローバルなイネーブル化（CLI） 1028
インターフェイスでの UDLD のイネーブル化（CLI） 1029
UDLD のモニタおよびメンテナンス 1031
UDLD の追加リファレンス 1031
UDLD の機能情報 1032

第 IX 部 : Lightweight アクセス ポイント 1033

第 50 章 アクセス ポイント ディスカバリ用のデバイスの設定 1035
機能情報の確認 1035
アクセス ポイント ディスカバリ用のデバイスの設定の前提条件 1035
アクセス ポイント ディスカバリ用のデバイスの設定の制約事項 1036

アクセス ポイント ディスカバリ用のデバイスの設定に関する情報 1037
アクセス ポイント通信プロトコル 1037
アクセス ポイントの join 情報の表示 1037
アクセス ポイント接続プロセスのトラブルシューティング 1037
アクセス ポイント ディスカバリの設定方法 1039
アクセス ポイントの Syslog サーバの設定（CLI） 1039
アクセス ポイントの join 情報のモニタリング（CLI） 1039
アクセス ポイント ディスカバリ用のデバイスの設定例 1040
すべてのアクセス ポイントの MAC アドレスの表示：例 1040
Lightweight Cisco Aironet アクセス ポイントの DHCP オプション 43 の設定例 1041
AP パススルーの設定 1042
AP パススルーについて 1042
AP パススルーの設定 1042

第 51 章 データ暗号化の設定 1045
機能情報の確認 1045
データ暗号化の設定の前提条件 1045
データ暗号化の設定に関する制約事項 1046
データの暗号化について 1046
データ暗号化の設定方法 1046
データ暗号化の設定（CLI） 1046
データ暗号化の設定例 1047
すべてのアクセス ポイントのデータ暗号化の状態の表示：例 1047

第 52 章 再送信間隔および再試行回数の設定 1049
機能情報の確認 1049
アクセス ポイントの再送信間隔と再試行回数の設定の前提条件 1049
再送信間隔および再試行回数について 1050
アクセス ポイントの再送信間隔と再試行回数の設定方法 1050
アクセス ポイントの再送信間隔と再試行回数の設定（CLI） 1050
CAPWAP の最大伝送単位情報の表示（CLI） 1051

アクセス ポイントの再送信間隔と再試行回数の設定例 1052
CAPWAP 再送信の詳細の表示：例 1052
最大伝送単位情報の表示：例 1052

第 53 章 適応型ワイヤレス侵入防御システムの設定 1053
機能情報の確認 1053
wIPS 設定の前提条件 1053
アクセス ポイントでの wIPS の設定方法 1054
アクセス ポイントでの wIPS の設定（CLI） 1054
wIPS 情報のモニタリング 1056
アクセス ポイントでの wIPS の設定例 1056
モニタ設定チャネル セットの表示：例 1056
wIPS 情報の表示：例 1057

第 54 章 アクセス ポイントの認証の設定 1059
機能情報の確認 1059
アクセス ポイントの認証を設定するための前提条件 1059
アクセス ポイントの認証の設定の制約事項 1060
アクセス ポイントに対する認証の設定について 1060
アクセス ポイントの認証の設定方法 1061
アクセス ポイントのグローバル資格情報の設定（CLI） 1061
アクセス ポイントの認証の設定（CLI） 1062
認証のスイッチの設定（CLI） 1066
アクセス ポイントの認証の設定例 1067
アクセス ポイントの認証設定の表示：例 1067

第 55 章 自律アクセス ポイントの Lightweight モードへの変換 1069
機能情報の確認 1069
Autonomous アクセス ポイントの Lightweight モードへの変換の前提条件 1070
Lightweight モードに変換される Autonomous アクセス ポイントについて 1070
Lightweight モードから Autonomous モードへの復帰 1070

DHCP オプション 43 および DHCP オプション 60 の使用 1070
変換したアクセス ポイントがクラッシュ情報をデバイスに送信する方法 1071
変換したアクセス ポイントからのメモリ コア ダンプのアップロード 1071
変換されたアクセス ポイントの MAC アドレスの表示 1071
Lightweight アクセス ポイントの静的 IP アドレスの設定 1072
Lightweight アクセス ポイントの Autonomous アクセス ポイントへの再変換方法 1072
Lightweight アクセス ポイントを Autonomous モードに戻す方法（CLI） 1072
モード ボタンと TFTP サーバを使用して Lightweight アクセス ポイントを Autonomous モードに戻す方法 1073
アクセス ポイントの認可（CLI） 1073
変換したアクセス ポイントでの Reset ボタンのディセーブル化（CLI） 1075
AP クラッシュ ログ情報のモニタリング 1076
アクセス ポイントでの固定 IP アドレスの設定方法 1076
アクセス ポイントでの固定 IP アドレスの設定（CLI） 1076
TFTP リカバリ手順を使用したアクセス ポイントのリカバリ 1078
Autonomous アクセス ポイントを Lightweight モードに変換する場合の設定例 1078
アクセス ポイントの IP アドレス設定の表示：例 1078
アクセス ポイントのクラッシュ ファイル情報の表示：例 1079

第 56 章 **Cisco ワークグループ ブリッジの使用** 1081
機能情報の確認 1081
Cisco ワークグループ ブリッジと Cisco 以外のワークグループ ブリッジについて 1081
ワークグループ ブリッジ状態のモニタリング 1082
WGB の問題のデバッグ（CLI） 1082
ワークグループ ブリッジの設定例 1084
WGB の設定：例 1084

第 57 章 **プローブ要求フォワーディングの設定** 1085
機能情報の確認 1085
プローブ要求フォワーディングの設定について 1085
プローブ要求フォワーディングの設定方法（CLI） 1085

第 58 章 RFID トラッキングの最適化 1089
機能情報の確認 1089
アクセス ポイントでの RFID トラッキングの最適化 1089
アクセス ポイントでの RFID トラッキングの最適化方法 1090
アクセス ポイントでの RFID トラッキングの最適化（CLI） 1090
RFID トラッキングの最適化の設定例 1091
モニタ モードでのすべてのアクセス ポイントの表示：例 1091

第 59 章 国番号の設定 1093
機能情報の確認 1093
国番号の設定の前提条件 1093
国番号の設定について 1094
国番号の設定方法（CLI） 1094
国番号の設定例 1097
国番号のチャネル リストの表示：例 1097

第 60 章 リンク遅延の設定 1099
機能情報の確認 1099
リンク遅延の設定の前提条件 1099
リンク遅延の設定の制約事項 1100
リンク遅延の設定について 1100
TCP MSS 1100
リンク テスト 1100
リンク遅延の設定方法 1101
リンク遅延の設定（CLI） 1101
TCP MSS の設定方法 1104
TCP MSS の設定（CLI） 1104
リンク テストの実行（CLI） 1105
リンク遅延の設定例 1105
リンク テストの実行：例 1105

リンク遅延情報の表示：例 1106
TCP MSS 設定の表示：例 1107

第 61 章 **Power over Ethernet の設定** 1109
機能情報の確認 1109
Power over Ethernet の設定について 1109
Power over Ethernet の設定方法 1110
Power over Ethernet の設定（CLI） 1110
Power over Ethernet の設定例 1111
Power over Ethernet 情報の表示：例 1111

第 X 部： **モビリティ** 1113

第 62 章 **モビリティについて** 1115
概要 1115
有線およびワイヤレス モビリティ 1116
モビリティの機能 1117
低遅延ローミングを実現するスティッキ アンカリング 1118
ブリッジ ドメイン ID および L2/L3 ローミング 1119
リンク ダウンの動作 1119
モビリティ コントローラのプラットフォーム固有のスケール要件 1120

第 63 章 **モビリティ ネットワーク要素** 1121
Mobility Agent 1121
モビリティ コントローラ 1122
Mobility Oracle 1123
ゲスト コントローラ 1124

第 64 章 **モビリティ制御プロトコル** 1125
モビリティ制御プロトコルについて 1125
最初のアソシエーションとローミング 1125

最初のアソシエーション 1126
スイッチ内のハンドオフ 1128
スイッチ ピア グループ内のハンドオフ 1128
スイッチ ピア グループ間のハンドオフ 1129
サブ ドメイン間のハンドオフ 1130
モビリティ グループ間のハンドオフ 1131

第 65 章 モビリティの設定 1133
モビリティ コントローラの設定 1133
統合アクセス コントローラの設定 1133
ピア グループ、ピア グループ メンバー、ブリッジ ドメイン ID の作成（CLI） 1133
ローカル モビリティ グループの設定（CLI） 1135
ピア モビリティ グループの追加（CLI） 1136
ローミング動作のオプション パラメータの設定 1136
モビリティ コントローラの Mobility Oracle への指定（CLI） 1137
ゲスト コントローラの設定 1138
ゲスト アンカーの設定 1139
モビリティ エージェントの設定 1140
モビリティ コントローラの指定によるモビリティ エージェントの設定（CLI） 1140
モビリティ エージェントのモビリティ コントローラの設定（CLI） 1141
モビリティ エージェントへのモビリティ コントローラの役割の追加 1141
モビリティ エージェントのオプション パラメータの設定（CLI） 1142
モビリティ コントローラによるモビリティ エージェントの管理 1142
モビリティ コントローラによるモビリティ エージェントの管理 1142
モビリティ コントローラによるモビリティ エージェントの管理に関する制約事項 1143
機能の履歴 1143
モビリティ コントローラによるモビリティ エージェントの管理について 1144
分散モードと一元化モード 1144
モビリティ コントローラによるモビリティ エージェントの管理に関する制約事項 1146
MA を管理する MC の設定（CLI） 1146

第 XI 部： マルチプロトコル ラベル スイッチング（MPLS） 1157

第 66 章 マルチプロトコル ラベル スイッチング（MPLS） 1159

シスコ スイッチでのマルチプロトコル ラベル スイッチング 1159

機能情報の確認 1159

MPLS に関する情報 1159

MPLS の概要 1159

MPLS の機能の説明 1160

ラベル スイッチング機能 1160

ラベル バインディングの配布 1160

MPLS の設定方法 1161

MPLS スイッチング用のスイッチの設定 1161

MPLS スイッチングの構成の確認 1162

MPLS 転送用のスイッチの設定 1162

MPLS 転送の構成の確認 1163

MPLS レイヤ 3 VPN 1164

MPLS QoS EXP の分類とマーキング 1165

用語集 1165

第 67 章 マルチキャスト バーチャル プライベート ネットワークの設定 1167

マルチキャスト VPN の設定 1167

機能情報の確認 1167

マルチキャスト VPN の設定に関する前提条件 1168

マルチキャスト VPN の設定の制限 1168

マルチキャスト VPN の設定について 1168

マルチキャスト VPN の操作 1168

マルチキャスト VPN の利点 1168

マルチキャスト VPN ルーティングおよび転送とマルチキャスト ドメイン 1169

マルチキャスト配信ツリー 1169

マルチキャスト トンネル インターフェイス 1171

マルチキャスト VPN での BGP の MDT アドレス ファミリ 1172
マルチキャスト VPN の設定方法 1172
データ マルチキャスト グループの設定 1172
VRF のデフォルト MDT グループの設定 1174
マルチキャスト VPN での BGP の MDT アドレス ファミリの設定 1177
MDT デフォルト グループの情報の確認 1179
マルチキャスト VPN の設定例 1180
例：MVPN および SSM の設定 1180
例：マルチキャスト ルーティングの VPN のイネーブル化 1180
例：データ MDT グループ用のマルチキャスト グループ アドレス範囲の設定 1180
例：マルチキャスト ルートの数の制限 1180
マルチキャスト VPN の設定に関するその他の参考資料 1181

第 XII 部： **Network Management** 1183

第 68 章 **Cisco IOS Configuration Engine の設定** 1185
機能情報の確認 1185
Configuration Engine を設定するための前提条件 1185
Configuration Engine の設定に関する制約事項 1186
Configuration Engine の設定について 1186
Cisco Configuration Engine ソフトウェア 1186
コンフィギュレーション サービス 1187
イベント サービス 1188
名前空間マッパー 1188
Cisco Networking Service ID およびデバイスのホスト名 1188
ConfigID 1189
DeviceID 1189
ホスト名および DeviceID 1189
ホスト名、DeviceID、および ConfigID 1190
Cisco IOS CNS エージェント 1190
初期設定 1190

差分（部分的）設定 1191
コンフィギュレーションの同期 1191
自動 CNS 設定 1192
Configuration Engine の設定方法 1193
CNS イベント エージェントのイネーブル化 1193
Cisco IOS CNS エージェントのイネーブル化 1195
Cisco IOS CNS エージェントの初期設定のイネーブル化 1197
DeviceID の更新 1202
Cisco IOS CNS エージェントの部分的設定のイネーブル化 1204
CNS 設定のモニタリング 1206
その他の参考資料 1207

第 69 章 **Cisco Discovery Protocol の設定** 1209
機能情報の確認 1209
CDP に関する情報 1209
CDP の概要 1209
CDP のデフォルト設定 1210
CDP の設定方法 1210
CDP 特性の設定 1210
CDP のディセーブル化 1212
CDP のイネーブル化 1213
インターフェイス上での CDP のディセーブル化 1215
インターフェイス上での CDP のイネーブル化 1216
CDP のモニタおよびメンテナンス 1217
その他の参考資料 1219

第 70 章 **簡易ネットワーク管理プロトコルの設定** 1221
機能情報の確認 1221
SNMP の前提条件 1221
SNMP の制約事項 1224
SNMP に関する情報 1225

SNMP の概要 1225
SNMP マネージャ機能 1225
SNMP エージェント機能 1226
SNMP コミュニティ ストリング 1226
SNMP MIB 変数アクセス 1227
SNMP 通知 1227
SNMP ifIndex MIB オブジェクト値 1228
SNMP のデフォルト設定 1228
SNMP 設定時の注意事項 1228
SNMP の設定方法 1229
SNMP エージェントのディセーブル化 1229
コミュニティ ストリングの設定 1231
SNMP グループおよびユーザの設定 1234
SNMP 通知の設定 1237
エージェント コンタクトおよびロケーションの設定 1244
SNMP を通して使用する TFTP サーバの制限 1245
SNMP のトラップフラグの設定 1247
SNMP ワイヤレス トラップ通知のイネーブル化 1249
SNMP ステータスのモニタリング 1250
SNMP の例 1251
その他の参考資料 1252
簡易ネットワーク管理プロトコルの機能の履歴と情報 1253

第 71 章 サービス レベル契約の設定 1255
機能情報の確認 1255
SLA の制約事項 1255
SLA について 1256
Cisco IOS IP サービス レベル契約（SLA） 1256
Cisco IOS IP SLA でのネットワーク パフォーマンスの測定 1257
IP SLA レスポンダおよび IP SLA 制御プロトコル 1258
IP SLA の応答時間の計算 1259

IP SLA 動作のスケジューリング 1260
IP SLA 動作のしきい値のモニタリング 1260
UDP Jitter 1261
IP SLA 動作の設定方法 1262
デフォルト設定 1262
設定時の注意事項 1262
IP SLA レスポンダの設定 1263
IP SLA ネットワーク パフォーマンス測定の実装 1264
UDP ジッター動作を使用した IP サービス レベルの分析 1269
ICMP エコー動作を使用した IP サービス レベルの分析 1273
IP SLA 動作のモニタリング 1276
IP SLA 動作のモニタリングの例 1277
その他の参考資料 1278

第 72 章 ローカル ポリシーの設定 1281
機能情報の確認 1281
ローカル ポリシーの設定に関する制限 1281
ローカル ポリシーの設定に関する情報 1282
ローカル ポリシーの設定方法 1284
ローカル ポリシーの設定（CLI） 1284
インターフェイス テンプレートの作成（CLI） 1284
パラメータ マップの作成（CLI） 1285
クラス マップの作成（CLI） 1286
ポリシー マップの作成（CLI） 1287
WLAN 上のデバイスのローカル ポリシーの適用（CLI） 1288
ローカル ポリシーの監視 1289
例：ローカル ポリシーの設定 1290
ローカル ポリシーの設定に関する追加情報 1291
ローカル ポリシーの設定の実行に関する機能履歴 1292

第 73 章 SPAN および RSPAN の設定 1293

機能情報の確認 1293
SPAN および RSPAN の前提条件 1293
SPAN および RSPAN の制約事項 1294
SPAN および RSPAN について 1296
SPAN および RSPAN 1296
ローカル SPAN 1296
リモート SPAN 1298
SPAN と RSPAN の概念および用語 1299
SPAN および RSPAN と他の機能の相互作用 1305
SPAN と RSPAN とデバイス スタック 1307
フローベースの SPAN 1307
SPAN および RSPAN のデフォルト設定 1308
設定時の注意事項 1308
SPAN 設定時の注意事項 1308
RSPAN 設定時の注意事項 1309
FSPAN および FRSPAN 設定時の注意事項 1309
SPAN および RSPAN の設定方法 1310
ローカル SPAN セッションの作成 1310
ローカル SPAN セッションの作成および着信トラフィックの設定 1313
フィルタリングする VLAN の指定 1316
RSPAN VLAN としての VLAN の設定 1318
RSPAN 送信元セッションの作成 1320
フィルタリングする VLAN の指定 1322
RSPAN 宛先セッションの作成 1324
RSPAN 宛先セッションの作成および着信トラフィックの設定 1327
FSPAN セッションの設定 1329
FRSPAN セッションの設定 1333
SPAN および RSPAN 動作のモニタリング 1337
SPAN および RSPAN の設定例 1337
例：ローカル SPAN の設定 1337
例：RSPAN VLAN の作成 1338

その他の参考資料 1340
SPAN および RSPAN の機能の履歴と情報 1341

第 74 章 ERSPAN の設定 1343
ERSPAN の設定の前提条件 1343
ERSPAN 設定時の制約事項 1343
ERSPAN の設定に関する情報 1344
ERSPAN の概要 1344
ERSPAN 送信元 1345
ERSPAN の設定方法 1346
ERSPAN 送信元セッションの設定 1346
ERSPAN の設定例 1348
例：ERSPAN 送信元セッションの設定 1348
ERSPAN の確認 1348
その他の参考資料 1350
ERSPAN の設定に関する機能情報 1350

第 75 章 パケット キャプチャの設定 1353
パケット キャプチャの前提条件 1353
パケット キャプチャの前提条件 1353
パケット キャプチャの制約事項 1354
パケット キャプチャの制約事項 1354
パケット キャプチャの概要 1357
パケット キャプチャ ツールの概要 1357
Wireshark について 1358
Wireshark の概要 1358
キャプチャ ポイント 1358
接続ポイント 1359
Filters 1359
Actions 1360
キャプチャ パケットのメモリ内のバッファへのストレージ 1360

.pcap ファイルにキャプチャされたパケットのストレージ 1361
パケットのデコードおよび表示 1362
パケットのストレージおよび表示 1362
Wireshark キャプチャ ポイントのアクティブ化および非アクティブ化 1362
Wireshark 機能 1363
Wireshark のガイドライン 1365
デフォルトの Wireshark の設定 1368
組み込みパケット キャプチャについて 1369
組み込みパケット キャプチャの概要 1369
組み込みパケット キャプチャの利点 1369
パケット データ キャプチャ 1369
パケット キャプチャの設定 1370
Wireshark の設定方法 1370
キャプチャ ポイントの定義 1370
キャプチャ ポイント パラメータの追加または変更 1376
キャプチャ ポイント パラメータの削除 1378
キャプチャ ポイントの削除 1380
キャプチャ ポイントをアクティブまたは非アクティブにする 1381
キャプチャ ポイント バッファのクリア 1384
組み込みパケット キャプチャの実装方法 1386
パケット データ キャプチャの管理 1386
キャプチャされたデータのモニタリングとメンテナンス 1388
パケット キャプチャのモニタリング 1389
Wireshark の設定例 1389
例：.pcap ファイルからの概要出力の表示 1389
例：.pcap ファイルからの詳細出力の表示 1390
例：.pcap ファイルからパケット ダンプ出力の表示 1391
例：表示フィルタを使用した .pcap ファイルからのパケットの表示 1391
例：.pcap ファイルにキャプチャされたパケットの数を表示 1392
例：.pcap ファイルから単一パケット ダンプの表示 1392
例：.pcap ファイルにキャプチャされたパケットの統計情報を表示 1392

例：単純なキャプチャおよび表示 1393
例：単純なキャプチャおよび保存 1394
例：バッファのキャプチャの使用 1396
例：出力方向のパケットの簡単なキャプチャおよび保存 1403
組み込みパケット キャプチャの設定例 1404
例：パケット データ キャプチャの管理 1404
例：キャプチャされたデータのモニタリングとメンテナンス 1405
その他の参考資料 1407

第 76 章 **Flexible NetFlow の設定** 1409
Flexible NetFlow の前提条件 1409
Flexible Netflow に関する制約事項 1410
Flexible NetFlow に関する情報 1413
Flexible NetFlow の概要 1413
ワイヤレス Flexible NetFlow の概要 1413
以前の NetFlow と Flexible NetFlow の利点 1414
Flexible NetFlow のコンポーネント 1416
フロー レコード 1416
フロー エクスポータ 1421
フロー モニタ 1423
フロー サンプラー 1426
サポートされている Flexible NetFlow フィールド 1426
デフォルト設定 1432
Flexible NetFlow の設定方法 1432
カスタマイズしたフロー レコードの設定 1433
フロー エクスポータの作成 1436
カスタマイズしたフロー モニタの作成 1439
フロー サンプリングの設定および有効化フロー サンプラーの作成 1442
インターフェイスへのフローの適用 1443
VLAN 上でのブリッジ型 NetFlow の設定 1445
レイヤ 2 NetFlow の設定 1446

データ リンクの入出力方向にフロー モニタを適用する WLAN 設定 1447
IPV4 および IPv6 の入出力方向にフロー モニタを適用する WLAN 設定 1448
Flexible NetFlow の監視 1449
Flexible NetFlow の設定例 1449
例：フローの設定 1449
例：IPv4 入力トラフィックのモニタリング 1450
例：IPv4 出力トラフィックのモニタリング 1451
例：WLAN（入力方向）の IPv4 Flexible NetFlow の設定 1452
例：WLAN（出力方向）の IPv6 および転送フラグ Flexible NetFlow の設定 1453
例：WLAN（入力および出力の両方向）の IPv6 Flexible NetFlow の設定 1453
例：ワイヤレス入力トラフィックのモニタリング 1454
その他の参考資料 1455
Flexible NetFlow の機能情報 1456

第 XIII 部： **Network Powered Lighting** 1457

第 77 章 **COAP プロキシ サーバの設定** 1459
機能情報の確認 1459
COAP プロキシ サーバについて 1459
COAP の制約事項 1460
COAP プロキシ サーバでサポートされるハードウェア 1460
COAP プロキシ サーバの設定 1463
COAP プロキシの設定 1464
COAP エンドポイントの設定 1467
COAP プロキシ サーバのモニタリング 1468
例：COAP プロキシ サーバ 1469

第 78 章 **Autosmart ポートの設定** 1475
機能情報の確認 1475
Autosmart ポートに関する情報 1475
Autosmart ポート マクロ 1476

CISCO_LIGHT_AUTO_SMARTPORT によって実行されるコマンド 1476
Autosmart ポートのイネーブル化 1477
例：AutoSmart ポートのイネーブル化 1478

第 79 章 **2 イベント分類の設定 1479**
機能情報の確認 1479
2 イベント分類について 1479
2 イベント分類の設定 1480
例：2 イベント分類の設定 1480

第 80 章 **無停止型 POE の設定 1483**
機能情報の確認 1483
無停止型 POE 1483
高速 POE 1484
無停止型 POE および高速 POE 向けにサポートされるハードウェア 1484
POE の設定 1487
例：無停止型 POE の設定 1488

第 81 章 **FAQ 1489**
機能情報の確認 1489
FAQ 1489

第 XIV 部： **QoS 1493**

第 82 章 **QoS の設定 1495**
機能情報の確認 1496
自動 QoS の前提条件 1496
自動 QoS の制約事項 1496
自動 QoS の設定に関する情報 1497
自動 QoS の概要 1497
自動 QoS 短縮機能の概要 1498

自動 QoS グローバル設定テンプレート 1498
自動 QoS ポリシーとクラス マップ 1498
実行コンフィギュレーションでの自動 QoS の影響 1499
実行コンフィギュレーションでの自動 QoS 短縮機能の影響 1499
自動 QoS の設定方法 1500
自動 QoS の設定（CLI） 1500
自動 QoS のアップグレード（CLI） 1503
自動 QoS 短縮機能のイネーブル化 1505
自動 QoS の監視 1507
自動 QoS に関するトラブルシューティング 1507
自動 QoS の設定例 1508
例：auto qos trust cos 1508
例：auto qos trust dscp 1510
例：auto qos video cts 1513
例：auto qos video ip-camera 1516
例：auto qos video media-player 1519
例：auto qos voip trust 1521
例：auto qos voip cisco-phone 1524
例：auto qos voip cisco-softphone 1528
auto qos classify police 1533
auto qos global compact 1537
自動 QoS の関連情報 1537
自動 QoS に関する追加情報 1538
自動 QoS の機能履歴と情報 1539
機能情報の確認 1539
QoS の前提条件 1539
QoS コンポーネント 1540
QoS の用語 1541
QoS の概要 1541
QoS の概要 1541
モジュラ QoS コマンドライン インターフェイス 1541

ワイヤレス QoS の概要 1542
ワイヤレス用の QoS および IPv6 1543
有線およびワイヤレス アクセスでサポートされる機能 1543
ワイヤレス ターゲットでサポートされる QoS 機能 1545
ポート ポリシー 1547
無線ポリシー 1549
SSID ポリシー 1550
クライアント ポリシー 1550
階層型 QoS 1551
階層型ワイヤレス QoS 1552
QoS の実装 1553
レイヤ 2 フレームのプライオリティ ビット 1554
レイヤ 3 パケットのプライオリティ ビット 1555
分類を使用したエンドツーエンドの QoS ソリューション 1555
パケット分類 1555
QoS 有線モデル 1558
入力ポートのアクティビティ 1558
出力ポートのアクティビティ 1559
分類 1559
アクセス コントロール リスト 1559
クラス マップ 1560
ポリシー マップ 1561
ポリシング 1563
トークンバケット アルゴリズム 1564
マーキング 1564
パケット ヘッダーのマーキング 1565
スイッチ固有の情報のマーキング 1565
テーブル マップのマーキング 1565
トラフィックの調整 1567
ポリシング 1568
シェーピング 1569

キューイングおよびスケジューリング 1571
帯域幅 1572
重み付けテール ドロップ 1573
プライオリティ キュー 1574
キュー バッファ 1574
ワイヤレスでのキューイング 1576
信頼動作 1577
有線およびワイヤレス ポートの信頼動作 1577
Cisco IP Phone の信頼境界機能のポート セキュリティ 1578
ワイヤレス QoS モビリティ 1579
デバイス間ローミング 1579
デバイス内ローミング 1580
ワイヤレス QoS の貴金属ポリシー 1580
標準 QoS のデフォルト設定 1581
デフォルトの有線 QoS 設定 1581
デフォルトのワイヤレス QoS 設定 1583
QoS ポリシーのガイドライン 1583
有線ターゲットの QoS に関する制約事項 1583
ワイヤレス ターゲットの QoS に関する制約事項 1587
QoS の設定方法 1590
クラス、ポリシー、およびテーブル マップの設定 1590
トラフィック クラスの作成（CLI） 1590
トラフィック ポリシーの作成（CLI） 1593
クライアント ポリシーの設定 1598
クラスベースのパケット マーキングの設定（CLI） 1599
音声およびビデオに対するクラス マップの設定（CLI） 1605
トラフィック ポリシーのインターフェイスへの付加（CLI） 1606
WLAN での SSID またはクライアント ポリシーの適用（CLI） 1608
ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング（CLI） 1609

ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング（CLI） 1613
テーブル マップの設定（CLI） 1617
信頼の設定 1620
ワイヤレス トラフィックの信頼動作の設定（CLI） 1620
QoS の特性と機能の設定 1621
コール アドミッション制御の設定（CLI） 1621
帯域幅の設定（CLI） 1628
ポリシングの設定（CLI） 1631
プライオリティの設定（CLI） 1634
キューとシェーピングの設定 1636
出力キューの特性の設定 1636
キュー バッファの設定（CLI） 1637
キュー制限の設定（CLI） 1640
シェーピングの設定（CLI） 1643
貴金属ポリシーの設定（CLI） 1644
QoS のモニタリング 1646
QoS の設定例 1650
例：アクセス コントロール リストによる分類 1650
例：サービス クラス レイヤ 2 の分類 1650
例：サービス クラス DSCP の分類 1651
例：VLAN ID レイヤ 2 の分類 1651
例：DSCP 値または precedence 値による分類 1651
例：階層型分類 1652
例：階層型ポリシーの設定 1652
例：音声およびビデオの分類 1653
例：音声、ビデオ、およびマルチキャスト トラフィックで分類されたワイヤレス QoS ポリシー 1654
例：ダウンストリーム SSID ポリシーの設定 1655
例：入力 SSID ポリシー 1656
例：クライアント ポリシー 1657

例：平均レート シェーピングの設定 1660
例：キュー制限の設定 1661
例：キュー バッファの設定 1662
例：ポリシング アクションの設定 1662
例：ポリサーの VLAN 設定 1663
例：ポリシングの単位 1663
例：シングルレート 2 カラー ポリシング設定 1664
例：デュアルレート 3 カラー ポリシング設定 1665
例：テーブル マップのマーキング設定 1665
例：CoS マーキングを保持するテーブル マップの設定 1666
次の作業 1667
QoS に関する追加情報 1667
QoS の機能履歴と情報 1669

第 XV 部： 無線リソース管理 1671

第 83 章 無線リソース管理の設定 1673
機能情報の確認 1673
無線リソース管理の設定の前提条件 1673
無線リソース管理の制約事項 1674
無線リソース管理について 1674
無線リソースの監視 1675
RF グループについて 1675
RF グループ リーダー 1676
RF グループ名 1678
モビリティ コントローラ 1678
Mobility Agent 1679
RF グループ内の不正アクセス ポイント検出について 1679
送信電力の制御 1679
最小/最大送信電力の設定による TPC アルゴリズムの無効化 1680
チャネルの動的割り当て 1680

カバレッジ ホールの検出と修正 1683
RRM の設定方法 1683
高度な RRM CCX パラメータの設定（CLI） 1683
ネイバー探索タイプの設定（CLI） 1684
RRM プロファイルしきい値、監視チャネル、および監視間隔の設定（GUI） 1684
RF グループの設定 1686
RF グループ モードの設定（GUI） 1686
RF グループ選択モードの設定（CLI） 1687
RF グループ名の設定（CLI） 1688
RF グループ名の設定（GUI） 1689
802.11 静的 RF グループのメンバの設定（CLI） 1689
送信電力制御の設定 1690
送信電力制御のしきい値の設定（CLI） 1690
送信電力レベルの設定（CLI） 1690
送信電力制御の設定（GUI） 1691
802.11 RRM パラメータの設定 1692
高度な 802.11 チャネル割り当てパラメータの設定（CLI） 1692
動的チャネル割り当ての設定（GUI） 1695
802.11 カバレッジ ホール検出の設定（CLI） 1697
カバレッジ ホールの検出の設定（GUI） 1698
802.11 イベント ロギングの設定（CLI） 1700
802.11 統計情報の監視の設定（CLI） 1701
802.11 パフォーマンス プロファイルの設定（CLI） 1702
RF グループ内の不正アクセス ポイント検出の設定 1703
RF グループ内の不正アクセス ポイント検出の設定（CLI） 1703
RF グループ内の不正アクセス ポイント検出の有効化（GUI） 1704
RRM パラメータと RF グループ ステータスの監視 1705
RRM パラメータの監視 1705
RF グループ ステータスの監視（CLI） 1706
RF グループ ステータスの監視（GUI） 1707
例：RF グループの設定 1707

ED-RRM について 1708
Cisco ワイヤレス LAN コントローラで ED-RRM の設定（CLI） 1708
ED-RRM の設定（GUI） 1709
無線リソース管理に関するその他の参考ドキュメント 1709
無線リソース管理の設定を行うための機能履歴と情報 1710

第 84 章 **Cisco 2800/3800 シリーズ アクセス ポイントの XOR スロットの設定 1711**
XOR 無線に関する情報 1711
XOR 無線の設定（GUI） 1711
XOR 無線の設定（CLI） 1712
XOR 無線パラメータのモニタリング 1713

第 85 章 **Cisco 2800/3800 シリーズ アクセス ポイントの Flexible Radio Assignment の設定 1715**
Flexible Radio Assignment（FRA）に関する情報 1715
カバレッジ オーバーラップ ファクタ（COF） 1716
無線の役割の割り当て（Radio Role Assignment） 1717
クライアントネットワーク設定 1717
定常状態の動作 1718
FRA とデュアル 5-GHz の動作 1718
Flexible Radio Assignment の設定（CLI） 1719
クライアント ネットワーク設定（CLI）の構成 1720
Flexible Radio Assignment のリセット（CLI） 1720
マイクロ/マクロ モードの設定（CLI） 1721
マクロ/マイクロ遷移しきい値のモニタリング（CLI） 1721
プローブ抑制の設定（CLI） 1722
Flexible Radio Assignment のデバッグ（CLI） 1723

第 86 章 **設定の最適化されたローミング 1725**
ローミングの最適化について 1725
ローミングの最適化の制約事項 1726
ローミングの最適化の設定（CLI） 1726

第 87 章 設定の Rx SOP 1729
Rx-SOP に関する情報 1729
Rx SOP の設定（CLI） 1729

第 88 章 AirTime Fairness の設定 1731
Air Time Fairness について 1731
AirTime Fairness の設定、表示、および変更 1733
Cisco Air Time Fairness の設定（CLI） 1733
Cisco Air Time Fairness の表示（CLI） 1734
AP の AirTime Fairness パラメータの変更（CLI） 1735

第 89 章 CA での RF プロファイルの設定 1737
CA での RF プロファイルの前提条件 1737
CA での RF プロファイルの制約事項 1737
CA での RF プロファイルについて 1738
RF プロファイルのカスタマイズ 1739
バンド選択設定 1739
カバレッジ ホール軽減設定 1739
動的チャネル割り当て設定 1740
高密度設定 1740
ロード バランシング設定 1741
スタジアム ビジョン設定 1741
伝送パワー コントロール設定 1741
CA での RF プロファイルの設定方法 1741
RF プロファイル パラメータの設定 1741

第 XVI 部： ルーティング 1745

第 90 章 双方向フォワーディング検出の設定 1747
双方向フォワーディング検出 1747

機能情報の確認 1747
双方向フォワーディング検出の前提条件 1747
双方向フォワーディング検出の制約事項 1748
双方向フォワーディング検出について 1748
BFD の動作 1748
障害検出に BFD を使用することの利点 1752
双方向フォワーディング検出の設定方法 1753
インターフェイスでの BFD セッション パラメータの設定 1753
ダイナミック ルーティング プロトコルに対する BFD サポートの設定 1754
スタティック ルーティングに対する BFD サポートの設定 1766
BFD エコー モードの設定 1768
BFD テンプレートの作成と設定 1770
BFD のモニタリングとトラブルシューティング 1771

第 91 章 **MSDP の設定** 1773
機能情報の確認 1773
MSDP の設定について 1773
MSDP の概要 1774
MSDP の動作 1774
MSDP の利点 1776
MSDP の設定方法 1776
MSDP のデフォルト設定 1776
デフォルトの MSDP ピアの設定 1776
SA ステートのキャッシング 1779
MSDP ピアからの送信元情報の要求 1781
スイッチから発信される送信元情報の制御 1782
送信元の再配信 1782
SA 要求メッセージのフィルタリング 1785
スイッチで転送される送信元情報の制御 1787
フィルタの使用法 1787
SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限 1790

スイッチで受信される送信元情報の制御 1791
MSDP メッシュ グループの設定 1793
MSDP ピアのシャットダウン 1795
境界 PIM デンス モード領域の MSDP への包含 1796
RP アドレス以外の発信元アドレスの設定 1797
MSDP のモニタリングおよびメンテナンス 1799
MSDP の設定例 1800
デフォルト MSDP ピアの設定：例 1800
SA ステートのキャッシング：例 1800
MSDP ピアからの送信元情報の要求：例 1800
スイッチから発信される送信元情報の制御：例 1801
スイッチから転送される送信元情報の制御：例 1801
スイッチで受信される送信元情報の制御：例 1801

第 92 章 **IP ユニキャスト ルーティングの設定** 1803
機能情報の確認 1804
IP ユニキャスト ルーティングの設定に関する情報 1804
IP ルーティングに関する情報 1804
ルーティング タイプ 1805
IP ルーティングおよびスイッチ スタック 1806
クラスレス ルーティング 1808
アドレス解決 1809
プロキシ ARP 1810
ICMP Router Discovery Protocol 1811
UDP ブロードキャスト パケットおよびプロトコル 1811
ブロードキャスト パケットの処理 1812
IP ブロードキャストのフラッディング 1812
IP ルーティングの設定方法 1813
IP アドレッシングの設定方法 1814
IP アドレス指定のデフォルト設定 1815
ネットワーク インターフェイスへの IP アドレスの割り当て 1816

サブネット ゼロの使用 1818
クラスレス ルーティングのディセーブル化 1819
アドレス解決方法の設定 1820
スタティック ARP キャッシュの定義 1820
ARP のカプセル化の設定 1822
プロキシ ARP のイネーブル化 1823
IP ルーティングがディセーブルの場合のルーティング支援機能 1824
プロキシ ARP 1824
デフォルト ゲートウェイ 1824
ICMP Router Discovery Protocol（IRDP） 1825
ブロードキャスト パケットの処理方法の設定 1828
ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化 1828
UDP ブロードキャスト パケットおよびプロトコルの転送 1830
IP ブロードキャスト アドレスの確立 1832
IP ブロードキャストのフラッディング 1833
IP アドレスのモニタリングおよびメンテナンス 1834
IP ユニキャスト ルーティングの設定方法 1836
IP ユニキャスト ルーティングのイネーブル化 1836
IP ルーティングのイネーブル化の例 1837
次の作業 1837
RIP 情報 1837
サマリー アドレスおよびスプリット ホライズン 1838
RIP の設定方法 1838
RIP のデフォルト設定 1838
基本的な RIP パラメータの設定 1839
RIP 認証の設定 1842
サマリー アドレスおよびスプリット ホライズンの設定 1844
スプリット ホライズンの設定 1845
サマリー アドレスおよびスプリット ホライズンの設定例 1847
OSPF に関する情報 1847
OSPF NSF 1848

OSPF NSF 認識 1848
OSPF NSF 対応 1848
OSPF エリア パラメータ 1849
その他の OSPF パラメータ 1850
LSA グループ ペーシング 1851
ループバック インターフェイス 1851
OSPF の設定方法 1852
OSPF のデフォルト設定 1852
基本的な OSPF パラメータの設定 1854
OSPF インターフェイスの設定 1855
OSPF エリア パラメータの設定 1858
その他の OSPF パラメータの設定 1860
LSA グループ ペーシングの変更 1862
ループバック インターフェイスの設定 1863
OSPF の監視 1864
OSPF の設定例 1865
例：基本的な OSPF パラメータの設定 1865
EIGRP に関する情報 1866
EIGRP の機能 1866
EIGRP コンポーネント 1866
EIGRP NSF 1867
EIGRP NSF 認識 1868
EIGRP NSF 対応 1868
EIGRP スタブ ルーティング 1869
EIGRP の設定方法 1870
EIGRP のデフォルト設定 1870
基本的な EIGRP パラメータの設定 1872
EIGRP インターフェイスの設定 1874
EIGRP ルート認証の設定 1876
EIGRP のモニタリングおよびメンテナンス 1878
BGP に関する情報 1878

BGP ネットワーク トポロジ 1879
NSF 認識 1880
BGP ルーティングに関する情報 1881
ルーティング ポリシーの変更 1881
BGP 判断属性 1882
ルート マップ 1884
BGP フィルタリング 1884
BGP フィルタリングのプレフィックス リスト 1884
BGP コミュニティ フィルタリング 1885
BGP ネイバーおよびピア グループ 1886
集約ルート 1886
ルーティング ドメイン コンフェデレーション 1886
BGP ルート リフレクタ 1886
ルート ダンプニング 1887
BGP の追加情報 1887
BGP の設定方法 1888
BGP のデフォルト設定 1888
BGP ルーティングのイネーブル化 1893
ルーティング ポリシー変更の管理 1896
BGP 判断属性の設定 1897
ルート マップによる BGP フィルタリングの設定 1899
ネイバーによる BGP フィルタリングの設定 1900
アクセス リストおよびネイバーによる BGP フィルタリングの設定 1902
BGP フィルタリング用のプレフィックス リストの設定 1903
BGP コミュニティ フィルタリングの設定 1904
BGP ネイバーおよびピア グループの設定 1906
ルーティング テーブルでの集約アドレスの設定 1909
ルーティング ドメイン連合の設定 1911
BGP ルート リフレクタの設定 1912
ルート ダンプニングの設定 1913
BGP のモニタリングおよびメンテナンス 1915

BGP の設定例 1916
例：ルータでの BGP の設定 1916
ISO CLNS ルーティングに関する情報 1918
コネクションレス型ルーティング 1918
IS-IS ダイナミック ルーティング 1919
NSF 認識 1920
IS-IS グローバル パラメータ 1920
IS-IS インターフェイス パラメータ 1921
ISO CLNS ルーティングの設定方法 1922
IS-IS のデフォルト設定 1922
IS-IS ルーティングのイネーブル化 1923
IS-IS グローバル パラメータの設定 1926
IS-IS インターフェイス パラメータの設定 1930
ISO IGRP と IS-IS のモニタリングおよびメンテナンス 1933
ISO CLNS ルーティングの設定例 1935
例：IS-IS ルーティングの設定 1935
Multi-VRF CE に関する情報 1936
Multi-VRF CE の概要 1937
ネットワーク トポロジ 1937
パケット転送処理 1938
ネットワーク コンポーネント 1939
VRF 認識サービス 1939
Multi-VRF CE の設定方法 1940
Multi-VRF CE のデフォルト設定 1940
Multi-VRF CE の設定時の注意事項 1941
VRF の設定 1943
VRF 認識サービスの設定 1944
ARP 用 VRF 認識サービスの設定 1945
ping 用 VRF 認識サービスの設定 1945
SNMP 用 VRF 認識サービスの設定 1946
uRPF 用 VRF 認識サービスの設定 1947

VRF 認識 RADIUS の設定 1948
syslog 用 VRF 認識サービスの設定 1948
traceroute 用 VRF 認識サービスの設定 1949
FTP および TFTP 用 VRF 認識サービスの設定 1950
マルチキャスト VRF の設定 1951
VPN ルーティング セッションの設定 1953
BGP PE/CE ルーティング セッションの設定 1954
Multi-VRF CE のモニタリング 1956
Multi-VRF CE の設定例 1956
Multi-VRF CE の設定例 1956
ユニキャスト リバース パス転送の設定 1960
プロトコル独立機能 1961
分散型シスコ エクスプレス フォワーディング 1961
シスコ エクスプレス フォワーディングに関する情報 1961
シスコ エクスプレス フォワーディングの設定方法 1962
等コスト ルーティング パスの個数 1964
等コスト ルーティング パスに関する情報 1964
等コスト ルーティング パスの設定方法 1964
スタティック ユニキャスト ルート 1965
スタティック ユニキャスト ルートに関する情報 1965
スタティック ユニキャスト ルートの設定 1966
デフォルトのルートおよびネットワーク 1967
デフォルトのルートおよびネットワークに関する情報 1967
デフォルトのルートおよびネットワークの設定方法 1968
ルーティング情報を再配信するためのルート マップ 1969
ルート マップの概要 1969
ルート マップの設定方法 1969
ルート配信の制御方法 1974
Policy-Based Routing：ポリシーベース ルーティング 1976
ポリシーベース ルーティングの概要 1976
PBR の設定方法 1977

ルーティング情報のフィルタリング 1980
受動インターフェイスの設定 1981
ルーティング アップデートのアドバタイズおよび処理の制御 1982
ルーティング情報の送信元のフィルタリング 1983
認証キーの管理 1985
前提条件 1985
認証キーの設定方法 1985
IP ネットワークのモニタリングおよびメンテナンス 1986

第 XVII 部： セキュリティ 1989

第 93 章 不正アクセスの防止 1991
機能情報の確認 1991
不正アクセスの防止 1991

第 94 章 パスワードおよび権限レベルによるスイッチ アクセスの制御 1993
機能情報の確認 1993
パスワードおよび権限によるスイッチ アクセスの制御の制約事項 1993
パスワードおよび権限レベルに関する情報 1994
デフォルトのパスワードおよび権限レベル設定 1994
追加のパスワード セキュリティ 1994
パスワードの回復 1995
端末回線の Telnet 設定 1995
ユーザ名とパスワードのペア 1996
権限レベル 1996
パスワードおよび権限レベルでスイッチ アクセスを制御する方法 1997
スタティック イネーブル パスワードの設定または変更 1997
暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 1998
パスワード回復のディセーブル化 2001
端末回線に対する Telnet パスワードの設定 2002
ユーザ名とパスワードのペアの設定 2004

コマンドの特権レベルの設定 2006
回線のデフォルト特権レベルの変更 2007
権限レベルへのログインおよび終了 2008
スイッチ アクセスのモニタリング 2009
パスワードおよび権限レベルの設定例 2009
例：スタティック イネーブル パスワードの設定または変更 2009
例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 2010
例：端末回線に対する Telnet パスワードの設定 2010
例：コマンドの権限レベルの設定 2010
その他の参考資料 2011

第 95 章 「Configuring TACACS+」 2013
機能情報の確認 2013
TACACS+ の前提条件 2013
TACACS+ の概要 2015
TACACS+ およびスイッチ アクセス 2015
TACACS+ の概要 2015
TACACS+ の動作 2017
方式リスト 2018
TACACS+ 設定オプション 2018
TACACS+ ログイン認証 2018
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可 2018
TACACS+ アカウンティング 2019
TACACS+ のデフォルト設定 2019
TACACS+ を設定する方法 2019
TACACS+ サーバ ホストの指定および認証キーの設定 2020
TACACS+ ログイン認証の設定 2021
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定 2024
TACACS+ アカウンティングの起動 2026
AAA サーバが到達不能な場合のルータとのセッションの確立 2027
TACACS+ のモニタリング 2027

第 96 章 **MACsec の暗号化** 2029

機能情報の確認 2029

MACsec 暗号化について 2029

Media Access Control Security と MACsec Key Agreement 2030

MKA ポリシー 2031

仮想ポート 2031

MACsec およびスタッキング 2032

MACsec、MKA、および 802.1x ホスト モード 2032

MKA および MACsec の設定 2038

MACsec MKA のデフォルト設定 2038

MKA ポリシーの設定 2039

インターフェイスでの MACsec の設定 2040

PSK を使用した MACsec MKA の設定 2043

PSK を使用した、インターフェイスでの MACsec MKA の設定 2044

EAP-TLS を使用した MACsec MKA の理解 2045

EAP-TLS を使用した MACsec MKA の前提条件 2045

EAP-TLS を使用した MACsec MKA の制限事項 2045

EAP-TLS を使用した MACsec MKA の設定 2045

リモート認証 2046

キー ペアの生成 2046

SCEP による登録の設定 2047

登録の手動設定 2048

802.1x 認証の有効化と AAA の設定 2051

EAP-TLS プロファイルと 802.1x クレデンシャルの設定 2052

インターフェイスでの 802.1x MACsec MKA 設定の適用 2053

ローカル認証 2054

ローカル認証を使用した EAP クレデンシャルの設定 2054

ローカル EAP-TLS 認証と認証プロファイルの設定 2055

SCEP による登録の設定 2056

登録の手動設定 2058

EAP-TLS プロファイルと 802.1x クレデンシャルの設定 2060
インターフェイスでの 802.1x MKA MACsec 設定の適用 2061
EAP-TLS を使用した MACsec MKA の確認 2062
Cisco TrustSecMACsec に関する情報 2064
Cisco TrustSec MACsec の設定 2066
手動モードでの Cisco TrustSec スイッチ間リンク セキュリティの設定 2066
設定例 2068
インターフェイスでの MACsec の設定 2068
EAP-TLS を使用した MACsec MKA の設定例 2071
例: : 証明書の登録 2071
例 : 802.1x 認証の有効化と AAA の設定 2071
例 : EAP-TLS プロファイルと 802.1x クレデンシャルの設定 2072
例 : インターフェイスでの 802.1 X、PKI、および MACsec の設定の適用 2072
Cisco TrustSec スイッチ間リンク セキュリティの設定例 2072

第 97 章 **RADIUS の設定** 2075
機能情報の確認 2075
RADIUS を設定するための前提条件 2075
RADIUS の設定に関する制約事項 2076
RADIUS に関する情報 2077
RADIUS およびスイッチ アクセス 2077
RADIUS の概要 2077
RADIUS の動作 2078
RADIUS 許可の変更 2079
Change-of-Authorization 要求 2081
CoA 要求応答コード 2082
CoA 要求コマンド 2084
セッション強制終了のスタック構成ガイドライン 2087
RADIUS のデフォルト設定 2088
RADIUS サーバ ホスト 2088
RADIUS ログイン認証 2089

AAA Server Groups 2089
AAA Authorization 2090
RADIUS アカウンティング 2090
ベンダー固有の RADIUS 属性 2090
ベンダー独自仕様の RADIUS サーバ通信 2105
RADIUS の設定方法 2106
RADIUS サーバ ホストの識別 2106
RADIUS ログイン認証の設定 2108
AAA サーバ グループの定義 2111
ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定 2113
RADIUS アカウンティングの起動 2114
すべての RADIUS サーバの設定 2116
ベンダー固有の RADIUS 属性を使用するデバイス設定 2117
ベンダー独自の RADIUS サーバとの通信に関するデバイスの設定 2119
デバイス 上での CoA の設定 2120
CoA 機能のモニタリング 2123
その他の参考資料 2124

第 98 章 **RADIUS over DTLS の設定** 2127
機能情報の確認 2127
RADIUS over DTLS の前提条件 2127
RADIUS over DTLS に関する情報 2128
RADIUS over DTLS を設定する方法 2128
DTLS サーバを設定する方法 2128
DTLS CoA 用にダイナミック認証を設定する方法 2129
RADIUS over DTLS のモニタリング 2131
RADIUS over DTLS の設定例 2132

第 99 章 **Kerberos の設定** 2133
機能情報の確認 2133

Kerberos によるスイッチ アクセスの制御の前提条件 2133
Kerberos に関する情報 2134
Kerberos とスイッチ アクセス 2134
Kerberos の概要 2134
Kerberos の動作 2137
境界スイッチに対する認証の取得 2137
KDC からの TGT の取得 2137
ネットワーク サービスに対する認証の取得 2138
Kerberos を設定する方法 2138
Kerberos 設定の監視 2138
その他の参考資料 2138

第 100 章 ローカル認証および許可の設定 2141
機能情報の確認 2141
ローカル認証および許可の設定方法 2141
スイッチのローカル認証および許可の設定 2141
ローカル認証および許可のモニタリング 2144
その他の参考資料 2144

第 101 章 セキュア シェル（SSH）の設定 2147
機能情報の確認 2147
セキュア シェルを設定するための前提条件 2147
セキュア シェルの設定に関する制約事項 2148
SSH に関する情報 2149
SSH およびスイッチ アクセス 2149
SSH サーバ、統合クライアント、およびサポートされているバージョン 2149
SSH 設定時の注意事項 2150
セキュア コピー プロトコルの概要 2151
セキュア コピー プロトコル 2151
SSH の設定方法 2152
SSH を実行するためのDeviceの設定 2152

SSH サーバの設定 2153
SSH の設定およびステータスのモニタリング 2156
その他の参考資料 2156
SSH の機能情報 2157

第 102 章 **SSH 認証の X.509v3 証明書 2159**
SSH 認証の X.509v3 証明書 2159
機能情報の確認 2159
SSH 認証の X.509v3 証明書 の前提条件 2159
SSH 認証の X.509v3 証明書 の制約事項 2160
SSH 認証用の X.509v3 証明書に関する情報 2160
デジタル証明書 2160
X.509v3 を使用したサーバおよびユーザ認証 2160
SSH 認証用の X.509v3 証明書の設定方法 2161
サーバ認証にデジタル証明書を使用するための IOS SSH サーバの設定 2161
ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定 2162
デジタル証明書を使用したサーバおよびユーザ認証の設定の確認 2164
SSH 認証用の X.509v3 証明書の設定例 2165
例：サーバ認証にデジタル証明書を使用するための IOS SSH サーバの設定 2165
例：ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定 2165
SSH 認証の X.509v3 証明書に関する追加情報 2165
SSH 認証の X.509v3 証明書 の機能情報 2166

第 103 章 **Secure Socket Layer HTTP の設定 2169**
機能情報の確認 2169
Secure Sockets Layer（SSL）HTTP に関する情報 2169
セキュア HTTP サーバおよびクライアントの概要 2169
CA のトラストポイント 2170
CipherSuite 2172
SSL のデフォルト設定 2173

SSL の設定時の注意事項 2173
セキュア HTTP サーバおよびクライアントの設定方法 2173
CA のトラストポイントの設定 2173
セキュア HTTP サーバの設定 2175
セキュア HTTP クライアントの設定 2180
セキュア HTTP サーバおよびクライアントのステータスのモニタリング 2181
その他の参考資料 2181

第 104 章 **IPv4 ACL の設定** 2185
機能情報の確認 2185
IPv4 アクセス コントロール リストを設定するための前提条件 2185
IPv4 アクセス コントロール リストの設定に関する制約事項 2186
ACL によるネットワーク セキュリティに関する情報 2187
ACL の概要 2188
アクセス コントロール エントリ 2188
ACL でサポートされるタイプ 2188
サポートされる ACL 2189
ACL 優先順位 2189
ポート ACL 2190
ルータ ACL 2191
VLAN マップ 2192
ACEおよびフラグメント化されるトラフィックとフラグメント化されていないトラフィック 2192
ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例 2193
ACL とスイッチ スタック 2194
アクティブ スイッチおよび ACL の機能 2194
スタック メンバおよび ACL の機能 2194
アクティブ スイッチの障害および ACL 2194
標準 IPv4 ACL および拡張 IPv4 ACL 2194
IPv4 ACL スイッチでサポートされていない機能 2195

アクセス リスト番号 2195
番号付き標準 IPv4 ACL 2196
番号付き拡張 IPv4 ACL 2196
名前付き IPv4 ACL 2197
ACL ロギング 2198
ハードウェアおよびソフトウェアによる IP ACL の処理 2199
VLAN マップの設定時の注意事項 2199
VLAN マップとルータ ACL 2200
VLAN マップとルータ ACL の設定時の注意事項 2200
ACL の時間範囲 2201
IPv4 ACL のインターフェイスに関する注意事項 2202
ACL の設定方法 2203
IPv4 ACL の設定 2203
番号付き標準 ACL の作成 2203
番号付き拡張 ACL の作成 2205
名前付き標準 ACL の作成 2210
名前付き拡張 ACL の作成 2211
ACL の時間範囲の設定 2213
端末回線への IPv4 ACL の適用 2214
インターフェイスへの IPv4 ACL の適用 2216
名前付き MAC 拡張 ACL の作成 2217
レイヤ 2 インターフェイスへの MAC ACL の適用 2219
VLAN マップの設定 2220
VLAN マップの作成 2222
VLAN への VLAN マップの適用 2224
IPv4 ACL のモニタリング 2225
ACL の設定例 2226
例：ACL での時間範囲を使用 2226
例：ACL へのコメントの挿入 2227
IPv4 ACL の設定例 2228
小規模ネットワークが構築されたオフィス用の ACL 2228

例：小規模ネットワークが構築されたオフィスの ACL 2228
例：番号付き ACL 2229
例：拡張 ACL 2229
例：名前付き ACL 2230
例：IP ACL に適用される時間範囲 2231
例：コメント付き IP ACL エントリの設定 2232
例：ACL ロギング 2232
ACL および VLAN マップの設定例 2234
例：パケットを拒否する ACL および VLAN マップの作成 2234
例：パケットを許可する ACL および VLAN マップの作成 2234
例：IP パケットのドロップおよび MAC パケットの転送のデフォルト アクション 2234
例：MAC パケットのドロップおよび IP パケットの転送のデフォルト アクション 2235
例：すべてのパケットをドロップするデフォルト アクション 2235
ネットワークでの VLAN マップの使用方法の設定例 2236
例：ワイヤリング クローゼットの設定 2236
例：別の VLAN にあるサーバへのアクセスの制限 2237
例：別の VLAN にあるサーバへのアクセスの拒否 2237
VLAN に適用されるルータ ACL と VLAN マップの設定例 2238
例：ACL およびスイッチド パケット 2238
例：ACL およびブリッジド パケット 2239
例：ACL およびルーテッド パケット 2239
例：ACL およびマルチキャスト パケット 2240
その他の参考資料 2241

第 105 章 **IPv6 ACL の設定** 2243
機能情報の確認 2243
IPv6 ACL の概要 2243
スイッチ スタックおよび IPv6 ACL 2244
ACL 優先順位 2244
VLAN マップ 2245
他の機能およびスイッチとの相互作用 2246

IPv6 ACL の制限 2246
IPv6 ACL のデフォルト設定 2247
IPv6 ACL の設定 2247
インターフェイスへの IPv6 ACL の付加 2252
VLAN マップの設定 2254
VLAN への VLAN マップの適用 2256
IPv6 ACL のモニタリング 2257
その他の参考資料 2258

第 106 章 **DHCP の設定** 2261
機能情報の確認 2261
DHCP に関する情報 2261
DHCP サーバ 2261
DHCP リレー エージェント 2262
DHCP スヌーピング 2262
オプション 82 データ挿入 2264
Cisco IOS DHCP サーバ データベース 2267
DHCP スヌーピング バインディング データベース 2267
DHCP スヌーピングおよびスイッチ スタック 2269
DHCP 機能の設定方法 2269
DHCP スヌーピングのデフォルト設定 2269
DHCP スヌーピング設定時の注意事項 2270
DHCP サーバの設定 2271
DHCP サーバとスイッチ スタック 2271
DHCP リレー エージェントの設定 2271
パケット転送アドレスの指定 2272
DHCP スヌーピングおよびオプション 82 を設定するための前提条件 2274
Cisco IOS DHCP サーバ データベースのイネーブル化 2276
DHCP スヌーピング情報のモニタリング 2276
DHCP サーバ ポートベースのアドレス割り当ての設定 2277
DHCP サーバ ポートベースのアドレス割り当ての設定に関する情報 2277

ポートベースのアドレス テーブルのデフォルト設定 2277
ポートベースのアドレス割り当て設定時の注意事項 2278
DHCP スヌーピング バインディング データベース エージェントのイネーブル化 2278
DHCP サーバ ポートベースのアドレス割り当てのイネーブル化 2280
DHCP サーバ ポートベースのアドレス割り当てのモニタリング 2281
その他の参考資料 2282

第 107 章 **IP ソース ガードの設定** 2285
機能情報の確認 2285
IP ソース ガードの概要 2286
IP ソース ガード 2286
スタティック ホスト用 IP ソース ガード 2286
IP ソース ガードの設定時の注意事項 2287
IP ソース ガードの設定方法 2289
IP ソース ガードのイネーブル化 2289
レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定 2290
IP ソース ガードのモニタリング 2292
その他の参考資料 2293

第 108 章 **ダイナミック ARP インスペクションの設定** 2295
機能情報の確認 2296
ダイナミック ARP インスペクションの制約事項 2296
ダイナミック ARP インスペクションの概要 2297
インターフェイスの信頼状態とネットワーク セキュリティ 2299
ARP パケットのレート制限 2301
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ 2301
廃棄パケットのロギング 2301
ダイナミック ARP インスペクションのデフォルト設定 2302
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ 2302
非 DHCP 環境での ARP ACL の設定 2303
DHCP 環境でのダイナミック ARP インスペクションの設定 2306

着信 ARP パケットのレート制限 2309
ダイナミック ARP インスペクション検証チェックの実行 2311
DAI のモニタリング 2313
DAI の設定の確認 2313
その他の参考資料 2314
機能情報の確認 2315
ダイナミック ARP インスペクションの制約事項 2315
ダイナミック ARP インスペクションの概要 2317
インターフェイスの信頼状態とネットワーク セキュリティ 2319
ARP パケットのレート制限 2320
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ 2320
廃棄パケットのロギング 2321
ダイナミック ARP インスペクションのデフォルト設定 2321
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ 2322
非 DHCP 環境での ARP ACL の設定 2322
DHCP 環境でのダイナミック ARP インスペクションの設定 2325
着信 ARP パケットのレート制限 2328
ダイナミック ARP インスペクション検証チェックの実行 2330
DAI のモニタリング 2332
DAI の設定の確認 2333
その他の参考資料 2334

第 109 章 **IEEE 802.1x ポートベースの認証の設定 2335**
機能情報の確認 2335
802.1x ポートベース認証について 2335
ポートベース認証プロセス 2336
ポートベース認証の開始およびメッセージ交換 2338
ポートベース認証の認証マネージャ 2340
ポートベース認証方法 2340
ユーザ単位 ACL および Filter-Id 2341
ポートベース認証マネージャ CLI コマンド 2342

許可ステートおよび無許可ステートのポート 2344
ポートベース認証とスイッチ スタック 2345
802.1X のホスト モード 2345
802.1x 複数認証モード 2346
ユーザごとのマルチ認証 VLAN 割り当て 2347
MAC 移動 2349
MAC 置換 2350
802.1x アカウンティング 2350
802.1x アカウンティング属性値ペア 2351
802.1x 準備状態チェック 2352
スイッチと RADIUS サーバ間の通信 2352
VLAN 割り当てを使用した 802.1x 認証 2353
ユーザ単位 ACL を使用した 802.1x 認証 2355
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証 2356
Cisco Secure ACS およびリダイレクト URL の属性と値のペア 2358
Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア 2359
VLAN ID ベース MAC 認証 2359
ゲスト VLAN を使用した 802.1x 認証 2359
制限付き VLAN を使用した 802.1x 認証 2361
アクセス不能認証バイパスを使用した 802.1x 認証 2362
複数認証ポートのアクセス不能認証バイパスのサポート 2362
アクセス不能認証バイパスの認証結果 2362
アクセス不能認証バイパス機能の相互作用 2363
802.1x クリティカル音声 VLAN 2364
802.1x ユーザ ディストリビューション 2365
802.1x ユーザ ディストリビューションの設定時の注意事項 2365
音声 VLAN ポートを使用した IEEE 802.1x 認証 2366
ポート セキュリティを使用した IEEE 802.1x 認証 2367
WoL 機能を使用した IEEE 802.1x 認証 2367
MAC 認証バイパスを使用した IEEE 802.1x 認証 2367
Network Admission Control レイヤ 2 IEEE 802.1x 検証 2369

柔軟な認証の順序設定 2369
Open1x 認証 2370
マルチドメイン認証 2371
Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ 2372
音声認識 802.1x セキュリティ 2374
コモン セッション ID 2375
802.1x ポートベース認証の設定方法 2375
802.1x 認証のデフォルト設定 2375
802.1x 認証設定時の注意事項 2377
802.1X 認証 2377
VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス 2378
MAC 認証バイパス 2379
ポートあたりのデバイスの最大数 2380
802.1x 準備状態チェックの設定 2380
音声認識 802.1x セキュリティの設定 2382
802.1x 違反モードの設定 2384
802.1X 認証の設定 2385
802.1x ポートベース認証の設定 2386
スイッチと RADIUS サーバ間の通信の設定 2388
ホスト モードの設定 2390
定期的な再認証の設定 2392
待機時間の変更 2393
スイッチからクライアントへの再送信時間の変更 2394
スイッチからクライアントへのフレーム再送信回数の設定 2395
再認証回数の設定 2396
MAC 移動のイネーブル化 2397
MAC 置換のイネーブル化 2398
802.1x アカウンティングの設定 2400
ゲスト VLAN の設定 2401
制限付き VLAN の設定 2402

制限付き VLAN の認証試行回数の設定 2404
クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定 2405
アクセス不能認証バイパスの設定例 2409
WoL を使用した 802.1x 認証の設定 2409
MAC 認証バイパスの設定 2411
802.1x ユーザ ディストリビューションの設定 2412
VLAN グループの設定例 2412
NAC レイヤ 2 802.1x 検証の設定 2413
NEAT を使用したオーセンティケータ スイッチの設定 2415
NEAT を使用したサプリカント スイッチの設定 2417
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定 2419
ダウンロード可能な ACL の設定 2419
ダウンロード ポリシーの設定 2421
VLAN ID ベース MAC 認証の設定 2423
柔軟な認証順序の設定 2424
Open1x の設定 2425
ポート上での 802.1x 認証のディセーブル化 2427
802.1x 認証設定のデフォルト値へのリセット 2428
802.1x の統計情報およびステータスのモニタリング 2429
その他の参考資料 2430
IPv4 アクセス コントロール リストに関する機能情報 2431

第 110 章 **Web ベース認証の設定** 2433
機能情報の確認 2433
Web ベース認証の概要 2433
デバイスのロール 2434
ホストの検出 2435
セッションの作成 2435
認証プロセス 2436
ローカル Web 認証バナー 2437
Web 認証カスタマイズ可能な Web ページ 2439

ガイドライン 2439
認証プロキシ Web ページの注意事項 2441
成功ログインに対するリダイレクト URL の注意事項 2442
その他の機能と Web ベース認証の相互作用 2442
ポート セキュリティ 2442
LAN ポート IP 2443
Gateway IP 2443
ACL 2443
コンテキストベース アクセス コントロール 2443
EtherChannel 2443
Web ベース認証の設定方法 2444
デフォルトの Web ベース認証の設定 2444
Web ベース認証の設定に関する注意事項と制約事項 2444
認証ルールとインターフェイスの設定 2446
AAA 認証の設定 2448
スイッチ/RADIUS サーバ間通信の設定 2449
HTTP サーバの設定 2451
認証プロキシ Web ページのカスタマイズ 2452
成功ログインに対するリダイレクション URL の指定 2453
Web ベース認証パラメータの設定 2454
Web ベース認証ローカル バナーの設定 2455
Web ベース認証キャッシュ エントリの削除 2456
Web ベース認証ステータスの監視 2457

第 111 章 ポート単位のトラフィック制御の設定 2459
ポートベースのトラフィック制御の概要 2459
機能情報の確認 2460
ストーム制御に関する情報 2460
Storm Control 2460
トラフィック アクティビティの測定方法 2460
トラフィック パターン 2461

ストーム制御の設定方法 2462
ストーム制御およびしきい値レベルの設定 2462
スモール フレーム到着レートの設定 2465
保護ポートに関する情報 2467
保護ポート 2467
保護ポートのデフォルト設定 2468
保護ポートのガイドライン 2468
保護ポートの設定方法 2468
保護ポートの設定 2468
保護ポートの監視 2470
ポート ブロッキングに関する情報 2470
ポート ブロッキング 2470
ポート ブロッキングの設定方法 2470
インターフェイスでのフラッディング トラフィックのブロッキング 2470
ポート ブロッキングの監視 2472
ポート セキュリティの前提条件 2472
ポート セキュリティの制約事項 2472
ポート セキュリティの概要 2473
ポート セキュリティ 2473
セキュア MAC アドレスのタイプ 2473
スティッキ セキュア MAC アドレス 2473
セキュリティ違反 2474
ポート セキュリティ エージング 2475
ポート セキュリティとスイッチ スタック 2476
デフォルトのポート セキュリティ設定 2476
ポート セキュリティの設定時の注意事項 2476
ポートベースのトラフィック制御の概要 2478
ポート セキュリティの設定方法 2479
ポート セキュリティのイネーブル化および設定 2479
ポート セキュリティ エージングのイネーブル化および設定 2485
機能情報の確認 2487

ストーム制御に関する情報 2488
Storm Control 2488
トラフィック アクティビティの測定方法 2488
トラフィック パターン 2489
ストーム制御の設定方法 2489
ストーム制御およびしきい値レベルの設定 2489
スモール フレーム到着レートの設定 2493
機能情報の確認 2495
保護ポートに関する情報 2495
保護ポート 2495
保護ポートのデフォルト設定 2496
保護ポートのガイドライン 2496
保護ポートの設定方法 2496
保護ポートの設定 2496
保護ポートの監視 2497
次の作業 2497
その他の参考資料 2498
機能情報 2498
機能情報の確認 2499
ポート ブロッキングに関する情報 2499
ポート ブロッキング 2499
ポート ブロッキングの設定方法 2499
インターフェイスでのフラッディング トラフィックのブロッキング 2499
ポート ブロッキングの監視 2501
次の作業 2501
その他の参考資料 2501
機能情報 2502
ポート セキュリティの設定例 2503

第 112 章 IPv6 ファースト ホップ セキュリティの設定 2505
機能情報の確認 2505

IPv6 でのファースト ホップ セキュリティの前提条件 2506
IPv6 でのファースト ホップ セキュリティの制約事項 2506
IPv6 でのファースト ホップ セキュリティに関する情報 2506
SISF ベースの IPv4 および IPv6 デバイス トラッキングに関する情報 2510
SISF ベース デバイス トラッキング CLI への移行時の制限 2510
IPDT および IPv6 スヌーピング コマンドの SISF ベースの Device-Tracking コマンドへの移行 2511
IPDT、IPv6 スヌーピング、およびデバイス トラッキング CLI の互換性 2512
SISF ベースの IP デバイス トラッキングおよびスヌーピング ポリシーを作成する方法 2513
デバイス トラッキング ポリシーをインターフェイスにアタッチする方法 2515
デバイス トラッキング ポリシーを VLAN にアタッチする方法 2516
IPv6 スヌーピング ポリシーの設定方法 2517
IPv6 ネイバー プロービングの設定方法 2519
IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法 2523
IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 2524
IPv6 スヌーピング ポリシーを全体的に VLAN にアタッチする方法 2525
IPv6 バインディング テーブルの内容を設定する方法 2526
IPv6 ネイバー探索インスペクション ポリシーの設定方法 2527
IPv6 ネイバー探索インスペクション ポリシーをインターフェイスにアタッチする方法 2529
IPv6 ネイバー探索インスペクション ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 2530
IPv6 ネイバー探索インスペクション ポリシーを全体的に VLAN にアタッチする方法 2532
IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法 2533
IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法 2536
IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 2537
IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法 2538
IPv6 DHCP ガード ポリシーの設定方法 2539

IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法 2541
IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 2542
IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法 2544
IPv6 ソース ガードの設定方法 2544
IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法 2546
IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 2546
IPv6 プレフィックス ガードの設定方法 2547
IPv6 プレフィックス ガード ポリシーをインターフェイスにアタッチする方法 2549
IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 2550
IPv6 ファースト ホップ セキュリティの設定例 2551
例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 2551
例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 2551
その他の参考資料 2551

第 113 章 **Cisco TrustSec の設定** 2553
Cisco TrustSec の概要 2553
機能情報の確認 2553
Cisco TrustSec の機能 2554
Cisco TrustSec の機能情報 2557

第 114 章 **コントロール プレーン ポリシングの設定** 2559
機能情報の確認 2559
CoPP の制約事項 2559
コントロール プレーン ポリシングに関する情報 2560
CoPP の概要 2560
システム定義の CoPP の特徴 2561

ユーザ設定可能な CoPP の特徴 2564
CoPP の設定方法 2564
CPU キューの有効化またはポリサー レートの変更 2564
CPU キューの無効化 2566
すべての CPU キューに対するデフォルトのポリサー レートの設定 2567
CoPP の設定例 2568
例：CPU キューの有効化または CPU キューのポリサー レートの変更 2568
例：CPU キューの無効化 2569
例：すべての CPU キューに対するデフォルトのポリサー レートの設定 2570
CoPP のモニタリング 2571
CoPP に関する追加情報 2572
CoPP の機能履歴と情報 2573

第 115 章 ワイヤレス ゲスト アクセスの設定 2575
機能情報の確認 2575
ゲスト アクセスの前提条件 2575
ゲスト アクセスの制約事項 2576
ワイヤレス ゲスト アクセスについて 2576
高速安全ローミング 2576
ゲスト アクセスを設定する方法 2577
ロビー管理者アカウントの作成 2577
ゲスト ユーザ アカウントの設定 2578
モビリティ エージェント（MA）の設定 2579
モビリティ コントローラの設定 2581
Web 認証証明書の入手 2582
Web 認証証明書の表示 2582
デフォルトの Web 認証ログイン ページの選択 2583
外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択 2584
WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て 2586
AAA-Override の設定 2587

クライアントの負荷分散の設定 2588
事前認証 ACL の設定 2589
IOS ACL 定義の設定 2590
Webpassthrough の設定 2590
ゲスト アクセスの設定例 2591
例：Lobby Ambassador アカウントの作成 2591
例：Web 認証証明書の入手 2592
例：Web 認証証明書の表示 2593
例：ゲスト ユーザ アカウントの設定 2593
例：モビリティ コントローラの設定 2594
例：デフォルトの Web 認証ログイン ページの選択 2595
例：外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択 2595
例：WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て 2596
例：AAA-Override の設定 2596
例：クライアントの負荷分散の設定 2596
例：事前認証 ACL の設定 2597
例：IOS ACL 定義の設定 2597
例：Webpassthrough の設定 2597
ゲスト アクセスに関する追加情報 2598
ゲスト アクセスの機能履歴と情報 2599

第 116 章 不正なデバイスの管理 2601
機能情報の確認 2601
不正なデバイスについて 2602
不正検出の設定方法 2607
不正検出の設定（CLI） 2607
不正検出のモニタリング 2609
例：不正検出の設定 2609
不正検出に関する追加情報 2610
不正検出設定の機能履歴と情報 2611

機能情報の確認 2611
不正なデバイスについて 2611
不正検出の設定方法 2617
不正検出の設定（CLI） 2617
不正検出のモニタリング 2619
例：不正検出の設定 2619
不正検出に関する追加情報 2620
不正検出設定の機能履歴と情報 2621

第 117 章 不正なアクセス ポイントの分類 2623
機能情報の確認 2623
不正なアクセス ポイントの分類について 2623
不正なアクセス ポイントの分類の制限 2626
不正なアクセス ポイントの分類方法 2628
不正分類ルールの設定（CLI） 2628
例：不正なアクセス ポイントの分類 2631
不正なアクセス ポイントの分類に関する追加情報 2631
不正なアクセス ポイントの分類の機能履歴および情報 2632

第 118 章 wIPS の設定 2633
機能情報の確認 2633
wIPS について 2633
アクセス ポイントで wIPS を設定する方法 2641
アクセス ポイントでの wIPS の設定（CLI） 2641
wIPS 情報のモニタリング 2641
例：wIPS の設定 2642
wIPS の設定に関する追加情報 2642
wIPS 設定実行の機能履歴 2643

第 119 章 侵入検知システムの設定 2645
機能情報の確認 2645

侵入検知システムについて 2645
侵入検知システムを設定する方法 2646
IDS センサーの設定 2646
侵入検知システムのモニタリング 2647

第 XVIII 部： スタック マネージャおよびハイ アベイラビリティ 2649

第 120 章 スイッチ スタックの管理 2651
機能情報の確認 2651
スイッチ スタックの前提条件 2651
スイッチ スタックの制約事項 2652
スイッチ スタックに関する情報 2652
スイッチ スタックの概要 2652
スイッチ スタックでサポートされる機能 2653
スイッチ スタックのメンバーシップ 2654
スイッチ スタック メンバーシップの変更 2654
スタック メンバー番号 2655
スタック メンバーのプライオリティ値 2657
スイッチ スタック ブリッジ ID と MAC アドレス 2657
スイッチ スタック上の永続的 MAC アドレス 2658
アクティブ スイッチとスタンバイ スイッチの選択と再選択 2658
スイッチ スタックのコンフィギュレーション ファイル 2660
スタック メンバーを割り当てるためのオフライン設定 2661
割り当てられたスイッチのスイッチ スタックへの追加による影響 2662
スイッチ スタックの割り当てられたスイッチの交換による影響 2664
割り当てられたスイッチのスイッチ スタックからの削除による影響 2664
互換性のないソフトウェアを実行しているスイッチのアップグレード 2664
自動アップグレード 2664
自動アドバイス 2666
スイッチ スタックの管理接続 2667
IP アドレスによるスイッチ スタックへの接続 2668

コンソール ポートまたはイーサネット管理ポートによるスイッチ スタックへの接続 2668
スイッチ スタックの設定方法 2669
永続的 MAC アドレス機能のイネーブル化 2669
スタック メンバー番号の割り当て 2671
スタック メンバー プライオリティ値の設定 2672
スイッチ スタックへの新しいメンバーのプロビジョニング 2673
プロビジョニングされたスイッチ情報の削除 2674
スイッチ スタック内の非互換スイッチの表示 2675
スイッチ スタックでの互換性のないスイッチのアップグレード 2676
スイッチ スタックのトラブルシューティング 2676
スタック ポートの一時的なディセーブル化 2676
他のメンバーの起動中のスタック ポートの再イネーブル化 2677
デバイス スタックのモニタリング 2678
スイッチ スタックの設定例 2679
スイッチ スタックの設定のシナリオ 2679
永続的 MAC アドレス機能のイネーブル化：例 2681
スイッチ スタックへの新しいメンバーの割り当て：例 2681
show switch stack-ports summary コマンドの出力：例 2682
ソフトウェア ループバック：例 2683
スタック ケーブルが接続されたソフトウェア ループバック：例 2684
スタック ケーブルが接続されていないソフトウェア ループバック：例 2685
切断されたスタック ケーブルの特定：例 2685
スタック ポート間の不安定な接続の修正：例 2686
スイッチ スタックに関する追加情報 2687

第 121 章 **Cisco NSF with SSO の設定** 2689
機能情報の確認 2689
NSF with SSO の前提条件 2689
NSF with SSO の制約事項 2690
NSF with SSO に関する情報 2690

NSF with SSO の概要 2690
SSO の動作 2691
NSF の動作 2693
Cisco Express Forwarding; シスコ エクスプレス フォワーディング 2694
BGP の動作 2695
OSPF の動作 2696
EIGRP の動作 2696
Cisco NSF with SSO の設定方法 2697
SSO の設定 2697
SSO の設定例 2698
CEF NSF の確認 2698
NSF の BGP の設定 2699
BGP NSF の確認 2700
OSPF NSF の設定 2701
OSPF NSF の確認 2701
EIGRP NSF の設定 2702
EIGRP NSF の確認 2703

第 122 章

StackWise Virtual の設定 2705
機能情報の確認 2705
Cisco StackWise Virtual の制約事項 2705
Cisco StackWise Virtual の前提条件 2706
Cisco StackWise Virtual について 2706
StackWise Virtual の概要 2706
Cisco StackWise Virtual トポロジ 2707
Cisco StackWise Virtual 冗長性 2709
SSO 冗長性 2709
ノンストップ フォワーディング 2710
マルチシャーシ EtherChannel 2710
MEC ハッシュのサポート 2711
MEC 障害シナリオ 2711

Cisco StackWise Virtual のパケット処理 2712
StackWise Virtual リンク上のトラフィック 2712
Layer 2 Protocols 2713
Layer 3 Protocols 2714
デュアル アクティブ検出 2716
デュアル アクティブ検出リンク 2716
リカバリ アクション 2717
Cisco StackWise Virtual の実装 2717
Cisco StackWise Virtual の設定方法 2718
Cisco StackWise Virtual 設定の構成 2718
Cisco StackWise Virtual リンクの設定 2719
StackWise Virtual デュアル アクティブ検出リンクの設定 2720
Cisco StackWise Virtual の設定の確認 2720
Cisco StackWise Virtual の機能情報 2721

第 123 章 ワイヤレス ハイ アベイラビリティの設定 2723
機能情報の確認 2723
ハイ アベイラビリティについて 2723
冗長性に関する情報 2724
アクセス ポイントの冗長性の設定 2724
ハートビート メッセージの設定 2725
アクセス ポイントのステートフル スイッチオーバーについて 2726
グレースフル スイッチオーバーの開始 2727
ハイ アベイラビリティ用の EtherChannel の設定 2727
LACP の設定 2728
ハイ アベイラビリティのトラブルシューティング 2729
スタンバイ コンソールへのアクセス 2729
スイッチオーバー前 2730
スイッチオーバー後 2731
デバイス スタックのモニタリング 2731
LACP の設定：例 2732

第 XIX 部： システム管理 2735

第 124 章 スイッチの管理 2737

機能情報の確認 2737

デバイスの管理に関する情報 2737

システム日時の管理 2737

システム クロック 2738

ネットワーク タイム プロトコル 2738

NTP ストラタム 2740

NTP アソシエーション 2740

NTP セキュリティ 2740

NTP の実装 2740

NTP バージョン 4 2741

システム名およびシステム プロンプト 2742

スタックのシステム名およびシステム プロンプト 2742

デフォルトのシステム名とプロンプトの設定 2742

DNS 2742

DNS のデフォルト設定値 2743

ログイン バナー 2743

バナーのデフォルト設定 2743

MAC Address Table 2743

MAC アドレス テーブルの作成 2744

MAC アドレスおよび VLAN 2744

MAC アドレスおよびデバイスのスタック 2744

MAC アドレス テーブルのデフォルト設定 2745

ARP テーブルの管理 2745

デバイスを管理する方法 2746

手動による日付と時刻の設定 2746

システム クロックの設定 2746

タイム ゾーンの設定 2747

夏時間の設定 2748
システム名の設定 2751
DNS の設定 2752
Message-of-the-Day ログイン バナーの設定 2754
ログイン バナーの設定 2755
MAC アドレス テーブルの管理 2756
アドレス エージング タイムの変更 2756
MAC アドレス変更通知トラップの設定 2757
MAC アドレス移動通知トラップの設定 2760
MAC しきい値通知トラップの設定 2762
スタティック アドレス エントリの追加および削除 2764
ユニキャスト MAC アドレス フィルタリングの設定 2766
デバイスのモニタリングおよび保守の管理 2767
デバイス管理の設定例 2768
例：システム クロックの設定 2768
例：サマー タイムの設定 2768
例：MOTD バナーの設定 2769
例：ログイン バナーの設定 2769
例：MAC アドレス変更通知トラップの設定 2769
例：MAC しきい値通知トラップの設定 2770
例：MAC アドレス テーブルへのスタティック アドレスの追加 2770
例：ユニキャスト MAC アドレス フィルタリングの設定 2770
デバイス管理に関する追加情報 2771
デバイス管理に関する追加情報 2772
デバイス管理の機能履歴と情報 2774

第 125 章 ブート整合性の可視性 2775
機能情報の確認 2775
ブート整合性の可視性について 2775
ソフトウェア イメージとハードウェアの確認 2776
プラットフォーム ID とソフトウェア整合性の確認 2776

第 126 章 デバイスのセットアップ設定の実行 2781
機能情報の確認 2781
デバイスセットアップ設定の実行に関する情報 2781
デバイスブート プロセス 2782
ソフトウェア インストーラ機能 2783
ソフトウェアのブート モード 2783
インストール モードでのブート 2783
バンドル モードでのブート 2784
スイッチ スタックのブート モード 2785
デバイス 情報の割り当て 2785
デフォルトのスイッチ情報 2786
DHCP ベースの自動設定の概要 2786
DHCP クライアントの要求プロセス 2787
DHCP ベースの自動設定およびイメージ アップデート 2789
DHCP ベースの自動設定の制約事項 2789
DHCP 自動設定 2789
DHCP 自動イメージ アップデート 2789
DHCP サーバ設定時の注意事項 2790
TFTP サーバの目的 2791
DNS サーバの目的 2792
コンフィギュレーション ファイルの入手方法 2792
環境変数の制御方法 2793
一般的な環境変数 2794
TFTP の環境変数 2796
ソフトウェア イメージのリロードのスケジューリング 2796
デバイスセットアップ設定の実行方法 2797
DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定 2797
DHCP 自動イメージ アップデート（コンフィギュレーション ファイルおよびイメージ）の設定 2799
DHCP サーバからファイルをダウンロードするクライアントの設定 2802

複数の SVI への IP 情報の手動割り当て 2804
デバイスのスタートアップ コンフィギュレーションの変更 2805
システム コンフィギュレーションを読み書きするためのファイル名の指定 2805
スイッチの手動による起動 2806
Deviceをインストール モードで起動する場合 2808
Deviceをバンドル モードで起動する場合 2809
スイッチ スタックで特定のソフトウェア イメージを起動する場合 2810
ソフトウェア イメージのリロードのスケジュール設定 2812
デバイスのセットアップ設定のモニタリング 2813
例：デバイス実行コンフィギュレーションの確認 2813
例：インストール モードでのソフトウェアブートアップ ディスプレイ 2814
例：緊急インストール 2816
デバイス のセットアップを実行する場合の設定例 2817
例：DHCP サーバとしてのデバイスの設定 2817
例：DHCP 自動イメージ アップデートの設定 2818
例：DHCP サーバから設定をダウンロードするためのデバイスの設定 2818
例：ソフトウェア イメージのリロードのスケジューリング 2819
デバイスのセットアップの実行に関する追加情報 2819
WCM サブパッケージのインストール 2820
利点 2821
前提条件 2821
[Restrictions（機能制限）] 2821
WCM サブパッケージのインストール 2821
デバイスセットアップ設定の機能履歴と情報 2822

第 127 章 自律ネットワーキングの設定 2823
自律型ネットワーキング 2823
自律型ネットワーキングの前提条件 2823
自律型ネットワーキングの制約事項 2824
自律型ネットワーキングに関する情報 2824
自律型ネットワーキングの概要 2824

Autonomic Networking Infrastructure 2825
自律型ネットワーキングのチャネル検出 2827
自律型ネットワーキングにおける隣接関係の検出 2827
自律型ネットワーキングのサービス検出 2827
自律型コントロール プレーン 2828
自律型ネットワーキングの設定方法 2828
レジストラの設定 2828
自律型ネットワーキング コンフィギュレーションの検証とモニタリング 2830

第 128 章 **Right-To-Use ライセンスの設定** 2833
機能情報の確認 2833
RTU ライセンスの設定に関する制約事項 2833
RTU ライセンスの設定に関する情報 2834
Right-To-Use ライセンス 2834
Right-To-Use イメージ ベースのライセンス 2835
Right-To-Use ライセンスの状態 2835
スイッチ スタックのライセンスのアクティブ化 2836
モビリティ コントローラ モード 2836
Right-To-Use AP-Count ライセンス 2836
Right-to-Use AP-Count 評価ライセンス 2837
Right-To-Use Adder AP-Count 再ホスト ライセンス 2837
RTU ライセンスの設定方法 2838
イメージ ベース ライセンスのアクティブ化 2838
ap-count ライセンスのアクティブ化 2839
アップグレード ライセンスまたはキャパシティ Adder ライセンスの取得 2840
ライセンスの再ホスト 2841
モビリティ モードの変更 2841
RTU ライセンスのモニタリングおよびメンテナンス 2842
RTU ライセンスの設定例 2843
例：RTU イメージ ベースのライセンスのアクティブ化 2843
例：RTU ライセンス情報の表示 2844

例：RTU ライセンスの詳細の表示 2845
例：RTU ライセンスの不一致の表示 2847
例：RTU ライセンス使用状況の表示 2847
RTU ライセンスに関する追加情報 2848
RTU ライセンスの機能履歴と情報 2849

第 129 章 管理者のユーザ名とパスワードの設定 2851
機能情報の確認 2851
管理者のユーザ名とパスワードの設定について 2851
管理者のユーザ名とパスワードの設定 2852
例：管理者のユーザ名とパスワードの設定 2854
管理者のユーザ名とパスワードに関する追加情報 2855
管理者のユーザ名とパスワードの設定の機能履歴と情報 2856

第 130 章 802.11 パラメータおよび帯域選択の設定 2857
機能情報の確認 2857
帯域選択の制約事項、802.11 帯域とパラメータ 2857
帯域選択、802.11 帯域およびパラメータについて 2858
帯域選択 2858
802.11 帯域 2859
802.11n パラメータ 2859
802.11h パラメータ 2860
802.11 帯域とそのパラメータを設定する方法 2860
帯域選択の設定（CLI） 2860
802.11 帯域の設定（CLI） 2861
802.11n のパラメータの設定（CLI） 2864
802.11h のパラメータの設定（CLI） 2867
帯域選択、802.11 帯域およびパラメータの設定のモニタリング 2868
帯域選択と 802.11 帯域を使用した設定のモニタリング コマンド 2868
例：5 GHz 帯域の設定の確認 2869
例：24 GHz 帯域の設定の確認 2870

例：802.11h パラメータの状態の確認 2872
例：帯域選択設定の確認 2872
帯域選択、802.11 帯域およびパラメータの設定例 2873
例：帯域選択の設定 2873
例：802.11 帯域設定 2873
例：802.11n 設定 2874
例：802.11h 設定 2874
802.11 パラメータおよび帯域選択に関する追加情報 2875
802.11 パラメータおよび帯域選択設定の機能履歴と情報 2876

第 131 章 アグレッシブ ロード バランシングの設定 2877
機能情報の確認 2877
アグレッシブ ロード バランシングの制約事項 2877
アグレッシブ ロード バランシング パラメータの設定情報 2878
アグレッシブ ロード バランシング 2878
アグレッシブ ロード バランシングの設定方法 2880
アグレッシブなロード バランシングの設定（CLI） 2880
アグレッシブ ロード バランシングのモニタリング 2881
アグレッシブ ロード バランシングに関する追加情報 2881
アグレッシブ ロード バランシングの設定の機能履歴と情報 2882

第 132 章 クライアント ローミングの設定 2883
機能情報の確認 2883
クライアント ローミングの設定の制約事項 2883
クライアント ローミングについて 2884
サブネット間ローミング 2885
VoIP による通話ローミング 2885
CCX レイヤ 2 クライアント ローミング 2886
レイヤ 2 またはレイヤ 3 のローミング設定方法 2887
レイヤ 2 またはレイヤ 3 のローミング設定 2887
CCX クライアント ローミング パラメータの設定（CLI） 2888

モビリティ Oracle の設定 2890
モビリティ コントローラの設定 2891
モビリティ エージェントの設定 2893
クライアントのローミング パラメータのモニタリング 2894
モビリティ設定のモニタ 2894
クライアント ローミング設定に関する追加情報 2896
クライアント ローミング設定の機能履歴と情報 2897

第 133 章 **有線ネットワークでの Application Visibility and Control の設定** 2899
機能情報の確認 2899
有線ネットワークでの Application Visibility and Control について 2900
サポートされる AVC クラス マップおよびポリシー マップのフォーマット 2900
有線 Application Visibility and Control の制限 2902
Application Visibility and Control の設定方法 2903
有線ネットワークでの Application Visibility and Control の設定 2903
インターフェイスでのアプリケーション認識の有効化 2903
AVC QoS ポリシーの作成 2904
スイッチ ポートへの QoS ポリシーの適用 2907
有線 AVC Flexible Netflow の設定 2908
NBAR2 カスタム アプリケーション 2914
HTTP のカスタマイズ 2915
SSL のカスタマイズ 2915
DNS のカスタマイズ 2916
複合カスタマイズ 2916
L3/L4 のカスタマイズ 2916
例：カスタム アプリケーションのモニタリング 2917
NBAR2 ダイナミック ヒットレス プロトコル パックのアップグレード 2917
NBAR2 プロトコル パックの前提条件 2917
NBAR2 プロトコル パックのロード 2918
Application Visibility and Control のモニタリング 2919
Application Visibility and Control のモニタリング（CLI） 2919

例：Application Visibility and Control 2920
例：Application Visibility and Control の設定 2920
基本的なトラブルシューティング（質問と回答） 2922
Application Visibility and Control に関する追加情報 2923
有線ネットワークでの Application Visibility and Control の機能履歴と情報 2924

第 134 章 ワイヤレス ネットワークでの Application Visibility and Control の設定 2925
機能情報の確認 2926
Application Visibility and Control について 2926
サポートされる AVC クラス マップおよびポリシー マップのフォーマット 2927
Application Visibility and Control の前提条件 2929
Application Visibility and Control によるDevice間ローミングに関するガイドライン 2930
Application Visibility and Control の制限 2930
Application Visibility and Control の設定方法 2932
Application Visibility and Control の設定（CLI） 2932
フロー レコードの作成 2932
フロー エクスポータの作成（オプション） 2934
フロー モニタの作成 2935
AVC QoS ポリシーの作成 2937
IPV4 の入出力方向にフロー モニタを適用する WLAN の設定 2945
Application Visibility and Control のモニタリング 2946
Application Visibility and Control のモニタリング（CLI） 2946
例：Application Visibility and Control 2948
例：アプリケーションの可視性設定 2948
例：Application Visibility and Control の QoS 設定 2948
例：ローカル プロファイリング ポリシーの QoS 属性の設定 2950
Application Visibility and Control に関する追加情報 2950
Application Visibility and Control の機能履歴と情報 2952

第 135 章 ロケーションの設定 2953
機能情報の確認 2953

ロケーションの設定に関する情報 2953
ロケーションの設定方法 2954
ロケーションの設定（CLI） 2954
クライアント、RFID タグ、および不正デバイスの NMSP 通知間隔の変更（CLI） 2957
クライアント、RFID タグ、および不正デバイスの NMSP 通知しきい値の変更（CLI） 2958
ロケーション設定および NMSP 設定のモニタリング 2959
ロケーション設定のモニタリング（CLI） 2959
NMSP 設定のモニタリング（CLI） 2959
例：ロケーションの設定 2960
例：NMSP の設定 2960
ロケーション設定に関する追加情報 2961
ロケーション設定の機能履歴と情報 2962

第 136 章 音声パラメータとビデオ パラメータの設定 2963
機能情報の確認 2963
音声およびビデオのパラメータの前提条件 2963
音声およびビデオのパラメータの制約事項 2964
音声パラメータとビデオ パラメータの設定について 2964
Call Admission Control（コール アドミッション制御） 2965
静的ベースの CAC 2965
load-based の CAC 2966
IOSd コール アドミッション制御 2966
Expedited Bandwidth Requests 2967
U-APSD 2968
Traffic Stream Metrics 2968
優先コール番号を使用した音声優先制御の設定について 2969
EDCA パラメータについて 2969
音声パラメータとビデオ パラメータの設定方法 2970
音声パラメータの設定（CLI） 2970
ビデオ パラメータの設定（CLI） 2973
SIP ベースの CAC の設定（CLI） 2976

優先コール番号の設定（CLI） 2977
EDCA パラメータの設定（CLI） 2979
音声およびビデオ パラメータのモニタリング 2980
音声およびビデオ パラメータの設定例 2983
例：音声およびビデオの設定 2983
音声およびビデオ パラメータに関する追加情報 2984
音声およびビデオ パラメータ設定の機能履歴と情報 2985

第 137 章 RFID タグ追跡の設定 2987
機能情報の確認 2987
RFID タグ追跡の設定について 2987
RFID タグ トラッキングの設定方法 2988
RFID タグ追跡の設定（CLI） 2988
RFID タグ トラッキング情報のモニタリング 2989
RFID タグ トラッキングに関する追加情報 2989
RFID タグ トラッキング設定の機能履歴と情報 2990

第 138 章 ロケーションの設定 2991
機能情報の確認 2991
ロケーションの設定に関する情報 2991
ロケーションの設定方法 2992
ロケーションの設定（CLI） 2992
クライアント、RFID タグ、および不正デバイスの NMSP 通知間隔の変更（CLI） 2995
クライアント、RFID タグ、および不正デバイスの NMSP 通知しきい値の変更（CLI） 2996
ロケーション設定および NMSP 設定のモニタリング 2997
ロケーション設定のモニタリング（CLI） 2997
NMSP 設定のモニタリング（CLI） 2997
例：ロケーションの設定 2998
例：NMSP の設定 2998
ロケーション設定に関する追加情報 2999

ロケーション設定の機能履歴と情報 3000

第 139 章 **Cisco Hyperlocation** 3001

機能情報の確認 3001

Cisco Hyperlocation の制約事項 3001

Cisco Hyperlocation について 3001

Cisco Hyperlocation の設定：グローバル設定（CLI） 3003

AP グループへの Cisco Hyperlocation の設定（CLI） 3005

HyperLocation BLE ビーコン パラメータの設定 3007

AP への Hyperlocation BLE ビーコン パラメータの設定 3008

第 140 章 **フロー制御のモニタリング** 3011

機能情報の確認 3011

フロー制御の概要 3011

フロー制御のモニタリング 3011

例：フロー制御のモニタリング 3012

フロー制御のモニタリングに関する追加情報 3013

フロー制御のモニタリングに関する機能履歴および情報 3014

第 141 章 **SDM テンプレートの設定** 3015

機能情報の確認 3015

SDM テンプレートの設定に関する情報 3015

SDM テンプレート 3015

SDM テンプレートとスイッチ スタック 3017

SDM テンプレートの設定方法 3017

SDM テンプレートの設定 3017

スイッチ SDM テンプレートの設定 3017

SDM テンプレートのモニタリングおよびメンテナンス 3019

SDM テンプレートの設定例 3019

例：SDM テンプレートの設定 3019

例：SDM テンプレートの表示 3019

SDM テンプレートに関する追加情報 3020
SDM テンプレートの設定の機能履歴と情報 3021

第 142 章 システム メッセージ ログの設定 3023
機能情報の確認 3023
システム メッセージ ログの設定に関する情報 3023
システム メッセージ ロギング 3023
システム ログ メッセージのフォーマット 3024
デフォルトのシステム メッセージ ロギングの設定 3025
syslog メッセージの制限 3026
システム メッセージ ログの設定方法 3026
メッセージ表示宛先デバイスの設定 3026
ログ メッセージの同期化 3029
メッセージ ロギングのディセーブル化 3030
ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化 3031
ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化 3032
メッセージ重大度の定義 3033
履歴テーブルおよび SNMP に送信される syslog メッセージの制限 3034
UNIX Syslog デーモンへのメッセージのロギング 3035
システム メッセージ ログのモニタリングおよびメンテナンス 3036
コンフィギュレーション アーカイブ ログのモニタリング 3036
システム メッセージ ログの設定例 3036
例：システム メッセージのスタック構成 3036
例：スイッチ システム メッセージ 3037
システム メッセージ ログに関する追加情報 3037
システム メッセージ ログの機能履歴と情報 3038

第 143 章 オンライン診断の設定 3039
機能情報の確認 3039
オンライン診断の設定に関する情報 3039
オンライン診断 3039

オンライン診断の設定方法 3040
オンライン診断テストの開始 3040
オンライン診断の設定 3041
オンライン診断のスケジューリング 3041
ヘルス モニタリング診断の設定 3042
オンライン診断のモニタリングおよびメンテナンス 3046
オンライン診断テストとテスト結果の表示 3046
オンライン診断テストの設定例 3046
例：診断テストの開始 3046
例：ヘルス モニタリング テストの設定 3047
例：診断テストのスケジューリング 3047
例：オンライン診断の表示 3047
オンライン診断に関する追加情報 3049
オンライン診断設定の機能履歴と情報 3050

第 144 章 コンフィギュレーション ファイルの管理 3051
コンフィギュレーション ファイルの管理の前提条件 3051
コンフィギュレーション ファイルの管理の制約事項 3051
コンフィギュレーション ファイルの管理について 3052
コンフィギュレーション ファイルのタイプ 3052
コンフィギュレーション モードおよびコンフィギュレーション ソースの選択 3052
CLI を使用したコンフィギュレーション ファイルの変更 3053
コンフィギュレーション ファイルの場所 3053
ネットワーク サーバからデバイスへのコンフィギュレーション ファイルのコピー 3054
Deviceから TFTP サーバへのコンフィギュレーション ファイルのコピー 3054
デバイスから RCP サーバへのコンフィギュレーション ファイルのコピー 3055
デバイスから FTP サーバへのコンフィギュレーション ファイルのコピー 3057
VRF によるファイルのコピー 3058
スイッチから別のスイッチへのコンフィギュレーション ファイルのコピー 3058
NVRAM より大きいコンフィギュレーション ファイル 3058
コンフィギュレーション ファイルの圧縮 3059

コンフィギュレーションのクラス A フラッシュ ファイル システム上のフラッシュ メモリへの格納 3059
ネットワークからのコンフィギュレーション コマンドのロード 3059
コンフィギュレーション ファイルをダウンロードするデバイスの設定 3060
ネットワークとホストのコンフィギュレーション ファイル 3060
コンフィギュレーション ファイル情報の管理方法 3060
コンフィギュレーション ファイル情報の表示（CLI） 3060
コンフィギュレーション ファイルの変更（CLI） 3061
Deviceから TFTP サーバへのコンフィギュレーション ファイルのコピー（CLI） 3063
次の作業 3064
Deviceから RCP サーバへのコンフィギュレーション ファイルのコピー（CLI） 3064
例 3065
次の作業 3066
デバイスから FTP サーバへのコンフィギュレーション ファイルのコピー(CLI) 3066
例 3067
次の作業 3068
TFTP サーバからデバイスへのコンフィギュレーション ファイルのコピー（CLI） 3068
次の作業 3069
rcp サーバからデバイスへのコンフィギュレーション ファイルのコピー（CLI） 3069
例 3070
次の作業 3071
FTP サーバからデバイスへのコンフィギュレーション ファイルのコピー（CLI） 3071
例 3072
次の作業 3073
NVRAM より大きいコンフィギュレーション ファイルの保守 3073
コンフィギュレーション ファイルの圧縮（CLI） 3073
コンフィギュレーションのクラス A フラッシュ ファイル システム上のフラッシュ メモリへの格納（CLI） 3075
ネットワークからのコンフィギュレーション コマンドのロード（CLI） 3076
フラッシュ メモリからスタートアップまたは実行コンフィギュレーションへのコンフィギュレーション ファイルのコピー（CLI） 3077

フラッシュ メモリ ファイル システム間でのコンフィギュレーション ファイルのコピー（CLI） 3078
FTP サーバからフラッシュ メモリ デバイスへのコンフィギュレーション ファイルのコピー（CLI） 3080
次の作業 3081
RCP サーバからフラッシュ メモリ デバイスへのコンフィギュレーション ファイルのコピー（CLI） 3081
TFTP サーバからフラッシュ メモリ デバイスへのコンフィギュレーション ファイルのコピー（CLI） 3082
スタートアップ コンフィギュレーション ファイルでのコンフィギュレーション コマンドの再実行（CLI） 3083
スタートアップ コンフィギュレーションのクリア（CLI） 3083
指定されたコンフィギュレーション ファイルの削除（CLI） 3084
クラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定（CLI） 3085
次の作業 3087
コンフィギュレーション ファイルをダウンロードするデバイスの設定 3088
ネットワーク コンフィギュレーション ファイルをダウンロードするデバイスの設定（CLI） 3088
ホスト コンフィギュレーション ファイルをダウンロードするデバイスの設定（CLI） 3089
その他の参考資料 3091

第 145 章 コンフィギュレーションの置換とロールバック 3093
コンフィギュレーションの置換とロールバックの前提条件 3093
コンフィギュレーションの置換とロールバックの制約事項 3094
コンフィギュレーションの置換とロールバックについて 3094
コンフィギュレーション アーカイブ 3094
コンフィギュレーションの置換 3095
コンフィギュレーション ロールバック 3096
コンフィギュレーション ロールバック変更確認 3097
コンフィギュレーションの置換とロールバックの利点 3097
コンフィギュレーションの置換とロールバックの使用方法 3097

コンフィギュレーション アーカイブの作成（CLI） 3097
コンフィギュレーションの置換またはロールバックの実行（CLI） 3100
機能のモニタリングおよびトラブルシューティング（CLI） 3102
コンフィギュレーションの置換とロールバックの設定例 3105
コンフィギュレーション アーカイブの作成 3105
現在の実行コンフィギュレーションを保存された Cisco IOS コンフィギュレーション ファイルで置換 3105
スタートアップ コンフィギュレーション ファイルへの復帰 3106
configure confirm コマンドを使用したコンフィギュレーション置換操作の実行 3106
コンフィギュレーション ロールバック操作の実行 3106
その他の参考資料 3107

第 146 章 フラッシュ ファイル システムの操作 3111
フラッシュ ファイル システムについて 3111
使用可能なファイル システムの表示 3112
デフォルト ファイル システムの設定 3114
ファイル システムのファイルに関する情報の表示 3115
ディレクトリの変更および作業ディレクトリの表示（CLI） 3115
ディレクトリの作成（CLI） 3116
ディレクトリの削除 3117
ファイルのコピー 3117
スタック内のDeviceから同じスタックの別のDeviceにファイルをコピーする 3118
ファイルの削除 3119
ファイルの作成、表示および抽出（CLI） 3120
その他の参考資料 3122

第 147 章 スイッチ ソフトウェアのアップグレード 3125
スイッチ ソフトウェアのアップグレード 3125

第 148 章 条件付きデバッグとラジオアクティブ トレース 3127
機能情報の確認 3127

条件付きデバッグの概要 3128
ラジオアクティブ トレースの概要 3128
条件付きデバッグおよび放射線トレース 3129
トレースファイルの場所 3129
条件付きデバッグの設定 3129
L2 マルチキャストの放射線トレース 3132
トレース ファイルの推奨ワークフロー 3132
ボックス外へのトレース ファイルのコピー 3133
条件付きデバッグの設定例 3133
条件付きデバッグのモニタリング 3134

第 149 章 ソフトウェア設定のトラブルシューティング 3135
機能情報の確認 3135
ソフトウェア設定のトラブルシューティングに関する情報 3136
スイッチのソフトウェア障害 3136
のパスワードを紛失したか忘れた場合 デバイス 3136
Power over Ethernet（PoE）ポート 3136
電力消失によるポートの障害 3137
不正リンク アップによるポート障害 3137
ping 3137
レイヤ 2 Traceroute 3138
レイヤ 2 の traceroute のガイドライン 3138
IP Traceroute 3139
Time Domain Reflector ガイドライン 3140
debug コマンド 3141
システム レポート 3141
スイッチのオンボード障害ロギング 3144
ファン障害 3145
CPU 使用率が高い場合に起こりうる症状 3145
ソフトウェア設定のトラブルシューティング方法 3146
ソフトウェア障害からの回復 3146

パスワードを忘れた場合の回復 3148
パスワード回復がイネーブルになっている場合の手順 3149
パスワード回復がディセーブルになっている場合の手順 3151
スイッチ スタック問題の回避 3153
自動ネゴシエーションの不一致の防止 3154
SFP モジュールのセキュリティと識別に関するトラブルシューティング 3154
SFP モジュール ステータスのモニタリング 3155
ping の実行 3155
温度のモニタリング 3156
物理パスのモニタリング 3156
IP traceroute の実行 3157
TDR の実行および結果の表示 3157
デバッグおよびエラー メッセージ出力のリダイレクト 3157
show platform forward コマンドの使用 3158
show debug コマンドの使用方法 3158
OBFL の設定 3158
ソフトウェア設定のトラブルシューティングの確認 3159
OBFL 情報の表示 3159
例：高い CPU 使用率に関する問題と原因の確認 3160
ソフトウェア設定のトラブルシューティングのシナリオ 3162
Power over Ethernet（PoE）に関するトラブルシューティングのシナリオ 3162
ソフトウェアのトラブルシューティングの設定例 3166
例：IP ホストの ping 3166
例：IP ホストに対する traceroute の実行 3167
例：すべてのシステム診断をイネーブルにする 3168
ソフトウェア設定のトラブルシューティングに関する追加情報 3169
ソフトウェア設定のトラブルシューティングの機能履歴と情報 3170

第 XX 部： **VideoStream** 3171

第 150 章 **VideoStream の設定** 3173

機能情報の確認 3173
VideoStream の前提条件 3173
VideoStream の設定に関する制限 3174
VideoStream について 3174
VideoStream の設定方法 3174
メディア ストリームのマルチキャストダイレクトのグローバル設定 3174
802.11 帯域のメディア ストリームの設定 3176
ビデオ ストリーミング用の WLAN 設定 3177
メディア ストリームの削除 3178
メディア ストリームの監視 3179

第 XXI 部： VLAN 3181

第 151 章 VTP の設定 3183
機能情報の確認 3183
VTP の前提条件 3183
VTP の制約事項 3184
VTP の概要 3185
VTP 3185
VTP Domain 3185
VTP モード 3186
VTP アドバタイズ 3188
VTP バージョン 2 3188
VTP バージョン 3 3189
VTP プルーニング 3190
VTP とデバイス スタック 3192
VTP 設定時の注意事項 3192
VTP の設定要件 3192
VTP の設定 3192
VTP 設定のためのドメイン名 3193
VTP ドメインのパスワード 3193

VTP バージョン 3194
VTP の設定方法 3195
VTP モードの設定（CLI） 3195
VTP バージョン 3 のパスワードの設定（CLI） 3197
VTP バージョン 3 のプライマリ サーバの設定（CLI） 3199
VTP バージョンのイネーブル化（CLI） 3199
VTP プルーニングのイネーブル化（CLI） 3201
ポート単位の VTP の設定（CLI） 3202
VTP ドメインへの VTP クライアント の追加（CLI） 3204
VTP のモニタ 3206
VTP の設定例 3206
例：スイッチをプライマリ サーバとして設定する 3206
次の作業 3207
その他の参考資料 3207
VTP の機能履歴と情報 3209

第 152 章 **VLAN の設定** 3211
機能情報の確認 3211
VLAN の前提条件 3211
VLAN の制約事項 3212
VLAN について 3212
論理ネットワーク 3212
サポートされる VLAN 3213
VLAN ポート メンバーシップ モード 3214
VLAN コンフィギュレーション ファイル 3215
標準範囲 VLAN 設定時の注意事項 3216
拡張範囲 VLAN 設定時の注意事項 3217
VLAN の設定方法 3218
標準範囲 VLAN の設定方法 3218
イーサネット VLAN の作成または変更（CLI） 3218
VLAN の削除（CLI） 3222

VLAN へのスタティック アクセス ポートの割り当て（CLI） 3223
拡張範囲 VLAN の設定方法 3225
拡張範囲 VLAN の作成（CLI） 3225
VLAN のモニタリング 3227
次の作業 3228
その他の参考資料 3229
VLAN の機能履歴と情報 3231

第 153 章 VLAN グループの設定 3233
機能情報の確認 3233
VLAN グループの前提条件 3233
VLAN グループの制約事項 3234
VLAN グループについて 3234
VLAN グループの設定方法 3235
VLAN グループの作成（CLI） 3235
VLAN グループの削除（CLI） 3235
WLAN への VLAN グループの追加（CLI） 3236
VLAN グループの VLAN の表示（CLI） 3237
次の作業 3237
その他の参考資料 3237
VLAN グループの機能履歴と情報 3239

第 154 章 VLAN トランクの設定 3241
機能情報の確認 3241
VLAN トランクの前提条件 3241
VLAN トランクの制約事項 3242
VLAN トランクについて 3243
トランキングの概要 3243
トランキング モード 3243
レイヤ 2 インターフェイス モード 3244
トランクでの許可 VLAN 3245

トランク ポートでの負荷分散 3245
STP プライオリティによるネットワーク負荷分散 3245
STP パス コストによるネットワーク負荷分散 3246
機能の相互作用 3246
VLAN トランクの設定方法 3247
トランク ポートとしてのイーサネット インターフェイスの設定 3247
トランク ポートの設定（CLI） 3247
トランクでの許可 VLAN の定義（CLI） 3249
プルーニング適格リストの変更（CLI） 3251
タグなしトラフィック用ネイティブ VLAN の設定（CLI） 3252
トランク ポートの負荷分散の設定 3254
STP ポート プライオリティによる負荷分散の設定（CLI） 3254
STP パス コストによる負荷分散の設定（CLI） 3257
次の作業 3260
その他の参考資料 3260
VLAN トランクの機能履歴と情報 3262

第 155 章 音声 VLAN の設定 3263
機能情報の確認 3263
音声 VLAN の前提条件 3263
音声 VLAN の制約事項 3264
音声 VLAN に関する情報 3264
音声 VLAN 3264
Cisco IP Phone の音声トラフィック 3264
Cisco IP Phone のデータ トラフィック 3265
音声 VLAN 設定時の注意事項 3265
音声 VLAN の設定方法 3267
Cisco IP Phone の音声トラフィックの設定（CLI） 3267
着信データ フレームのプライオリティ設定（CLI） 3269
音声 VLAN のモニタリング 3271
次の作業 3271

その他の参考資料 3271
音声 VLAN の機能履歴と情報 3273

第 156 章 プライベート VLAN の設定 3275
機能情報の確認 3275
プライベート VLAN の前提条件 3275
プライベート VLAN の制約事項 3276
プライベート VLAN について 3277
プライベート VLAN ドメイン 3277
Secondary VLANs 3278
プライベート VLAN ポート 3278
ネットワーク内のプライベート VLAN 3279
プライベート VLAN での IP アドレッシング方式 3280
複数のデバイスにまたがるプライベート VLAN 3280
プライベート VLAN の他機能との相互作用 3281
プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック 3281
プライベート VLAN と SVI 3282
プライベート VLAN とデバイススタック 3282
ダイナミック MAC アドレスを備えたプライベート VLAN 3283
スタティック MAC アドレスを備えたプライベート VLAN 3283
プライベート VLAN と VACL/QOS との相互作用 3283
プライベート VLAN および HA サポート 3284
プライベート VLAN 設定時の注意事項 3285
プライベート VLAN のデフォルト設定 3285
セカンダリ VLAN およびプライマリ VLAN の設定 3285
プライベート VLAN ポートの設定 3287
プライベート VLAN の設定方法 3288
プライベート VLAN の設定 3288
プライベート VLAN 内の VLAN の設定および対応付け 3289
プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 3293

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 3294
セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング 3296
プライベート VLAN のモニタ 3298
プライベート VLAN の設定例 3299
例：プライベート VLAN 内の VLAN の設定および関連付け 3299
例：ホスト ポートとしてのインターフェイスの設定 3299
例：プライベート VLAN 無差別ポートとしてのインターフェイスの設定 3300
例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする 3301
例：プライベート VLAN のモニタリング 3301
次の作業 3301
その他の参考資料 3302

第 XXII 部： **WLAN** 3305

第 157 章 **WLAN の設定** 3307
機能情報の確認 3307
WLAN の前提条件 3307
WLAN の制約事項 3308
WLAN について 3309
バンドの選択 3309
オフチャネル スキャンの延期 3310
DTIM 期間 3311
セッション タイムアウト 3312
Cisco Client Extensions 3312
ピアツーピア ブロッキング 3312
診断チャネル 3313
WLAN ごとの RADIUS 送信元サポート 3313
WLAN の設定方法 3314
WLAN の作成（CLI） 3314
WLAN の削除（CLI） 3315
WLAN の検索（CLI） 3315

WLAN のイネーブル化（CLI） 3316
WLAN のディセーブル（CLI） 3317
汎用 WLAN プロパティの設定（CLI） 3317
高度な WLAN プロパティの設定（CLI） 3319
WLAN プロパティの監視（CLI） 3322
次の作業 3323
その他の参考資料 3323
WLAN の機能情報 3324

第 158 章 **リモート LAN の設定** 3325
機能情報の確認 3325
リモート LAN の設定に関する前提条件 3325
リモート LAN の制約事項 3326
リモート LAN について 3326
リモート LAN の設定（CLI） 3326
リモート LAN の設定例 3328
AP グループ固有の CLI の設定 3331
ポートへの PoE の設定 3332
AP への LAN オーバーライドの設定 3332

第 159 章 **DHCP for WLANs の設定** 3333
機能情報の確認 3333
DHCP for WLANs を設定するための前提条件 3333
DHCP for WLANs の設定に関する制約事項 3335
Dynamic Host Configuration Protocol について 3335
内部 DHCP サーバ 3336
外部 DHCP サーバ 3336
DHCP 割り当て 3337
DHCP オプション 82 について 3338
DHCP スコープの設定 3339
DHCP スコープについて 3339

DHCP for WLANs の設定方法 3339
WLAN 用の DHCP 設定（CLI） 3339
DHCP スコープの設定（CLI） 3342
その他の参考資料 3342
DHCP for WLANs の機能情報 3343

第 160 章 **WLAN セキュリティの設定** 3345
機能情報の確認 3345
レイヤ 2 セキュリティの前提条件 3345
AAA Override について 3346
WLAN セキュリティの設定方法 3347
静的 WEP および 802.1X レイヤ 2 セキュリティ パラメータの設定（CLI） 3347
静的 WEP レイヤ 2 セキュリティ パラメータの設定（CLI） 3348
WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（CLI） 3349
802.1X レイヤ 2 セキュリティ パラメータの設定（CLI） 3350
その他の参考資料 3352
WLAN レイヤ 2 セキュリティに関する機能情報 3353

第 161 章 **WLAN ごとのクライアント カウントの設定** 3355
機能情報の確認 3355
WLAN ごとのクライアント カウントの設定に関する制約事項 3355
WLAN ごとのクライアント カウントの設定について 3356
WLAN ごとのクライアント カウントを設定する方法 3356
WLAN ごとのクライアント カウントの設定（CLI） 3356
WLAN ごとの各 AP のクライアント数の設定（CLI） 3357
WLAN あたりの AP 無線ごとのクライアント数の設定（CLI） 3358
クライアントの接続の監視（CLI） 3358
クライアント接続に関する追加情報 3359
WLAN ごとのクライアント接続に関する機能情報 3360

第 162 章 **802.11w の設定** 3361

機能情報の確認 3361
802.11w の前提条件 3361
802.11w の制約事項 3362
802.11w に関する情報 3362
802.11w の設定方法 3363
802.11w の設定（CLI） 3363
802.11w のディセーブル（CLI） 3365
802.11w の監視（CLI） 3366
802.11w に関する追加情報 3367
802.11w の機能に関する情報 3369

第 163 章 **Wi-Fi Direct クライアント ポリシーの設定** 3371
機能情報の確認 3371
Wi-Fi Direct クライアント ポリシーの制限 3371
Wi-Fi Direct クライアント ポリシーについて 3372
Wi-Fi Direct クライアント ポリシーの設定方法 3372
Wi-Fi Direct クライアント ポリシーの設定（CLI） 3372
Wi-Fi Direct クライアント ポリシーのディセーブル（CLI） 3374
Wi-Fi Direct クライアント ポリシーの監視（CLI） 3374
Wi-Fi Direct クライアント ポリシーに関する追加リファレンス 3375
Wi-Fi Direct クライアント ポリシーに関する機能情報 3376

第 164 章 **802.11r BSS の高速移行の設定** 3377
機能情報の確認 3377
802.11R 高速移行の制約事項 3377
802.11R 高速移行について 3378
802.11r 高速移行を設定する方法 3380
オープン WLAN での 802.11r 高速移行の設定（CLI） 3380
Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI） 3382
PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI） 3383
802.11r 高速移行のディセーブル（CLI） 3384

802.11r 高速移行の監視（GUI） 3385
802.11r 高速移行の監視（CLI） 3385
802.11r 高速移行に関する追加情報 3387
802.11r 高速移行の機能に関する情報 3388

第 165 章 経由ローミングの設定 3389
機能情報の確認 3389
経由ローミングの制約事項 3389
経由ローミングについて 3390
経由ローミングの設定方法 3391
経由ローミングの設定（CLI） 3391
経由ローミングの監視 3393
経由ローミングの設定例 3393
経由ローミングに関する追加情報 3394
経由ローミング設定の機能履歴と情報 3395

第 166 章 アクセス ポイント グループの設定 3397
機能情報の確認 3397
AP グループを設定するための前提条件 3397
アクセス ポイント グループの設定に関する制約事項 3398
アクセス ポイント グループについて 3399
アクセス ポイント グループの設定方法 3399
アクセス ポイント グループの作成 3399
AP グループへのアクセス ポイントの割り当て 3400
アクセス ポイント グループの表示 3401
その他の参考資料 3401
アクセス ポイント グループの機能履歴と情報 3402

第 XXIII 部： データ モデル 3403

第 167 章 YANG データモデルの設定 3405

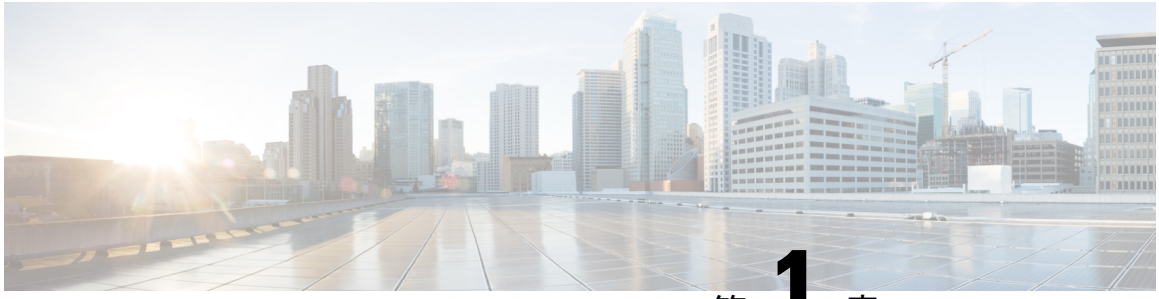
機能情報の確認 3405
データ モデルの概要：プログラムによる設定と各種の標準規格に準拠した設定 3405
NETCONF 3406
データ モデルの設定方法 3407
NETCONF の設定 3407
NETCONF オプションの設定 3408
SNMP の設定 3408
データ モデルに関する追加情報 3409
データ モデルの機能情報 3410

第 168 章 プログラマビリティ：ネットワーク ブートローダ 3411
機能情報の確認 3411
プログラマビリティに関する情報 3412
ネットワーク ブートローダの概要 3412
プラグ アンド プレイ エージェントの概要 3414
プログラマビリティの設定方法：ネットワーク ブートローダ 3415
ブートローダの設定 3415
プログラマビリティの設定例：ネットワーク ブートローダ 3416
例：ブートローダの設定 3416
プログラマビリティに関するその他の参考資料：ネットワーク ブートローダ 3416
プログラマビリティの機能情報：ネットワーク ブートローダ 3417

第 I 部

オーディオ ビデオ ブリッジング

- オーディオ ビデオ ブリッジング （1 ページ）



第 1 章

オーディオ ビデオ ブリッジング

- 機能情報の確認 （1 ページ）
- オーディオ ビデオ ブリッジング ネットワークの概要 （1 ページ）
- AVB ネットワークの設定 （8 ページ）
- AVB ネットワークのモニタリング （17 ページ）
- AVB 設定とモニタリングの例 （19 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

オーディオ ビデオ ブリッジング ネットワークの概要

オーディオ ビデオ ブリッジング（AVB）について

オーディオとビデオの設備導入は従来、アナログの単一用途型ポイントツーポイント一方向リンクとなっています。デジタル伝送への移行もまた、ポイントツーポイント一方向リンク アーキテクチャを維持し続けていました。専用の接続モデルによって、プロフェッショナル向けおよびコンシューマ向けのアプリケーションの配線が多くなり、管理と運用が難しくなっていました。

相互運用可能な方法でイーサネット ベースのオーディオ/ビデオ導入の採用を加速させるために、IEEE は IEEE オーディオ ビデオ ブリッジング標準（IEEE 802.1BA）と同一水準に達しま

した。これにより、エンドポイントとネットワークが全体として機能し、コンシューマ向けアプリケーション間の高品質 A/V ストリーミングをイーサネット インフラストラクチャを介してプロフェッショナル向けオーディオ/ビデオにまで可能にするメカニズムが定義されます。

（注）

- AVB は、スタック構成のシステムではサポートされません。
- AVB は、EtherChannel インターフェイスではサポートされません。
- AVB は、STP 対応ネットワークでのみサポートされます。

関連トピック

AVB の設定 （8 ページ）
AVB のモニタリング （17 ページ）
AVB の例 （19 ページ）

AVB をサポートするライセンス

AVB は、次の 2 つのライセンス レベルでのみサポートされます。

- ipbase
- ipservices

AVB の利点

AVB は、イーサネット ベースの音声およびビデオの送信を可能にする標準ベースのメカニズムであり、次の利点があります。

- 最大遅延保証
- 時間同期
- 帯域幅保証
- プロフェッショナル グレード

AVB ネットワークのコンポーネント

AVB プロトコルは、すべてのデバイスが AVB 対応であるドメインでのみ動作します。AVB ネットワークは、AVB 送話者、AVB リスナー、AVB スイッチおよびグランドマスタ クロックの送信元で構成されます。

- AVB 送話者：ストリームの送信元またはプロデューサである AVB エンド ステーション。つまり、マイク、ビデオ カメラなど。
- AVB リスナー：ストリームの宛先またはコンシューマである AVB エンド ステーション。つまり、スピーカー、ビデオ画面など。
- AVB スイッチ：IEEE802.1 AVB 基準に準拠するイーサネット スイッチ。

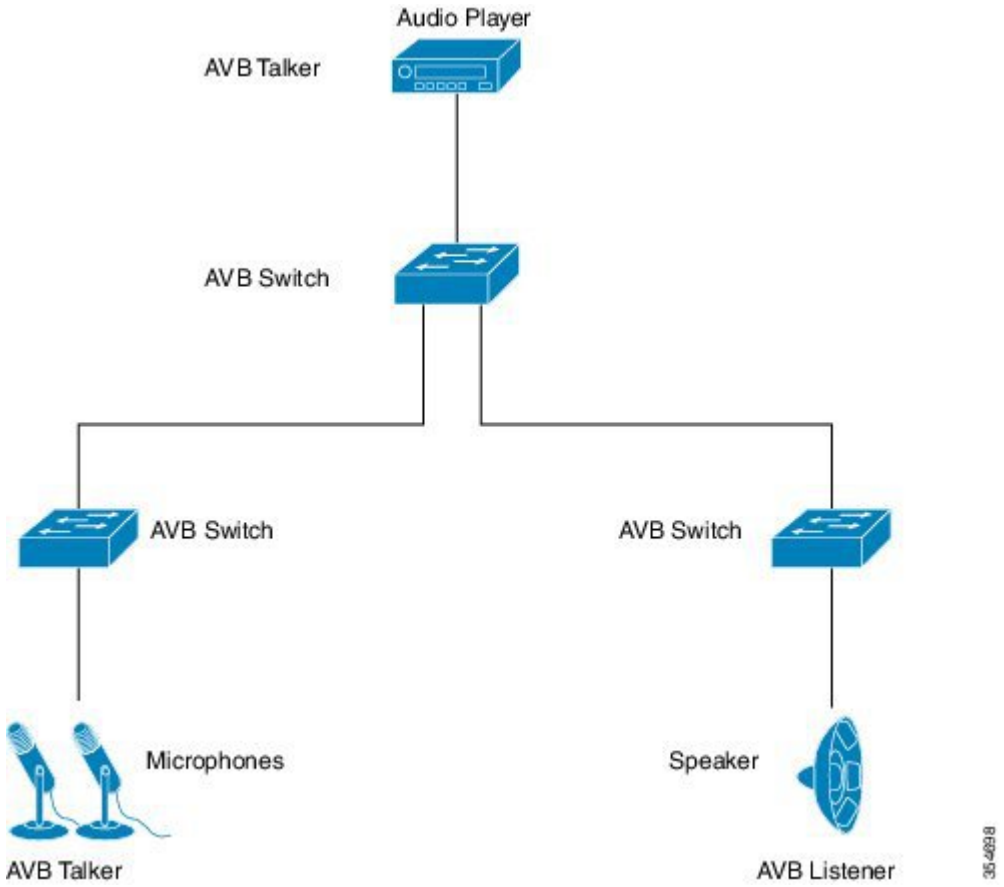
- AVB ストリーム：ストリーム予約プロトコル（SRP）に準拠するストリームの予約に関連付けられているデータ ストリーム。

（注） 時には、「ブリッジ」という単語が使用されます。このコンテキストでは、スイッチと言及します。

IEEE 802.1BA 仕様では、AVB 送話者がグランドマスタに対応している必要があります。一般的な導入では、ネットワーク ノードをグランドマスタにすることもできますが、そのノードがグランドマスタ対応デバイスからタイミングを調達または引き出し、IEEE 802.1AS を使用して AVB ネットワークにそのタイミングを提供できることが条件となります。

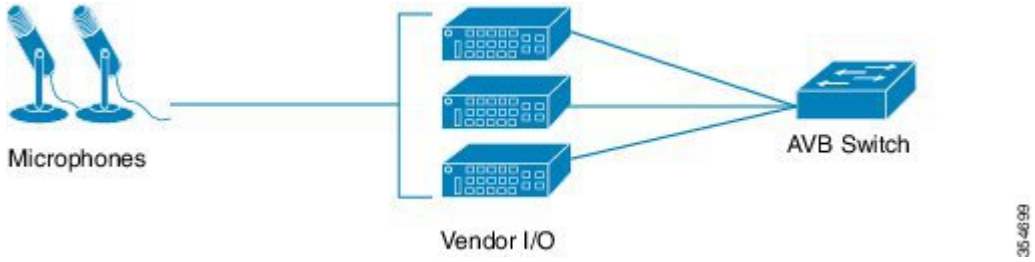
図 1 に、さまざまなコンポーネントによる AVB ネットワークの簡略図を示します。

図 *1*：図 *1*：*AVB* ネットワーク



多くの場合、音声/ビデオ エンドポイント（マイク、スピーカーなど）は、アナログ デバイスです。AVB エンドポイント ベンダーは、図 2 に示すように、広範な音声/ビデオ処理を提供し、AVB イーサネット インターフェイスにエンドポイントを集約する、デジタル信号プロセッサ（DSP）と I/O デバイスを導入します。

図 *2:* 図 *2* : ベンダーの音声 *I/O* システム



AVB でサポートされる SKU

AVB は、次の Catalyst 3850 および Catalyst 3650 SKU でサポートされます。

- WS-C3650-24PDM
- WS-C3650-48FQM
- WS-C3850-12X48U
- WS-C3850-12XS
- WS-C3850-16XS
- WS-C3850-24XS
- WS-C3850-24XU
- WS-C3850-32XS
- WS-C3850-48XS

（注） Cisco IOS XE Denali 16.3.1 では、AVB は WS-3850-12X48U の非 mGig インターフェイスでのみサポートされます。Cisco IOS XE Denali 16.3.2 以降では、AVB は WS-3850-12X48U および WS-C3850-24XU の mGig インターフェイスでサポートされます。

Generalized Precision Time Protocol（gPTP）について

Generalized Precision Time Protocol（gPTP）は IEEE 802.1AS 標準規格で、AVB ネットワーク内でブリッジとエンドポイントデバイスのクロックを同期する機能を提供します。これにより、時間認識ブリッジと送話者およびリスナー間でグランドマスタークロック（BMCA）を選択するメカニズムが定義されます。グランドマスタは、時間認識ネットワークで確立され、下位のノードに時間を分散して同期を可能にする時間階層のルートです。

時刻同期には、ネットワーク ノードでのリンク遅延とスイッチ遅延の測定も必要です。gptp スイッチは IEEE 1588 境界クロックであり、ピアツーピア遅延機能を使用してリンク遅延の測定も行います。計算された遅延は PTP メッセージの修正フィールドに追加され、エンドポイントに伝えられます。送話者とリスナーはこの gPTP 時刻を共有クロック基準として使用し、こ

の時刻はメディア クロックを中継して回復するために使用されます。gPTP は現在、ドメイン 0 のみを定義しており、これはスイッチがサポートするものです。

ピアツーピア遅延の機能は、STP によってブロックされたポートでも動作します。他の PTP メッセージはブロックされたポート上で送信されません。

PTP ドメインでは、ベスト マスター クロック（BMC）アルゴリズムがクロックとポートを階層型方式（クロックとポートの状態が含まれています）に編成します。

クロック

- グランドマスタ（GM/GMC）
- 境界クロック(BC)

ポート ステート

- Master（M）
- スレーブ（S）
- パッシブ（P）

関連トピック

gPTP の設定 （10 ページ）
gPTP のモニタリング （17 ページ）
gPTP の例 （22 ページ）

Multiple Stream Reservation Protocol（MSRP）について

Multiple Stream Reservation Protocol（MSRP）は、要求された QoS でネットワークを介してデータ ストリームの送信と受信を保証するネットワーク リソースを予約する機能をエンド ステーションに提供します。これは、AVB デバイス（送話者、リスナーおよびスイッチ）で必要なコア プロトコルの 1 つです。これにより、送話者は AVB スイッチのネットワークを介してストリームをアドバタイズでき、リスナーはストリームを受信するための登録を行えるようになります。

MSRP は、AVB をサポートするための主要なソフトウェア プロトコル モジュールです。これにより、ストリームの確立とティアダウンが可能になります。これは gPTP と連動し、ストリームの遅延情報を更新します。また、QoS モジュールと連動し、ストリームに要求された帯域幅を保証するハードウェア リソースを設定します。クレジット ベースのシェーパーに必要な QoS シェーピング パラメータも提供します。

関連トピック

MSRP のモニタリング （18 ページ）
MSRP の例 （25 ページ）

MSRP の機能

MSRP が実行する機能は次のとおりです。

- 送話者がストリームをアドバタイズできるようにし、リスナーがストリームを検出して登録を行えるようにします。
- 1 人の送話者と 1 人以上のリスナーとの間にイーサネット経由のパスを確立します。
- AVB ストリームに保証された帯域幅を提供します。
- 遅延の上限を保証します。
- 送話者と各リスナーとの間で最も問題となるエンドツーエンド遅延を検出してレポートします。
- 送話者とリスナー間のパスが帯域幅要件を満たすことができない場合に、障害の原因と場所をレポートします。
- さまざまな遅延対象を含む複数のトラフィック クラスをサポートします。
- AVB トラフィックを制限することによってスタベーションからベスト エフォート型トラフィックを保護します。
- MSRP 送話者宣言は、STP によってブロックされるポートでは転送されません。
- MSRP は、STP TCN 通知をリッスンし、ストリームを切断、変更、確立する MSRP 宣言を生成します。

QoSHQoS について

AVB ネットワークは、時間的に制約がある音声およびビデオ ストリームの帯域幅および最小遅延制限を保証します。AVB は、送話者からリスナーへのトラフィックで最も問題となる遅延対象に基づいて、クラス A およびクラス B を時間的に制約があるストリームとして定義します。

2 つのストリームの遅延対象は次のように示されます。

- SR-Class A：2ms
- SR-Class B: 50ms

ホップごとの最も問題となる遅延の影響を要約すると、SR クラス A の場合は合計で 2 ms 以下、SR クラス B の場合は 50ms 以下の全体的なエンドツーエンド遅延となります。送話者からリスナーへの一般的な 7 ホップの AVB 導入は、これらの遅延要件を満たします。

優先度のコードポイントは、特定のストリームにトラフィックをマッピングします。フレームの転送動作は、この優先度に基づいています。クレジットベースのシェーパーは、遅延対象が満たされるように、特定のアウトバウンドキューで予約済みの帯域幅に従って、これらのストリームの送信をシェーピングするために使用されます。

Cisco XE Denali 16.3.2 以降では、AVB の階層型 QoS のサポートが有効になっています。AVB の階層型 QoS ポリシーは、2 レベルの親子ポリシーです。AVB 親ポリシーは、音声、ビデオ トラフィック ストリーム（SR クラス A、SR クラス B）と標準的なベストエフォートのイーサネット トラフィック（非 SR）からのネットワーク制御パケットを分離し、それに応じてスト

リームを管理します。階層型 QoS では、トラフィック管理をより細かい粒度で実行する、複数のポリシー レベルでQoS動作を指定できます。階層型ポリシーは次のように使用できます。

- 親クラスが子ポリシー上で複数のキューをシェーピングする
- 集約トラフィックの特定のポリシー マップ アクションを適用する
- クラス固有のポリシー マップ アクションを適用する

policy-map *AVB-Output-Child-Policy* および **policy-map** *AVB-Input-Child-Policy* コマンドを使用して、入力および出力の HQoS 子ポリシーのクラスマップとそのアクションのみを変更できます。

（注） たとえば、SR クラス A cos 3 や SR クラス B Cos 2 など、親ポリシーに設定された PCP でマッピングするように子ポリシーの PCP を変更してはいけません。

階層型ポリシング

階層型ポリシングは、入力および出力インターフェイスでサポートされます。階層型QoSは、SR および非 SR クラス関連のルールをそれぞれ親ポリシーと子ポリシーに分けます。AVB SR クラスは、MSRP クライアントによって完全に制御されるため、SR クラス属性を含む親ポリシーは MSRP によって管理されます。エンドユーザには、非 SR クラス属性を含む子ポリシーに対する完全な制御権があり、子ポリシーのみを変更できます。

AVB HQoS 子ポリシーは、ユーザが変更可能で、ユーザが startup-config への設定を保存すると、設定を保存するように NVGEN されます。したがって、AVB HQoS 子ポリシーの設定はリロード後でも保持されます。

関連トピック

HQoS の設定 （12 ページ）
HQoS のモニタリング （18 ページ）
HQoS の例 （28 ページ）

マルチ VLAN 登録プロトコル（MVRP）について

マルチVLAN登録プロトコル（MVRP）は、MRPに基づくアプリケーションです。MVRPは、各 VLAN ID に関するダイナミック VLAN 登録エントリのコンテンツのダイナミック メンテナンスを行い、含まれている情報を他のブリッジに伝達する機能を提供します。この情報を使用して、MVRP 対応デバイスは、現在アクティブなメンバーを持つ VLAN に関連付けられている VLAN ID のセットの知識を動的に確立して更新することができ、それによって、ポートとそのメンバーは到達可能になります。

AVB の観点から、MVRP は送話者とリスナーで必須です。AVB とは関係なく、MVRP は VLAN 対応スイッチでの IEEE 802.1Q 要件です。ただし、AVB の場合は、スイッチでの VLAN の手動設定で十分です。

（注） MVRP が機能するには、VTP を無効モードまたはトランスペアレント モードにする必要があります。

関連トピック

MVRP の設定 （14 ページ）
MVRP のモニタリング （19 ページ）
MVRP の例 （38 ページ）

AVB ネットワークの設定

AVB の設定

この項では、AVB で使用可能なさまざまな設定について説明します。

関連トピック

オーディオ ビデオ ブリッジング（AVB）について （1 ページ）
AVB のモニタリング （17 ページ）
AVB の例 （19 ページ）

スイッチでの AVB のイネーブル化

スイッチで次のコマンドを使用して、AVB を有効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**avb** 例：	スイッチで AVB をイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config)# avb`	
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

次のタスク

スイッチで AVB をディセーブルにするには、このコマンドの「**no**」形式を使用します。

デバイスでの AVB の設定

次のコマンドを使用して、dot1q トランク ポートとして AVB デバイスの接続パスに沿ってインターフェイスを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface te1/1/1`	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	ポートをトランク ポートとして設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**vlan 2** 例： `Device(config)# vlan 2`	スイッチで VLAN 2 を設定します。
ステップ 7	**avb** 例： `Device(config-vlan)# avb`	指定されたインターフェイスで AVB を設定します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

次のタスク

スイッチで AVB をディセーブルにするには、このコマンドの「**no**」形式を使用します。

gPTP の設定

この項では、gPTP で使用可能なさまざまな設定について説明します。

関連トピック

Generalized Precision Time Protocol（gPTP）について （4 ページ）
gPTP のモニタリング （17 ページ）
gPTP の例 （22 ページ）

gPTP の有効化

AVB がスイッチで有効になると、AVB の gPTP も有効になります。

また、次に示すコマンドを使用して gPTP を有効にすることもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ptp profile dot1as** 例： `Device(config)# ptp profile dot1as`	ポート上で gPTP をイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

PTP クロックの値の設定

次のコマンドを使用して、ptp クロックの priority1 と priority2 の値を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ptp priority1** 例： `Device(config)# ptp priority1`	ptp クロック priority1 の値を設定します。 0 ～ 255：これは ptp クロック プライオリティの値の範囲です。この範囲の値を選択します。 （注） priority1 の値が 255 に設定されると、クロックはグランドマスタになることはできません。
ステップ 4	**ptp priority2** 例： `Device(config)# ptp priority2`	ptp クロック priority2 の値を設定します。 0 ～ 255：これは ptp クロック プライオリティの値の範囲です。この範囲の値を選択します。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードに戻ります。

HQoS の設定

この項では、HQoS で使用可能なさまざまな設定について説明します。

関連トピック

QoSHQoS について （6 ページ）
HQoS のモニタリング （18 ページ）
HQoS の例 （28 ページ）

HQoS のイネーブル化

AVB がスイッチで有効になると、AVB の HQoS も有効になります。

フラットなポリシー形式から階層型ポリシー形式への移行：注意事項と制約事項

AVB についてフラットなポリシー形式から階層型ポリシー形式に移行する際は、次の注意事項に従ってください。

- Cisco IOS XE Denali 16.3.1 から Cisco IOS XE Denali 16.3.2 にアップグレードすると、デバイスのスタートアップ コンフィギュレーションにある QoS ポリシーはエラーを伴って失

敗します。デバイスにHQoSポリシーを適切にインストールするには、次の手順に従います。

1. **no avb** コマンドを使用して、AVB をグローバルに無効にします。

（注） AVB を無効にすると、すべてのポリシー マップとクラス マップが設定から自動的に削除されます。しかし、アクセスリストは自動的に削除されません。アクセスリストは手動で削除する必要があります。Cisco IOS XE Denali 16.3.2 にアップグレードする前に、すべての QoS ポリシーの構成要素が削除されていることを確認します。

2. **avb** コマンドを使用して AVB を有効にします。AVB が有効になると、AVB の HQoS も有効になります。

- 階層型ポリシー形式がサポートされているリリースから、フラットなポリシー形式がサポートされているリリースに移行することは推奨されていません。
- 変更できるのは子ポリシーのみです。親ポリシーは、MSRP によって完全に制御されます。
- **show running config** コマンドは子ポリシーのみ表示します。
- Cisco IOS XE Denali 16.3.2 以降では、**show running config interface** コマンドを使用しても、接続されているポリシーの詳細は表示されません。接続されているポリシーのすべての詳細を表示するには、**show policy-map interface** コマンドを使用します。

階層型 QoS ポリシーの形式

次に、入力インターフェイスでの階層型再マーキング ポリシーの例を示します。

```
policy-map AVB-Input-Child-Policy
 class VOIP-DATA-CLASS
    set dscp EF
 class MULTIMEDIA-CONF-CLASS
    set dscp AF41
 class BULK-DATA-CLASS
    set dscp AF11
 class TRANSACTIONAL-DATA-CLASS
    set dscp AF21
 class SCAVENGER-DATA-CLASS
    set dscp CS1
 class SIGNALING-CLASS
    set dscp CS3
 class class-default
    set dscp default

policy-map AVB-Input-Policy-Remark-AB
 class AVB-SR-A-CLASS
    set cos 0 (set 0 for boundary & SR class A PCP value for core port)
 class AVB-SR-B-CLASS
    set cos 0 (set 0 for boundary & SR class B PCP value for core port)
```

```
 class class-default
    service-policy AVB-Input-Child-Policy

policy-map AVB-Input-Policy-Remark-A
 class AVB-SR-A-CLASS
    set cos 0 (set 0 for boundary & SR class A PCP value for core port)
 class class-default
    service-policy AVB-Input-Child-Policy

policy-map AVB-Input-Policy-Remark-B
 class AVB-SR-B-CLASS
    set cos 0 (set 0 for boundary & SR class B PCP value for core port)
 class class-default
    service-policy AVB-Input-Child-Policy

policy-map AVB-Input-Policy-Remark-None
 class class-default
    service-policy AVB-Input-Child-Policy
```

次に、出力インターフェイスでの階層型キューイング ポリシーの例を示します。

```
policy-map AVB-Output-Child-Policy
 class VOIP-PRIORITY-QUEUE
   bandwidth remaining percent 30
   queue-buffers ratio 10
 class MULTIMEDIA-CONFERENCING-STREAMING-QUEUE
   bandwidth remaining percent 15
   queue-limit dscp AF41 percent 80
   queue-limit dscp AF31 percent 80
   queue-limit dscp AF42 percent 90
   queue-limit dscp AF32 percent 90
   queue-buffers ratio 10
 class TRANSACTIONAL-DATA-QUEUE
   bandwidth remaining percent 15
   queue-limit dscp AF21 percent 80
   queue-limit dscp AF22 percent 90
   queue-buffers ratio 10
 class BULK-SCAVENGER-DATA-QUEUE
   bandwidth remaining percent 15
   queue-limit dscp AF11 percent 80
   queue-limit dscp AF12 percent 90
   queue-limit dscp CS1 percent 80
   queue-buffers ratio 15
 class class-default
   bandwidth remaining percent 25
   queue-buffers ratio 25

policy-map AVB-Output-Policy
 class AVB-SR-A-CLASS
   priority level 1 (Shaper value based on stream registration)
 class AVB-SR-B-CLASS
   priority level 2 (Shaper value based on stream registration)
 class CONTROL-MGMT-QUEUE
   priority level 3 percent 15
 class class-default
   bandwidth remaining percent 100
   queue-buffers ratio 80
   service-policy AVB-Output-Child-Policy
```

MVRP の設定

この項では、MVRP で使用可能なさまざまな設定について説明します。

関連トピック

マルチ VLAN 登録プロトコル（MVRP）について （7 ページ）
MVRP のモニタリング （19 ページ）
MVRP の例 （38 ページ）

MVRP のイネーブル化

次のコマンドを使用して、トポロジ内のスイッチで MVRP を有効にして Vlan 伝達を有効にできます。

（注） MVRP を介したダイナミック VLAN の作成を有効にする前に、VTP モードを**トランスペアレント** モードまたは**オフ** モードに変更する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mvrp global** 例： `Device(config)# mvrp global`	MVRP グローバル コンフィギュレーション モードを開始します。

ステップ 4	**vtp mode** {**transparent** | **off**}
	例：
	`Device(config)# vtp mode transparent`
	例：
	`Device(config)# vtp mode off`
		VTP を**トランスペアレント** モードまたは**オフ** モードに設定します。

	コマンドまたはアクション	目的
ステップ 5	**mvrp vlan create** 例： `Device(config)# mvrp vlan create`	スイッチで MVRP をイネーブルにします。

スイッチ インターフェイスでの MVRP の設定

次のコマンドを使用して、スイッチ インターフェイスに MVRP を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface te1/1/1`	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	**mvrp registration** {*fixed* | *forbidden* | *normal*} 例： `Device(config-if)# mvrp registration fixed`	MADインスタンスにMVRPを登録します。 • fixed：固定登録 • forbidden：禁止登録 • normal：通常の登録
ステップ 5	**mvrp timer** {*join* | *leave* | *leave-all* | *periodic*} 例： `Device(config-if)# mvrp timer join`	MVRP タイマーを設定します。 • join：タイマーは、ASMに適用される送信機会の間の間隔を制御します。

	コマンドまたはアクション	目的
		• leave：タイマーは、MT ステートに移行する前に LV ステートで待機する RSM を制御します。 • leave-all：タイマーは、LeaveAll SM が LeaveAll PDU を生成する頻度を制御します。 • periodic：定期タイマー
ステップ 6	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。

AVB ネットワークのモニタリング

AVB のモニタリング

AVB の詳細を表示するには、次の表のコマンドを使用します。

コマンド	目的
show avb domain	AVB ドメインを表示します。
show avb streams	AVB ストリーム情報を表示します。

関連トピック

AVB の設定 （8 ページ）
オーディオ ビデオ ブリッジング（AVB）について （1 ページ）

gPTP のモニタリング

gPTP プロトコルの詳細を表示するには、次の表のコマンドを使用します。

コマンド	目的
show ptp brief	インターフェイスの ptp の簡易ステータスを表示します。
show ptp clock	ptp クロック情報を表示します。
show ptp parent	親クロックの情報を表示します。

コマンド	目的
show ptp port	ptp ポート情報を表示します。
show platform software fed switch active ptp if-id {interface-id}	ポートの ptp ステータスに関する詳細情報を表示します。

関連トピック

gPTP の設定 （10 ページ）
Generalized Precision Time Protocol（gPTP）について （4 ページ）

MSRP のモニタリング

MSRP の詳細を表示するには、次の表のコマンドを使用します。

コマンド	目的
show msrp streams	MSRP ストリーム情報を表示します。
show msrp streams detailed	MSRP ストリームの詳細情報を表示します。
show msrp streams brief	MSRP ストリームの概要情報を表示します。
show msrp port bandwidth	MSRP ポート帯域幅情報を表示します。

関連トピック

Multiple Stream Reservation Protocol（MSRP）について （5 ページ）

HQoS のモニタリング

HQoS の詳細を表示するには、次の表のコマンドを使用します。

コマンド	目的
show run	すべての子ポリシー マップの詳細を表示します。
show policy-map	ポリシー マップ設定の詳細を表示します。
show policy-map interface *interface-id* [**input** | **output**]	AVB QoS 統計情報を表示します。入力のパケット カウンタと出力のバイト カウンタは、QoS 統計情報のために考慮されます。

関連トピック

HQoS の設定 （12 ページ）
QoSHQoS について （6 ページ）

MVRP のモニタリング

MVRP の詳細を表示するには、次の表のコマンドを使用します。

コマンド	目的
show mvrp summary	MVRP サマリー情報を表示します。
show mvrp interface	インターフェイスの MVRP 情報を表示します。

関連トピック

MVRP の設定 （14 ページ）
マルチ VLAN 登録プロトコル（MVRP）について （7 ページ）

AVB 設定とモニタリングの例

AVB の例

次に、AVB ドメインを表示する例を示します。

```
Device#show avb domain

AVB Class-A
    Priority Code Point     : 3
    VLAN                    : 2
    Core ports              : 1
    Boundary ports          : 67

AVB Class-B
    Priority Code Point     : 2
    VLAN                    : 2
    Core ports              : 1
    Boundary ports          : 67

--------------------------------------------------------------------------------
Interface    State       Delay    PCP  VID  Information
--------------------------------------------------------------------------------
Te1/0/1        down      N/A                       Oper state not up
Te1/0/2        down      N/A                       Oper state not up
Te1/0/3        down      N/A                       Oper state not up
Te1/0/4        down      N/A                       Oper state not up
Te1/0/5          up      N/A                   Port is not asCapable
Te1/0/6        down      N/A                       Oper state not up
Te1/0/7        down      N/A                       Oper state not up
Te1/0/8        down      N/A                       Oper state not up
Te1/0/9        down      N/A                       Oper state not up
Te1/0/10       down      N/A                       Oper state not up
```

```
Te1/0/11       down      N/A                          Oper state not up
Te1/0/12       down      N/A                          Oper state not up
Te1/0/13       down      N/A                          Oper state not up
Te1/0/14       down      N/A                          Oper state not up
Te1/0/15       down      N/A                          Oper state not up
Te1/0/16       down      N/A                          Oper state not up
 Te1/0/17      down      N/A                          Oper state not up
Te1/0/18       down      N/A                          Oper state not up
Te1/0/19         up      N/A                      Port is not asCapable
Te1/0/20       down      N/A                          Oper state not up
Te1/0/21       down      N/A                          Oper state not up
Te1/0/22       down      N/A                          Oper state not up
Te1/0/23         up      N/A                      Port is not asCapable
Te1/0/24       down      N/A                          Oper state not up
Te1/0/25       down      N/A                          Oper state not up
Te1/0/26       down      N/A                          Oper state not up
Te1/0/27       down      N/A                          Oper state not up
Te1/0/28       down      N/A                          Oper state not up
Te1/0/29         up      N/A                      Port is not asCapable
Te1/0/30       down      N/A                          Oper state not up
Te1/0/31       down      N/A                          Oper state not up
Te1/0/32       down      N/A                          Oper state not up
Te1/0/33       down      N/A                          Oper state not up
Te1/0/34       down      N/A                          Oper state not up
Te1/0/35         up      N/A                      Port is not asCapable
Te1/0/36       down      N/A                          Oper state not up
Te1/0/37       down      N/A                          Oper state not up
Te1/0/38       down      N/A                          Oper state not up
Te1/0/39         up    507ns
   Class-  A        core            3    2

   Class-  B        core            2    2

Te1/0/40       down      N/A                          Oper state not up
Te1/0/41       down      N/A                          Oper state not up
Te1/0/42       down      N/A                          Oper state not up
Te1/0/43       down      N/A                          Oper state not up
Te1/0/44       down      N/A                          Oper state not up
Te1/0/45       down      N/A                          Oper state not up
Te1/0/46       down      N/A                          Oper state not up
Te1/0/47       down      N/A                          Oper state not up
Te1/0/48       down      N/A                          Oper state not up
Te1/1/1        down      N/A                          Oper state not up
Te1/1/2        down      N/A                          Oper state not up
Te1/1/3        down      N/A                          Oper state not up
Te1/1/4        down      N/A                          Oper state not up
Te1/1/5        down      N/A                          Oper state not up
Te1/1/6        down      N/A                          Oper state not up
Te1/1/7        down      N/A                          Oper state not up
Te1/1/8        down      N/A                          Oper state not up
Te1/1/9        down      N/A                          Oper state not up
```

```
Te1/1/10       down      N/A                        Oper state not up
Te1/1/11       down      N/A                        Oper state not up
Te1/1/12       down      N/A                        Oper state not up
Te1/1/13       down      N/A                        Oper state not up
Te1/1/14       down      N/A                        Oper state not up
Te1/1/15       down      N/A                        Oper state not up
Te1/1/16       down      N/A                        Oper state not up
Fo1/1/1        down      N/A                        Oper state not up
Fo1/1/2        down      N/A                        Oper state not up
Fo1/1/3        down      N/A                        Oper state not up
Fo1/1/4        down      N/A                        Oper state not up
-----------------------------------------------------------------------------------------------------------
```

次に、AVB ストリーム情報を表示する例を示します。

```
Device#show avb streams

Stream ID:         0011.0100.0001:1    Incoming Interface:    Te1/1/1
    Destination  : 91E0.F000.FE00
    Class        : A
    Rank         : 1
    Bandwidth    : 6400 Kbit/s

    Outgoing Interfaces:

-------------------------------------------------------------------------

    Interface        State      Time of Last Update        Information


-------------------------------------------------------------------------

    Te1/1/1           Ready      Tue Apr 26 01:25:40.634


Stream ID:         0011.0100.0002:2    Incoming Interface:    Te1/1/1
    Destination  : 91E0.F000.FE01
    Class        : A
    Rank         : 1
    Bandwidth    : 6400 Kbit/s

    Outgoing Interfaces:

-------------------------------------------------------------------------

    Interface        State      Time of Last Update        Information


-------------------------------------------------------------------------

    Te1/1/1           Ready      Tue Apr 26 01:25:40.634
```

関連トピック

AVB の設定 （8 ページ）
オーディオ ビデオ ブリッジング（AVB）について （1 ページ）

gPTP の例

このコマンドは、インターフェイスの ptp の簡易ステータスを表示するために使用できます。

```
Device#show ptp brief

Interface                       Domain    PTP State
FortyGigabitEthernet1/1/1       0         FAULTY
FortyGigabitEthernet1/1/2       0         SLAVE
GigabitEthernet1/1/1            0         FAULTY
GigabitEthernet1/1/2            0         FAULTY
GigabitEthernet1/1/3            0         FAULTY
GigabitEthernet1/1/4            0         FAULTY
TenGigabitEthernet1/0/1         0         FAULTY
TenGigabitEthernet1/0/2         0         FAULTY
TenGigabitEthernet1/0/3         0         MASTER
TenGigabitEthernet1/0/4         0         FAULTY
TenGigabitEthernet1/0/5         0         FAULTY
TenGigabitEthernet1/0/6         0         FAULTY
TenGigabitEthernet1/0/7         0         MASTER
TenGigabitEthernet1/0/8         0         FAULTY
TenGigabitEthernet1/0/9         0         FAULTY
TenGigabitEthernet1/0/10        0         FAULTY
TenGigabitEthernet1/0/11        0         MASTER
TenGigabitEthernet1/0/12        0         FAULTY
TenGigabitEthernet1/0/13        0         FAULTY
TenGigabitEthernet1/0/14        0         FAULTY
TenGigabitEthernet1/0/15        0         FAULTY
TenGigabitEthernet1/0/16        0         FAULTY
TenGigabitEthernet1/0/17        0         FAULTY
TenGigabitEthernet1/0/18        0         FAULTY
TenGigabitEthernet1/0/19        0         MASTER
TenGigabitEthernet1/0/20        0         FAULTY
TenGigabitEthernet1/0/21        0         FAULTY
TenGigabitEthernet1/0/22        0         FAULTY
TenGigabitEthernet1/0/23        0         FAULTY
TenGigabitEthernet1/0/24        0         FAULTY
TenGigabitEthernet1/1/1         0         FAULTY
TenGigabitEthernet1/1/2         0         FAULTY
TenGigabitEthernet1/1/3         0         FAULTY
TenGigabitEthernet1/1/4         0         FAULTY
TenGigabitEthernet1/1/5         0         FAULTY
TenGigabitEthernet1/1/6         0         FAULTY
TenGigabitEthernet1/1/7         0         FAULTY
TenGigabitEthernet1/1/8         0         FAULTY
```

このコマンドは、ptp クロック情報を表示するために使用できます。

```
Device#show ptp clock

PTP CLOCK INFO
  PTP Device Type: Boundary clock
  PTP Device Profile: IEEE 802/1AS Profile
  Clock Identity: 0x4:6C:9D:FF:FE:4F:95:0
  Clock Domain: 0
  Number of PTP ports: 38
  PTP Packet priority: 4
  Priority1: 128
  Priority2: 128
  Clock Quality:
        Class: 248
        Accuracy: Unknown
        Offset (log variance): 16640
  Offset From Master(ns): 0
  Mean Path Delay(ns): 0
  Steps Removed: 3
  Local clock time: 00:12:13 UTC Jan 1 1970
```

このコマンドは、親のクロック情報を表示するために使用できます。

```
Device#show ptp parent

PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0xB0:7D:47:FF:FE:9E:B6:80
  Parent Port Number: 3
  Observed Parent Offset (log variance): 16640
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x4:6C:9D:FF:FE:67:3A:80
  Grandmaster Clock Quality:
        Class: 248
        Accuracy: Unknown
        Offset (log variance): 16640
        Priority1: 0
        Priority2: 128
```

このコマンドは、ptp ポート情報を表示するために使用できます。

```
Device#show ptp port

PTP PORT DATASET: FortyGigabitEthernet1/1/1
```

```
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 1
  PTP version: 2
  Port state: FAULTY
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000000

 PTP PORT DATASET: FortyGigabitEthernet1/1/2
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 2
  PTP version: 2
  Port state: FAULTY
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
 --More—
```

このコマンドは、特定のインターフェイスのポート情報を表示するために使用できます。

```
Device#show ptp port gi1/0/26

PTP PORT DATASET: GigabitEthernet1/0/26
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 28
  PTP version: 2
  Port state: MASTER
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
  Sync interval(log mean): 0
  Delay Mechanism: Peer to Peer
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000000
```

このコマンドは、を表示するために使用できます。

```
Device#show platform software fed switch active ptp if-id 0x20

Displaying port data for if_id 20
========================================
```

```
Port Mac Address 04:6C:9D:4E:3A:9A
Port Clock Identity 04:6C:9D:FF:FE:4E:3A:80
Port number 28
PTP Version 2
domain_value 0
dot1as capable: FALSE
sync_recpt_timeout_time_interval 375000000 nanoseconds
sync_interval 125000000 nanoseconds
neighbor_rate_ratio 0.000000
neighbor_prop_delay 0 nanoseconds
compute_neighbor_rate_ratio: TRUE
compute_neighbor_prop_delay: TRUE
port_enabled: TRUE
ptt_port_enabled: TRUE
current_log_pdelay_req_interval 0
pdelay_req_interval 0 nanoseconds
allowed_lost_responses 3
neighbor_prop_delay_threshold 2000 nanoseconds
is_measuring_delay : FALSE
Port state: : MASTER
sync_seq_num 22023
delay_req_seq_num 23857
num sync messages transmitted  0
num sync messages received  0
num followup messages transmitted  0
num followup messages received  0
num pdelay requests transmitted  285695
num pdelay requests received  0
num pdelay responses transmitted  0
num pdelay responses received 0
num pdelay followup responses transmitted  0
num pdelay followup responses received  0
```

関連トピック

gPTP の設定 （10 ページ）
Generalized Precision Time Protocol（gPTP）について （4 ページ）

MSRP の例

次に、MSRP ストリーム情報を表示する例を示します。

```
Device#show msrp streams

-------------------------------------------------------------------------------
Stream ID Talker Listener
Advertise Fail Ready ReadyFail AskFail
R | D R | D R | D R | D R | D
-------------------------------------------------------------------------------
yy:yy:yy:yy:yy:yy:0001 1 | 2 0 | 0 1 | 0 0 | 1 1 | 0
zz:zz:zz:zz:zz:zz:0002 1 | 0 0 | 1 1 | 0 0 | 0 0 | 1
```

次に、詳細な MSRP ストリーム情報を表示する例を示します。

```
Device#show msrp streams detail

Stream ID:         0011.0100.0001:1
    Stream Age: 01:57:46 (since Mon Apr 25 23:41:11.413)
    Create Time: Mon Apr 25 23:41:11.413
    Destination Address: 91E0.F000.FE00
    VLAN Identifier: 1
    Data Frame Priority: 3 (Class A)
    MaxFrameSize: 100
    MaxIntervalFrames: 1 frames/125us
    Stream Bandwidth: 6400 Kbit/s
    Rank: 1
    Received Accumulated Latency: 20
    Stream Attributes Table:

---------------------------------------------------------------------------

    Interface          Attr State    Direction    Type

---------------------------------------------------------------------------

      Gi1/0/1          Register       Talker      Advertise
      Attribute Age: 01:57:46 (since Mon Apr 25 23:41:11.413)
      MRP Applicant: Very Anxious Observer, send None
      MRP Registrar: In
      Accumulated Latency: 20
    ----
      Te1/1/1         Declare         Talker      Advertise
      Attribute Age: 00:19:52 (since Tue Apr 26 01:19:05.525)
      MRP Applicant: Quiet Active, send None
      MRP Registrar: In
      Accumulated Latency: 20
    ----
      Te1/1/1         Register        Listener    Ready
      Attribute Age: 00:13:17 (since Tue Apr 26 01:25:40.635)
      MRP Applicant: Very Anxious Observer, send None
      MRP Registrar: In
    ----
      Gi1/0/1         Declare         Listener    Ready
      Attribute Age: 00:13:17 (since Tue Apr 26 01:25:40.649)
      MRP Applicant: Quiet Active, send None
      MRP Registrar: In
```

次に、MSRP ストリーム情報を簡潔に表示する例を示します。

```
Device#show msrp streams brief
```

```
Legend: R = Registered, D = Declared.
--------------------------------------------------------------------------------
Stream ID              Destination         Bandwidth   Talkers
Listeners  Fail
                       Address              (Kbit/s)    R | D      R |
 D
--------------------------------------------------------------------------------
0011.0100.0001:1       91E0.F000.FE00     6400          1 | 1      1 |
 1    No
0011.0100.0002:2       91E0.F000.FE01     6400          1 | 1      1 |
 1    No
0011.0100.0003:3       91E0.F000.FE02     6400          1 | 1      1 |
 1    No
0011.0100.0004:4       91E0.F000.FE03     6400          1 | 1      1 |
 1    No
0011.0100.0005:5       91E0.F000.FE04     6400          1 | 1      1 |
 1    No
0011.0100.0006:6       91E0.F000.FE05     6400          1 | 1      1 |
 1    No
0011.0100.0007:7       91E0.F000.FE06     6400          1 | 1      1 |
 1    No
0011.0100.0008:8       91E0.F000.FE07     6400          1 | 1      1 |
 1    No
0011.0100.0009:9       91E0.F000.FE08     6400          1 | 1      1 |
 1    No
0011.0100.000A:10      91E0.F000.FE09     6400          1 | 1      1 |
 1    No
--------------------------------------------------------------------------------
```

次に、MSRP ポート帯域幅情報を表示する例を示します。

```
Device#show msrp port bandwidth

--------------------------------------------------------------------------------
Ethernet      Capacity       Assigned       Available       Reserved

Interface     (Kbit/s)        A | B          A | B           A | B
--------------------------------------------------------------------------------
Te1/0/1     10000000         75 | 0         75 | 75          0 | 0
Te1/0/2     10000000         75 | 0         75 | 75          0 | 0
Te1/0/3     1000000          75 | 0         75 | 75          0 | 0
Te1/0/4     10000000         75 | 0         75 | 75          0 | 0
Te1/0/5     10000000         75 | 0         75 | 75          0 | 0
Te1/0/6     10000000         75 | 0         75 | 75          0 | 0
Te1/0/8     10000000         75 | 0         75 | 75          0 | 0
Te1/0/9     10000000         75 | 0         75 | 75          0 | 0
Te1/0/10    10000000         75 | 0         75 | 75          0 | 0
Te1/0/11    10000000         75 | 0         75 | 75          0 | 0
Te1/0/12    10000000         75 | 0         75 | 75          0 | 0
Te1/0/13    1000000          75 | 0         75 | 75          0 | 0
```

```
Te1/0/14    10000000        75 | 0        75 | 75        0 | 0
Te1/0/15    10000000        75 | 0        75 | 75        0 | 0
Te1/0/16    10000000        75 | 0        75 | 75        0 | 0
Te1/0/17    10000000        75 | 0        75 | 75        0 | 0
Te1/0/18    10000000        75 | 0        75 | 75        0 | 0
Te1/0/19    1000000         75 | 0        75 | 75        0 | 0
Te1/0/20    10000000        75 | 0        75 | 75        0 | 0
Te1/0/21    10000000        75 | 0        75 | 75        0 | 0
Te1/0/22    10000000        75 | 0        75 | 75        0 | 0
Te1/0/23    10000000        75 | 0        75 | 75        0 | 0
Te1/0/24    10000000        75 | 0        75 | 75        0 | 0
Gi1/1/1     1000000         75 | 0        75 | 75        0 | 0
Gi1/1/2     1000000         75 | 0        75 | 75        0 | 0
Gi1/1/3     1000000         75 | 0        75 | 75        0 | 0
Gi1/1/4     1000000         75 | 0        75 | 75        0 | 0
Te1/1/1     10000000        75 | 0        75 | 75        0 | 0
Te1/1/2     10000000        75 | 0        75 | 75        0 | 0
Te1/1/3     10000000        75 | 0        75 | 75        0 | 0
Te1/1/4     10000000        75 | 0        75 | 75        0 | 0
Te1/1/5     10000000        75 | 0        75 | 75        0 | 0
Te1/1/6     10000000        75 | 0        75 | 75        0 | 0
Te1/1/7     10000000        75 | 0        75 | 75        0 | 0
Te1/1/8     10000000        75 | 0        75 | 75        0 | 0
Fo1/1/1     40000000        75 | 0        75 | 75        0 | 0
Fo1/1/2     40000000        75 | 0        75 | 75        0 | 0
```

関連トピック

Multiple Stream Reservation Protocol（MSRP）について （5 ページ）

HQoS の例

次に、AVB が有効になっている場合に、すべてのポリシー マップ設定の詳細を表示する例を示します。

```
Device#show policy-map

  Policy Map AVB-Input-Policy-Remark-B
    Class AVB-SR-CLASS-A
      set cos 3
    Class AVB-SR-CLASS-B
      set cos 0
    Class class-default
      service-policy AVB-Input-Child-Policy

  Policy Map AVB-Input-Policy-Remark-A
    Class AVB-SR-CLASS-A
      set cos 0
    Class AVB-SR-CLASS-B
      set cos 2
    Class class-default
      service-policy AVB-Input-Child-Policy
```

```
Policy Map AVB-Output-Policy-Default
  Class AVB-SR-CLASS-A
    priority level 1 1 (%)
  Class AVB-SR-CLASS-B
    priority level 2 1 (%)
  Class AVB-CONTROL-MGMT-QUEUE
    priority level 3 15 (%)
  Class class-default
    bandwidth remaining 100 (%)
    queue-buffers ratio 70
    service-policy AVB-Output-Child-Policy

Policy Map AVB-Input-Policy-Remark-AB
  Class AVB-SR-CLASS-A
    set cos 0
  Class AVB-SR-CLASS-B
    set cos 0
  Class class-default
    service-policy AVB-Input-Child-Policy

Policy Map AVB-Input-Policy-Remark-None
  Class AVB-SR-CLASS-A
    set cos 3
  Class AVB-SR-CLASS-B
    set cos 2
  Class class-default
    service-policy AVB-Input-Child-Policy

Policy Map AVB-Input-Child-Policy
  Class AVB-VOIP-DATA-CLASS
    set dscp ef
  Class AVB-MULTIMEDIA-CONF-CLASS
    set dscp af41
  Class AVB-BULK-DATA-CLASS
   set dscp af11
  Class AVB-TRANSACTIONAL-DATA-CLASS
    set dscp af21
  Class AVB-SCAVENGER-DATA-CLASS
    set dscp cs1
  Class AVB-SIGNALING-CLASS
    set dscp cs3
  Class class-default
    set dscp default

Policy Map AVB-Output-Child-Policy
  Class AVB-VOIP-PRIORITY-QUEUE
    bandwidth remaining 30 (%)
    queue-buffers ratio 30
  Class AVB-MULTIMEDIA-CONF-STREAMING-QUEUE
    bandwidth remaining 15 (%)
```

```
      queue-limit dscp af41 percent 80
      queue-limit dscp af31 percent 80
      queue-limit dscp af42 percent 90
      queue-limit dscp af32 percent 90
      queue-buffers ratio 15
    Class AVB-TRANSACTIONAL-DATA-QUEUE
      bandwidth remaining 15 (%)
      queue-limit dscp af21 percent 80
      queue-limit dscp af22 percent 90
      queue-buffers ratio 15
    Class AVB-BULK-SCAVENGER-DATA-QUEUE
      bandwidth remaining 15 (%)
      queue-limit dscp af11 percent 80
      queue-limit dscp af12 percent 90
      queue-limit dscp cs1 percent 80
      queue-buffers ratio 15
    Class class-default
      bandwidth remaining 25 (%)
      queue-buffers ratio 25
```

次に、AVB が無効になっている場合に、すべてのポリシー マップ設定の詳細を表示する例を示します。

```
Device#show policy-map

Building configuration...

Current configuration : 2079 bytes
!
policy-map AVB-Input-Child-Policy
class AVB-VOIP-DATA-CLASS
  set dscp ef
class AVB-MULTIMEDIA-CONF-CLASS
  set dscp af41
class AVB-BULK-DATA-CLASS
  set dscp af11
class AVB-TRANSACTIONAL-DATA-CLASS
  set dscp af21
class AVB-SCAVENGER-DATA-CLASS
  set dscp cs1
class AVB-SIGNALING-CLASS
  set dscp cs3
class class-default
  set dscp default
policy-map AVB-Output-Child-Policy
class AVB-VOIP-PRIORITY-QUEUE
  bandwidth remaining percent 30
```

```
  queue-buffers ratio 30
class AVB-MULTIMEDIA-CONF-STREAMING-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp af41 percent 80
  queue-limit dscp af31 percent 80
  queue-limit dscp af42 percent 90
  queue-limit dscp af32 percent 90
  queue-buffers ratio 15
class AVB-TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp af21 percent 80
  queue-limit dscp af22 percent 90
  queue-buffers ratio 15
class AVB-BULK-SCAVENGER-DATA-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp af11 percent 80
  queue-limit dscp af12 percent 90
  queue-limit dscp cs1 percent 80
  queue-buffers ratio 15
class class-default
  bandwidth remaining percent 25
  queue-buffers ratio 25
!
end
```

次に、AVB が有効になっている場合に、すべてのクラス マップ設定の詳細を表示する例を示します。

```
Device#show class-map

Class Map match-any AVB-VOIP-DATA-CLASS (id 31)
   Match   dscp ef (46)
   Match cos  5

Class Map match-any AVB-BULK-DATA-CLASS (id 33)
   Match access-group name AVB-BULK-DATA-CLASS-ACL

Class Map match-any AVB-VOIP-PRIORITY-QUEUE (id 37)
   Match   dscp cs4 (32) cs5 (40) ef (46)
   Match   precedence 4  5
   Match cos  5

Class Map match-any AVB-MULTIMEDIA-CONF-CLASS (id 32)
   Match access-group name AVB-MULTIMEDIA-CONF-CLASS-ACL

Class Map match-any AVB-SIGNALING-CLASS (id 36)
   Match access-group name AVB-SIGNALING-CLASS-ACL
```

```
Class Map match-any AVB-MULTIMEDIA-CONF-STREAMING-QUEUE (id 38)
   Match   dscp af41 (34) af42 (36) af43 (38)
   Match   dscp af31 (26) af32 (28) af33 (30)
   Match cos  4

Class Map match-any AVB-BULK-SCAVENGER-DATA-QUEUE (id 40)
   Match   dscp cs1 (8) af11 (10) af12 (12) af13 (14)
   Match   precedence 1
   Match cos  1

Class Map match-any AVB-TRANSACTIONAL-DATA-CLASS (id 34)
   Match access-group name AVB-TRANSACTIONAL-DATA-CLASS-ACL

Class Map match-any AVB-TRANSACTIONAL-DATA-QUEUE (id 39)
   Match   dscp af21 (18) af22 (20) af23 (22)

Class Map match-any AVB-SR-CLASS-B (id 42)
   Match cos  2

Class Map match-any AVB-SR-CLASS-A (id 41)
   Match cos  3

Class Map match-any AVB-SCAVENGER-DATA-CLASS (id 35)
   Match access-group name AVB-SCAVENGER-DATA-CLASS-ACL

Class Map match-any AVB-CONTROL-MGMT-QUEUE (id 43)
   Match ip  dscp cs2 (16)
   Match ip  dscp cs3 (24)
   Match ip  dscp cs6 (48)
   Match ip  dscp cs7 (56)
   Match ip  precedence 6
   Match ip  precedence 7
   Match ip  precedence 3
   Match ip  precedence 2
   Match cos  6
   Match cos  7
```

次に、AVB が無効になっている場合に、すべてのクラス マップ設定の詳細を表示する例を示します。

```
Device#show class-map

Building configuration...

Current configuration : 2650 bytes
!
class-map match-any AVB-VOIP-DATA-CLASS
match dscp ef
 match cos  5
```

```
class-map match-any AVB-BULK-DATA-CLASS
match access-group name AVB-BULK-DATA-CLASS-ACL
class-map match-any AVB-VOIP-PRIORITY-QUEUE
match dscp cs4  cs5  ef
 match precedence 4  5
 match cos  5
class-map match-any AVB-MULTIMEDIA-CONF-CLASS
match access-group name AVB-MULTIMEDIA-CONF-CLASS-ACL
class-map match-any AVB-SIGNALING-CLASS
match access-group name AVB-SIGNALING-CLASS-ACL
class-map match-any AVB-MULTIMEDIA-CONF-STREAMING-QUEUE
match dscp af41  af42  af43
 match dscp af31  af32  af33
 match cos  4
class-map match-any AVB-BULK-SCAVENGER-DATA-QUEUE
match dscp cs1  af11  af12  af13
 match precedence 1
 match cos  1
class-map match-any AVB-TRANSACTIONAL-DATA-CLASS
match access-group name AVB-TRANSACTIONAL-DATA-CLASS-ACL
class-map match-any AVB-TRANSACTIONAL-DATA-QUEUE
match dscp af21  af22  af23
class-map match-any AVB-SCAVENGER-DATA-CLASS
match access-group name AVB-SCAVENGER-DATA-CLASS-ACL
end
```

次に、すべての AVB QoS 統計情報を表示する例を示します。

```
Device#show policy-map interface gigabitEthernet 1/0/15

GigabitEthernet1/0/15

  Service-policy input: AVB-Input-Policy-Remark-AB

    Class-map: AVB-SR-CLASS-A (match-any)
      0 packets
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos 0

    Class-map: AVB-SR-CLASS-B (match-any)
      0 packets
      Match: cos  2
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos 0
```

```
Class-map: class-default (match-any)
  0 packets
  Match: any

  Service-policy : AVB-Input-Child-Policy

    Class-map: AVB-VOIP-DATA-CLASS (match-any)
      0 packets
      Match:  dscp ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos 3

    Class-map: AVB-MULTIMEDIA-CONF-CLASS (match-any)
      0 packets
      Match: access-group name AVB-MULTIMEDIA-CONF-CLASS-ACL
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af41

    Class-map: AVB-BULK-DATA-CLASS (match-any)
      0 packets
      Match: access-group name AVB-BULK-DATA-CLASS-ACL
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af11

    Class-map: AVB-TRANSACTIONAL-DATA-CLASS (match-any)
      0 packets
      Match: access-group name AVB-TRANSACTIONAL-DATA-CLASS-ACL
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af21

    Class-map: AVB-SCAVENGER-DATA-CLASS (match-any)
      0 packets
      Match: access-group name AVB-SCAVENGER-DATA-CLASS-ACL
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp cs1

    Class-map: AVB-SIGNALING-CLASS (match-any)
      0 packets
```

```
        Match: access-group name AVB-SIGNALING-CLASS-ACL
          0 packets, 0 bytes
          5 minute rate 0 bps
        QoS Set
          dscp cs3

      Class-map: class-default (match-any)
        0 packets
        Match: any
        QoS Set
          dscp default

Service-policy output: AVB-Output-Policy-Default

  queue stats for all priority classes:
    Queueing
    priority level 3

    (total drops) 0
    (bytes output) 7595

  queue stats for all priority classes:
    Queueing
    priority level 2

    (total drops) 0
    (bytes output) 0

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AVB-SR-CLASS-A (match-any)
    0 packets
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 1% (10000 kbps), burst bytes 250000,

    Priority Level: 1

  Class-map: AVB-SR-CLASS-B (match-any)
    0 packets
    Match: cos  2
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 1% (10000 kbps), burst bytes 250000,
```

```
  Priority Level: 2

Class-map: AVB-CONTROL-MGMT-QUEUE (match-any)
  0 packets
  Match: ip dscp cs2 (16)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip dscp cs3 (24)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip dscp cs6 (48)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip dscp cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip precedence 6
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip precedence 7
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip precedence 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip precedence 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  6
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  7
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 15% (150000 kbps), burst bytes 3750000,

  Priority Level: 3

Class-map: class-default (match-any)
  0 packets
  Match: any
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 80%
  queue-buffers ratio 70

  Service-policy : AVB-Output-Child-Policy

    Class-map: AVB-VOIP-PRIORITY-QUEUE (match-any)
```

```
  0 packets
  Match:  dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match:  precedence 4  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 30%
  queue-buffers ratio 30

Class-map: AVB-MULTIMEDIA-CONF-STREAMING-QUEUE (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  queue-limit dscp 26 percent 80
  queue-limit dscp 28 percent 90
  queue-limit dscp 34 percent 80
  queue-limit dscp 36 percent 90
  (total drops) 0
  (bytes output) 0
  bandwidth remaining 15%

  queue-buffers ratio 15

Class-map: AVB-TRANSACTIONAL-DATA-QUEUE (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  0
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  queue-limit dscp 18 percent 80
```

```
    queue-limit dscp 20 percent 90
    (total drops) 0
    (bytes output) 0
    bandwidth remaining 15%

    queue-buffers ratio 15

  Class-map: AVB-BULK-SCAVENGER-DATA-QUEUE (match-any)
    0 packets
    Match:  dscp cs1 (8) af11 (10) af12 (12) af13 (14)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match:  precedence 1
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  1
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    queue-limit dscp 8 percent 80
    queue-limit dscp 10 percent 80
    queue-limit dscp 12 percent 90
    (total drops) 0
    (bytes output) 0
    bandwidth remaining 15%

    queue-buffers ratio 15

  Class-map: class-default (match-any)
    0 packets
    Match: any
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

関連トピック

HQoS の設定 （12 ページ）
QoSHQoS について （6 ページ）

MVRP の例

次に、MVRP サマリー情報を表示する例を示します。

```
Device#show mvrp summary

MVRP global state           : enabled
```

```
MVRP VLAN creation          : enabled
VLANs created via MVRP      : 2,567
MAC learning auto provision : disabled
Learning disabled on VLANs  : none
----------------------------------------------------------------------------------------------------------------
```

次に、インターフェイス MVRP 情報を表示する例を示します。

```
Device#show mvrp interface

Port          Status    Registrar State
Te1/0/47      on              normal
Te1/1/3       off             normal

Port          Join Timeout       Leave Timeout   Leaveall Timeout
Periodic

Timeout
Te1/0/47      20                 60              1000               100
Te1/1/3       20                 60              1000               100

Port          Vlans Declared
Te1/0/47      1-2,567,900
Te1/1/3       none

Port          Vlans Registered
Te1/0/47      2,567
Te1/1/3       none

Port          Vlans Registered and in Spanning Tree Forwarding State
Te1/0/47      2,567
Te1/1/3       none
```

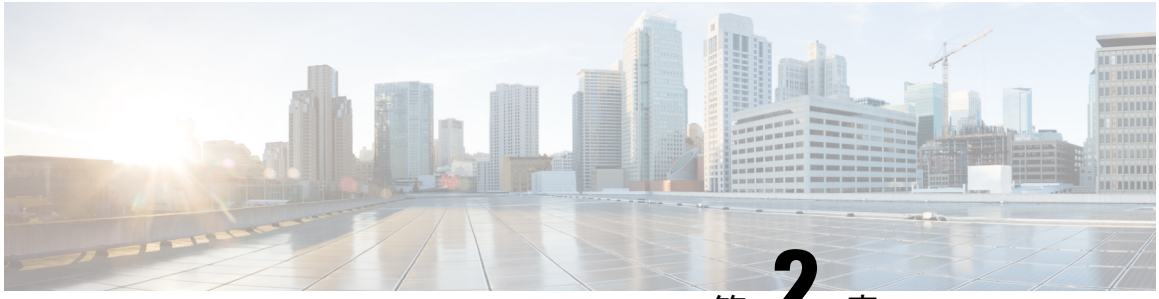
関連トピック

MVRP の設定 （14 ページ）
マルチ VLAN 登録プロトコル（MVRP）について （7 ページ）

第 II 部

キャンパス ファブリック

• キャンパス ファブリック （43 ページ）



第 2 章

キャンパス ファブリック

-
- キャンパス ファブリック （43 ページ）

キャンパス ファブリック

キャンパス ファブリックでは、ポリシーベースのセグメンテーションの構成に基づいて仮想ネットワークを構築する基本的なインフラストラクチャが提供されます。このモジュールでは、デバイス上でキャンパス ファブリックを設定する方法について説明します。

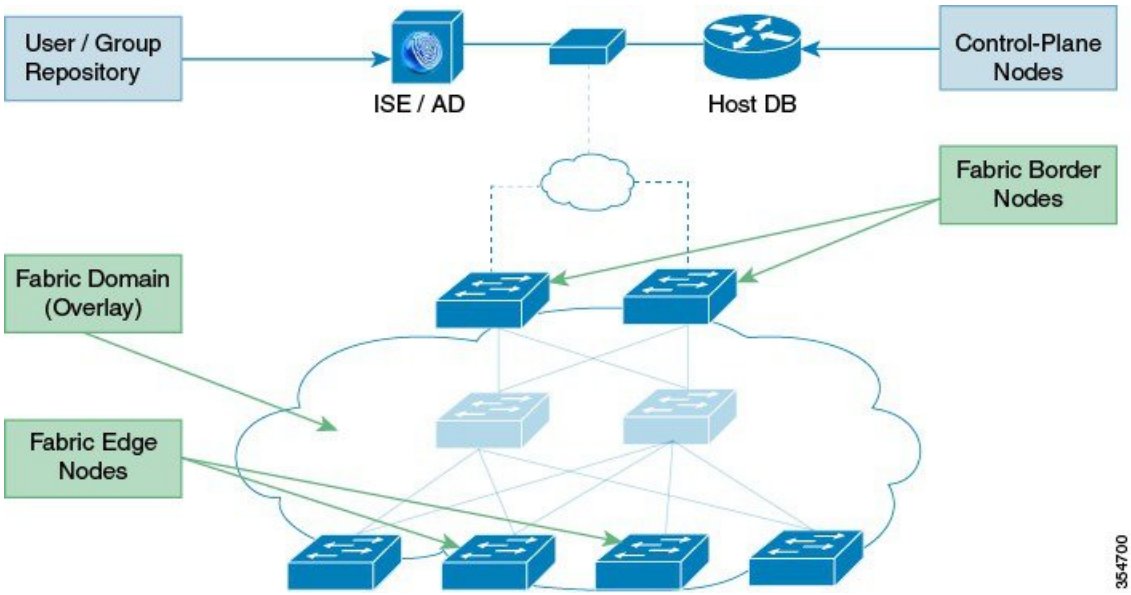
キャンパス ファブリックの概要

キャンパス ファブリック オーバーレイ プロビジョニングは、3 つの主要コンポーネントで構成されます。

- コントロール プレーン
- データ プレーン
- ポリシー プレーン

ファブリック ドメイン要素について

次の図は、ファブリック ドメインを構成する要素を示しています。



- ファブリック エッジ デバイス：ファブリック ドメインに接続するユーザとデバイスに接続性を提供します。ファブリックエッジデバイスは、エンドポイントを識別して認証し、エンドポイント ID 情報をファブリック ホスト追跡データベースに登録します。また、入力時にカプセル化を、出力時にカプセル化解除を行い、ファブリック ドメインに接続されたエンドポイント間でトラフィックの転送を行います。
- ファブリック コントロール プレーン デバイス：ホスト追跡データベースに、オーバーレイ到達可能性情報および endpoints-to-routing-locator マッピングを提供します。コントロール プレーン デバイスは、ローカルエンドポイントを持つファブリック エッジデバイスから登録を受信し、エッジ デバイスからのリモート エンドポイントを検索する要求を解決します。ネットワークに冗長性をもたせるために、内部（ファブリック境界デバイス）および外部（Cisco CSR1000v などの指定されたコントロール プレーン デバイス）に最大 3 台のコントロール プレーン デバイスを設定できます。
- ファブリック境界デバイス：従来のレイヤ3ネットワークまたは異なるファブリック ドメインをローカル ドメインに接続し、VRF および SGT 情報などの到達可能性情報とポリシー情報を 1 つのドメインから別のドメインに変換します。
- 仮想コンテキスト：レイヤ3ルーティングテーブルの複数のインスタンスを作成するために、Virtual Routing and Forwarding（VRF）を使用して、デバイス レベルで仮想化を提供します。コンテキストまたは VRF は、IP アドレス全体のセグメンテーションを行い、オーバーラップしたアドレス空間とトラフィックの分離を可能にします。ファブリック ドメインに最大 32 のコンテキストを設定できます。
- ホスト プール：ファブリック ドメイン内のエンドポイントを IP プールにグループ化し、VLAN ID および IP サブネットで識別します。

キャンパス ファブリック設定時の注意事項

キャンパスファブリック要素を設定する場合は、次の注意事項および制約事項を考慮してください。

- 各ファブリック ドメインに設定するコントロール プレーン デバイスは 3 台までです。
- 各ファブリック エッジ デバイスは、最大 2000 のホストをサポートします。
- 各コントロール プレーン デバイスは、最大 5000 のファブリック エッジ デバイス登録をサポートします。
- 各ファブリック ドメインに設定する仮想コンテキストは 32 個までです。

ファブリック オーバーレイの設定方法

ファブリック エッジ デバイスの設定

ファブリック エッジ デバイスを設定するには、次の手順を実行します。

始める前に

デバイスが確実に到達できるように、各エッジ デバイスに loopback0 IP アドレスを設定します。 **ip lisp source-locator loopback0** コマンドをアップリンク インターフェイスで実行していることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**fabric auto** 例： `Device(config)#fabric auto`	自動ファブリックプロビジョニングを有効にして、自動ファブリック コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的

ステップ 4	**domain** {**default** | **name** *fabric domain name*}
	例：
	`Device(config-fabric-auto)#domain default`
	`Device(config-fabric-auto)#domain name exampledomain`
		デフォルトのファブリック ドメインを設定し、ドメイン コンフィギュレーションモードを開始します。**name** キーワードを使用して、新しいファブリック ドメインを追加することができます。このコマンドの **no** バージョンを使用すると、ファブリック ドメインが削除されます。デフォルト ドメインを設定するか、または新しいファブリック ドメインを作成できますが、両方はできません。

ステップ 5	**control-plane** *ipv4 address* **auth_key** *key* 例： `Device(config-fabric-auto-domain)#control-plane 198.51.100.2 auth_key examplekey123`	コントロール プレーン デバイスの IP アドレスおよび認証キーを設定して、ファブリック エッジデバイスがコントロールプレーンデバイスと通信できるようにします。 非コントロール プレーンの **control-plane** *ipv4 address* **auth_key** *key* コマンドを使用すると、ファブリック ドメインからコントロールプレーンデバイスが削除されます。エッジデバイスには、最大 3 つのコントロール プレーンの IP アドレスを指定できます。
ステップ 6	**border** *ipv4 address* 例： `Device(config-fabric-auto-domain)#border 198.51.100.4`	ファブリック境界デバイスの IP アドレスを設定し、ファブリック エッジデバイスがファブリック境界デバイスと通信できるようにします。エッジデバイスには、最大 2 つの境界 IP アドレスを指定できます。
ステップ 7	**context name** *name* **id** *ID* 例： `Device(config-fabric-auto-domain)#context name eg-context id 10`	新しいコンテキストをファブリック ドメインで作成し、それに ID を割り当てます。コンテキストまたは VRF は、IP アドレス全体のセグメンテーションを行い、オーバーラップしたアドレス空間とトラフィックの分離を可能にします。ファブリック ドメインに最大 32 のコンテキストを設定できます。この手順は、ホストプールにコンテキストを関連付ける場合に必須となります。

	コマンドまたはアクション	目的
ステップ 8	**host-pool name** *name* 例： `Device(config-fabric-auto-domain)#host-pool name VOICE_DOMAIN`	ファブリック ドメインのエンドポイントをグループ化するための IP プールを作成し、ホスト プール コンフィギュレーション モードを開始します。
ステップ 9	**host-vlan** *ID* 例： `Device(config-fabric-auto-domain-host-pool)#host-vlan 10`	ホスト プールに関連付ける VLAN ID を設定します。
ステップ 10	**context name** *name* 例： `Device(config-fabric-auto-domain-host-pool)#context name eg-context`	（任意）コンテキストまたは VRF をホスト プールに関連付けます。ファブリック ドメインに最大 32 のコンテキストを設定できます。
ステップ 11	**gateway** *IP address/ mask* 例： `Device(config-fabric-auto-domain-host-pool)#gateway 192.168.1.254/24`	ホスト プールのルーティング ゲートウェイ IP アドレスとサブネット マスクを設定します。このアドレスおよびサブネットマスクは、アンダーレイに接続しているアップリンク インターフェイスにエンドポイントをマッピングするために使用されます。
ステップ 12	**use-dhcp** *IP address* 例： `Device(config-fabric-auto-domain-host-pool)#use-dhcp 172.10.1.1`	ホスト プールの DHCP サーバ アドレスを設定します。ホストプールに複数の DHCP アドレスを設定できます。DHCP サーバ アドレスを削除するには、**no use-dhcp** *IP address* コマンドを使用します。
ステップ 13	**exit** 例： `Device(config-fabric-auto-domain)# exit`	
ステップ 14	**show fabric domain** 例： `Device# show fabric domain`	ファブリック ドメインの設定を表示します。この設定の一部として、追加の CLI コマンドが自動的に生成されます。詳細については、「ファブリック エッジ デバイスの自動設定されたコマンド」を参照してください。ファブリッ

	コマンドまたはアクション	目的
		クエッジデバイスの自動設定されたコマンド （48 ページ）

ファブリック エッジ デバイスの自動設定されたコマンド

ファブリック オーバーレイ プロビジョニングの一部として、一部の LISP ベースの設定、SGT（セキュリティ グループ タグ）設定および EID から RLOC へのマッピング設定が自動生成され、実行コンフィギュレーションで表示されます。

たとえば、エッジ デバイス（ループバック アドレス 2.1.1.1/32）に対する次の設定シナリオを考えてみます。

```
device(config)#fabric auto
device(config-fabric-auto)#domain default
device(config-fabric-auto-domain)#control-plane 192.168.1.4 auth-key example-key1
device(config-fabric-auto-domain)#control-plane 192.168.1.5 auth-key example-key2
device(config-fabric-auto-domain)#border 192.168.1.6
device(config-fabric-auto-domain)#context name example-context ID 10
device(config-fabric-auto-domain)#host-pool name VOICE_DOMAIN
device(config-fabric-auto-domain-host-pool)#vlan 10
device(config-fabric-auto-domain-host-pool)#context example-context
device(config-fabric-auto-domain-host-pool)#gateway 192.168.1.254/24
device(config-fabric-auto-domain-host-pool)#use-dhcp 209.165.201.6
```

以下は、ファブリック エッジ設定の出力例です。

```
device#show running-config
router lisp
encapsulation vxlan
locator-set default.RLOC
IPv4-interface Loopback0 priority 10 weight 10
exit
!
eid-table default instance-id 0
exit
!
eid-table vrf example-context instance-id 10
dynamic-eid example-context.EID.VOICE_DOMAIN
database-mapping 192.168.1.0/24 locator-set default.RLOC
exit
!
exit
!
loc-reach-algorithm lsb-reports ignore
disable-ttl-propagate
ipv4 sgt
ipv4 use-petr 192.168.1.6 priority 10 weight 10
ipv4 itr map-resolver 192.168.1.4
ipv4 itr map-resolver 192.168.1.5
ipv4 itr
ipv4 etr map-server 192.168.1.4 key example-key1
ipv4 etr map-server 192.168.1.5 key example-key2
ipv4 etr
exit
!
```

ファブリック コントロール プレーン デバイスの設定

コントロール プレーン デバイスを設定するには、次の手順を実行します。

始める前に

デバイスが確実に到達できるように、各エッジ デバイスに loopback0 IP アドレスを設定します。 **ip lisp source-locator loopback0** コマンドをアップリンク インターフェイスで実行していることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**fabric auto** 例： `Device(config)#fabric auto`	自動ファブリック プロビジョニングを有効にして、自動ファブリック コンフィギュレーション モードを開始します。

ステップ 4	**domain** { **default** | **name** *fabric domain name*}
	例：
	`Device(config-fabric-auto)#domain default`
	`Device(config-fabric-auto)#domain nameexampledomain`
		デフォルトのファブリック ドメインを設定し、ドメイン コンフィギュレーション モードを開始します。**name** キーワードを使用して、新しいファブリック ドメインを追加することができます。

ステップ 5	**control-plane self auth_key** キー 例： `Device(config-fabric-auto-domain)#control-plane self auth_key example-key1`	設定したホストプレフィックスに対し、認証キーでコントロール プレーン サービスを有効にします。
ステップ 6	**host-prefix** *prefix* **context name***name* **id** *ID* 例：	新しいコンテキストまたは VRF を作成し、それに ID を割り当てます。コンテキストを指定しない場合、デフォルトのコンテキストが使用されます。

	コマンドまたはアクション	目的
	Device(config-fabric-auto-domain)# **host-prefix** *192.168.1.0/24* **context name** *example-context* **id** *10*	
ステップ 7	**exit** 例： Device(config-fabric-auto-domain)# **exit**	
ステップ 8	**show fabric domain** 例： Device# **show fabric domain**	コントロール プレーン デバイス設定を表示します。この設定の一部として、追加のCLIコマンドが自動生成されます。

ファブリック境界デバイスの設定

デバイスをファブリック境界デバイスとして設定するには、次の手順を実行します。

始める前に

デバイスが確実に到達できるように、各エッジ デバイスに loopback0 IP アドレスを設定します。 **ip lisp source-locator loopback0** コマンドをアップリンク インターフェイスで実行していることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Device> **enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： Device# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**fabric auto** 例： Device(config)#**fabric auto**	自動ファブリック プロビジョニングを有効にして、自動ファブリック コンフィギュレーションモードを開始します。
ステップ 4	**domain** { **default** | **name** *fabric domain name*} 例：	デフォルトのファブリック ドメインを設定し、ドメイン コンフィギュレーションモードを開始します。**name** キーワードを使用して、新しいファブリッ

	コマンドまたはアクション	目的
	Device(config-fabric-auto)#**domain default** Device(config-fabric-auto)#**domain name *exampledomain***	ク ドメインを追加することができます。
ステップ 5	**control-plane** *ipv4 address* **auth_key** *key* 例： Device(config-fabric-auto-domain)#**control-plane 198.51.100.2 auth_key example-key1**	コントロール プレーン デバイスの IP アドレスおよび認証キーを設定して、ファブリック境界デバイスがコントロールプレーンデバイスと通信できるようにします。
ステップ 6	**border self** 例： Device(config-fabric-auto-domain)#**border self**	ファブリック境界デバイスとしてデバイスを有効にします。
ステップ 7	**context name** *name* **id***ID* 例： Device(config-fabric-auto-domain)#**context name *example-nh* id *10***	新しいコンテキストまたはVRFを作成し、それに新しいIDを割り当てます。コンテキストを設定しない場合、デフォルトのコンテキストが使用されます。
ステップ 8	**host-prefix** *prefix* **context name** *name* 例： Device(config-fabric-auto-domain)#**host-prefix *192.168.1.0/24* context name *eg-context***	コンテキストを使用してホスト プレフィックスまたはサブネットマスクを作成します。
ステップ 9	**exit** 例： Device(config-fabric-auto-domain)#**exit**	
ステップ 10	**show fabric domain** 例： Device# **show fabric domain**	ファブリック境界デバイス設定を表示します。

キャンパス ファブリックでのセキュリティ グループ タグとポリシーの適用

キャンパス ファブリック オーバーレイは、ファブリック ドメイン内のデバイス間で送信元グループ タグ（SGT）を伝達します。パケットは、仮想拡張LAN（VXLAN）を使用してカプセル化され、ヘッダーにSGT情報を伝えます。エッジデバイスを設定すると、**ipv4 sgt** コマンドが自動生成されます。エッジデバイスのIPアドレスにマッピングされたSGTは、カプセル化

されたパケット内に運ばれ、宛先デバイスに伝達されます。このデバイスでは、パケットがカプセル化解除され、送信元グループ アクセス コントロール リスト（SGACL）のポリシーが適用されます。

Cisco TrustSec と送信元グループ タグの詳細については、『Cisco TrustSec Switch Configuration Guide』を参照してください。

キャンパス ファブリック オーバーレイを使用したマルチキャスト

キャンパス ファブリック オーバーレイを使用して、ネイティブのマルチキャスト機能のないコア ネットワークを介してマルチキャスト トラフィックを伝送することができます。キャンパス ファブリック オーバーレイによって、エッジ デバイスでヘッドエンドを複製してマルチキャスト トラフィックのユニキャスト転送が可能になります。

（注） キャンパス ファブリックでサポートされるのは、Protocol Independent Multicast（PIM）スパース モードおよび PIM Source Specific Multicast（SSM; 送信元特定マルチキャスト）のみです。デンス モードはキャンパス ファブリックでサポートされていません。

キャンパス ファブリックのマルチキャスト PIM スパース モードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** 例： `Device(config)#ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**ip pim rp-address***rp address* 例： `Device(config)#ip pim rp-address 10.1.0.2`	マルチキャスト グループの Protocol Independent Multicast（PIM）ランデブーポイント（RP）のアドレスをスタティックに設定します。

	コマンドまたはアクション	目的
ステップ 5	**interface LISP** *interface number* 例： `Device(config)#interface LISP 0`	Protocol Independent Multicast（PIM）スパース モードを有効にする LISP インターフェイスおよびサブインターフェイスを指定します。
ステップ 6	**ip pim sparse-mode** 例： `Device(config-if)#ip pim sparse-mode`	スパースモードの動作用インターフェイスで Protocol Independent Multicast（PIM）を有効にします。
ステップ 7	**exit** 例： `Device(config-if)#exit`	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 8	**interface***interface typeinterface number* 例： `Device(config)#interface GigabitEthernet0/0/0`	エンドポイント側のインターフェイスを設定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 9	**ip pim sparse-mode** 例： `Device(config-if)#ip pim sparse-mode`	スパースモード動作用のファブリックドメイン側のインターフェイスで Protocol Independent Multicast（PIM）を有効にします。
ステップ 10	**end**	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。
ステップ 11	**show ip mroute***multicast ip-address*	デバイスのマルチキャストルートを確認します。
ステップ 12	**ping***multicast ip-address*	マルチキャスト アドレスに ping を実行することによって、基本的なマルチキャスト接続を確認します。
ステップ 13	**show ip mfib**	IPv4 マルチキャスト転送情報ベース（MFIB）の転送エントリとインターフェイスが表示されます。

キャンパス ファブリックのマルチキャスト PIM SSM の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** 例： `Device(config)#ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**ip pim ssm** {**default** | **range** { *access-list-number* | *access-list-name* 例： `Device(config)#ip pim ssm default`	IP マルチキャスト アドレスの Source Specific Multicast（SSM）範囲を定義します。
ステップ 5	**interface LISP** *interface number* 例： `Device(config)#interface LISP 0`	Protocol Independent Multicast（PIM）スパース モードを有効にする LISP インターフェイスおよびサブインターフェイスを指定します。
ステップ 6	**ip pim sparse-mode** 例： `Device(config-if)#ip pim sparse-mode`	スパースモード動作用の指定したインターフェイスで Protocol Independent Multicast（PIM）を有効にします。
ステップ 7	**exit** 例： `Device(config-if)#exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 8	**interface***interface typeinterface number* 例： `Device(config)#interface GigabitEthernet0/0/0`	エンドポイント側のインターフェイスを設定し、インターフェイスコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**ip pim sparse-mode** 例： `Device(config-if)#ip pim sparse-mode`	スパースモード動作用のファブリックドメイン側のインターフェイスで Protocol Independent Multicast（PIM）を有効にします。
ステップ 10	**ip igmp version 3** 例： `Device(config-if)#ip igmp version 3`	インターフェイス上で IGMP バージョン 3 を設定します。
ステップ 11	**end**	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。
ステップ 12	**show ip mroute***multicast ip-address*	デバイスのマルチキャストルートを確認します。
ステップ 13	**ping***multicast ip-address*	マルチキャストアドレスに ping を実行することによって、基本的なマルチキャスト接続を確認します。
ステップ 14	**show ip mfib**	IPv4 マルチキャスト転送情報ベース（MFIB）の転送エントリとインターフェイスが表示されます。

キャンパス ファブリックのデータ プレーン セキュリティ

キャンパス ファブリック データ プレーン セキュリティにより、ファブリック ドメイン内からのトラフィックのみを宛先のエッジデバイスによってカプセル化解除できます。ファブリックドメイン内のエッジ デバイスと境界デバイスは、データ パケットによって伝送される送信元のルーティング ロケータ（RLOC）、すなわちアップリンク インターフェイス アドレスが、ファブリック ドメインのメンバーであることを確認します。

データ プレーン セキュリティにより、カプセル化されたデータ パケット内のエッジ デバイスの送信元アドレスがスプーフィングされることはありません。ファブリック ドメイン以外からのパケットは送信元 RLOC が無効であり、エッジ デバイスと境界デバイスによるカプセル化解除時にブロックされます。

エッジ デバイスのデータ プレーン セキュリティの設定

始める前に

- デバイスが確実に到達できるように、各エッジ デバイスに loopback0 IP アドレスを設定します。Ensure

ip lisp source-locator loopback0 コマンドをアップリンク インターフェイスに適用していることを確認します。

- アンダーレイ設定が設定されていることを確認します。
- エッジ デバイス、コントロール プレーン デバイス、および境界デバイスを設定済みであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router lisp** 例： `Device(config)# router lisp`	LISP コンフィギュレーション モードを開始します。
ステップ 4	**decapsulation filter rloc source member** 例： `Device(config-router-lisp)# decapsulation filter rloc source member`	ファブリック ドメイン内のカプセル化されたパケットの送信元RLOC（アップリンク インターフェイス）アドレスの検証を有効にします。
ステップ 5	**exit** 例： `Device(config-router-lisp)# exit`	LISP コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**show lisp** [**session** ［**established**］ | **vrf** ［*vrf-name* [**session** [*peer-address*]]]] 例： `Device# show lisp session`	信頼性の高い転送セッションの情報を表示します。複数の転送セッションがある場合は、対応する情報が表示されます。
ステップ 7	**show lisp decapsulation filter** ［*IPv4-rloc-address* | *IPv6-rloc-address*］［**eid-table** *eid-table-vrf* | **instance-id** *iid*］ 例：	エッジ デバイスの RLOC アドレス設定の詳細（手動設定されたかまたは検出されたか）を表示します。

	コマンドまたはアクション	目的
	`Device# show lisp decapsulation filter instance-id 0`	

コントロール プレーン デバイスのデータ プレーン セキュリティの設定

始める前に

- デバイスが確実に到達できるように、各コントロール プレーン デバイスに loopback0 IP アドレスを設定します。Ensure

  ip lisp source-locator loopback0 コマンドをアップリンク インターフェイスに適用していることを確認します。

- アンダーレイ設定が設定されていることを確認します。
- エッジ デバイス、コントロール プレーン デバイス、および境界デバイスを設定済みであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router lisp** 例： `Device(config)# router lisp`	LISP コンフィギュレーション モードを開始します。
ステップ 4	**map-server rloc members distribute** 例： `Device(config-router-lisp)# map-server rloc members distribute`	ファブリック ドメイン内のエッジ デバイスへの、EIDプレフィックスのリストの配布を有効にします。
ステップ 5	**exit** 例： `Device(config-router-lisp)# exit`	LISP コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**show lisp** [**session** ［**established**］ | **vrf** ［*vrf-name* [**session** [*peer-address*]]]] 例： `Device# show lisp session`	信頼性の高い転送セッションの情報を表示します。複数の転送セッションがある場合は、対応する情報が表示されます。
ステップ 7	**show lisp decapsulation filter** ［*IPv4-rloc-address* | *IPv6-rloc-address*］［**eid-table** *eid-table-vrf* | **instance-id** *iid*］ 例： `Device# show lisp decapsulation filter instance-id 0`	（手動設定または検出された）アップリンク インターフェイス アドレス設定の詳細を表示します。

境界デバイスのデータ プレーン セキュリティの設定

始める前に

- デバイスが確実に到達できるように、各境界デバイスに loopback0 IP アドレスを設定します。Ensure

  ip lisp source-locator loopback0 コマンドをアップリンク インターフェイスに適用していることを確認します。

- アンダーレイ設定が設定されていることを確認します。
- エッジ デバイス、コントロール プレーン デバイス、および境界デバイスを設定済みであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router lisp** 例： `Device(config)# router lisp`	LISP コンフィギュレーション モードを開始します。
ステップ 4	**decapsulation filter rloc source member** 例： `Device(config-router-lisp)# decapsulation filter rloc source member`	ファブリック ドメイン内のカプセル化されたパケットの送信元RLOC（アップリンク インターフェイス）アドレスの検証を有効にします。
ステップ 5	**exit** 例： `Device(config-router-lisp)# exit`	LISP コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**show lisp** [**session** ［**established**］ | **vrf** ［*vrf-name* [**session** [*peer-address*]]]] 例： `Device# show lisp session`	信頼性の高い転送セッションの情報を表示します。複数の転送セッションがある場合は、対応する情報が表示されます。
ステップ 7	**show lisp decapsulation filter** ［*IPv4-rloc-address* | *IPv6-rloc-address*］［**eid-table** *eid-table-vrf* | **instance-id** *iid*］ 例： `Device# show lisp decapsulation filter instance-id 0`	（手動設定または検出された）RLOCアドレス設定の詳細を表示します。

キャンパス ファブリック設定の例

次に、エッジ設定に対する **show running-configuration** コマンドの出力例を示します。

```
device#show running-config
fabric auto
!
domain default
control-plane 198.51.100.2 auth-key example-key1
border 192.168.1.6
context name eg-context id 10
!
host-pool name VOICE_VLAN
context eg-context
vlan 10
gateway 192.168.1.254/24
use-dhcp 172.10.1.1
exit
exit
router lisp
locator-set default.RLOC
IPv4-interface Loopback0 priority 10 weight 10
```

```
exit
!
encapsulation vxlan
eid-table default instance-id 0
exit
!
eid-table vrf eg-context instance-id 10
dynamic-eid eg-context.EID.VOICE_VLAN
database-mapping 192.168.1.0/24 locator-set default.RLOC
exit
!
exit
!
loc-reach-algorithm lsb-reports ignore
disable-ttl-propagate
ipv4 sgt
ipv4 use-petr 192.168.1.6 priority 10 weight 10
ipv4 itr map-resolver 192.168.1.4
ipv4 itr map-resolver 192.168.1.5
ipv4 itr
ipv4 etr map-server 192.168.1.4 key example-key1
ipv4 etr map-server 192.168.1.5 key example-key2
ipv4 etr
exit
```

次に、コントロール プレーン設定に対する **show running-configuration** コマンドの出力例を示します。

```
!
fabric auto
domain default
control-plane auth-key example-key1
exit
!
ip vrf eg-context
!
vlan name VOICE_VLAN id 10
interface Vlan 10
ip address 192.168.1.254 255.255.255.0
ip helper-address global 172.10.1.1
no ip redirects
ip local-proxy-arp
ip route-cache same-interface
no lisp mobility liveness test
lisp mobility default.EID.VOICE_VLAN
router lisp
eid-table default
dynamic-default.EID.VOICE_VLAN
database-mapping 192.168.1.0/24 locator-set FD_DEFAULT.RLOC
router lisp
site FD_Default
authentication-key example-key1
exit
ipv4 map-server
ipv4 map-resolver
exit
```

次に、境界デバイス設定に対する **show running-configuration** コマンドの出力例を示します。

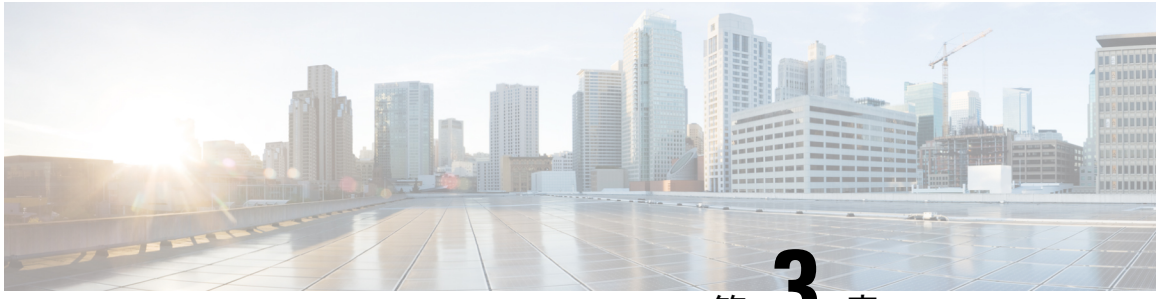
```
!fabric auto
!
domain default
control-plane 198.51.100.2 auth-key example-key1
border self
context name eg-context id 10
```

```
!
host-prefix 192.168.1.0/24 context name eg-context
!
host-pool name Voice
context eg-context
use-dhcp 172.10.1.1
exit
!
host-pool name doc
exit
exit
exit
router lisp
encapsulation vxlan
loc-reach-algorithm lsb-reports ignore
disable-ttl-propagate
ipv4 sgt
ipv4 proxy-etr
ipv4 proxy-itr 1.1.1.1
ipv4 itr map-resolver 198.51.100.2
ipv4 etr map-server 198.51.100.2 key example-key1
exit
```

第 III 部

CleanAir

- Cisco CleanAir の設定 （65 ページ）
- Bluetooth Low Energy の設定 （93 ページ）



第 3 章

Cisco CleanAir の設定

- 機能情報の確認 （65 ページ）
- CleanAir の前提条件 （65 ページ）
- CleanAir の制約事項 （66 ページ）
- CleanAir について （67 ページ）
- CleanAir の設定方法 （73 ページ）
- コントローラの GUI を使用した Cisco CleanAir の設定 （82 ページ）
- Cisco Spectrum Expert の設定 （82 ページ）
- CleanAir パラメータのモニタリング （83 ページ）
- CleanAir の設定例 （87 ページ）
- CleanAir に関する FAQ （88 ページ）
- その他の参考資料 （90 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

CleanAir の前提条件

Cisco CleanAir は、CleanAir 対応のアクセス ポイントにのみ設定できます。

次のアクセス ポイント モードを使用して、Cisco CleanAir スペクトラム モニタリングを実行できるのは、Cisco CleanAir 対応のアクセス ポイントだけです。

- Local：このモードでは、Cisco CleanAir 対応の各アクセス ポイント無線によって、現在の動作チャネルだけに関する電波品質と干渉検出のレポートが作成されます。

- Monitor：Cisco CleanAir が監視モードで有効になっていると、そのアクセス ポイントによって、モニタされているすべてのチャネルに関する電波品質と干渉検出のレポートが作成されます。

  次のオプションを使用できます。

  - All：すべてのチャネル
  - DCA：DCA リストによって管理されるチャネル選択
  - Country：規制区域内で合法なすべてのチャネル

  （注） アクセス ポイントは Prime インフラストラクチャでは AQ ヒートマップに参加しません。

- SE-Connect：このモードを使用すると、外部の Microsoft Windows XP または Vista PC で実行されている Spectrum Expert アプリケーションを Cisco CleanAir 対応のアクセス ポイントに接続して、詳細なスペクトラムデータを表示および分析できるようになります。Spectrum Expert アプリケーションは、デバイスをバイパスしてアクセス ポイントに直接接続します。SE-Connect モードのアクセス ポイントからは、Wi-Fi、RF、スペクトラムデータがデバイスに提供されません。すべての CleanAir システム機能は、AP がこのモードになっていて、クライアントが実行されていない間、一時停止状態になります。このモードは、リモート トラブルシューティングのみを対象としています。Spectrum Expert のアクティブな接続は最大で 3 つまで可能です。

関連トピック

2.4 GHz 帯域の CleanAir のイネーブル化 （73 ページ）
2.4 GHz での電波品質とデバイスの CleanAir アラームの設定 （74 ページ）
2.4 GHz デバイスの干渉レポートの設定 （75 ページ）
5 GHz 帯域の CleanAir のイネーブル化 （77 ページ）
5 GHz での電波品質とデバイスの CleanAir アラームの設定 （77 ページ）
5 GHz デバイスの干渉レポートの設定 （79 ページ）

CleanAir の制約事項

- 監視モードのアクセス ポイントは、Wi-Fi トラフィックまたは 802.11 パケットを送信しません。これらは Radio Resource Management（RRM）計画から除外され、隣接アクセス ポイントのリストに含まれません。IDR クラスタリングは、デバイスがネットワーク内の隣接アクセス ポイントを検出する機能に依存しています。複数のアクセス ポイントから関係する干渉デバイスを検出する機能を使用できるのは、監視モードのアクセス ポイント間に限られます。

- ローカル モード アクセス ポイント 5 つに対して監視モード アクセス ポイント 1 つという比率をお勧めします。これは、最適なカバレッジのためにネットワーク設計および専門ガイダンスによって異なる場合があります。
- Spectrum Expert（Windows XP ラップトップ クライアント）と AP 間では ping が可能である必要があります。不可能な場合は正しく動作しません。

関連トピック

2.4 GHz 帯域の CleanAir のイネーブル化 （73 ページ）
2.4 GHz での電波品質とデバイスの CleanAir アラームの設定 （74 ページ）
2.4 GHz デバイスの干渉レポートの設定 （75 ページ）
5 GHz 帯域の CleanAir のイネーブル化 （77 ページ）
5 GHz での電波品質とデバイスの CleanAir アラームの設定 （77 ページ）
5 GHz デバイスの干渉レポートの設定 （79 ページ）

CleanAir について

Cisco CleanAir は、共有ワイヤレス スペクトラムに関する問題に予防的に対応するスペクトラム インテリジェンス ソリューションです。共有スペクトラムのユーザすべてを確認できます（ネイティブデバイスと外部干渉源の両方）。また、この情報に基づいてネットワークが対処できるようにします。たとえば、干渉デバイスを手動で削除することも、システムが自動的に干渉からチャネルを変更することもできます。

Cisco CleanAir システムは CleanAir 対応アクセス ポイント、ワイヤレス コントローラ モジュール、モビリティ コントローラ、モビリティ アンカーと次世代のスイッチで構成されます。アクセス ポイントは、直接またはモビリティ アンカーを介してモビリティ コントローラに加わります。工業、科学、医療用（ISM）帯域で動作するすべてのデバイスに関する情報を収集し、それを潜在的な干渉源として識別、評価し、デバイスに転送します。デバイスは、アクセス ポイントを制御し、スペクトラムのデータを収集し、これらの情報を要求に応じて Cisco Prime Infrastructure（PI）または Cisco Mobility Services Engine（MSE）に転送します。

すべてのネットワーキング設定はモビリティ コントローラでのみ実行できます。設定を MA モードで実行することはできません。ただし、すべての CleanAir ワイヤレス レベル設定を、モビリティ アンカーを使用して実行できます。

ライセンス不要の帯域で動作するあらゆるデバイスについて、それが何であるか、どこにあるか、ワイヤレス ネットワークにどのような影響を与えるか、およびそれに対する対処方法が Cisco CleanAir によって示されます。これにより RF が簡素化されます。

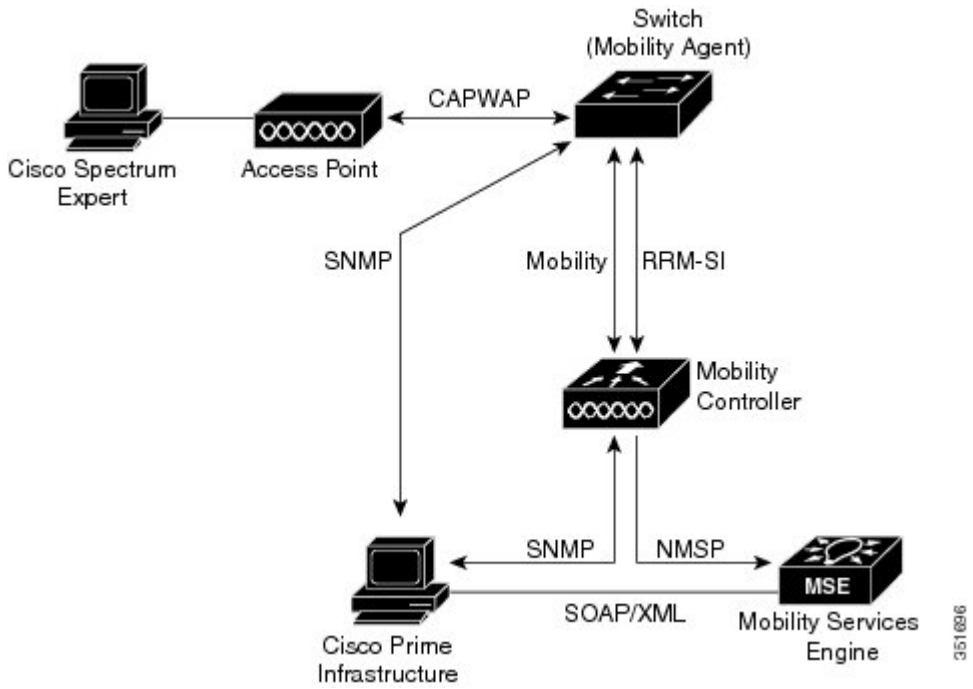
ワイヤレス LAN システムは、ライセンス不要の 2.4 GHz および 5 GHz ISM 帯域で動作します。この帯域では電子レンジ、コードレス電話、Bluetooth デバイスなどの多数の機器が動作しているため、Wi-Fi の動作に悪影響が生じる可能性があります。

Voice over Wireless や IEEE 802.11n 無線通信などの非常に高度な WLAN サービスの一部は、ISM 帯域を合法的に使用する他の機器からの干渉によって、重大な影響を受ける可能性があります。Cisco CleanAir 機能の統合により、この無線周波数 (RF) 干渉の問題に対処します。

Cisco CleanAir のコンポーネント

Cisco CleanAir の基本的なアーキテクチャは、Cisco CleanAir 対応 AP およびデバイスで構成されます。Cisco Prime Infrastructure（PI）、Mobility Services Engine（MSE）、Cisco Spectrum Expert はオプションのシステム コンポーネントです。Cisco PI と MSE は、履歴グラフ、干渉デバイスの追跡、ロケーション サービス、インパクト分析などの高度なスペクトラム機能のユーザ インターフェイスを提供します。

図 *3 : Cisco CleanAir* ソリューション



Cisco CleanAir テクノロジーを搭載したアクセス ポイントは、非 Wi-Fi 干渉源に関する情報を収集し、それを処理して MA に転送します。アクセス ポイントはコントローラに AQR と IDR レポートを送信します。

モビリティ コントローラ（MC）は CleanAir 対応のアクセス ポイントを制御および設定し、スペクトラム データを収集し、それを処理して PI および MSE に提供します。MC は CleanAir の基本機能およびサービスを設定し、現在のスペクトラム情報を表示するローカル ユーザ インターフェイス（GUI および CLI）を提供します。また、MC は、RRM TPC と DCM を使用して、干渉デバイスを検出、マージ、および軽減します。干渉デバイスのマージの詳細については、干渉デバイスのマージ （71 ページ）を参照してください。

Cisco PI は、機能のイネーブル化と設定、統合表示情報、履歴 AQ レコードとレポート エンジンを含む、CleanAir の先進的なユーザ インターフェイスを提供します。また、PI は、干渉デバイス、AQ のトレンド、およびアラートのグラフも表示します。

Cisco MSE は、干渉デバイスの場所および履歴の追跡に必要となるもので、複数のコントローラにわたる干渉レポートを調整および統合します。MSE は、包括的な Over-the-Air 脅威の検

出、特定および軽減を行う適応型ワイヤレス侵入防御システム（WIPS）サービスも提供します。また、MSE は、すべての干渉データをマージします。

スペクトラム アナライザで提供されるような RF 分析プロットの生成に使用できる詳細なスペクトラム データを入手するには、Cisco Spectrum Expert アプリケーションを実行している Microsoft Windows XP または Vista の PC に直接接続するように、Cisco CleanAir 対応アクセス ポイントを設定します。

Cisco CleanAir システムにおいて、デバイスは次のような処理を実行します。

- アクセス ポイントにおける Cisco CleanAir 機能を設定する。
- Cisco CleanAir の機能の設定やデータ収集のためのインターフェイスを提供する（、CLI、SNMP）。
- スペクトラム データを表示する。
- アクセス ポイントから AQR を収集して処理し、電波品質データベースに保存する。AQR には、特定されたすべての発生源からの干渉全体に関する情報（電波品質の指標（AQI）で表す）や、最も重大な干渉カテゴリの概要が記載されます。また CleanAir システムでは、干渉の種類ごとのレポートに未分類の干渉情報を含めることができ、未分類の干渉デバイスによる干渉が頻繁に生じる場合に対処することができます。
- アクセス ポイントから干渉デバイス レポート（IDR）を収集して処理し、干渉デバイス データベースに保存する。
- スペクトラム データを Prime インフラストラクチャおよび MSE に転送する。

Cisco CleanAir で使用される用語

表 *1 : CleanAir* 関連の用語

用語	説明
AQI	電波品質の指標。AQI は空気汚染物質に基づいた電波品質の指標です。AQI が 0 の場合は不良で、AQI が 85 より大きいと良好です。
AQR	電波品質レポート。AQR には特定されたすべての発生源からの干渉全体に関する情報（AQI で表される）や、最も重大な干渉カテゴリの概要が示されます。AQR は 15 分ごとにモビリティ コントローラに送信され、30 秒ごとに迅速モードで送信されます。
DC	デューティ サイクル。チャネルがデバイスで使用される時間の割合。
EDRRM	EDRRM イベント駆動型 RRM。EDRRM は、緊急事態にあるアクセス ポイントが、正常な RRM 間隔をバイパスし、すぐにチャネルを変更できるようにします。
IDR	アクセス ポイントがコントローラに送信する干渉デバイス レポート。
ISI	干渉の重大度指標。ISI は、干渉の重大度の指標です。

用語	説明
MA	モビリティエージェント。MAは、ワイヤレスモジュールが実行されているアクセス スイッチか、内部 MA が実行されている MC です。MA は、モバイル クライアント（MA が実行されているデバイスへのアクセス ポイントに接続されている）用のクライアント モビリティのステート マシンを維持するワイヤレス コンポーネントです。
MC	モビリティ コントローラ。MC は、ピア グループ間のローミング イベントのモビリティ管理サービスを提供します。MC は管理用の一元的な接続ポイントを提供し、すべてのモビリティ エージェントのモビリティ設定、ピア グループ メンバーシップ、およびメンバーのリストのサブドメインに、設定を送信します。
RSSI	受信信号強度インジケータ。RSSI は受信した無線信号における電力の測定値です。アクセス ポイントはこの電力で干渉デバイスを認識します。

Cisco CleanAir で検出できる干渉の種類

Cisco CleanAir では、干渉を検出し、その干渉の発生箇所や重大度をレポートし、さまざまな緩和方法を推奨することができます。これらの緩和方法には、Persistent Device Avoidance（PDA）と Event Driven RRM（EDRRM）という 2 つの方法があります。新規（New）

Wi-Fi チップをベースとする RF 管理システムには、次のような共通の特性があります。

- Wi-Fi 信号として識別できない RF エネルギーはノイズとして報告される。
- チャネル計画の割り当てに使用するノイズの測定値は、一部のクライアントデバイスに悪影響を及ぼす可能性のある不安定さや急速な変化を避けるために、一定の期間において平均化される傾向がある。
- 測定値が平均化されることで、測定値の精度が低下する。そのため、平均化された後、クライアントに混乱をもたらす信号が緩和を必要とするものに見えない場合がある。
- 現在使用できる RF 管理システムは、本質的にはすべて事後対応型である。

Cisco CleanAir はこれらと異なり、ノイズの発生源だけでなく、その場所や WLAN に対する潜在的な影響まで明確に特定することができます。このような情報を入手することにより、ネットワーク内におけるノイズを考慮し、理にかなった、可能であれば予防的な判断を行うことができます。CleanAir では、次の 2 種類の干渉イベントが一般的です。

- 永続的干渉
- 突発的干渉

永続的干渉イベントは、本質的に固定型のデバイスから発生し、断続的ではあるものの、干渉が大規模に反復して繰り返されるものを指します。たとえば、休憩室に設置してある電子レンジの場合を考えます。このような装置が動作するのは、1 回に付き 1 ～ 2 分程度です。しかし一旦動作すると、ワイヤレス ネットワークと、関係するクライアントのパフォーマンスに非常に大きな影響が生じます。Cisco CleanAir を使用すると、電子レンジなどの装置を無秩序なノイズとしてではなく明確に識別できるようになります。また、その装置によって影響を受ける帯域の部分を正確に特定できます。そして、その設置場所も特定できるため、最も大きな影響を受けるアクセス ポイントを判別することができます。そして、この情報を使用して RRM に

指示し、範囲内にあるアクセスポイントに対してこの干渉源を避けるようなチャネル計画を選択させることができます。この干渉は1日の大部分にわたって発生するものではないため、既存のRF管理アプリケーションによって、影響を受けるアクセスポイントのチャネルの再変更が試みられている場合もあります。しかし、永続的デバイスの回避は、干渉源が周期的に検出されて永続的な状態が新たに発生する限り影響があり続けるという点で独特です。Cisco CleanAirシステムでは、電子レンジが存在することを認識し、それを将来のすべての計画に取り込みます。電子レンジまたはその近くのアクセスポイントを移動させた場合は、このアルゴリズムによってRRMが自動的に更新されます。

（注） Event Driven RRM（EDRRM）は、Cisco CleanAir対応でローカルモードにあるアクセスポイントによってのみ動作します。

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャネル、またはある範囲内のチャネルが完全に妨害を受けます。Cisco CleanAirのEvent Driven RRM（EDRRM）機能を使用すると、電波品質（AQ）に対してしきい値を設定できます。しきい値を超過した場合には、影響を受けたアクセスポイントに対してチャネル変更がただちに行われます。ほとんどのRF管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAirではAQ測定値を使用してスペクトラムを連続的に評価するため、対応策を30秒以内に実行します。たとえば、アクセスポイントがビデオカメラからの干渉を受けた場合は、そのカメラが動作し始めてから30秒以内にチャネル変更によってアクセスポイントを回復させることができます。Cisco CleanAirでは干渉源の識別と位置の特定も行うため、後からその装置の永続的な緩和処理も実行できます。

Bluetoothデバイスの場合、Cisco CleanAir対応のアクセスポイントで干渉の検出と報告を行うことができるのは、そのデバイスがアクティブに送信しているときだけです。Bluetoothデバイスには、さまざまなパワーセーブモードがあります。たとえば、接続されたデバイス間でデータまたは音声がストリーム化されている最中に干渉が検出されます。

干渉デバイスのマージ

干渉デバイス（ID）メッセージはモビリティコントローラ（MC）で処理されます。モビリティアンカー（MA）がAPからIDメッセージを転送するため、メッセージはMCで処理されます。MCでは、さまざまなMAに接続されたAP全体のネイバー情報を表示できます。

IDマージのロジックにはAPネイバー情報が必要です。ネイバー情報がRRMモジュールから取得されます。このapiは直接MCに接続されたAPにのみネイバー情報を提供します。

現在、MAのAPネイバーリストは3分に一度MCと同期されます。したがって、このapiが取得したAPネイバーリストは最大で3分古いものである可能性があります。この遅延により、検出時のデバイスのマージで遅延が生じます。後続の定期的なマージが更新されたネイバー情報を受け取り、マージが発生します。

永続的デバイス

屋外型ブリッジや電子レンジなどの一部の干渉デバイスは、必要な場合にのみ送信を行います。通常のRF管理基準では短時間の定期的な動作はたいていは検出されないままになるため、このようなデバイスによってローカルの WLAN に対する大規模な干渉が引き起こされる可能性があります。CleanAir を使用すると、RRM DCA アルゴリズムによって、この影響が検出、測定、登録、記録され、DCA アルゴリズムが調整されます。このため、その干渉源と同じ場所にあるチャネル計画によって、その永続的デバイスによって影響を受けるチャネルの使用が最小限に留められます。Cisco CleanAir では、永続的デバイスの情報を検出してデバイスに保存し、チャネルの干渉の緩和に利用します。

永続的デバイスの検出

CleanAir対応で監視モードのアクセス ポイントでは、設定されているすべてのチャネルで永続的デバイスに関する情報を収集して、この情報をコントローラに保存します。ローカル/ブリッジ モードの AP は、稼働チャネルでのみ干渉デバイスを検出します。

永続的デバイスの回避

永続的デバイス（PD）が CleanAir モジュールで検出されると、MA の RRM モジュールに報告されます。この情報は、RRM モジュールに送信される後続の EDRRM イベント駆動型 RRM（ED-RRM）により、チャネル選択で使用されます。

EDRRM および AQR の更新モード

EDRRM は、緊急事態にあるアクセス ポイントが、正常な RRM 間隔をバイパスしてすぐにチャネルを変更できるようにするための機能です。CleanAir アクセス ポイントは AQ を常に監視し、AQ を 15 分ごとに報告します。AQ は分類された干渉デバイスのみを報告します。EDRRM の主なメリットは極めて短期間の処理時間です。干渉デバイスがアクティブ チャネルで動作しており、EDRRM をトリガーするのに十分な AQ の低下を引き起こした場合、クライアントはそのチャネルまたはアクセス ポイントを使用できなくなります。チャネルからアクセス ポイントを削除する必要があります。EDRRM はデフォルトではイネーブルになっていません。最初に CleanAir をイネーブルにしてから、EDRRM をイネーブルにします。

AQR は MC 上でのみ利用できます。モード設定およびタイマーは MA の無線制御ブロック（RCB）で保持されます（MA に接続された AP の場合）。EMS/NMS で利用できる最新の API の変更はありません。RCB（スペクトラムの設定およびタイマー）はローカルで使用可能なため、直接接続された AP には変更は必要ありません。リモート AP（MA に接続された AP）の場合は、3 つの新しい制御メッセージが追加されています。この 3 つのメッセージは、特定の AP MAC アドレスおよびスロットに対するイネーブル、タイマーの再起動、迅速な更新モードのディセーブルについてです。

関連トピック

CleanAir-Events の EDRRM の設定 （80 ページ）

CleanAir ハイ アベイラビリティ

CleanAir の設定（ネットワークおよび無線）は、スイッチオーバー時にはステートフルです。MC では、組み込みインスツルメンテーション コア（EICORE）により、アクティブおよびスタンバイ ノード全体でのネットワーク構成の同期が実現されます。無線設定は、HA インフラストラクチャを使用して同期されます。MA 上の CleanAir の設定は、join 時に MC から取得されます。ネットワーク構成は MA 上の EICORE には保存されていないため、HA インフラストラクチャを使用して同期されます。

CleanAir データ（AQ と IDR）レポートはステートフルではありません。つまり、スタンバイとアクティブ ノードは同期されません。スイッチオーバー時に AP が現在アクティブなスロットにレポートを送信します。RRM クライアント（HA インフラストラクチャ クライアント）は CleanAir の HA 同期に使用されます。

CleanAir の設定方法

2.4 GHz 帯域の CleanAir のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ap dot11 24ghz cleanair**
	例：
	`Device(config)#ap dot11 24ghz cleanair`
	`Device(config)#no ap dot11 24ghz cleanair`
		802.11b ネットワークでの CleanAir 機能をイネーブルにします。802.11b ネットワークでの CleanAir をディセーブルにするには、このコマンドに **no** を追加します。

ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件 （65 ページ）
CleanAir の制約事項 （66 ページ）
CleanAir に関する FAQ （88 ページ）

2.4 GHz での電波品質とデバイスの CleanAir アラームの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz cleanair alarm air-quality threshold** *threshold_value* 例： `Device(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50`	すべての 2.4 GHz デバイスについて、電波品質のしきい値のアラームを設定します。アラームをディセーブルにするには、このコマンドの **no** 形式を追加します。
ステップ 3	**ap dot11 24ghz cleanair alarm device** {**bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee** } 例： `Device(config)#ap dot11 24ghz cleanair alarm device canopy`	2.4 GHz デバイスのアラームを設定します。アラームをディセーブルにするには、**no** 形式のコマンドを追加します。 • **bt-discovery**：Bluetooth の検出。 • **bt-link**：Bluetooth リンク。 • **canopy**：Canopy デバイス。 • **cont-tx**：連続トランスミッタ。 • **dect-like**：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話。 • **fh**：802.11 周波数ホッピング デバイス。 • **inv**：スペクトラム反転 WiFi 信号を使用するデバイス。 • **jammer**：電波妨害装置。 • **mw-oven**：電子レンジ。 • **nonstd**：非標準 Wi-Fi チャネルを使用するデバイス。 • **report**：干渉デバイスのレポート。 • **superag**：802.11 SuperAG デバイス。 • **tdd-tx**：TDD トランスミッタ。

	コマンドまたはアクション	目的
		• **video**：ビデオ カメラ。 • **wimax-fixed**：WiMax 固定。 • **wimax-mobile**：WiMax モバイル。 • **xbox**：Xbox。 • **zigbee**：802.15.4 デバイス。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件 （65 ページ）
CleanAir の制約事項 （66 ページ）
CleanAir に関する FAQ （88 ページ）

2.4 GHz デバイスの干渉レポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ap dot11 24ghz cleanair device {bt-discovery | bt-link | canopy | cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile | xbox | zigbee }**
	例：
	`デバイス(config)# ap dot11 24ghz cleanair device bt-discovery`
	`デバイス(config)# ap dot11 24ghz cleanair device bt-link`
	`デバイス(config)# ap dot11 24ghz cleanair device canopy`
		デバイスに報告するように 2.4 GHz 干渉デバイスを設定します。設定をディセーブルにするには、このコマンドの **no** 形式を使用します。
		• **bt-discovery**：Bluetooth の検出
		• **bt-link**：Bluetooth リンク
		• **canopy**：Canopy デバイス
		• **cont-tx**：連続トランスミッタ
		• **dect-like**：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話

	コマンドまたはアクション	目的
	デバイス(config)# **ap dot11 24ghz cleanair device cont-tx** デバイス(config)# **ap dot11 24ghz cleanair device dect-like** デバイス(config)# **ap dot11 24ghz cleanair device fh** デバイス(config)# **ap dot11 24ghz cleanair device inv** デバイス(config)# **ap dot11 24ghz cleanair device jammer** デバイス(config)# **ap dot11 24ghz cleanair device mw-oven** デバイス(config)# **ap dot11 24ghz cleanair device nonstd** デバイス(config)# **ap dot11 24ghz cleanair device report** デバイス(config)# **ap dot11 24ghz cleanair device superag** デバイス(config)# **ap dot11 24ghz cleanair device tdd-tx** デバイス(config)# **ap dot11 24ghz cleanair device video** デバイス(config)# **ap dot11 24ghz cleanair device wimax-fixed** デバイス(config)# **ap dot11 24ghz cleanair device wimax-mobile** デバイス(config)# **ap dot11 24ghz cleanair device xbox** デバイス(config)# **ap dot11 24ghz cleanair device zigbee**	• **fh**：802.11 周波数ホッピング デバイス • **inv**：スペクトラム反転 WiFi 信号を使用するデバイス • **jammer**：電波妨害装置 • **mw-oven**：電子レンジ • **nonstd**：非標準 WiFi チャネルを使用するデバイス • **report**：説明なし • **superag**：802.11 SuperAG デバイス • **tdd-tx**：TDD トランスミッタ • **video**：ビデオ カメラ • **wimax-fixed**：WiMax 固定 • **wimax-mobile**：WiMax モバイル • **xbox**：Xbox • **zigbee**：802.15.4 デバイス
ステップ 3	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件 （65 ページ）
CleanAir の制約事項 （66 ページ）
CleanAir に関する FAQ （88 ページ）

5 GHz 帯域の CleanAir のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ap dot11 5ghz cleanair**
	例：
	`Device(config)#ap dot11 5ghz cleanair`
	`Device(config)#no ap dot11 5ghz cleanair`
		802.11a ネットワークでの CleanAir 機能をイネーブルにします。802.11a ネットワークでの CleanAir をディセーブルにするには、このコマンドに **no** を追加します。

ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件 （65 ページ）
CleanAir の制約事項 （66 ページ）
CleanAir に関する FAQ （88 ページ）

5 GHz での電波品質とデバイスの CleanAir アラームの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 5ghz cleanair alarm air-quality threshold** *threshold_value* 例： `Device(config)#ap dot11 5ghz cleanair alarm air-quality threshold 50`	すべての 5 GHz デバイスについて、電波品質のしきい値のアラームを設定します。アラームをディセーブルにするには、このコマンドの **no** 形式を追加します。

	コマンドまたはアクション	目的
ステップ 3	**ap dot11 5ghz cleanair alarm device**{**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **radar** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**} 例： `Device(config)#ap dot11 5ghz cleanair alarm device`	5 GHz デバイスのアラームを設定します。アラームをディセーブルにするには、このコマンドの **no** 形式を追加します。 • **canopy**：Canopy デバイス。 • **cont-tx**：連続トランスミッタ。 • **dect-like**：Digital Enhanced Cordless Communication（DECT）デジタルコードレス電話。 • **fh**：802.11 周波数ホッピング デバイス。 • **inv**：スペクトラム反転 WiFi 信号を使用するデバイス。 • **jammer**：電波妨害装置。 • **nonstd**：非標準 WiFi チャネルを使用するデバイス。 • **radar**：レーダー。 • **report**：干渉デバイスのレポート。 • **superag**：802.11 SuperAG デバイス。 • **tdd-tx**：TDD トランスミッタ。 • **video**：ビデオ カメラ。 • **wimax-fixed**：WiMax 固定。 • **wimax-mobile**：WiMax モバイル。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件 （65 ページ）
CleanAir の制約事項 （66 ページ）
CleanAir に関する FAQ （88 ページ）

5 GHz デバイスの干渉レポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ap dot11 5ghz cleanair device {canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile}**
	例：
	`デバイス(config)#ap dot11 5ghz cleanair device canopy`
	`デバイス(config)#ap dot11 5ghz cleanair device cont-tx`
	`デバイス(config)#ap dot11 5ghz cleanair device dect-like`
	`デバイス(config)#ap dot11 5ghz cleanair device inv`
	`デバイス(config)#ap dot11 5ghz cleanair device jammer`
	`デバイス(config)#ap dot11 5ghz cleanair device nonstd`
	`デバイス(config)#ap dot11 5ghz cleanair device radar`
	`デバイス(config)#ap dot11 5ghz cleanair device report`
	`デバイス(config)#ap dot11 5ghz cleanair device superag`
	`デバイス(config)#ap dot11 5ghz cleanair device tdd-tx`
	`デバイス(config)#ap dot11 5ghz cleanair device video`
	`デバイス(config)#ap dot11 5ghz cleanair device wimax-fixed`
		デバイスに報告するように 5 GHz 干渉デバイスを設定します。干渉デバイスのレポートをディセーブルにするには、このコマンドの **no** 形式を追加します。
		• **canopy**：Canopy デバイス
		• **cont-tx**：連続トランスミッタ
		• **dect-like**：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話
		• **fh**：802.11 周波数ホッピング デバイス
		• **inv**：スペクトラム反転 WiFi 信号を使用するデバイス
		• **jammer**：電波妨害装
		• **nonstd**：非標準 WiFi チャネルを使用するデバイス
		• **radar**：レーダー
		• **report**：干渉デバイスのレポート
		• **superag**：802.11 SuperAG デバイス
		• **tdd-tx**：TDD トランスミッタ
		• **video**：ビデオ カメラ
		• **wimax-fixed**：WiMax 固定
		• **wimax-mobile**：WiMax モバイル

	コマンドまたはアクション	目的
	デバイス(config)#**ap dot11 5ghz cleanair device wimax-mobile**	
ステップ 3	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件 （65 ページ）
CleanAir の制約事項 （66 ページ）
CleanAir に関する FAQ （88 ページ）

CleanAir-Events の EDRRM の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： Device# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** 例： Device(config)#**ap dot11 24ghz rrm channel cleanair-event** Device(config)#**no ap dot11 24ghz rrm channel cleanair-event**	EDRRM の cleanair イベントをイネーブルにします。EDRRM をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** [**sensitivity** {**high** | **low** | **medium**}] 例： Device(config)#**ap dot11 24ghz rrm channel cleanair-event sensitivity high**	cleanair-event の EDRRM の感度を設定します。 • [High]：電波品質（AQ）の値で示される、非 Wi-Fi 干渉に対する最も高い感度を指定します。 • [Low]：AQ の値で示される、非 Wi-Fi 干渉に対する最も低い感度を指定します。

	コマンドまたはアクション	目的
		• [Medium]：AQの値で示される、非Wi-Fi干渉に対する中程度の感度を指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権EXECモードに戻ります。また、Ctrl+Zキーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

EDRRMおよびAQRの更新モード （72ページ）

永続的デバイスの回避の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 {24ghz | 5ghz} rrm channel device** 例： `Device(config)#ap dot11 24ghz rrm channel device`	802.11チャネル割り当てでの永続的非Wi-Fiデバイスの回避をイネーブルにします。永続的デバイスの回避をディセーブルにするには、このコマンドの **no** 形式を追加します。
ステップ 3	**end** 例： `Device(config)# end`	特権EXECモードに戻ります。また、Ctrl+Zキーを押しても、グローバル コンフィギュレーション モードを終了できます。

コントローラの GUI を使用した Cisco CleanAir の設定

Cisco Spectrum Expert の設定

Spectrum Expert の設定（CLI）

始める前に

- Spectrum Expert（Windows XP ラップトップ クライアント）とアクセス ポイント間で ping が可能である必要があります。不可能な場合は正しく動作しません。
- Spectrum Expert コンソールとアクセス ポイントとの間に接続を確立する前に、IP アドレスのルーティングが正しく設定され、途中にあるすべてのファイアウォールでネットワーク スペクトラム インターフェイス（NSI）ポートが開かれていることを確認します。
- アクセス ポイントは、2.4 GHz の周波数をポート 37540 で、5 GHz の周波数をポート 37550 でリスニングする TCP サーバである必要があります。これらのポートは、Spectrum Expert アプリケーションが NSI プロトコルを使用してアクセス ポイントに接続するために、開かれている必要があります。
- **show ap name** *ap_name* **config dot11** {**24ghz** | **5ghz**} コマンドを使用して、デバイス CLI から NSI キーを確認できます。

手順

ステップ 1 次のコマンドを入力して、アクセス ポイントに SE-Connect モードを設定します。

ap name *ap_name* **mode se-connect**

例：

```
Device#ap name Cisco_AP3500 mode se-connect
```

ステップ 2 アクセス ポイントをリブートするように求められたら、「**Y**」と入力します。

ステップ 3 次のコマンドを入力して、アクセス ポイントの NSI キーを表示します。

show ap name *ap_name* **config dot11** {**24ghz** | **5ghz**}

例：

```
Device#show ap name Cisco_AP3500 config dot11 24ghz

<snippet>
CleanAir Management Information
    CleanAir Capable                            : Yes
    CleanAir Management Admin State             : Enabled
    CleanAir Management Operation State         : Up
    CleanAir NSI Key                            : 274F1F9B1A5206683FAF57D87BFFBC9B
    CleanAir Sensor State                       : Configured
```

```
<snippet>
```

次のタスク

Windows PC で、Cisco Spectrum Expert をダウンロードします。

- URL http://www.cisco.com/cisco/software/navigator.html から、Cisco Software Center にアクセスします。
- [Product] > [Wireless] > [Cisco Spectrum Intelligence] > [Cisco Spectrum Expert] > [Cisco Spectrum Expert Wi-Fi] の順にクリックし、Spectrum Expert 4.1.11 の実行可能ファイル（*.exe）をダウンロードします。
- PC で Spectrum Expert アプリケーションを実行します。
- [Connect to Sensor] ダイアログボックスが表示されたら、アクセス ポイントの IP アドレスを入力し、アクセス ポイントの無線を選択し、認証のために 16 バイトのネットワーク スペクトラム インターフェイス（NSI）キーを入力します。Spectrum Expert アプリケーションによって、NSI プロトコルを使用して、アクセス ポイントへの TCP/IP による直接接続が開かれます。

  SE-Connect モードのアクセス ポイントがデバイスに join すると、アクセス ポイントから Spectrum Capabilities 通知メッセージが送信され、これにデバイスは Spectrum Configuration Request で応答します。この要求には 16 バイトのランダム NSI キーが含まれます。このキーは NSI 認証で使用するためにデバイスで作成されたものです。デバイスはアクセス ポイントごとにキーを 1 つ作成し、アクセス ポイントはこのキーをリブートするまで保存します。

  （注） Spectrum Expert コンソール接続は、アクセス ポイントの無線ごとに最大 3 つまで確立できます。

- Spectrum Expert アプリケーションの右下隅にある [Slave Remote Sensor] テキスト ボックスを選択して、Spectrum Expert コンソールがアクセス ポイントに接続されていることを確認します。デバイスが 2 台接続されている場合は、このテキスト ボックスにアクセス ポイントの IP アドレスが表示されます。
- Spectrum Expert アプリケーションを使用して、アクセス ポイントからのスペクトラム データを表示および分析します。

CleanAir パラメータのモニタリング

次のコマンドを使用して CleanAir パラメータをモニタできます。

表 *2 : CleanAir* のモニタリング用コマンド

コマンド	説明
show ap dot11 24ghz cleanair air-quality summary	2.4 GHz 帯域の CleanAir 電波品質（AQ）のデータを表示します
show ap dot11 24ghz cleanair air-quality worst	2.4 GHz 帯域の CleanAir 電波品質（AQ）の最悪のデータを表示します
show ap dot11 24ghz cleanair config	2.4 GHz 帯域の CleanAir の設定を表示します
show ap dot11 24ghz cleanair device type all	2.4 GHz 帯域のすべての CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type bt-discovery	2.4 GHz 帯域の BT Discovery タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type bt-link	2.4 GHz 帯域の BT Link タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type canopy	2.4 GHz 帯域の Canopy タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type cont-tx	2.4 GHz 帯域の Continuous transmitter タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type dect-like	2.4 GHz 帯域の DECT Like タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type fh	2.4 GHz 帯域の 802.11FH タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type inv	2.4 GHz 帯域の WiFi Inverted タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type jammer	2.4 GHz 帯域の Jammer タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type mw-oven	2.4 GHz 帯域の MW Oven タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type nonstd	2.4 GHz 帯域の WiFi Inv.Ch タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type persistent	2.4 GHz 帯域の Persistent タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type superag	2.4 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します

コマンド	説明
show ap dot11 24ghz cleanair device type tdd-tx	2.4 GHz 帯域の TDD Transmit タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type video	2.4 GHz 帯域の Video Camera タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type wimax-fixed	2.4 GHz 帯域の WiMax Fixed タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type wimax-mobile	2.4 GHz 帯域の WiMax Mobile タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type xbox	2.4 GHz 帯域の Xbox タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type zigbee	2.4 GHz 帯域の zigbee タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair air-quality summary	5 GHz 帯域の CleanAir 電波品質（AQ）のデータを表示します
show ap dot11 5ghz cleanair air-quality worst	5 GHz 帯域の CleanAir 電波品質（AQ）の最悪のデータを表示します
show ap dot11 5ghz cleanair config	5 GHz 帯域の CleanAir の設定を表示します
show ap dot11 5ghz cleanair device type all	5 GHz 帯域のすべての CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type canopy	5 GHz 帯域の Canopy タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type cont-tx	5 GHz 帯域の Continuous TX タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type dect-like	5 GHz 帯域の DECT Like タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type inv	5 GHz 帯域の WiFi Inverted タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type jammer	5 GHz 帯域の Jammer タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type nonstd	5 GHz 帯域の WiFi Inv.Ch タイプの CleanAir 干渉源を表示します

コマンド	説明
show ap dot11 5ghz cleanair device type persistent	5 GHz 帯域の Persistent タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type superag	5 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type tdd-tx	5 GHz 帯域の TDD Transmit タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type video	5 GHz 帯域の Video Camera タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type wimax-fixed	5 GHz 帯域の WiMax Fixed タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type wimax-mobile	5 GHz 帯域の WiMax Mobile タイプの CleanAir 干渉源を表示します

干渉デバイスのモニタリング

CleanAir 対応のアクセス ポイントで干渉デバイスが検出されると、複数のセンサーによる同じデバイスの検出をマージして、クラスタが作成されます。各クラスタには一意の ID を割り当てます。一部のデバイスは、実際に必要になるまで送信時間を制限することによって電力を節約しますが、その結果、スペクトラム センサーでのそのデバイスの検出が一時的に停止します。その後、このデバイスはダウンとして適正にマークされます。ダウンしたデバイスは、スペクトラムデータベースから適正に削除されます。ある特定のデバイスに対する干渉源検出がすべてレポートされる場合は、クラスタ ID を長期間にわたって有効とし、デバイス検出が増大しないようにします。同じデバイスが再度検出された場合は、元のクラスタ ID とマージして、そのデバイスの検出履歴を保持します。

たとえば、Bluetooth 対応のヘッドフォンが電池を使用して動作している場合があります。このようなデバイスでは、実際に必要とされていない場合には送信機を停止するなど、電力消費を減らすための方法が採用されています。このようなデバイスは、分類処理の対象として現れたり、消えたりを繰り返すように見えます。CleanAir では、このようなデバイスを管理するために、クラスタ ID をより長く保持し、検出時には同じ 1 つのレコードに再度マージされるようにします。この処理によってユーザ レコードの処理が円滑になり、デバイスの履歴が正確に表現されるようになります。

CleanAir の設定例

2.4 GHz 帯域での CleanAir およびアクセス ポイントのイネーブル化：例

次に、チャネルで動作する 2.4 GHz 帯域の CleanAir とアクセス ポイントをイネーブルにする例を示します。

```
Device#configure terminal
Device(config)#ap dot11 24ghz cleanair
Device(config)#exit
Device#ap name TAP1 dot11 24ghz cleanair
Device#end
```

2.4 GHz での電波品質とデバイスの CleanAir アラームの設定：例

次に、2.4 GHz 電波品質のしきい値 50 dBm および Xbox デバイス用に CleanAir アラームを設定する例を示します。

```
Device#configure terminal
Device(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50
Device(config)#ap dot11 24ghz cleanair alarm device xbox
Device(config)#end
```

5 GHz デバイスの干渉レポートの設定：例

次に、5 GHz デバイスの干渉レポートを設定する例を示します。

```
Device#configure terminal
Device(config)#ap dot11 5ghz cleanair alarm device xbox
Device(config)#end
```

CleanAir-Events の EDRRM の設定：例

次に、2.4 GHz 帯域の EDRRM の cleanair-event をイネーブルにし、非 Wi-Fi 干渉に対する高い感度を設定します。

```
Device#configure terminal
Device(config)#ap dot11 24ghz rrm channel cleanair-event
Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
Device(config)#end
```

永続的デバイスの回避の設定：例

次に、2.4 GHz 帯域で永続的非 Wi-Fi デバイスの回避をイネーブルにする例を示します。

```
Device#configure terminal
Device(config)#ap dot11 24ghz rrm channel device
Device(config)#end
```

SE-Connect モードのアクセス ポイントの設定：例

次に、SE-Connect モードのアクセス ポイントを設定する例を示します。

```
Device#ap name Cisco_AP3500 mode se-connect
```

CleanAir に関する FAQ

Q. MC が稼働しているかどうかを確認するにはどうすればよいですか。

A. MC が稼働しているかどうかを確認するには、 **show wireless mobility summary** コマンドを使用します。

次に、モビリティ サマリーを表示する例を示します。

```
Device#show wireless mobility summary

Mobility Controller Summary:
Mobility Role                                   : Mobility Controller
Mobility Protocol Port                          : 16666
Mobility Group Name                             : MG-AK
Mobility Oracle                                 : Disabled
Mobility Oracle IP Address                      : 0.0.0.0
DTLS Mode                                       : Enabled
Mobility Domain ID for 802.11r                  : 0x39b2
Mobility Keepalive Interval                     : 10
Mobility Keepalive Count                        : 3
Mobility Control Message DSCP Value             : 48
Mobility Domain Member Count                    : 2
Link Status is Control Link Status : Data Link Status
Controllers configured in the Mobility Domain:
IP              Public IP       Group Name      Multicast IP     Link Status
-------------------------------------------------------------------------------
9.6.136.10      -               MG-AK           0.0.0.0          UP   : UP
```

Q. 複数のアクセス ポイントが同じ干渉デバイスを検出しますが、デバイスはそれらを別個のクラスタとして表示するか、疑いのあるさまざまなデバイスをクラスタ化して示します。このようになるのはなぜですか。

A. デバイスがこれらのアクセス ポイントによって検出されたデバイスのマージを検討するためには、アクセス ポイントが RF ネイバーである必要があります。アクセス ポイントがネイバー関係を確立するためには時間がかかります。デバイスの再起動後、または RF グループの変更などのイベントの後は、クラスタリングがそれほど正確ではなくなります。

Q. デバイスを使用して 2 台のモニタ モード アクセス ポイントをマージできますか。

A. いいえ。デバイスを使用して 2 台のモニタ モード アクセス ポイントをマージすることはできません。MSE を使用した場合にのみ、モニタ モード アクセス ポイントをマージできます。

Q. ネイバー アクセス ポイントを表示するにはどうすればよいですか。

A. ネイバー アクセス ポイントを表示するには、次のコマンドを使用します。 **show ap** *ap_name* **auto-rf dot11** {**24ghz** | **5ghz**}

次に、ネイバー アクセス ポイントを表示する例を示します。

```
Device#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz

<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0                          :  -12 dBm on   1 (10.10.0.5)
```

```
  AP 0C85.25AB.CCA0 slot 0                                  :  -24 dBm on   6 (10.10.0.5)

  AP 0C85.25C7.B7A0 slot 0                                  :  -26 dBm on  11 (10.10.0.5)

  AP 0C85.25DE.2C10 slot 0                                  :  -24 dBm on   6 (10.10.0.5)

  AP 0C85.25DE.C8E0 slot 0                                  :  -14 dBm on  11 (10.10.0.5)

  AP 0C85.25DF.3280 slot 0                                  :  -31 dBm on   6 (10.10.0.5)

  AP 0CD9.96BA.5600 slot 0                                  :  -44 dBm on   6 (10.0.0.2)
  AP 24B6.5734.C570 slot 0                                  :  -48 dBm on  11 (10.0.0.2)
<snippet>
```

Q. CleanAir で利用可能なデバッグ コマンドはどれですか。

A. CleanAir のデバッグ コマンドは次のとおりです。

debug cleanair {**all** | **error** | **event** | **internal-event** | **nmsp** | **packet**}

debug rrm {**all** | **channel** | **detail** | **error** | **group** | **ha** | **manager** | **message** | **packet** | **power** | **prealarm** | **profile** | **radar** | **rf-change** | **scale** | **spectrum**}

Q. CleanAir アラームが干渉デバイスに対して生成されないのはなぜですか。

A. アクセス ポイントが CleanAir 対応であり、CleanAir がアクセス ポイントとデバイスの両方でイネーブルにされていることを確認します。

Q. Cisco Catalyst 3850 シリーズ スイッチは、モビリティ エージェント（MA）として機能できますか。

A. はい。Cisco Catalyst 3850 シリーズ スイッチは MA として機能できます。

Q. CleanAir 設定は MA で使用できますか。

A. リリース 3.3 SE 以降、CleanAir 設定は MA で使用できます。MA で CleanAir の次の 2 種類のコマンドを使用できます。

- **show ap dot11 5ghz cleanair config**
- **show ap dot11 24ghz cleanair config**

関連トピック

2.4 GHz 帯域の CleanAir のイネーブル化 （73 ページ）
2.4 GHz での電波品質とデバイスの CleanAir アラームの設定 （74 ページ）
2.4 GHz デバイスの干渉レポートの設定 （75 ページ）
5 GHz 帯域の CleanAir のイネーブル化 （77 ページ）
5 GHz での電波品質とデバイスの CleanAir アラームの設定 （77 ページ）
5 GHz デバイスの干渉レポートの設定 （79 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CleanAir コマンドと詳細	『*CleanAir Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』
ハイ アベイラビリティ構成	『*High Availability Configuration Guide, Cisco IOS XE Release 3SE (Cisco 5700 Series Wireless Controllers)*』
ハイ アベイラビリティ コマンドと詳細	『*High Availability Command Reference, Cisco IOS XE Release 3SE (Cisco 5700 Series Wireless Controllers)*』

エラー メッセージ デコーダ

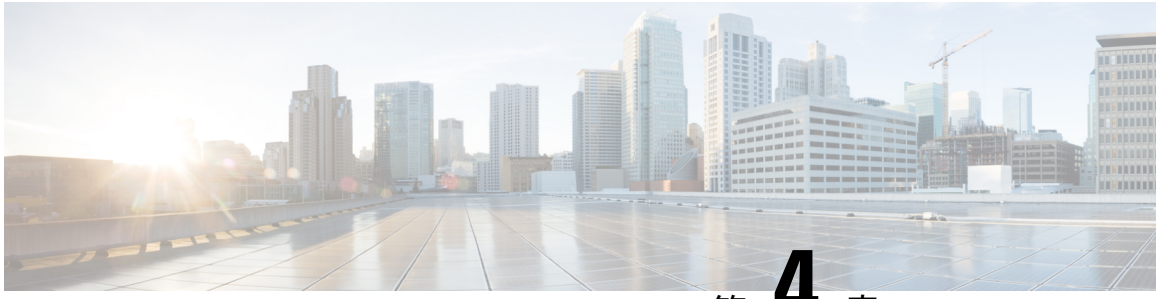
説明	Link
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support



第 4 章

Bluetooth Low Energy の設定

- Bluetooth Low Energy について （93 ページ）
- Bluetooth Low Energy ビーコンのイネーブル化 （94 ページ）

Bluetooth Low Energy について

Bluetooth Low Energy（BLE）は、モバイル デバイスのロケーション サービスの向上を目的とした、ワイヤレス パーソナル エリア ネットワーク テクノロジーです。戦略的な場所に配置された小型の Bluetooth タグ デバイスは、汎用一意識別子（UUID）と、それらの ID としてメジャー フィールドおよびマイナー フィールドを送信します。これらの詳細は、bluetooth 対応のスマートフォンおよびデバイスで取り上げられています。これらのデバイスのロケーション情報は、対応するバックエンドサーバに送信されます。その後、関連するアドバタイズメントとその他の重要な情報が、このロケーション固有の情報を使用してデバイスにプッシュされます。

また、BLE 機能では、BLE ビーコン管理のサポートが提供され、Cisco WLAN システム内で使用される場合はその動作が指定されます。Cisco CleanAir を使用して、アクセス ポイントは iBeacon 信号を識別し、ペイロード コンテンツを復号化できます。抽出されたタグ デバイスの詳細は、デバイスのより良い管理のために使用されます。

干渉源としてタグ デバイスを扱い、干渉場所などの既存のシステム機能を使用して、タグ デバイスをワイヤレス LAN 展開のマップ ディスプレイ上に配置でき、その動作をモニタできます。この他、欠落しているタグの情報も取得できます。この機能を使用して、顧客から提供された所定のホワイトリストと対照して、各タグ（またはタグのファミリ）に関連付けられている固有識別子を使用している不正なタグおよび悪意のあるタグを確認できます。管理機能を使用して、不正なタグ、欠落したタグ、または移動したタグに基づいて、アラートを表示したり電子メールで送信したりできます。

BLE 機能の制限事項

- 無線インフラストラクチャは、Cisco CleanAir をサポートする必要があります。
- 最大 250 個の固有の BLE ビーコン（クラスタ エントリ）と 1000 個のデバイス エントリのみをサポートします。

使用エリア

BLE 機能では、デバイス（スマートフォンまたは bluetooth 対応デバイス）のきめ細かな場所の詳細が提供されるので、状況依存アドバタイジングおよびその他の情報をユーザにプッシュできます。アプリケーションの使用可能エリアには、小売店、博物館、動物園、医療機関、フィットネス、セキュリティ、アドバタイジングなどがあります。

Bluetooth Low Energy ビーコンのイネーブル化

Bluetooth Low Energy（BLE）検出は、デフォルトでイネーブルになっています。無効になっている BLE を有効にするには、次に示す手順を使用します。

始める前に

- 無線インフラストラクチャは、Cisco CleanAir をサポートする必要があります。
- Cisco CleanAir 設定と show コマンドは、モビリティ コントローラ(MC)モードでのみ使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Controller# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no] ap dot11 24ghz cleanair device [ble-beacon]** 例： `Controller(config)# ap dot11 24ghz cleanair device ble-beacon`	802.11b ネットワークでの BLE 機能をイネーブルにします。802.11b ネットワークで BLE 機能を無効にするには、このコマンドの **no** 形式を使用します。
ステップ 3	**exit** 例： `Controller(config)# exit`	特権 EXEC モードに戻ります。

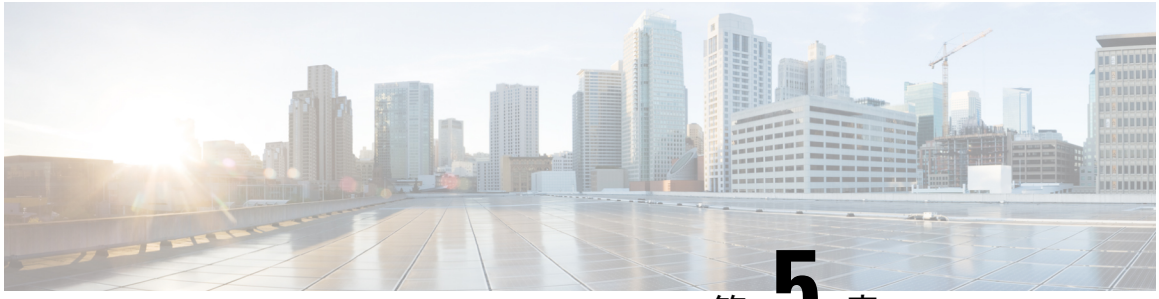
ステップ 4	**show ap dot11 24ghz cleanair config**
	例：
	`Controller# show ap dot11 24ghz cleanair config`
	
	`Interference Device Settings:`
	`  Interference Device Reporting..... : Enabled`
	`  Bluetooth Link..... : Enabled`
		（任意）BLE ビーコン設定を表示します。

	コマンドまたはアクション	目的
	Microwave Oven..... : Enabled BLE Beacon..... : Enabled	
ステップ 5	**show ap dot11 24ghz cleanair device type ble-beacon** 例： Controller# show ap dot11 24ghz cleanair device type ble-beacon DC = Duty Cycle (%) ISI = Interference Severity Index (1-Low Interference, 100-High Interference) RSSI = Received Signal Strength Index (dBm) DevID = Device ID No ClusterID DevID Type AP Name ISI RSSI DC Channel ——————————————————————— 1 2c:92:80:00:00:22 0xa001 BLE Beacon 5508_3_AP3600_f839 -- -74 0 unknown	（任意）BLE ビーコンのデバイス タイプ情報を表示します。

第 IV 部

インターフェイスおよびハードウェア コンポーネント

- インターフェイス特性の設定 （99 ページ）
- Auto-MDIX の設定 （141 ページ）
- イーサネット管理ポートの設定 （147 ページ）
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定 （153 ページ）
- システム MTU の設定 （175 ページ）
- 内部電源装置の設定 （187 ページ）
- PoE の設定 （191 ページ）
- Cisco eXpandable Power System（XPS）2200 の設定 （207 ページ）
- EEE の設定 （219 ページ）



第 5 章

インターフェイス特性の設定

- インターフェイス特性の設定に関する情報 （99 ページ）
- インターフェイスの特性の設定方法 （114 ページ）
- インターフェイス特性のモニタ （132 ページ）
- インターフェイス特性の設定例 （134 ページ）
- インターフェイス特性機能の追加情報 （138 ページ）
- インターフェイス特性の設定の機能履歴と情報 （139 ページ）

インターフェイス特性の設定に関する情報

インターフェイス タイプ

ここでは、デバイスでサポートされているインターフェイスの異なるタイプについて説明します。また、インターフェイスの物理特性に応じた設定手順についても説明します。

（注） このスタック対応デバイスの背面にあるスタック ポートはイーサネット ポートではないため、設定できません。

ポートベースの VLAN

VLANは、ユーザの物理的な位置に関係なく、機能、チーム、またはアプリケーションなどで論理的に分割された、スイッチによるネットワークです。ポートで受信したパケットが転送されるのは、その受信ポートと同じVLANに属するポートに限られます。異なるVLAN上のネットワーク デバイスは、VLAN 間でトラフィックをルーティングするレイヤ 3 デバイスがなければ、互いに通信できません。

VLANに分割することにより、VLAN内でトラフィック用の堅固なファイアウォールを実現します。また、各 VLAN には固有の MAC アドレス テーブルがあります。VLAN が認識されるのは、ローカル ポートが VLAN に対応するように設定されたとき、VLAN トランキング プロ

トコル（VTP）トランク上のネイバーからその存在を学習したとき、またはユーザがVLANを作成したときです。スタック全体のポートを使用して VLAN を形成できます。

VLANを設定するには、**vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して、VLAN コンフィギュレーション モードを開始します。標準範囲 VLAN（VLAN ID 1 ～ 1005）の VLAN 設定は、VLAN データベースに保存されます。VTP がバージョン 1 または 2 の場合に、拡張範囲 VLAN（VLAN ID が 1006 ～ 4094）を設定するには、最初に VTP モードをトランスペアレントに設定する必要があります。トランスペアレント モードで作成された拡張範囲VLANは、VLANデータベースには追加されませんが、デバイスの実行コンフィギュレーションに保存されます。VTP バージョン 3 では、クライアントまたはサーバ モードで拡張範囲 VLAN を作成できます。これらの VLAN は VLAN データベースに格納されます。

スイッチ スタックでは、VLAN データベースはスタック内のすべてのスイッチにダウンロードされ、スタック内のすべてのスイッチによって同じ VLAN データベースが構築されます。スタックのすべてのスイッチで実行コンフィギュレーションおよび保存済みコンフィギュレーションが同一です。

switchport インターフェイス コンフィギュレーション コマンドを使用すると、VLAN にポートが追加されます。

- インターフェイスを特定します。
- トランク ポートには、トランク特性を設定し、必要に応じて所属できる VLAN を定義します。
- アクセス ポートには、所属する VLAN を設定して定義します。

スイッチ ポート

スイッチポートは、物理ポートに対応付けられたレイヤ2専用インターフェイスです。スイッチ ポートは 1 つまたは複数の VLAN に所属します。スイッチ ポートは、アクセス ポートまたはトランク ポートにも使用できます。ポートは、アクセス ポートまたはトランク ポートに設定できます。また、ポート単位で Dynamic Trunking Protocol（DTP）を稼働させ、リンクのもう一端のポートとネゴシエートすることで、スイッチ ポート モードも設定できます。スイッチポートは、物理インターフェイスおよび関連付けられているレイヤ2プロトコルの管理に使用され、ルーティングやブリッジングは処理しません。

スイッチ ポートの設定には、**switchport** インターフェイス コンフィギュレーション コマンドを使用します。

Access Ports

アクセス ポートは（音声 VLAN ポートとして設定されている場合を除き）1 つの VLAN だけに所属し、その VLAN のトラフィックだけを伝送します。トラフィックは、VLAN タグが付いていないネイティブ形式で送受信されます。アクセス ポートに着信したトラフィックは、ポートに割り当てられている VLAN に所属すると見なされます。アクセス ポートがタグ付きパケット（スイッチ間リンク（ISL）またはタグ付き IEEE 802.1Q）を受信した場合、そのパケットはドロップされ、送信元アドレスは学習されません。

サポートされているアクセス ポートのタイプは、次のとおりです。

- スタティック アクセス ポート。このポートは、手動でVLANに割り当てます（IEEE 802.1xで使用する場合はRADIUS サーバを使用します。

また、Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。

Trunk Ports

トランク ポートは複数の VLAN のトラフィックを伝送し、デフォルトで VLAN データベース内のすべての VLAN のメンバとなります。

デフォルトでは、トランク ポートは、VTPに認識されているすべてのVLANのメンバですが、トランク ポートごとに VLAN の許可リストを設定して、VLAN メンバーシップを制限できます。許可 VLAN のリストは、その他のポートには影響を与えませんが、対応トランク ポートには影響を与えます。デフォルトでは、使用可能なすべての VLAN（VLAN ID 1 ～ 4094）が許可リストに含まれます。トランク ポートは、VTP が VLAN を認識し、VLAN がイネーブル状態にある場合に限り、VLAN のメンバーになることができます。VTP が新しいイネーブル VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバになり、トラフィックはその VLAN のトランク ポート間で転送されます。VTP が、VLAN のトランク ポートの許可リストに登録されていない、新しいイネーブル VLAN を認識した場合、ポートはその VLAN のメンバーにはならず、その VLAN のトラフィックはそのポート間で転送されません。

トンネル ポート

トンネル ポートは IEEE 802.1Q トンネリングで使用され、サービスプロバイダー ネットワークのカスタマーのトラフィックを、同じ VLAN 番号を使用するその他のカスタマーから分離します。サービスプロバイダー エッジ スイッチのトンネル ポートからカスタマーのスイッチの IEEE 802.1Q トランク ポートに、非対称リンクを設定します。エッジ スイッチのトンネル ポートに入るパケットには、カスタマーの VLAN ですでに IEEE802.1Q タグが付いており、カスタマーごとに IEEE 802.1Q タグの別のレイヤ（メトロ タグと呼ばれる）でカプセル化され、サービスプロバイダー ネットワークで一意の VLAN ID が含まれます。タグが二重に付いたパケットは、その他のカスタマーのものとは異なる、元のカスタマーの VLAN が維持されてサービスプロバイダー ネットワークを通過します。発信インターフェイス、およびトンネル ポートでは、メトロ タグが削除されてカスタマーのネットワークのオリジナル VLAN 番号が取得されます。

トンネル ポートは、トランク ポートまたはアクセス ポートにすることができず、それぞれのカスタマーに固有の VLAN に属する必要があります。

ルーテッド ポート

ルーテッドポートは物理ポートであり、ルータ上にあるポートのように動作しますが、ルータに接続されている必要はありません。ルーテッド ポートは、アクセス ポートとは異なり、特定の VLAN に対応付けられていません。VLAN サブインターフェイスをサポートしない点を除けば、通常のルータ インターフェイスのように動作します。ルーテッド ポートは、レイヤ

3 ルーティング プロトコルで設定できます。ルーテッド ポートはレイヤ 3 インターフェイス専用で、DTP や STP などのレイヤ 2 プロトコルはサポートしません。

ルーテッド ポートを設定するには、**no switchport** インターフェイス コンフィギュレーション コマンドでインターフェイスをレイヤ 3 モードにします。次に、ポートに IP アドレスを割り当て、ルーティングをイネーブルにし、**ip routing** および **router** *protocol* グローバル コンフィギュレーション コマンドを使用してルーティング プロトコルの特性を指定します。

（注） **no switchport** インターフェイス コンフィギュレーション コマンドを実行すると、インターフェイスがいったんシャットダウンしてから再度イネーブルになります。これにより、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 2 モードのインターフェイスをレイヤ 3 モードにした場合、影響のあるインターフェイスに関連する以前の設定が消失する可能性があります。

ソフトウェアに、設定できるルーテッド ポートの個数制限はありません。ただし、ハードウェアには限界があるため、この個数と設定されている他の機能の数との相互関係によって CPU パフォーマンスに影響が及ぶことがあります。

（注） IP Base イメージは、スタティック ルーティングと Routing Information Protocol（RIP）をサポートします。フル レイヤ 3 ルーティングまたはフォールバック ブリッジングの場合は、スタンドアロン デバイスまたはアクティブなデバイス上で IP Services イメージを有効にする必要があります。

スイッチ仮想インターフェイス

スイッチ仮想インターフェイス（SVI）は、スイッチ ポートの VLAN を、システムのルーティング機能またはブリッジング機能に対する 1 つのインターフェイスとして表します。1 つの VLAN に関連付けることができる SVI は 1 つだけです。VLAN に対して SVI を設定するのは、VLAN 間でルーティングするため、またはデバイスに IP ホスト接続を提供するためだけです。デフォルトでは、SVI はデフォルト VLAN（VLAN 1）用に作成され、リモート デバイスの管理を可能にします。追加の SVI は明示的に設定する必要があります。

（注） インターフェイス VLAN 1 は削除できません。

SVI はシステムにしか IP ホスト接続を行いません。SVI は、VLAN インターフェイスに対して **vlan** インターフェイス コンフィギュレーション コマンドを実行したときに初めて作成されます。VLAN は、ISL または IEEE 802.1Q カプセル化トランク上のデータ フレームに関連付けられた VLAN タグ、あるいはアクセス ポート用に設定された VLAN ID に対応します。トラフィックをルーティングするそれぞれの VLAN に対して VLAN インターフェイスを設定し、IP アドレスを割り当ててください。

スイッチ スタックまたはデバイスは合計 1005 個の VLAN および SVI をサポートしますが、ハードウェアの制限のため、SVIおよびルーテッド ポートの数と設定する他の機能の数との相互関係によって、CPU のパフォーマンスに影響が及ぶことがあります。

物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

SVI 自動ステート除外

VLAN 上の複数のポートを装備した SVI のライン ステートは、次の条件を満たしたときにはアップ状態になります。

- VLAN が存在し、デバイスの VLAN データベースでアクティブです。
- VLAN インターフェイスが存在し、管理上のダウン状態ではありません。
- 少なくとも 1 つのレイヤ 2（アクセスまたはトランク）ポートが存在し、この VLAN のリンクがアップ状態であり、ポートが VLAN でスパニングツリー フォワーディング ステートです。

（注） 対応する VLAN リンクに属する最初のスイッチポートが起動し、STP フォワーディング ステートになると、VLANインターフェイスのプロトコル リンク ステートがアップ状態になります。

VLANに複数のポートがある場合のデフォルトのアクションでは、VLAN内のすべてのポートがダウンすると SVI もダウン状態になります。SVI 自動ステート除外機能を使用して、SVI ラインステート アップオアダウン計算に含まれないようにポートを設定できます。たとえば、VLAN 上で1つのアクティブ ポートだけがモニタリング ポートである場合、他のすべてのポートがダウンすると VLAN もダウンするよう自動ステート除外機能をポートに設定できます。ポートがイネーブルである場合、**autostate exclude** は、ポート上でイネーブルであるすべての VLAN に適用されます。

VLAN 内の 1 つのレイヤ 2 ポートに収束時間がある場合（STP リスニング/ラーニング ステートからフォワーディング ステートへの移行）、VLAN インターフェイスが起動します。これにより、ルーティング プロトコルなどの機能は、完全に動作した場合と同様にVLANインターフェイスを使用せず、ルーティング ブラック ホールなどの他の問題を最小限にします。

EtherChannel ポート グループ

EtherChannel ポート グループは、複数のスイッチ ポートを 1 つのスイッチ ポートとして扱います。このようなポート グループは、デバイス間、またはデバイスおよびサーバ間で高帯域接続を行う単一論理ポートとして動作します。EtherChannel は、チャネルのリンク全体でトラフィックの負荷を分散させます。EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが残りのリンクに切り替えられます。複数のトランク ポートを 1 つの論理トランク ポートに、複数のアクセス ポートを 1 つの論理アクセス ポートに、複数のトンネル ポートを 1 つの論理トンネル ポートに、または複数のルーテッド ポートを1つの論理ルーテッドポートにグループ化できます。ほとんどのプロトコルは単一のまたは集約スイッチ ポートで動作し、ポート グループ内の物理ポートを認識しません。例外は、

DTP、Cisco Discovery Protocol（CDP）、およびポート集約プロトコル（PAgP）で、物理ポート上でしか動作しません。

EtherChannel を設定するとき、ポートチャネル論理インターフェイスを作成し、EtherChannel にインターフェイスを割り当てます。レイヤ3インターフェイスの場合は、**interface port-channel** グローバル コンフィギュレーション コマンドを使用して手動で論理インターフェイスを作成します。そのあと、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。レイヤ 2 インターフェイスの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスをダイナミックに作成します。このコマンドは物理および論理ポートをバインドします。

10 ギガビット イーサネット インターフェイス

10ギガビットイーサネットインターフェイスは全二重モードでだけ動作します。インターフェイスはスイッチ ポートまたはルーテッド ポートとして設定可能です。

Cisco TwinGig Converter Module の詳細については、デバイスのハードウェア インストレーション ガイドおよびトランシーバ モジュールのマニュアルを参照してください。

マルチギガビット イーサネット

マルチギガビット イーサネット（mGig）機能を使用して、Cisco 802.11ac Wave2 アクセス ポイント（AP）イーサネット ポートで 1Gbps を超える速度を設定できます。この技術は、自動帯域幅ネゴシエーションによって、従来の CAT5e ケーブル以上の速度のケーブル型式を超える、100 Mbps、1 Gbps、2.5 Gbps、および 5 Gbps の速度をサポートします。マルチギガビット イーサネットは、次のスイッチの Cisco 3800 シリーズのアクセス ポイントでサポートされます。

以下は、mGig 機能をサポートしているシスコ スイッチです。

- WS-C3850-12X48U
- WS-C3850-24XU

マルチギガビットイーサネットは、チャネルの両端でサポートされる最高速度でリンクを確立するためにポートが自動ネゴシエーションページを交換するマルチレート速度をサポートします。高ノイズ環境では、ポート速度のダウンシフトがインターフェイスで有効になっているときは、より高速なリンクが確立できない場合、または確立されたリンクの品質が PHY によるリンクの再確立を必要とするレベルに下がった場合、ライン レートは自動的に低い速度にダウングレードします。次のダウンシフト速度値が推奨されます。

- 10Gbs（5Gbs にダウンシフト）
- 5Gbs（2.5Gbs にダウンシフト）
- 2.5Gbs（1Gbs にダウンシフト）
- 1Gbs（100Mbs にダウンシフト）

Power over Ethernet（PoE）ポート

Power over Ethernet（PoE）対応デバイス ポートでは、回路に電力が供給されていないことをスイッチが検出した場合、接続している次のデバイスに電力が自動的に供給されます。

- シスコ先行標準受電デバイス（Cisco IP Phone や Cisco Aironet アクセス ポイントなど）
- IEEE 802.3af 準拠の受電装置

受電デバイスが PoE スイッチ ポートおよび AC 電源に接続されている場合、冗長電力として利用できます。受電装置が PoE ポートにだけ接続されている場合、受電装置には冗長電力は供給されません。

スイッチの USB ポートの使用

デバイスには、USB ミニ タイプ B コンソール ポートと USB タイプ A ポートの 2 つの USB ポートが前面パネルにあります。

USB ミニタイプ B コンソール ポート

デバイスには、次のコンソール ポートがあります。

- USB ミニタイプ B コンソール接続
- RJ-45 コンソール ポート

コンソール出力は両方のポートに接続されたデバイスに表示されますが、コンソール入力は一度に 1 つのポートしかアクティブになりません。デフォルトでは、USB コネクタは RJ-45 コネクタよりも優先されます。

（注） Windows PC には、USB ポートのドライバが必要です。ドライバ インストレーションの手順については、ハードウェア インストレーション ガイドを参照してください。

付属の USB Type A-to-USB mini-Type B ケーブルを使用して、PC またはその他のデバイスをデバイスに接続します。接続されたデバイスには、ターミナルエミュレーションアプリケーションが必要です。デバイスが、ホスト機能をサポートする電源投入デバイス（PC など）への有効な USB 接続を検出すると、RJ-45 コンソールからの入力はただちにディセーブルになり、USB コンソールからの入力がイネーブルになります。USB 接続が削除されると、RJ-45 コンソールからの入力はただちに再度イネーブルになります。デバイスの LED は、どのコンソール接続が使用中であるかを示します。

コンソール ポート変更ログ

ソフトウェア起動時に、ログに USB または RJ-45 コンソールのいずれがアクティブであるかが示されます。スタックの各デバイスがこのログを生成します。すべてのデバイスは常にまず RJ-45 メディア タイプを表示します。

サンプル出力では、Device 1 には接続された USB コンソール ケーブルがあります。ブートローダが USB コンソールに変わらなかったため、Device 1 からの最初のログは、RJ-45 コンソールを示しています。少したってから、コンソールが変更され、USB コンソール ログが表示されます。Device 2 およびDevice 3 には接続された RJ-45 コンソール ケーブルがあります。

```
switch-stack-1
*Mar  1 00:01:00.171: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
*Mar  1 00:01:00.431: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.


switch-stack-2
*Mar  1 00:01:09.835: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.

switch-stack-3
*Mar  1 00:01:10.523: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

USB ケーブルが取り外されるか、PC が USB 接続を非アクティブ化すると、ハードウェアは自動的に RJ-45 コンソール インターフェイスに変わります。

```
switch-stack-1
Mar  1 00:20:48.635: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

コンソール タイプが常に RJ-45 であるように設定でき、さらに USB コネクタの無活動タイムアウトを設定できます。

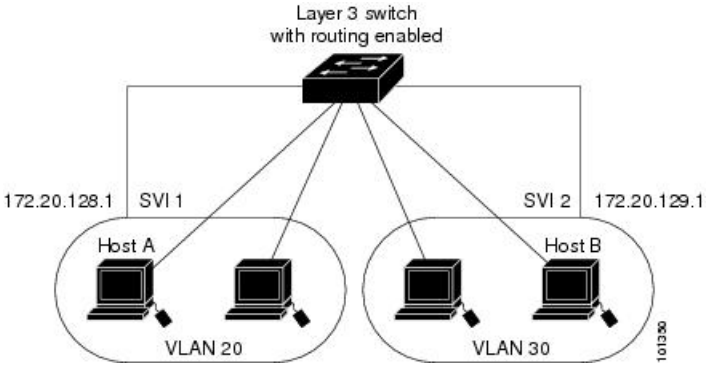
USB タイプ A ポート

USB タイプ A ポートは、外部 USB フラッシュ デバイス（サム ドライブまたは USB キーとも呼ばれる）へのアクセスを提供します。このポートは、容量 128 MB ～ 8 GB の Cisco USB フラッシュ ドライブをサポートします（ポート密度 128 MB、256 MB、1 GB、4 GB、8 GB の USB デバイスがサポートされます）。標準 Cisco IOS コマンドライン インターフェイス（CLI）コマンドを使用して、フラッシュデバイスの読み取り、書き込み、および、コピー元やコピー先として使用できます。デバイスを USB フラッシュ ドライブから起動するようにも設定できます。

インターフェイスの接続

単一 VLAN 内のデバイスは、スイッチを通じて直接通信できます。異なる VLAN に属すポート間では、ルーティングデバイスを介さなければデータを交換できません。標準のレイヤ2デバイスを使用すると、異なる VLAN のポートは、ルータを通じて情報を交換する必要があります。ルーティングが有効に設定されたデバイスの使用により、IP アドレスを割り当てた SVI で VLAN 20 および VLAN 30 の両方を設定すると、外部ルータを使用せずに、デバイスを介してホスト A からホスト B にパケットを直接送信できます。

図 *4 :* スイッチと *VLAN* との接続



（注） LAN Base イメージを実行中のデバイスは SVI 上で 16 のスタティック ルートのみの設定をサポートします。

IP Services イメージがデバイスまたはアクティブなデバイス上で動作している場合は、デバイスが 2 つの方式（ルーティングとフォールバック ブリッジング）を使用してインターフェイス間のトラフィックを転送します。IP Base イメージがデバイスまたはアクティブなデバイス上に存在する場合は、基本ルーティング（スタティック ルーティングと RIP）だけがサポートされます。可能な場合は、高いパフォーマンスを維持するために、転送をデバイス ハードウェアで実行します。ただし、ハードウェアでルーティングされるのはイーサネット II カプセル化された IPv4 パケットだけです。非 IP トラフィックと、他のカプセル化方式を使用しているトラフィックは、ハードウェアによってフォールバック ブリッジングされます。

- ルーティング機能は、すべての SVI およびルーテッド ポートで有効にできます。デバイスは IP トラフィックだけをルーティングします。IP ルーティング プロトコル パラメータとアドレス設定が SVI またはルーテッド ポートに追加されると、このポートで受信した IP トラフィックはルーティングされます。
- フォールバック ブリッジングは、デバイスでルーティングされないトラフィックや DECnet などのルーティングできないプロトコルに属しているトラフィックを転送します。また、フォールバック ブリッジングは、2 つ以上の SVI またはルーテッド ポート間のブリッジングによって、複数の VLAN を 1 つのブリッジ ドメインに接続します。フォールバック ブリッジングを設定する場合は、ブリッジ グループに SVI またはルーテッド ポートを割り当てます。各 SVI またはルーテッド ポートにはそれぞれ 1 つしかブリッジ グループが割り当てられません。同じグループ内のすべてのインターフェイスは、同じブリッジ ドメインに属します。

インターフェイス コンフィギュレーション モード

デバイスは、次のインターフェイス タイプをサポートします。

- 物理ポート：デバイス ポートおよびルーテッド ポート

- VLAN：スイッチ仮想インターフェイス
- ポート チャネル：EtherChannel インターフェイス

インターフェイス範囲も設定できます。

物理インターフェイス（ポート）を設定するには、インターフェイス タイプ、スタック メンバー番号（スタッキング対応スイッチのみ）、モジュール番号、およびデバイス ポート番号を指定して、インターフェイスコンフィギュレーション モードを開始します。

- タイプ：10/100/1000 Mbps イーサネット ポートにはギガビット イーサネット（gigabitethernet または gi）、10,000 Mbps には 10 ギガビット イーサネット（tengigabitethernet または te）、Small Form-Factor Pluggable（SFP）モジュールにはギガビット イーサネット インターフェイス（gigabitethernet または gi）です。
- スタック メンバ番号：スタック内のデバイスを識別する番号。デバイスの番号範囲は 1 ～ 9 で、初めてデバイスを初期化したときに割り当てられます。デバイス スタックに組み込まれる前のデフォルトのデバイス番号は 1 です。デバイスにスタック メンバ番号が割り当てられている場合、別の番号が割り当てられるまでその番号が維持されます。

  スタック モードでスイッチ ポート LED を使用して、デバイスのスタック メンバー番号を識別できます。
- モジュール番号：デバイス上のモジュールまたはスロット番号：スイッチ（ダウンリンク）ポートは 0 で、アップリンク ポートは 1 です。
- ポート番号：デバイス上のインターフェイス番号。10/100/1000 ポート番号は常に 1 から始まり、デバイスの向かって一番左側のポートから順に付けられています。たとえば、gigabitethernet1/0/1 または gigabitethernet1/0/8 のようになります。

  SFP アップリンク ポートを装着したデバイスの場合、モジュール番号は 1 で、ポート番号が振り直されます。デバイスに 10/100/1000 ポートが 24 個ある場合、SFP モジュール ポートは、gigabitethernet1/1/1 ～ gigabitethernet1/1/4、または tengigabitethernet1/1/1 ～ tengigabitethernet1/1/4 になります。

デバイス上のインターフェイスの位置を物理的に確認することで、物理インターフェイスを識別できます。**show** 特権 EXEC コマンドを使用して、スイッチ上の特定のインターフェイスまたはすべてのインターフェイスに関する情報を表示することもできます。以降、この章では、主に物理インターフェイスの設定手順について説明します。

次に、スタッキング対応デバイスでインターフェイスを識別する例を示します。

- スタンドアロン デバイスの 10/100/1000 ポート 4 を設定するには、次のコマンドを入力します。

```
Device(config)# interface gigabitethernet1/0/4
```

- スタンドアロン デバイスに 10 ギガビット イーサネット ポート 1 を設定するには、次のコマンドを入力します。

```
Device(config)# interface tengigabitethernet1/0/1
```

- スタック メンバー 3 に 10 ギガビット イーサネット ポートを設定するには、次のコマンドを入力します。

```
Device(config)# interface tengigabitethernet3/0/1
```

- スタンドアロン デバイスの 1 番めの SFP モジュール（アップリンク）ポートを設定するには、次のコマンドを入力します。

```
Device(config)# interface gigabitethernet1/1/1
```

イーサネット インターフェイスのデフォルト設定

インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ3モードのインターフェイスをレイヤ2モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。

次の表は、レイヤ2インターフェイスにのみ適用される一部の機能を含む、イーサネットインターフェイスのデフォルト設定を示しています。

表 *3*: レイヤ *2* イーサネット インターフェイスのデフォルト設定

機能	デフォルト設定
動作モード	レイヤ 2 またはスイッチング モード（**switchport** コマンド）
VLAN 許容範囲	VLAN 1 ～ 4094
デフォルト VLAN（アクセス ポート用）	VLAN 1（レイヤ 2 インターフェイスだけ）
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1（レイヤ 2 インターフェイスだけ）
VLAN トランキング	Switchport mode dynamic auto（DTP をサポート）（レイヤ 2 インターフェイスだけ）
ポート イネーブル ステート	すべてのポートがイネーブル
ポート記述	未定義

機能	デフォルト設定
速度	自動ネゴシエーション（10 ギガビット インターフェイス上では未サポート）
デュプレックス モード	自動ネゴシエーション（10 ギガビット インターフェイス上では未サポート）
フロー制御	フロー制御は**receive: off**に設定されます。送信パケットでは常にオフです。
EtherChannel（PAgP）	すべてのイーサネット ポートでディセーブル。
ポート ブロッキング（不明マルチキャストおよび不明ユニキャスト トラフィック）	ディセーブル（ブロッキングされない）（レイヤ 2 インターフェイスだけ）。
ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御	ディセーブル
保護ポート	ディセーブル（レイヤ 2 インターフェイスだけ）。
ポート セキュリティ	ディセーブル（レイヤ 2 インターフェイスだけ）。
PortFast	ディセーブル
Auto-MDIX	イネーブル （注） 受電デバイスがクロス ケーブルでスイッチに接続されている場合、スイッチは、IEEE 802.3af に完全には準拠していない、Cisco IP Phone やアクセスポイントなどの準規格の受電をサポートしていない場合があります。これは、スイッチ ポート上で Automatic Medium-Dependent Interface Crossover（Auto-MIDX）がイネーブルかどうかは関係ありません。
Power over Ethernet（PoE）	イネーブル（auto）

インターフェイス速度およびデュプレックス モード

スイッチのイーサネットインターフェイスは、全二重または半二重モードのいずれかで、10、100、 1000 または 10,000 Mb/s で動作します。全二重モードの場合、2 つのステーションが同時にトラフィックを送受信できます。通常、10 Mbps ポートは半二重モードで動作します。これは、各ステーションがトラフィックを受信するか、送信するかのどちらか一方しかできないことを意味します。

スイッチ モデルには、ギガビット イーサネット（10/100/1000 Mbps）ポート、10 ギガビット イーサネット ポート、および SFP モジュールをサポートする Small Form-Factor Pluggable（SFP）モジュール スロットが含まれます。

速度とデュプレックス モードの設定時の注意事項

インターフェイス速度とデュプレックスモードを設定する際には、次のガイドラインに注意してください。

- 10 ギガビット イーサネット ポートは、速度機能およびデュプレックス機能をサポートしていません。これらのポートは、10,000 Mbps、全二重モードでだけ動作します。
- ギガビット イーサネット（10/100/1000 Mbps）ポートは、すべての速度オプションとデュプレックス オプション（自動、半二重、全二重）をサポートします。ただし、1000 Mbps で稼働させているギガビットイーサネットポートは、半二重モードをサポートしません。
- SFP モジュール ポートの場合、次の SFP モジュール タイプによって速度とデュプレックスの CLI（コマンドライン インターフェイス）オプションが変わります。
  - 1000 BASE-*x*（*x* は、BX、CWDM、LX、SX、および ZX）SFP モジュール ポートは、**speed** インターフェイス コンフィギュレーション コマンドで **nonegotiate** キーワードをサポートします。デュプレックス オプションはサポートされません。
  - 1000BASE-T SFP モジュール ポートは、10/100/1000 Mbps ポートと同一の速度とデュプレックス オプションをサポートします。
- 回線の両側で自動ネゴシエーションがサポートされる場合は、デフォルトの **auto** ネゴシエーションを使用することを強くお勧めします。
- 一方のインターフェイスが自動ネゴシエーションをサポートし、もう一方がサポートしない場合は、両方のインターフェイス上でデュプレックスと速度を設定します。サポートする側で **auto** 設定を使用しないでください。
- STP がイネーブルの場合にポートを再設定すると、デバイスがループの有無を調べるために最大で 30 秒かかる可能性があります。STP の再設定が行われている間、ポート LED はオレンジに点灯します。

⚠

注意 インターフェイス速度とデュプレックスモードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

IEEE 802.3x フロー制御

フロー制御により、接続しているイーサネットポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。あるポートで輻輳が生じ、それ以上はトラフィックを受信できなくなった場合、ポーズフレームを送信することによって、その状態が解消されるまで送信を中止するように、

そのポートから相手ポートに通知します。ポーズ フレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、輻輳時のデータ パケット損失が防止されます。

（注） フロー制御は、Catalyst 3850 および Catalyst 3650 シリーズ スイッチ（CSCul33405）ではサポートされません。

（注） スイッチ ポートは、ポーズ フレームを受信できますが、送信はできません。

flowcontrolインターフェイス コンフィギュレーション コマンドを使用して、インターフェイスのポーズ フレームを受信（**receive**）する能力を **on**、**off**、または **desired** に設定します。デフォルトの状態は **off** です。

desired に設定した場合、インターフェイスはフロー制御パケットの送信を必要とする接続デバイス、または必要ではないがフロー制御パケットを送信できる接続デバイスに対して動作できます。

デバイスのフロー制御設定には、次のルールが適用されます。

- **receive on** （または**desired**）：ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要のある、または送信できる接続デバイスと組み合わせて使用できます。ポーズ フレームの受信は可能です。
- **receive off**：フロー制御はどちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。

レイヤ 3 インターフェイス

デバイスは、次のレイヤ 3 インターフェイスのタイプをサポートします。

- SVI：トラフィックをルーティングする VLAN に対応する SVI を設定する必要があります。SVI は、**interface vlan** グローバル コンフィギュレーション コマンドのあとに VLAN ID を入力して作成します。SVI を削除するには、**no interface vlan** グローバル コンフィギュレーション コマンドを使用します。インターフェイス VLAN 1 は削除できません。

  （注） 物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

  SVI を設定するとき、SVI ラインステート ステータスを判断する際に含めないようにするため、SVI 自動ステート除外を SVI のポートに設定することもできます。

- ルーテッド ポート：ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ 3 モードに設定された物理ポートです。

- レイヤ 3 EtherChannel ポート：EtherChannel インターフェイスは、ルーテッド ポートで構成されます。

レイヤ 3 デバイスは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。

デバイスまたはデバイス スタックで設定可能な SVI とルーテッド ポートの数に対して定義された制限はありません。ただし、ハードウェアには限界があるため、SVI およびルーテッド ポートの個数と、設定されている他の機能の個数の組み合わせによっては、CPU利用率が影響を受けることがあります。デバイスが最大限のハードウェア リソースを使用している場合にルーテッド ポートまたは SVI を作成しようとすると、次のような結果になります。

- 新たなルーテッドポートを作成しようとすると、デバイスはインターフェイスをルーテッド ポートに変換するための十分なリソースがないことを示すメッセージを表示し、インターフェイスはスイッチポートのままとなります。
- 拡張範囲の VLAN を作成しようとすると、エラー メッセージが生成され、拡張範囲の VLAN は拒否されます。
- VLAN トランキング プロトコル（VTP）が新たな VLAN をデバイスに通知すると、使用可能な十分なハードウェア リソースがないことを示すメッセージを送り、その VLAN をシャットダウンします。**show vlan** ユーザ EXEC コマンドの出力に、サスペンド ステートの VLAN が示されます。
- デバイスが、ハードウェアのサポート可能な数を超える VLAN とルーテッド ポートが設定されたコンフィギュレーションを使って起動を試みると、VLAN は作成されますが、ルーテッド ポートはシャットダウンされ、デバイスはハードウェア リソースが不十分であるという理由を示すメッセージを送信します。

すべてのレイヤ 3 インターフェイスには、トラフィックをルーティングするための IP アドレスが必要です。次の手順は、レイヤ3インターフェイスとしてインターフェイスを設定する方法およびインターフェイスに IP アドレスを割り当てる方法を示します。

（注） 物理ポートがレイヤ 2 モードである（デフォルト）場合は、**no switchport** インターフェイス コンフィギュレーション コマンドを実行してインターフェイスをレイヤ3モードにする必要があります。**no switchport** コマンドを実行すると、インターフェイスがディセーブルになってから再度イネーブルになります。これにより、インターフェイスが接続しているデバイスに関するメッセージが生成されることがあります。さらに、レイヤ2モードのインターフェイスをレイヤ3モードにすると、影響を受けたインターフェイスに関連する前の設定情報は失われ、インターフェイスはデフォルト設定に戻る可能性があります。

Digital Optical Monitoring

スイッチは、業界標準の SFF 8724 Multi-Source Agreement（MSA）に従って、Digital Optical Monitoring（DOM）機能をサポートしています。この機能によって、光入出力パワー、温度、

電圧を監視できます。これらのパラメータはしきい値に対して監視され、スイッチに取り付けられているトランシーバのしきい値違反を表示できます。

この機能は、DOM に対応しているすべてのトランシーバでサポートされていますが、デフォルトでは無効になります。

DOM 対応トランシーバの識別

cisco.com に公開されている以下の情報を参照してください。https://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/DOM_matrix.html

または

お使いのデバイスで DOM に対応したトランシーバの一覧を表示できます。特権 EXEC モードで、**show interfaces transceiver supported-list** コマンドを入力します。

インターフェイスの特性の設定方法

インターフェイスの設定

次の一般的な手順は、すべてのインターフェイス設定プロセスに当てはまります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** 例： `Device(config)# interface`	インターフェイス タイプ、デバイス番号（スタック対応スイッチのみ）、およびコネクタの数を識別します。

	コマンドまたはアクション	目的
	gigabitethernet1/0/1 Device(config-if)#	（注） インターフェイス タイプとインターフェイス番号の間にスペースを入れる必要はありません。たとえば、前出の行の場合は、**gigabitethernet 1/0/1**、**gigabitethernet1/0/1**、**gi 1/0/1**、または **gi1/0/1** のいずれかを指定できます。
ステップ 4	各 **interface** コマンドの後ろに、インターフェイスに必要なインターフェイス コンフィギュレーション コマンドを続けて入力します。	インターフェイス上で実行するプロトコルとアプリケーションを定義します。別のインターフェイス コマンドまたは **end** を入力して特権 EXEC モードに戻ると、コマンドが収集されてインターフェイスに適用されます。
ステップ 5	**interface range** または **interface range macro**	（任意）インターフェイスの範囲を設定します。 （注） ある範囲内で設定したインターフェイスは、同じタイプである必要があります。また、同じ機能オプションを指定して設定しなければなりません。
ステップ 6	**show interfaces**	スイッチ上のまたはスイッチに対して設定されたすべてのインターフェイスのリストを表示します。デバイスがサポートする各インターフェイスまたは指定したインターフェイスのレポートが出力されます。

インターフェイスに関する記述の追加

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Device> **enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	記述を追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**description** *string* 例： `Device(config-if)# description Connects to Marketing`	インターフェイスに関する説明を追加します（最大 240 文字）。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id***description**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイス範囲の設定

同じ設定パラメータを持つ複数のインターフェイスを設定するには、**interface range** グローバル コンフィギュレーション コマンドを使用します。インターフェイス レンジ コンフィギュレーション モードを開始すると、このモードを終了するまで、入力されたすべてのコマンド パラメータはその範囲内のすべてのインターフェイスに対するものと見なされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface range** {*port-range* | **macro** *macro_name*} 例： `Device(config)# interface range macro`	設定するインターフェイス範囲（VLAN または物理ポート）を指定し、インターフェイス コンフィギュレーション モードを開始します。 • **interface range** コマンドを使用すると、最大 5 つのポート範囲または定義済みマクロを 1 つ設定できます。 • **macro** 変数については、インターフェイス レンジ マクロの設定および使用方法（118 ページ）を参照してください。 • カンマで区切った *port-range* では、各エントリに対応するインターフェイス タイプを入力し、カンマの前後にスペースを含めます。 • ハイフンで区切った *port-range* では、インターフェイス タイプの再入力は不要ですが、ハイフンの前後にスペースを入力する必要があります。 （注） この時点で、通常のコンフィギュレーション コマンドを使用して、範囲内のすべてのインターフェイスにコンフィギュレーション パラメータを適用します。各コマンドは、入力されたとおりに実行されます。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** [*interface-id*] 例： `Device# show interfaces`	指定した範囲内のインターフェイスの設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイス レンジ マクロの設定および使用方法

インターフェイス レンジ マクロを作成すると、設定するインターフェイスの範囲を自動的に選択できます。**interface range macro** グローバル コンフィギュレーション コマンドで **macro** キーワードを使用するには、まず **define interface-range** グローバル コンフィギュレーション コマンドでマクロを定義する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**define interface-range** *macro_name interface-range* 例：	インターフェイス範囲マクロを定義して、NVRAM に保存します。

	コマンドまたはアクション	目的
	`Device(config)# define interface-range enet_list gigabitethernet1/0/1 - 2`	• *macro_name* は、最大 32 文字の文字列です。 • マクロには、カンマで区切ったインターフェイスを 5 つまで指定できます。 • それぞれの *interface-range* は、同じポート タイプで構成されていなければなりません。 （注） **interface range macro** グローバル コンフィギュレーション コマンドで **macro** キーワードを使用するには、まず **define interface-range** グローバル コンフィギュレーション コマンドでマクロを定義する必要があります。
ステップ 4	**interface range macro** *macro_name* 例： `Device(config)# interface range macro enet_list`	*macro_name* の名前でインターフェイス範囲マクロに保存された値を使用することによって、設定するインターフェイスの範囲を選択します。 ここで、通常のコンフィギュレーション コマンドを使用して、定義したマクロ内のすべてのインターフェイスに設定を適用できます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config|include define** 例： `Device# show running-config | include define`	定義済みのインターフェイス範囲マクロの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

イーサネット インターフェイスの設定

インターフェイス速度およびデュプレックス パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/3`	設定する物理インターフェイスを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	**speed** {**10** | **100** | **1000** | **2500** | **5000** | **10000** | **auto** [**10** | **100** | **1000** | **2500** | **5000** | **10000**] | **nonegotiate**} 例： `Device(config-if)# speed 10`	インターフェイスに対する適切な速度パラメータを入力します。 • **10**、**100**、**1000**、**2500**、**5000** または **10000** を入力して、インターフェイスの速度を指定します。 • インターフェイスに接続されたデバイスと自動ネゴシエーションが行えるようにするには、**auto** を入力します。速度を指定しする際に **auto** キーワードも設定する場合、ポートは指定の速度でのみ自動ネゴシエートします。 • **nonegotiate** キーワードを使用できるのは、SFP モジュール ポートに

	コマンドまたはアクション	目的
		対してだけです。SFP モジュール ポートは1000 Mbpsだけで動作しますが、自動ネゴシエーションをサポートしていないデバイスに接続されている場合は、ネゴシエートしないように設定できます。
ステップ 5	**duplex** {**auto** | **full** | **half**} 例： `Device(config-if)# duplex half`	このコマンドは、10 ギガビット イーサネット インターフェイスでは使用できません。 インターフェイスのデュプレックス パラメータを入力します。 半二重モードをイネーブルにします（10または100Mbpsのみで動作するインターフェイスの場合）。1000 Mbpsで動作するインターフェイスには半二重モードを設定できません。 デュプレックス設定を行うことができるのは、速度が **auto** に設定されている場合です。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id* 例： `Device# show interfaces gigabitethernet1/0/3`	インターフェイス速度およびデュプレックス モードの設定を表示します。
ステップ 8	**copyrunning-configstartup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

マルチギガビット イーサネット パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**interface tengigabitethernet** *interface number* 例： `Device(config)#interface tengigabitethernet 1/1/37`	10 ギガビット イーサネット インターフェイスを設定します。
ステップ 2	**speed auto** 例： `Device(config-if)#speed auto`	速度を自動速度ネゴシエーションに設定します。
ステップ 3	**downshift-enable** 例： `Device(config-if)#downshift-enable`	指定されたインターフェイスでダウンシフトをイネーブルにします。ダウンシフトを有効にすると、リンク品質が十分でない場合、またはリンクが継続的にダウンしている場合に、速度が低い値にシフトダウンされます。
ステップ 4	**end** 例： `Device(config-if)#end`	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces downshift** 例： `Device# show interfaces downshift`	（任意）すべてのマルチギガビットポートのダウンシフト ステータスを表示します。
ステップ 6	**show intefaces** *interface--number***downshift** 例： `Device# show interfaces TenGigabitEthernet 1/0/1 downshift`	（任意）指定されたマルチギガビットポートのダウンシフト ステータスを表示します。

	コマンドまたはアクション	目的
ステップ 7	**show intefaces downshift module** *module-number* 例： `Device# show interface downshift module 1`	（任意）指定されたモジュールのダウンシフト ステータスを表示します。
ステップ 8	**show ap name** *ap-name* **ethernet statistics** 例： `Device#show ap name testAP ethernet statistics`	（任意）特定の AP のイーサネット統計情報を表示します。

IEEE 802.3x フロー制御の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定する物理インターフェイスを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	**flowcontrol** {**receive**} {**on** | **off** | **desired**} 例： `Device(config-if)# flowcontrol receive on`	ポートのフロー制御モードを設定します。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show interfaces** *interface-id* 例： `Device# show interfaces gigabitethernet1/0/1`	インターフェイス フロー制御の設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

レイヤ 3 インターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {**gigabitethernet** *interface-id*} | {**vlan** *vlan-id*} | {**port-channel** *port-channel-number*} 例： `Device(config)# interface gigabitethernet1/0/2`	レイヤ 3 インターフェイスとして設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no switchport** 例： `Device(config-if)# no switchport`	物理ポートに限り、レイヤ 3 モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**ip address** *ip_address subnet_mask* 例： `Device(config-if)# ip address 192.20.135.21 255.255.255.0`	IP アドレスおよび IP サブネットを設定します。
ステップ 6	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** [*interface-id*]	設定を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

論理レイヤ 3 GRE トンネル インターフェイスの設定

始める前に

総称ルーティング カプセル化（GRE）は、仮想ポイントツーポイント リンク内でネットワーク層プロトコルをカプセル化するために使用されるトンネリング プロトコルです。GRE トンネルは、カプセル化のみを提供し、暗号化は提供しません。

注目 Cisco IOS XE Release 3.7.2E 以降では、GRE トンネルは Cisco Catalyst スイッチのハードウェアでサポートされます。GRE でトンネル オプションを設定しない場合、パケットはハードウェアでスイッチングされます。GRE でトンネル オプション（キーやチェックサムなど）を設定すると、パケットはソフトウェアでスイッチングされます。最大 10 個の GRE トンネルがサポートされます。

（注） アクセス コントロール リスト（ACL）や Quality of Service（QoS）などその他の機能は、GRE トンネルではサポートされません。

GRE トンネルを設定する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	**interface tunnel** *number* 例： `Device(config)#interface tunnel 2`	インターフェイスでトンネリングをイネーブルにします。
ステップ 2	**ip address***ip_addresssubnet_mask* 例： `Device(config)#ip address 100.1.1.1 255.255.255.0`	IP アドレスおよび IP サブネットを設定します。
ステップ 3	**tunnel source** {*ip_address* | *type_number*} 例： `Device(config)#tunnel source 10.10.10.1`	トンネル送信元を設定します。
ステップ 4	**tunnel destination** {*host_name* | *ip_address*} 例： `Device(config)#tunnel destination 10.10.10.2`	トンネル宛先を設定します。
ステップ 5	**tunnel mode gre ip** 例： `Device(config)#tunnel mode gre ip`	トンネル モードを設定します。
ステップ 6	**end** 例： `Device(config)#end`	コンフィギュレーション モードを終了します。

SVI 自動ステート除外の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	レイヤ2インターフェイス（物理ポートまたはポート チャネル）を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport autostate exclude** 例： `Device(config-if)# switchport autostate exclude`	SVI ライン ステート（アップまたはダウン）のステータスを定義する際、アクセスまたはトランク ポートを除外します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running config interface** *interface-id*	（任意）実行コンフィギュレーションを表示します。 設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスのシャットダウンおよび再起動

インターフェイスをシャットダウンすると、指定されたインターフェイスのすべての機能がディセーブルになり、使用不可能であることがすべてのモニタ コマンドの出力に表示されます。この情報は、すべてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。ルーティング アップデートには、インターフェイス情報は含まれません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {**vlan** *vlan-id*} | {**gigabitethernet***interface-id*} | {**port-channel** *port-channel-number*} 例： `Device(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを選択します。
ステップ 4	**shutdown** 例： `Device(config-if)# shutdown`	インターフェイスをシャットダウンします。
ステップ 5	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイスを再起動します。
ステップ 6	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# end`	
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。

コンソール メディア タイプの設定

コンソール メディア タイプを RJ-45 に設定するには、次の手順を実行します。RJ-45 としてコンソールを設定すると、USB コンソール オペレーションはディセーブルになり、入力は RJ-45 コネクタからのみ供給されます。

この設定はスタックのすべてのスイッチに適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lineconsole 0** 例： `Device(config)# line console 0`	コンソールを設定し、ライン コンフィギュレーション モードを開始します。
ステップ 4	**media-typerj45** 例： `Device(config-line)# media-type rj45`	コンソール メディア タイプが RJ-45 ポート以外に設定されないようにします。このコマンドを入力せず、両方のタイプが接続された場合は、デフォルトで USB ポートが使用されます。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

USB 無活動タイムアウトの設定

無活動タイムアウトを設定している場合、USB コンソール ポートがアクティブ化されているものの、指定された時間内にポートで入力アクティビティがないときに、RJ-45 コンソール ポートが再度アクティブになります。タイムアウトのために USB コンソール ポートは非アクティブ化された場合、USB ポートを切断し、再接続すると、動作を回復できます。

（注） 設定された無活動タイムアウトはスタックのすべてのデバイスに適用されます。しかし、あるデバイスのタイムアウトはスタック内の別のデバイスにタイムアウトを発生させません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lineconsole 0** 例： `Device(config)# line console 0`	コンソールを設定し、ライン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**usb-inactivity-timeout** *timeout-minutes* 例： `Device(config-line)# usb-inactivity-timeout 30`	コンソール ポートの無活動タイムアウトを指定します。指定できる範囲は1～240分です。デフォルトでは、タイムアウトが設定されていません。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Digital Optical Monitoring の有効化

トランシーバのモニタリングを有効にするには、次の手順を完了します。

（注）

- SFP と RJ45 のプロビジョニングを行うコンボ ポートの場合は、SFP トランシーバがスロットまたはポートに差し込まれているが、メディア タイプが SFP に設定されていないと、DOM はグローバルにトランシーバのモニタリングが有効な場合のみ機能します。
- CISCO-ENTITY-SENSOR-MIB トラップは、しきい値違反後に一度だけ送信されます。ただし、SYSLOG メッセージはモニタリング間隔に従って送信されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**transceiver type all** 例：	トランシーバ タイプ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# transceiver type`	
ステップ 4	**monitoring interval***seconds* 例： `Device(config-xcvr-type)# monitoring interval 500`	すべてのオプティカル トランシーバのモニタリングを有効にします。 モニタリング パラメータのポーリングが発生する間隔を指定できます。有効な範囲は 300 ～ 3600 秒で、デフォルト設定は 600 秒です。

次のタスク

モニタリングを有効にした後は、これらの **show** コマンドを使用してデバイスのリアルタイムパラメータを表示できます。

- **show interfaces transceiver**
- **show interfaces transceiver detail**
- **show interfaces** *interface-id* **transceiver**

インターフェイス特性のモニタ

インターフェイス ステータスの監視

特権EXECプロンプトにコマンドを入力することによって、ソフトウェアおよびハードウェアのバージョン、コンフィギュレーション、インターフェイスに関する統計情報などのインターフェイス情報を表示できます。

表 *4*: インターフェイス用の *show* コマンド

コマンド	目的
show interfaces *interface-id***status** [**err-disabled**]	インターフェイスのステータスまたはerrdisableステートにあるインターフェイスのリストを表示します。
show interfaces [*interface-id*] **switchport**	スイッチング（非ルーティング）ポートの管理上および動作上のステータスを表示します。このコマンドを使用すると、ポートがルーティングまたはスイッチングのどちらのモードにあるかが判別できます。
show interfaces [*interface-id*] **description**	1 つのインターフェイスまたはすべてのインターフェイスに関する記述とインターフェイスのステータスを表示します。

コマンド	目的
show ip interface [*interface-id*]	IP ルーティング用に設定されたすべてのインターフェイスまたは特定のインターフェイスについて、使用できるかどうかを表示します。
show interface [*interface-id*] **stats**	インターフェイスのパスごとに入出力パケットを表示します。
show interfaces *interface-id*	（任意）インターフェイスの速度およびデュプレックスを表示します。
show interfacestransceiverdom-supported-list	（任意）接続 SFP モジュールの Digital Optical Monitoring（DOM）ステータスを表示します。
show interfaces transceiver properties	（任意）インターフェイスの温度、電圧、電流量を表示します。
show interfaces [*interface-id*] [{**transceiver properties** | **detail**}] *module number*]	SFP モジュールに関する物理および動作ステータスを表示します。
show running-config interface [*interface-id*]	インターフェイスに対応する RAM 上の実行コンフィギュレーションを表示します。
show version	ハードウェア設定、ソフトウェア バージョン、コンフィギュレーションファイルの名前と送信元、およびブート イメージを表示します。
show controllers ethernet-controller *interface-id***phy**	インターフェイスの Auto-MDIX 動作ステートを表示します。

インターフェイスおよびカウンタのクリアとリセット

表 *5:* インターフェイス用の ***clear*** コマンド

コマンド	目的
clear counters [*interface-id*]	インターフェイス カウンタをクリアします。
clear interface *interface-id*	インターフェイスのハードウェア ロジックをリセットします。
clear line [*number* | **console 0** | **vty** *number*]	非同期シリアル回線に関するハードウェア ロジックをリセットします。

（注） **clear counters** 特権 EXEC コマンドは、簡易ネットワーク管理プロトコル（SNMP）を使用して取得されたカウンタをクリアしません。**show interface** 特権 EXEC コマンドで表示されるカウンタのみをクリアします。

インターフェイス特性の設定例

インターフェイスの説明の追加：例

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# description Connects to Marketing
Device(config-if)# end
Device# show interfaces gigabitethernet1/0/2 description
Interface Status         Protocol Description
Gi1/0/2   admin down     down     Connects to Marketing
```

インターフェイスのダウンシフト ステータスの表示：例

次に、すべてのマルチギガビットポートのダウンシフトステータスを表示する例を示します。

```
Device# show interfaces downshift

Port         Enabled         Active         AdminSpeed        OperSpeed
Te2/0/37       yes            no              auto              auto
Te2/0/38       yes            no              auto              10G
Te2/0/39       yes            no              auto              auto
Te2/0/40       yes            no              auto              10G
Te2/0/41       yes            no              auto              auto
Te2/0/42       yes            no              auto              auto
Te2/0/43       yes            yes             auto              5000
Te2/0/44       yes            no              auto              auto
Te2/0/45       yes            yes             auto              2500
Te2/0/46       yes            no              auto              auto
Te2/0/47       yes            no              auto              10G
Te2/0/48       yes            no              auto              auto
```

次に、指定したマルチギガビットポートのダウンシフトステータスを表示する例を示します。

```
Device# show interfaces  te2/0/43 downshift

Port         Enabled         Active             AdminSpeed        OperSpeed
Te2/0/43       yes             yes                10G               5000
```

コマンド出力のフィールドについて、以下に説明します。

Port	インターフェイス番号を表示します
イネーブル	指定したポートでダウンシフトが有効（yes）または無効（no）であることを示します
Active	ダウンシフトがインターフェイスで発生しているかどうかを示します
AdminSpeed	ユーザが設定した速度（または）デフォルトのインターフェイス速度を表示します
OperSpeed	インターフェイスの現在の動作速度を表示します。

インターフェイス範囲の設定：例

この例では、**interface range** グローバル コンフィギュレーション コマンドを使用して、スイッチ 1 上のポート 1 ～ 4 で速度を 100 Mb/s に設定する例を示します。

```
Device# configure terminal
Device(config)# interface range gigabitethernet1/0/1 - 4
Device(config-if-range)# speed 100
```

この例では、カンマを使用して範囲に異なるインターフェイスタイプ ストリングを追加して、ギガビット イーサネット ポート 1 ～ 3 と、10 ギガビット イーサネット ポート 1 および 2 の両方をイネーブルにし、フロー制御ポーズ フレームを受信できるようにします。

```
Device# configure terminal
Device(config)# interface range gigabitethernet1/0/1 - 3 , tengigabitethernet1/0/1 - 2
Device(config-if-range)# flowcontrol receive on
```

インターフェイス レンジ モードで複数のコンフィギュレーション コマンドを入力した場合、各コマンドは入力した時点で実行されます。インターフェイス レンジモードを終了した後で、コマンドがバッチ処理されるわけではありません。コマンドの実行中にインターフェイス レンジコンフィギュレーションモードを終了すると、一部のコマンドが範囲内のすべてのインターフェイスに対して実行されない場合もあります。コマンドプロンプトが再表示されるのを待ってから、インターフェイス範囲コンフィギュレーション モードを終了してください。

インターフェイス レンジ マクロの設定および使用方法：例

次に、*enet_list* という名前のインターフェイス範囲マクロを定義してスイッチ 1 上のポート 1 および 2 を含め、マクロ設定を確認する例を示します。

```
Device# configure terminal
Device(config)# define interface-range enet_list gigabitethernet1/0/1 - 2
Device(config)# end
Device# show running-config | include define
define interface-range enet_list GigabitEthernet1/0/1 - 2
```

次に、複数のタイプのインターフェイスを含む マクロ *macro1* を作成する例を示します。

```
Device# configure terminal
Device(config)# define interface-range macro1 gigabitethernet1/0/1 - 2,
gigabitethernet1/0/5 - 7, tengigabitethernet1/0/1 -2
Device(config)# end
```

次に、インターフェイス レンジ マクロ *enet_list* に対するインターフェイス レンジ コンフィギュレーション モードを開始する例を示します。

```
Device# configure terminal
Device(config)# interface range macro enet_list
Device(config-if-range)#
```

次に、インターフェイス レンジ マクロ *enet_list* を削除し、処理を確認する例を示します。

```
Device# configure terminal
Device(config)# no define interface-range enet_list
Device(config)# end
Device# show run | include define
Device#
```

インターフェイス速度およびデュプレックス モードの設定：例

次に、インターフェイス速度を 100 Mb/s に、10/100/1000 Mbps ポートのデュプレックス モードを半二重に設定する例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# speed 10
Device(config-if)# duplex half
```

次に、10/100/1000 Mbps ポートで、インターフェイスの速度を 100 Mbps に設定する例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# speed 100
```

レイヤ 3 インターフェイスの設定：例

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)# ip address 192.20.135.21 255.255.255.0
Device(config-if)# no shutdown
```

コンソール メディア タイプの設定：例

次に、USB コンソール メディア タイプをディセーブルにし、RJ-45 コンソール メディア タイプをイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# media-type rj45
```

この設定は、スタック内のすべてのアクティブな USB コンソール メディア タイプを終了します。ログにはこの終了の発生が示されます。次に、スイッチ 1 のコンソールが RJ-45 に戻る例を示します。

```
*Mar  1 00:25:36.860: %USB_CONSOLE-6-CONFIG_DISABLE: Console media-type USB disabled by
 system configuration, media-type reverted to RJ45.
```

この時点で、スタック内のどのスイッチも USB コンソールでの入力を受け付けません。ログのエントリには、コンソール ケーブルがいつ接続されたかが示されています。USB コンソール ケーブルが switch 2 に接続されている場合、入力は提供されません。

```
*Mar  1 00:34:27.498: %USB_CONSOLE-6-CONFIG_DISALLOW: Console media-type USB is disallowed
 by system configuration, media-type remains RJ45. (switch-stk-2)
```

次に、前の設定を逆にして、ただちにすべての接続された USB コンソールをアクティブにする例を示します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# no media-type rj45
```

USB 無活動タイムアウトの設定：例

次に、無活動タイムアウトを 30 分に設定する例を示します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# usb-inactivity-timeout 30
```

設定をディセーブルにするには、次のコマンドを使用します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# no usb-inactivity-timeout
```

設定された分数の間に USB コンソール ポートで（入力）アクティビティがなかった場合、無活動タイムアウト設定が RJ-45 ポートに適用され、ログにこの発生が示されます。

```
*Mar  1 00:47:25.625: %USB_CONSOLE-6-INACTIVITY_DISABLE: Console media-type USB disabled
 due to inactivity, media-type reverted to RJ45.
```

この時点で、USB コンソール ポートを再度アクティブ化する唯一の方法は、ケーブルを取り外し、再接続することです。

スイッチのUSBケーブルが取り外され再接続された場合、ログは次のような表示になります。

```
*Mar  1 00:48:28.640: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.
```

インターフェイス特性機能の追加情報

関連資料

関連項目	マニュアル タイトル
プラットフォームに依存しないコマンド リファレンス	*Interface and Hardware Command Reference, Cisco IOS XE Release 3.2SE (Catalyst 3850 Switches)*
プラットフォームに依存しない設定情報	*Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
なし	--

MIB

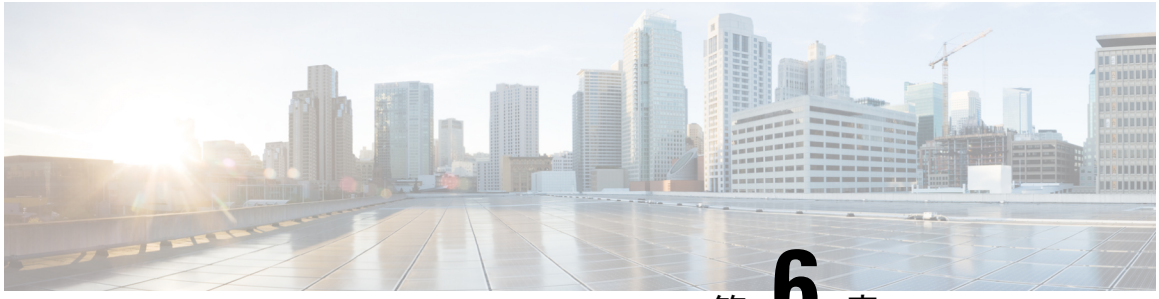
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

インターフェイス特性の設定の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。
Cisco IOS XE 3.7.2E	ハードウェアに GRE トンネルを設定するためのサポート。GRE でトンネル オプションを設定しない場合、パケットはハードウェアでスイッチングされます。
Cisco IOS XE Denali 16.3.2	mGig インターフェイスでのダウンシフトのサポートが導入されました。 インターフェイスでポート速度のダウンシフトが有効になっているときに、リンク品質が悪い場合またはリンクが継続的にダウン状態にある場合、ライン レートが自動的にダウングレードして低速になります。
Cisco IOS XE Denali 16.3.6	デジタル オプティカル モニタリングがサポートされるようになりました。この機能によって、光入出力パワー、温度、電圧を監視できます。 この機能は、DOM に対応しているすべてのトランシーバでサポートされていますが、デフォルトでは無効になります。



第 6 章

Auto-MDIX の設定

- Auto-MDIX の前提条件 （141 ページ）
- Auto-MDIX の制約事項 （141 ページ）
- Auto-MDIX の設定に関する情報 （142 ページ）
- Auto-MDIX の設定方法 （142 ページ）
- Auto-MDIX の設定例 （143 ページ）
- その他の参考資料 （144 ページ）
- Auto-MDIX の機能履歴と情報 （145 ページ）

Auto-MDIX の前提条件

インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。

デフォルトで Automatic Medium-Dependent Interface Crossover（Auto-MDIX）機能がイネーブルに設定されます。

Auto-MDIX は、すべての 10/100/1000 Mbps インターフェイスと、10/100/1000BASE-TX Small Form-Factor Pluggable（SFP）モジュール インターフェイスでサポートされています。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

Auto-MDIX の制約事項

受電デバイスがクロス ケーブルでデバイスに接続されている場合、デバイスは、IEEE 802.3af に完全には準拠していない、Cisco IP Phone やアクセス ポイントなどの準規格の受電をサポー

トしていない場合があります。これは、スイッチ ポート上で Automatic Medium-Dependent Interface Crossover（Auto-MIDX）がイネーブルかどうかは関係ありません。

Auto-MDIX の設定に関する情報

インターフェイスでの Auto-MDIX

自動メディア依存型インターフェイスクロスオーバー（MDIX）がイネーブルになっているインターフェイスでは、必要なケーブル接続タイプ（ストレートまたはクロス）が自動的に検出され、接続が適切に設定されます。Auto-MDIX 機能を使用せずにデバイスを接続する場合、サーバ、ワークステーション、またはルータなどのデバイスの接続にはストレート ケーブルを使用し、他のデバイスやリピータの接続にはクロス ケーブルを使用する必要があります。Auto-MDIX がイネーブルの場合、他のデバイスとの接続にはどちらのケーブルでも使用でき、ケーブルが正しくない場合はインターフェイスが自動的に修正を行います。ケーブル接続の詳細については、ハードウェア インストレーション ガイドを参照してください。

次の表に、Auto-MDIX の設定およびケーブル接続ごとのリンク ステートを示します。

表 *6 :* リンク状態と *Auto-MDIX* の設定

ローカル側の Auto-MDIX	リモート側の Auto-MDIX	ケーブル接続が正しい場合	ケーブル接続が正しくない場合
点灯	点灯	リンク アップ	リンク アップ
点灯	消灯	リンク アップ	リンク アップ
消灯	点灯	リンク アップ	リンク アップ
消灯	消灯	リンク アップ	リンク ダウン

Auto-MDIX の設定方法

インターフェイスでの Auto-MDIX の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定する物理インターフェイスを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	**speed auto** 例： `Device(config-if)# speed auto`	接続されたデバイスと速度の自動ネゴシエーションを行うようにインターフェイスを設定します。
ステップ 5	**duplex auto** 例： `Device(config-if)# duplex auto`	接続されたデバイスとデュプレックスモードの自動ネゴシエーションを行うようにインターフェイスを設定します。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Auto-MDIX の設定例

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto
Device(config-if)# duplex auto
Device(config-if)# mdix auto
Device(config-if)# end
```

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

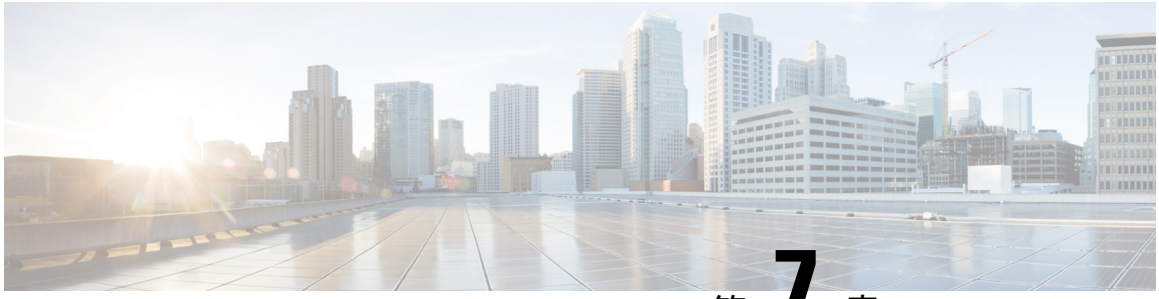
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Auto-MDIX の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。



第 7 章

イーサネット管理ポートの設定

- 機能情報の確認 （147 ページ）
- イーサネット管理ポートの前提条件 （147 ページ）
- イーサネット管理ポートに関する情報 （147 ページ）
- イーサネット管理ポートの設定方法 （150 ページ）
- その他の参考資料 （151 ページ）
- イーサネット管理ポートの機能情報 （152 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

イーサネット管理ポートの前提条件

PC をイーサネット管理ポートに接続するときに、最初に IP アドレスを割り当てる必要があります。

イーサネット管理ポートに関する情報

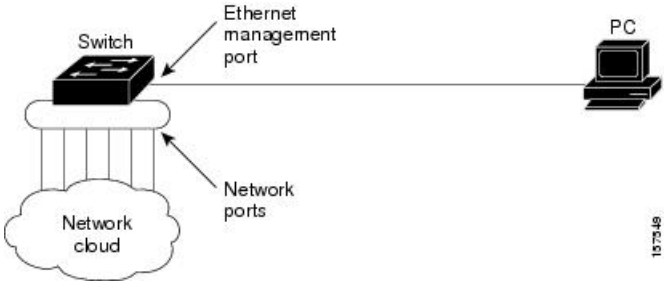
Gi0/0 または *GigabitEthernet0/0* ポートとも呼ばれるイーサネット管理ポートは、PC を接続する VRF（VPN ルーティング/転送）インターフェイスです。ネットワークの管理に、デバイス

コンソール ポートの代わりとしてイーサネット管理ポートを使用できます。デバイス スタックを管理するときに、PC をスタック メンバ上のイーサネット管理ポートに接続します。

デバイスへのイーサネット管理ポートの直接接続

図 *5: PC* とスイッチの接続

次の図は、デバイスまたはスタンドアロン デバイスに対して、イーサネット管理ポートを PC に接続する方法を示します。

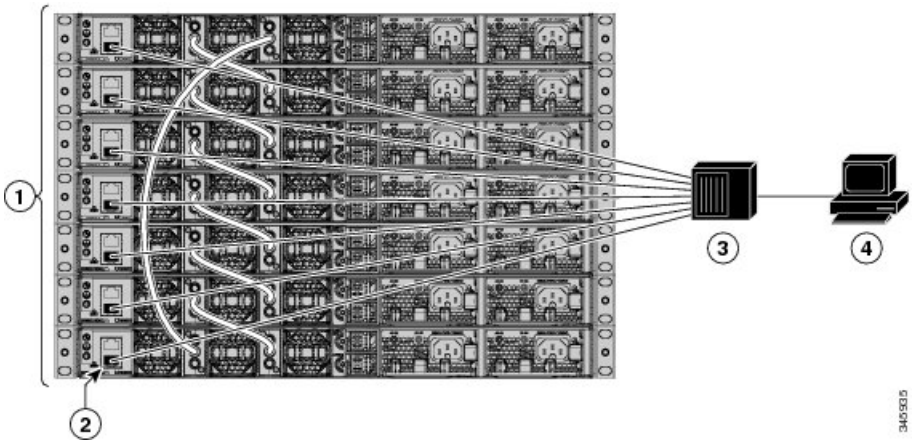


ハブを使用したスタックデバイスへのイーサネット管理ポートの接続

スタック デバイスのみのスタックでは、スタック メンバ上のすべてのイーサネット管理ポートが、PC が接続されるハブに接続されます。アクティブ スイッチのイーサネット管理ポートからのアクティブ リンクは、ハブを経由して PC とつながっています。アクティブ デバイスに障害が発生し、新しいアクティブ デバイスが選択された場合、アクティブ リンクは、新しいアクティブ デバイス上のイーサネット管理ポートから PC までになります。

図 *6: PC* とデバイス スタックの接続

次の図は、PC がハブを使用してデバイス スタックに接続する方法を示しています。



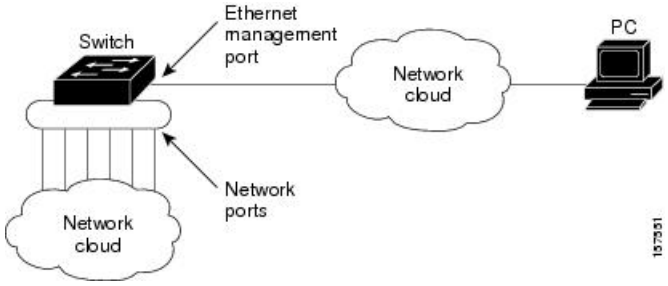
1	スイッチ スタック	3	ハブ
2	管理ポート	4	PC

イーサネット管理ポートおよびルーティング

デフォルトでは、イーサネット管理ポートは有効です。デバイスは、イーサネット管理ポートからネットワーク ポートにパケットをルーティングできず、その逆もできません。イーサネット管理ポートはルーティングをサポートしていませんが、ポート上でルーティングプロトコルを有効にすることが必要となる場合もあります。

図 7: ルーティング プロトコルを有効にしたネットワーク例

PC とデバイスが複数のホップ分離れていて、パケットが PC に到達するには複数のレイヤ 3 デバイスを経由しなければならない場合に、イーサネット管理ポート上のルーティングプロトコルを有効にします。



上記の図では、イーサネット管理ポートとネットワーク ポートが同じルーティング プロセスに関連付けられている場合、ルートは次のように伝播されます。

- イーサネット管理ポートからのルートは、ネットワーク ポートを通してネットワークに伝播されます。
- ネットワーク ポートからのルートは、イーサネット管理ポートを通してネットワークに伝播されます。

イーサネット管理ポートとネットワーク ポートの間ではルーティングはサポートされていないため、これらのポート間のトラフィックの送受信はできません。このような状況になると、これらのポート間にデータ パケット ループが発生し、デバイスおよびネットワークの動作が中断されます。このループを防止するには、イーサネット管理ポートとネットワーク ポートの間のルートを回避するためにルート フィルタを設定してください。

サポートされるイーサネット管理ポートの機能

イーサネット管理ポートは次の機能をサポートします。

- Express Setup（スイッチ スタックでのみ）
- Network Assistant
- パスワード付きの Telnet
- TFTP
- セキュア シェル（SSH）
- Dynamic Host Configuration Protocol（DHCP）ベースの自動設定

- SNMP（ENTITY-MIB および IF-MIB のみ）
- IP ping
- インターフェイス機能
  - 速度：10 Mb/s、100 Mb/s、1000 Mb/s、および自動ネゴシエーション
  - デュプレックス モード：全二重、半二重、自動ネゴシエーション
  - ループバック検出
- Cisco Discovery Protocol（CDP）
- DHCP リレー エージェント
- IPv4 アクセス コントロール リスト（ACL）
- ルーティング プロトコル

注意 イーサネット管理ポートの機能をイネーブルにする前に機能がサポートされていることを確認してください。イーサネット管理ポートのサポートされていない機能を設定しようとすると、機能は正しく動作せず、デバイスに障害が発生するおそれがあります。

イーサネット管理ポートの設定方法

イーサネット管理ポートのディセーブル化およびイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface gigabitethernet0/0** 例： `Device(config)# interface gigabitethernet0/0`	CLI でイーサネット管理ポートを指定します。
ステップ 3	**shutdown** 例： `Device(config-if)# shutdown`	イーサネット管理ポートをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**no shutdown** 例： `Device(config-if)# no shutdown`	イーサネット管理ポートをイネーブルにします。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	**show interfaces gigabitethernet0/0** 例： `Device# show interfaces gigabitethernet0/0`	リンク ステータスを表示します。 PC へのリンク ステータスを調べるには、イーサネット管理ポートの LED をモニタします。リンクがアクティブな場合、LED はグリーン（オン）であり、リンクが停止中の場合は、LED はオフです。POST エラーがある場合は、LED はオレンジです。

次のタスク

イーサネット管理ポートを使用したスイッチの管理または設定に進みます。*Network Management Configuration Guide*（*Catalyst 3850 Switches*）を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ブートローダ設定	『*System Management Configuration Guide (Catalyst 3850 Switches)*』
ブートローダ コマンド	『*System Management Command Reference (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

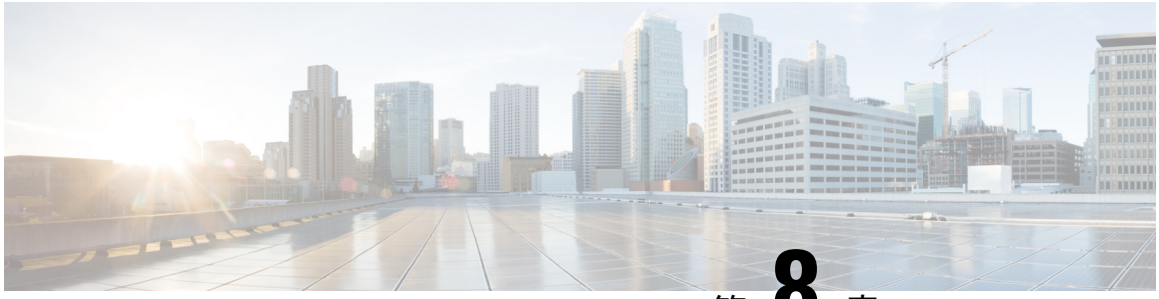
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

イーサネット管理ポートの機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。



第 8 章

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定

- 機能情報の確認 （153 ページ）
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要 （154 ページ）
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定方法 （159 ページ）
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定例 （170 ページ）
- LLDP、LLDP-MED、ワイヤード ロケーション サービスのモニタリングとメンテナンス （170 ページ）
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの追加情報 （172 ページ）
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの機能情報 （173 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要

LLDP

Cisco Discovery Protocol（CDP）は、すべてのシスコ製デバイス（ルータ、ブリッジ、アクセス サーバ、スイッチ、およびコントローラ）のレイヤ2（データ リンク層）上で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、ネットワーク接続されている他のシスコ デバイスを自動的に検出し、識別できます。

デバイスでは他社製のデバイスをサポートし他のデバイス間の相互運用性を確保するために、IEEE 802.1AB リンク層検出プロトコル（LLDP）をサポートしています。LLDP は、ネットワーク デバイスがネットワーク上の他のデバイスに自分の情報をアドバタイズするために使用するネイバー探索プロトコルです。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する 2 つのシステムで互いの情報を学習できます。

LLDP でサポートされる TLV

LLDP は一連の属性をサポートし、これらを使用してネイバーデバイスを検出します。属性には、Type、Length、および Value の説明が含まれていて、これらを TLV と呼びます。LLDP をサポートするデバイスは、ネイバーとの情報の送受信に TLV を使用できます。このプロトコルは、設定情報、デバイス機能、およびデバイス ID などの詳細情報をアドバタイズできます。

スイッチは、次の基本管理 TLV をサポートします。これらは必須の LLDP TLV です。

- ポート記述 TLV
- システム名 TLV
- システム記述 TLV
- システム機能 TLV
- 管理アドレス TLV

次の IEEE 固有の LLDP TLV もアドバタイズに使用されて LLDP-MED をサポートします。

- ポート VLAN ID TLV（IEEE 802.1 に固有の TLV）
- MAC/PHY コンフィギュレーション/ステータス TLV（IEEE 802.3 に固有の TLV）

LLDP および Cisco デバイス のスタック

デバイス スタックは、ネットワーク内の 1 つのデバイスとして表示されます。したがって、LLDP は、個々のスタック メンバではなく、デバイス スタックを検出します。

LLDP-MED

LLDP for Media Endpoint Devices（LLDP-MED）は LLDP の拡張版で、IP 電話などのエンドポイント デバイスとデバイスなどのネットワーク デバイスの間で動作します。特に VoIP アプリケーションをサポートし、検出機能、ネットワーク ポリシー、Power over Ethernet（PoE）、インベントリ管理、およびロケーション情報に関する TLV を提供します。デフォルトで、すべての LLDP-MED TLV がイネーブルです。

LLDP-MED でサポートされる TLV

LLDP-MED では、次の TLV がサポートされます。

- LLDP-MED 機能 TLV

  LLDP-MED エンドポイントは、接続装置がサポートする機能と現在イネーブルになっている機能を識別できます。

- ネットワーク ポリシー TLV

  ネットワーク接続デバイスとエンドポイントはともに、VLAN 設定、および関連するレイヤ 2 とレイヤ 3 属性をポート上の特定アプリケーションにアドバタイズできます。たとえば、スイッチは使用する VLAN 番号を IP 電話に通知できます。IP 電話は任意のデバイスに接続し、VLAN 番号を取得してから、コール制御の通信を開始できます。

  ネットワーク ポリシー プロファイル TLV を定義することによって、VLAN、サービス クラス（CoS）、Diffserv コード ポイント（DSCP）、およびタギング モードの値を指定して、音声と音声信号のプロファイルを作成できます。その後、これらのプロファイル属性は、スイッチで中央集約的に保守され、IP 電話に伝播されます。

- 電源管理 TLV

  LLDP-MED エンドポイントとネットワーク接続デバイスの間で拡張電源管理を可能にします。デバイスおよび IP 電話は、デバイスの受電方法、電源プライオリティ、デバイスの消費電力などの電源情報を通知することができます。

  LLDP-MED は拡張電源 TLV もサポートして、きめ細かな電力要件、エンドポイント電源プライオリティ、およびエンドポイントとネットワークの接続デバイスの電源ステータスをアドバタイズします。LLDP がイネーブルでポートに電力が供給されているときは、電力 TLV によってエンドポイント デバイスの実際の電力要件が決定するので、それに応じてシステムの電力バジェットを調整することができます。デバイスは要求を処理し、現在の電力バジェットに基づいて電力を許可または拒否します。要求が許可されると、スイッチは電力バジェットを更新します。要求が拒否された場合、デバイスは、ポートの電力をオフに切り替え、Syslog メッセージを生成して電力バジェットを更新します。LLDP-MED がディセーブルの場合や、エンドポイントが LLDP-MED 電力 TLV をサポートしていない場合は、初期割り当て値が接続終了まで使用されます。

  power inline {**auto** [**max** *max-wattage*] | **never** | **static** [**max** *max-wattage*]} インターフェイス コンフィギュレーション コマンドを入力して、電力設定を変更できます。PoE インターフェイスはデフォルトで **auto** モードに設定されています。値を指定しない場合は、最大電力（30 W）が供給されます。

- インベントリ管理 TLV

  エンドポイントは、デバイスにエンドポイントの詳細なインベントリ情報を送信することが可能です。インベントリ情報には、ハードウェア リビジョン、ファームウェア バージョン、ソフトウェア バージョン、シリアル番号、メーカー名、モデル名、Asset ID TLV などがあります。

- ロケーション TLV

  デバイスからのロケーション情報をエンドポイントデバイスに提供します。ロケーション TLV はこの情報を送信することができます。

  - 都市ロケーション情報

    都市アドレス情報および郵便番号情報を提供します。都市ロケーション情報の例には、地名、番地、郵便番号などがあります。

  - ELIN ロケーション情報

    発信側のロケーション情報を提供します。ロケーションは、緊急ロケーション識別番号（ELIN）によって決定されます。これは、緊急通報を Public Safety Answering Point（PSAP）にルーティングする電話番号で、PSAP はこれを使用して緊急通報者にコールバックすることができます。

  - 地理的なロケーション情報

    スイッチの緯度、経度、および高度などのスイッチ位置の地理的な詳細を指定します。

  - カスタム ロケーション

    スイッチの位置のカスタマイズされた名前と値を入力します。

ワイヤード ロケーション サービス

デバイスは、接続されているデバイスのロケーション情報およびアタッチメント追跡情報を Cisco Mobility Services Engine（MSE）に送信するのにロケーション サービス機能を使用します。トラッキングされたデバイスは、ワイヤレス エンドポイント、ワイヤード エンドポイント、またはワイヤード デバイスまたはコントローラになります。デバイスは、MSE にネットワーク モビリティ サービス プロトコル（NMSP）のロケーション通知および接続通知を介して、デバイスのリンク アップ イベントおよびリンク ダウン イベントを通知します。

MSE がデバイスに対して NMSP 接続を開始すると、サーバ ポートが開きます。MSE がデバイスに接続する場合は、バージョンの互換性を確保する 1 組のメッセージ交換およびサービス交換情報があり、その後にロケーション情報の同期が続きます。接続後、デバイスは定期的にロケーション通知および接続通知を MSE に送信します。インターバル中に検出されたリンク アップ イベントまたはリンク ダウン イベントは、集約されてインターバルの最後に送信されます。

デバイスがリンク アップ イベントまたはリンク ダウン イベントでデバイスの有無を確認した場合は、スイッチは、MAC アドレス、IP アドレス、およびユーザ名のようなクライアント固

有情報を取得します。クライアントが LLDP-MED または CDP に対応している場合は、デバイスは LLDP-MED ロケーション TLV または CDP でシリアル番号および UDI を取得します。

デバイス機能に応じて、デバイスは次のクライアント情報をリンク アップ時に取得します。

- ポート接続で指定されたスロットおよびポート。
- クライアント MAC アドレスで指定された MAC アドレス。
- ポート接続で指定された IP アドレス。
- 802.1X ユーザ名（該当する場合）。
- デバイス カテゴリは、*wired station* として指定されます。
- ステートは *new* として指定されます。
- シリアル番号、UDI。
- モデル番号
- デバイスによる関連付け検出後の時間（秒）

デバイス機能に応じて、デバイスは次のクライアント情報をリンク ダウン時に取得します。

- 切断されたスロットおよびポート。
- MAC アドレス
- IP アドレス
- 802.1X ユーザ名（該当する場合）。
- デバイス カテゴリは、*wired station* として指定されます。
- ステートは *delete* として指定されます
- シリアル番号、UDI。
- デバイスによる関連付け解除検出後の時間（秒）

デバイスがシャットダウンする場合は、スイッチは、MSE との NMSP 接続を終了する前に、ステートの *delete* および IP アドレスとともに接続情報通知を送信します。MSE は、この通知を、デバイスに関連付けられているすべてのワイヤードクライアントに対する関連付け解除として解釈します。

デバイス上のロケーションアドレスを変更すると、デバイスは、影響を受けるポートを識別する NMSP ロケーション通知メッセージ、および変更されたアドレス情報を送信します。

デフォルトの LLDP 設定

表 *7:* デフォルトの *LLDP* 設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	ディセーブル（すべての TLV との送受信）
LLDP インターフェイス ステート	ディセーブル
LLDP 受信	ディセーブル
LLDP 転送	ディセーブル
LLDP med-tlv-select	ディセーブル（すべての LLDP-MED TLV への送信）。LLDP がグローバルにイネーブルにされると、LLDP-MED-TLV もイネーブルになります。

LLDP に関する制約事項

- インターフェイスがトンネル ポートに設定されていると、LLDP は自動的にディセーブルになります。
- 最初にインターフェイス上にネットワークポリシー プロファイルを設定した場合、インターフェイス上に **switchport voice vlan** コマンドを適用できません。**switchport voice vlan** *vlan-id* がすでに設定されているインターフェイスには、ネットワーク ポリシー プロファイルを適用できます。このように、そのインターフェイスには、音声または音声シグナリング VLAN ネットワーク ポリシー プロファイルが適用されます。
- ネットワーク ポリシープロファイルを持つインターフェイス上では、スタティック セキュア MAC アドレスを設定できません。

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定方法

LLDP のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lldp run** 例： `Device (config)# lldp run`	デバイスでLLDPをグローバルにイネーブルにします。
ステップ 4	**interface** *interface-id* 例： `Device (config)# interface gigabitethernet2/0/1`	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**lldp transmit** 例： `Device(config-if)# lldp transmit`	LLDP パケットを送信するようにインターフェイスをイネーブルにします。
ステップ 6	**lldp receive** 例： `Device(config-if)# lldp receive`	LLDP パケットを受信するようにインターフェイスをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show lldp** 例： `Device# show lldp`	設定を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

LLDP 特性の設定

LLDP 更新の頻度、情報を廃棄するまでの保持期間、および初期化遅延時間を設定できます。送受信する LLDP および LLDP-MED TLV も選択できます。

（注） ステップ 2 ～ 5 は任意であり、どの順番で実行してもかまいません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**lldp holdtime** *seconds* 例： `Device(config)# lldp holdtime 120`	（任意）デバイスから送信された情報を受信側デバイスが廃棄するまで保持する必要がある期間を指定します。 指定できる範囲は 0 ～ 65535 秒です。デフォルトは 120 秒です。
ステップ 4	**lldp reinit** *delay* 例： `Device(config)# lldp reinit 2`	（任意）任意のインターフェイス上で LLDP の初期化の遅延時間（秒）を指定します。 指定できる範囲は 2 ～ 5 秒です。デフォルトは 2 秒です。
ステップ 5	**lldp timer** *rate* 例： `Device(config)# lldp timer 30`	（任意）インターフェイス上で LLDP の更新の遅延時間（秒）を指定します。 指定できる範囲は 5 ～ 65534 秒です。デフォルトは 30 秒です。
ステップ 6	**lldp tlv-select** 例： `Device(config)# tlv-select`	（任意）送受信する LLDP TLV を指定します。
ステップ 7	**interface** *interface-id* 例： `Device (config)# interface gigabitethernet2/0/1`	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**lldp med-tlv-select** 例： `Device (config-if)# lldp med-tlv-select inventory management`	（任意）送受信する LLDP-MED TLV を指定します。
ステップ 9	**end** 例： `Device (config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show lldp** 例： `Device# show lldp`	設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

LLDP-MED TLV の設定

デフォルトでは、デバイスはエンドデバイスからLLDP-MEDパケットを受信するまで、LLDPパケットだけを送信します。スイッチは、MED TLV を持つ LLDP も送信します。LLDP-MEDエントリが期限切れになった場合は、スイッチは再び LLDP パケットだけを送信します。

lldp インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスが次の表にリストされている TLV を送信しないように設定できます。

表 8 : LLDP-MED TLV

LLDP-MED TLV	説明
inventory-management	LLDP-MED インベントリ管理 TLV
場所	LLDP-MED ロケーション TLV
network-policy	LLDP-MED ネットワーク ポリシー TLV
power-management	LLDP-MED 電源管理 TLV

インターフェイスで TLV をイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device (config)# interface gigabitethernet2/0/1`	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lldp med-tlv-select** 例： `Device(config-if)# lldp med-tlv-select inventory management`	イネーブルにする TLV を指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Network-Policy TLV の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**network-policy profile** *profile number* 例： `Device(config)# network-policy profile 1`	ネットワーク ポリシー プロファイル番号を指定し、ネットワーク ポリシー コンフィギュレーション モードを開始します。指定できる範囲は 1 ～ 4294967295 です。
ステップ 4	{**voice** | **voice-signaling**} **vlan** [*vlan-id* {**cos** *cvalue* | **dscp** *dvalue*}] | [[**dot1p** {**cos** *cvalue* | **dscp** *dvalue*}] | **none** | **untagged**] 例： `Device(config-network-policy)# voice vlan 100 cos 4`	ポリシー属性の設定： • **voice**：音声アプリケーション タイプを指定します。 • **voice-signaling**：音声シグナリング アプリケーション タイプを指定します。 • **vlan**：音声トラフィックのネイティブ VLAN を指定します。 • *vlan-id*：（任意）音声トラフィックの VLAN を指定します。指定できる範囲は 1 ～ 4094 です。 • **cos** *cvalue*：（任意）設定された VLAN に対するレイヤ 2 プライオリティ サービス クラス（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。 • **dscp** *dvalue*：（任意）設定された VLAN に対する DiffServ コード ポイント（DSCP）値を指定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 46 です。 • **dot1p**：（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話を設定します。

	コマンドまたはアクション	目的
		• **none**：（任意）音声 VLAN に関して IP Phone に指示しません。IP Phone のキー パッドから入力された設定を使用します。 • **untagged**：（任意）IP Phone を、タグなしの音声トラフィックを送信するよう設定します。これが IP Phone のデフォルト設定になります。 • **untagged**：（任意）IP Phone を、タグなしの音声トラフィックを送信するよう設定します。これが IP Phone のデフォルト設定になります。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *interface-id* 例： `Device (config)# interface gigabitethernet2/0/1`	ネットワーク ポリシープロファイルを設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**network-policy** *profile number* 例： `Device(config-if)# network-policy 1`	ネットワーク ポリシープロファイル番号を指定します。
ステップ 8	**lldp med-tlv-select network-policy** 例： `Device(config-if)# lldp med-tlv-select network-policy`	ネットワーク ポリシー TLV を指定します。
ステップ 9	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 10	**show network-policy profile** 例： `Device# show network-policy profile`	設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ロケーション TLV およびワイヤード ロケーション サービスの設定

エンドポイントのロケーション情報を設定し、その設定をインターフェイスに適用するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**location** {**admin-tag** *string* | **civic-location identifier** {*id* | **host**} | **elin-location** *string* **identifier** *id* | **custom-location identifier** {*id* | **host**} | **geo-location identifier** {*id* | **host**}}
	例：
	`Device(config)# location civic-location identifier 1`
	`Device(config-civic)# number 3550`
	`Device(config-civic)# primary-road-name "Cisco Way"`
	`Device(config-civic)# city "San Jose"`
	`Device(config-civic)# state CA`
	`Device(config-civic)# building 19`
		エンドポイントにロケーション情報を指定します。
		• **admin-tag**：管理タグまたはサイト情報を指定します。
		• **civic-location**：都市ロケーション情報を指定します。
		• **elin-location**：緊急ロケーション情報（ELIN）を指定します。
		• **custom-location**：カスタム ロケーション情報を指定します。
		• **geo-location**：地理空間的なロケーション情報を指定します。

	コマンドまたはアクション	目的

	`Device(config-civic)# room C6`
	`Device(config-civic)# county "Santa Clara"`
	`Device(config-civic)# country US`
		• **identifier** *id*：都市、ELIN、カスタム、または地理ロケーションの ID を指定します。
		• **host**：ホストの都市、カスタム、または地理ロケーションを指定します。
		• *string*：サイト情報またはロケーション情報を英数字形式で指定します。

ステップ 3	**exit** 例： `Device(config-civic)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**interface** *interface-id* 例： `Device (config)# interface gigabitethernet2/0/1`	ロケーション情報を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**location** {**additional-location-information** *word* | **civic-location-id** {*id* | **host**} | **elin-location-id** *id* | **custom-location-id** {*id* | **host**} | **geo-location-id** {*id* | **host**} } 例： `Device(config-if)# location elin-location-id 1`	インターフェイスのロケーション情報を入力します。 • **additional-location-information**：ロケーションまたは場所に関する追加情報を指定します。 • **civic-location-id**：インターフェイスにグローバル都市ロケーション情報を指定します。 • **elin-location-id**：インターフェイスに緊急ロケーション情報を指定します。 • **custom-location-id**：インターフェイスにカスタム ロケーション情報を指定します。 • **geo-location-id**：インターフェイスの地理空間のロケーション情報を指定します。

	コマンドまたはアクション	目的
		• **host**：ホストのロケーションの ID を指定します。 • *word*：追加のロケーション情報を指定する語またはフレーズを指定します。 • *id*：都市、ELIN、カスタム、または地理ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

ステップ 7	次のいずれかを使用します。
	• **show location admin-tag** *string*
	• **show location civic-location identifier** *id*
	• **show location elin-location identifier** *id*
	例：
	`Device# show location admin-tag`
	または
	`Device# show location civic-location identifier`
	または
	`Device# show location elin-location identifier`
		設定を確認します。

ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

デバイス上でのワイヤード ロケーション サービスのイネーブル化

始める前に

ワイヤード ロケーションが機能するためには、まず、**ip device tracking** グローバル コンフィギュレーション コマンドを入力する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**nmsp notification interval** {**attachment** | **location**} *interval-seconds* 例： `Device(config)# nmsp notification interval location 10`	NMSP 通知間隔を指定します。 **attachment**：接続通知間隔を指定します。 **location**：ロケーション通知間隔を指定します。 *interval-seconds*：デバイスから MSE にロケーション更新または接続更新が送信されるまでの期間（秒）。指定できる範囲は 1 ～ 30 です。デフォルト値は 30 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show network-policy profile** 例： `Device# show network-policy profile`	設定を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定例

Network-Policy TLV の設定：例

次に、CoS を持つ音声アプリケーションの VLAN 100 を設定して、インターフェイス上のネットワーク ポリシー プロファイルおよびネットワーク ポリシー TLV をイネーブルにする例を示します。

```
# configure terminal
(config)# network-policy 1
(config-network-policy)# voice vlan 100 cos 4
(config-network-policy)# exit
(config)# interface gigabitethernet1/0/1
(config-if)# network-policy profile 1
(config-if)# lldp med-tlv-select network-policy
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
config-network-policy)# voice vlan dot1p cos 4
config-network-policy)# voice vlan dot1p dscp 34
```

LLDP、LLDP-MED、ワイヤード ロケーション サービスのモニタリングとメンテナンス

以下は、LLDP、LLDP-MED、ワイヤードロケーションサービスのモニタリングとメンテナンスのコマンドです。

コマンド	説明
clear lldp counters	トラフィック カウンタを0にリセットします。

コマンド	説明
clear lldp table	LLDP ネイバー情報テーブルを削除します。
clear nmsp statistics	NMSP 統計カウンタをクリアします。
show lldp	送信頻度、送信するパケットのホールドタイム、LLDP 初期化の遅延時間のような、インターフェイス上のグローバル情報を表示します。
show lldp entry *entry-name*	特定のネイバーに関する情報を表示します。 アスタリスク（*）を入力すると、すべてのネイバーの表示、またはネイバーの名前の入力が可能です。
show lldp interface [*interface-id*]	LLDPがイネーブルに設定されているインターフェイスに関する情報を表示します。 表示対象を特定のインターフェイスに限定できます。
show lldp neighbors [*interface-id*] [**detail**]	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、ポート ID など、ネイバーに関する情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show lldp traffic	送受信パケットの数、廃棄したパケットの数、認識できない TLV の数など、LLDP カウンタを表示します。
show location admin-tag *string*	指定した管理タグまたはサイトのロケーション情報を表示します。
show location civic-location identifier *id*	特定のグローバル都市ロケーションのロケーション情報を表示します。
show location elin-location identifier *id*	緊急ロケーションのロケーション情報を表示します。
show network-policy profile	設定されたネットワークポリシー プロファイルを表示します。
show nmsp	NMSP 情報を表示します。

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの追加情報

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

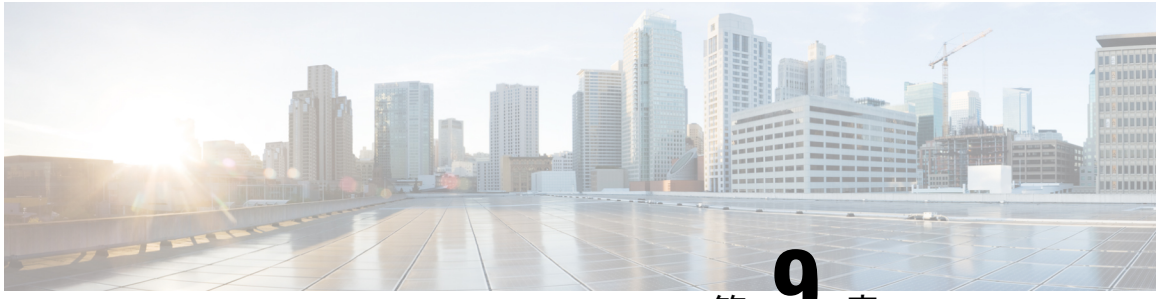
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。



第 9 章

システム MTU の設定

- 機能情報の確認 （175 ページ）
- MTU に関する情報 （176 ページ）
- MTU サイズの設定方法 （177 ページ）
- システム MTU の設定例 （179 ページ）
- システム MTU の設定例 （179 ページ）
- システム MTU に関する追加情報 （179 ページ）
- システム MTU の機能情報 （180 ページ）
- 機能情報の確認 （180 ページ）
- MTU に関する情報 （180 ページ）
- MTU サイズの設定方法 （181 ページ）
- システム MTU の設定例 （184 ページ）
- システム MTU の設定例 （184 ページ）
- システム MTU に関する追加情報 （184 ページ）
- システム MTU の機能情報 （185 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

MTU に関する情報

すべてのデバイス インターフェイスで送受信されるフレームのデフォルト MTU サイズは、1500 バイトです。

システム MTU の制約事項

システム MTU 値を設定する場合、次の注意事項に留意してください。

- デバイスはインターフェイス単位では MTU をサポートしていません。
- **system mtu** *bytes* グローバル コンフィギュレーション コマンドを入力すると、デバイス でコマンドが有効になりません。このコマンドが有効になるのは、ファスト イーサネット ポートにおけるシステム MTU サイズに対してだけです。

システム MTU 値の適用

スイッチ スタックでは、スイッチ メンバーに適用される MTU 値は、スタックの設定によって異なります。次のスタック設定がサポートされます。

次の表では、MTU 値の適用方法を示します。

表 *9 : MTU* の値

設定（Configuration）	system mtu コマンド	ip mtu コマンド	ipv6 mtu コマンド
スタンドアロン スイッチまたはスイッチ スタック	スイッチまたはスイッチ スタックで **system mtu** コマンドを入力できますが、システム MTU 値は有効になりません。 指定できる範囲は 1500 ～ 9198 バイトです。	**ip mtu** *bytes* コマンドを使用します。 範囲は 832 ～ 1500 バイトです。 （注） IP MTU 値は、適用可能な値ですが、設定できません。	**ipv6 mtu** *bytes* コマンドを使用します。 指定できる範囲は 1280 からシステム ジャンボ MTU 値（バイト単位）までです。 （注） IPv6 MTU 値は、適用可能な値ですが、設定できません。

IP または IPv6 MTU 値の上限は、スイッチスイッチ スタックの設定に基づいており、現在適用されているシステム MTU 値または 値を参照しています。MTU サイズの設定については、このリリースのコマンド リファレンスの **system mtu** グローバル コンフィギュレーション コマンドを参照してください。

MTU サイズの設定方法

システム MTU の設定

スイッチドおよびルーテッド パケットの MTU サイズを変更するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**system mtu** *bytes* 例： `Device(config)# system mtu 1900`	（任意）すべてのギガビットイーサネットおよび10ギガビットイーサネットインターフェイスのMTUサイズを変更します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copyrunning-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。
ステップ 6	**reload** 例： `Device# reload`	オペレーティング システムをリロードします。
ステップ 7	**show system mtu** 例： `Device# show system mtu`	設定を確認します。

Protocol-Specific MTU の設定

ルーテッド パケットの最大伝送単位（MTU）サイズを変更するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface* 例： `Device(config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip mtu** *bytes* 例： `Device(config-if)# ip mtu 68`	IPv4 MTU サイズを変更します。
ステップ 4	**ipv6 mtu** *bytes* 例： `Device(config-if)# ipv6 mtu 1280`	（任意）IPv6 MTU サイズを設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copyrunning-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。
ステップ 7	**reload** 例： `Device# reload`	オペレーティング システムをリロードします。
ステップ 8	**show system mtu** 例： `Device# show system mtu`	設定を確認します。

システム MTU の設定例

システム MTU の設定例

例：プロトコル固有 MTU の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/0
Switch(config-if)# ip mtu 900
Switch(config-if)# ipv6 mtu 1286
Switch(config-if)# end
```

例：システム MTU の設定

```
Switch# configure terminal
Switch(config)# system mtu 1600
Switch(config)# exit
```

システム MTU に関する追加情報

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

システム MTU の機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

MTU に関する情報

すべてのデバイス インターフェイスで送受信されるフレームのデフォルト MTU サイズは、1500 バイトです。

システム MTU の制約事項

システム MTU 値を設定する場合、次の注意事項に留意してください。

- デバイスはインターフェイス単位では MTU をサポートしていません。
- **system mtu** *bytes* グローバル コンフィギュレーション コマンドを入力すると、デバイス でコマンドが有効になりません。このコマンドが有効になるのは、ファスト イーサネット ポートにおけるシステム MTU サイズに対してだけです。

システム MTU 値の適用

スイッチ スタックでは、スイッチ メンバーに適用される MTU 値は、スタックの設定によって異なります。次のスタック設定がサポートされます。

次の表では、MTU 値の適用方法を示します。

表 *10 : MTU* の値

設定（Configuration）	system mtu コマンド	ip mtu コマンド	ipv6 mtu コマンド
スタンドアロン スイッチまたは スイッチ スタック	スイッチまたはスイッチ スタックで **system mtu** コマンドを入力できますが、システム MTU 値は有効になりません。 指定できる範囲は 1500 ～ 9198 バイトです。	**ip mtu** *bytes* コマンドを使用します。 範囲は 832 ～ 1500 バイトです。 （注） IP MTU 値は、適用可能な値ですが、設定できません。	**ipv6 mtu** *bytes* コマンドを使用します。 指定できる範囲は 1280 からシステム ジャンボ MTU 値（バイト単位）までです。 （注） IPv6 MTU 値は、適用可能な値ですが、設定できません。

IP または IPv6 MTU 値の上限は、スイッチスイッチ スタックの設定に基づいており、現在適用されているシステム MTU 値または 値を参照しています。MTU サイズの設定については、このリリースのコマンド リファレンスの **system mtu** グローバル コンフィギュレーション コマンドを参照してください。

MTU サイズの設定方法

システム MTU の設定

スイッチドおよびルーテッド パケットの MTU サイズを変更するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**system mtu** *bytes* 例： `Device(config)# system mtu 1900`	（任意）すべてのギガビットイーサネットおよび10ギガビットイーサネットインターフェイスのMTUサイズを変更します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copyrunning-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。
ステップ 6	**reload** 例： `Device# reload`	オペレーティング システムをリロードします。
ステップ 7	**show system mtu** 例： `Device# show system mtu`	設定を確認します。

Protocol-Specific MTU の設定

ルーテッド パケットの最大伝送単位（MTU）サイズを変更するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface* 例： `Device(config)# interface gigabitethernet0/0`	インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	**ip mtu** *bytes* 例： `Device(config-if)# ip mtu 68`	IPv4 MTU サイズを変更します。
ステップ 4	**ipv6 mtu** *bytes* 例： `Device(config-if)# ipv6 mtu 1280`	（任意）IPv6 MTU サイズを設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copyrunning-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。
ステップ 7	**reload** 例： `Device# reload`	オペレーティング システムをリロードします。
ステップ 8	**show system mtu** 例： `Device# show system mtu`	設定を確認します。

システム MTU の設定例

システム MTU の設定例

例：プロトコル固有 MTU の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/0
Switch(config-if)# ip mtu 900
Switch(config-if)# ipv6 mtu 1286
Switch(config-if)# end
```

例：システム MTU の設定

```
Switch# configure terminal
Switch(config)# system mtu 1600
Switch(config)# exit
```

システム MTU に関する追加情報

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

システム MTU の機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 10 章

内部電源装置の設定

- 内部電源装置に関する情報 （187 ページ）
- 内部電源装置の設定方法 （187 ページ）
- 内部電源装置のモニタ （188 ページ）
- 内部電源装置の設定例 （188 ページ）
- その他の参考資料 （189 ページ）
- 内部電源装置の機能履歴と情報 （190 ページ）

内部電源装置に関する情報

電源装置に関する情報については、デバイスのインストレーション ガイドを参照してください。

内部電源装置の設定方法

内部電源装置の設定

power supply EXEC コマンドを使用すると、デバイスの内部電源装置の設定および管理ができます。デバイスは、**no power supply** EXEC コマンドをサポートしていません。

ユーザ EXEC モードで開始し、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**power supply** *switch_number* **slot**{**A** | **B**}{**off** | **on**} 例： `Device# power supply 1 slot A on`	次のいずれかのキーワードを使用して、指定した電源装置を **off** または **on** に設定します。 • **A**：スロット A の電源を選択します。

	コマンドまたはアクション	目的
		• **B**：スロットBの電源装置を選択します。 （注） 電源装置のスロット B は、デバイスの外側エッジに近いほうです。 • **off**：電源装置をオフに設定します。 • **on**：電源装置をオンに設定します。 デフォルトでは、デバイスの電源装置は **on** です。
ステップ **2**	**show environment power** 例： `Device# show environment power`	設定を確認します。

内部電源装置のモニタ

表 *11 :* 電源装置の *show* コマンド

コマンド	目的
show environment power [**all** | **switch***switch_number*]	（任意）スタック内の各デバイスまたは指定したデバイスの内部電源装置のステータスを表示します。指定できる範囲は、スタック内のデバイス メンバ番号に従って 1 ～ 9 です。 デバイス キーワードは、スタック対応デバイス上でだけ使用できます。

内部電源装置の設定例

次に、スロット A の電源装置をオフに設定する例を示します。

```
Device# power supply 1 slot A off
Disabling Power supply A may result in a power loss to PoE devices and/or switches ...
Continue? (yes/[no]): yes
Device#
Jun 10 04:52:54.389: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered off
Jun 10 04:52:56.717: %PLATFORM_ENV-1-FAN_NOT_PRESENT: Fan is not present
Device#
```

次に、スロット A の電源装置をオンに設定する例を示します。

```
Device# power supply 1 slot A on
Jun 10 04:54:39.600: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered on
```

次に、**show env power** コマンドの出力例を示します。

```
Device# show env power

SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--- ------------------  ----------  ---------------  -------  -------  -----
1A  PWR-C1-715WAC       LIT161010UE  OK              Good     Good     715
1B  Not Present

Device#
```

表 *12 : show env power* ステータスの説明

フィールド	説明
OK	電源装置が存在し、電力が良好です。
Not Present	電源装置が未搭載です。
No Input Power	電源装置は存在しますが、入力電力が供給されていません。
Disabled	電源装置が存在し、入力電力は供給されていますが、電源装置が CLI によってオフになっています。
Not Responding	電源装置が認識されていないか、障害が発生しています。
Failure-Fan	電源装置のファンに障害が発生しています。

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

内部電源装置の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。
Cisco IOS XE 3.3SE	**slot** キーワードが **frufep** キーワードに代わるものとして使用されるようになりました。

第 11 章

PoE の設定

- 機能情報の確認 （191 ページ）
- PoE について （191 ページ）
- PoE の設定方法 （198 ページ）
- 電力ステータスのモニタ （203 ページ）
- その他の参考資料 （204 ページ）
- PoE の機能情報 （204 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

PoE について

Power over Ethernet（PoE）ポート

Power over Ethernet（PoE）対応デバイス ポートでは、回路に電力が供給されていないことをスイッチが検出した場合、接続している次のデバイスに電力が自動的に供給されます。

- シスコ先行標準受電デバイス（Cisco IP Phone や Cisco Aironet アクセス ポイントなど）
- IEEE 802.3af 準拠の受電装置

受電デバイスが PoE スイッチ ポートおよび AC 電源に接続されている場合、冗長電力として利用できます。受電装置が PoE ポートにだけ接続されている場合、受電装置には冗長電力は供給されません。

サポート対象のプロトコルおよび標準

デバイスは PoE のサポートで次のプロトコルと規格を使用します。

- 電力消費について CDP を使用：受電装置は、消費している電力量をデバイスに通知します。デバイスはこの電力消費に関するメッセージに応答しません。デバイスは、PoE ポートに電力を供給するか、このポートへの電力を取り除くだけです。
- シスコ インテリジェント電力管理：受電装置およびデバイスは、電力ネゴシエーション CDP メッセージによって電力消費レベルについてネゴシエーションを行います。このネゴシエーションにより、7 W より多くを消費する高電力のシスコ受電デバイスは、最も高い電力モードで動作できるようになります。受電デバイスは、最初に低電力モードでブートして 7 W 未満の電力を消費し、ネゴシエーションを行って高電力モードで動作するための十分な電力を取得します。受電装置が高電力モードに切り替わるのは、デバイスから確認を受信した場合に限られます。

  高電力装置は、電力ネゴシエーション CDP をサポートしないデバイスで低電力モードで動作できます。

  シスコのインテリジェントな電力管理の機能には、電力消費に関して CDP との下位互換性があるため、デバイスは、受信する CDP メッセージに従って応答します。CDP はサードパーティの受電デバイスをサポートしません。このため、デバイスは IEEE 分類を使用して装置の消費電力を判断します。
- IEEE 802.3a：この規格の主な機能は、受電装置の検出、電力の管理、切断の検出です。オプションとして受電装置の電力分類があります。詳細については、この規格を参照してください。
- Cisco UPoE 機能は、CDP や LLDP などのレイヤ 2 電力ネゴシエーション プロトコルを使用して、シグナル ペアおよび RJ-45 イーサネット ケーブルのスペア ペアの両方に、最大 60 W の電力（2 X 30 W）を供給します。4 線式 Cisco 独自開発スペ アペア電力 TLV での 30 W 以上の LLDP および CDP 要求により、スペア ペアに電力を供給できます。

関連トピック

Cisco Universal Power Over Ethernet （197 ページ）

受電装置の検出および初期電力割り当て

デバイスは、PoE 対応ポートがシャットダウンの状態でなく、PoE はイネーブルになっていて（デフォルト）、接続した装置は AC アダプタから電力供給されていない場合、シスコの先行標準受電装置または IEEE 準拠の受電装置を検出します。

装置の検出後、デバイスは、次のように装置のタイプに応じて電力要件を判断します。

- 初期電力割り当ては、受電デバイスが要求する最大電力量です。デバイスは、受電装置を検出および電力供給する場合、この電力を最初に割り当てます。デバイスが受電装置から

CDP メッセージを受信し、受電装置が CDP 電力ネゴシエーション メッセージを通じてデバイスと電力レベルをネゴシエートしたときに、初期電力割り当てが調整される場合があります。

- デバイスは検出した IEEE 装置を消費電力クラス内で分類します。デバイスは、電力バジェットに使用可能な電力量に基づいて、ポートに通電できるかどうかを決定します。表 13 : IEEE 電力分類 （193 ページ） に、各種レベルの一覧を示します。

表 *13 : IEEE* 電力分類

クラス	デバイスから要求される最大電力レベル
0（クラス ステータスは不明）	15.4 W
1	4 W
2	7 W
3	15.4 W
4	30 W（IEEE 802.3at タイプ 2 準拠の受電デバイスの場合）

デバイスは電力要求をモニタリングおよび追跡して必要な場合にだけ電力供給を許可します。デバイスは自身の電力バジェット（PoE のデバイスで使用可能な電力量）を追跡します。電力の供給許可または拒否がポートで行われると、デバイスはパワーアカウンティング計算を実行し、電力バジェットを最新に保ちます。

電力がポートに適用されたあとで、デバイスは CDP を使用して、接続されたシスコ受電装置の *CDP* 固有の電力消費要件を調べます。この要件は、CDP メッセージに基づいて割り当てられる電力量です。これに従って、デバイスは電力バジェットを調整します。これは、サードパーティの PoE 装置には適用されません。デバイスは要件を処理して電力の供給を許可または拒否します。要求が許可されると、デバイスは電力バジェットを更新します。要求が拒否された場合は、デバイスはポートの電力がオフに切り替わっていることを確認し、syslog メッセージを生成して LED を更新します。受電装置はより多くの電力について、デバイスとのネゴシエーションを行うこともできます。

PoE+ では、受電装置が最大 30 W の電力ネゴシエーションのために、Media Dependent Interface（MDI）の Type, Length, and Value description（TLV）、Power-via-MDI TLV で IEEE 802.3at および LLDP 電源を使用します。シスコの先行標準受電装置および IEEE 受電装置では、CDP または IEEE 802.3at power-via-MDI 電力ネゴシエーション メカニズムにより最大 30 W の電力レベルを要求できます。

（注） クラス 0、クラス 3、およびクラス 4 の受電装置の初期割り当ては 15.4 W です。装置が起動し、CDP または LLDP を使用して 15.4 W を超える要求を送信する場合、最大 30 W を割り当てることができます。

（注） ソフトウェア コンフィギュレーション ガイドおよびコマンド リファレンスでは、CDP 固有の電力消費要件を実際電力消費要件と呼んでいます。

不足電圧、過電圧、オシレータ障害、または短絡状態による障害をデバイスが検出した場合、ポートへの電源をオフにし、syslog メッセージを生成し、電力バジェットと LED を更新します。

PoE 機能は、デバイスがスタック メンバーであるかどうかに関係なく、同じように動作します。電力バジェットはデバイスごとであり、スタックの他のデバイスとは無関係です。新しいアクティブ デバイスの選択は、PoE の動作に影響を与えません。アクティブ デバイスは、スタック内のすべてのデバイスおよびポートの PoE のステータスを追跡し続け、出力表示にそのステータスを含めます。

スタック可能なデバイスでは、StackPower もサポートされます。これによって、電源スタックケーブルでデバイスを接続する場合、スタック内の複数のシステムの電源モジュールで負荷を分担できます。最大 4 つのスタック メンバーの電源モジュールを 1 つの大規模な電源モジュールとして管理できます。

電力管理モード

デバイスでは、次の PoE モードがサポートされます。

- **auto**：接続されている装置で電力が必要であるかどうか、デバイスが自動的に検出します。ポートに接続されている受電装置をデバイスが検出し、デバイスに十分な電力がある場合、スイッチは電力を供給して電力バジェットを更新し、先着順でポートの電力をオンに切り替えて LED を更新します。LED の詳細については、ハードウェア インストレーション ガイドを参照してください。

  すべての受電装置用としてデバイスに十分な電力がある場合は、すべての受電装置が起動します。デバイスに接続された受電装置すべてに対し十分な電力が利用できる場合、すべての装置に電力を供給します。使用可能な PoE がない場合、または他の装置が電力供給を待機している間に装置の接続が切断されて再接続した場合、どの装置へ電力を供給または拒否されるかが判断できなくなります。

  許可された電力がシステムの電力バジェットを超えている場合、デバイスは電力を拒否し、ポートへの電力がオフになっていることを確認したうえで syslog メッセージを生成し、LED を更新します。電力供給が拒否された後、デバイスは定期的に電力バジェットを再確認し、継続して電力要求の許可を試みます。

  デバイスにより電力を供給されている装置が、さらに壁面コンセントに接続している場合、デバイスは装置に電力を供給し続ける場合があります。このとき、装置がデバイスから受電しているか、AC 電源から受電しているかにかかわらず、デバイスは引き続き装置へ電力を供給していることを報告し続ける場合があります。

  受電装置が取り外された場合、デバイスは切断を自動的に検出し、ポートから電力を取り除きます。非受電装置を接続しても、その装置に障害は発生しません。

ポートで許可される最大ワット数を指定できます。受電装置の IEEE クラス最大ワット数が設定されている最大値より大きい場合、デバイスはそのポートに電力を供給しません。デバイスが受電装置に電力供給したが、受電装置が設定の最大値より多くの電力を CDP メッセージによって後で要求した場合、デバイスはポートの電力を取り除きます。その受電デバイスに割り当てられていた電力は、グローバル電力バジェットに送られます。ワット数を指定しない場合、デバイスは最大値の電力を供給します。任意の PoE ポートで **auto** 設定を使用してください。auto モードがデフォルト設定です。

- **static**：デバイスは、受電装置が接続されていなくてもポートに電力をあらかじめ割り当て、そのポートで電力が使用できるようにします。デバイスは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電装置からの CDP メッセージによって調節されることはありません。これは、電力があらかじめ割り当てられていることから、最大ワット数以下の電力を使用するすべての受電デバイスが固定ポートに接続されている場合に電力が保証されるためです。ポートはもう先着順方式ではなくなります。

  ただし、受電装置の IEEE クラスが最大ワット数を超えると、デバイスは装置に電力を供給しません。受電装置が最大ワット数を超える電力を消費していることを CDP メッセージによってデバイスが認識すると、デバイスは受電装置をシャットダウンします。

  ワット数を指定しない場合、デバイスは最大値をあらかじめ割り当てます。デバイスは、受電装置を検出した場合に限り、ポートに電力を供給します。優先順位が高いインターフェイスには、**static** 設定を使用してください。

- **never**：デバイスは受電装置の検出をディセーブルにして、電力が供給されていない装置が接続されても、PoE ポートに電力を供給しません。PoE 対応ポートに電力を絶対に適用せず、そのポートをデータ専用ポートにする場合に限り、このモードを使用してください。

ほとんどの場合、デフォルトの設定（自動モード）の動作は適切に行われ、プラグアンドプレイ動作が提供されます。それ以上の設定は必要ありません。しかし、プライオリティの高い PoE ポートを設定したり、PoE ポートをデータ専用にしたり、最大ワット数を指定して高電力受電デバイスをポートで禁止したりする場合は、このタスクを実行します。

スタック対応デバイスでは、StackPower もサポートされます。これによって、電源スタックケーブルで最大4つのデバイスを接続する場合、スタック内の複数のシステムでデバイス電源モジュールで負荷を分担できます。

電力モニタリングおよび電力ポリシング

リアルタイムの消費電力のポリシングをイネーブルにした場合、受電装置が最大割り当て（カットオフ電力値）を超えて電力を消費すると、デバイスはアクションを開始します。

PoE がイネーブルである場合、デバイスは受電装置のリアルタイムの電力消費を検知します。接続されている受電装置のリアルタイム電力消費をデバイスが監視することを、電力モニタリングまたは電力検知といいます。また、デバイスはパワーポリシング機能を使用して消費電力をポリシングします。

電力モニタリングは、シスコのインテリジェントな電力管理および CDP ベースの消費電力に対して下位互換性があります。電力モニタリングはこれらの機能とともに動作して、PoE ポートが受電デバイスに電力を供給できるようにします。

デバイスは次のようにして、接続されている装置のリアルタイム電力消費を検知します。

1. デバイスは、個々のポートでリアルタイム消費電力をモニタリングします。
2. デバイスは、ピーク時の電力消費を含め、電力消費を記録します。デバイスは CISCO-POWER-ETHERNET-EXT-MIB を介して情報を報告します。
3. 電力ポリシングがイネーブルの場合、デバイスはリアルタイムの消費電力を装置に割り当てられた最大電力と比較して、消費電力をポリシングします。最大消費電力は、PoE ポートでカットオフ電力とも呼ばれます。

   装置がポートで最大電力割り当てを超える電力を使用すると、デバイスはポートへの電力をオフにしたり、またはデバイス コンフィギュレーションに基づいて受電装置に電力を供給しながらデバイスが syslog メッセージを生成して LED（ポート LED はオレンジ色で点滅）を更新したりすることができます。デフォルトでは、すべての PoE ポートで消費電力のポリシングはディセーブルになっています。

   PoE の errdisable ステートからのエラー回復がイネーブルの場合、指定の時間の経過後、デバイスは PoE ポートを errdisable ステートから自動的に回復させます。

   エラー回復がディセーブルの場合、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを使用して、手動で PoE ポートをイネーブルにできます。
4. ポリシングがディセーブルである場合、受電装置が PoE ポートに割り当てられた最大電力より多くの量を消費しても対処されないため、デバイスに悪影響を与える場合があります。

電力消費値

ポートの初期電力割り当ておよび最大電力割り当てを設定することができます。ただし、これらの値は、デバイスが PoE ポートの電力をオンまたはオフにするときを指定するために設定する値です。最大電力割り当ては、受電デバイスの実際の電力消費と同じではありません。デバイスによって電力ポリシングに使用される実際のカットオフ電力値は、設定済みの電力値と同等ではありません。

電力ポリシングがイネーブルの場合、デバイスは、スイッチ ポートで、受電装置の消費電力を超える消費電力ポリシングを行います。最大電力割り当てを手動で設定する場合、スイッチ ポートと受電デバイス間のケーブルでの電力損失を考慮する必要があります。カットオフ電力とは、受電デバイスの定格消費電力とケーブル上での最悪時の電力損失を合計したものです。

デバイスの PoE がイネーブルの場合、電力ポリシングをイネーブルにすることを推奨します。たとえば、ポリシングがディセーブルで、**power inline auto max6300** インターフェイス コンフィギュレーション コマンドを使用してカットオフ値を設定すると、PoE ポートに設定される最大電力割り当ては 6.3 W（6300 mW）です。装置が最大で 6.3 W の電力を必要とする場合、デバイスはポートに接続されている装置に電力を供給します。CDP によるパワー ネゴシエーション実施後の値または IEEE 分類値が設定済みカットオフ値を超えると、デバイスは接続されている装置に電力を供給しなくなります。デバイスが PoE ポートで電力をオンにしたあとは、デバイスは受電装置のリアルタイム電力消費のポリシングを行わないので、受電装置は最大割り当て量を超えて電力を消費できることになり、デバイスと、他の PoE ポートに接続されている受電装置に悪影響を及ぼすことがあります。

スタンドアロンデバイスでは内部電源装置がサポートされるため、受電装置が利用できる総電力量は電源装置の設定によって異なります。

- 電源装置を取り外して、低電力の新しい電源装置に交換すると、デバイスは受電装置に対して十分な電力を供給できなくなり、デバイスはautoモードでポート番号の降順に従ってPoEポートへの電力供給を拒否します。デバイスがこれでも十分な電力を利用できない場合、デバイスは、static モードでポート番号の降順に従って PoE ポートへの電力供給を拒否します。
- 新しい電源装置の電力が前の電源装置より大きく、デバイスが大電力を使用できる場合、デバイスは static モードでポート番号の昇順に従って PoE ポートへの電力供給を許可します。これでもまだ使用可能な電力がある場合、スイッチデバイスは、ポート番号の昇順に従って auto モードで PoE ポートへの電力供給を許可します。

スタック対応デバイスでは、StackPower もサポートされます。これによって、電源スタックケーブルでデバイスを接続する場合、スタック内の複数のシステムの電源モジュールで負荷を分担できます。最大4つのスタック メンバーの電源モジュールを1つの大規模な電源モジュールとしてまとめて管理できます。

Cisco Universal Power Over Ethernet

Cisco Universal Power Over Ethernet（Cisco UPOE）は、シグナル ペア（導線 1、2、3、6）付きの RJ-45 ケーブルのスペア ペア（導線 4、5、7、8）を使用して、IEEE 802.at PoE 標準を拡張するシスコ独自のテクノロジーで、標準のイーサネット ケーブル配線インフラストラクチャ（クラス D 以上）により最大 60 W の電力を供給する機能を提供します。スペア ペアの電力は、スイッチ ポートとエンドデバイスが Cisco UPOE 対応であることを CDP または LLDP を使用して相互に識別し、エンドデバイスがスペア ペアの電力のイネーブル化を要求したときにイネーブルになります。スペア ペアに給電されると、エンドデバイスは、CDP または LLDP を使用して、スイッチから最大 60 W の電力をネゴシエートできます。

エンド デバイスがシグナル ペアおよびスペア ペアの両方で PoE 対応であるが、Cisco UPOE に必要な CDP または LLDP の拡張をサポートしない場合、4 ペアの強制モード設定により自動的にスイッチ ポートからシグナル ペアおよびスペア ペアの両方の電力がイネーブルになります。

PoE の設定方法

PoE ポートの電力管理モードの設定

（注） PoE 設定を変更するとき、設定中のポートでは電力が低下します。新しい設定、その他の PoE ポートの状態、電力バジェットの状態により、そのポートの電力は再びアップしない場合があります。たとえば、ポート 1 が自動でオンの状態になっていて、そのポートを固定モードに設定するとします。デバイスはポート 1 から電力を取り除き、受電デバイスを検出してポートに電力を再び供給します。ポート 1 が自動でオンの状態になっていて、最大ワット数を 10 W に設定した場合、デバイスはポートから電力を取り除き、受電デバイスを再び検出します。デバイスは、受電デバイスがクラス 1、クラス 2、またはシスコ専用受電デバイスのいずれかの場合に、ポートに電力を再び供給します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**power inline** {**auto** [**max** *max-wattage*] | **never** | **static** [**max** *max-wattage*]} 例： `Device(config-if)# power inline auto`	ポートの PoE モードを設定します。キーワードの意味は次のとおりです。 • **auto**：受電装置の検出をイネーブルにします。十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。これがデフォルト設定です。 • **max** *max-wattage*：ポートで許可されている電力を制限します。値を指

	コマンドまたはアクション	目的
		定しない場合は、最大電力が供給されます。 • **max** *max-wattage*：ポートで許可されている電力を制限します。Cisco UPoE ポートの範囲は 4000 ～ 60000 mW です。 値を指定しない場合は、最大電力が供給されます。 • **never**：装置の検出とポートへの電力供給をディセーブルにします。 （注） ポートにシスコの受電デバイスが接続されている場合は、**power inline never** コマンドでポートを設定しないでください。問題のあるリンクアップが発生し、ポートが errdisable ステートになることがあります。 • **static**：受電装置の検出をイネーブルにします。デバイスが受電デバイスを検出する前に、ポートへの電力を事前に割り当てます（確保します）。デバイスは、装置が接続されていなくてもこのポートに電力を予約し、装置の検出時に電力が供給されることを保証します。 デバイスは、自動モードに設定されたポートに電力を割り当てる前に、固定モードに設定されたポートに PoE を割り当てます。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show power inline** [*interface-id* | **module** *switch-number*] 例： `Device# show power inline`	デバイスまたはデバイス スタック、指定したインターフェイス、または指定したスタック メンバに関する PoE ステータスを表示します。

	コマンドまたはアクション	目的
		module*switch-number* キーワードは、スタッキング対応デバイスだけでサポートされます。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

シグナル/スペア ペアの電力のイネーブル化

（注） エンド デバイスがスペア ペアのインライン パワー給電に未対応の場合、またはエンド デバイスが Cisco UPoE に CDP または LLDP 拡張をサポートしている場合は、このコマンドを入力しないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**power inline four-pair forced** 例： `Device(config-if)# power inline four-pair forced`	スイッチ ポートから信号ペアおよびスペア ペアの両方の電力をイネーブルにします。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

電力ポリシングの設定

デフォルトでは、デバイスは接続されている受電装置の消費電力をリアルタイムでモニタリングします。消費電力に対するポリシングを行うようにデバイスを設定できます。デフォルトではポリシングはディセーブルです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**power inline police** [**action** {**log** | **errdisable**}] 例： `Device(config-if)# power inline police`	ポートでリアルタイム消費電力が最大電力割り当てを超えるときに、次のいずれかのアクションを実行するようにデバイスを設定します。 • **power inline police**：PoE ポートをシャット ダウンし、ポートへの電力供給をオフにし、PoE ポートを error-disabled ステートに移行します。

	コマンドまたはアクション	目的
		（注） **errdisable detect cause inline-power** グローバル コンフィギュレーション コマンドを使用すると、PoE errdisable の原因についてエラー検出をイネーブルにできます。**errdisable recovery cause inline-power interval** *interval* グローバル コンフィギュレーション コマンドを使用すると、PoE errdisable ステートから回復するためのタイマーをイネーブルにすることもできます。 • **power inline police action errdisable**：リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、ポートへの電力をオフにします。 • **power inline police action log**：ポートへの電源供給を継続し、syslog メッセージを生成します。 **action log** キーワードを入力しない場合、デフォルトのアクションによってポートがシャットダウンされ、errdisable ステートになります。
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	次のいずれかを使用します。 • **errdisable detect cause inline-power** • **errdisable recovery cause inline-power** • **errdisable recovery interval** 間隔 例： `Device(config)# errdisable detect cause inline-power`	（任意）PoE errdisable ステートからのエラー回復をイネーブルにし、PoE 回復メカニズム変数を設定します。 デフォルトでは、回復間隔は 300 秒です。 **interval** *interval* では、error-disabled ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。

	コマンドまたはアクション	目的

	`Device(config)# errdisable recovery cause inline-power`
	
	`Device(config)# errdisable recovery interval 100`	

ステップ 7	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

ステップ 8	次のいずれかを使用します。
	• **show power inline police**
	• **show errdisable recovery**
	例：
	`Device# show power inline police`
	
	`Device# show errdisable recovery`
		電力モニタリングステータスを表示し、エラー回復設定を確認します。

ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

電力ステータスのモニタ

表 *14*：電力ステータスの *show* コマンド

コマンド	目的
show env power switch [*switch-number*]	（任意）スタック内の各スイッチまたは指定したスイッチの内部電源装置のステータスを表示します。 指定できる範囲は、スタック内のスイッチ メンバ番号に従って 1 ～ 9 です。次のキーワードは、スタック対応スイッチ上でだけ使用できます。
show power inline [*interface-id* | **module** *switch-number*]	スイッチまたはスイッチスタック、インターフェイス、またはスタック内の特定のスイッチの PoE ステータスを表示します。
show power inline police	電力ポリシングのデータを表示します。

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

PoE の機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

リリース	変更内容
Cisco IOS XE 3.3SE	**four-pair forced** キーワードが追加されました。

第 12 章

Cisco eXpandable Power System（XPS）2200 の設定

このモジュールの構成は次のとおりです。

- XPS 2200 の設定に関する制約事項 （207 ページ）
- XPS 2200 の設定について （207 ページ）
- XPS 2200 を設定する方法 （212 ページ）
- XPS 2200 のモニタリングおよびメンテナンス （216 ページ）
- その他の参考資料 （216 ページ）

XPS 2200 の設定に関する制約事項

- スイッチ電源装置をバックアップするためにXPS電源装置をRPSモードで使用する場合、XPS の最小ワット数の電源装置は、RPS モードの XPS ポートに接続されているスイッチで最大ワット数の電源装置よりも、ワット数が大きい必要があります。
- RPS モードで各 XPS 電源装置がバックアップできるスイッチ電源装置は、そのサイズにかかわらず、1 台だけです。
- 電源スタックから（スイッチまたは XPS の）電源装置を取り外す場合は、取り外すことによって使用可能な電力が使い尽くされて、負荷制限が発生しないように注意する必要があります。

XPS 2200 の設定について

Cisco eXpandable Power System（XPS）2200 の概要

Cisco eXpandable Power System（XPS）2200 は、独立型電源システムで、Catalyst スイッチに接続できます。XPS 2200 は、接続されている装置で電源装置の故障が発生した場合、その装置にバックアップ電力を供給できます。また、Catalyst電源スタックでは、電源スタック バジェッ

トに追加の電力を供給できます。XPS 2200 の電源ポートと内部電源装置は、冗長電源（RPS）モードまたはスタック電源（SP）モードで動作できます。

スタック電源モードは、電源スタックに属するスタック対応スイッチでのみ使用されます。XPS が含まれていない場合、電源スタックはリンク トポロジで動作し、最大 4 台のスイッチで構成できます。2 つのスタックをマージする場合は、スイッチの合計数が 4 台を超えないようにしてください。XPS を電源スタックに追加すると、スタック内で最大 9 台のスイッチと XPS を接続し、スタック電源のリング トポロジ動作と同じような電力バジェットを電源スタックのメンバに提供できます。

SP ポートを経由して XPS に接続されたすべての Catalyst スイッチは同じ電源スタックに属し、XPS とスイッチから供給されるすべての電力はスタック内のすべてのスイッチで共有されます。電源共有がデフォルトのモードですが、XPS は、リング トポロジでサポートされているのと同じスタック電源モード（厳密または厳密でない電源共有モードと冗長モード）をサポートします。

電源装置が 2 台ある場合、1 台を RPS モードにし、もう 1 台を SP モードにするという混在モードで動作させることができます。ポートと電源装置は、XPS 2200 の使用目的に合わせて設定できます。

XPS 2000 には、RPS ロールまたは自動スタック電源（Auto-SP）ロール（デフォルト）で動作できる 9 個の電源ポートがあります。動作モードは、ポートに接続するスイッチの種類によって決まります。CLI を使用して、スタック可能なスイッチに適用するモードを強制的に RPS にすることもできます。

- LAN Base イメージを実行している Catalyst スイッチまたは Catalyst（スタック非対応）スイッチをポートに接続すると、ポートのモードは RPS になり、XPS 2200 は、スイッチの電源装置が停止した場合にバックアップとして機能します。
- IP Base または IP Services ライセンスを実行している Catalyst（スタック可能）スイッチをポートに接続すると、ポートのモードは SP になり、このスイッチはスタック電源システムの一部になることができます。

XPS は電源ポートに接続されている任意のスイッチで設定します。任意の XPS ポートを使用して設定でき、XPS に接続されている任意のスイッチから任意のポートを設定できます。複数のスイッチで XPS コンフィギュレーション コマンドを入力した場合、適用された最後の設定が有効になります。

すべての XPS 設定はスイッチで実行できますが、XPS 2200 では専用のソフトウェアが実行されています。このソフトウェアは、XPS サービス ポートを使用してアップグレードできます。

XPS 2200 電源モード

XPS には 2 台の電源装置があり、それぞれ RPS モードまたは SP モードで動作できます。

SP モードでは、XPS のすべての SP ポートは同じ電源スタックに属します。電源スタックに XPS を入れると、スタックのトポロジはスター トポロジになり、最大 9 台のメンバ スイッチと XPS 2200 で構成されます。SP モードの 1 台または 2 台の XPS 電源装置は、電力バジェットの計算で考慮されます。両方の XPS 電源装置が RPS モードの場合、電源スタックは、SP

モードの XPS ポートに接続されているスイッチだけで構成され、電力バジェットはそれらのスイッチの電源装置によって決まります。

電源装置のロールに不整合がある場合、たとえば、1 つの XSP ポートが RPS に設定されていて、電源装置が両方とも SP モードの場合、XPS はこの不整合を検出してエラー メッセージを送信します。

RPS モード

両方の XPS 電源装置を RPS モードにすると、XPS は、ワット数が等しいまたは小さいスイッチの電源装置について、2 台の電源装置の故障をバックアップできます。XPS で最小ワット数の電源装置は、RPS モードの XPS ポートに接続されているスイッチで最大ワット数の電源装置よりも、ワット数が大きい必要があります。

1 台の電源装置だけが RPS モードの場合、故障した電源装置のワット数がかなり小さい場合でも XPS がバックアップできるのは 1 台の電源装置だけです。たとえば、XPS 1100 W の電源装置が RPS モードで、2 台の 350 W のスイッチ電源装置が故障した場合、XPS がバックアップできるのは、いずれか一方のスイッチ電源装置だけです。

RPS モードの 1 台の XPS 電源装置がスイッチ電源装置をバックアップしていて、別のスイッチ電源装置が故障した場合、XPS によるバックアップは受けられないというメッセージが表示されます。故障した電源装置が復旧すると、XPS は他の電源装置をバックアップできるようになります。

1 台のスイッチに取り付けられている 2 台の故障した電源装置を XPS がバックアップしている場合（XPS 電源装置は両方とも RPS モード）、故障した電源装置が両方とも修理されるか交換されるまで、XPS は他のスイッチの電源装置をバックアップできません。

1 台の電源装置が RPS モード、もう 1 台が SP モードの混在モードで、1 台のスイッチに取り付けられている 2 台の電源装置が故障した場合、XPS はいずれか一方の電源装置しかバックアップできないので、XPS は両方の電源装置への電力供給を拒否します。このため、スイッチはシャットダウンします。これは混在電源モードでのみ発生します。

スイッチは RPS に設定されているポートに接続されているが、電源装置が両方とも RPS でない場合、RPS ポート設定は拒否され、XPS はスイッチを電源スタックに追加しようとします。スイッチが SP モードで動作できない（スタック可能なスイッチでない）場合、ポートはディセーブルになります。

RPS モードのポートには、プライオリティを設定できます。デフォルトのプライオリティは、XPS ポート番号に基づき、ポート 1 が最もプライオリティが高いポートです。プライオリティの高いポートには、プライオリティの低いポートよりも優先的にバックアップ電力が供給されます。プライオリティの低いポートに接続されているスイッチをバックアップしているときにプライオリティの高いポートに接続されているスイッチで電源装置の故障が発生した場合、XPS は、プライオリティの高いポートに電力を供給するためにプライオリティの低いポートへの電力を削減します。

スタック電源モード

スタック電源モードは、電源スタックに属する Catalyst スイッチでのみ使用します。XPS が含まれていない場合、電源スタックはリンク トポロジで動作し、最大 4 台のスイッチで構成でき

ます。XPSを電源スタックに追加すると、スタック内で最大9台のスイッチとXPSを接続し、スタック電源のリング トポロジ動作と同じような電力バジェットを電源スタックのメンバに提供できます。

SPポートを経由してXPSに接続されたすべてのCatalystスイッチは同じ電源スタックに属し、XPS とスイッチから供給されるすべての電力はスタック内のすべてのスイッチで共有されます。電源共有がデフォルトのモードですが、XPS は、リング トポロジでサポートされているのと同じスタック電源モード（厳密または厳密でない電源共有モードと冗長モード）をサポートします。

XPSはネイバー探索を使用して電源スタックを作成します。XPSは未設定ポートでCatalystスイッチを検出すると、そのポートをSPポートとしてマークするので、そのスイッチは電源スタックに追加されます。XPSはスイッチに通知し、電力バジェット配分プロセスを開始し、電源スタックに属するスイッチの要件、プライオリティ、現在の電力割り当て、およびスタック集約電源能力に基づいて各スイッチにバジェットを割り当てます。

XPSは電力バジェットを各スイッチに送信します。各スイッチに必要な最大電力を供給するために使用できる入力電力が足りない場合、電力はプライオリティに基づいて分配されます。最初にプライオリティの最も高いスイッチに必要な電力が分配され、その後にすでに電力が割り当てられているすべての受電デバイスにプライオリティ順に電力が分配されます。残りの電力はスタック全体で均等に分配されます。

RPS ポートのプライオリティ（1 ～ 9）は、スタック電源のプライオリティに影響しません。スタック電源に参加している各スイッチには、独自のシステム プライオリティ、およびそのポートに接続される装置用の高および低プライオリティがあります。これらのプライオリティは、リング トポロジと同様にスタック電源で使用されます。システム、高プライオリティのポート、および低プライオリティのポートにスタック電源のプライオリティを設定するには、スイッチ スタック電源コンフィギュレーション モードで **power-priority switch**、**power-priority high**、および **power-priority low** コマンドを使用します。システムまたは一連の受電デバイスがデフォルトのプライオリティを使用している場合、XPS は、自動的にプライオリティ（1 ～ 27）を割り当てます。この際、MAC アドレスの小さいほうに高いプライオリティを割り当てます。

電源スタック モードは、電源共有、厳密な電源共有、冗長、厳密な冗長の 4 つです。電源スタック モードを設定するには、電源スタック コンフィギュレーション モードで **mode** {**power-sharing** | **redundant**} [**strict**] コマンドを使用します。**power-sharing** または **redundant** の設定は、スタックの電力バジェットに影響し、**strict** を指定するかどうかは、バジェットの減少によって負荷制限が発生しないときの PoE アプリケーションの動作に影響します。

- （厳密または厳密でない）電源共有モードの場合、スタックの電力バジェットは、スタック内のすべての電源装置の出力容量を累積した値から 30 W の予約電力を引いた値です。これはデフォルトです。
- （厳密または厳密でない）冗長モードの場合、スタックの電力バジェットは、電源スタックで最大の電源装置の出力容量を引いた後で使用できる合計電力から 30 W を引いた値です。冗長モードでは、1 台の電源装置が故障した場合にスイッチまたは受電デバイスで停電または負荷制限が発生しないことが保証されます。ただし、複数の電源装置が故障した場合、負荷制限が発生する可能性があります。

- 厳密なモードで、入力電力の損失が原因で電力バジェットの減少が発生し、ハードウェアの負荷制限は発生しなかった場合、電力の割り当て量が使用可能なPoE電力量を下回るか等しくなるまで、XPSは、プライオリティの低いほうから順に受電デバイスへの電力供給を自動的に拒否し始めます。
- 厳密でないモードでは、電力の減少が発生した場合、電力の割り当て量をバジェット内に収めることが許可されます。

たとえば、PoEバジェットの合計（使用可能な電力）が400 Wのシステムは、バジェットから390 W（割り当て電力）を受電デバイスに割り当てることができます。装置に割り当てる電力は、その装置に必要な最大電力量です。一連の受電デバイスが実際に消費する電力（消費電力）は通常、割り当て電力と等しくなりません。この例では、実際の電力は約200 Wである可能性があります。スタック内での電力損失によって使用可能な電力が210 Wに減った場合、この電力量は受電デバイスが消費する電力を維持するのに十分ですが、最悪の場合の割り当て電力を下回っています。システムはバジェット内に収まります。厳密なモードでは、スタックは、割り当て電力が210 W以下になるまで、すぐに受電デバイスへの電力供給を拒否します。厳密でないモードでは、何も動作は行われず、状態を維持できます。厳密でないモードで実際の消費電力が 210 W を上回った場合、これによって負荷制限が発生し、プライオリティ レベルの最も低いすべての受電デバイスまたはスイッチへの電力が失われる可能性があります。

混在モード

XPS 2200は混在モードでも動作できます。このモードでは、スイッチと接続するポートはRPSと SP の場合があります。この設定では、少なくとも 1 台の電源装置を RPS 電源装置にする必要があります。XPS の電源装置がバックアップできるスイッチ電源装置は、1 台だけです。また、その XPS 電源装置は、RPS モードの XPS ポートに接続されているスイッチで最大ワット数の電源装置よりも、ワット数が大きい必要があります。

SP ポートに接続されたスイッチは、1 つの電源スタックに属します。SP スイッチに十分な大きさの電力バジェットがある場合、XPS に SP 電源装置は必要ありません。XPS 電源装置を設定すると、その電力は電源スタックで共有する電源プールに追加されます。

XPS 2200 システムのデフォルト

ポートのデフォルトロールはAuto-SPです。このロールでは、ポートに接続されているスイッチによって電源モードが決まります（LAN Base イメージを実行している Catalyst の場合は RPS。IP Base または IP Services イメージを実行している Catalyst スイッチの場合は SP）。

XPS 電源装置 A（PS1）のデフォルトは RPS モードです。電源装置 B（PS2）のデフォルトは SP モードです。

すべてのポートと電源装置のデフォルト モードはイネーブルです。

RPS に設定されているポートでは、デフォルトのプライオリティはポート番号と同じです。

XPS 2200 を設定する方法

XPS は、XPS ポートに接続されている任意のスイッチで設定できます。複数のスイッチで XPS コンフィギュレーション コマンドを入力した場合、適用された最後の設定が有効になります。スイッチ コンフィギュレーション ファイルに保存されるのは、スイッチとポートの名前だけです。

システム名の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**power xps** *switch-number* **name** {*name* | **serialnumber**}	（注） *switch-number* は、Catalyst スイッチにのみ表示され、1～9 の値でデータ スタック内のスイッチ番号を表します。 XPS 2200 システムの名前を設定します。 • *name*：XPS 2000 ポートの名前を入力します。名前には最大 20 文字が使用できます。 • **serialnumber**：XPS 2200 のシリアル番号をシステム名として使用します。
ステップ 4	**power xps** *switch-number* **port** {*name* | **hostname** | **serialnumber**}	（注） *switch-number* は、Catalyst スイッチにのみ表示され、1～9 の値でデータ スタック内のデバイス 番号を表します。 デバイス に接続されている XPS 2200 ポートの名前を設定します。

	コマンドまたはアクション	目的
		• *name*：XPS 2000 ポートの名前を入力します。 • **serialnumber**：ポートに接続されているデバイスのシリアル番号を使用します。 • **hostname**：ポートに接続されているデバイスのホスト名を使用します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show env xps system**	設定したシステムとポートの名前を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

XPS ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**power xps** *switch-number***port** {*number* | **connected**} **mode** {**disable** | **enable**}	（注） *switch-number* は、Catalyst スイッチにのみ表示され、1 ～ 9 の値でデータ スタック内のスイッチ番号を表します。 ポートをイネーブルまたはディセーブルに設定します。 • *number*：XPS 2200 ポート番号を入力します。指定できる範囲は 1 ～ 9 です。

	コマンドまたはアクション	目的
		• **connected**：スイッチが接続されているポート番号がわからない場合は、このキーワードを入力します。 • **mode disable**：XPS ポートをディセーブル（シャットダウン）にします。 （注） XPS ポートをディセーブルにすることは、ケーブルを取り外すことに似ているので、**show** コマンドの出力では同じに見えます。物理的なケーブルが接続されている場合、**enable** キーワードを使用してポートをイネーブルにできます。 • **mode enable**：XPS ポートをイネーブルにします。これはデフォルトです。
ステップ 3	**power xps** *switch-number***port** {*number* | **connected**} **role** {**auto** | **rps**}	（注） *switch-number* は、1 ～ 9 の値でデータ スタック内のスイッチ番号を表します。 XPS ポートの役割を設定します。 • **role auto**：ポートのモードは、ポートに接続されているスイッチによって決まります。これはデフォルトです。 • **role RPS**：XPS は、スイッチ電源装置が故障した場合にバックアップとして機能します。この設定では、少なくとも 1 台の RPS 電源装置を RPS モードにする必要があります。
ステップ 4	**power xps** *switch-number***port** {*number* | **connected**} **priority** *port-priority* 例： `Device`	（注） *switch-number* は、1 ～ 9 の値でデータ スタック内のスイッチ番号を表します。

	コマンドまたはアクション	目的
		ポートの RPS プライオリティを設定します。複数の電源装置が故障した場合、プライオリティの高いポートはプライオリティの低いポートよりも優先されます。このコマンドは、ポートのモードが RPS の場合にだけ有効です。ポートのモードがスタック電源の場合、スタック電源コマンドを使用してプライオリティを設定します。 • **priority** *port-priority*：ポートの RPS プライオリティを設定します。指定できる範囲は 1 ～ 9 です。1 が最も高いプライオリティです。デフォルトのプライオリティは XPS ポート番号です。
ステップ 5	**show env xps port**	ポートの XPS 設定を確認します。

XPS 電源装置の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**power xps** *switch-number* **supply** {**A** | **B**} **mode** {**rps** | **sp**}	（注） *switch-number* は、1 ～ 9 の値でデータ スタック内のスイッチ番号を表します。 XPS 電源装置のモードを設定します。 • **supply** {**A** | **B**}：設定する電源装置を選択します。左側が電源装置 A（PS1 と表示）で、右側が電源装置 B（PS2）です。 • **mode rps**：接続しているスイッチをバックアップするには、電源装置のモードを RPS に設定します。これ

	コマンドまたはアクション	目的
		は電源装置 A（PS1）のデフォルト設定です。 • **mode sp**：電源スタックに参加するには、電源装置のモードをスタック電源（SP）に設定します。これは電源装置 B（PS2）のデフォルト設定です。
ステップ 3	**power xps** *switch-number***supply** {**A** | **B**} {**on** | **off**}	（注） *switch-number* は、1 ～ 9 の値でデータ スタック内のスイッチ番号を表します。 XPS 電源装置をオンまたはオフに設定します。デフォルトは、2 台ともオンです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show env xps power**	XPS 電源装置のステータスを表示します。

XPS 2200 のモニタリングおよびメンテナンス

コマンド	目的
show env xps system	設定したシステムとポートの名前を確認します。
show env xps port	ポートの XPS 設定を確認します。
show env xps power	XPS 電源装置のステータスを表示します。

その他の参考資料

ここでは、スイッチ管理に関する参考資料について説明します。

XPS 2200 の機能履歴と情報

表 *15 : XPS 2200* の機能情報

リリース	機能
Cisco IOS XE 15.2.(3)E1	XPS 2200 機能が導入されます

関連資料

関連項目	マニュアル タイトル
スタック電源の設定	Consolidated Platform Configuration Guide, Cisco IOS XE 3.7E and Later (Catalyst 3850 Switches)

標準

標準	マニュアル タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB の場所を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用して、[Cisco Access Products] メニューからプラットフォームを選択します。 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

第 13 章

EEE の設定

- EEE について （219 ページ）
- EEE の制約事項 （219 ページ）
- EEE の設定方法 （220 ページ）
- EEE の監視 （221 ページ）
- EEE の設定例 （222 ページ）
- その他の参考資料 （222 ページ）
- EEE 設定の機能履歴と情報 （223 ページ）

EEE について

EEE の概要

Energy Efficient Ethernet (EEE) は、アイドル時間にイーサネット ネットワークの消費電力を減らすように設計された IEEE 802.3az の標準です。

低電力アイドル（LPI）モードをサポートするデバイスで EEE をイネーブルにできます。このようなデバイスは、低い使用率のときにLPIモードを開始して、電力を節約できます。LPIモードでは、リンクの両端にあるシステムは、特定のサービスをシャットダウンして、電力を節約できます。EEE は上位層プロトコルおよびアプリケーションに対して透過的であるように、LPI モードに移行したり、LPI モードから移行する必要があるプロトコルを提供します。

デフォルトの EEE 設定

EEE はデフォルトでディセーブルになっています。

EEE の制約事項

EEE には、次の制約事項があります。

- EEE の設定を変更すると、デバイスがレイヤ 1 の自動ネゴシエーションを再起動しなければならないため、インターフェイスがリセットされます。
- 受信パスでデータを受け入れる前により長いウェイク アップ時間を必要とするデバイスのリンク層検出プロトコル（LLDP）をイネーブルにする必要がある場合があります。これにより、デバイスは送信リンク パートナーから拡張システムのウェイク アップ時間についてネゴシエーションできます。

EEE の設定方法

EEE 対応リンク パートナーに接続されているインターフェイスの EEE をイネーブルまたはディセーブルにできます。

EEE のイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**power efficient-ethernet auto** 例： `Device(config-if)# power efficient-ethernet auto`	特定のインターフェイスで EEE をイネーブルにします。EEE がイネーブルの場合、デバイスはリンク パートナーに EEE をアドバタイズし、自動ネゴシエートします。
ステップ 4	**no power efficient-ethernet auto** 例： `Device(config-if)# no power efficient-ethernet auto`	指定したインターフェイス上で EEE をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

EEE の監視

表 *16 : EEE* 設定を表示するコマンド

コマンド	目的
show eee capabilities interface *interface-id*	指定インターフェイスの EEE 機能を表示します。
show eee status interface *interface-id*	指定したインターフェイスの EEE ステータス情報を表示します。
show eee counters interface *interface-id*	指定したインターフェイスの EEE 機能を表示します。

次に、**show eee** コマンドの例を示します。

```
Switch#show eee capabilities interface gigabitEthernet 2/0/1
Gi2/0/1
EEE(efficient-ethernet): yes (100-Tx and 1000T auto)
Link Partner : yes (100-Tx and 1000T auto)

ASIC/Interface : EEE Capable/EEE Enabled
```

```
Switch#show eee status interface gigabitEthernet 2/0/1
Gi2/0/1 is up
EEE(efficient-ethernet): Operational
Rx LPI Status : Low Power
Tx LPI Status : Low Power
Wake Error Count : 0

ASIC EEE STATUS
Rx LPI Status : Receiving LPI
Tx LPI Status : Transmitting LPI
Link Fault Status : Link Up
Sync Status : Code group synchronization with data stream intact
```

```
Switch#show eee counters interface gigabitEthernet 2/0/1

LP Active Tx Time (10us) : 66649648
LP Transitioning Tx : 462
LP Active Rx Time (10us) : 64911682
LP Transitioning Rx : 153
```

EEE の設定例

次に、インターフェイスで EEE をイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# power efficient-ethernet auto
```

次に、インターフェイスで EEE をディセーブルにする例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no power efficient-ethernet auto
```

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

EEE 設定の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 V 部

IPv6

- MLD スヌーピングの設定 （227 ページ）
- IPv6 ユニキャスト ルーティングの設定 （245 ページ）
- IPv6 マルチキャストの実装 （283 ページ）
- IPv6 クライアント IP アドレス ラーニングの設定 （315 ページ）
- IPv6 WLAN セキュリティの設定 （343 ページ）
- IPv6 ACL の設定 （365 ページ）
- IPv6 Web 認証の設定 （385 ページ）
- IPv6 クライアント モビリティの設定 （397 ページ）
- IPv6 モビリティの設定 （405 ページ）

第 14 章

MLD スヌーピングの設定

このモジュールには、MLD スヌーピングの設定の詳細が含まれています。

- 機能情報の確認 （227 ページ）
- IPv6 MLD スヌーピングの設定に関する情報 （227 ページ）
- IPv6 MLD スヌーピングの設定方法 （232 ページ）
- MLD スヌーピング情報の表示 （242 ページ）
- MLD スヌーピングの設定例 （243 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IPv6 MLD スヌーピングの設定に関する情報

（注） この IPv6 MLD スヌーピングを使用するには、スイッチが LAN Base イメージを実行している必要があります。

スイッチ上で Multicast Listener Discovery（MLD）スヌーピングを使用して、スイッチド ネットワーク内のクライアントおよびルータに IP Version 6（IPv6）マルチキャスト データを効率的に配信することができます。特に明記しない限り、スイッチという用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。

（注） スタック構成をサポートしているのは、LAN Base イメージを実行している Catalyst 2960-X スイッチだけです。

（注） IPv6 を使用するには、デュアル IPv4 および IPv6 スイッチング データベース管理（SDM）テンプレートがスイッチに設定されている必要があります。

LAN ベース フィーチャ セットが稼働しているスイッチでは、ルーティング テンプレートはサポートされません。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

MLD スヌーピングの概要

IP Version 4（IPv4）では、レイヤ 2 スイッチはインターネット グループ管理プロトコル（IGMP）スヌーピングを使用して、動的にレイヤ 2 インターフェイスを設定することにより、マルチキャスト トラフィックのフラッディングを抑制します。そのため、マルチキャスト トラフィックは IP マルチキャスト デバイスに対応付けられたインターフェイスにだけ転送されます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピングを使用すると、IPv6 マルチキャスト データは VLAN（仮想 LAN）内のすべてのポートにフラッディングされるのではなく、データを受信するポートのリストに選択的に転送されます。このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャスト ルータで使用されるプロトコルで、ルータに直接接続されたリンク上のマルチキャスト リスナー（IPv6 マルチキャスト パケットを受信するノード）の存在、および隣接ノードを対象とするマルチキャスト パケットを検出します。MLD は IGMP から派生しています。MLD バージョン 1（MLDv1）は IGMPv2 と、MLD バージョン 2（MLDv2）は IGMPv3 とそれぞれ同等です。MLD は Internet Control Message Protocol バージョン 6（ICMPv6）のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の 2 つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピング：MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 基本スヌーピング（MBSS）：MLDv2 制御パケットを使用して、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。

（注） スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 拡張スヌーピングをサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できます。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェアおよびハードウェアで構築されます。その後、スイッチはハードウェアで IPv6 マルチキャストアドレスに基づくブリッジングを実行します。

IPv6 マルチキャスト標準に従い、スイッチは自身の MAC アドレスの下位 4 オクテットと MAC アドレス 33:33:00:00:00:00 の論理 OR を実行して、MAC マルチキャストアドレスを抽出します。たとえば、IPv6 の MAC アドレス FF02:DEAD:BEEF:1:3 は、イーサネットの MAC アドレス 33:33:00:01:00:03 にマッピングされます。

IPv6 宛先アドレスと MAC 宛先アドレスが一致しない場合、マルチキャスト パケットは一致しません。スイッチは、一致しないパケットをハードウェア ベースの MAC アドレス テーブルによって転送します。MAC 宛先アドレスが MAC アドレス テーブルにない場合、スイッチは受信したポートと同じ VLAN 内のすべてのポートにパケットをフラッディングします。

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

- Listener Query：IGMPv2 クエリーと同等で、General Query または Mulicast-Address-Specific Query（MASQ）のいずれかになります。
- Multicast Listener Report：IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージ：IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートします。

メッセージの送受信の結果生じるメッセージ タイマーおよびステート移行は、IGMPv2 メッセージの場合と同じです。リンクに対してローカルで有効な IPv6 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done メッセージに応答します。また、スイッチはレポート抑制、レポート プロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト グループ アドレス設定もサポートします。

MLDスヌーピングがディセーブルの場合、すべてのMLDクエリーが入力VLANでフラッディングされます。

MLDスヌーピングがイネーブルの場合、受信されたMLDクエリーが入力VLANでフラッディングされ、クエリーのコピーはCPUに送信され、処理されます。MLDスヌーピングでは、受信されたクエリーからIPv6マルチキャストアドレスデータベースを構築します。MLDスヌーピングは、マルチキャスト ルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、VLANのクエリアIP送信元アドレス、VLAN内のクエリア ポートを学習して、マルチキャストアドレス エージングを維持します。

（注） IPv6マルチキャスト ルータがCatalyst 6500スイッチであり、拡張VLAN（範囲1006 ～ 4094）を使用する場合、Catalyst 2960、2960-S、2960-C、2960-X、または2960-CXスイッチがVLAN上でクエリーを受信できるようにするため、IPv6 MLDスヌーピングをCatalyst 6500スイッチの拡張VLANでイネーブルにする必要があります。標準範囲VLAN（1 ～ 1005）の場合、IPv6 MLDスヌーピングをCatalyst 6500スイッチのVLANでイネーブルにする必要はありません。

グループがMLDスヌーピング データベースに存在する場合、スイッチはMLDv1レポートを送信して、グループ固有のクエリーに応答します。このグループが不明の場合、グループ固有のクエリーは入力VLANにフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Doneメッセージ（IGMP Leaveメッセージと同等）を送信できます。スイッチがMLDv1 Doneメッセージを受信した際に、即時脱退がイネーブルでなければ、スイッチは メッセージを受信したポートにMASQを送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポート メンバーシップの削除を設定できます。1つのアドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対するレポートがない場合のみです。デフォルトの回数は2回です。

マルチキャスト ルータ検出

IGMPスヌーピングと同様に、MLDスヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1スヌーピング クエリーおよびIPv6 PIMv2パケットにより行われます。
- 複数のルータが同じレイヤ2インターフェイス上にある場合、MLDスヌーピングではポート上の単一のマルチキャスト ルータ（直前にルータ制御パケットを送信したルータ）を追跡します。

- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの 5 分に基づきます。ポート上で制御パケットが 5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合のみです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出された後は、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポートが受信されると、IPv6 マルチキャスト グループ アドレスが VLAN の MLD データベースに入力されます。その後、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナー メッセージ抑制）は自動的にイネーブルになります。レポート抑制により、スイッチはグループで受信された最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポーティングもサポートします。MLDv1 MASQ が受信されると、スイッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバ ポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ（IGMP Leave メッセージと同等）を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。VLAN で即時脱退をイネーブルにする場合は（IGMP スヌーピングと同様に）、ポートに単一のホストが接続されている VLAN でのみこの機能を使用します。ポートがグループの最後のメンバである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に（1 つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバーシップが削除される時期を MASQ 数の観点か

ら制御できます。アドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、**ipv6 mld snooping last-listener-query count** グローバル コンフィギュレーション コマンドにより設定されます。デフォルトの回数は 2 回です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。最大応答時間は、**ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドにより設定します。削除されたポートがマルチキャスト アドレスの最後のメンバである場合は、マルチキャストアドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

即時脱退がイネーブルでない場合に、ポートが MLD Done メッセージを受信すると、スイッチはポートで MASQ を生成して、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信します。ポートがマルチキャスト グループから削除される前に、送信される MASQ 数およびスイッチが応答を待機する時間を任意で設定できます。

MLDv1 即時脱退をイネーブルにした場合、スイッチはポートで MLD Done メッセージを検出するとただちに、マルチキャスト グループからポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバが 1 つだけ存在する場合に限定してください。同一ポートにマルチキャスト グループのクライアントが複数ある場合は、VLAN で即時脱退をイネーブルにしてはなりません。

トポロジ変更通知処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して、トポロジ変更通知（TCN）送信請求をイネーブルにすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリーによりすべての IPv6 マルチキャスト トラフィックをフラッディングするよう VLAN に設定してから、選択されたポートにのみマルチキャスト データの送信を開始します。この値は、**ipv6 mld snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用して設定します。デフォルトでは、2 つのクエリーが送信されます。スイッチが VLAN 内の STP ルートになる場合、またはスイッチがユーザにより設定された場合は、リンクに対してローカルで有効な IPv6 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。これは IGMP スヌーピングの場合と同じです。

IPv6 MLD スヌーピングの設定方法

MLD スヌーピングのデフォルト設定

表 *17 : MLD* スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング（グローバル）	ディセーブル

機能	デフォルト設定
MLD スヌーピング（VLAN 単位）	イネーブルVLAN MLD スヌーピングが実行されるためには、MLD スヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャスト アドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	ディセーブル
MLD スヌーピングの堅牢性変数	グローバル：2、VLAN 単位：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー カウント	グローバル：2、VLAN 単位：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナークエリーインターバル	グローバル：1000（1 秒）、VLAN：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバルのインターバルを使用します。
TCN クエリー送信請求	ディセーブル
TCN クエリー カウント	2
MLD リスナー抑制	ディセーブル

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。
- IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要が

あります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにできます。
- スイッチまたはスイッチ スタックに保持可能なマルチキャスト エントリの最大数は、設定された SDM テンプレートによって決まります。
- スイッチまたはスイッチ スタックに保持可能なアドレス エントリの最大数は 4000 です。

スイッチでのMLDスヌーピングのイネーブル化またはディセーブル化（CLI）

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定はグローバル設定を上書きします。つまり、MLD スヌーピングはデフォルト ステート（イネーブル）の VLAN インターフェイスでのみイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

スイッチで MLD スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping** 例： `Device(config)# ipv6 mld snooping`	スイッチで MLD スヌーピングをイネーブルにします。
ステップ 3	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 4	**copy running-config startup-config** 例： `Device(config)# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 5	**reload** 例： `Device(config)# reload`	OS（オペレーティング システム）をリロードします。

VLAN での MLD スヌーピングのイネーブル化またはディセーブル化（CLI）

VLAN で MLD スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping** 例： `Device(config)# ipv6 mld snooping`	スイッチで MLD スヌーピングをイネーブルにします。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* 例： `Device(config)# ipv6 mld snooping vlan 1`	VLAN で MLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

	コマンドまたはアクション	目的
		（注） VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。
ステップ 4	**end** 例： `Device(config)# ipv6 mld snooping vlan 1`	特権 EXEC モードに戻ります。

スタティック マルチキャスト グループの設定（CLI）

ホストまたはレイヤ 2 ポートは、通常マルチキャスト グループにダイナミックに加入しますが、VLAN に IPv6 マルチキャスト アドレスおよび メンバ ポートをスタティックに設定することもできます。

マルチキャスト グループのメンバとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **static** *ipv6_multicast_address* **interface** *interface-id* 例： `Device(config)# ipv6 mld snooping vlan 1 static FF12::3 interface gigabitethernet 0/1`	マルチキャスト グループのメンバとしてレイヤ 2 ポートにマルチキャスト グループを設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • *ipv6_multicast_address* は、128 ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式でなければなりません。

	コマンドまたはアクション	目的
		• *interface-id* は、メンバ ポートです。物理インターフェイスまたはポート チャネル（1 ～ 48）に設定できます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 4	次のいずれかを使用します。
	• **show ipv6 mld snooping address**
	• **show ipv6 mld snooping address vlan** *vlan-id*
	例：
	`Device# show ipv6 mld snooping address`
	または
	`Device# show ipv6 mld snooping vlan 1`
		スタティック メンバ ポートおよび IPv6 アドレスを確認します。

マルチキャスト ルータ ポートの設定（CLI）

（注） マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

VLAN にマルチキャスト ルータ ポートを追加するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id* 例：	マルチキャスト ルータの VLAN ID を指定して、マルチキャスト ルータにインターフェイスを指定します。

	コマンドまたはアクション	目的
	`Device(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet 0/2`	• 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping mrouter** [**vlan** *vlan-id*] 例： `Device# show ipv6 mld snooping mrouter vlan 1`	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。

MLD 即時脱退のイネーブル化（CLI）

MLDv1 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **immediate-leave** 例： `Device(config)# ipv6 mld snooping vlan 1 immediate-leave`	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**show ipv6 mld snooping vlan** *vlan-id* 例： `Device# show ipv6 mld snooping vlan 1`	VLANインターフェイス上で即時脱退がイネーブルになっていることを確認します。

MLD スヌーピング クエリーの設定（CLI）

スイッチまたはVLANにMLDスヌーピング クエリーの特性を設定するには、特権EXECモードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping robustness-variable** *value* 例： `Device(config)# ipv6 mld snooping robustness-variable 3`	（任意）スイッチが一般クエリーに応答しないリスナー（ポート）を削除する前に、送信されるクエリー数を設定します。指定できる範囲は 1 ～ 3 です。デフォルトは 2 です。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* **robustness-variable** *value* 例： `Device(config)# ipv6 mld snooping vlan 1 robustness-variable 3`	（任意）VLAN 単位でロバストネス変数を設定します。これにより、MLD レポート応答がない場合にマルチキャストアドレスがエージングアウトされるまでに、MLDスヌーピングが送信する一般クエリー数が決定されます。指定できる範囲は 1 ～ 3 です。デフォルトは 0 です。0 に設定すると、使用される数はグローバルな堅牢性変数の値になります。
ステップ 4	**ipv6 mld snooping last-listener-query-count** *count* 例： `Device(config)# ipv6 mld snooping last-listener-query-count 7`	（任意）MLDクライアントがエージングアウトされる前にスイッチが送信するMASQ数を設定します。指定できる範囲は 1 ～ 7 です。デフォルトは 2 です。クエリーは 1 秒後に送信されます。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-count** *count* 例： `Device(config)# ipv6 mld snooping vlan 1 last-listener-query-count 7`	（任意）VLAN 単位でラストリスナークエリーカウントを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は 1 ～ 7 です。デフォルトは 0 です。0 に設定すると、グローバルなカウント値が使用されます。クエリーは 1秒後に送信されます。
ステップ 6	**ipv6 mld snooping last-listener-query-interval** 間隔 例： `Device(config)# ipv6 mld snooping last-listener-query-interval 2000`	（任意）スイッチが MASQ を送信したあと、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。指定できる範囲は、100 ～ 32,768 ミリ秒です。デフォルト値は 1000（1 秒）です。
ステップ 7	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-interval** *interval* 例： `Device(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 2000`	（任意）VLAN 単位で last-listener クエリーインターバルを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0 ～ 32,768 ミリ秒です。デフォルトは 0 です。0 に設定すると、グローバルな最後のリスナークエリーインターバルが使用されます。
ステップ 8	**ipv6 mld snooping tcn query solicit** 例： `Device(config)# ipv6 mld snooping tcn query solicit`	（任意）トポロジ変更通知（TCN）をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラフィックすべてをフラッディングしてから、マルチキャストデータをマルチキャストデータの受信を要求するポートに対してのみ送信します。デフォルトでは、TCN はディセーブルに設定されています。
ステップ 9	**ipv6 mld snooping tcn flood query count** *count* 例： `Device(config)# ipv6 mld snooping tcn flood query count 5`	（任意）TCN がイネーブルの場合、送信される TCN クエリー数を指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 10	**end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**show ipv6 mld snooping querier** [**vlan** *vlan-id*] 例： `Device(config)# show ipv6 mld snooping querier vlan 1`	（任意）スイッチまたはVLANのMLDスヌーピングクエリア情報を確認します。

MLD リスナー メッセージ抑制のディセーブル化（CLI）

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、スイッチはマルチキャスト ルータ クエリーごとに 1 つの MLD レポートのみを転送します。メッセージ抑制がディセーブルの場合は、複数のマルチキャスト ルータに MLD レポートが転送されます。

MLD リスナー メッセージ抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ipv6 mld snooping listener-message-suppression** 例： `Device(config)# no ipv6 mld snooping listener-message-suppression`	MLD メッセージ抑制をディセーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping** 例： `Device# show ipv6 mld snooping`	IPv6 MLD スヌーピング レポート抑制がディセーブルであることを確認します。

MLD スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インターフェイスのMLDスヌーピング情報を表示できます。また、MLDスヌーピング用に設定された VLAN の IPv6 グループ アドレス マルチキャスト エントリを表示することもできます。

表 *18 : MLD* スヌーピング情報表示用のコマンド

コマンド	目的
show ipv6 mld snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、***vlan***vlan-id を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習され、手動で設定されたマルチキャストルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。 （任意）個々の VLAN に関する情報を表示するには、***vlan***vlan-id を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。 （任意）***vlan****vlan-id* を入力して、単一の VLAN 情報を表示します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping address [**vlan** *vlan-id*] [**count** | **dynamic** | **user**]	すべての IPv6 マルチキャスト アドレス情報あるいはスイッチまたは VLAN の特定の IPv6 マルチキャスト アドレス情報を表示します。 • **count** を入力して、スイッチまたは VLAN のグループ数を表示します。 • **dynamic** を入力して、スイッチまたは VLAN の MLD スヌーピング学習済みグループ情報を表示します。 • **user** を入力して、スイッチまたは VLAN の MLD スヌーピング ユーザ設定グループ情報を表示します。

コマンド	目的
show ipv6 mld snooping address vlan *vlan-id* [*ipv6-multicast-address*]	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。

MLD スヌーピングの設定例

スタティックなマルチキャスト グループの設定：例

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet

          1/0/1
Device(config)# end
```

マルチキャスト ルータ ポートの設定：例

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet

          0/2
Device(config)# exit
```

MLD 即時脱退のイネーブル化：例

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 130 immediate-leave
Device(config)# exit
```

MLD スヌーピング クエリーの設定：例

次に、MLD スヌーピングのグローバルな堅牢性変数を 3 に設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping robustness-variable 3
Device(config)# exit
```

次に、VLAN の MLD スヌーピングの最後のリスナー クエリー カウントを 3 に設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Device(config)# exit
```

次に、MLD スヌーピングの最後のリスナー クエリー インターバル（最大応答時間）を 2000（2 秒）に設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping last-listener-query-interval 2000
Device(config)# exit
```

第 15 章

IPv6 ユニキャスト ルーティングの設定

- 機能情報の確認 （245 ページ）
- IPv6 ユニキャスト ルーティングの設定について （245 ページ）
- DHCP for IPv6 アドレス割り当ての設定 （274 ページ）
- IPv6 ユニキャスト ルーティングの設定例 （279 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IPv6 ユニキャスト ルーティングの設定について

この章では、スイッチに IPv6 ユニキャスト ルーティングを設定する方法について説明します。

（注） この章のすべての IPv6 機能を使用するには、スイッチまたはスタック マスターが IP サービス フィーチャ セットを実行している必要があります。IP ベースのフィーチャ セットを実行しているスイッチは、IPv6 スタティック ルーティング、IPv6 の RIP、および OSPF をサポートします。LAN ベースのフィーチャ セットが稼働しているスイッチは、IPv6 ホスト機能だけをサポートします。

IPv6 の概要

IPv4 ユーザは IPv6 に移行することができ、エンドツーエンドのセキュリティ、Quality of Service（QoS）、およびグローバルに一意なアドレスのようなサービスを利用できます。IPv6 アドレス スペースによって、プライベート アドレスの必要性が低下し、ネットワーク エッジの境界ルータで Network Address Translation（NAT; ネットワーク アドレス変換）処理を行う必要性も低下します。

シスコの IPv6 の実装方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 およびこの章のその他の機能については、

- 『*Cisco IOS IPv6 Configuration Library*』を参照してください。
- Cisco.com の [Search] フィールドを使用して、Cisco IOS ソフトウェア マニュアルを特定します。たとえば、スタティック ルートについての情報が必要な場合は、[Search] フィールドで *Implementing Static Routes for IPv6* と入力すると、スタティック ルートについて調べられます。

IPv6 Addresses

スイッチがサポートするのは、IPv6 ユニキャスト アドレスのみです。サイトローカルなユニキャスト アドレスおよびマルチキャスト アドレスはサポートされません。

IPv6 の 128 ビット アドレスは、コロンで区切られた一連の 8 つの 16 進フィールド（n:n:n:n:n:n:n:n. の形式）で表されます。次に、IPv6 アドレスの例を示します。

2031:0000:130F:0000:0000:09C0:080F:130B

実装を容易にするために、各フィールドの先行ゼロは省略可能です。上記アドレスは、先行ゼロを省略した次のアドレスと同じです。

2031:0:130F:0:0:9C0:80F:130B

2 つのコロン（::）を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この短縮形を使用できるのは、各アドレス内で 1 回のみです。

2031:0:130F::09C0:080F:130B

IPv6 アドレス形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Information About Implementing Basic Connectivity for IPv6」の章では、次の項の内容がスイッチに適用されます。

- IPv6 アドレス形式
- IPv6 アドレス タイプ：ユニキャスト
- IPv6 アドレス タイプ：マルチキャスト
- 「IPv6 Address Output Display」

- 簡易 IPv6 パケット ヘッダー

サポート対象の IPv6 ユニキャスト ルーティング機能

ここでは、スイッチでサポートされている IPv6 プロトコル機能について説明します。

スイッチは、IPv6 の Routing Information Protocol（RIP）、および Open Shortest Path First（OSPF）バージョン 3 プロトコルによる IPv6 ルーティング機能を提供します。等コスト ルートは 16 個までサポートされ、IPv4 および IPv6 フレームを回線レートで同時に転送できます。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクに対してローカルなユニキャスト アドレスをサポートします。サイトに対してローカルなユニキャスト アドレスはサポートされていません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能グローバル ユニキャスト プレフィックスの付いた IPv6 アドレスです。このアドレス構造を使用すると、ルーティング プレフィックスを厳格に集約することができ、グローバル ルーティング テーブル内のルーティング テーブル エントリ数が制限されます。これらのアドレスは、組織を経由して最終的にインターネット サービス プロバイダーに至る集約リンク上で使用されます。

  これらのアドレスはグローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID によって定義されます。現在のグローバル ユニキャスト アドレス割り当てには、バイナリ値 001（2000::/3）で開始するアドレス範囲が使用されます。プレフィックスが 2000::/3（001）～ E000::/3（111）のアドレスには、Extended Unique Identifier（EUI）64 フォーマットの 64 ビット インターフェイス ID を設定する必要があります。

- リンクに対してローカルなユニキャストアドレスをすべてのインターフェイスに自動的に設定するには、修飾 EUI フォーマット内で、リンクに対してローカルなプレフィックス FE80::/10（1111 1110 10）およびインターフェイスID を使用します。ネイバー探索プロトコル（NDP）およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。ローカル リンク上のノードは、リンクに対してローカルなアドレスを使用します。通信する場合に、グローバルに一意なアドレスは不要です。IPv6 ルータは、リンクに対してローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章にある IPv6 ユニキャスト アドレスに関する項を参照してください。

IPv6 の DNS

IPv6 は、ドメイン ネーム システム（DNS）のレコード タイプを、DNS 名前/アドレスおよびアドレス/名前の検索プロセスでサポートします。DNS AAAA リソース レコード タイプは IPv6 アドレスをサポートし、IPv4 の A アドレス レコードと同等です。スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス MTU ディスカバリ

スイッチはシステム最大伝送単位（MTU）の IPv6 ノードへのアドバタイズおよびパス MTU ディスカバリをサポートします。パス MTU ディスカバリを使用すると、ホストは指定されたデータ パスを通るすべてのリンクの MTU サイズを動的に検出して、サイズに合せて調整できます。IPv6 では、パスを通るリンクの MTU サイズが小さくてパケット サイズに対応できない場合、パケットの送信元がフラグメンテーションを処理します。

ICMPv6

IPv6 のインターネット制御メッセージ プロトコル（ICMP）は、ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。IPv6 では、ネイバー探索プロトコルおよびパス MTU ディスカバリに ICMP パケットも使用されます。

ネイバー探索

スイッチは、IPv6 対応の NDP、ICMPv6 の最上部で稼働するプロトコル、および NDP をサポートしない IPv6 ステーション対応のスタティック ネイバー エントリをサポートします。IPv6 ネイバー探索プロセスは ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 未満のルートに対して ICMPv6 リダイレクトをサポートしています。マスク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトがサポートされません。

ネイバー探索スロットリングにより、IPv6 パケットをルーティングするためにネクスト ホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。IPv6 パケットのネクストホップがスイッチによってアクティブに解決しようとしている同じネイバーである場合は、そのようなパケットが追加されると、スイッチはそのパケットをドロップします。このドロップにより、CPU に余分な負荷がかからないようになります。

デフォルト ルータ プリファレンス

スイッチは、ルータのアドバタイズメント メッセージの拡張機能である、IPv6 Default Router Prefernce（DRP）をサポートします。DRP では、特にホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合に、ホストが適切なルータを選択する機能が向上しました。スイッチは、Route Information Option（RFC 4191）をサポートしません。

IPv6 ホストは、オフリンク宛先へのトラフィック用にルータを選択する、デフォルト ルータ リストを維持します。次に、宛先用に選択されたルータは、宛先キャッシュに格納されます。IPv6 NDP では、到達可能であるルータまたは到達可能性の高いルータが、到達可能性が不明または低いルータよりも優先されます。NDP は、到達可能または到達可能の可能性があるルータとして、常に同じルータを選択するか、またはルータ リストから繰り返し使用できます。DRP を使用することにより、IPv6 ホストが、両方ともが到達可能または到達可能の可能性がある 2 台のルータを差別化するように設定できます。

DRP for IPv6 の詳細情報については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチではステートレス自動設定が使用されているため、ホストやモバイル IP アドレスの管理のような、リンク、サブネット、およびサイトアドレス指定の変更を管理することができます。ホストはリンクに対してローカルな独自アドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をアドバタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- Ping、traceroute、Telnet、および TFTP
- IPv6 トランスポートによるセキュア シェル（SSH）
- IPv6 トランスポートによる HTTP サーバ アクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ
- IPv6 アドレスの Cisco Discovery Protocol（CDP）サポート

これらのアプリケーションの管理に関する詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

DHCP for IPv6 アドレスの割り当て

DHCPv6 を使用すると、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。このアドレス割り当て機能により、ホストが接続するネットワークに基づいて、適切なプレフィックス内での重複しないアドレス割り当てが管理されます。アドレスは、1 つまたは複数のプレフィックス プールから割り当てることができます。デフォルトのドメインおよび DNS ネーム サーバ アドレスなど、その他のオプションは、クライアントに戻すことができます。アドレスプールは、特定のインターフェイス、複数のインターフェイス上で使用する場合に割り当てられます。または、サーバが自動的に適切なプールを検出できます。

これらの機能の詳細および設定方法については、『*Cisco IOS IPv6 Configuration Guide*』を参照してください。

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 クライアント、サーバ、またはリレーエージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーキング デバイス間のルートを明示的に定義します。スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

RIP for IPv6

IPv6 の Routing Information Protocol（RIP）は、ルーティング メトリックとしてホップ カウントを使用するディスタンスベクトル プロトコルです。IPv6 アドレスおよびプレフィックスのサポート、すべての RIP ルータを含むマルチキャスト グループ アドレス FF02::9 を RIP アップデート メッセージの宛先アドレスとして使用する機能などがあります。

IPv6 の RIP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

『OSPF for IPv6』

IP Base フィーチャ セットを実行しているスイッチは、IPv6 の Open Shortest Path First（OSPF）（IP のリンクステート プロトコル）をサポートします。詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 の HSRP の設定

HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。IPv6 ホストは、IPv6 ネイバー探索ルータのアドバタイズメント メッセージによって使用可能なルータを学習します。これらのメッセージは定期的にマルチキャストされるか、ホストにより送信請求されます。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカル アドレスがあります。HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカルアドレスに送信されます。グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

（注） IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2（HSRPv2）をイネーブルにする必要があります。

EIGRP IPv6

スイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol（EIGRP）をサポートしています。IPv6 の EIGRP は稼働するインターフェイス上で設定されるため、グローバルな IPv6 アドレスは不要です。IP Lite を実行しているスイッチは EIGRPv6 スタブ ルーティングをサポートします。

EIGRP IPv6 インスタンスでは、実行する前に暗示的または明示的なルータ ID が必要です。暗示的なルータ ID はローカルの IPv6 アドレスを基にして作成されるため、すべての IPv6 ノードには常に使用可能なルータ ID があります。ただし、EIGRP IPv6 は IPv6 ノードのみが含まれるネットワークで稼働するため、使用可能な IPv6 ルータ ID がない場合があります。

EIGRP for IPv6 の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

EIGRPv6 スタブ ルーティング

EIGRPv6 スタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を低減させます。

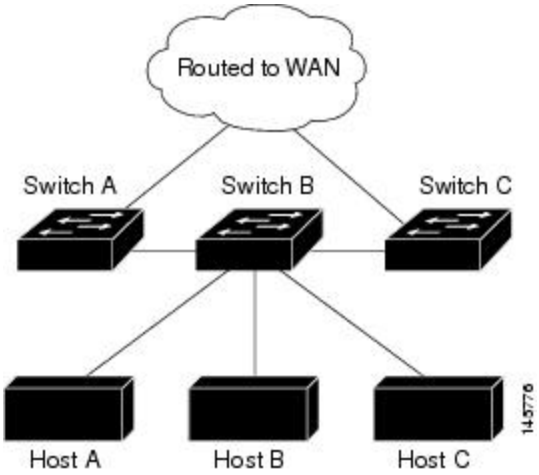
EIGRPv6 スタブ ルーティングを使用するネットワークでは、ユーザに対する IPv6 トラフィックの唯一の許容ルートは、EIGRPv6 スタブ ルーティングを設定しているスイッチ経由です。スイッチは、ユーザインターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRPv6 スタブ ルーティングを使用しているときは、EIGRPv6 を使用してスイッチだけをスタブとして設定するように、分散ルータおよびリモートルータを設定する必要があります。指定したルートだけがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブ ルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブ ルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。スタブ ルータは、ディストリビューション ルータを使用して適切なアップデートをすべてのピアに送信します。

次の図では、スイッチ B は EIGRPv6 スタブ ルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配信ルート、およびサマリー ルートをスイッチ A と C にアドバタイズします。 スイッチ B は、スイッチ A から学習したルートをアドバタイズしません（逆の場合も同様です）。

図 *8 : EIGRP* スタブ ルータ設定



EIGRPv6 スタブ ルーティングの詳細については、『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols, Release 12.4*』の「Implementing EIGRP for IPv6」を参照してください。

SNMP と Syslog、IPv6 による

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。IPv6 による Syslog は、このトランスポートのアドレス データタイプをサポートします。

IPv6 による SNMP および Syslog は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および Syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

IPv6 に関連するサポートでは、SNMP は既存の IP トランスポート マッピングを変更して、IPv4 と IPv6 を同時にサポートします。次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザ データグラム プロトコル（UDP）SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む、IPv6 による SNMP については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、IPv6 による Syslog については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 上の HTTP（S）

HTTP クライアントは要求を IPv4 HTTP サーバと IPv6 HTTP サーバの両方に送信し、これらのサーバは IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレスを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケット コールは、IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを選択します。受信ソケットは、IPv4 ソケットまたは IPv6 ソケットのいずれかです。リスニング ソケットは、接続を示す IPvv4 と IPv6 の両方の信号を待ち受け続けます。IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされています。

基本 TCP/IP スタックは、デュアル スタック環境をサポートします。HTTP には、TCP/IP スタック、およびネットワーク層相互作用を処理するためのソケットが必要です。

HTTP 接続を確立するには、基本ネットワーク接続（**ping**）がクライアントとサーバ ホストとの間に存在する必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

サポートされていない IPv6 ユニキャスト ルーティング機能

スイッチは、次の IPv6 機能をサポートしません。

- IPv6 バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）テーブルのサポート
- サイトローカルなアドレス宛ての IPv6 パケット
- IPv4/IPv6 や IPv6/IPv4 などのトンネリング プロトコル
- IPv4/IPv6 または IPv6/IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ
- IPv6 ユニキャスト Reverse-Path Forwarding
- IPv6 Web Cache Communication Protocol（WCCP）

IPv6 機能の制限

スイッチでは IPv6 はハードウェアに実装されるため、ハードウェア メモリ内の IPv6 圧縮アドレスによる制限がいくつか発生します。これらのハードウェア制限により、機能の一部が失われて、制限されます。

機能の制限は次のとおりです。

- スイッチはハードウェアで SNAP カプセル化 IPv6 パケットを転送できません。これらはソフトウェアで転送されます。
- スイッチはソースルート IPv6 パケットに関する QoS 分類をハードウェアで適用できません。

IPv6 とスイッチ スタック

スイッチにより、スタック全体で IPv6 転送がサポートされ、スタック マスターで IPv6 ホスト機能がサポートされます。スタック マスターは IPv6 ユニキャスト ルーティング プロトコルを実行してルーティング テーブルを計算します。スタック メンバー スイッチはテーブルを受信して、転送用にハードウェア IPv6 ルートを作成します。スタック マスターも、すべての IPv6 アプリケーションを実行します。

（注） スタック内で IPv6 パケットをルーティングするには、スタック内のすべてのスイッチで IP Base フィーチャ セットが稼動している必要があります。

新しいスイッチがスタック マスターになる場合、新しいマスターは IPv6 ルーティング テーブルを再計算してこれをメンバー スイッチに配布します。新しいスタック マスターが選択中およびリセット中の間には、スイッチ スタックによる IPv6 パケットの転送は行われません。スタック MAC アドレスが変更され、これによって IPv6 アドレスが変更されます。**ipv6 address** *ipv6-prefix/prefix length* **eui-64** インターフェイス コンフィギュレーション コマンドを使用して、拡張固有識別子（EUI）でスタック IPv6 アドレスを指定する場合、アドレスは、インターフェイス MAC アドレスに基づきます。IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化（CLI）（255 ページ）を参照してください。

スタック上で永続的な MAC アドレスを設定し、スタック マスターが変更された場合、スタック MAC アドレスは、約 4 分間、変更されません。

IPv6 スタック マスターおよびメンバーの機能は次のとおりです。

- スタック マスター
  - IPv6 ルーティングプロトコルの実行
  - ルーティング テーブルの生成
  - dCEFv6 を使用するスタック メンバーへのルーティング テーブルの配布
  - IPv6 ホスト機能および IPv6 アプリケーションの実行
- スタック メンバー（IP サービス フィーチャ セットを実行している必要があります）
  - スタック マスターからの CEFv6 ルーティング テーブルの受信
  - ハードウェアへのルートのプログラミング

（注） IPv6 パケットに例外（IPv6 オプション）がなく、スタック内のスイッチでハードウェア リソースが不足していない場合、IPv6 パケットがスタック全体にわたってハードウェアでルーティングされます。

  - マスターの再選択での CEFv6 テーブルのフラッシュ

IPv6 のデフォルト設定

表 *19 : IPv6* のデフォルト設定

機能	デフォルト設定
SDM テンプレート	アドバンスデスクトップ。デフォルトは拡張テンプレート

機能	デフォルト設定
IPv6 ルーティング	すべてのインターフェイスでグローバルにディセーブル
CEFv6 または dCEFv6	ディセーブル（IPv4 CEF および dCEF はデフォルトでイネーブル） （注） IPv6 ルーティングがイネーブルの場合、CEFv6 および dCEF6 は自動的にイネーブル
IPv6 アドレス	未設定

IPv6アドレッシングの設定とIPv6ルーティングのイネーブル化（CLI）

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチ上でグローバル転送する方法を説明します。

スイッチ上の IPv6 を設定する前に、次の注意事項に従ってください。

- スイッチでは、この章で説明されたすべての機能がサポートされるわけではありません。サポートされていない IPv6 ユニキャスト ルーティング機能 （253 ページ）を参照してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、16 ビット値を使用したコロン区切りの 16 進形式で指定したアドレスで *ipv6-address* 変数および *ipv6-prefix* 変数を入力する必要があります。*prefix-length* 変数（スラッシュ（/）で始まる）は、プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバル IPv6 アドレスを設定する必要があります。インターフェイス上で IPv6 アドレスを設定すると、リンクに対してローカルなアドレスの設定、およびそのインターフェイスに対する IPv6 のアクティブ化が自動的に行われます。設定されたインターフェイスは、次に示す、該当リンクの必須マルチキャスト グループに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャストアドレスの送信要求ノードマルチキャスト グループ FF02:0:0:0:0:1:ff00::/104（このアドレスはネイバー探索プロセスで使用される）
- すべてのノードを含む、ルータリンクに対してローカルなマルチキャストグループ FF02::1
- すべてのルータを含む、リンクに対してローカルなマルチキャスト グループ FF02::2

インターフェイスから IPv6 アドレスを削除するには、**noipv6 address** *ipv6-prefix/prefix length***eui-64** または **no ipv6 address** *ipv6-address***link-local** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから手動で設定したすべての IPv6 アドレスを削除するに

は、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスで明示的に設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ルーティングをグローバルにディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。

IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

レイヤ 3 インターフェイスに IPv6 アドレスを割り当てて、IPv6 ルーティングをイネーブルにするは、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm preferdual-ipv4-and-ipv6** { **advanced** | **vlan**} 例： `Device(config)# sdm prefer dual-ipv4-and-ipv6 default`	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 • **advanced**：スイッチをデフォルト テンプレートに設定して、システム リソースを均衡化します。 • **vlan**：ハードウェアでのルーティングをサポートしないスイッチでの VLAN 設定を最大化します。 （注） advanced はすべてのライセンス レベルで使用できます。VLAN テンプレートは LAN Base ライセンスでのみ使用できます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**reload** 例： `Device# reload`	オペレーティング システムをリロードします。

	コマンドまたはアクション	目的
ステップ 5	**configureterminal** 例： `Device# configure terminal`	スイッチのリロード後、グローバルコンフィギュレーションモードを開始します。
ステップ 6	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。インターフェイスは物理インターフェイス、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できます。
ステップ 7	**noswitchport** 例： `Device(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。

ステップ 8	次のいずれかを使用します。
	• **ipv6 address** *ipv6-prefix/prefix length* **eui-64**
	• **ipv6 address** *ipv6-address/prefix length*
	• **ipv6 address** *ipv6-address* **link-local**
	• **ipv6 enable**
	• **ipv6 address***WORD*
	• **ipv6 address***autoconfig*
	• **ipv6 address***dhcp*
	例：
	`Device(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64`
	`Device(config-if)# ipv6 address 2001:0DB8:c18:1::/64`
	`Device(config-if)# ipv6 address 2001:0DB8:c18:1:: link-local`
	`Device(config-if)# ipv6 enable`
		• IPv6 アドレスの下位 64 ビットの拡張固有識別子（EUI）を使用して、グローバル IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイス上で IPv6 処理がイネーブルになります。
		• インターフェイスの IPv6 アドレスを手動で設定します。
		• インターフェイスで IPv6 がイネーブルな場合に自動設定されるリンクローカルなアドレスでなく、インターフェイス上の特定のリンクローカルなアドレスを使用するように指定します。このコマンドにより、インターフェイス上で IPv6 処理がイネーブルになります。
		• インターフェイスに IPv6 リンクローカルなアドレスを自動設定し、インターフェイスでの IPv6 処

	コマンドまたはアクション	目的
		理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。
ステップ 9	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**ip routing** 例： `Device(config)# ip routing`	スイッチ上でIPルーティングをイネーブルにします。
ステップ 11	**ipv6unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データ パケットの転送をイネーブルにします。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show ipv6 interface** *interface-id* 例： `Device# show ipv6 interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 14	**copyrunning-configstartup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

IPv4 および IPv6 プロトコル スタックの設定（CLI）

IPv4 および IPv6 を両方サポートし、IPv6 ルーティングがイネーブルになるようにレイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

（注） IPv6 アドレスが設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： `Switch(config)# ip routing`	スイッチ上でルーティングをイネーブルにします。
ステップ 3	**ipv6 unicast-routing** 例： `Switch(config)# ipv6 unicast-routing`	スイッチ上で IPv6 データ パケットの転送をイネーブルにします。
ステップ 4	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 5	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 6	**ip address** *ip-address mask* [**secondary**] 例： `Switch(config-if)# ip address 10.1.2.3 255.255.255`	インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを指定します。
ステップ 7	次のいずれかを使用します。	• グローバル IPv6 アドレスを指定します。ネットワーク プレフィック

	コマンドまたはアクション	目的
	• **ipv6 address** *ipv6-prefix/prefix length* **eui-64** • **ipv6 address** *ipv6-address/prefix length* • **ipv6 address** *ipv6-address* **link-local** • **ipv6 enable** • **ipv6 address***WORD* • **ipv6 address***autoconfig* • **ipv6 address***dhcp*	スだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。 • インターフェイスで IPv6 がイネーブルな場合に自動設定されるリンクローカルなアドレスでなく、インターフェイス上のリンクローカルなアドレスを使用するように指定します。 • インターフェイスに IPv6 リンクローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。 （注） インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。 • **show interface** *interface-id* • **show ip interface** *interface-id* • **show ipv6 interface** *interface-id*	入力を確認します。
ステップ 10	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

デフォルト ルータ プリファレンスの設定（CLI）

ルータ アドバタイズメント（RA）メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドによって設定される DRP とともに送信されます。DRP が設定されていない場合は、RA は中小規模のプリファレンスとともに送信されます。

リンク上の2つのルータが等価ではあっても、等コストではないルーティングを提供する可能性がある場合、およびポリシーでホストがいずれかのルータを選択するよう指示された場合は、DRP が有効です。

IPv6 の DRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

インターフェイス上のルータに DRP を設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始して、DRP を指定するレイヤ 3 インターフェイスを特定します。
ステップ 3	**ipv6 nd router-preference** {**high** | **medium** | **low**} 例： `Device(config-if)# ipv6 nd router-preference medium`	スイッチ インターフェイス上のルータに DRP を指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**showipv6interface** 例：	設定を確認します。

	コマンドまたはアクション	目的
	`Device# show ipv6 interface`	
ステップ 6	**copyrunning-configstartup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 ICMP レート制限の設定（CLI）

ICMP レート制限はデフォルトでイネーブルです。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルト バケット サイズ（バケットに格納される最大トークン数）は 10 です。

ICMP レート制限パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 icmp error-interval** *interval* [*bucketsize*] 例： `Device(config)# ipv6 icmp error-interval 50 20`	IPv6 ICMP エラー メッセージの間隔とバケット サイズを設定します。 • *interval*：バケットに追加されるトークンの間隔（ミリ秒）。指定できる範囲は 0 ～ 2147483647 ミリ秒です。 • *bucketsize*：（任意）バケットに格納される最大トークン数。指定できる範囲は 1 ～ 200 です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**show ipv6 interface** [*interface-id*] 例： `Device# show ipv6 interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 5	**copyrunning-configstartup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 の CEF および dCEF の設定

シスコ エクスプレス フォワーディング（CEF）は、ネットワーク パフォーマンスを最適化するためのレイヤ 3 IP スイッチング テクノロジーです。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に振り分けることができます。スイッチ スタックでは、ハードウェアによって distributed CEF（dCEF）が使用されます。IPv4 CEF および dCEF はデフォルトでイネーブルです。IPv6 CEF および dCEF はデフォルトでディセーブルですが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ルーティングが設定されていない場合は、IPv6 CEF および dCEF は自動的にディセーブルになります。IPv6 CEF および dCEF は、設定中にディセーブルにできません。IPv6 ステータスを確認するには、**show ipv6 cef** 特権 EXEC コマンドを入力します。

IPv6 ユニキャスト パケットをルーティングするには、最初に **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して、IPv6 ユニキャスト パケットの転送をグローバルに設定してから、**ipv6 address** インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイスに IPv6 アドレスおよび IPv6 処理を設定する必要があります。

CEF および dCEF の設定に関する詳細情報については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のスタティック ルーティングの設定（CLI）

スタティック IPv6 ルートを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、インターフェイスに IPv6 アドレスを設定して少なくとも 1 つのレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

スタティック IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*] 例： `Device(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130`	スタティック IPv6 ルートを設定します。 • *ipv6-prefix*：スタティック ルートの宛先となる IPv6 ネットワーク。スタティック ホスト ルートを設定する場合は、ホスト名も設定できます。 • */prefix length*：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。 • *ipv6-address*：指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。ネクスト ホップの IPv6 アドレスを直接接続する必要はありません。再帰処理が実行されて、直接接続されたネクスト ホップの IPv6 アドレスが検出されます。このアドレスは RFC 2373 に記載された形式（16 ビット値を使用したコロン区切りの 16 進表記で指定）で設定する必要があります。 • *interface-id*：Point-To-Point（ポイントツーポイント）インターフェイスおよびブロードキャスト インターフェイスからのダイレクト スタティック ルートを指定します。ポイントツーポイント インターフェイスの場合、ネクスト ホップの

	コマンドまたはアクション	目的
		IPv6 アドレスを指定する必要はありません。ブロードキャスト インターフェイスの場合は、常にネクスト ホップの IPv6 アドレスを指定するか、または指定したプレフィックスをリンクに割り当てて、リンクに対してローカルなアドレスをネクスト ホップとして指定する必要があります。パケットの送信先となるネクスト ホップの IPv6 アドレスを指定することもできます。 （注） リンクに対してローカルなアドレスをネクスト ホップとして使用する場合は、*interface-id* を指定する必要があります（リンクに対してローカルなネクスト ホップを隣接ルータに設定する必要もあります）。 • *administrative distance*：（任意）アドミニストレーティブ ディスタンス。指定できる範囲は 1 ～ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルート タイプよりも、スタティック ルートが優先します。フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスを使用します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	次のいずれかを使用します。 • **show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface**	IPv6 ルーティング テーブルの内容を表示して、設定を確認します。 • **interface** *interface-id*：（任意）出力インターフェイスとして指定された

	コマンドまたはアクション	目的

	interface-id] [**detail**]][**recursive**] [**detail**]
	• **show ipv6 route static** [*updated*]
	例：
	`Device# show ipv6 static 2001:0DB8::/32 interface gigabitethernet2/0/1`
	または
	`Device# show ipv6 route static`
		インターフェイスを含むスタティック ルートのみを表示します。
		• **recursive**：（任意）再帰スタティック ルートのみを表示します。**recursive** キーワードは **interface** キーワードと相互に排他的です。ただし、コマンド構文に IPv6 プレフィックスが指定されているかどうかに関係なく、使用することができます。
		• **detail**：（任意）次に示す追加情報を表示します。
		• 有効な再帰ルートの場合、出力パス セットおよび最大分解深度
		• 無効なルートの場合、ルートが無効な理由

ステップ 5	**copyrunning-configstartup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

RIP for IPv6 の設定（CLI）

IPv6 RIP を実行するようにスイッチを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにして、IPv6 RIP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

IPv6 の RIP ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**ipv6 router rip** *name* 例： `Device(config)# ipv6 router rip cisco`	IPv6 RIP ルーティング プロセスを設定し、このプロセスに対してルータ コンフィギュレーション モードを開始します。
ステップ 3	**maximum-paths** *number-paths* 例： `Device(config-router)# maximum-paths 6`	（任意）IPv6 RIP がサポートできる等コストルートの最大数を定義します。指定できる範囲は 1 ～ 32 で、デフォルトは 16 ルートです。
ステップ 4	**exit** 例： `Device(config-router)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 6	**ipv6 rip** *name***enable** 例： `Device(config-if)# ipv6 rip cisco enable`	指定された IPv6 RIP ルーティング プロセスをインターフェイス上でイネーブルにします。
ステップ 7	**ipv6 rip** *name***default-information** {**only** | **originate**} 例： `Device(config-if)# ipv6 rip cisco`	（任意）IPv6 デフォルト ルート（::/0）を RIP ルーティング プロセス アップデートに格納して、指定インターフェイスから送信します。

	コマンドまたはアクション	目的
	default-information only	（注） 任意のインターフェイスから IPv6 デフォルト ルート（::/0）を送信したあとに、ルーティングループが発生しないようにするために、ルーティングプロセスは任意のインターフェイスで受信したすべてのデフォルトルートを無視します。 • **only**：このインターフェイスから送信するアップデートに、デフォルトルートを格納し、その他のすべてのルートを含めない場合に選択します。 • **originate**：このインターフェイスから送信するアップデートに、デフォルトルートおよびその他のすべてのルートを格納する場合に選択します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 9	次のいずれかを使用します。
	• **show ipv6 rip** [*name*] [**interface***interface-id*] [**database**] [**next-hops**]
	• **show ipv6 rip**
	例：
	`Device# show ipv6 rip cisco interface gigabitethernet2/0/1`
	または
	`Device# show ipv6 rip`
		• 現在の IPv6 RIP プロセスに関する情報を表示します。
		• IPv6 ルーティングテーブルの現在の内容を表示します。

ステップ 10	**copyrunning-configstartup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーションファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

OSPF for IPv6 の設定（CLI）

ネットワークでは、IPv6 の OSPF をカスタマイズできます。ただし、IPv6 の OSPF のデフォルト設定は、ほとんどのカスタマーおよび機能の要件を満たします。

次の注意事項に従ってください。

- IPv6 コマンドのデフォルト設定を変更する場合は注意してください。デフォルト設定を変更すると、IPv6 ネットワークの OSPF に悪影響が及ぶことがあります。
- インターフェイスで IPv6 OSPF をイネーブルにする前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 OSPF をイネーブルにするレイヤ 3 インターフェイスで IPv6 をイネーブルにする必要があります。

IPv6 の OSPF ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPF for IPv6」の章を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router ospf** *process-id* 例： `Device(config)# ipv6 router ospf 21`	プロセスに対して OSPF ルータ コンフィギュレーションモードをイネーブルにします。プロセス ID は、IPv6 OSPF ルーティング プロセスをイネーブルにする場合に管理上割り当てられる番号です。この ID はローカルに割り当てられ、1 ～ 65535 の正の整数を指定できます。
ステップ 3	**area** *area-id* **range** {*ipv6-prefix/prefix length*} [**advertise** | **not-advertise**] [**cost** *cost*] 例： `Device(config)# area .3 range`	（任意）エリア境界でルートを統合および集約します。 • *area-id*：ルートをサマライズするエリアの ID。10 進数または IPv6

	コマンドまたはアクション	目的
	`2001:0DB8::/32 not-advertise`	プレフィックスのどちらかを指定できます。 • *ipv6-prefix/prefix length*：宛先 IPv6 ネットワーク、およびプレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進数。10 進値の前にスラッシュ（/）を付加する必要があります。 • **advertise**：（任意）アドバタイズするアドレス範囲ステータスを設定し、タイプ 3 のサマリー リンク ステート アドバタイズメント（LSA）を生成します。 • **not-advertise**：（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。Type3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。 • **cost** *cost*：（任意）現在のサマリー ルートのメトリックまたはコストを設定します。宛先への最短パスを判別する場合に、OSPF SPF 計算で使用します。指定できる値は 0 ～ 16777215 です。
ステップ 4	**maximum paths** *number-paths* 例： `Device(config)# maximum paths 16`	（任意）IPv6 OSPF がルーティング テーブルに入力する必要がある、同じ宛先への等コストルートの最大数を定義します。指定できる範囲は 1 ～ 32 で、デフォルトは 16 です。
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 7	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*] 例： `Device(config-if)# ipv6 ospf 21 area .3`	インターフェイスで IPv6 の OSPF をイネーブルにします。 • **instance** *instance-id*：（任意）インスタンス ID。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 9	次のいずれかを使用します。
	• **show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-id*]
	• **show ipv6 ospf** [*process-id*] [*area-id*]
	例：
	`Device# show ipv6 ospf 21 interface gigabitethernet2/0/1`
	または
	`Device# show ipv6 ospf 21`
		• OSPF インターフェイスに関する情報を表示します。
		• OSPF ルーティング プロセスに関する一般情報を表示します。

ステップ 10	**copyrunning-configstartup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

IPv6 の EIGRP の設定

IPv6 EIGRP を実行するようにスイッチを設定する前に、 **ip routing global configuration** グローバル コンフィギュレーション コマンドを入力してルーティングをイネーブルにし、**ipv6**

unicast-routing global グローバル コンフィギュレーション コマンドを入力して IPv6 パケットの転送をイネーブルにして、IPv6 EIGRP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにします。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定済みのルータ ID を確認してから、**router-id** コマンドを使用します。

EIGRP IPv4 の場合と同様に、EIGRPv6 を使用して EIGRP IPv6 インターフェイスを指定し、これらのサブセットを受動インターフェイスとして選択できます。**passive-interface** コマンドを使用してインターフェイスをパッシブに設定してから、選択したインターフェイスで **no passive-interface** コマンドを使用してこれらのインターフェイスをアクティブにします。受動インターフェイスでは、EIGRP IPv6 を設定する必要がありません。

設定手順の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 ユニキャスト リバース パス転送の設定

ユニキャスト リバース パス転送（ユニキャスト RPF）機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造（スプーフィングされた）送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。たとえば、Smurf や Tribal Flood Network（TFN）など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタすることを攻撃者が阻止できるようにします。パブリック アクセスを提供するインターネット サービス プロバイダー（ISP）の場合、uRPF が IP ルーティング テーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、そのような攻撃をそらします。この処理により、ISP のネットワーク、その顧客、および残りのインターネットが保護されます。

- ユニキャスト RPF は、IP サービスでのみでサポートされます。
- スイッチが複数のスイッチ タイプが混在する混合ハードウェア スタック内にある場合は、ユニキャスト RPF を設定しないでください。

IP ユニキャスト RPF 設定の詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「*Other Security Features*」の章を参照してください。

IPv6 の表示

次のコマンドの構文および使用方法の詳細については、Cisco IOS のコマンド リファレンスを参照してください。

表 *20 : IPv6* をモニタリングするコマンド

コマンド	目的
show ipv6 access-list	アクセス リストのサマリーを表示します。

コマンド	目的
show ipv6 cef	IPv6 の Cisco エクスプレス フォワーディングを表示します。
show ipv6 interface*interface-id*	IPv6 インターフェイスのステータスと設定を表示します。
show ipv6 mtu	宛先キャッシュごとに IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュ エントリを表示します。
show ipv6 ospf	IPv6 OSPF 情報を表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 protocols	スイッチの IPv6 ルーティング プロトコルのリストを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 route	IPv6 ルートテーブルエントリを表示します。
show ipv6 routers	ローカル IPv6 ルータを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 ***21 : EIGRP IPv6*** 情報を表示するためのコマンド

コマンド	目的
show ipv6 eigrp [*as-number*] *interface*	EIGRP IPv6 用に設定されたインターフェイスの情報を表示します。
show ipv6 eigrp [*as-number*] *neighbor*	EIGRP IPv6 で検出されたネイバーを表示します。
show ipv6 interface[*as-number*] *traffic*	送受信される EIGRP IPv6 パケット数を表示します。

コマンド	目的
show ipv6 eigrptopology [*as-number* | *ipv6-address*] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors** | **Base**]	IPv6 トポロジテーブルの EIGRP エントリを表示します。

DHCP for IPv6 アドレス割り当ての設定

この項では、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 クライアント、サーバ、またはリレー エージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」の章を参照してください。

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトで、DHCPv6 機能はスイッチに設定されています。

DHCPv6 アドレス割り当ての設定時の注意事項

DHCPv6 アドレス割り当てを設定する場合は、次の注意事項に従ってください。

- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイス上でイネーブルである必要があります。
  - SVI：**interface vlan** *vlan_id* コマンドを使用して作成された VLAN インターフェイスです。
  - レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel port-channel-number** コマンドを使用して作成されたポートチャネル論理インターフェイス。
- スイッチは、DHCPv6 クライアント、サーバ、またはリレーエージェントとして動作できます。DHCPv6 クライアント、サーバ、およびリレー機能は、インターフェイスで相互に排他的です。
- DHCPv6 クライアント、サーバ、またはリレー エージェントは、マスター スイッチ上でだけ稼働します。スタック マスターの再選出があった場合、新しいマスター スイッチは DHCPv6 設定を維持します。ただし、DHCP サーバ データベース リース情報のローカルの RAM コピーは、維持されません。

DHCPv6 サーバ機能のイネーブル化（CLI）

DHCPv6 プールの特性を変更するには、**no** 形式の DHCP プール コンフィギュレーション モード コマンドを使用します。インターフェイスに対して DHCPv6 サーバ機能をディセーブルに

するには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスで DHCPv6 サーバをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 dhcp pool** *poolname* 例： `Device(config)# ipv6 dhcp pool 7`	DHCP プール コンフィギュレーション モードを開始して、IPv6 DHCP プールの名前を定義します。プール名は、記号文字列（Engineering など）または整数（0 など）です。
ステップ 3	**address prefix** *IPv6-prefix* {**lifetime**} {*t1 t1* | **infinite**} 例： `Device(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime 3600`	（任意）アドレス割り当て用のアドレス プレフィックスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 **lifetime** *t1 t1*：IPv6 アドレス プレフィックスが有効な状態を維持するタイムインターバル（秒）を指定します。指定できる範囲は 5 ～ 4294967295 秒です。間隔を指定しない場合は、**infinite** を指定します。
ステップ 4	**link-address** *IPv6-prefix* 例： `Device(config-dhcpv6)# link-address 2001:1002::0/64`	（任意）link-address IPv6 プレフィックスを指定します。 着信インターフェイス上のアドレスまたはパケットのリンクアドレスが指定した IPv6 プレフィックスに一致する場合、サーバは設定情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

	コマンドまたはアクション	目的
ステップ 5	**vendor-specific** *vendor-id* 例： `Device(config-dhcpv6)# vendor-specific 9`	（任意）ベンダー固有のコンフィギュレーション モードを開始して、ベンダー固有のID番号を指定します。この番号は、ベンダーの IANA プライベートエンタープライズ番号です。指定できる範囲は 1 ～ 4294967295 です。
ステップ 6	**suboption** *number* {**address** *IPv6-address* | **ascii** *ASCII-string* | **hex** *hex-string*} 例： `Device(config-dhcpv6-vs)# suboption 1 address 1000:235D::`	（任意）ベンダー固有のサブオプション番号を入力します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプションパラメータで定義されているように入力します。
ステップ 7	**exit** 例： `Device(config-dhcpv6-vs)# exit`	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 8	**exit** 例： `Device(config-dhcpv6)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するインターフェイスを指定します。
ステップ 10	**ipv6dhcpserver** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**] 例： `Device(config-if)# ipv6 dhcp server automatic`	インターフェイスに対して DHCPv6 サーバ機能をイネーブルにします。 • *poolname*：（任意）IPv6 DHCP プールのユーザ定義の名前。プール名は、記号文字列（Engineering など）または整数（0 など）です。 • **automatic**：（任意）サーバが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。

	コマンドまたはアクション	目的
		• **rapid-commit**：（任意）2つのメッセージを交換する方式を許可します。 • **preference** 値：（任意）サーバによって送信されるアドバタイズメントメッセージ内のプリファレンスオプションで指定するプリファレンス値を設定します。有効な範囲は 0 ～ 255 です。デフォルトのプリファレンス値は 0 です。 • **allow-hint**：（任意）サーバが SOLICIT メッセージに含まれるクライアントの提案を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントのヒントを無視します。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 12	次のいずれかを実行します。
	• **show ipv6 dhcp pool**
	• **show ipv6 dhcp interface**
	例：
	`Device# show ipv6 dhcp pool`
	または
	`Device# show ipv6 dhcp interface`
		• DHCPv6 プール設定を確認します。
		• DHCPv6 サーバ機能がインターフェイス上でイネーブルであることを確認します。

ステップ 13	**copyrunning-configstartup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

DHCPv6 クライアント機能のイネーブル化（CLI）

このタスクでは、インターフェイスに対してDHCPv6クライアントをイネーブルにする方法を説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイスコンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ipv6 address dhcp** [**rapid-commit**] 例： `Device(config-if)# ipv6 address dhcp rapid-commit`	インターフェイスで DHCPv6 サーバから IPv6 アドレスを取得できるようにします。 **rapid-commit**：（任意）アドレス割り当てに2つのメッセージを交換する方式を許可します。
ステップ 4	**ipv6 dhcp client request** [**vendor-specific**] 例： `Device(config-if)# ipv6 dhcp client request vendor-specific`	（任意）インターフェイスでベンダー固有のオプションを要求できるようにします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showipv6dhcpinterface** 例： `Device# show ipv6 dhcp interface`	DHCPv6クライアントがインターフェイスでイネーブルになっていることを確認します。

IPv6 ユニキャスト ルーティングの設定例

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化：例

次に、IPv6 プレフィックス 2001:0DB8:c18:1::/64 に基づく、リンクに対してローカルなアドレスおよびグローバル アドレスを使用して、IPv6 をイネーブルにする例を示します。EUI-64 インターフェイス ID が、両方のアドレスの下位 64 ビットで使用されます。**show ipv6 interface** EXEC コマンドの出力は、インターフェイスのリンクに対してローカルなプレフィックス FE80::/64 にインターフェイス ID（20B:46FF:FE2F:D940）を付加する方法を示すために追加されています。

```
Device(config)# ipv6 unicast-routing
Device(config)# interface gigabitethernet1/0/11
Device(config-if)# no switchport
Device(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Device(config-if)# end
Device# show ipv6 interface gigabitethernet1/0/11
GigabitEthernet1/0/11 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

デフォルト ルータ プリファレンスの設定：例

次に、インターフェイス上のルータに高い DRP を設定する例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 nd router-preference high
Device(config-if)# end
```

IPv4 および IPv6 プロトコル スタックの設定：例

次に、インターフェイス上で IPv4 および IPv6 ルーティングをイネーブルにする例を示します。

```
Device(config)# ip routing
Device(config)# ipv6 unicast-routing
Device(config)# interface fastethernet1/0/11
Device(config-if)# no switchport
Device(config-if)# ip address 192.168.99.1 255.255.255.0
Device(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Device(config-if)# end
```

DHCPv6 サーバ機能のイネーブル化：例

次の例では、*engineering* という IPv6 アドレス プレフィックスを持つプールを設定する方法を示します。

```
Device# configure terminal
Device(config)# ipv6 dhcp pool engineering
Device(config-dhcpv6)#address prefix 2001:1000::0/64
Device(config-dhcpv6)# end
```

次に、3 リンクアドレスおよび IPv6 アドレス プレフィックスを持つ *testgroup* と呼ばれるプールを設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 dhcp pool testgroup
Device(config-dhcpv6)# link-address 2001:1001::0/64
Device(config-dhcpv6)# link-address 2001:1002::0/64
Device(config-dhcpv6)# link-address 2001:2000::0/48
Device(config-dhcpv6)# address prefix 2001:1003::0/64
Device(config-dhcpv6)# end
```

次の例では、*350* というベンダー固有オプションを持つプールを設定する方法を示します。

```
Device# configure terminal
Device(config)# ipv6 dhcp pool 350
Device(config-dhcpv6)# address prefix 2001:1005::0/48
Device(config-dhcpv6)# vendor-specific 9
Device(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Device(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Device(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能のイネーブル化：例

次に、IPv6 アドレスを取得して、rapid-commit オプションをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# ipv6 address dhcp rapid-commit
```

IPv6 ICMP レート制限の設定：例

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
Device(config)#ipv6 icmp error-interval 50 20
```

IPv6 のスタティック ルーティングの設定：例

次に、アドミニストレーティブ ディスタンスが 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
Device(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130
```

IPv6 の RIP の設定：例

次に、最大 8 の等コスト ルートにより RIP ルーティング プロセス *cisco* をイネーブルにし、インターフェイス上でこれをイネーブルにする例を示します。

```
Device(config)# ipv6 router rip cisco
Device(config-router)# maximum-paths 8
Device(config)# exit
Device(config)# interface gigabitethernet2/0/11
Device(config-if)# ipv6 rip cisco enable
```

IPv6 の表示：例

次に、**show ipv6 interface** 特権 EXEC コマンドの出力例を示します。

```
Device# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

```
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
<output truncated>
```

第 16 章

IPv6 マルチキャストの実装

- 機能情報の確認 （283 ページ）
- IPv6 マルチキャスト ルーティングの実装に関する情報 （283 ページ）
- IPv6 マルチキャストの実装 （293 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IPv6 マルチキャスト ルーティングの実装に関する情報

この章では、スイッチに IPv6 マルチキャスト ルーティングを実装する方法について説明します。

従来の IP 通信では、ホストはパケットを単一のホスト（ユニキャスト伝送）またはすべてのホスト（ブロードキャスト伝送）に送信できます。IPv6マルチキャストは、第三の方式を提供するものであり、ホストが単一のデータ ストリームをすべてのホストのサブセット（グループ伝送）に同時に送信できるようにします。

IPv6 マルチキャストの概要

IPv6 マルチキャスト グループは、特定のデータ ストリームを受信する受信側の任意のグループです。このグループには、物理的境界または地理的境界はありません。受信側は、インターネット上または任意のプライベート ネットワーク内の任意の場所に配置できます。特定のグ

ループへのデータ フローの受信に関与する受信側は、ローカル スイッチに対してシグナリングすることによってそのグループに加入する必要があります。このシグナリングは、MLD プロトコルを使用して行われます。

スイッチは、MLD プロトコルを使用して、直接接続されているサブネットにグループのメンバが存在するかどうかを学習します。ホストは、MLD レポート メッセージを送信することによってマルチキャスト グループに加入します。ネットワークでは、各サブネットでマルチキャストデータのコピーを1つだけ使用して、潜在的に無制限の受信側にデータが伝送されます。トラフィックの受信を希望する IPv6 ホストはグループ メンバと呼ばれます。

グループ メンバに伝送されるパケットは、単一のマルチキャスト グループ アドレスによって識別されます。マルチキャスト パケットは、IPv6 ユニキャスト パケットと同様に、ベストエフォート型の信頼性を使用してグループに伝送されます。

マルチキャスト環境は、送信側と受信側で構成されます。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージをリッスンして受信できます。

マルチキャストアドレスがマルチキャストグループの受信先として選択されます。送信者は、データグラムの宛先アドレスとしてグループのすべてのメンバに到達するためにそのアドレスを使用します。

マルチキャストグループ内のメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。マルチキャストグループ内のメンバの場所または数に制約はありません。ホストは、一度に複数のマルチキャスト グループのメンバにすることができます。

マルチキャストグループがどの程度アクティブであるか、その期間、およびメンバーシップはグループおよび状況によって異なります。メンバを含むグループにアクティビティがない場合もあります。

IPv6 マルチキャスト ルーティングの実装

Cisco IOS ソフトウェアでは、IPv6 マルチキャスト ルーティングを実装するため、次のプロトコルがサポートされています。

- MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャスト アドレスを宛先としたマルチキャスト パケットを受信するために使用するノード）を検出するために IPv6 スイッチで使用されます。MLD には 2 つのバージョンがあります。MLD バージョン 1 はバージョン 2 のインターネット グループ管理プロトコル（IGMP）for IPv4 をベースとしています。MLD バージョン 2 はバージョン 3 の IGMP for IPv4 をベースとしています。Cisco IOS ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 と MLD バージョン 1 の両方が使用されます。MLD バージョン 2 は、MLD バージョン 1 と完全な下位互換性があります（RFC 2710 で規定）。MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているスイッチと相互運用します。MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。
- PIM-SM は、相互に転送されるマルチキャストパケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。

- PIM in Source Specific Multicast（PIM-SSM）はPIM-SMと類似していますが、IPマルチキャストアドレスを宛先とした特定の送信元アドレス（または特定の送信元アドレスを除くすべてのアドレス）からのパケットを受信する対象をレポートする機能を別途備えています。

IPv6 マルチキャスト リスナー ディスカバリ プロトコル

キャンパス ネットワークでマルチキャストの実装を開始するには、ユーザは最初に、誰がマルチキャストを受信するかを定義する必要があります。MLD プロトコルは、直接接続されているリンク上のマルチキャスト リスナー（たとえば、マルチキャスト パケットを受信するノード）の存在を検出するため、およびこれらのネイバー ノードを対象にしている特定のマルチキャスト アドレスを検出するために、IPv6 スイッチによって使用されます。これは、ローカル グループおよび送信元固有のグループ メンバーシップの検出に使用されます。

MLD プロトコルは、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャスト トラフィックのフローを自動的に制御および制限する手段を提供します。

マルチキャスト クエリアとマルチキャスト ホスト

マルチキャスト クエリアは、クエリー メッセージを送信して、特定のマルチキャスト グループのメンバーであるネットワーク デバイスを検出するネットワーク デバイス（スイッチなど）です。

マルチキャスト ホストは、受信側（スイッチを含む）としてレポート メッセージを送信し、クエリアにホスト メンバーシップを通知します。

同じ送信元からのマルチキャスト データ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは、MLD レポートを使用して、マルチキャスト グループに対する加入および脱退を行ったり、グループ トラフィックの受信を開始したりします。

MLD では、メッセージの伝送に インターネット制御メッセージ プロトコル（ICMP）が使用されます。すべての MLD メッセージはホップ制限が 1 のリンクローカルであり、すべてにスイッチ アラート オプションが設定されています。スイッチ アラート オプションは、ホップバイホップ オプション ヘッダーの実装を意味します。

MLD アクセス グループ

MLD アクセス グループは、Cisco IOS IPv6 マルチキャスト スイッチでの受信側アクセス コントロールを実現します。この機能では、受信側が加入できるグループのリストを制限し、SSM チャネルへの加入に使用される送信元を許可または拒否します。

受信側の明示的トラッキング

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、この機能により、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

Protocol Independent Multicast

PIM（Protocol Independent Multicast）は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。PIM は、ユニキャスト ルーティング プロトコルとは独立して動作し、他のプロトコルと同様に、マルチキャスト ルート アップデートの送受信を実行します。ユニキャスト ルーティング テーブルに値を入力するために LAN でどのユニキャスト ルーティング プロトコルが使用されているかどうかにかかわらず、Cisco IOS PIM では、独自のルーティング テーブルを構築および管理する代わりに、既存のユニキャスト テーブル コンテンツを使用して、Reverse Path Forwarding（RPF）チェックを実行します。

PIM-SM または PIM-SSM のいずれかを使用するように IPv6 マルチキャストを設定することも、ネットワークで PIM-SM と PIM-SSM の両方を使用することもできます。

PIM スパース モード

IPv6 マルチキャストでは、PIM-SM を使用したドメイン内マルチキャスト ルーティングがサポートされています。PIM-SM は、ユニキャスト ルーティングを使用して、マルチキャスト ツリー構築用のリバースパス情報を提供しますが、特定のユニキャスト ルーティング プロトコルには依存しません。

PIM-SM は、トラフィックに対して明示的な要求がある場合を除いて、各マルチキャストに関与しているスイッチの数が比較的少なく、これらのスイッチがグループのマルチキャスト パケットを転送しないときに、マルチキャストネットワークで使用されます。PIM-SMは、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SMは最初に共有ツリーを使用しますが、これにはRPの使用が必要となります。

要求は、ツリーのルート ノードに向けてホップバイホップで送信される PIM join を使用して行われます。PIM-SM のツリーのルート ノードは、共有ツリーの場合は RP、最短パス ツリー（SPT）の場合はマルチキャスト送信元に直接接続されているファーストホップ スイッチになります。RP はマルチキャスト グループを追跡し、マルチキャスト パケットを送信するホストはそのホストのファーストホップ スイッチによって RP に登録されます。

PIM join がツリーの上位方向に送信されると、要求されたマルチキャスト トラフィックがツリーの下位方向に転送されるように、パス上のスイッチがマルチキャスト転送ステートを設定します。マルチキャスト トラフィックが不要になったら、スイッチはルート ノードに向けてツリーの上位方向に PIM prune を送信し、不必要なトラフィックをプルーニング（削除）送信します。この PIM prune がホップごとにツリーを上位方向に移動する際、各スイッチはその転送状態を適切に更新します。最終的に、マルチキャスト グループまたは送信元に関連付けられている転送ステートは削除されます。

マルチキャスト データの送信側は、マルチキャスト グループを宛先としたデータを送信します。送信側の指定スイッチ（DR）は、これらのデータ パケットを受け取り、ユニキャストでカプセル化し、RPに直接送信します。RPは、カプセル化されたこれらのデータパケットを受信し、カプセル化を解除し、共有ツリー上に転送します。そのあと、パケットは、RP ツリー上のスイッチの（*, G）マルチキャスト ツリー ステートに従って、RP ツリー ブランチの任意の場所に複製され、そのマルチキャスト グループのすべての受信側に最終的に到達します。

RP へのデータ パケットのカプセル化のプロセスは登録と呼ばれ、カプセル化されたパケットは PIM レジスタ パケットと呼ばれます。

IPv6 BSR：RP マッピングの設定

ドメイン内の PIM スイッチは、各マルチキャスト グループを正しい RP アドレスにマッピングできる必要があります。PIM-SM 対応の BSR プロトコルは、グループと RP のマッピング情報をドメイン全体に迅速に配布するためのダイナミック適応メカニズムを備えています。IPv6 BSR 機能を使用すると、到達不能になった RP が検出され、マッピング テーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。

すべての PIM-SM マルチキャスト グループを RP の IP または IPv6 アドレスに関連付ける必要があります。新しいマルチキャスト送信側が送信を開始すると、そのローカル DR がこれらのデータ パケットを PIM register メッセージにカプセル化し、そのマルチキャスト グループの RP に送信します。新しいマルチキャスト受信側が加入すると、そのローカル DR がそのマルチキャスト グループの RP に PIM join メッセージを送信します。PIM スイッチは、（*, G）join メッセージを送信するとき、RP 方向への次のスイッチを認識して、G（グループ）がそのスイッチにメッセージを送信できるようにする必要があります。また、PIM スイッチは、（*, G）ステートを使用してデータ パケットを転送するとき、G を宛先としたパケットの正しい着信インターフェイスを認識する必要があります。これは、他のインターフェイスに着信するパケットを拒否する必要があるためです。

ドメイン内の少数のスイッチが候補ブートストラップ スイッチ（C-BSR）として設定され、単一の BSR がそのドメイン用に選択されます。また、ドメイン内の一連のスイッチが候補 RP（C-RP）として設定されます。通常、これらのスイッチは、C-BSR として設定されているものと同じスイッチです。候補 RP は、候補 RP アドバタイズメント（C-RP-Adv）メッセージをそのドメインの BSR に定期的にユニキャストし、RP になる意思をアドバタイズします。C-RP-Adv メッセージには、アドバタイズを行っている C-RP のアドレス、およびグループ アドレスとマスク長のフィールドの任意のリストが含まれています。これらのフィールドは、立候補のアドバタイズの対象となるグループ プレフィックスを示します。BSR は、定期的に発信するブートストラップ メッセージ（BSM）にこれらの一連の C-RP とそれに対応するグループ プレフィックスを含めます。BSM は、ドメイン全体にホップバイホップで配布されます。

双方向 BSR がサポートされているため、双方向 RP を C-RP メッセージおよび BSM の双方向範囲でアドバタイズできます。システム内のすべてのスイッチは、BSM で双方向範囲を使用できる必要があります。使用できない場合は、双方向 RP 機能が機能しません。

PIM-Source Specific Multicast (PIM-SSM)

PIM-SSM は、SSM の実装をサポートするルーティング プロトコルであり、PIM-SM から派生したものです。ただし、PIM-SM では PIM join を受けてすべてのマルチキャスト送信元からデータが送信されるのに対し、SSM機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラム トラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネット ブロードキャスト トラフィックが拒否されます。さらに、SSM では、RP と共有ツリーを使用する代わりに、マルチキャスト グループの送信元アドレスで見つかった情報を使用します。この情報は、MLD メンバーシップ レポートによっ

てラストホップ スイッチにリレーされる送信元アドレスを通して受信側から提供されます。その結果として、送信元に直接つながる最短パス ツリーが得られます。

SSM では、データグラムは（S, G）チャネルに基づいて配信されます。1 つの（S, G）チャネルのトラフィックは、IPv6 ユニキャスト送信元アドレス S とマルチキャスト グループ アドレス G を IPv6 宛先アドレスとして使用するデータグラムで構成されます。システムは、（S, G）チャネルのメンバになることによって、このトラフィックを受信します。シグナリングは不要ですが、受信側は特定の送信元からのトラフィックを受信する場合は（S, G）チャネルに加入し、トラフィックを受信しない場合はチャネルから脱退する必要があります。

SSM を動作させるには、MLD バージョン 2 が必要です。MLD を使用すると、ホストが送信元の情報を提供できるようになります。MLD を使用して SSM を動作させるには、Cisco IOS IPv6 スイッチ、アプリケーションが実行されているホスト、およびアプリケーション自体で SSM がサポートされている必要があります。

ルーティング可能アドレスの hello オプション

IPv6 内部ゲートウェイ プロトコルを使用してユニキャスト ルーティング テーブルを構築する場合、アップストリーム スイッチ アドレスを検出するための手順では、PIM ネイバーとネクストホップ スイッチが同じスイッチを表しているかぎり、これらのアドレスは常に同じであるものと想定されます。ただし、スイッチがリンク上に複数のアドレスを持つ場合は、このことが当てはまるとはかぎりません。

この状況は IPv6 において、2 つの一般的な状況で発生することがあります。1 つめの状況は、ユニキャスト ルーティング テーブルが IPv6 内部ゲートウェイ プロトコル（マルチキャスト BGP など）によって構築されない場合に発生します。2 つめの状況は、RP のアドレスがダウンストリーム スイッチとサブネット プレフィックスを共有している場合に発生します（RP スイッチ アドレスはドメインワイドにする必要があるため、リンクローカル アドレスにはできないことに注意してください）。

ルーティング可能アドレスの hello オプションによって、PIM プロトコルでこのような状況を回避できます。このためには、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージ オプションを追加します。PIM スイッチが何らかのアドレスのアップストリーム スイッチを検出すると、RPF 計算の結果は、PIM ネイバーのアドレス自体に加えて、このオプションのアドレスとも比較されます。このオプションにはそのリンク上の PIM スイッチの考えられるアドレスがすべて含まれているため、対象の PIM スイッチがこのオプションをサポートしている場合、常に RPF 計算の結果が含まれます。

PIM メッセージにサイズ制限があることと、ルーティング可能アドレスの hello オプションが単一の PIM hello メッセージ内に収まる必要があるため、インターフェイスで設定できるアドレスの制限は 16 個になっています。

PIM IPv6 スタブ ルーティング

PIM スタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動し、リソースの利用率を軽減します。

PIM スタブ ルーティングを使用するネットワークでは、ユーザに対する IPv6 トラフィックの唯一の許容ルートは、PIM スタブ ルーティングを設定しているスイッチ経由です。PIM 受動

インターフェイスは、VLAN などのレイヤ 2 アクセス ドメイン、または他のレイヤ 2 デバイスに接続されているインターフェイスに接続されます。直接接続されたマルチキャスト レシーバおよび送信元のみが、レイヤ 2 アクセス ドメインで許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

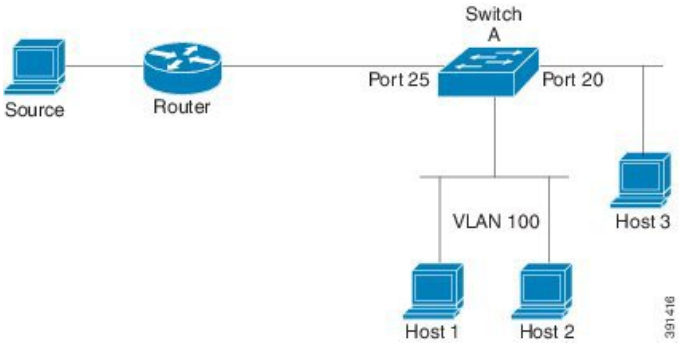
PIM スタブ ルーティングを使用しているときは、IPv6 マルチキャスト ルーティングを使用し、スイッチだけを PIM スタブ ルータとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。スイッチは分散ルータ間の伝送トラフィックをルーティングしません。スイッチのルーテッドアップリンク ポートも設定する必要があります。SVI の場合は、スイッチのアップリンク ポートを使用できません。

また、PIM スタブ ルーティングをスイッチに設定するときは、EIGRP スタブ ルーティングも設定する必要があります。詳細については、EIGRPv6 スタブ ルーティング （251 ページ）を参照してください。

冗長 PIM スタブ ルータ トポロジーはサポートされません。単一のアクセス ドメインにマルチキャスト トラフィックを転送している複数の PIM ルータがある場合、冗長トポロジーが存在します。PIM メッセージはブロックされ、PIM アサートおよび指定されたルータ選出メカニズムは PIM 受動インターフェイスではサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけがサポートされます。非冗長トポロジーを使用することで、PIM 受動インターフェイスはそのアクセス ドメインで唯一のインターフェイスおよび指定ルータであると想定します。

次に示す図では、スイッチ A ルーテッドアップリンク ポート 25 がルータに接続され、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。この設定により、直接接続されたホストはマルチキャスト発信元からトラフィックを受信できます。詳細については、PIM IPv6 スタブ ルーティングの設定 （303 ページ）を参照してください。

図 *9 : PIM* スタブ ルータ設定



スタティック mroute

IPv6 スタティック mroute は、RPF チェックを変化させるために使用する IPv4 スタティック mroute とほぼ同様に動作します。IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、RPF チェックに対するスタティック ルート サポートを拡張するこ

とによって実装されます。スタティック mroute では、等コスト マルチパス mroute がサポートされています。また、ユニキャスト専用スタティック ルートもサポートされています。

MRIB

マルチキャストルーティング情報ベース（MRIB）は、マルチキャストルーティングプロトコル（ルーティング クライアント）によってインスタンス化されるマルチキャスト ルーティング エントリのプロトコル非依存リポジトリです。その主要機能は、ルーティング プロトコルとマルチキャスト転送情報ベース（MFIB）間の非依存性を実現することです。また、クライアント間の調整および通信ポイントとしても機能します。

ルーティング クライアントは、MRIB が提供するサービスを使用して、ルーティング エントリをインスタンス化し、他のクライアントによってルーティングエントリに加えられた変更を取得します。MRIB では、ルーティング クライアント以外に、転送クライアント（MFIB インスタンス）や特別なクライアント（MLD など）も扱われます。MFIB は、MRIB からその転送エントリを取得し、パケットの受信に関連するイベントについてMRIBに通知します。これらの通知は、ルーティング クライアントによって明示的に要求されることも、MFIB によって自発的に生成されることもあります。

MRIB のもう 1 つの重要な機能は、同じマルチキャスト セッション内でマルチキャスト接続を確立する際に、複数のルーティング クライアントの調整を可能にすることです。また、MRIB では、MLD とルーティング プロトコル間の調整も可能です。

MFIB

MFIB は、IPv6 ソフトウェア用のプラットフォーム非依存およびルーティング プロトコル非依存ライブラリです。その主な目的は、転送テーブルが変更されたときに、Cisco IOS プラットフォームに、IPv6 マルチキャスト転送テーブルおよび通知を読み取るインターフェイスを提供することです。MFIB が提供する情報には、明確に定義された転送セマンティクスが含まれています。この情報は、プラットフォームが特定のハードウェアまたはソフトウェア転送メカニズムに容易に変換できる設計になっています。

ネットワーク内でルーティングまたはトポロジが変更されると、IPv6 ルーティング テーブルがアップデートされ、これらの変更が MFIB に反映されます。MFIB は、IPv6 ルーティング テーブル内の情報に基づいて、ネクストホップ アドレス情報を管理します。MFIB エントリとルーティング テーブル エントリの間には 1 対 1 の相互関係があるため、MFIB には既知のすべてのルートが含まれ、高速スイッチングや最適スイッチングなどのスイッチング パスに関連付けられているルート キャッシュ管理の必要がなくなります。

MFIB

（注） 分散 MFIB は、マスターが他のスタック メンバーに MFIB 情報を配布するスタック環境でのみ意味を持ちます。次のセクションでは、ラインカードは単にスタックのメンバー スイッチです。

MFIB（MFIB）は、分散型プラットフォーム上でマルチキャスト IPv6 パケットをスイッチングするために使用されます。また、MFIB には、ラインカード間での複製に関するプラットフォーム固有の情報も含まれることがあります。転送ロジックのコアを実装する基本 MFIB ルーチンは、すべての転送環境に共通です。

MFIB は、次の機能を実装します。

- ラインカードで生成されたデータ駆動型プロトコル イベントを PIM にリレーします。
- MFIB プラットフォーム アプリケーション プログラム インターフェイス（API）を提供し、ハードウェア アクセラレーション エンジンのプログラミングを担っている、プラットフォーム固有のコードに MFIB の変更を伝播します。また、この API には、ソフトウェアでパケットをスイッチングしたり（パケットがデータ駆動型イベントのトリガーとなっている場合に必要）、ソフトウェアにトラフィックの統計情報をアップロードしたりするエントリ ポイントも含まれています。

また、MFIB および MRIB サブシステムを組み合わせて使用すると、スイッチが各ラインカードでMFIBデータベースの「カスタマイズ」コピーを保有したり、MFIB関連のプラットフォーム固有の情報を RP からラインカードに転送したりできるようになります。

IPv6マルチキャストのプロセス スイッチングおよび高速スイッチング

統合 MFIB は、IPv6 マルチキャストでの PIM-SM および PIM-SSM に対するファスト スイッチングおよびプロセス スイッチングの両サポートを提供するために使用されます。プロセス スイッチングでは、の IOS デーモンが各パケットの調査、書き換え、および転送を行う必要があります。最初にパケットが受信され、システム メモリにコピーされます。次に、スイッチがルーティング テーブル内でレイヤ 3 ネットワーク アドレスを検索します。そのあと、レイヤ 2 フレームがネクストホップの宛先アドレスで書き換えられ、発信インターフェイスに送信されます。また、IOSd は、巡回冗長検査（CRC）も計算します。このスイッチング方式は、IPv6 パケットをスイッチングする方式の中でスケーラビリティが最も低い方式です。

IPv6 マルチキャストの高速スイッチングを使用すると、スイッチは、プロセス スイッチングよりも高いパケット転送パフォーマンスを実現できます。従来ルート キャッシュに格納される情報は、IPv6 マルチキャスト スイッチング用にいくつかのデータ構造に格納されます。これらのデータ構造では、ルックアップが最適化され、パケット転送を効率的に行えるようになっています。

IPv6 マルチキャスト転送では、PIM プロトコル ロジックで許可されていれば、最初のパケットのファスト スイッチングが行われます。IPv6 マルチキャストの高速スイッチングでは、MAC カプセル化ヘッダーが事前に計算されます。IPv6 マルチキャストの高速スイッチングでは、MFIB を使用して、IPv6 送信先プレフィックス ベースのスイッチング判定が行われます。IPv6 マルチキャストの高速スイッチングでは、MFIB に加えて、隣接関係テーブルを使用して、レイヤ 2 アドレッシング情報が付加されます。隣接関係テーブルでは、すべての MFIB エントリのレイヤ 2 ネクストホップ アドレスが管理されます。

隣接が検出されると、隣接関係テーブルにそのデータが入力されます。（ARP などを使用して）隣接エントリが作成されるたびに、その隣接ノードのリンク層ヘッダーが事前に計算され、隣接関係テーブルに格納されます。ルートが決定されると、そのヘッダーはネクスト ホッ

プおよび対応する隣接エントリを指します。そのあと、そのヘッダーはパケット スイッチング時のカプセル化に使用されます。

ロード バランシングと冗長性の両方に対応するようにスイッチが設定されている場合など、ルートには送信先プレフィックスへの複数のパスが存在することがあります。解決されたパスごとに、そのパスのネクストホップ インターフェイスに対応する隣接へのポインタが追加されます。このメカニズムは、複数のパスでのロード バランシングに使用されます。

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 機能では、マルチプロトコル BGP for IPv6 拡張を提供し、IPv4 BGP と同じ機能と機能性をサポートします。マルチキャスト BGP に対する IPv6 拡張には、IPv6 マルチキャスト アドレス ファミリ、ネットワーク層到達可能性情報（NLRI）、および IPv6 アドレスを使用するネクスト ホップ（宛先へのパス内の次のスイッチ）属性のサポートが含まれています。

マルチキャスト BGP は、ドメイン間 IPv6 マルチキャストの配布を可能にする、拡張された BGP です。マルチプロトコル BGP では、複数のネットワーク層プロトコル アドレス ファミリ（IPv6 アドレス ファミリなど）および IPv6 マルチキャスト ルートに関するルーティング情報を伝送します。IPv6 マルチキャスト アドレス ファミリには、IPv6 PIM プロトコルによる RPF ルックアップに使用される複数のルートが含まれており、マルチキャスト BGP IPv6 は、同じドメイン間転送を提供します。ユニキャスト BGP が学習したルートは IPv6 マルチキャストには使用されないため、ユーザは、BGP で IPv6 マルチキャストを使用する場合は、マルチプロトコル BGP for IPv6 マルチキャストを使用する必要があります。

マルチキャスト BGP 機能は、個別のアドレス ファミリ コンテキストを介して提供されます。Subsequent Address Family Identifier（SAFI）では、属性で伝送されるネットワーク層到達可能性情報のタイプに関する情報を提供します。マルチプロトコル BGP ユニキャストでは SAFI 1 メッセージを使用し、マルチプロトコル BGP マルチキャストでは SAFI 2 メッセージを使用します。SAFI 1 メッセージは、ルートは IP ユニキャストだけに使用でき、IP マルチキャストには使用できないことを示します。この機能があるため、IPv6 ユニキャスト RIB 内の BGP ルートは、IPv6 マルチキャスト RPF ルックアップでは無視される必要があります。

IPv6 マルチキャスト RPF ルックアップを使用して、異なるポリシーおよびトポロジ（IPv6 ユニキャストとマルチキャストなど）を設定するよう、個別の BGP ルーティング テーブルが維持されています。マルチキャスト RPF ルックアップは、IP ユニキャスト ルート ルックアップと非常によく似ています。

IPv6 マルチキャスト BGP テーブルと関連付けられている MRIB はありません。ただし、必要な場合、IPv6 マルチキャスト BGP は、ユニキャスト IPv6 RIB で動作します。マルチキャスト BGP では、IPv6 ユニキャスト RIB へのルートの挿入や更新は行いません。

IPv6 マルチキャストの実装

IPv6 マルチキャスト ルーティングのイネーブル化

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 multicast-routing** 例： `Device (config)# ipv6 multicast-routing`	すべての IPv6 対応インターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルになっているすべてのスイッチ インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにします。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD プロトコルのカスタマイズおよび確認

インターフェイスでの MLD のカスタマイズおよび確認

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* 例： `(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 3	**ipv6 mld join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]}	指定したグループおよび送信元に対して MLD レポートを設定します。

	コマンドまたはアクション	目的
	例： `(config-if) # ipv6 mld join-group FF04::10`	
ステップ 4	**ipv6 mld access-group** *access-list-name* 例： `(config-if) # ipv6 access-list acc-grp-1`	ユーザに IPv6 マルチキャストの受信側アクセスコントロールの実行を許可します。
ステップ 5	**ipv6 mld static-group** [*group-address*] [**include** | **exclude**] {*source-address* | source-list [*acl*]} 例： `(config-if) # ipv6 mld static-group ff04::10 include 100::1`	指定したインターフェイスにマルチキャストグループのトラフィックをスタティックに転送し、MLD ジョイナがインターフェイスに存在するかのようにインターフェイスが動作するようにします。
ステップ 6	**ipv6 mld query-max-response-time** *seconds* 例： `(config-if) # ipv6 mld query-max-response-time 20`	MLD キューにアドバタイズされる最大応答時間を設定します。
ステップ 7	**ipv6 mld query-timeout** *seconds* 例： `(config-if) # ipv6 mld query-timeout 130`	スイッチがインターフェイスのクエリアとして引き継ぐまでのタイムアウト値を設定します。
ステップ 8	**exit** 例： `(config-if) # exit`	このコマンドを 2 回入力して、インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードを開始します。
ステップ 9	**show ipv6 mldgroups [link-local]** [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**] 例： `# show ipv6 mld groups GigabitEthernet 1/0/1`	スイッチに直接接続されており、MLD を介して学習したマルチキャスト グループを表示します。

	コマンドまたはアクション	目的
ステップ 10	**show ipv6 mld groups summary** 例： `# show ipv6 mld groups summary`	MLD キャッシュに存在する (*, G) および (S, G) メンバーシップ レポートの番号を表示します。
ステップ 11	**show ipv6 mldinterface** [*type number*] 例： `# show ipv6 mld interface GigabitEthernet 1/0/1`	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 12	**debug ipv6 mld** [*group-name* | *group-address* | *interface-type*] 例： `# debug ipv6 mld`	MLD プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 13	**debug ipv6 mld explicit** [*group-name* | *group-address* 例： `# debug ipv6 mld explicit`	ホストの明示的トラッキングに関連する情報を表示します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD グループ制限の実装

インターフェイス単位の MLD 制限とグローバル MLD 制限は相互に独立して機能します。インターフェイス単位の MLD 制限とグローバル MLD 制限の両方を同じスイッチで設定できます。MLD 制限の数は、グローバルの場合もインターフェイス単位の場合も、デフォルトでは設定されません。ユーザが制限を設定する必要があります。インターフェイス単位のステート制限またはグローバル ステート制限を超えるメンバーシップ レポートは無視されます。

MLD グループ制限のグローバルな実装

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mld** [*vrf vrf-name*] **state-limit** *number* 例： `Device(config)# ipv6 mld state-limit 300`	MLD ステートの数をグローバルに制限します。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD グループ制限のインターフェイス単位での実装

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface type** *number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 mld limit** *number* [**except**]*access-list* 例： `Device(config-if)# ipv6 mld limit 100`	MLD ステートの数をインターフェイス単位で制限します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

受信側の明示的トラッキングによってホストの動作を追跡するための設定

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* 例： `(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 3	**ipv6 mld explicit-tracking** *access-list-name* 例： `(config-if)# ipv6 mld explicit-tracking list1`	ホストの明示的トラッキングをイネーブルにします。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD トラフィック カウンタのリセット

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mldtraffic** 例： `# clear ipv6 mld traffic`	すべての MLD トラフィック カウンタをリセットします。
ステップ 2	**show ipv6 mldtraffic** 例： `# show ipv6 mld traffic`	MLD トラフィック カウンタを表示します。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD インターフェイス カウンタのクリア

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mldcounters** *interface-type* 例： `# clear ipv6 mld counters Ethernet1/0`	MLD インターフェイス カウンタをクリアします。
ステップ 2	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM の設定

ここでは、PIM の設定方法について説明します。

PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 pim **rp-address** *ipv6-address*[*group-access-list*] 例： `(config) # ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C acc-grp-1`	特定のグループ範囲の PIM RP のアドレスを設定します。
ステップ 3	**exit** 例： `(config) # exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権EXEC モードに戻します。
ステップ 4	**show ipv6 piminterface** [state-on] [**state-off**] [*type-number*] 例：	PIM に対して設定されたインターフェイスに関する情報を表示します。

	コマンドまたはアクション	目的
	`# show ipv6 pim interface`	
ステップ 5	**show ipv6 pimgroup-map** [*group-name* | group-address] | [*group-range* | *group-mask*] [**info-source {bsr** | **default** | **embedded-rp** | **static**}] 例： `# show ipv6 pim group-map`	IPv6 マルチキャスト グループ マッピング テーブルを表示します。
ステップ 6	**show ipv6 pimneighbor** [**detail**] [*interface-type interface-number* | **count**] 例： `# show ipv6 pim neighbor`	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。
ステップ 7	**show ipv6 pimrange-list** [**config**] [*rp-address* | *rp-name*] 例： `# show ipv6 pim range-list`	IPv6 マルチキャスト範囲リストに関する情報を表示します。
ステップ 8	**show ipv6 pimtunnel** [*interface-type interface-number*] 例： `# show ipv6 pim tunnel`	インターフェイス上の PIM レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示します。
ステップ 9	**debug ipv6 pim** [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **mvpn** | **neighbor**] 例： `# debug ipv6 pim`	PIM プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM オプションの設定

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pimspt-threshold infinity** [**group-list** *access-list-name*] 例： `(config) # ipv6 pim spt-threshold infinity group-list acc-grp-1`	PIM リーフ スイッチが指定したグループの SPT に加入するタイミングを設定します。
ステップ 3	**ipv6 pimaccept-register** {**list** *access-list* | **route-map** *map-name*} 例： `(config) # ipv6 pim accept-register route-map reg-filter`	RP のレジスタを許可または拒否します。
ステップ 4	**interface** *type number* 例： `(config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイスコンフィギュレーション モードにします。
ステップ 5	**ipv6 pim dr-priority** *value* 例： `(config-if) # ipv6 pim dr-priority 3`	PIM スイッチの DR プライオリティを設定します。
ステップ 6	**ipv6 pim hello-interval** *seconds* 例： `(config-if) # ipv6 pim hello-interval 45`	インターフェイスにおける PIM hello メッセージの頻度を設定します。
ステップ 7	**ipv6 pim join-prune-interval** *seconds* 例： `(config-if) # ipv6 pim join-prune-interval 75`	指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。
ステップ 8	**exit** 例： `(config-if) # exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**ipv6 pimjoin-prune statistic** [*interface-type*] 例： `(config-if) # show ipv6 pim join-prune statistic`	各インターフェイスの最後の集約パケットに関する平均 join-prune 集約を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

PIM トラフィック カウンタのリセット

PIM が誤動作する場合、または予想される PIM パケット数が送受信されていることを確認するために、ユーザは PIM トラフィック カウンタをクリアできます。トラフィック カウンタがクリアされたら、ユーザは show ipv6 pim traffic コマンドを入力して、PIM が正しく機能していること、および PIM パケットが正しく送受信されていることを確認できます。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 pimtraffic** 例： `# clear ipv6 pim traffic`	PIM トラフィック カウンタをリセットします。
ステップ 2	**show ipv6 pimtraffic** 例： `# show ipv6 pim traffic`	PIM トラフィック カウンタを表示します。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット

MRIB を使用するのに設定は不要です。ただし、特定の状況においては、ユーザは PIM トポロジテーブルをクリアして MRIB 接続をリセットし、MRIB 情報を確認する必要がある場合があります。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 pimtopology** [*group-name* | *group-address*] 例： `# clear ipv6 pim topology FF04::10`	PIM トポロジ テーブルをクリアします。
ステップ 2	**show ipv6 mribclient** [**filter**] [**name** {*client-name* | *client-name*: **client-id**}] 例： `# show ipv6 mrib client`	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 3	**show ipv6 mribroute** {**link-local** | **summary** | [*sourceaddress-or-name* | *] [*groupname-or-address*[*prefix-length*]]] 例： `# show ipv6 mrib route`	MRIB ルート情報を表示します。
ステップ 4	**show ipv6 pimtopology** [*groupname-or-address* [*sourceaddress-or-name*] | **link-local** | **route-count** [**detail**]] 例： `# show ipv6 pim topology`	特定のグループまたはすべてのグループの PIM トポロジテーブル情報を表示します。
ステップ 5	**debug ipv6 mribclient** 例： `# debug ipv6 mrib client`	MRIB クライアント管理アクティビティに対するデバッグをイネーブルにします。
ステップ 6	**debug ipv6 mribio** 例： `# debug ipv6 mrib io`	MRIB I/O イベントに対するデバッグをイネーブルにします。
ステップ 7	**debug ipv6 mrib proxy** 例： `# debug ipv6 mrib proxy`	分散型スイッチプラットフォームにおけるスイッチプロセッサとラインカード間の MRIB プロキシアクティビティに対するデバッグをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 8	**debug ipv6 mribroute** [*group-name* | *group-address*] 例： `# debug ipv6 mrib route`	MRIB ルーティング エントリ関連のアクティビティに関する情報を表示します。
ステップ 9	**debug ipv6 mribtable** 例： `# debug ipv6 mrib table`	MRIB テーブル管理アクティビティに対するデバッグをイネーブルにします。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM IPv6 スタブ ルーティングの設定

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャストルーティングをサポートします。サポート対象のPIMインターフェイスは、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類です。PIM パッシブ モードに設定されているルーテッド インターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過させたり転送したりするのは MLD トラフィックだけです。

PIM IPv6 スタブ ルーティングの設定時の注意事項

- PIM スタブ ルーティングを設定する前に、スタブ ルータと中央のルータの両方に IPv6 マルチキャストルーティングが設定されている必要があります。また、スタブ ルータのアップリンク インターフェイス上に、PIM モード（スパースモード）が設定されている必要があります。
- PIM スタブ ルータは、ディストリビューション ルータ間の伝送トラフィックのルーティングは行いません。ユニキャスト（EIGRP）スタブ ルーティングではこの動作が強制されます。PIM スタブ ルータの動作を支援するためにユニキャスト スタブ ルーティングを設定する必要があります。詳細については、EIGRPv6 スタブ ルーティング （251 ページ）を参照してください。
- 直接接続されたマルチキャスト（MLD）レシーバおよび送信元だけが、レイヤ2アクセス ドメインで許可されます。アクセス ドメインでは、PIM プロトコルはサポートされません。
- 冗長 PIM スタブ ルータ トポロジーはサポートされません。

IPv6 PIM ルーティングのデフォルト設定

この表に、Device用の IPv6 PIM ルーティングのデフォルト設定について示します。

表 *22 :* マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル
PIM マルチキャスト境界	なし。
候補 BSR	ディセーブル
候補 RP	ディセーブル
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

IPv6 PIM スタブ ルーティングのイネーブル化

始める前に

PIM スタブ ルーティングは IPv6 ではデフォルトでディセーブルです。インターフェイス上で PIM スタブ ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 multicast pim-passive-enable** 例： `Device(config-if)# ipv6 multicast pim-passive-enable`	スイッチで IPv6 マルチキャスト PIM ルーティングをイネーブルにします。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 9/0/6`	PIM スタブ ルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを MLD スタティック グループに結合する必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース モードをイネーブルにして、静的に接続されたメンバーとして VLAN を MLD スタティック グループに結合し、VLAN、MLD スタティック グループ、および物理インターフェイスで MLD スヌーピングをイネーブルにする必要があります。

	コマンドまたはアクション	目的
		これらのインターフェイスには、IPv6 アドレスを割り当てる必要があります。
ステップ 5	**ipv6 pim** 例： `Device(config-if)# ipv6 pim`	インターフェイスで PIM をイネーブルにします。
ステップ 6	**ipv6 pim** {**bsr**} | {**dr-priority** | *value*} | {**hello-interval** | *seconds*} | {**join-prune-interval** | *seconds*} | {**passive**} 例： `Device(config-if)# ipv6 pim bsr|dr-priority|hello-interval|join-prune-interval|passive`	インターフェイスでさまざまな PIM スタブ機能を設定します。 **bsr** を入力して PIM スイッチの BSR を設定します。 **dr-priority** を入力して、PIM スイッチの DR プライオリティを設定します。 **hello-interval** を入力して、インターフェイスの PIM hello メッセージの頻度を設定します。 **join-prune-interval** を入力して、指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。 **passive** を入力して、パッシブ モードの PIM を設定します。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

IPv6 PIM スタブ ルーティングのモニタ

表 *23 : PIM* スタブ設定の *show* コマンド

コマンド	目的
show ipv6 pim interface `Device# show ipv6 pim interface`	各インターフェイスで有効になっている PIM スタブを表示します。
show ipv6 mld groups `Device# show ipv6 mld groups`	特定のマルチキャスト グループを結合した対象クライアントを表示します。

コマンド	目的
show ipv6 mroute `Device# show ipv6 mroute`	ソースから対象クライアントへのマルチキャストストリーム転送を確認します。

BSR の設定

ここでの作業について、以下に説明します。

BSR の設定および BSR 情報の確認

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pimbsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*] 例： `(config) # ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10`	候補 BSR になるようにスイッチを設定します。
ステップ 3	**interface** *type number* 例： `(config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 pim bsr border** 例： `(config-if) # ipv6 pim bsr border`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**exit** 例： `(config-if) # exit`	このコマンドを2回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**show ipv6 pim** bsr {**election** | **rp-cache** | **candidate-rp**} 例： `(config-if) # show ipv6 pim bsr election`	PIM BSR プロトコル処理に関連する情報を表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BSR への PIM RP アドバタイズメントの送信

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** seconds] 例： `(config) # ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0`	BSR に PIM RP アドバタイズメントを送信します。
ステップ 3	**interface** *type number* 例： `(config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 pim bsr border** 例： `(config-if) # ipv6 pim bsr border`	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

限定スコープ ゾーン内で BSR を使用できるようにするための設定

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pim bsr candidate rp** *ipv6-address* [*hash-mask-length*] [**priority** priority-value] 例： `(config) # ipv6 pim bsr candidate bsr 2001:DB8:1:1:4`	候補 BSR になるようにスイッチを設定します。
ステップ 3	**ipv6 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** seconds] 例： `(config) # ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6`	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。
ステップ 4	**interface** *type number* 例： `(config-if) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**ipv6 multicast boundary scope** *scope-value* 例： `(config-if) # ipv6 multicast boundary scope 6`	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定

IPv6 BSR スイッチは、スコープと RP のマッピングを候補 RP メッセージから学習するのではなく、直接アナウンスするようにスタティックに設定できます。ユーザは、スコープと RP のマッピングをアナウンスするように BSR スイッチを設定して、BSR をサポートしていない RP がその BSR にインポートされるように設定できます。この機能をイネーブルにすると、ローカルの候補 BSR スイッチの既知のリモート RP が、企業の BSR ドメインの外部に配置されている RP を学習できるようになります。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pim bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] 例： `(config)# ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0`	指定した候補 RP の BSR からスコープと RP のマッピングを直接アナウンスします。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピングの設定

SSM マッピング機能をイネーブルにすると、DNS ベースの SSM マッピングが自動的にイネーブルになります。つまり、スイッチは、マルチキャスト MLD バージョン 1 レポートの送信元を DNS サーバから検索するようになります。

スイッチ設定に応じて、DNS ベースのマッピングまたはスタティック SSM マッピングのいずれかを使用できます。スタティック SSM マッピングを使用する場合は、複数のスタティック SSM マッピングを設定できます。複数のスタティック SSM マッピングを設定すると、一致するすべてのアクセス リストの送信元アドレスが使用されるようになります。

（注） DNS ベースの SSM マッピングを使用するには、スイッチは正しく設定されている DNS サーバを少なくとも 1 つ見つける必要があります。スイッチは、その DNS サーバに直接接続される可能性があります。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mldssm-map enable** 例： `(config) # ipv6 mld ssm-map enable`	設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**no ipv6 mldssm-map query dns** 例： `(config) # no ipv6 mld ssm-map query dns`	DNS ベースの SSM マッピングをディセーブルにします。
ステップ 4	**ipv6 mldssm-map static** *access-list source-address* 例： `(config-if) # ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1`	スタティック SSM マッピングを設定します。
ステップ 5	**exit** 例： `(config-if) # exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権EXEC モードに戻します。
ステップ 6	**show ipv6 mldssm-map** [*source-address*] 例： `(config-if) # show ipv6 mld ssm-map`	SSM マッピング情報を表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スタティック mroute の設定

IPv6 のスタティック マルチキャスト ルート（mroute）は、IPv6 スタティック ルートの拡張として実装できます。スイッチを設定する際には、ユニキャスト ルーティング専用としてスタティック ルートを使用するか、マルチキャスト RPF 選択専用としてスタティック マルチキャスト ルートを使用するか、またはユニキャスト ルーティングとマルチキャスト RPF 選択の両方にスタティック ルートを使用するように設定できます。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 route** {*ipv6-prefix / prefix-length ipv6-address* | *interface-type interface-number ipv6-address*]}	スタティック IPv6 ルートを確立します。この例は、ユニキャスト ルーティングとマルチキャスト RPF 選択の両方に使

	コマンドまたはアクション	目的
	[*administrative-distance*] [*administrative-multicast-distance* | *unicast* | *multicast*] [**tag** *tag*] 例： `(config) # ipv6 route 2001:DB8::/64 6::6 100`	用されるスタティック ルートを示しています。
ステップ 3	**exit** 例： `# exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権EXEC モードに戻します。
ステップ 4	**show ipv6 mroute** [link-local | [*group-name* | *group-address* [*source-address* | *source-name*]] [**summary**] [**count**] 例： `# show ipv6 mroute ff07::1`	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 5	**show ipv6 mroute** [**link-local** | *group-name* | *group-address*] **active** [*kbps*] 例： `(config-if) # show ipv6 mroute active`	スイッチ上のアクティブなマルチキャスト ストリームを表示します。
ステップ 6	**show ipv6 rpf** [*ipv6-prefix*] 例： `(config-if) # show ipv6 rpf 2001::1:1:2`	特定のユニキャスト ホスト アドレスおよびプレフィックスの RPF 情報を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 マルチキャストでの MFIB の使用

IPv6 マルチキャスト ルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。

IPv6 マルチキャストでの MFIB の動作の確認

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 mfib** [**linkscope** | **verbose** | *group-address-name* | *ipv6-prefix / prefix-length* | *source-address-name* | **count** | **interface** | **status** | **summary**] 例： `# show ipv6 mfib`	IPv6 MFIB での転送エントリおよびインターフェイスを表示します。
ステップ 2	**show ipv6 mfib** [all | linkscope | group-name | group-address [source-name | source-address]] **count** 例： `# show ipv6 mfib ff07::1`	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 3	**show ipv6 mfib interface** 例： `# show ipv6 mfib interface`	IPv6 マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示します。
ステップ 4	**show ipv6 mfib status** 例： `# show ipv6 mfib status`	一般的な MFIB 設定と動作ステータスを表示します。
ステップ 5	**show ipv6 mfibsummary** 例： `# show ipv6 mfib summary`	IPv6 MFIB エントリおよびインターフェイスの数に関するサマリー情報を表示します。
ステップ 6	**debug ipv6 mfib** [*group-name* | *group-address*] [**adjacency** | **db** | **fs** | **init** | **interface** | **mrib** [**detail**] | **nat** | **pak** | **platform** | **ppr** | **ps** | **signal** | **table**] 例： `# debug ipv6 mfib FF04::10 pak`	IPv6 MFIB に対するデバッグ出力をイネーブルにします。

MFIB トラフィック カウンタのリセット

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mfibcounters** [*group-name* | **group-address** [*source-address* | *source-name*]] 例： `# clear ipv6 mfib counters FF04::10`	アクティブなすべての MFIB トラフィック カウンタをリセットします。

第 17 章

IPv6 クライアント IP アドレス ラーニングの設定

- IPv6 クライアント アドレス ラーニングの前提条件 （315 ページ）
- IPv6 クライアント アドレス ラーニングについて （316 ページ）
- IPv6 ユニキャストの設定（CLI） （322 ページ）
- RA ガード ポリシーの設定（CLI） （322 ページ）
- RA ガード ポリシーの適用（CLI） （323 ページ）
- RA スロットル ポリシーの設定（CLI） （324 ページ）
- VLAN への RA スロットル ポリシーの適用（CLI） （325 ページ）
- IPv6 ネイバー プロービングの設定方法 （326 ページ）
- IPv6 スヌーピングの設定（CLI） （330 ページ）
- IPv6 ND 抑制ポリシーの設定（CLI） （330 ページ）
- VLAN/PortChannel での IPv6 スヌーピングの設定 （331 ページ）
- Switch での IPv6 の設定（CLI） （332 ページ）
- DHCP プールの設定（CLI） （333 ページ）
- DHCP を使用しないステートレス自動アドレス設定の設定（CLI） （334 ページ）
- DHCP によるステートレス自動アドレス設定の設定（CLI） （335 ページ）
- ステートフル DHCP のローカル設定（CLI） （336 ページ）
- ステートフル DHCP の外部的設定（CLI） （338 ページ）
- IPv6 アドレス ラーニング設定の確認 （339 ページ）
- その他の参考資料 （340 ページ）
- IPv6 クライアント アドレス ラーニングの機能情報 （341 ページ）

IPv6 クライアント アドレス ラーニングの前提条件

IPv6 クライアント アドレス ラーニングを設定する前に、IPv6 をサポートするようにワイヤレス クライアントを設定します。

関連トピック

RA ガード ポリシーの設定（CLI） （322 ページ）

IPv6 クライアント アドレス ラーニングについて

クライアント アドレス ラーニングは、アソシエーション、再アソシエーション、非認証、タイムアウト時に、ワイヤレス クライアントの IPv4 および IPv6 アドレス、デバイスによって維持されるクライアント遷移ステートについて学習するために、デバイスで設定されます。

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定（SLACC）
- ステートフル DHCPv6
- 静的設定

これらの方法のいずれの場合も、IPv6 クライアントは常にネイバー送信要求 DAD（重複アドレス検出）要求を送信して、ネットワークに重複する IP アドレスがないようにします。デバイスはクライアントの NDP および DHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習します。

SLAAC アドレス割り当て

IPv6 クライアント アドレス割り当て用の最も一般的な方法は、ステートレス アドレス自動設定（SLAAC）です。SLAAC はクライアントが IPv6 プレフィクスに基づいてアドレスを自己割り当てするシンプルなプラグアンドプレイ接続を提供します。このプロセスが実現しました。

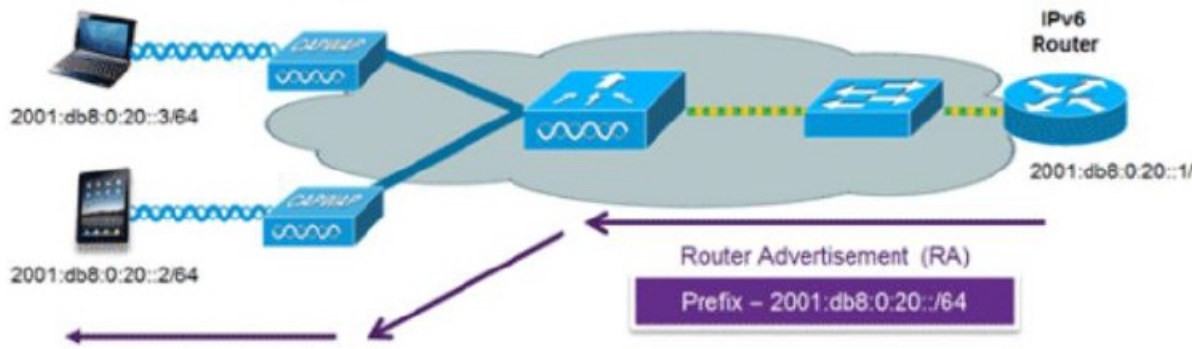
次のように、ステートレス アドレス自動設定（SLAAC）は設定されています。

- ホストは、ルータ送信要求メッセージを送信します。
- ホストは、ルータ アドバタイズメント メッセージを待機します。
- ホストは、ルータ アドバタイズメント メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、これを 64 ビット EUI-64 アドレス（イーサネットの場合、MAC アドレスから作成されます）と組み合わせて、グローバル ユニキャスト メッセージを作成します。ホストは、デフォルト ゲートウェイとして、ルータ アドバタイズメント メッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 重複アドレス検出は、選択されるランダムアドレスが他のクライアントと重複しないように、IPv6 クライアントによって実行されます。
- アルゴリズムの選択はクライアントに依存し、多くの場合は設定できます。

次の 2 種類のアルゴリズムに基づいて IPv6 アドレスの最後の 64 ビットが学習可能です。

- インターフェイスの MAC アドレスに基づく EUI-64、または
- ランダムに生成されるプライベート アドレス。

図 *10 : SLAAC* アドレス割り当て



Cisco 対応 IPv6 ルータからの次の Cisco IOS コンフィギュレーション コマンドを使用して、SLAAC のアドレッシングとルータ アドバタイズメントをイネーブルにします。

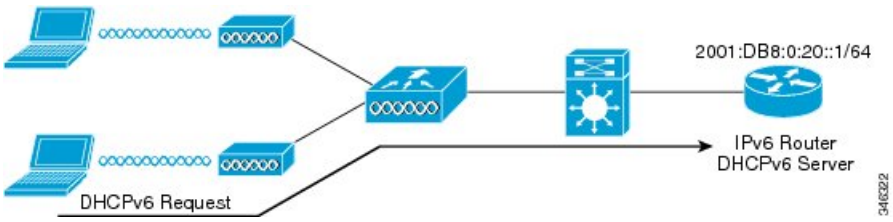
```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

関連トピック

IPv6 スヌーピングの設定（CLI） （330 ページ）
DHCP プールの設定（CLI） （333 ページ）
DHCP を使用しないステートレス自動アドレス設定の設定（CLI） （334 ページ）
DHCP によるステートレス自動アドレス設定の設定（CLI） （335 ページ）
ステートフル DHCP のローカル設定（CLI） （336 ページ）
ステートフル DHCP の外部的設定（CLI） （338 ページ）

ステートフル DHCPv6 アドレス割り当て

図 *11 :* ステートフル *DHCPv6* アドレス割り当て



DHCPv6 の使用は、SLAAC がすでに導入されている場合は、IPv6 クライアント接続で要求されません。DHCPv6 にはステートレスおよびステートフルという 2 種類の動作モードがあります。

DHCPv6 ステートレス モードは、ルータ アドバタイズメントで使用できない追加のネットワーク情報をクライアントに提供するために使用しますが、これはIPv6アドレスではありません。すでに SLAAC によって提供されているためです。この情報には DNS ドメイン名、DNS サーバ、その他の DHCP ベンダー固有オプションを含めることができます。このインターフェイス設定は、SLAAC をイネーブルにしてステートレス DHCPv6 を実装する Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

マネージド モードとも呼ばれる DHCPv6 ステートフル オプションは、DHCPv4 と同様に動作します。つまり、クライアント SLAAC のとおりにアドレスの最後の 64 ビットを生成するのではなく、固有のアドレスをそれぞれのクライアントに割り当てます。次のインターフェイス設定は、ローカル Deviceのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
end
```

次のインターフェイス設定は、外部DHCP サーバのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp_relay destination 2001:DB8:0:20::2
end
```

関連トピック

IPv6 スヌーピングの設定（CLI） （330 ページ）

DHCP プールの設定（CLI）（333 ページ）
DHCP を使用しないステートレス自動アドレス設定の設定（CLI）（334 ページ）
DHCP によるステートレス自動アドレス設定の設定（CLI）（335 ページ）
ステートフル DHCP のローカル設定（CLI）（336 ページ）
ステートフル DHCP の外部的設定（CLI）（338 ページ）

静的 IP アドレス割り当て

クライアントにスタティックに設定されたアドレス。

ルータ要求

ルータ送信要求メッセージは、ローカル ルーティングに関する情報を入手できる、またはステートレス自動設定を設定できるルータ アドバタイズメントを送信するようにローカル ルータを促進するために、ホスト コントローラによって発行されます。ルータ アドバタイズメントは定期的に送信され、起動時または再起動操作後などに、ホストはルータ送信要求を使用して即時ルータ アドバタイズメントを要求します。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI）（330 ページ）

ルータ アドバタイズメント

ルータ アドバタイズメント メッセージは、ルータから定期的に送信されるか、ホストからのルータ送信要求メッセージへの応答として送信されます。これらのメッセージに含まれる情報は、ホストでステートレス自動設定を実行し、ルーティングテーブルを変更するために使用されます。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI）（330 ページ）

ネイバー探索

IPv6 ネイバー ディスカバリとは、近隣のノード間の関係を決定するメッセージとプロセスのことです。ネイバー ディスカバリは、IPv4 で使用されていた ARP、ICMP ルータ探索、および ICMP リダイレクトに代わるものです。

信頼できるバインディング テーブル データベースを構築するために、IPv6 ネイバー ディスカバリ検査によってネイバー ディスカバリ メッセージが分析され、準拠しない IPv6 ネイバー ディスカバリ パケットはドロップされます。 スイッチ内のネイバー バインディング テーブルでは、各 IPv6 アドレスと、アソシエートされた MAC アドレスが追跡されます。クライアントは、ネイバー バインディング タイマーに従って、テーブルから消去されます。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI）（330 ページ）

ネイバー探索抑制

ワイヤレス クライアントの IPv6 アドレスは、デバイスによってキャッシュされます。デバイスが IPv6 アドレスを検索する NS マルチキャストを受信して、デバイスによって特定された目的のアドレスがクライアントのいずれかに属している場合、デバイスはクライアントに代わって NA メッセージで応答します。このプロセスによって IPv4 のアドレス解決プロトコル（ARP）テーブルと同等のテーブルが生成されますが、より効率的であり、たいていの場合、使用されるメッセージは少なくなります。

（注） デバイスがプロキシのように動作し NA で応答するのは、**ipv6 nd suppress** コマンドが設定されている場合だけです。

デバイスにワイヤレス クライアントの IPv6 アドレスがない場合、デバイスは NA で応答せず、NS パケットをワイヤレス側に転送します。この問題を解決するために、NS マルチキャスト フォワーディング ノブが用意されています。このノブがイネーブルの場合、デバイスは存在しない（キャッシュ欠落）IPv6 アドレスの NS パケットを取得し、ワイヤレス側に転送します。このパケットは、目的のワイヤレス クライアントに到達し、クライアントは NA で応答します。

このキャッシュ ミス シナリオが発生するのはまれで、完全な IPv6 スタックが実装されていないクライアントが、NDP 時にそれらの IPv6 アドレスをアドバタイズしない可能性はほとんどありません。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI） （330 ページ）

RA ガード

IPv6 クライアントは、IPv6 アドレスを設定し、IPv6 ルータ アドバタイズメント（RA）パケットに基づいてルータ テーブルにデータを入力します。RA ガード機能は、有線ネットワークの RA ガード機能に類似しています。RA ガードは、ワイヤレス クライアントから発信される不要な、または不正な RA パケットをドロップすることによって、IPv6 ネットワークのセキュリティを強化します。この機能が設定されていないと、悪意のある IPv6 ワイヤレス クライアントが、多くの場合は高い優先順位で、それ自体をネットワークのルータとして通知する可能性があり、そのため、正規の IPv6 ルータよりも優先されることになります。

また、RA ガードは、着信 RA を調べて、メッセージまたはスイッチ設定で検出された情報のみに基づいて、それらをスイッチするかブロックするかを決定します。受信したフレームで使用できる情報は、RA の検証に有用です。

- フレームが受信されるポート
- IPv6 送信元アドレス
- プレフィックス リスト

スイッチで作成された次の設定情報は、受信した RA フレームで検出された情報に対して検証するときに RA ガードで使用できます。

- RA ガード メッセージの受信用に信頼できる/信頼できないポート
- RA 送信者の信頼できる/信頼できない送信元 IPv6 アドレス
- 信頼できる/信頼できないプレフィックス リストおよびプレフィックス範囲
- ルータ プリファレンス

RA ガードはデバイスで行われます。デバイスで RA メッセージをドロップするようにデバイスを設定できます。すべての IPv6 RA メッセージがドロップされ、それによって他のワイヤレス クライアントおよびアップストリーム有線ネットワークが悪意のある IPv6 クライアントから保護されます。

```
//Create a policy for RA Guard//
ipv6 nd raguard policy raguard-router
trusted-port
device-role router

//Applying the RA Guard Policy on port/interface//
interface tengigabitethernet1/0/1 (Katana)
interface gigabitethernet1/0/1 (Edison)

ipv6 nd raguard attach-policy raguard-router
```

関連トピック

RA ガード ポリシーの設定（CLI） （322 ページ）
RA ガード ポリシーの適用（CLI） （323 ページ）
RA スロットル ポリシーの設定（CLI） （324 ページ）
VLAN への RA スロットル ポリシーの適用（CLI） （325 ページ）

RA スロットリング

RA スロットリングは、コントローラがワイヤレス ネットワーク宛ての RA パケットを強制的に制限できるようにします。RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。クライアントが RS パケットを送信すると、RA がクライアントに返送されます。この RA は、コントローラを通過でき、クライアントにユニキャストされます。このプロセスによって、新しいクライアントやローミング クライアントが RA スロットリングの影響を受けないようにすることができます。

関連トピック

RA ガード ポリシーの設定（CLI） （322 ページ）
RA ガード ポリシーの適用（CLI） （323 ページ）
RA スロットル ポリシーの設定（CLI） （324 ページ）
VLAN への RA スロットル ポリシーの適用（CLI） （325 ページ）

IPv6 ユニキャストの設定（CLI）

IPv6 ユニキャストはスイッチとコントローラで常にイネーブルにする必要があります。IPv6 ユニキャスト ルーティングはディセーブルに設定されています。

始める前に

IPv6ユニキャストデータグラムの転送をイネーブルにするには、グローバル コンフィギュレーション モードで **ipv6 unicast-routing** コマンドを使用します。IPv6 ユニキャスト データグラムの転送をディセーブルにするには、このコマンドの **no** 形式を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 unicast routing** 例： `Device (config)# ipv6 unicast routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

RA ガード ポリシーの設定（CLI）

IPv6 クライアント アドレスを追加し、IPv6 ルータ アドバタイズメント パケットに基づいてルータ テーブルに入力するには、デバイスで RA ガード ポリシーを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd raguard policy raguard-router** 例： `Device(config)# ipv6 nd raguard policy raguard-router`	RA ガード ポリシー名を定義して、RA ガード ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**trustedport** 例： `Device(config-ra-guard)# trustedport`	（任意）このポリシーが信頼できるポートに適用されることを指定します。
ステップ 4	**device-role router** 例： `Device(config-ra-guard)# device-role router`	ポートに接続されているデバイスのロールを指定します。
ステップ 5	**exit** 例： `Device(config-ra-guard)# exit`	RA ガード ポリシー コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。

関連トピック

RA ガード （320 ページ）
RA スロットリング （321 ページ）
RA ガード ポリシーの適用（CLI） （323 ページ）
RA スロットル ポリシーの設定（CLI） （324 ページ）
VLAN への RA スロットル ポリシーの適用（CLI） （325 ページ）
IPv6 クライアント アドレス ラーニングの前提条件 （315 ページ）

RA ガード ポリシーの適用（CLI）

デバイスで RA ガード ポリシーを適用すると、すべての信頼できない RA がブロックされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface tengigabitethernet 1/0/1** 例： `Device (config)# interface tengigabitethernet 1/0/1`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 nd raguard attach-policy raguard-router** 例： `Device(config-if)# ipv6 nd raguard attach-policy raguard-router`	指定したインターフェイスに IPv6 RA ガード機能を適用します。
ステップ 4	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

関連トピック

RA ガード ポリシーの設定（CLI）（322 ページ）
RA ガード（320 ページ）
RA スロットリング（321 ページ）
RA スロットル ポリシーの設定（CLI）（324 ページ）
VLAN への RA スロットル ポリシーの適用（CLI）（325 ページ）

RA スロットル ポリシーの設定（CLI）

強制的に制限できるように RA スロットル ポリシーを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd ra-throttler policy ra-throttler1** 例： `Device(config)# ipv6 nd ra-throttler policy ra-throttler1`	ルータ アドバタイズメント（RA）スロットラ ポリシー名を定義して、IPv6 RA スロットル ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**throttleperiod500** 例： `Device(config-nd-ra-throttle)# throttleperiod 500`	IPv6 RA スロットラ ポリシーのスロットル期間を設定します。

	コマンドまたはアクション	目的
ステップ 4	**max-through10** 例： `Device(config-nd-ra-throttle)# max-through 500`	スロットル期間ごとに、VLANあたりのマルチキャスト RA を制限します。
ステップ 5	**allow-atleast 5at-most 10** 例： `Device(config-nd-ra-throttle)# allow-atleast 5 at-most 10`	RA スロットラ ポリシーのスロットル期間ごとに、デバイスあたりのマルチキャスト RA 数を制限します。

関連トピック

RA ガード ポリシーの設定（CLI）（322 ページ）
RA ガード ポリシーの適用（CLI）（323 ページ）
RA ガード（320 ページ）
RA スロットリング（321 ページ）
VLAN への RA スロットル ポリシーの適用（CLI）（325 ページ）

VLAN への RA スロットル ポリシーの適用（CLI）

VLAN に RA スロットル ポリシーを適用します。RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration 1** 例： `Device(config)# vlan configuration 1`	VLANまたはVLANの集合を設定して、VLAN コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd ra throttler attach-policy ra-throttler1** 例： `Device(config-vlan)# ipv6 nd ra throttler attach-policy ra-throttler1`	VLAN または VLAN の集合に IPv6 RA スロットル ポリシーを接続します。

関連トピック

RA ガード ポリシーの設定（CLI）（322 ページ）
RA ガード ポリシーの適用（CLI）（323 ページ）
RA スロットル ポリシーの設定（CLI）（324 ページ）
RA ガード（320 ページ）
RA スロットリング（321 ページ）

IPv6 ネイバー プロービングの設定方法

IPv6 ネイバー プロービングが機能するには、バインディング テーブルにデータを入力する必要があります。このタスクは、バインディング テーブル内のエントリのライフ サイクルで微調整を行うために実行します。

1 つの IPv6 クライアントは、随時に複数の IPv6 アドレスを持つことができます。**show ipv6 neighbor binding mac** *mac_address* コマンドを実行すると、これらのアドレスの状態は、そのクライアント MAC アドレスの IPv6 ネイバー バインディング テーブルで `REACHABLE` として表示されます。これらのアドレス上で300秒間コントロールアクティビティがない場合、アドレスは `STALE` 状態に移行し、それ以降はクライアントで使用できなくなります。

device-tracking tracking コマンドを使用して定期プローブ（デフォルトの間隔は 300 秒）をすべての IPv6 クライアントに送信し、クライアントの IPv6 アドレスがエージ アウトしておらず、`STALE` 状態に移行していないことを確かめます。これらのプローブは、送信元 IP アドレスがすべてゼロ、つまり、重複アドレス検出（DAD）プローブのスイッチから送信されます。DAD プローブに応答しないために 300 後にエージ アウトするクライアントがいくつか存在します。

（注） IPv6 ネイバー プロービングは、IP アドレスを取得するかまたは維持するのが難しいホストに関してネットワークの問題がある場合のみ、有効にしてください。特に、ホストが IP リースの更新をネゴシエーションしているときの時間枠内でDADプローブがホストに発行されると、DAD チャレンジによりホストが IP アドレスを放棄することがあります。不必要に IPv6 ネイバー プロービングを有効にすると、予期しないホストの動作が生じる場合があります。

（注） Cisco IOS 15.2(5)E リリース以前の場合は、インターフェイス レベルで IPv6 スヌーピング ポリシーを削除し、VLAN レベルでポリシーをアタッチする必要があります。手順 8 と手順 9 を実行し、VLAN レベルで IPv6 スヌーピング ポリシーをアタッチします。

IPv6 ネイバー プロービングが VLAN で有効な場合は、トランク ポートを介する学習やホストを無効にするために、追加の設定を実行する必要があります。トランク ポートを介した学習を無効にするには、**trusted-port** および **device-role switch** でポリシーを設定する必要があります。この設定では、トランク ポートに接続されている他のアクセス スイッチに、それぞれが接続しているホストに対してファースト ホップ セキュリティを提供するポリシーを用意する必要があります。各スイッチはそれぞれのホストに対してセキュリティを提供する必要があります。手順 10 ～ 12 を実行し、これらの属性でポリシーを設定します。

以下の手順を実行し、IPv6 ネイバー プロービングを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**device-trackingtracking** 例： `Device(config)# device-tracking tracking`	IPv6 ネイバー プロービングを有効にします。 IPv6 ネイバー プロービングを無効にするには、このコマンドの **no** フォームを使用します。
ステップ 4	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 1810`	インターフェイス コンフィギュレーション モードを開始して、IP 情報が割り当てられている VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
ステップ 5	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
		（注） **ipv6 enable** を設定して VLAN に SVI を作成すると、結果として、SVI のリンク ローカル アドレスがプローブのソース アドレスとして使われます。このため、プロービングは DAD メッセージではなく、NS メッセージとして実行されます。この設定ではプローブ応答のレートが高くなります。一部のホストは DAD リクエストを無視することがあります。ただし、NS メッセージにはすべてのホストが応答します。
ステップ 6	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイスをイネーブルにします。 dot1x を IPv4 に対して有効にする場合、dot1x が有効になっているインターフェイス上のポリシーは自動的に設定され、トラッキングは特に IPv6 ネイバー プロービングに対して有効になります。この場合、グローバル設定レベルでトラッキング動作を変更しても、これらの自動的に設定されているポリシーのトラッキングには何の影響もありません。トラッキングはすべてのインターフェイスで常に有効になります。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 1815`	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 9	**ipv6 snooping** [**attach-policy** *policy_name*] 例：	すべてのスイッチおよびスタック インターフェイスで、IPv6 スヌーピング ポ

	コマンドまたはアクション	目的
	`Device(config-vlan-config)# ipv6 snooping attach-policy example_policy`	リシーを指定した VLAN にアタッチします。attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。デフォルトポリシーは、セキュリティ レベル guard、デバイス ロール node、プロトコル ndp および dhcp です。 （注） すべてのインターフェイスで同じユーザ定義のポリシーが設定されている場合、このポリシーを VLAN 上に設定して、インターフェイスから削除できます。インターフェイス上に設定されているポリシーが異なる場合、インターフェイスに設定されているポリシーは削除しないでください。上記のデフォルト ポリシーは VLAN レベルで適用してください。
ステップ 10	**ipv6 snooping policy** *policy_name* 例： `Device(config-vlan-config)# ipv6 snooping policy example_policy`	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始します。
ステップ 11	**trusted-port** 例： `Device(config-ipv6-snooping)# trusted-port`	信頼できるポートにするポートを設定します。
ステップ 12	**device-roleswitch** 例： `Device(config-ipv6-snooping)# device-role switch`	スイッチに接続されているデバイスの役割を設定します。
ステップ 13	**end** 例： `Device(config-ipv6-snooping)# end`	設定モードを終了します。

IPv6 スヌーピングの設定（CLI）

IPv6 スヌーピングはスイッチとコントローラで常にイネーブルにする必要があります。

始める前に

クライアント マシンで IPv6 をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan configuration 1** 例： `Device(config)# vlan configuration 1`	VLAN コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 snooping** 例： `Device(config-vlan)# ipv6 snooping`	Vlan で IPv6 スヌーピングをイネーブルにします。
ステップ 3	**ipv6 nd suppress** 例： `Device(config-vlan-config)# ipv6 nd suppress`	Vlan で IPv6 ND 抑制をイネーブルにします。
ステップ 4	**exit** 例： `Device(config-vlan-config)# exit`	設定を保存し、Vlan コンフィギュレーション モードを終了します。

関連トピック

SLAAC アドレス割り当て （316 ページ）
ステートフル DHCPv6 アドレス割り当て （317 ページ）

IPv6 ND 抑制ポリシーの設定（CLI）

IPv6 ネイバー探索（ND）マルチキャスト抑制機能では、ドロップする（およびターゲットに代わって送信要求に応答する）、またはユニキャスト トラフィックに変換することで、できるだけ多くの ND マルチキャスト ネイバー送信要求（NS）メッセージを停止します。この機能は、レイヤ2スイッチまたはワイヤレス コントローラで実行され、適切なリンクの処理に必要な制御トラフィックの量を減らすために使用されます。

アドレスがバインディング テーブルに挿入されると、マルチキャスト アドレスに送信されたアドレス解決要求が代行受信され、デバイスはアドレスの所有者に代わって応答するか、レイヤ 2 で要求をユニキャスト メッセージに変換して宛先に転送します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device(config)# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd suppress policy** 例： `Device (config)# ipv6 nd suppress policy`	ND 制御ポリシー名を定義して ND 制御ポリシー コンフィギュレーション モードを開始します。

関連トピック

ルータ要求 （319 ページ）
ルータ アドバタイズメント （319 ページ）
ネイバー探索 （319 ページ）
ネイバー探索抑制 （320 ページ）

VLAN/PortChannel での IPv6 スヌーピングの設定

ネイバー探索（ND）抑制は、VLAN またはスイッチ ポートでイネーブルまたはディセーブルにできます。

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan config901** 例： `Device(config)# vlan config901`	VLAN を作成し、VLAN コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ipv6 nd suppress** 例： `Device(config-vlan)# ipv6 nd suppress`	VLAN に IPv6 nd 抑制を適用します。
ステップ 3	**end** 例： `Device(config-vlan)# end`	VLAN コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。
ステップ 4	**interface gi1/0/1** 例： `Device (config)# interface gi1/0/1`	ギガビット イーサネット ポート インターフェイスを作成します。
ステップ 5	**ipv6 nd suppress** 例： `Device(config-vlan)# ipv6 nd suppress`	インターフェイスに IPv6 nd 抑制を適用します。
ステップ 6	**end** 例： `Device(config-vlan)# end`	VLAN コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。

Switch での IPv6 の設定（CLI）

インターフェイス上の IPv6 を設定するには、この設定例を使用します。

始める前に

クライアント上の IPv6 および有線インフラストラクチャ上の IPv6 サポートをイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address fe80::1 link-local**
	例：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
	2001:DB8:0:1:FFFF:1234::5/64 Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64	
ステップ 3	**ipv6 enable** 例： Device(config)# ipv6 enable	（任意）インターフェイス上で IPv6 をイネーブルにします。
ステップ 4	**end** 例： Device(config)# end	インターフェイスモードを終了します。

DHCP プールの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**ipv6 dhcp pool Vlan21** 例： Device(config)# ipv6 dhcp pool vlan1	コンフィギュレーション モードを開始し、VLAN の IPv6 DHCP プールを設定します。
ステップ 2	**address prefix 2001:DB8:0:1:FFFF:1234::/64lifetime 300 10** 例： Device(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10	コンフィギュレーション DHCP モードを開始し、VLAN のアドレス プールとそのライフタイムを設定します。
ステップ 3	**dns-server 2001:100:0:1::1** 例： Device(config-dhcpv6)# dns-server 2001:20:21::1	DHCP プールの DNS サーバを設定します。
ステップ 4	**domain-name example.com** 例： Device(config-dhcpv6)# domain-name example.com	完全な非修飾ホスト名になるようにドメイン名を設定します。
ステップ 5	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

SLAAC アドレス割り当て （316 ページ）
ステートフル DHCPv6 アドレス割り当て （317 ページ）

DHCP を使用しないステートレス自動アドレス設定の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address fe80::1 link-local**
	例：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 3	**ipv6 enable** 例： `Device(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

ステップ 4	**no ipv6 nd managed-config-flag**
	例：
	`Device(config)#interface vlan 1`
	`Device(config-if)# no ipv6 nd managed-config-flag`
		接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。

ステップ 5	**no ipv6 nd other-config-flag** 例： `Device(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

SLAAC アドレス割り当て （316 ページ）
ステートフル DHCPv6 アドレス割り当て （317 ページ）

DHCPによるステートレス自動アドレス設定の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address fe80::1 link-local**
	例：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 3	**ipv6 enable** 例： `Device(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

ステップ 4	**no ipv6 nd managed-config-flag**
	例：
	`Device(config)#interface vlan 1`
	`Device(config-if)# no ipv6 nd managed-config-flag`
		接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。

ステップ 5	**ipv6 nd other-config-flag** 例： `Device(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 6	**end** 例： `Device(config)# end`	インターフェイスモードを終了します。

関連トピック

SLAAC アドレス割り当て （316 ページ）

ステートフル DHCPv6 アドレス割り当て （317 ページ）

ステートフル DHCP のローカル設定（CLI）

このインターフェイス設定は、ローカル のステートフル DHCPv6 を実装している Cisco IOS Ipv6 ルータ用です。Device

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 を設定します。
ステップ 3	**ipv6 dhcp pool `IPv6_DHCPPOOL`** 例： `Device (config)# ipv6 dhcp pool IPv6_DHCPPOOL`	コンフィギュレーションモードを開始し、VLAN の IPv6 DHCP プールを設定します。
ステップ 4	**address prefix `2001:DB8:0:1:FFFF:1234::/64`** 例： `Device (config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64`	プールに入力するアドレス範囲を指定します。
ステップ 5	**dns-server `2001:100:0:1::1`** 例： `Device (config-dhcpv6)# dns-server 2001:100:0:1::1`	DHCP クライアントに DNS サーバのオプションを提供します。
ステップ 6	**domain-name `example.com`** 例： `Device (config-dhcpv6)# domain-name example.com`	DHCP クライアントにドメイン名オプションを提供します。
ステップ 7	**exit** 例： `Device (config-dhcpv6)# exit`	前のモードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**interface vlan1** 例： `Device (config)# interface vlan 1`	インターフェイスモードを開始して、ステートフル DHCP を設定します。
ステップ 9	**description IPv6-DHCP-Stateful** 例： `Device (config-if)# description IPv6-DHCP-Stateful`	ステートフル IPv6 DHCP の説明を入力します。
ステップ 10	**ipv6 address 2001:DB8:0:20::1/64** 例： `Device (config-if)# ipv6 address 2001:DB8:0:20::1/64`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 11	**ip address 192.168.20.1 255.255.255.0** 例： `Device (config-if)# ip address 192.168.20.1 255.255.255.0`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 12	**ipv6 nd prefix 2001:db8::/64no-advertise** 例： `Device (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	アドバタイズしてはならない、IPv6 ルーティングプレフィックスアドバタイズメントを設定します。
ステップ 13	**ipv6 nd managed-config-flag** 例： `Device (config-if)# ipv6 nd managed-config-flag`	ホストでアドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 14	**ipv6 nd other-config-flag** 例： `Device (config-if)# ipv6 nd other-config-flag`	ホストで非アドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 15	**ipv6 dhcp server IPv6_DHCPPOOL** 例： `Device (config-if)# ipv6 dhcp server IPv6_DHCPPOOL`	インターフェイスに DHCP サーバを設定します。

関連トピック

SLAAC アドレス割り当て （316 ページ）
ステートフル DHCPv6 アドレス割り当て （317 ページ）

ステートフル DHCP の外部的設定（CLI）

このインターフェイス設定は、外部DHCPサーバのステートフルDHCPv6を実装しているCisco IOS IPv6ルータ用です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	ユニキャスト用にIPv6を設定します。
ステップ 3	**dns-server 2001:100:0:1::1** 例： `Device (config-dhcpv6)# dns-server 2001:100:0:1::1`	DHCPクライアントにDNSサーバのオプションを提供します。
ステップ 4	**domain-name example.com** 例： `Device (config-dhcpv6)# domain-name example.com`	DHCPクライアントにドメイン名オプションを提供します。
ステップ 5	**exit** 例： `Device (config-dhcpv6)# exit`	前のモードに戻ります。
ステップ 6	**interface vlan1** 例： `Device (config)# interface vlan 1`	インターフェイスモードを開始して、ステートフル DHCP を設定します。
ステップ 7	**description IPv6-DHCP-Stateful** 例： `Device (config-if)# description IPv6-DHCP-Stateful`	ステートフル IPv6 DHCP の説明を入力します。
ステップ 8	**ipv6 address 2001:DB8:0:20::1/64** 例： `Device (config-if)# ipv6 address 2001:DB8:0:20::1/64`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。

	コマンドまたはアクション	目的
ステップ 9	**ip address** `192.168.20.1 255.255.255.0` 例： `Device (config-if)# ip address 192.168.20.1 255.255.255.0`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 10	**ipv6 nd prefix** `2001:db8::/64` **no-advertise** 例： `Device (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	アドバタイズしてはならない、IPv6 ルーティングプレフィックスアドバタイズメントを設定します。
ステップ 11	**ipv6 nd managed-config-flag** 例： `Device (config-if)# ipv6 nd managed-config-flag`	ホストでアドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 12	**ipv6 nd other-config-flag** 例： `Device (config-if)# ipv6 nd other-config-flag`	ホストで非アドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 13	**ipv6 dhcp_relaydestination** `2001:DB8:0:20::2` 例： `Device (config-if)# ipv6 dhcp_relay destination 2001:DB8:0:20::2`	インターフェイスに DHCP サーバを設定します。

関連トピック

SLAAC アドレス割り当て （316 ページ）
ステートフル DHCPv6 アドレス割り当て （317 ページ）

IPv6 アドレス ラーニング設定の確認

次に、**show ipv6 dhcp pool** コマンドの出力例を示します。このコマンドは、デバイス上の IPv6 サービス設定を表示します。vlan 21 の設定済みプールの詳細には、プールからアドレスを現在使用している 6 つのクライアントが表示されます。

手順

	コマンドまたはアクション	目的

ステップ 1	**show ipv6 dhcp pool**
	例：
	`Deviceshow ipv6 dhcp pool`
	`DHCPv6 pool: vlan21`
	`Address allocation prefix: 2001:DB8:0:1:FFFF:1234::/64 valid 86400 preferred 86400 (6 in use, 0 conflicts)`
	`DNS server: 2001:100:0:1::1`
	`Domain name: example.com`
	`Active clients: 6`
		デバイス上の IPv6 サービス設定を表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	『*IPv6 Command Reference (Catalyst 3850 Switches)*』
IP コマンド リファレンス	『*IP Command Reference (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 クライアント アドレス ラーニングの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 クライアント アドレス ラーニング機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 18 章

IPv6 WLAN セキュリティの設定

- IPv6 WLAN セキュリティの前提条件 （343 ページ）
- IPv6 WLAN セキュリティの制限 （343 ページ）
- IPv6 WLAN セキュリティについて （344 ページ）
- IPv6 WLAN セキュリティの設定方法 （347 ページ）
- その他の参考資料 （362 ページ）
- IPv6 WLAN セキュリティの機能情報 （363 ページ）

IPv6 WLAN セキュリティの前提条件

クライアント VLAN をデバイスで設定された WLAN にマッピングする必要があります。

IPv6 WLAN セキュリティの制限

RADIUS サーバのサポート

- 冗長性を保つために複数の RADIUS サーバが設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバでユーザデータベースを同一にする必要があります。

Radius ACS サポート

- Cisco Secure Access Control Server（ACS）とデバイスの両方で、RADIUS を設定する必要があります。
- RADIUS は、Cisco Secure ACS バージョン 3.2 以降のリリースでサポートされます。

IPv6 WLAN セキュリティについて

RADIUS の概要

Remote Authentication Dial-In User Service（RADIUS）とは、ネットワークへの管理アクセス権を取得しようとするユーザに対して中央管理されたセキュリティ機能を提供する、クライアント/サーバプロトコルです。これは、ローカルEAPに類似したバックエンドデータベースとして機能し、認証サービスおよびアカウンティング サービスを提供します。

- 認証：デバイスにログインしようとするユーザを検証するプロセス。

  デバイスでRADIUSサーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。複数のデータベースを設定する場合は、バックエンド データベースを試行する順序を指定します。

- アカウンティング：ユーザによる処理と変更を記録するプロセス。

  ユーザによる処理が正常に実行される度に、RADIUSアカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。RADIUS アカウンティング サーバが到達不能の場合、ユーザは中断なく、セッションを続行できます。

ユーザ データグラム プロトコル：RADIUS では、その転送にユーザ データグラム プロトコル（UDP）を使用します。RADIUS では、1 つのデータベースが保持されます。そして、UDP ポート 1812 で受信認証要求がリッスンされ、UDP ポート 1813 で受信アカウンティング要求がリッスンされます。アクセス コントロールを要求するデバイスは、クライアントとして動作し、サーバから AAA サービスを要求します。デバイスとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

複数の RADIUS アカウンティングおよび認証サーバを設定します。たとえば、1 台の RADIUS 認証サーバを中央に配置し、複数の RADIUS アカウンティング サーバを異なる地域に配置できます。同じタイプのサーバを複数設定すると、最初のサーバで障害が発生したり、接続不能になったりしても、コントローラは、必要に応じて 2 台目や 3 台目あるいはそれ以降のサーバへの接続を自動的に試行します。

RADIUS 方式が WLAN に対して設定されている場合、デバイスは WLAN に対して設定されている RADIUS 方式を使用します。ローカル EAP を使用するように WLAN を設定すると、WLAN で設定されている RADIUS 方式はローカルをポイントします。WLAN には、使用するローカル EAP プロファイルの名前を設定する必要もあります。

RADIUS 方式が WLAN に対して設定されていない場合、デバイスはグローバル モードで定義されているデフォルトの RADIUS 方式を使用します。

ローカル EAP について

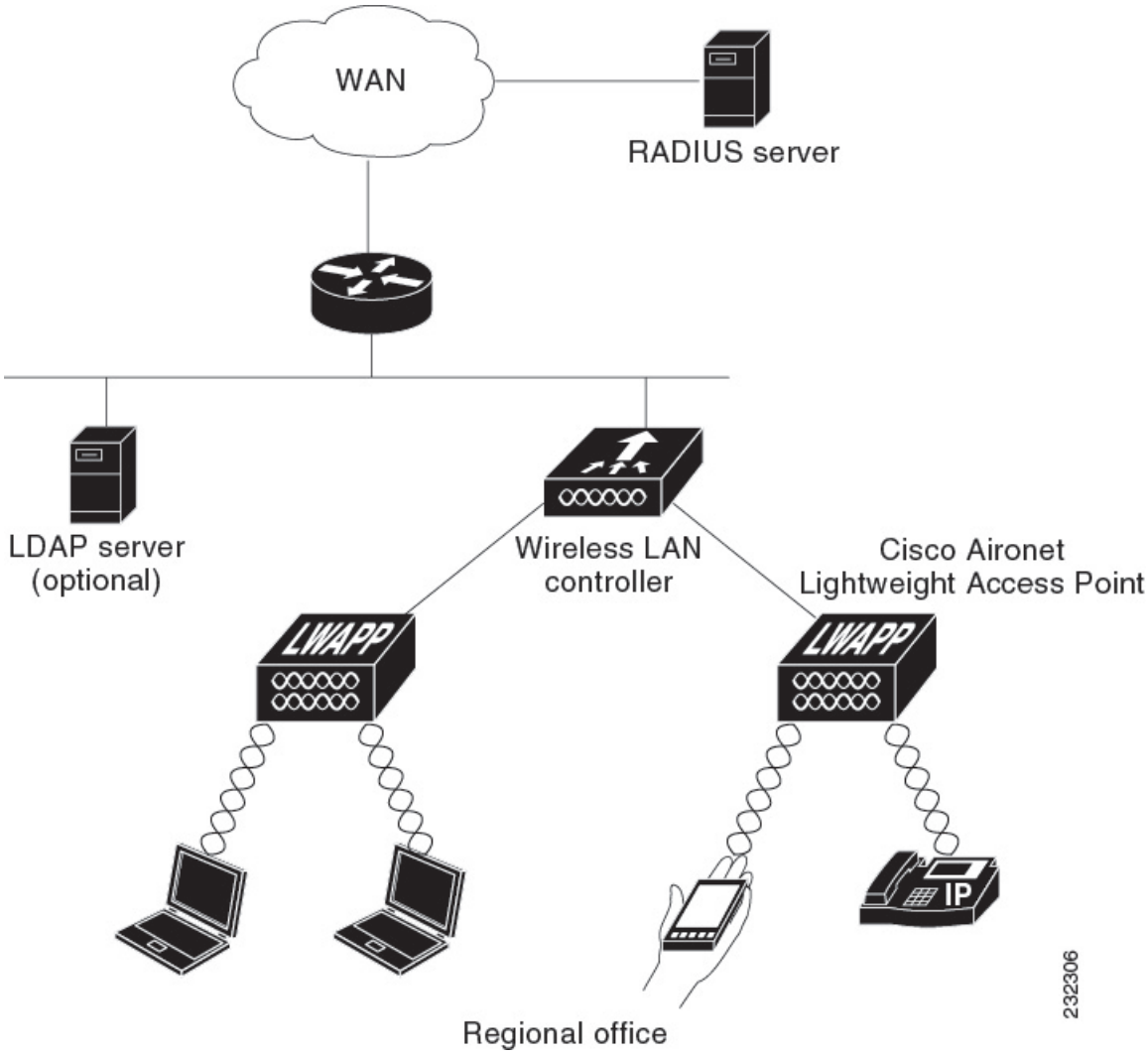
ローカル EAP は、ユーザおよびワイヤレス クライアントのローカル認証を可能にする認証方式です。この方式は、バックエンドシステムが妨害されたり、外部認証サーバが停止した場合でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。ローカル EAP を有効にすると、デバイスは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバに依存する必要がなくなります。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザのクレデンシャルを取得して、ユーザを認証します。ローカル EAP では、コントローラとワイヤレス クライアント間で、LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC 認証方式をサポートします。

EAP プロファイル名なしで実施される、または存在しない名前の EAP プロファイルが実施される場合、EAP はデフォルトでローカル認証用の EAP 方式を割り当てません。

（注） LDAP バックエンドデータベースでは、ローカル EAP 方式として、EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC がサポートされます。LEAP、EAP-FAST/MSCHAPv2、および PEAPv0。MSCHAPv2 は平文のパスワードを返すように LDAP サーバが設定されている場合にのみサポートされます。

（注） デバイスは、Microsoft Active Directory や Novell の eDirectory などの外部 LDAP データベースに対するローカル EAP 認証をサポートしています。Novell の eDirectory に対するローカル EAP 認証用にコントローラを設定する方法の詳細については、『Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database』ホワイトペーパーを参照してください。

図 *12 :* ローカル *EAP* の例



関連トピック

ローカル ユーザの作成 （347 ページ）
クライアント VLAN とインターフェイスの作成 （347 ページ）
EAP プロファイルの設定 （349 ページ）
クライアント VLAN の作成 （359 ページ）
外部 RADIUS サーバを使用した 802.1x WLAN の作成 （361 ページ）

IPv6 WLAN セキュリティの設定方法

ローカル認証の設定

ローカル ユーザの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**username aaa_test** 例： `Device(config)# username aaa_test`	ユーザ名を作成します。
ステップ 3	**password 0 aaa_test** 例： `Device(config)# usernameaaa_test password 0 aaa_test`	ユーザ名のパスワードを割り当てます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Device# configure terminal
Device(config)# username aaa_test password 0 aaa_test
Device(config)# end
```

関連トピック

IPv6 WLAN セキュリティについて （344 ページ）

クライアント VLAN とインターフェイスの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**vlan** 例： `Device(config)# vlan 137`	VLAN を作成します。
ステップ 3	**exit** 例： `Device (config-vlan)# exit`	VLAN コンフィギュレーション モードを終了します。
ステップ 4	**interface vlan vlan_ID** 例： `Device (config)# interface vlan 137`	インターフェイスに VLAN を関連付けます。
ステップ 5	**ip address** 例： `Device(config-if)# ip address 10.7.137.10 255.255.255.0`	VLAN インターフェイスに IP アドレスを割り当てます。
ステップ 6	**ipv6 address** 例： `Device(config-if)#ipv6 address 2001:db8::20:1/64`	VLAN インターフェイスに IPv6 アドレスを割り当てます。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

```
Device# configure terminal
Device(config)# vlan 137
Device(config-vlan)#exit
Device(config)#interface vlan 137
Device(config-if)#ip address 10.7.137.10 255.255.255.0
Device(config-if)#ipv6 address 2001:db8::20:1/64
Device(config-if)#end
```

関連トピック

IPv6 WLAN セキュリティについて （344 ページ）

EAP プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**eap profile name** 例： `Device(config)# eap profile wcm_eap_prof`	EAP プロファイルを作成します。
ステップ 2	**method leap** 例： `Device(config-eap-profile)# method leap`	プロファイルで EAP-LEAP 方式を設定します。
ステップ 3	**method tls** 例： `Device(config-eap-profile)# method tls`	プロファイルでEAP-TLS方式を設定します。
ステップ 4	**method peap** 例： `Device(config-eap-profile)# method peap`	プロファイルで PEAP 方式を設定します。
ステップ 5	**method mschapv2** 例： `Device(config-eap-profile)# method mschapv2`	プロファイルで EAP-MSCHAPV2 方式を設定します。
ステップ 6	**method md5** 例： `Device(config-eap-profile)# method md5`	プロファイルで EAP-MD5 方式を設定します。
ステップ 7	**method gtc** 例： `Device(config-eap-profile)# method gtc`	プロファイルで EAP-GTC 方式を設定します。

ステップ 8	**method fast profile my-fast**
	例：
	`Device(config-eap-profile)# eap method fast profile my-fast`
	`Device (config-eap-profile)#description my_local eap profile`
		my-fast という EAP プロファイルを作成します。

	コマンドまたはアクション	目的
ステップ 9	**description my_localeap profile** 例： `Device (config-eap-profile)#description my_local eap profile`	ローカルプロファイルの説明を指定します。
ステップ 10	**exit** 例： `Device (config-eap-profile)# exit`	eapプロファイルコンフィギュレーション モードを終了します。
ステップ 11	**eap method fast profilemyFast** 例： `Device (config)# eap method fast profile myFast`	EAP 方式プロファイルを設定します。

ステップ 12	**authority-id** `[identity|information]`
	例：
	`Device(config-eap-method-profile)# authority-id identity my_identity`
	`Device(config-eap-method-profile)#authority-id information my_information`
		EAP 方式プロファイルの認証局 ID および情報を設定します。

ステップ 13	**local-key 0 key-name** 例： `Device(config-eap-method-profile)# local-key 0 test`	ローカル サーバ キーを設定します。
ステップ 14	**pac-password 0 password** 例： `Device(config-eap-method-profile)# pac-password 0 test`	手動の PAC プロビジョニング用の PAC パスワードを設定します。
ステップ 15	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーションモードを終了できます。

例

```
Device(config)#eap profile wcm_eap_prof
Device(config-eap-profile)#method leap
Device(config-eap-profile)#method tls
Device(config-eap-profile)#method peap
Device(config-eap-profile)#method mschapv2
Device(config-eap-profile)#method md5
Device(config-eap-profile)#method gtc
```

```
Device(config-eap-profile)#eap method fast profile my-fast
Device (config-eap-profile)#description my_local eap profile
Device(config-eap-profile)# exit
Device (config)# eap method fast profile myFast
Device(config-eap-method-profile)#authority-id identity my_identity
Device(config-eap-method-profile)#authority-id information my_information
Device(config-eap-method-profile)#local-key 0 test
Device(config-eap-method-profile)#pac-password 0 test
Device(config-eap-method-profile)# end
```

関連トピック

IPv6 WLAN セキュリティについて （344 ページ）

ローカル認証モデルの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 2	**authentication dot1x default local** 例： `Device(config)# aaa authentication dot1x default local`	他の方法が見つからない場合、dot1x でデフォルトのローカル RADIUS を使用する必要があることを意味します。
ステップ 3	**dot1x method_list local** 例： `Device(config)# aaa authentication dot1x wcm_local local`	wcm_local 方式リスト用のローカル認証を割り当てます。
ステップ 4	**aaa authentication dot1x dot1x_name local** 例： `Device(config)# aaa authentication dot1x aaa_auth local`	dot1x 方式用のローカル認証を設定します。
ステップ 5	**aaa authorization credential-download name local** 例： `Device(config)# aaa authorization credential-download wcm_author local`	Local/RADIUS/LDAP から EAP クレデンシャルをダウンロードするようにローカル データベースを設定します。
ステップ 6	**aaa local authentication auth-name authorization authorization-name** 例：	ローカル認証および許可を選択します。

	コマンドまたはアクション	目的
	`Device(config)# aaa local authentication wcm_local authorization wcm_author`	
ステップ 7	**session ID** 例： `Device(config)# aaa session-id common`	AAA のセッション ID を設定します。
ステップ 8	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	dot.1x システム認証制御をイネーブルにします。

例

```
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default local
Device(config)# aaa authentication dot1x wcm-local local
Device(config)# aaa authentication dot1x aaa_auth local
Device(config)# aaa authorization credential-download wcm_author local
Device(config)# aaa local authentication wcm_local authorization wcm_author
Device(config)# aaa session-id common
Device(config)# dot1x system-auth-control
```

クライアント WLAN の作成

（注） この例では、ダイナミック WEP の 802.1x を使用しています。ワイヤレス クライアントでサポートされ、デバイスで設定可能な他の任意のセキュリティ メカニズムも使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**wlan wlan name <identifier> SSID** 例： `Device(config)# wlan wlanProfileName 1 ngwcSSID`	WLAN を作成します。
ステップ 3	**broadcast-ssid** 例：	WLAN で SSID をブロードキャストするように設定します。

	コマンドまたはアクション	目的
	`Device(config-wlan)# broadcast-ssid`	
ステップ 4	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WLAN の wpa をディセーブルにして、802.1x をイネーブルにします。
ステップ 5	**security dot1x** 例： `Device(config-wlan)# security dot1x`	WLAN の 802.1x 暗号化セキュリティを設定します。
ステップ 6	**security** dot1x authentication-list *wcm-local* 例： `Device(config-wlan)# security dot1x authentication-list wcm-local`	dot1x 認証用に WLAN へのサーバ グループ マッピングを設定します。
ステップ 7	**local-auth wcm_eap_prof** 例： `Device (config-wlan)# local-auth wcm_eap_profile`	ローカル認証用に WLAN に eap プロファイルを設定します。
ステップ 8	**client vlan** *137* 例： `Device(config-wlan)# client vlan 137`	WLAN に VLAN を関連付けます。
ステップ 9	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

```
Device# config terminal
Device(config)#wlan wlanProfileName 1 ngwcSSID
Device(config-wlan)#broadcast-ssid
Device(config-wlan)#no security wpa
Device(config-wlan)#security dot1x
Device(config-wlan)#security dot1x authentication-list wcm-local
Device (config-wlan)# local-auth wcm_eap_prof
Device(config-wlan)#client vlan 137
Device(config-wlan)#no shutdown
Device(config-wlan)#end
Device#
```

関連トピック

WPA2+AES 用クライアント VLAN の作成 （355 ページ）

WPA2+AES でのローカル認証の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**aaa new model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 3	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	dot1x システム認証制御をイネーブルにします。
ステップ 4	**aaa authentication dot1x default local** 例： `Device(config)# aaa authentication dot1x default local`	デフォルト dot1x 方式用のローカル認証を設定します。
ステップ 5	**aaa local authorization credential-download default local** 例： `Device(config)# aaa authorization credential-download default local`	ローカル サーバから EAP クレデンシャルをダウンロードするようにデフォルトデータベースを設定します。
ステップ 6	**aaa local authentication default authorization default** 例： `Device(config)# aaa local authentication default authorization default`	デフォルトのローカル認証および許可を選択します。
ステップ 7	**eap profile wcm_eap_profile** 例： `Device(config)#eap profile wcm_eap_profile`	EAP プロファイルを作成します。
ステップ 8	**method leap** 例：	プロファイルで EAP-LEAP 方式を設定します。

	コマンドまたはアクション	目的
	`Device(config)# method leap`	
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# dot1x system-auth-control
Device(config)# aaa authentication dot1x default local
Device(config)# aaa authorization credential-download default local
Device(config)# aaa local authentication default authorization default
Device(config)#eap profile wcm_eap_profile
Device(config)# method leap
Device(config)# end
```

WPA2+AES 用クライアント VLAN の作成

ローカル認証の WPA2+AES タイプの VLAN を作成します。この VLAN は、後で WLAN にマッピングされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan vlan_ID** 例： `Device (config)# vlan 105`	VLAN を作成します。
ステップ 3	**exit** 例： `Device (config-vlan)# exit`	VLAN モードを終了します。
ステップ 4	**interface** vlan **vlan_ID** 例： `Device(config)# interface vlan 105`	インターフェイスに VLAN を関連付けます。
ステップ 5	**ip address** 例： `Device(config-if)# ip address 10.8.105.10 255.255.255.0`	VLAN インターフェイスに IP アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 6	**ipv6 address** 例： `Device(config-if)#ipv6 address 2001:db8::10:1/64`	VLAN インターフェイスに IPv6 アドレスを割り当てます。
ステップ 7	**exit** 例： `Device (config-if)# exit`	インターフェイスモードを終了します。

```
Device# configure terminal
Device(config)# vlan105
Device (config-vlan)# exit
Device (config)# interface vlan 105
Device(config-if)#ip address 10.8.105.10 255.255.255.0
Device(config-if)#ipv6 address 2001:db8::10:1/64
Device(config-if)#exit
Device(config)#
```

関連トピック

クライアント WLAN の作成 （352 ページ）

WPA2+AES 用 WLAN の作成

WLAN を作成し、WPA2+AES 用に作成されたクライアント VLAN にマッピングします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。

ステップ 2	**wlan wpas2-aes-wlan 1 wpas2-aes-wlan**
	例：
	`Device(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan`
	`Device(config-wlan)#`
		WLAN を作成します。

ステップ 3	**client vlan 105**
	例：
	`Device(config-wlan)#client vlan 105`
	`Device(config-wlan)#`
		クライアント VLAN に WLAN をマッピングします。

ステップ 4	**local-auth wcm_eap_profile** 例：	WLAN に EAP プロファイルを作成し、設定します。

	コマンドまたはアクション	目的
	`Device(config-wlan)#local-auth wcm_eap_profile`	
ステップ 5	**security dot1x authentication-list default** 例： `Device(config-wlan)#security dot1x authentication-list default`	デフォルトの dot1x 認証リストを使用します。

ステップ 6	**no shutdown**
	例：
	`Device(config-wlan)#no shutdown`
	`Device(config-wlan)#`
		WLAN をイネーブルにします。

ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Device# configure terminal
Device(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan
Device(config-wlan)#client vlan 105
Device(config-wlan)#local-auth wcm_eap_profile
Device(config-wlan)#security dot1x authentication-list default
Device(config-wlan)#no shutdown
Device(config-wlan)# exit
```

外部 RADIUS サーバの設定

RADIUS 認証サーバ ホストの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**radius server One** 例： `Device (config)# radius server One`	RADIUS サーバを作成します。
ステップ 3	**address ipv4 address auth-portauth_port_number acct-port acct_port_number** 例：	RADIUS サーバの IPv4 アドレスを設定します。

	コマンドまたはアクション	目的
	`Device (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813`	
ステップ 4	**address ipv6 address auth-portauth_port_number acct-port acct_port_number** 例： `Device (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813`	RADIUS サーバの IPv6 アドレスを設定します。
ステップ 5	**key 0cisco** 例： `Device (config-radius-server)# key 0 cisco`	**exit**
ステップ 6	例： `Device (config-radius-server)# exit`	RADIUS サーバ モードを終了します。

```
Device# configure terminal
Device (config)# radius server One
Device (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813
Device (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813
Device (config-radius-server)# key 0 cisco
Device (config-radius-server)#exit
```

関連トピック

RADIUS 認証サーバ グループの設定 （358 ページ）

RADIUS 認証サーバ グループの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**aaa new-model** 例： `Device(config)#aaa new-model`	AAA 認証モデルを作成します。

ステップ 3	**aaa group server radius wcm_rad**
	例：
	`Device(config)# aaa group server radius wcm_rad`
	`Device(config-sg-radius)#`
		RADIUS サーバ グループを作成します。

	コマンドまたはアクション	目的

ステップ 4	**server <ip address>auth-port1812acct-port1813**
	例：
	`Device(config-sg-radius)# server One auth-port 1812 acct-port 1813`
	`Device(config-sg-radius)# server Two auth-port 1812 acct-port 1813`
	`Device(config-sg-radius)# server Three auth-port 1812 acct-port 1813`
		ステップ 3 で作成した RADIUS グループにサーバを追加します。RADIUS アカウンティング サーバおよび認証サーバの UDP ポートを設定します。

ステップ 5	**aaa authentication dot1x method_list group wcm_rad** 例： `Device(config)# aaa authentication dot1x method_list group wcm_rad`	RADIUS グループに方式リストをマッピングします。
ステップ 6	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	RADIUS グループのシステム認証制御をイネーブルにします。
ステップ 7	**aaa session-idcommon** 例： `Device(config)# aaa session-id common`	RADIUS グループから、特定のコールに対して送信されるすべてのセッション ID 情報が同じであることを確認します。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius wcm_rad
Device(config-sg-radius)# server One auth-port 1812 acct-port 1813
Device(config-sg-radius)# server Two auth-port 1812 acct-port 1813
Device(config-sg-radius)# server Three auth-port 1812 acct-port 1813
Device(config)# aaa authentication dot1x method_list group wcm_rad
Device(config)# dot1x system-auth-control
Device(config)# aaa session-id common
Device(config)#
```

関連トピック

RADIUS 認証サーバ ホストの設定 （357 ページ）

クライアント VLAN の作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**vlan 137** 例： `Device(config)# vlan 137`	VLAN を作成してインターフェイスに関連付けます。
ステップ 3	**exit** 例： `Device (config-vlan)# exit`	VLAN モードを終了します。
ステップ 4	**interface vlan 137** 例： `Device (config)# interface vlan 137`	インターフェイスに VLAN を割り当てます。
ステップ 5	**ip address 10.7.137.10 255.255.255.0** 例： `Device(config-if)# ip address 10.7.137.10 255.255.255.0`	VLAN インターフェイスに IPv4 アドレスを割り当てます。
ステップ 6	**ipv6 address 2001:db8::30:1/64** 例： `Device(config-if)# ipv6 address 2001:db8::30:1/64`	VLAN インターフェイスに IPv6 アドレスを割り当てます。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Device# configure terminal
Device(config)# vlan137
Device(config-vlan)# exit
Device(config)# interface vlan137
Device(config-if)# ip address 10.7.137.10 255.255.255.0
Device(config-if)# ipv6 address 2001:db8::30:1/64
Device(config-if)# end
```

関連トピック

外部 RADIUS サーバを使用した 802.1x WLAN の作成 （361 ページ）
IPv6 WLAN セキュリティについて （344 ページ）

外部 RADIUS サーバを使用した 802.1x WLAN の作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**wlan ngwc-1x<ssid>ngwc-1x** 例： `Device(config)# wlan ngwc_8021x 2 ngwc_8021x`	802.1x 認証用の新しい WLAN を作成します。
ステップ 3	**broadcast-ssid** 例： `Device(config-wlan)# broadcast-ssid`	WLAN で SSID をブロードキャストするように設定します。
ステップ 4	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WLAN の WPA をディセーブルにして、802.1x をイネーブルにします。
ステップ 5	**security dot1x** 例： `Device(config-wlan)# security dot1x`	WLAN の 802.1x 暗号化セキュリティを設定します。
ステップ 6	**security dot1x authentication-list wcm-rad** 例： `Device(config-wlan)# security dot1x authentication-list wcm-rad`	dot1x 認証用に WLAN へのサーバ グループ マッピングを設定します。
ステップ 7	**client vlan 137** 例： `Device(config-wlan)# client vlan 137`	WLAN に VLAN を関連付けます。
ステップ 8	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

```
Device# configure terminal
Device(config)#wlan ngwc_8021x 2 ngwc_8021x
Device(config-wlan)# broadcast-ssid
Device(config-wlan)# no security wpa
Device(config-wlan)# security dot1x
Device(config-wlan)# security dot1x authentication-list wcm-rad
Device(config-wlan)# client vlan 137
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

関連トピック

クライアント VLAN の作成 （359 ページ）
IPv6 WLAN セキュリティについて （344 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	『*IPv6 Command Reference (Catalyst 3850 Switches)*』
WLAN コマンド リファレンス	『*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』
WLAN の設定	『*WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 WLAN セキュリティの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 WLAN セキュリティ機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 19 章

IPv6 ACL の設定

- IPv6 ACL の前提条件 （365 ページ）
- IPv6 ACL の制限 （365 ページ）
- IPv6 ACL について （366 ページ）
- IPv6 ACL の設定 （369 ページ）
- IPv6 ACL の設定方法 （370 ページ）
- IPv6 ACL の確認 （377 ページ）
- IPv6 ACL の設定例 （378 ページ）
- その他の参考資料 （382 ページ）
- IPv6 ACL の機能情報 （383 ページ）

IPv6 ACL の前提条件

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。また、スイッチで IP ベース フィーチャ セットが稼働している場合、入力ルータ ACL を作成しそれを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

関連トピック

IPv6 ACL の作成 （370 ページ）

IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

デバイスは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- デバイスは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。

- デバイスは再帰 ACL（**reflect** キーワード）をサポートしません。
- デバイスは IPv6 フレームに MAC ベース ACL を適用しません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポートまたはSVI）にACLを適用する場合、デバイスはインターフェイスで ACL がサポートされるかどうかを判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ（ACE）を追加しようとする場合、デバイスは現在インターフェイスに適用されている ACL に ACE が追加されることを許可しません。

IPv6 ACL について

アクセス コントロール リスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます）。デバイスで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、またはワイヤレス クライアントとやり取りするデータ トラフィックの制御用の WLAN、あるいは中央処理装置（CPU）宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

Web 認証用に事前認証 ACL を作成することもできます。このような ACL は、認証が完了するまでに特定のタイプのトラフィックを許可するために使用されます。

IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

（注） ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

IPv6 ACL の概要

スイッチは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンド トラフィックまたはインバウンド トラフィックでサポートされます。IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。

- IPv6 ポート ACL は、レイヤ 2 インターフェイスのインバウンド トラフィックでだけサポートされます。IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。

IP ベース フィーチャ セットが稼働しているスイッチは、入力ルータ IPv6 ACL だけをサポートします。ポート ACL または出力ルータ IPv6 ACL はサポートされません。

（注） サポートされない IPv6 ACL を設定した場合、エラー メッセージが表示され、その設定は有効になりません。

スイッチは、IPv6 トラフィックの Virtual LAN（VLAN）ACL（VLAN マップ）をサポートしません。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

- SVI に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド IP パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに

  着信したパケットはポート ACL によってフィルタリングされます。発信ルーテッド IPv6 パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。

（注） いずれかのポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

関連トピック

IPv6 ACL の作成 （370 ページ）
インターフェイスへの IPv6 の適用 （375 ページ）
WLAN IPv6 ACL の作成 （376 ページ）
IPv6 ACL の表示 （377 ページ）

ACL のタイプ

ユーザあたりの IPv6 ACL

ユーザあたりの ACL の場合、テキスト文字列として、完全アクセス制御エントリ（ACE）が ACS で設定されます。

ACE はコントローラで設定されません。ACE は `ACCESS-Accept` 属性でデバイスに送信され、クライアント用に直接適用されます。ワイヤレス クライアントが外部デバイスにローミングするときに、ACE が、AAA 属性としてモビリティ ハンドオフ メッセージで外部デバイスに送信されます。ユーザあたりの ACL を使用した出力方向はサポートされていません。

フィルタ ID IPv6 ACL

filter-Id ACL の場合、完全な ACE および `acl name(filter-id)` がデバイスで設定され、`filter-id` のみが ACS で設定されます。`filter-id` は ACCESS-Accept 属性でデバイスに送信され、デバイスは ACE の filter-id をルックアップしてから、クライアントに ACE を適用します。クライアント L2 が外部デバイスにローミングするときに、filter-id だけがモビリティ ハンドオフ メッセージで外部デバイスに送信されます。ユーザあたりの ACL を使用した出力フィルタ ACL はサポートされていません。外部デバイスは filter-id と ACE を事前に設定する必要があります。

ダウンロード可能 IPv6 ACL

ダウンロード可能 ACL（dACL）の場合、完全な ACE および `dacl` 名はすべて ACS だけで設定されます。

（注） コントローラは ACL を設定しません。

ACS は `dacl` 名をデバイスに対しその `ACCESS-Accept` 属性で送信します。さらに `dacl` 名を使用して、ACE のために `dACL` 名が ACS に、`access-request` 属性によって戻されます。

ACS は `access-accept` 属性でデバイスの対応する ACE に応答します。ワイヤレス クライアントが外部デバイスにローミングするときに、`dacl` 名だけがモビリティ ハンドオフ メッセージで外部デバイスに送信されます。外部デバイスは、`dacl` 名の ACS サーバにアクセスして ACE を取得します。

IPv6 ACL とスイッチ スタック

スタック マスターは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバーに配信します。

（注） スイッチ スタック内で IPv6 を完全に機能させるには、すべてのスタック メンバーで拡張 IP サービス フィーチャ セットが稼働している必要があります。

新しいスイッチがスタック マスターを引き継ぐと、ACL 設定がすべてのスタック メンバーに配信されます。メンバ スイッチは、新しいスタック マスターによって配信された設定との同期をとり、不要なエントリを一掃します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、スタック マスターは変更内容をすべてのスタック メンバーに配信します。

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します。

始める前に

IPv6 ACL を設定する場合は、事前にデュアル IPv4 および IPv6 SDM テンプレートのいずれかを選択する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。	
ステップ 2	IPv6 ACL が、トラフィックをブロックする（拒否）または通過させる（許可）よう設定します。	
ステップ 3	トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。	
ステップ 4	インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。	

IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージ プロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。

- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリが満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはインターフェイスでドロップされます。

（注） 追加できなかった ACL と同じタイプのパケットのみ（ipv4、ipv6、MAC）がインターフェイスでドロップされます。

IPv6 ACL の設定方法

IPv6 ACL の作成

IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 access-list** *acl_name* 例： `ipv6 access-list access-list-name`	名前を使用して IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 3	**{deny|permit} protocol** 例：	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit

	コマンドまたはアクション	目的
	`{deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]`	を指定します。次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • source-ipv6-prefix/prefix-length または destination-ipv6-prefix/ prefix-length は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 • host source-ipv6-address または destination-ipv6-address には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 •（任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、lt（より小さい）、gt（より大きい）、eq（等しい）、neq（等しくない）、range（包含範囲）があります。 source-ipv6-prefix/prefix-length 引数のあとの operator は、送信元ポートに一致する必要があります。destination-ipv6-prefix/prefix-length 引数のあとの operator は、宛先ポートに一致する必要があります。 •（任意）port-number は、0 ～ 65535 の 10 進数または TCP あるいは UDP

	コマンドまたはアクション	目的
		ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）dscp value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィッククラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）fragments を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • （任意）log を指定すると、エントリと一致するパケットに関するログメッセージがコンソールに送信されます。log-input を指定すると、ログエントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 • （任意）routing を入力して、IPv6 パケットのルーティングを指定します。 • （任意）sequence value を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。 • （任意）time-range name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 4	**{deny|permit} tcp** 例： `{deny | permit} tcp {source-ipv6-prefix/prefix-length |`	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。パラメータはステップ 3 で説明されているパ

	コマンドまたはアクション	目的
	`any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	ラメータと同じですが、次に示すオプションのパラメータが追加されています。 • ack：確認応答（ACK）ビット セット • established：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • fin：終了ビット セット。送信元からのデータはそれ以上ありません。 • neq {port | protocol}：所定のポート番号上にないパケットだけを照合します。 • psh：プッシュ機能ビット セット • range {port | protocol}：ポート番号の範囲内のパケットだけを照合します。 • rst：リセット ビット セット • syn：同期ビット セット • urg：緊急ポインタ ビット セット
ステップ 5	**{deny|permit} udp** 例： `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port |protocol}] [range {port |protocol}] [routing][sequence value][time-range name]`	（任意）UDP アクセス リストおよびアクセス条件を定義します。 ユーザ データグラム プロトコルの場合は、udp を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [port]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。
ステップ 6	**{deny|permit} icmp** 例： `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]`	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージ プロトコルの場合は、icmp を入力します。ICMP パラメータはステップ 3a の IP プ

	コマンドまたはアクション	目的
	`{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]`	ロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • icmp-type：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0～255 です。 • icmp-code：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-message：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、?キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show ipv6 access-list** 例： `show ipv6 access-list`	アクセス リストの設定を確認します。
ステップ 9	**copy running-config startup-config** 例： `copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv6 ACL の前提条件 （365 ページ）
IPv6 ACL の概要 （366 ページ）
インターフェイスへの IPv6 の適用 （375 ページ）

WLAN IPv6 ACL の作成 （376 ページ）
IPv6 ACL の表示 （377 ページ）

インターフェイスへの IPv6 の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する手順について説明します。レイヤ 2 およびレイヤ 3 インターフェイスの発信または着信トラフィックに IPv6 ACL を適用できます。IPv6 ACL はレイヤ 3 インターフェイスの着信管理トラフィックにだけ適用できます。

インターフェイスへのアクセスを制御する管理には、特権EXECモードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface interface_id** 例： `Device# interface interface-id`	アクセス リストを適用するレイヤ 2 インターフェイス（ポート ACL 用）またはレイヤ3スイッチ仮想インターフェイス（ルータ ACL 用）を特定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** 例： `Device# no switchport`	レイヤ2モード（デフォルト）からレイヤ3モードにインターフェイスを変更します（ルータ ACL を適用する場合のみ）。
ステップ 4	**ipv6 address** *ipv6_address* 例： `Device# ipv6 address ipv6-address`	レイヤ3インターフェイス（ルータ ACL 用）で Ipv6 アドレスを設定します。 （注） このコマンドは、レイヤ 2 インターフェイスでは、またはインターフェイスに明示的な IPv6 アドレスが設定されている場合には、必要ありません。
ステップ 5	**ipv6 traffic-filter** *acl_name* 例： `Device# ipv6 traffic-filter access-list-name {in | out}`	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ステップ 7	**show running-config interface tenGigabitEthernet 1/0/3**
	例：
	`Device# show running-config interface tenGigabitEthernet 1/0/3`
	`.....`
	`.....`
	`Building configuration .....`
	`.....`
	`Current configuration : 98 bytes`
	`!`
	`interface TenGigabitEthernet1/0/3`
	` switchport mode trunk`
	` ipv6 traffic-filter MyFilter out`
	`end`
		設定の概要を示します。

ステップ 8	**copy running-config startup-config** 例： `copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv6 ACL の作成 （370 ページ）
IPv6 ACL の概要 （366 ページ）
WLAN IPv6 ACL の作成 （376 ページ）
IPv6 ACL の表示 （377 ページ）

WLAN IPv6 ACL の作成

手順

	コマンドまたはアクション	目的
ステップ 1	**ipv6 traffic-filter acl** *acl_name* 例： `Device(config-wlan)# ipv6 traffic-filter acl <acl_name>`	名前付き WLAN ACL を作成します。
ステップ 2	**ipv6 traffic-filter acl web** 例：	WLAN ACL の事前認証を作成します。

	コマンドまたはアクション	目的
	`Device(config-wlan)# ipv6 traffic-filter acl web <acl_name-preauth>`	

```
Device(config-wlan)# ipv6 traffic-filter acl <acl_name>
Device(config-wlan)#ipv6 traffic-filter acl web <acl_name-preauth>
```

関連トピック

IPv6 ACL の作成 （370 ページ）
インターフェイスへの IPv6 の適用 （375 ページ）
IPv6 ACL の概要 （366 ページ）
IPv6 ACL の表示 （377 ページ）

IPv6 ACL の確認

IPv6 ACL の表示

1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**show access-list** 例： `Device# show access-lists`	デバイスに設定されたすべてのアクセス リストを表示します。
ステップ 2	**show ipv6 access-list** *acl_name* 例： `Device# show ipv6 access-list [access-list-name]`	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

関連トピック

IPv6 ACL の作成 （370 ページ）
インターフェイスへの IPv6 の適用 （375 ページ）
WLAN IPv6 ACL の作成 （376 ページ）
IPv6 ACL の概要 （366 ページ）

IPv6 ACL の設定例

例：IPv6 ACL の作成

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番めの拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番めの許可エントリは、その他のすべてのトラフィックを許可します。暗黙の全否定の条件が各 IPv6 アクセス リストの末尾にあるため、2 番めの許可エントリは必要です。

（注） ロギングは、レイヤ 3 インターフェイスでのみサポートされます。

```
Device(config)# ipv6 access-list CISCO
Device(config-ipv6-acl)# deny tcp any any gt 5000
Device (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Device(config-ipv6-acl)# permit icmp any any
Device(config-ipv6-acl)# permit any any
```

例：IPv6 ACL の適用

次に、レイヤ 3 インターフェイスの発信トラフィックに対して、アクセス リスト Cisco を適用する例を示します。

```
Device(config)# interface TenGigabitEthernet 1/0/3

Device(config-if)# no switchport
Device(config-if)# ipv6 address 2001::/64 eui-64
Device(config-if)# ipv6 traffic-filter CISCO out
```

例：IPv6 ACL の表示

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Device #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

次に、show ipv6 access-lists 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Device# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
```

```
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

例：RA スロットリングと NS 抑制の設定

このタスクでは、省電力のワイヤレスクライアントが頻繁な非請求の定期的RAに影響されないように、RA スロットル ポリシーを作成する方法について説明します。非請求タイプのマルチキャスト RA は、コントローラによってスロットルされます。

始める前に

クライアント マシンで IPv6 をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd ra-throttler policy Mythrottle** 例： `Device (config)# ipv6 nd ra-throttler policy Mythrottle`	Mythrottle という RA スロットラ ポリシーを作成します。
ステップ 3	**throttle-period 20** 例： `Device (config-nd-ra-throttle)# throttle-period 20`	スロットリングを適用する時間間隔セグメントを特定します。
ステップ 4	**max-through 5** 例： `Device (config-nd-ra-throttle)# max-through 5`	許容する初期 RA の数を特定します。
ステップ 5	**allow at-least 3 at-most 5** 例： `Device (config-nd-ra-throttle)# allow at-least 3 at-most 5`	初期RAが送信された後に、間隔セグメントの終了まで許容されるRAの数を特定します。
ステップ 6	**switch (config)# vlan configuration 100** 例： `Device (config)# vlan configuration 100`	vlan あたりの設定を作成します。

	コマンドまたはアクション	目的
ステップ 7	**ipv6 nd suppress** 例： `Device (config)# ipv6 nd suppress`	Vlan でネイバー探索をディセーブルにします。
ステップ 8	**ipv6 nd ra-th attach-policy attach-policy_name** 例： `Device (config)# ipv6 nd ra-throttle attach-policy attach-policy_name`	ルータ アドバタイズメント スロットリングをイネーブルにします。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例：RA ガード ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**ipv6 nd raguard policy MyPloicy** 例： `Device (config)# ipv6 nd raguard policy MyPolicy`	
ステップ 2	**trusted-port** 例： `Device (config-nd-raguard)# trusted-port`	上記で作成したポリシーの信頼できるポートを設定します。

ステップ 3	**device-role router**
	例：
	`Device (config-nd-raguard)# device-role [host|monitor|router|switch]`
	`Device (config-nd-raguard)# device-role router`
		上記で作成した信頼できるポートにRAを送信可能な信頼できるデバイスを定義します。

ステップ 4	**interface tenGigabitEthernet 1/0/1** 例： `Device (config)# interface tenGigabitEthernet 1/0/1`	信頼できるデバイスにインターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 nd raguard attach-policy MyPolicy** 例： `Device (config-if)# ipv6 nd raguard attach-policy Mypolicy`	ポートから受信した RA を信頼するようにポリシーを設定し、接続します。
ステップ 6	**vlan configuration 19-21,23** 例： `Device (config)# vlan configuration 19-21,23`	ワイヤレス クライアントの vlan を設定します。
ステップ 7	**ipv6 nd suppress** 例： `Device (config-vlan-config)# ipv6 nd suppress`	無線上でND メッセージを抑制します。
ステップ 8	**ipv6 snooping** 例： `Device (config-vlan-config)# ipv6 snooping`	IPv6 トラフィックをキャプチャします。
ステップ 9	**ipv6 nd raguard attach-policy MyPolicy** 例： `Device (config-vlan-config)# ipv6 nd raguard attach-policy Mypolicy`	ワイヤレス クライアントの vlan に RA ガード ポリシーを接続します。
ステップ 10	**ipv6 nd ra-throttler attach-policy Mythrottle** 例： `Device (config-vlan-config)#ipv6 nd ra-throttler attach-policy Mythrottle`	ワイヤレス クライアントの vlan に RA スロットリング ポリシーを接続します。

例：IPv6 ネイバー バインディングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**ipv6 neighbor binding** [vlan]**19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc** 例：	送信元 MAC アドレスとして aaa.bbb.ccc が設定されたインターフェイス te1/0/3 を介して VLAN 19 で送信する場合にのみ有効なネイバー 2001:db8::25:4 を設定して検証します。

	コマンドまたはアクション	目的
	`Device (config)# ipv6 neighbor binding vlan 19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc`	

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	『*IPv6 Command Reference (Catalyst 3850 Switches)*』
ACL 設定	『*Security Configuration Guide (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 ACL の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 ACL 機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 20 章

IPv6 Web 認証の設定

- IPv6 Web 認証の前提条件 （385 ページ）
- IPv6 Web 認証の制限 （385 ページ）
- IPv6 Web 認証について （386 ページ）
- IPv6 Web 認証の設定方法 （387 ページ）
- IPv6 Web 認証の確認 （392 ページ）
- その他の参考資料 （394 ページ）
- IPv6 Web 認証の機能情報 （395 ページ）

IPv6 Web 認証の前提条件

次の設定を、IPv6 Web 認証を開始する前に行う必要があります。

- IPv6 デバイス トラッキング
- IPv6 DHCP スヌーピング
- wlan 上の 802.1x タイプのセキュリティをディセーブルにします。
- 各 WLAN には、vlan が関連付けられている必要があります。
- デフォルトの wlan 設定を **shutdown** から **no shutdown**に変更します。

関連トピック

WLAN のセキュリティのイネーブル化 （388 ページ）

IPv6 Web 認証の制限

次の制限は、IPv6 Web 認証の使用時に適用されます。

関連トピック

WLAN のセキュリティのイネーブル化 （388 ページ）

IPv6 Web 認証について

Web 認証は、レイヤ 3 セキュリティ機能です。デバイスでは、有効なユーザ名とパスワードを入力するまで、特定のクライアントからの IP トラフィック（DHCP および DNS 関連パケットを除く）を拒否します。これはサプリカントまたはクライアントユーティリティを必要としないシンプルな認証方式です。一般に Web 認証は、ゲスト アクセス ネットワークを展開する顧客が使用します。HTTP と HTTPS の両方からのトラフィックで、ページがログイン ページを表示できるようにします。

（注） Web 認証は、データ暗号化を提供せず、通常は、接続が常に重要になるホット スポットまたはキャンパス環境用のシンプルなゲスト アクセスとして使用されます。

WLAN は、Web ベース認証の**security webauth** として設定されます。デバイスは次のタイプの Web ベース認証をサポートしています。

- Web 認証：クライアントが Web ページにクレデンシャルを入力し、次に Wlan コントローラによって検証されます。
- Web 同意：Wlan コントローラは、[Accept/Deny] ボタンが用意されたポリシー ページを提供します。ネットワークにアクセスするには、[Accept] ボタンをクリックします。

（注） デバイスでサポートされる Web 認証の最大連続セッションは 1 秒間に 40 個です。

一般に Wlan はオープン認証用に設定されます。つまり、レイヤ 2 認証なしで、Web ベースの認証メカニズムが使用されるときに設定されます。

Web 認証プロセス

次のイベントは、WLAN が Web 認証用に設定されている場合に発生します。

- ユーザは、Web ブラウザを開き、URL アドレスとして、たとえば、*http://www.example.com* を入力します。クライアントは、この URL の DNS 要求を送信して、宛先の IP アドレスを取得します。デバイスは DNS 要求を DNS サーバにバイパスし、サーバは宛先 *www.example.com* の IP アドレスが含まれている DNS 応答で応答します。次にこれがワイヤレス クライアントに転送されます。
- クライアントは、宛先 IP アドレスで TCP 接続を開こうとします。*www.example.com* の IP アドレス宛ての TCP SYN パケットを送信します。
- デバイスにはクライアントに設定されたルールがあり、*www.example.com* のプロキシとして機能できません。*www.example.com* の IP アドレスとしての送信元とともにクライアントに TCP SYN-ACK パケットを戻します。クライアントは、スリーウェイ TCP ハンドシェイクを完了するために TCP ACK パケットを戻し、TCP 接続が完全に確立されます。

- クライアントは、*www.example.com* 宛ての HTTP GET パケットを送信します。デバイスはこのパケットをインターセプトし、リダイレクト処理用に送信します。HTTP アプリケーション ゲートウェイは、クライアントによって要求された HTTP GET への応答として、HTML 本文を準備し送信します。この HTML では、クライアントはデバイスのデフォルトの Web ページ（たとえば、*http://<Virtual-Server-IP>/login.html*）に転送されます。
- クライアントは、たとえば、*www.example.com* などの IP アドレスとの TCP 接続を閉じます。
- クライアントは仮想 IP に移動する場合に、デバイスの仮想 IP アドレスで TCP 接続を開こうとします。デバイスに、仮想 IP 用の TCP SYN パケットを送信します。
- デバイスは TCP SYN-ACK で返答し、クライアントはハンドシェイクを完了するために、TCP ACK をデバイスに戻します。
- クライアントは、ログイン ページの要求のために、仮想 IP 宛ての */login.html* 用に HTTP GET を送信します。
- この要求は、デバイスの Web サーバで許可され、サーバはデフォルト ログイン ページで応答します。クライアントは、ユーザがログインできるブラウザ ウィンドウでログイン ページを受信します。

関連トピック

WPA のディセーブル化 （387 ページ）
WLAN のセキュリティのイネーブル化 （388 ページ）
WLAN のパラメータ マップのイネーブル化 （389 ページ）
WLAN の認証リストのイネーブル化 （389 ページ）
グローバル Web 認証 WLAN パラメータ マップの設定 （390 ページ）
WLAN の設定 （390 ページ）
グローバル コンフィギュレーション モードの IPv6 のイネーブル化 （392 ページ）
パラメータ マップの確認 （392 ページ）
認証リストの確認 （393 ページ）

IPv6 Web 認証の設定方法

WPA のディセーブル化

始める前に

802.1x をディセーブルにします。一般的な Web 認証では、レイヤ 2 セキュリティを使用しません。レイヤ 2 セキュリティを削除するには、この設定を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan test1 2 test1** 例： `Device(config)# wlan test1 2 test1`	WLAN を作成し、SSID を割り当てます。
ステップ 3	**no security** wpa 例： `Device(config-wlan)# no security wpa`	Wlan に対して WPA のサポートをディセーブルにします。

次のタスク

次をイネーブルにします。

- セキュリティ Web 認証
- パラメータ ローカル
- 認証リスト

関連トピック

Web 認証プロセス （386 ページ）

WLAN のセキュリティのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**parameter-map type web-auth global** 例： `Device(config)# parameter-map type web-auth global`	すべての Web 認証 wlan にパラメータ マップを適用します。
ステップ 2	**virtual-ip ipv4 192.0.2.1** 例： `Device(config-params-parameter-map)# virtual-ip ipv4 192.0.2.1`	仮想ゲートウェイの IPv4 アドレスを定義します。

	コマンドまたはアクション	目的
ステップ 3	**virtual-ip ipv6 2001:db8::24:2** 例： `Device(config-params-parameter-map)# virtual-ip ipv6 2001:db8::24:2`	仮想ゲートウェイの IPv6 アドレスを定義します。

関連トピック

IPv6 Web 認証の前提条件 （385 ページ）
IPv6 Web 認証の制限 （385 ページ）
Web 認証プロセス （386 ページ）

WLAN のパラメータ マップのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**security web-auth parameter-map <mapname>** 例： `Device(config-wlan)# security web-auth parameter-map webparalocal`	wlan 用の Web 認証をイネーブルにし、パラメータ マップを作成します。

関連トピック

Web 認証プロセス （386 ページ）

WLAN の認証リストのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**security web-auth authentication-list webauthlistlocal** 例： `Device(config-wlan)# security web-auth`	wlan 用の Web 認証をイネーブルにし、ローカル Web 認証リストを作成します。

関連トピック

Web 認証プロセス （386 ページ）

グローバル Web 認証 WLAN パラメータ マップの設定

この例を使用して、グローバル Web 認証 WLAN を設定し、パラメータ マップを追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	**parameter-map type webauth global** 例： `Device (config)# parameter-map type webauth global`	グローバル Web 認証を設定し、パラメータ マップを追加します。
ステップ 2	**virtual-ip ipv6 2001:db8:4::1** 例： `Device (config-params-parameter-map)# virtual-ip ipv6 2001:db8:4::1`	認証用のワイヤレス クライアントに表示される仮想ゲートウェイ IP アドレスを定義します。
ステップ 3	**ratelimit init-state-sessions 120** 例： `Device (config-params-parameter-map)# ratelimit init-state-sessions 120`	グローバル レート制限を設定して、デバイスで Web クライアントが使用できる帯域幅を制限し、オーバーフラッディング攻撃を防止します。
ステップ 4	**max-https-conns 70** 例： `Device (config-params-parameter-map)# max-http-conns 70`	オーバーフラッディング攻撃を防止するため、デバイスで試行される http 接続の最大数を設定します。

関連トピック

Web 認証プロセス （386 ページ）
WLAN の設定 （390 ページ）

WLAN の設定

始める前に

- WLAN は、Vlan が関連付けられている必要があります。デフォルトでは、新しい Wlan は常に設定要件に応じて変更できる Vlan 1 に関連付けられます。
- WLAN を *no shutdown* に設定して、イネーブルにします。デフォルトでは、Wlan は *shutdown* パラメータで設定され、ディセーブルです。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *1* 例： `Device(config-wlan)# wlan 1 name vicweb ssid vicweb`	wlan を作成し、SSID を割り当てます。
ステップ 2	**client vlan** *interface ID* 例： `Device(config-wlan)# client vlan VLAN0136`	クライアントを vlan インターフェイスに割り当てます。
ステップ 3	**security web-auth authentication list webauthlistlocal** 例： `Device(config-wlan)# security web-auth authentication-list webauthlistlocal`	wlan 用の Web 認証を設定します。
ステップ 4	**security web-auth parameter-map global** 例： `Device(config-wlan)# security web-auth parameter-map global`	wlan にパラメータ マップを設定します。
ステップ 5	**no security wpa** 例： `Device(config-wlan)# no security wpa`	wlan のセキュリティ ポリシーを設定します。これにより wlan がイネーブルになります。
ステップ 6	**no shutdown** 例： `Device(config-wlan)# no shutdown`	Wlanを設定して、イネーブルにします。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

グローバル Web 認証 WLAN パラメータ マップの設定 （390 ページ）
Web 認証プロセス （386 ページ）
グローバル コンフィギュレーション モードの IPv6 のイネーブル化 （392 ページ）

グローバル コンフィギュレーション モードの IPv6 のイネーブル化

Web 認証用にグローバル コンフィギュレーションの IPv6 をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**web-auth global** 例： `Device(config)# parameter-map type webauth global`	パラメータ マップのタイプを Web 認証としてグローバルに設定します。
ステップ 3	**virtual IPv6** 例： `Device(config-params-parameter-map)# virtual-ip ipv6`	Web 認証用の仮想 IP として IPv6 を選択します。 （注） Web 認証用の優先 IP として IPv4 を選択することもできます。

関連トピック

WLAN の設定 （390 ページ）
Web 認証プロセス （386 ページ）
パラメータ マップの確認 （392 ページ）

IPv6 Web 認証の確認

パラメータ マップの確認

Wlan に対して設定したパラメータ マップを確認するには、**show running configuration** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show running config** 例： `Deviceshow running config`	デバイスの実行コンフィギュレーション全体を表示します。パラメータ マップのグレップを行い結果を表示します。

```
wlan alpha 2 alpha
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list webauthlistlocal
 security web-auth parameter-map webparalocal
```

関連トピック

グローバル コンフィギュレーション モードの IPv6 のイネーブル化 （392 ページ）
Web 認証プロセス （386 ページ）
認証リストの確認 （393 ページ）

認証リストの確認

Wlan に対して設定した認証リストを確認するには、**show running configuration** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show running configuration** 例： `Device#show running-config`	Wlan の設定を表示します。 `Device# show running-config`
ステップ 2	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Device#show running-config
 ..................................
 ..................................
 ..................................
 wlan alpha 2 alpha
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list webauthlistlocal
 security web-auth parameter-map webparalocal
 ..................................
 ..................................
 ..................................
```

関連トピック

パラメータ マップの確認 （392 ページ）
Web 認証プロセス （386 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	『*IPv6 Command Reference (Catalyst 3850 Switches)*』
Web 認証設定	『*Security Configuration Guide (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 Web 認証の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 Web 認証機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 21 章

IPv6 クライアント モビリティの設定

- IPv6 クライアント モビリティの前提条件 （397 ページ）
- IPv6 クライアント モビリティの制限 （397 ページ）
- IPv6 クライアント モビリティについて （398 ページ）
- IPv6 クライアント モビリティの確認 （402 ページ）
- IPv6 クライアント モビリティのモニタリング （402 ページ）
- その他の参考資料 （403 ページ）
- IPv6 クライアント モビリティの機能情報 （404 ページ）

IPv6 クライアント モビリティの前提条件

ワイヤレス IPv6 クライアント接続をイネーブルにするには、基礎となる有線ネットワークで、SLAAC または DHCPv6 などの IPv6 ルーティングおよびアドレス割り当て機能をサポートしている必要があります。デバイスは IPv6 ルータに対する L2 隣接関係が必要です。また、VLAN はパケットがデバイスに着信するときにタグを付ける必要があります。AP は、IPv6 ネットワーク上で接続を必要としません。すべてのトラフィックが AP とデバイス間の IPv4 CAPWAP トンネル内でカプセル化されるためです。

IPv6 クライアント モビリティの制限

- IPv6 クライアント モビリティを使用する場合、クライアントはスタティック ステートレス自動設定（Windows XP クライアントなど）またはステートフル DHCPv6 IP アドレッシング（Windows 7 クライアントなど）とともに IPv6 をサポートする必要があります。
- ステートフル DHCPv6 IP アドレッシングが円滑に動作できるようにするには、DHCPv6 サーバとして動作するように設定された DHCP for IPv6 機能をサポートするスイッチまたはルータ（デバイスなど）、または組み込み DHCPv6 サーバを備えた Windows 2008 サーバなどの専用サーバが必要です。Cisco Catalyst 3850 スイッチおよび Cisco Catalyst 5700 スイッチは、（内部的に）DHCPv6 サーバとして機能できます。

（注） Cisco Catalyst 3850 スイッチに SDM IPv6 テンプレートをロードするには、**sdm prefer dual-ipv4** および **v6** デフォルト コマンドを入力し、スイッチをリセットします。

IPv6 クライアント モビリティについて

デバイスは、IPv6 専用ノードまたはデュアル スタック ノードに対し IPv6 モビリティをサポートします。IPv6 クライアント モビリティは次のレイヤに分かれます。

- リンク層および
- ネットワーク層

リンク層は、リンク層接続を失うことなく、同じ SSID で識別される同一 BSS（基本サービス セット）の任意の AP にクライアントがローミングできるようにする 802.11 プロトコルによって処理されます。

ただし、リンク層モビリティは、ローミング中にワイヤレス クライアントのレイヤ 3 アプリケーションがシームレスに動作を継続するには十分ではありません。Cisco IOSd のワイヤレス モビリティ モジュールは、モビリティ トンネリングを使用して、クライアントが異なるスイッチ上の異なるサブネット間をローミングするときに、クライアントのレイヤ 3 PoP（Point of Presence）用のシームレスな接続を維持します。

IPv6 は、プロトコルの TCP/IP スイートの IPv4 に代わることを目的とした次世代ネットワーク層インターネット プロトコルです。この新しいバージョンでは、一意のグローバル IP アドレスを必要とするユーザとアプリケーションに対応するためのインターネット グローバル アドレス空間を増大させます。IPv6 は、128 ビットの送信元アドレスおよび宛先アドレスを組み込むことにより、32 ビットの IPv4 アドレスよりも格段に多くのアドレスを提供します。

コントローラをまたいだ IPv6 クライアントをサポートするには、IPv6 クライアントが同じレイヤ 3 ネットワーク上にとどまるように、ICMPv6 メッセージを特別に処理する必要があります。デバイスは、ICMPv6 メッセージを代行受信することで IPv6 クライアントを追跡し、シームレスなモビリティを提供して、ネットワーク攻撃からネットワークを保護します。NDP（ネイバー ディスカバリ パケット）パケットは、マルチキャストからユニキャストに変換され、クライアントごとに個別に配信されます。この固有なソリューションによって、ネイバーディスカバリ パケットとルータ アドバタイズメント パケットの VLAN 間でのリークを防止できます。クライアントは、特定のネイバー ディスカバリ パケットおよびルータ アドバタイズメントパケットを受信することで IPv6 アドレス指定が適切であることを確認し、不要なマルチキャスト トラフィックを回避します。

IPv6 モビリティの設定は、IPv4 モビリティと同一であり、シームレスなローミングを実現するためにクライアント側で別個のソフトウェアを使用する必要はありません。デバイスは、同じモビリティ グループに属している必要があります。IPv4 と IPv6 の両クライアント モビリティが、デフォルトで有効になります。

IPv6 クライアント モビリティは次のことに使用されます。

- レイヤ 2 およびレイヤ 3 ローミングでのクライアント IPv6 複数アドレスの維持
- IPv6 ネイバー探索プロトコル（NDP）パケットの管理
- クライアントの IPv6 アドレスの学習

ルータ アドバタイズメントの使用

ネイバー探索プロトコル（NDP）はリンク層で動作し、リンク上の他のノードの検出を行います。他のノードのリンク層アドレスを特定し、使用可能なルータを検索し、他のアクティブなネイバー ノードのパスに関する到達可能性情報を維持します。

ルータ アドバタイズメント（RA）は、使用可能なルータを検出し、IPv6 アドレス、リンク MTU などを生成するネットワーク プレフィクスを取得するためにホストで使用される IPv6 ネイバー探索プロトコル（NDP）パケットの 1 つです。ルータは、定期的またはホスト ルータ送信要求メッセージへの応答として RA を送信します。

IPv6 ワイヤレス クライアント モビリティは IPv6 RA パケットを管理します。集約アクセスデバイスは、リンクローカル全ノード マルチキャスト RA パケットをローカルおよび RA が受信される同じ VLAN にマップされたローミング ワイヤレス ノードに転送します。

図 1 では、ワイヤレス ノード モビリティでのリンクローカル全ノード マルチキャスト RA の転送の問題について説明します。

図 *13*：ルータ *2* から無効な *RA* を受け取るローミング クライアント

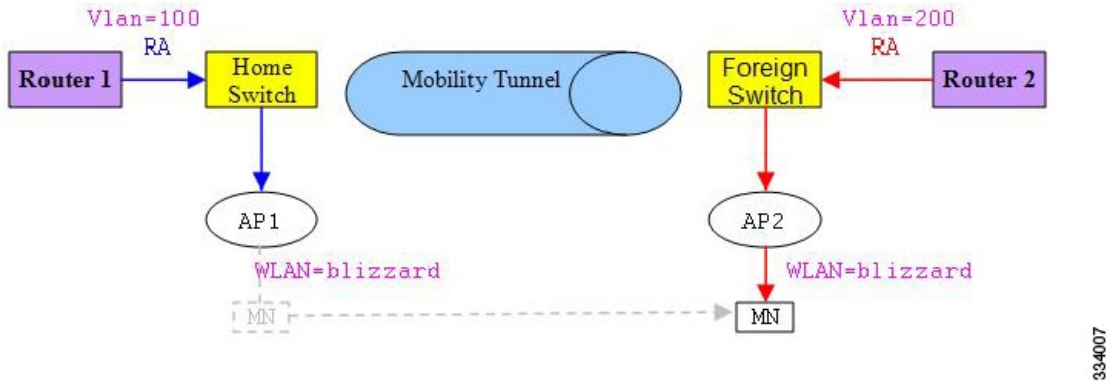
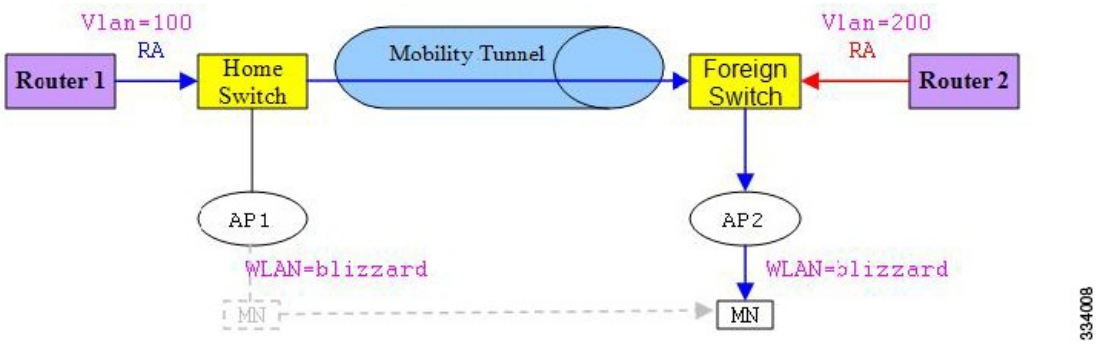


図 2 では、ローミング クライアント「MN」が外部スイッチで VLAN 200 から RA をどのように受信するか、および新しい IP アドレスを取得してどのように L3 モビリティの PoP（Point of Presence）に入るかを示しています。

図 *14*：ルータ *1* から有効な *RA* を受け取るローミング クライアント



関連トピック

IPv6 クライアント モビリティの確認 （402 ページ）
IPv6 クライアント モビリティのモニタリング （402 ページ）

RA スロットリングと NS 抑制

頻繁な非請求タイプの定期的RAによる制約を受けないように省電力ワイヤレス クライアントを保護するため、コントローラで非請求タイプのマルチキャスト RA をスロットルできます。

関連トピック

IPv6 クライアント モビリティの確認 （402 ページ）
IPv6 クライアント モビリティのモニタリング （402 ページ）

IPv6 アドレス ラーニング

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定（SLAAC）
- ステートフル DHCPv6
- 静的設定

これらの方法の場合、IPv6 クライアントは常に NS DAD（重複アドレス検出）要求を送信して、ネットワークに重複する IP アドレスがないようにします。デバイスはクライアントの NDP および DHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習し、コントローラ データベースを更新します。データベースは、クライアントの新しい IP アドレスについて通知します。

関連トピック

IPv6 クライアント モビリティの確認 （402 ページ）
IPv6 クライアント モビリティのモニタリング （402 ページ）

複数の IP アドレスの処理

RUN 状態後に新しい IP アドレスが受信されると、追加の場合も削除の場合も、コントローラは表示目的でそのローカルデータベース上の新しいIPアドレスを更新します。基本的に、IPv6 は既存または IPv4 の場合と同じ PEM ステート マシン コード フローを使用します。IP アドレスが、たとえば、外部エンティティによってPrime Infrastructureから要求されると、コントローラは、すべての使用可能な IP アドレス、IPv4 および IPv6 を外部エンティティへの API/SPI インターフェイスに含めます。

IPv6 クライアントは、様々な目的でスタックから複数の IP アドレスを取得できます。たとえば、リンクローカル トラフィックのリンクローカル アドレスおよびルーティング可能な固有のローカル アドレスまたはグローバル アドレスがあります。

クライアントが DHCP 要求状態にあり、コントローラが IPv4 または IPv6 アドレス用にデータベースから最初の IP アドレスの通知を受信すると、PEM はクライアントを RUN 状態に移行させます。

RUN状態後に新しいIPアドレスが受信されるときは、追加の場合も削除の場合も、コントローラは表示目的でそのローカル データベース上の新しい IP アドレスを更新します。

IP アドレスが、たとえば、外部エンティティによって Prime Infrastructure から要求されると、コントローラは、使用可能な IP アドレス、IPv4 および IPv6 を外部エンティティに提供します。

関連トピック

IPv6 クライアント モビリティの確認 （402 ページ）
IPv6 クライアント モビリティのモニタリング （402 ページ）

IPv6 Configuration

デバイスは IPv4 クライアントと同様にシームレスに IPv6 クライアントをサポートします。管理者は、IPV6、IPv6 スヌーピングおよびスロットリング機能を有効にするには、Vlan を手動で設定する必要があります。これにより、デバイスとそのさまざまなクライアント間でのスロットリングを NDP パケットで行えます。

関連トピック

IPv6 クライアント モビリティの確認 （402 ページ）
IPv6 クライアント モビリティのモニタリング （402 ページ）

ハイ アベイラビリティ

スイッチはクライアント IP アドレスが学習しにくいときにワイヤレス クライアントと同期します。スイッチオーバーが発生すると、IPv6 ネイバー バインディング テーブルがスタンバイ ステートに同期されます。ただし、スイッチオーバーが完了し、ネイバーバインディングテーブルがそのクライアントの最新情報で更新されると、ワイヤレス クライアント自体はアソシエート解除され、新しいアクティブ ステートに再アソシエートされます。

再アソシエーション時に、クライアントが他の AP に移動すると、バインディング テーブル内の元のエントリがしばらくの間ダウンとマークされ、期限切れになります。

別の AP からスイッチを結合する新しいエントリの場合は、新しい IP アドレスが学習されて、コントローラのデータベースに通知されます。

（注） この機能は、Cisco Catalyst 3850 スイッチでのみ使用できます。

関連トピック

IPv6 クライアント モビリティの確認 （402 ページ）
IPv6 クライアント モビリティのモニタリング （402 ページ）

IPv6 クライアント モビリティの確認

表 25 に示すコマンドは、IPv6 クライアント モビリティに適用されます。

表 *24 : Cisco 5760 WLC* の *IPv6* クライアント モビリティを確認するためのコマンド

コマンド	説明
debug mobility ipv6	すべてのワイヤレス クライアント IPv6 モビリティのデバッグをイネーブルにします。
debug **client** **mac-address** **(mac-addr)**	ワイヤレス クライアントのデバッグを表示します。デバッグ情報の MAC アドレスを入力します。

関連トピック

ルータ アドバタイズメントの使用 （399 ページ）
RA スロットリングと NS 抑制 （400 ページ）
IPv6 アドレス ラーニング （400 ページ）
複数の IP アドレスの処理 （401 ページ）
IPv6 Configuration （401 ページ）
ハイ アベイラビリティ （401 ページ）
IPv6 クライアント モビリティのモニタリング （402 ページ）

IPv6 クライアント モビリティのモニタリング

表 26 のコマンドは、デバイススイッチで IPv6 クライアント モビリティをモニタリングするために使用されます。

表 *25 : IPv6* クライアント モビリティ コマンドのモニタリング

コマンド	説明
show wireless client summary	アクティブなクライアントのワイヤレス固有設定を表示します。
show wireless client mac-address (mac-addr)	アクティブなクライアントのワイヤレス固有設定をその MAC アドレスに基づいて表示します。

関連トピック

IPv6 クライアント モビリティの確認 （402 ページ）
ルータ アドバタイズメントの使用 （399 ページ）
RA スロットリングと NS 抑制 （400 ページ）
IPv6 アドレス ラーニング （400 ページ）
複数の IP アドレスの処理 （401 ページ）
IPv6 Configuration （401 ページ）
ハイ アベイラビリティ （401 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	『*IPv6 Command Reference (Catalyst 3850 Switches)*』
モビリティ設定	『*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 クライアント モビリティの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 クライアント モビリティ機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 22 章

IPv6 モビリティの設定

- IPv6 モビリティの前提条件 （405 ページ）
- IPv6 モビリティについて （405 ページ）
- IPv6 モビリティの設定方法 （406 ページ）
- IPv6 モビリティのモニタリング （406 ページ）
- その他の参考資料 （409 ページ）
- IPv6 モビリティの機能情報 （410 ページ）

IPv6 モビリティの前提条件

モビリティとその関連のインフラストラクチャを設定して使用できるようにする必要があります。

IPv6 モビリティについて

モビリティ（ローミング）は、できるだけ低遅延で、確実かつスムーズに、あるアクセスポイントから別のアクセス ポイントへのアソシエーションを維持する無線 LAN クライアントの機能です。この項では、デバイスが無線ネットワークに存在する場合のモビリティの動作について説明します。

あるワイヤレス クライアントがアクセス ポイントにアソシエートして認証すると、アクセスポイントのデバイスは、クライアントデータベースにそのクライアントに対するエントリを設定します。このエントリには、クライアントの MAC アドレス、IP アドレス、セキュリティ コンテキストおよびアソシエーション、Quality of Service（QoS）コンテキスト、WLAN、およびアソシエートされたアクセスポイントが含まれます。デバイスはこの情報を使用してフレームを転送し、ワイヤレス クライアントで送受信されるトラフィックを管理します。

ワイヤレス クライアントがそのアソシエーションをあるアクセス ポイントから別のアクセスポイントへ移動する場合、デバイスは新たにアソシエートするアクセスポイントでクライアントのデータベースをアップデートするだけです。必要に応じて、新たなセキュリティ コンテキストとアソシエーションも確立されます。しかし、クライアントが 1 つのデバイスに接続されたアクセス ポイントから別のデバイスに接続されたアクセス ポイントにローミングする際に

は、プロセスはより複雑になります。また、同一のサブネット上でこれらのデバイスが動作しているかどうかによっても異なります。

コントローラ間ローミング

クライアントが新たなデバイスに接続されたアクセスポイントへアソシエートする場合、新たなデバイスはモビリティメッセージを元のデバイスと交換し、スティッキアンカリングがディセーブルの場合に、クライアントのデータベースエントリは新たなデバイスに移動されます。

関連トピック

IPv6 モビリティのモニタリング （406 ページ）

スティッキ アンカリングでのサブネット内ローミング、およびサブネット間ローミング

サブネット間ローミングは、デバイスがクライアントのローミングに関するモビリティ メッセージを交換する点でコントローラ間ローミングと似ています。ただし、クライアントのデータベースエントリを新しいデバイスに移動するのではなく、元のデバイスのクライアントデータベース内で該当クライアントに「アンカー」エントリのマークが付けられます。このデータベース エントリが新しいデバイスのクライアント データベースにコピーされ、新しいデバイス内で「外部」エントリのマークが付けられます。ローミングはワイヤレスクライアントには透過的なまま行われ、クライアントは元の IP アドレスを保持します。

サブネット間ローミングでは、アンカーと外部の両デバイスのWLANに、ソースベースのルーティングやソースベースのファイアウォールは設定せずに同一のネットワーク アクセス権限を設定する必要があります。そのようにしない場合、ハンドオフ後クライアントにネットワーク接続上の問題が発生することがあります。

モビリティの設定の詳細については、『Cisco 5700 Wireless LAN Controller Mobility Configuration Guide, Cisco IOS XE, Release 3.2SE』を参照してください。

関連トピック

IPv6 モビリティのモニタリング （406 ページ）

IPv6 モビリティの設定方法

IPv6 モビリティのモニタリング

この章では、モビリティ関連IPv6設定を表示します。モビリティ関連の設定を確認するには、『Cisco 5700 Wireless LAN Controller Mobility Configuration Guide, Cisco IOS XE 3.2SE』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 neighbors binding mac C0C1.C06B.C4E2** 例： `Device# show ipv6 neighbors binding mac C0C1.C06B.C4E2`	IPv6 関連のモビリティ設定を表示します。

例

```
Device# show ipv6 neighbors binding mac C0C1.C06B.C4E2
Binding Table has 45 entries, 37 dynamic (limit 100)
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other Packet,
API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    IPv6 address                              Link-Layer addr Interface vlan prlvl  age
 state    Time left
L   FE80:20:25::16                            2037.064C.BA71  Vl25        25  0100 3137mn
 REACHABLE
L   FE80:20:24::16                            2037.064C.BA41  Vl24        24  0100 3137mn
 REACHABLE
L   FE80:20:23::16                            2037.064C.BA44  Vl23        23  0100 3137mn
 REACHABLE
ND  FE80:20:23::13                            2037.0653.6BC4  Te1/0/1     23  0005   85s
 REACHABLE  223 s try 0
ND  FE80:20:22::17                            2037.064D.06F6  Te1/0/1     22  0005    3mn
 REACHABLE  92 s try 0
L   FE80:20:22::16                            2037.064C.BA76  Vl22        22  0100 3137mn
 REACHABLE
ND  FE80:20:22::13                            2037.0653.6BF6  Te1/0/1     22  0005  165s
 REACHABLE  136 s try 0
ND  FE80:20:22::12                            2037.064C.94F6  Te1/0/1     22  0005   23s
 REACHABLE  281 s try 0
ND  FE80:20:22::2                             0022.550E.8FC3  Te1/0/1     22  0005   18s
 REACHABLE  295 s try 0
ND  FE80:20:21::17                            2037.064D.06E8  Te1/0/1     21  0005    4mn
 REACHABLE  60 s try 0
L   FE80:20:21::16                            2037.064C.BA68  Vl21        21  0100 3137mn
 REACHABLE
ND  FE80:20:21::13                            2037.0653.6BE8  Te1/0/1     21  0005   57s
 REACHABLE  252 s try 0
ND  FE80:20:21::12                            2037.064C.94E8  Te1/0/1     21  0005    4s
 REACHABLE  297 s
ND  FE80:20:21::2                             0022.550E.8FC2  Te1/0/1     21  0005    2s
 REACHABLE  307 s try 0
ND  FE80::F866:8BE0:12E4:39CF                 C0C1.C06B.C4E2  Ca4         21  0005    3mn
 REACHABLE  89 s try 0
ND  FE80::6D0A:DB33:D69E:91C7                 0050.B606.A6CE  Te1/0/1     22  0005  135s
 REACHABLE  171 s try 0
ND  FE80::985:8189:9937:BB05                  8CA9.8295.09CC  Ca0         21  0005   15s
 REACHABLE  287 s
ND  FE80::20:24:13                            2037.0653.6BC1  Te1/0/1     24  0005  155s
```

```
 REACHABLE  145 s try 0
L   2001:20:23::16                          2037.064C.BA44  Vl23        23  0100 3137mn
 REACHABLE
DH  2001:20:22:0:C96C:AF29:5DDC:2689        0050.B606.A6CE  Te1/0/1     22  0024   19s
 REACHABLE  286 s try 0(16574
DH  2001:20:22:0:A46B:90B2:F0DB:F952        0050.B606.A6CE  Te1/0/1     22  0024 2339mn
 STALE      32401 s
DH  2001:20:22:0:7DFD:14EC:B1E4:1172        0050.B606.A6CE  Te1/0/1     22  0024 2339mn
 STALE      24394 s
DH  2001:20:22:0:7CB3:D6DD:FD6A:50F         0050.B606.A6CE  Te1/0/1     22  0024 2333mn
 STALE      29195 s
DH  2001:20:22:0:6D32:AF24:FDE1:2504        0050.B606.A6CE  Te1/0/1     22  0024  509mn
 STALE      118821 s
DH  2001:20:22:0:5106:5AD:FE98:A2F0         0050.B606.A6CE  Te1/0/1     22  0024 2328mn
 STALE      31362 s
ND  2001:20:22::201:13                      0050.B606.A6CE  Te1/0/1     22  0005   49s
 REACHABLE  264 s try 0
L   2001:20:22::16                          2037.064C.BA76  Vl22        22  0100 3137mn
 REACHABLE
ND  2001:20:22::13                          2037.0653.6BF6  Te1/0/1     22  0005  175s
 REACHABLE  131 s try 0
ND  2001:20:22::2                           0022.550E.8FC3  Te1/0/1     22  0005   28s
 REACHABLE  274 s try 0
ND  2001:20:21:0:F866:8BE0:12E4:39CF        C0C1.C06B.C4E2  Ca4         21  0005    4mn
 REACHABLE  21 s try 0
ND  2001:20:21:0:C085:9D4C:4521:B777        0021.CC73.AA17  Te1/0/1     21  0005   11s
 REACHABLE  290 s try 0
ND  2001:20:21:0:6233:4BFF:FE1A:744C        6033.4B1A.744C  Ca4         21  0005    3mn
 REACHABLE  108 s try 0
ND  2001:20:21:0:447E:745D:2F48:1C68        8CA9.8295.09CC  Ca0         21  0005   34s
 REACHABLE  276 s
ND  2001:20:21:0:3920:DDE8:B29:AD51         C0C1.C06B.C4E2  Ca4         21  0005    3mn
 REACHABLE  87 s try 0
ND  2001:20:21:0:1016:A333:FAD5:6E66        0021.CC73.AA17  Te1/0/1     21  0005    4mn
 REACHABLE  18 s try 0
ND  2001:20:21:0:C42:E317:BA9B:EB17         6033.4B1A.744C  Ca4         21  0005    4mn
 REACHABLE  61 s try 0
ND  2001:20:21:0:985:8189:9937:BB05         8CA9.8295.09CC  Ca0         21  0005  135s
 REACHABLE  173 s try 0
ND  2001:20:21::201:20                      0021.CC73.AA17  Te1/0/1     21  0005    4mn
 REACHABLE  43 s try 0
ND  2001:20:21::17                          2037.064D.06E8  Te1/0/1     21  0005    4mn
 REACHABLE  50 s try 0
L   2001:20:21::16                          2037.064C.BA68  Vl21        21  0100 3137mn
 REACHABLE
ND  2001:20:21::13                          2037.0653.6BE8  Te1/0/1     21  0005   67s
 REACHABLE  237 s try 0
ND  2001:20:21::12                          2037.064C.94E8  Te1/0/1     21  0005    5mn
 REACHABLE  512 ms try 0
ND  2001:20:21::2                           0022.550E.8FC2  Te1/0/1     21  0005   12s
 REACHABLE  294 s try 0
```

関連トピック

コントローラ間ローミング （406 ページ）
スティッキ アンカリングでのサブネット内ローミング、およびサブネット間ローミング（406 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	『*IPv6 Command Reference (Catalyst 3850 Switches)*』
モビリティ設定	『*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 モビリティの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 モビリティ機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 VI 部

IP

- 『Configuring HSRP』 （413 ページ）
- NHRP の設定 （441 ページ）
- VRRPv3 プロトコルのサポート （453 ページ）
- GLBP の設定 （471 ページ）

第 23 章

『Configuring HSRP』

• HSRP の設定 （413 ページ）

HSRP の設定

この章では、ホットスタンバイルータプロトコル（HSRP）を使用する方法について説明します。これによって、IP トラフィック ルーティングに冗長性を提供し、個々のルータのアベイラビリティに依存しないルーティングを実現します。

レイヤ 2 モードの HSRP のバージョンを使用すると、クラスタ コマンド スイッチが故障した場合、クラスタ管理を引き継ぐ冗長コマンド スイッチを設定することもできます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

HSRP の設定に関する情報

HSRP の概要

HSRP は、デフォルト ゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファーストホップ冗長性を確保することでネットワークのアベイラビリティを高めるシスコの標準方式です。HSRP を使用すると、特定のルータのアベイラビリティに依存せず IP トラフィックをルーティングできます。また、一連のルータ インターフェイスを組み合わせることで、1 台の仮想ルータ、または LAN 上のホストへのデフォルト ゲートウェイのように機能させるこ

とができます。ネットワークまたはセグメント上に HSRP を設定すると、仮想 MAC（メディア アクセス コントロール）アドレス、および設定されたルータ グループ間で共有される IP アドレスを使用できるようになりHSRP が設定された複数のルータは、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスを使用できるようになります。仮想ルータは、実際には存在しません。仮想ルータは、相互にバックアップ機能を提供するように設定されている複数のルータの共通のターゲットを表します。1 台のルータがアクティブなルータとして、もう 1 台のルータがスタンバイ ルータとして選択されます。スタンバイ ルータは、指定されたアクティブ ルータが故障した場合に、グループの MAC アドレスおよび IP アドレスを制御するルータです。

（注） HSRP グループ内のルータには、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）など、HSRP をサポートする任意のルータ インターフェイスを指定できます。

HSRP は、ネットワーク上のホストからの IP トラフィックに冗長性を提供することで、ネットワークのアベイラビリティを高めます。アクティブ ルータは、ルータ インターフェイスのグループ内でパケットのルーティングを実行するために選択されたルータです。スタンバイ ルータは、アクティブ ルータが故障した場合、または事前に設定した条件が満たされた場合に、ルーティング作業を引き継ぐルータです。

HSRP は、ホストがルータ ディスカバリ プロトコルをサポートしておらず、選択されたルータのリロードや電源故障時に新しいルータに切り替えることができない場合に有効です。HSRP をネットワーク セグメントに設定すると、HSRP は仮想 MAC アドレスと IP アドレスを 1 つずつ提供します。このアドレスは、HSRP が動作するルータ インターフェイス グループ内のルータ インターフェイス間で共有できます。プロトコルによってアクティブ ルータとして選択されたルータは、グループの MAC アドレス宛てのパケットを受信し、ルーティングします。n 台のルータで HSRP が稼働している場合、n +1 個の IP アドレスおよび MAC アドレスが割り当てられます。

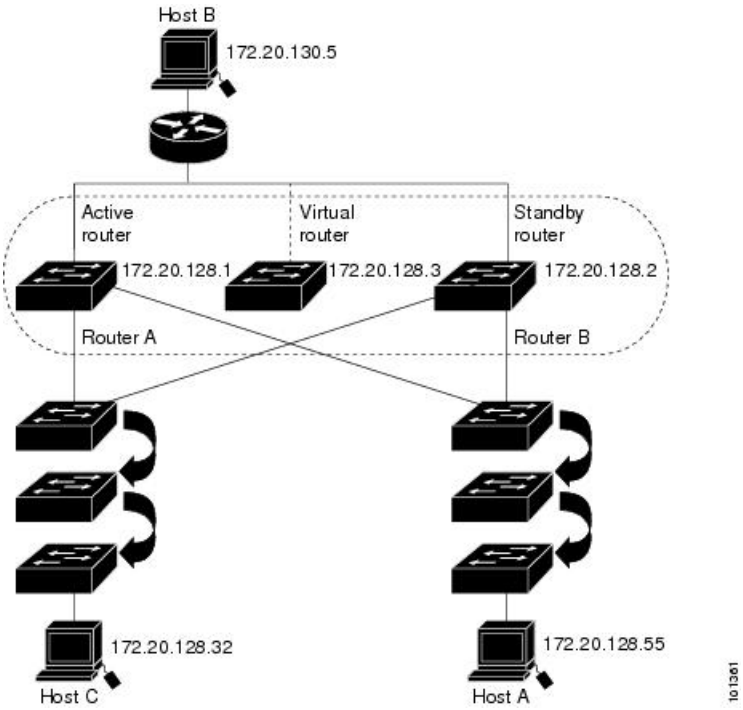
指定されたアクティブ ルータの故障を HSRP が検出すると、選択されているスタンバイ ルータがホットスタンバイ グループの MAC アドレスおよび IP アドレスの制御を引き継ぎます。この時点で新しいスタンバイ ルータも選択されます。HSRP が稼働しているデバイスは、マルチキャスト UDP ベースの hello パケットを送受信することにより、ルータ障害の検出、アクティブ ルータおよびスタンバイ ルータの指定を行います。インターフェイスに HSRP が設定されている場合、そのインターフェイスではインターネット制御メッセージプロトコル（ICMP）のリダイレクト メッセージが自動的にイネーブルになっています。

レイヤ 3 で動作するスイッチおよびスイッチ スタック間で複数のホット スタンバイ グループを設定すると、冗長ルータをさらに活用できます。そのためには、インターフェイスに設定するホットスタンバイ コマンド グループごとにグループ番号を指定します。たとえば、スイッチ 1 のインターフェイスをアクティブ ルータ、スイッチ 2 のインターフェイスをスタンバイ ルータとして設定できます。また、スイッチ 2 の別のインターフェイスをアクティブ ルータ、スイッチ 1 の別のインターフェイスをスタンバイ ルータとして設定することもできます。

次の図に、HSRP 用に設定されたネットワークのセグメントを示します。各ルータには、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスが設定されています。ルータ A の IP アドレスをネットワーク上のホストに設定する代わりに、デフォルト ルータとして仮想ルータ

の IP アドレスを設定します。ホスト C からホスト B にパケットが送信される場合、ホスト C は仮想ルータの MAC アドレスにパケットを送信します。何らかの理由により、ルータ A がパケットの転送を停止すると、ルータ B が仮想 IP アドレスおよび仮想 MAC アドレスに応答してアクティブ ルータとなり、アクティブ ルータの作業を行います。ホスト C は引き続き仮想ルータの IP アドレスを使用し、ホスト B 宛のパケットをアドレッシングします。ルータ B はそのパケットを受信し、ホスト B に送信します。ルータ B は HSRP の機能を使用し、ルータ A が動作を再開するまで、ホスト B のセグメント上のユーザと通信する必要があるホスト C のセグメント上のユーザに連続的にサービスを提供します。また、ホスト A セグメントとホスト B の間で、引き続き通常のパケット処理機能を実行します。

図 *15 : HSRP* の一般的な構成



レイヤ 3 で動作するスイッチおよびスイッチ スタック間で複数のホット スタンバイ グループを設定すると、冗長ルータをさらに活用できます。そのためには、インターフェイスに設定するホットスタンバイ コマンド グループごとにグループ番号を指定します。たとえば、スイッチ 1 のインターフェイスをアクティブ ルータ、スイッチ 2 のインターフェイスをスタンバイ ルータとして設定できます。また、スイッチ 2 の別のインターフェイスをアクティブ ルータ、スイッチ 1 の別のインターフェイスをスタンバイ ルータとして設定することもできます。

HSRP のバージョン

Cisco IOS XE Release 3.3SE 以降の製品は、下記のホットスタンバイ ルータ プロトコル（HSRP）バージョンをサポートしています。

スイッチでは、次の HSRP バージョンがサポートされます。

- HSRPv1：HSRP のバージョン 1（デフォルトのバージョン）。次の機能があります。

- HSRP グループ番号は 0 ～ 255 まで使用できます。
- HSRPv1 は 224.0.0.2 のマルチキャスト アドレスを使用して hello パケットを送信しますが、これは Cisco Group Management Protocol（CGMP）の脱退処理と競合します。HSRPv1 と CGMP は相互に排他的なため、同時には使用できません。

- HSRPv2：HSRP のバージョン 2。このバージョンには次の機能があります。
  - HSRPv2 は 224.0.0.102 のマルチキャスト アドレスを使用して hello パケットを送信します。HSRPv2 と CGMP 脱退処理は相互に排他的ではありません。同時に使用できます。
  - HSRPv2 のパケット形式は、HSRPv1 とは異なります。
  - HSRP グループ番号は 0 ～ 4095 まで使用できます。

HSRPv1 を実行しているスイッチは、ルータの送信元 MAC アドレスが仮想 MAC アドレスのため、hello パケットを送信した物理的なルータを特定できません。

HSRPv2 のパケット形式は、HSRPv1 とは異なります。HSRPv2 パケットは、パケットを送信した物理ルータの MAC アドレスを格納できる 6 バイトの識別子フィールドを持った、Type Length Value（TLV）形式を使用します。

HSRPv1 を実行しているインターフェイスが HSRPv2 パケットを取得した場合、このタイプフィールドは無視されます。

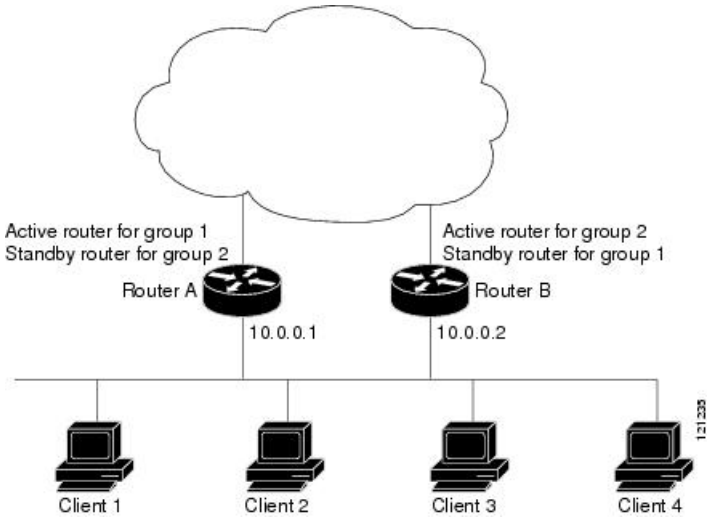
MHSRP

スイッチは、Multiple HSRP（MHSRP）をサポートします。MHSRP は HSRP の拡張版で、複数の HSRP グループ間でのロードシェアリングが可能です。ホストネットワークからサーバネットワークまで、ロード バランシングを実現して複数のスタンバイ グループ（およびパス）を使用するために、MHSRP を設定できます。

下の図では、半分のクライアントがルータ A に設定されており、もう半分はルータ B に設定されています。ルータ A およびルータ B の設定により、合計 2 つの HSRP グループが確立されています。グループ 1 では、ルータ A に最高のプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブ ルータになり、ルータ B がスタンバイ ルータとなります。グループ 2 では、ルータ B に最も高いプライオリティが割り当てられているため、ルータ B がデフォルトのアクティブ ルータであり、ルータ A がスタンバイ ルータです。通常の運用では、2 つのルータが IP トラフィック負荷を分散します。いずれかのルータが使用できなくなると、もう一方のルータがアクティブになり、使用できないルータのパケット転送機能を引き継ぎます。

（注） MHSRP では、ルータに障害が発生して正常に戻った場合にプリエンプションによりロードシェアリングを復元するために、**standby preempt** インターフェイス コンフィギュレーション コマンドを HSRP インターフェイスで入力する必要があります。

図 *16 : MSHRP* ロード シェアリング



SSO HSRP

SSO HSRP は、冗長なルート プロセッサ（RP）を装備したデバイスがステートフル スイッチオーバー（SSO）冗長モード用に設定されているときの HSRP の動作を変更します。ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。

この機能を使用すると、HSRP の SSO 情報がスタンバイ RP に同期されるため、HSRP 仮想 IP アドレスを使用して送信されるトラフィックをスイッチオーバー中も引き続き転送できるほか、データの損失やパスの変更も発生しません。さらに、HSRP アクティブ デバイスの両方の RP に障害が発生しても、スタンバイ状態の HSRP デバイスが HSRP アクティブ デバイスとして処理を引き継ぎます。

この機能は、動作の冗長モードが SSO に設定されている場合にデフォルトでイネーブルになっています。

HSRP およびスイッチ スタック

HSRP の hello メッセージは、スタック マスターで生成されます。HSRP がアクティブであるスタック マスターに障害が発生すると、HSRP アクティブ ステートのフラッピングが生じることがあります。これは、新規スタック マスターが選択および初期化されている間に HSRP hello メッセージが生成されず、スタック マスターが故障したあとでないとスタンバイ ルータがアクティブにならない可能性があるためです。

IPv6 の HSRP の設定

IPServices および IPBase フィーチャ セットを実行中のスイッチは、IPv6 のホットスタンバイ ルータ プロトコル（HSRP）をサポートします。HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。IPv6 ホストは、IPv6 ネイバー探索ルータのアドバタイズメント メッセージによって使用可能なルー

タを学習します。これらのメッセージは定期的にマルチキャストされるか、ホストにより送信請求されます。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカル アドレスがあります。

HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

（注） IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2（HSRPv2）をイネーブルにする必要があります。

HSRP の設定方法

HSRP のデフォルト設定

表 *26 : HSRP* のデフォルト設定

機能	デフォルト設定
HSRP バージョン	Version 1
HSRP グループ	未設定
スタンバイ グループ番号	0
スタンバイ MAC アドレス	0000.0c07.acXX に指定されたシステム。XX は、HSRP グループ番号
スタンバイ プライオリティ	100
スタンバイ遅延	0（遅延なし）
スタンバイでのインターフェイス プライオリティの追跡	10
スタンバイ hello 時間	3 秒
スタンバイ ホールドタイム	10 秒

HSRP 設定時の注意事項

- HSRPv2 および HSRPv1 は相互に排他的です。HSRPv2 は、同じインターフェイス上で HSRPv1 と一緒には動作しません（その逆も同様）。
- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - ルーテッドポート：インターフェイス コンフィギュレーション モードで **no switchport** コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。
  - SVI：グローバル コンフィギュレーション モードで **interface vlan** *vlan_id* によって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
  - レイヤ 3 モードの Etherchannel ポート チャネル：グローバル コンフィギュレーション モードで **interface port-channel** *port-channel-number* を使用し、イーサネット インターフェイスをチャネル グループにバインドして作成されたポートチャネル論理インターフェイスです。
- すべてのレイヤ 3 インターフェイスに IP アドレスを割り当てる必要があります。
-
- インターフェイスの HSRP バージョンを変更する場合、HSRP グループは新しい MAC アドレスを持つことになるため、リセットされます。
- Catalyst スイッチが混在するスタックでのみ：
- IPv4 の HSRP および IPv6 の HSRP は相互に排他的です。両方を同時にイネーブルにはできません。
- HSRPv2 および HSRP のグループ番号を設定する場合、256 の倍数の範囲のグループ番号を使用する必要があります。有効な範囲は 0 ～ 255、256 ～ 511、512 ～ 767、3840 ～ 4095 などです。
- 有効なグループ番号、無効なグループ番号の例：
- 2、150、225 の番号でグループを設定する場合、3850 の番号を持つ他のグループは設定できません。これは、0 ～ 255 の範囲内ではありません。
- 520、600、700 の番号でグループを設定する場合、900 の番号を持つ他のグループは設定できません。これは、512 ～ 767 の範囲内ではありません。

（注） HSRP のミリ秒タイマーはサポートされません。

HSRP のイネーブル化

インターフェイス コンフィギュレーション コマンド **standby ip** は、設定されているインターフェイスで HSRP をアクティブ化します。IP アドレスを指定した場合は、IP アドレスがホットスタンバイ グループの指定アドレスとして使用されます。IP アドレスを指定しなかった場

合は、スタンバイ機能によってアドレスが学習されます。指定アドレスを使用し、LAN 上に少なくとも 1 つのレイヤ 3 ポートを設定する必要があります。IP アドレスを設定すると、常に、現在使用されている別の指定アドレスが、設定した IP アドレスに変更されます。

standby ip コマンドがインターフェイス上でイネーブルに設定され、プロキシ ARP がイネーブルの場合、インターフェイスのホットスタンバイ ステートがアクティブになると、プロキシ ARP 要求に対する応答は、ホットスタンバイ グループの MAC アドレスを使用して実行されます。インターフェイスが別のステートの場合、プロキシ ARP の応答は抑制されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	インターフェイスコンフィギュレーション モードを開始し、HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	**standby version** {**1** | **2**} 例： `Switch(config-if)# standby version 1`	（任意）インターフェイスに HSRP バージョンを設定します。 • 1：HSRPv1 を選択します。 • 2：HSRPv2 を選択します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、インターフェイスはデフォルトの HSRP バージョンである HSRPv1 を実行します。
ステップ 4	**standby** [*group-numberip-address*] **ip** [[**secondary**]] 例： `Switch(config-if)# standby 1 ip`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）group-number：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）ip-address：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定しま

	コマンドまたはアクション	目的
		す。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります
ステップ 6	**show standby** [*interface-idgroup* [ ]] 例： `Switch # show standby`	スタンバイ グループの設定を確認します。
ステップ 7	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

HSRP のプライオリティの設定

standby priority, **standby preempt**、および **standby track** インターフェイス コンフィギュレーション コマンドはいずれも、アクティブ ルータとスタンバイ ルータを検索するための特性、および新しいアクティブ ルータが処理を引き継いだ場合の動作を設定するために使用できます。

HSRP プライオリティを設定する場合の注意事項は、次のとおりです。

- プライオリティを割り当てておくと、アクティブ ルータおよびスタンバイ ルータを選択できます。プリエンプションがイネーブルの場合は、プライオリティが最高のルータがア

クティブルータになります。プライオリティが等しい場合は、現在アクティブなルータに変更はありません。

- 最大の値（1 ～ 255）が、最高のプライオリティ（アクティブ ルータになる確率が最も高い）を表します。
- プライオリティ、プリエンプト、またはその両方を設定するときは、少なくとも 1 つのキーワード（**priority**、**preempt**、または両方）を指定する必要があります。
- インターフェイスが **standby track** コマンドによって設定されている場合、ルータ上の別のインターフェイスがダウンすると、デバイスのプライオリティが動的に変更されることもあります。
- **standby track** インターフェイス コンフィギュレーション コマンドを実行すると、ルータのホットスタンバイ プライオリティとインターフェイスのアベイラビリティが関連付けられます。この機能は、HSRP 用に設定されていないインターフェイスを追跡する場合に有効です。追跡対象のインターフェイスが故障すると、トラッキングが設定されているデバイスのホットスタンバイ プライオリティが 10 減少します。追跡対象でないインターフェイスの場合は、そのステートが変わっても、設定済みデバイスのホットスタンバイ プライオリティは変わりません。ホットスタンバイ用に設定されたインターフェイスごとに、追跡するインターフェイスのリストを個別に設定できます。
- **standby track** *interface-priority* インターフェイス コンフィギュレーション コマンドを実行すると、追跡対象のインターフェイスがダウンした場合のホットスタンバイ プライオリティの減少幅を指定できます。インターフェイスが稼働状態に戻ると、プライオリティは同じ分だけ増加します。
- *interface-priority* 値が設定されている場合に、複数の追跡対象インターフェイスがダウンすると、設定済みプライオリティの減少幅が累積されます。プライオリティ値が設定されていない追跡対象インターフェイスが故障した場合、デフォルトの減少幅は 10 です。この値は累積されません。
- インターフェイスに対してルーティングを最初にイネーブルにした時点で、完全なルーティング テーブルは存在しません。このインターフェイスがプリエンプトに設定されている場合はアクティブ ルータになりますが、十分なルーティング処理はできません。この問題を解決するには、ルータがルーティング テーブルを更新できるように遅延時間を設定します。

インターフェイスに HSRP プライオリティ特性を設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例：	インターフェイス コンフィギュレーション モードを開始し、プライオリティを設定する HSRP インターフェイスを入力します。

	コマンドまたはアクション	目的
	`Switch(config)# interface gigabitethernet1/0/1`	
ステップ 3	**standby** ［*group-number*］ **priority***priority* 例： `Switch(config-if)# standby 120 priority 50`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は1～255です。デフォルトプライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）group-number：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 4	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum***seconds*］ ［**reload***seconds*］ ［**sync***seconds*］］ 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカルルータのプライオリティがアクティブルータよりも高い場合は、アクティブルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカルルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは0です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカルルータがリロードの後アクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は0～3600（1時間）で、デフォルトは0です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は0～3600秒（1時間）で、デフォルトは0です（引き継ぐ前の遅延はありません）。

	コマンドまたはアクション	目的
		デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	**standby** ［*group-number*］ **track** *type number*［*interface-priority*］ 例： `Switch(config-if)# standby track interface gigabitethernet1/1/1`	他のインターフェイスを追跡するようにインターフェイスを設定します。この設定により、他のインターフェイスの1つがダウンした場合は、そのデバイスのホットスタンバイ プライオリティが減少します。 • （任意）group-number：コマンドが適用されるグループ番号です。 • type：追跡対象のインターフェイスタイプを（インターフェイス番号とともに）入力します。 • number：追跡対象のインターフェイス番号を（インターフェイス タイプとともに）入力します。 • （任意）interface-priority：インターフェイスがダウンした場合、または稼働状態に戻った場合に、ルータのホットスタンバイ プライオリティを減少または増加させる幅を入力します。デフォルト値は 10 です。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MHSRP の設定

MHSRP およびロード バランシングをイネーブルにするには、MHSRP の項の *MHSRP* ロード シェアリングの図に示したように、グループのアクティブ ルータとして 2 つのルータを設定し、スタンバイ ルータとして仮想ルータを設定します。ルータに障害が発生して正常に戻った場合、プリエンプションを発生させてロードバランシングを復元するために、**standby preempt** インターフェイス コンフィギュレーション コマンドをそれぞれの HSRP インターフェイスで入力する必要があります。

ルータ A はグループ 1 のアクティブ ルータとして、ルータ B はグループ 2 のアクティブ ルータとして設定されています。ルータ A の HSRP インターフェイスの IP アドレスは 10.0.0.1、グループ 1 のスタンバイ プライオリティは 110（デフォルトは 100）です。ルータ B の HSRP インターフェイスの IP アドレスは 10.0.0.2、グループ 2 のスタンバイ プライオリティは 110 です。

グループ 1 は仮想 IP アドレス 10.0.0.3 を使用し、グループ 2 は仮想 IP アドレス 10.0.0.4 を使用します。

ルータ A の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* 例： `Switch (config)# interface gigabitethernet1/0/1`	インターフェイスタイプを設定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	**no switchport** 例： `Switch (config)# no switchport`	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 4	**ip address** *ip-address mask* 例： `Switch (config-if)# 10.0.0.1 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Switch (config-if)# standby 1 ip 10.0.0.3`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホッ

	コマンドまたはアクション	目的
		トスタンバイ ルータ インターフェイスの仮想IPアドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想IPアドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 6	**standby** ［*group-number*］ **priority** *priority* 例： `Switch(config-if)# standby 1 priority 110`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 7	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］ 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時

	コマンドまたはアクション	目的
		間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカルルータがリロードの後アクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカルルータがアクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 8	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Switch (config-if)# standby 2 ip 10.0.0.4`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイルータインターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。

	コマンドまたはアクション	目的
		• （任意）**secondary**：IP アドレスがセカンダリホットスタンバイルータインターフェイスであることを指定します。ルータがセカンダリルータとスタンバイルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 9	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］ 例： `Switch(config-if)# standby 2 preempt delay 300`	ルータを **preempt** に設定し、ローカルルータのプライオリティがアクティブルータよりも高い場合は、アクティブルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカルルータがアクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカルルータがリロードの後アクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカルルータがアクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。

	コマンドまたはアクション	目的
		デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

ルータ B の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* 例： `Switch (config)# interface gigabitethernet1/0/1`	インターフェイスタイプを設定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	**no switchport** 例： `Switch (config)# no switchport`	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 4	**ip address** *ip-address mask* 例： `Switch (config-if)# 10.0.0.2 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Switch (config-if)# standby 1 ip 10.0.0.3`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グルー

	コマンドまたはアクション	目的
		プが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想IPアドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想IPアドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 6	**standby** ［*group-number*］ **priority** *priority* 例： `Switch(config-if)# standby 1 priority 110`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 7	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］ 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。

	コマンドまたはアクション	目的
		• （任意）**delay minimum**：ローカルルータがアクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカルルータがリロードの後アクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカルルータがアクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 8	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Switch (config-if)# standby 2 ip 10.0.0.4`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインター

	コマンドまたはアクション	目的
		フェイスに対して仮想IPアドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 9	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］ 例： `Switch(config-if)# standby 2 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された

	コマンドまたはアクション	目的
		秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

HSRP 認証およびタイマーの設定

HSRP認証ストリングを設定したり、helloタイムインターバルやホールドタイムを変更することもできます。

これらの属性を設定する場合の注意事項は次のとおりです。

- 認証ストリングはすべてのHSRPメッセージで暗号化されずに送信されます。相互運用できるように、接続されたすべてのルータおよびアクセス サーバに同じ認証ストリングを設定する必要があります。認証ストリングが一致しないと、HSRP によって設定された他のルータから、指定されたホットスタンバイ IP アドレスおよびタイマー値を学習できません。
- スタンバイ タイマー値が設定されていないルータまたはアクセス サーバは、アクティブ ルータまたはスタンバイ ルータからタイマー値を学習できます。アクティブ ルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。
- ホットスタンバイ グループのすべてのルータで、同じタイマー値を使用する必要があります。通常、*holdtime* は *hellotime* の 3 倍以上です。

インターフェイスにHSRPの認証とタイマーを設定するには、特権EXECモードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Switch(config) # interface gigabitethernet1/0/1`	インターフェイスコンフィギュレーション モードを開始し、プライオリティを設定するHSRPインターフェイスを入力します。
ステップ 3	**standby** [*group-number*] **authentication** *string* 例： `Switch(config-if) # standby 1 authentication word`	（任意）**authentication** *string*：すべてのHSRPメッセージで伝達されるストリングを入力します。認証ストリングには8文字までを指定できます。デフォルトのストリングは **cisco** です。 （任意）*group-number*：コマンドが適用されるグループ番号です。
ステップ 4	**standby** [*group-number*] **timers***hellotime holdtime* 例： `Switch(config-if) # standby 1 timers 5 15`	（任意）helloパケット間隔、およびアクティブ ルータのダウンを他のルータが宣言するまでの時間を設定します。 • *group-number*：コマンドが適用されるグループ番号です。 • （任意）*hellotime*：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は0～3600秒（1時間）で、デフォルトは0です（引き継ぐ前の遅延はありません）。 • *holdtime*：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は0～3600（1時間）で、デフォルトは0です（リロードの後、引き継ぐ前の遅延はありません）。
ステップ 5	**end** 例： `Switch(config-if) # end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ICMP リダイレクト メッセージの HSRP サポートのイネーブル化

HSRP が設定されたインターフェイスでは、ICMP リダイレクト メッセージが自動的にイネーブルになります。ICMP は、エラーをレポートするためのメッセージ パケットや IP 処理に関連する他の情報を提供する、ネットワーク層インターネット プロトコルです。ICMP には、ホストへのエラー パケットの方向付けや送信などの診断機能があります。この機能は、HSRP を介した発信 ICMP リダイレクト メッセージをフィルタリングします。HSRP では、ネクストホップ IP アドレスが HSRP 仮想 IP アドレスに変更される可能性があります。詳細については、『Cisco IOS IP Configuration Guide, Release 12.4』を参照してください。

HSRP グループおよびクラスタリングの設定

デバイスが HSRP スタンバイ ルーティングに参加し、クラスタリングがイネーブルの場合は、同じスタンバイ グループを使用して、コマンド スイッチの冗長性および HSRP の冗長性を確保できます。同じ HSRP スタンバイ グループをイネーブルにし、コマンド スイッチおよびルーティングの冗長性を確保するには、**cluster standby-group** *HSRP-group-name* [**routing-redundancy**] グローバル コンフィギュレーション コマンドを使用します。**routing-redundancy** キーワードを指定せずに同じ HSRP スタンバイ グループ名でクラスタを作成すると、そのグループに対する HSRP スタンバイ ルーティングはディセーブルになります。

HSRP の確認

HSRP コンフィギュレーションの確認

HSRP 設定を表示するには、次の特権 EXEC モードで次のコマンドを使用します。

show standby [*interface-idgroup* [ ]] [**brief**] [**detail**]

スイッチ全体、特定のインターフェイス、HSRP グループ、またはインターフェイスの HSRP グループに関する HSRP 情報を表示できます。HSRP 情報の概要または詳細のいずれを表示するかを指定することもできます。デフォルト表示は **detail** です。多数の HSRP グループがある場合に、修飾子を指定しないで **show standby** コマンドを使用すると、正確に表示されないことがあります。

例

```
Switch #show standby
VLAN1 - Group 1
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.182
Hot standby IP address is 172.20.128.3 configured
Active router is 172.20.128.1 expires in 00:00:09
Standby router is local
Standby virtual mac address is 0000.0c07.ac01
Name is bbb

VLAN1 - Group 100
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.262
```

```
Hot standby IP address is 172.20.138.51 configured
Active router is 172.20.128.1 expires in 00:00:09
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac64
Name is test
```

HSRP の設定例

HSRP のイネーブル化：例

次に、インターフェイスのグループ 1 で HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、HSRP を使用して学習されます。

（注） これは、HSRP をイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch # show standby
```

HSRP のプライオリティの設定：例

次に、ポートをアクティブにして、IP アドレスおよびプライオリティ 120（デフォルト値よりも高いプライオリティ）を設定して、アクティブ ルータになるまで 300 秒（5 分間）待機する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
Switch # show standby
```

MHSRP の設定：例

次に、*MHSRP* ロード シェアリングの図で示した MHSRP 設定をイネーブルにする例を示します。

ルータ A の設定

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
```

```
Switch(config-if)# standby 1 priority 110
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

ルータ B の設定

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 1 priority 110
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

HSRP 認証およびタイマーの設定：例

次に、グループ 1 のホットスタンバイ ルータを相互運用させるために必要な認証ストリングとして、word を設定する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

次に、hello パケット間隔が 5 秒、ルータがダウンしたと見なされるまでの時間が 15 秒となるように、スタンバイ グループ 1 のタイマーを設定する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

HSRP グループおよびクラスタリングの設定：例

次に、スタンバイ グループ my_hsrp をクラスタにバインドし、同じ HSRP グループをイネーブルにしてコマンド スイッチおよびルータの冗長性に使用する例を示します。このコマンドを実行できるのは、コマンド スイッチに対してだけです。スタンバイ グループの名前または番号が存在しない場合、またはスイッチがクラスタ メンバー スイッチである場合は、エラー メッセージが表示されます。

```
Switch # configure terminal
Switch(config) # cluster standby-group my_hsrp routing-redundancy
Switch(config-if)# end
```

HSRP の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
RFC 2281	『Cisco Hot Standby Router Protocol』

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

HSRP の設定に関する機能情報

表 *27 : HSRP* の設定に関する機能情報

リリース	機能情報
3SE	この機能が導入されました

第 24 章

NHRP の設定

Next Hop Resolution Protocol（NHRP）は、すべてのトンネル エンド ポイントを手動で設定するのではなく、ノンブロードキャストマルチアクセス（NBMA）ネットワークをダイナミックにマッピングする Address Resolution Protocol（ARP）と同様のプロトコルです。NHRP を使用すると、NBMA ネットワークに接続されたシステムは、そのネットワークに参加している他のシステムの NBMA（物理）アドレスをダイナミックに学習でき、これらのシステムが直接通信できるようになります。このプロトコルでは、ステーションのデータリンク アドレスを動的に決定することができる ARP と同様のソリューションが提供されます。

NHRP は、ハブがネクスト ホップ サーバ（NHS）であり、スポークがネクスト ホップ クライアント（NHC）である、クライアントおよびサーバのプロトコルです。ハブには、各スポークのパブリック インターフェイス アドレスが格納された NHRP データベースが保持されます。各スポークでは、起動時に NBMA 以外の（実際の）アドレスが登録され、ダイレクト トンネルを確立する場合は、NHRPデータベースに対し、宛先スポークのアドレスに関する照会が行われます。

このモジュールでは、Generic Routing Encapsulation（GRE）によって NHRP を設定する方法について説明します。Cisco IOS XE Denali 16.3.1 では、NHRP はスポーク設定のみをサポートします。

- 機能情報の確認 （441 ページ）
- NHRP の設定に関する情報 （442 ページ）
- NHRP の設定方法 （443 ページ）
- NHRP の設定例 （447 ページ）
- NHRP の設定に関する追加情報 （450 ページ）
- NHRP 設定の機能情報 （451 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NHRP の設定に関する情報

NHRP および NBMA のネットワークの相互作用

WAN ネットワークのほとんどは、ポイントツーポイント リンクの集まりです。仮想トンネル ネットワーク（総称ルーティング カプセル化（GRE）トンネルなど）もまた、ポイントツーポイント リンクの集まりです。これらのポイントツーポイント リンクの接続を効率的にスケーリングするために、通常は、単一またはマルチレイヤのハブアンドスポーク ネットワークにグループ化します。マルチポイント インターフェイス（GRE トンネル インターフェイスなど）を使用して、このようなネットワークのハブ ルータの設定を減らすことができます。その結果として生じるネットワークが NBMA ネットワークです。

単一のマルチポイント インターフェイスを通って到達可能なトンネル エンドポイントが複数あるため、この NBMA ネットワークを介してトンネル インターフェイスからパケットを転送するには、論理トンネル エンドポイントの IP アドレスから物理トンネル エンドポイントの IP アドレスへのマッピングが必要です。このマッピングはスタティックに設定することが可能ですが、これは、マッピングがダイナミックに検出または学習できる場合に推奨します。

NHRP は、これらの NBMA ネットワークの問題を軽減する ARP と同様のプロトコルです。NHRP を使用すると、NBMA ネットワークに接続されているシステムは、ネットワークの一部である他のシステムの NBMA アドレスをダイナミックに学習します。このため、これらのシステムは、トラフィックに中間ホップを使用せずに直接通信できるようになります。

ルータ、アクセス サーバ、およびホストは、NHRP を使用して、NBMA ネットワークに接続された他のルータおよびホストのアドレスを検出できます。部分メッシュ NBMA ネットワークには通常、NBMA ネットワークの背後に複数の論理ネットワークがあります。このような構成において、NBMA ネットワークを通るパケットは、出口ルータ（宛先ネットワークに最も近いルータ）に到着するまでに、NBMA ネットワーク上で複数のホップを発生させる必要がある場合があります。

NHRP 登録によって、これらの NBMA ネットワークのサポートが可能になります。

- NHRP 登録：NHRP を使用して、ネクスト ホップ クライアント（NHC）がネクスト ホップ サーバ（NHS）にダイナミックに登録されます。この登録機能により、特に、NHC がダイナミック物理 IP アドレスを持つか、物理 IP アドレスをダイナミックに変更するネットワーク アドレス変換（NAT）ルータの背後にある場合には、NHS で設定を変更しなくても、NHC が NBMA ネットワークに参加できるようになります。この場合、NHC の論理（VPN IP アドレス）と物理（NBMA IP）のマッピングを NHS で事前に設定することができません。

ダイナミックに構築されたハブアンドスポーク ネットワーク

NHRP により、NBMA ネットワークは最初、スポークの NHC とハブの NHS から複数の階層レイヤを構成できるハブアンドスポーク ネットワークとして配置されます。NHC は、NHS に到達するためのスタティック マッピング情報を使用して設定され、NHS に接続して NHRP 登録を NHS に送信します。この設定により、NHS はスポークのマッピング情報をダイナミックに学習できるため、ハブで必要な設定が減り、さらにスポークでダイナミック NBMA（物理）IP アドレスを取得できるようになります。

NHRP の設定方法

インターフェイス上での NHRP のイネーブル化

スイッチ上のインターフェイスに対して NHRP をイネーブルにするには、次の作業を行います。一般に、論理 NBMA ネットワーク内のすべての NHRP ステーションは、同じネットワーク ID を使用して設定する必要があります。

2 つ以上の NHRP ドメイン（GRE トンネル インターフェイス）が同じ NHRP ノード（スイッチ）で使用可能な場合は、NHRP ネットワーク ID を使用して、NHRP インターフェイスの NHRP ドメインを定義し、複数の NHRP ドメイン間またはネットワーク間で区別します。NHRP ネットワーク ID を使用すると、2 つの NHRP ネットワーク（クラウド）を同じスイッチ上に設定する場合に、それぞれを分けるのに役立ちます。

NHRP ネットワーク ID はローカル専用のパラメータです。これは、ローカル スイッチだけに対して意味があり、NHRP パケットで他の NHRP ノードに送信されることはありません。この理由から、2 台のスイッチが同じ NHRP ドメインに存在する場合、スイッチで設定される NHRP ネットワーク ID の実際の値は、もう一方のスイッチの NHRP ネットワーク ID と一致する必要はありません。NHRP パケットが GRE インターフェイス上に到着すると、そのインターフェイスで設定されている NHRP ネットワーク ID のローカル NHRP ドメインに割り当てられます。

同じ NHRP ネットワークに存在するすべてのスイッチ上の GRE インターフェイスでは、同じ NHRP ネットワーク ID を使用することを推奨します。こうすると、どの GRE インターフェイスがどの NHRP ネットワークのメンバであるかを追跡しやすくなります。

NHRP ドメイン（ネットワーク ID）は、スイッチ上の各 GRE トンネル インターフェイスで固有に設定できます。NHRP ドメインは、ルート上の GRE トンネル インターフェイス間をまたぐことができます。この場合、GRE トンネル インターフェイスで同じ NHRP ネットワーク ID を使用する効果は、2 つの GRE インターフェイスが単一の NHRP ネットワークに統合されることです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Switch(config)# interface tunnel 100`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaddress** *ip-address network-mask* 例： `Switch(config-if)# ip address 10.0.0.1 255.255.255.0`	IP をイネーブルにし、インターフェイスに IP アドレスを提供します。
ステップ 5	**ipnhrpnetwork-id** *number* 例： `Switch(config-if)# ip nhrp network-id 1`	インターフェイスで NHRP をイネーブルにします。
ステップ 6	**end** 例： `Switch(config)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

マルチポイント動作のための GRE トンネルの設定

マルチポイント（NMBA）動作のためのGRE トンネルを設定するには、次の作業を行います。

マルチポイント トンネル インターフェイスのトンネル ネットワークは、NBMA ネットワークと見なすことができます。同じスイッチ上で複数の GRE トンネルを設定する場合は、固有のトンネル ID キーまたは固有のトンネル送信元アドレスのいずれかを持っている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Switch(config)# interface tunnel 100`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address* 例： `Switch(config-if)# ip address 172.16.1.1 255.255.255.0`	インターフェイスに IP アドレスを設定します。
ステップ 5	**ip mtu** *bytes* 例： `Switch(config-if)# ip mtu 1400`	各インターフェイスにおいて送信される IP パケットの最大伝送単位（MTU）サイズを設定します。
ステップ 6	**ippimsparse-dense-mode** 例： `Switch(config-if)# ip pim sparse-dense-mode`	インターフェイスで Protocol Independent Multicast（PIM）をイネーブルにし、マルチキャスト グループの動作モードに応じて、インターフェイスをスパース モード動作またはデンス モード動作で処理します。
ステップ 7	**ipnhrpmap** *ip-address nbma-address* 例： `Switch(config-if)# ip nhrp map 172.16.1.2 10.10.10.2`	非ブロードキャスト マルチアクセス（NBMA）ネットワークに接続する宛先 IP アドレスの IP/NBMA アドレス マッピングをスタティックに設定します。 • *ip-address*：NBMA ネットワークを介して到達可能な宛先の IP アドレス。このアドレスは、NBMA アドレスにマッピングされます。

	コマンドまたはアクション	目的
		• *nbma-address*：NBMA ネットワークを介して直接到達可能なNBMAアドレス。アドレスの形式は、使用しているメディアによって異なります。たとえば、ATMはネットワーク サービス アクセス ポイント（NSAP）アドレスを所有し、イーサネットはMACアドレスを所有し、Switched Multimegabit Data Service（SMDS）はE.164アドレスを所有しています。このアドレスは、IPアドレスにマッピングされます。
ステップ 8	**ipnhrpmapmulticast** *nbma-address* 例： `Switch(config-if)# ip nhrp map multicast 10.10.10.2`	ブロードキャストの接続先として、またはトンネルネットワークを介して送信されるマルチキャストパケットとして使用されるノンブロードキャストマルチアクセス（NBMA）アドレスを設定します。
ステップ 9	**ipnhrpnetwork-id** *number* 例： `Switch(config-if)# ip nhrp network-id 1`	インターフェイスでNext Hop Resolution Protocol（NHRP）を有効にします。 • *number*：非ブロードキャストマルチアクセス（NBMA）ネットワークからの、グローバルに一意である 32 ビットのネットワーク ID。範囲は 1 ～ 4294967295 です。
ステップ 10	**ipnhrpnhs** *nhs-address* 例： `Switch(config-if)# ip nhrp nhs 172.16.1.2`	1 つ以上の NHRP サーバのアドレスを指定します。 • *nhs-address*：指定したネクストホップ サーバのアドレス。
ステップ 11	**tunnelsourcevlan** *interface-number* 例： `Switch(config-if)# tunnel source vlan 1`	トンネルインターフェイスの送信元アドレスを設定します。
ステップ 12	**tunneldestination** *ip-address* 例：	トンネルインターフェイスの宛先アドレスを設定します。

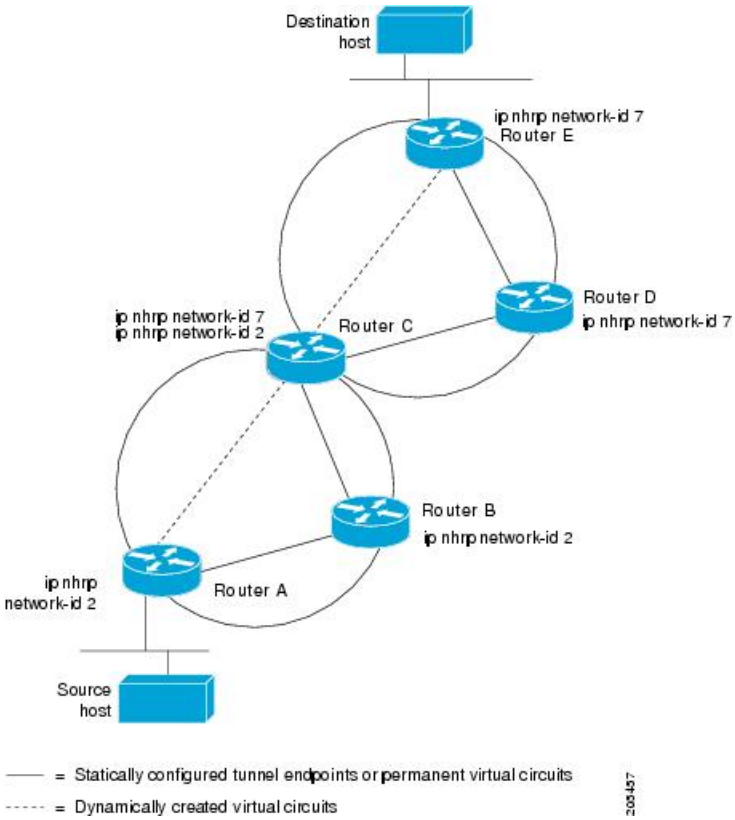
	コマンドまたはアクション	目的
	`Switch(config-if)# tunnel destination 10.10.10.2`	
ステップ 13	**end** 例： `Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NHRP の設定例

論理 NBMA の物理ネットワーク設計の例

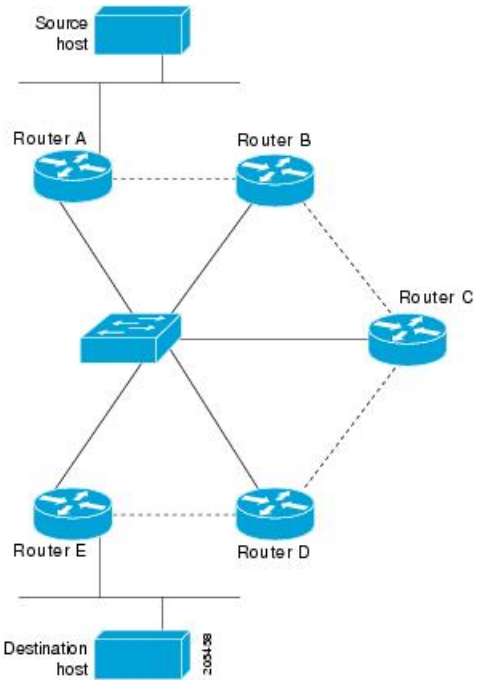
論理 NBMA ネットワークは、NHRP に参加し、同じネットワーク ID を持つインターフェイスおよびホストのグループと考えられます。次の図に、単一の物理 NBMA ネットワーク上に設定された（円で示される）2 つの論理 NBMA ネットワークを示します。ルータ A はルータ B およびルータ C と通信できます。それらが同じネットワーク ID（2）を共有するためです。また、ルータ C はルータ D およびルータ E とも通信できます。それらがネットワーク ID 7 を共有するためです。アドレス解決が完了した後、点線で示すように、ルータ A は IP パケットをホップ 1 回でルータ C に送信でき、ルータ C はそれをホップ 1 回でルータ E に送信できます。

図 *17 : 1* つの物理 *NBMA* ネットワーク上の *2* つの論理 *NBMA* ネットワーク



上図の 5 台のルータによる物理構成は、実際には下図のような構成である場合もあります。送信元ホストはルータ A に接続されており、宛先ホストはルータ E に接続されています。同じスイッチが 5 つのすべてのルータにサービスを提供し、1 つの物理 NBMA ネットワークを構成しています。

図 *18 : NBMA* ネットワーク例の物理構成



ここでも、上の最初の図を参照してください。最初、送信元ホストから宛先ホストへの IP パケットは、NHRP が NBMA アドレスでも解決するようになるまで、スイッチに接続された 5 台すべてのルータを通過して宛先に到達します。ルータ A は、IP パケットを初めて宛先ホストに向けて転送したときに、宛先ホストの IP アドレスに対する NHRP 要求も生成します。その要求がルータ C に転送され、応答が生成されます。2 つの論理 NBMA ネットワーク間の出力ルータであるため、ルータ C が応答します。

同様に、ルータ C は独自の NHRP 要求を生成し、これに対して、ルータ E が応答します。この例でも、送信元と宛先の間に発生する IP トラフィックが NBMA ネットワークを通過するためには、2 回のホップが必要です。これは、2 つの論理 NBMA ネットワーク間で IP トラフィックを転送する必要があるためです。NBMA ネットワークが論理的に分かれていなければ、必要なホップは 1 回だけです。

例：マルチポイント動作のための GRE トンネル

マルチポイント トンネルを使用すると、単一のトンネル インターフェイスを複数のネイバー スイッチに接続できます。ポイントツーポイント トンネルとは異なり、トンネルの宛先を設定する必要がありません。実際に、設定したとしても、トンネルの宛先は IP マルチキャスト アドレスに対応させる必要があります。

次の例では、スイッチ A とルータ B がイーサネット セグメントを共有しています。マルチポイント トンネル ネットワーク上で最小の接続が設定されるため、部分メッシュ NBMA ネットワークとして扱うことができるネットワークが作成されます。スタティック NHRP マップ エントリにより、スイッチ A はスイッチ B への到達方法を理解していて、その逆も同様です。

次に、GRE マルチポイント トンネルを設定する例を示します。

スイッチ A の設定

```
Switch(config)# interface tunnel 100 !Tunnel interface configured for PIM traffic
Switch(config-if)# no ip redirects
Switch(config-if)# ip address 192.168.24.1 255.255.255.252
Switch(config-if)# ip mtu 1400
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# ip nhrp map 192.168.24.3 172.16.0.1 !NHRP may optionally be configured
 to dynamically discover tunnel end points.
Switch(config-if)# ip nhrp map multicast 172.16.0.1
Switch(config-if)# ip nhrp network-id 1
Switch(config-if)# ip nhrp nhs 192.168.24.3
Switch(config-if)# tunnel source vlan 1
Switch(config-if)# tunnel destination 172.16.0.1
Switch(config-if)# end
```

スイッチ B の設定

```
Switch(config)# interface tunnel 100
Switch(config-if)# no ip redirects
Switch(config-if)# ip address 192.168.24.2 255.255.255.252
Switch(config-if)# ip mtu 1400
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# ip nhrp map 192.168.24.4 10.10.0.3
Switch(config-if)# ip nhrp map multicast 10.10.10.3
Switch(config-if)# ip nhrp network-id 1
Switch(config-if)# ip nhrp nhs 192.168.24.4
Switch(config-if)# tunnel source vlan 1
Switch(config-if)# tunnel destination 10.10.10.3
Switch(config-if)# end
```

NHRP の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Catalyst 3650 の設定	
Catalyst 3850 の設定	

RFC

RFC	タイトル
RFC 2332	『*NBMA Next Hop Resolution Protocol (NHRP)*』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポートおよびドキュメンテーション Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、ツール、技術マニュアルへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

NHRP 設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *28 : NHRP* 設定の機能情報

機能名	リリース	機能情報
Next Hop Resolution Protocol：ネクスト ホップ リソリューション プロトコル	Cisco IOS XE Polaris 16.3.1	Next Hop Resolution Protocol（NHRP）は、すべてのトンネル エンド ポイントを手動で設定するのではなく、ノンブロードキャスト マルチアクセス（NBMA）ネットワークをダイナミックにマッピングする Address Resolution Protocol（ARP）と同様のプロトコルです。NHRP を使用すると、NBMA ネットワークに接続されたシステムは、そのネットワークに参加している他のシステムの NBMA（物理）アドレスをダイナミックに学習でき、これらのシステムが直接通信できるようになります。

第 25 章

VRRPv3 プロトコルのサポート

- VRRPv3 プロトコルのサポート （453 ページ）

VRRPv3 プロトコルのサポート

Virtual Router Redundancy Protocol（VRRP）は、デバイスのグループを使用して単一の仮想デバイスを形成し、冗長性を実現することができます。これにより、仮想デバイスをデフォルトゲートウェイとして使用するように、LAN クライアントを設定できます。デバイスのグループを表す仮想デバイスは、「VRRP グループ」とも呼ばれます。VRRP バージョン 3（v3）のプロトコル サポート機能は、VRRP バージョン 2（v2）が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレスをサポートするための機能を提供します。このモジュールでは、VRRPv3 に関連する概念と、ネットワーク内で VRRP グループを作成してカスタマイズする方法について説明します。VRRPv3 プロトコル サポートを使用する利点は次のとおりです。

- マルチベンダー環境での相互運用性。
- VRRPv3 は、VRRPv2 が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレスの使用をサポートしています。
- VRRS 経路によるスケーラビリティの向上。

（注） このモジュールでは、VRRP と VRRPv3 は同じ意味で使用されています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VRRPv3 プロトコルのサポートの制限事項

- VRRPv3 は既存のダイナミック プロトコルの代替にはなりません。VRRPv3 は、マルチアクセス、マルチキャスト、または ブロードキャスト対応イーサネット LAN で使用するために設計されています。
- VRRPv3 は、イーサネット、ファストイーサネット、ブリッジグループ仮想インターフェイス（BVI）、およびギガビット イーサネット インターフェイス、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）、VRF を認識する MPLS VPN、および VLAN 上でサポートされます。
- BVI インターフェイスの初期化に関連して転送遅延が発生するため、VRRPv3 アドバタイズ タイマーの時間は BVI インターフェイスでの転送遅延時間より短く設定する必要があります。VRRPv3 アドバタイズ タイマーの時間を BVI インターフェイスでの転送遅延時間以上の値に設定すると、最近初期化された BVI インターフェイス上にある VRRP デバイスが無条件にマスター ロールを引き継げなくなります。BVIインターフェイスでの転送遅延を設定するには、**bridgeforward-time** コマンドを使用します。VRRP アドバタイズメント タイマーを設定するには、**vrrptimersadvertise** コマンドを使用します。
- VRRPv3 は、ステートフル スイッチオーバー（SSO）をサポートしていません。
- VRRP が VRRS 経路の冗長インターフェイスと同じネットワーク パス上で動作する場合にのみ、完全なネットワークの冗長性を実現できます。完全な冗長性のために、次の制約事項が適用されます。
  - VRRS 経路は、親 VRRP グループと異なる物理インターフェイスを共有したり、親 VRRP グループと異なる物理インターフェイスを持つサブインターフェイス上で設定することはできません。
  - VRRS 経路は、関連付けられた VLAN が親 VRRP グループが設定された VLAN と同じトランクを共有していない限り、スイッチ仮想インターフェイス（SVI）に設定することはできません。

VRRPv3 プロトコル サポートについて

VRRPv3 の利点

IPv4 と IPv6 のサポート

VRRPv3 は、VRRPv2 が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレス ファミリをサポートしています。

（注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。VRRPv3 を設定可能にするには、**fhrpversionvrrpv3** コマンドをグローバル コンフィギュレーション モードで使用する必要があります

冗長性

VRRP により、複数のデバイスをデフォルト ゲートウェイ デバイスとして設定できるようになり、ネットワークに単一障害点が生じる可能性を低減できます。

ロード シェアリング

LAN クライアントとのトラフィックを複数のデバイスで共有するように VRRP を設定できるため、利用可能なデバイス間でより公平にトラフィックの負荷を共有できます。

複数の仮想デバイス

VRRP はデバイスの物理インターフェイス上で（拡張の制限に従って）最大 255 の仮想デバイス（VRRP グループ）をサポートします。複数の仮想デバイスをサポートすることで、LAN トポロジ内で冗長化とロード シェアリングを実装できます。拡張環境では、VRRS 経路は VRRP 制御グループと組み合わせて使用する必要があります。

複数の IP アドレス

仮想デバイスは、セカンダリ IP アドレスを含め複数の IP アドレスを管理できます。そのため、イーサネット インターフェイスに複数のサブネットを設定した場合、サブネットごとに VRRP を設定できます。

（注） VRRP グループでセカンダリ IP アドレスを使用するには、プライマリ アドレスを同じグループで設定する必要があります。

プリエンプション

VRRP の冗長性スキームにより、仮想デバイス バックアップのプリエンプトが可能になり、より高いプライオリティが設定された仮想デバイス バックアップが、機能を停止した仮想デバイス マスターを引き継ぐようにできます。

（注） 優先度の低いマスターデバイスのプリエンプションは、オプションの遅延を使用してイネーブルにできます。

アドバタイズメント プロトコル

VRRPは、VRRPアドバタイズメント専用のインターネット割り当て番号局（IANA）標準マルチキャスト アドレスを使用します。IPv4 では、マルチキャスト アドレスは 224.0.0.18 です。IPv6 では、マルチキャスト アドレスは FF02:0:0:0:0:0:0:12 です。このアドレッシング方式によって、マルチキャストを提供するデバイス数が最小限になり、テスト機器でセグメント上の VRRP パケットを正確に識別できるようになります。IANA では VRRP に IP プロトコル番号 112 を割り当てていました。

VRRP デバイスのプライオリティおよびプリエンプション

VRRP 冗長性スキームの重要な一面に、VRRP デバイス プライオリティがあります。プライオリティにより、各 VRRP デバイスが実行する役割と、仮想マスター デバイスが機能を停止したときにどのようなことが起こるかが決定されます。

VRRP デバイス仮想デバイスの IP アドレスと物理インターフェイスの IP アドレスのオーナーである場合には、このデバイスが仮想マスター デバイスとして機能します。

VRRP デバイスが仮想バックアップ デバイスとして機能するかどうかや、仮想マスター デバイスが機能を停止した場合に仮想マスターデバイスを引き継ぐ順序も、プライオリティによって決定されます。各仮想バックアップ デバイスのプライオリティは、**priority** コマンドを使用して 1 ～ 254 の値に設定できます（**vrrpaddress-family** コマンドを使用して VRRP 設定モードに入り、**priority** オプションにアクセスします）。

たとえば、LAN トポロジのマスター仮想デバイスであるデバイス A が機能を停止した場合、選択プロセスが実行されて、仮想デバイス バックアップ B または C が引き継ぐかどうかが決定されます。デバイス B とデバイス C がそれぞれ プライオリティ 101 と 100 に設定されている場合、プライオリティの高いデバイス B が仮想デバイス マスターになります。デバイス B とデバイス C が両方ともプライオリティ 100 に設定されている場合、IP アドレスが高い方の仮想デバイス バックアップが選択されて仮想デバイス マスターになります。

デフォルトでは、プリエンプティブ設定はイネーブルになっています。この場合、仮想マスター デバイスになるように選択されている仮想バックアップ デバイスの中で、より高いプライオリティが設定されている仮想バックアップ デバイスが仮想マスターデバイスになります。このプリエンプティブ設定は、**no preempt** コマンドを使用して無効にできます（**vrrpaddress-family** コマンドを使用して VRRP 設定モードに入り、**no preempt** コマンドを入力します）。プリエンプションがディセーブルになっている場合は、元の仮想マスターデバイスが回復して再びマスターになるまで、仮想マスターデバイスになるように選択されている仮想バックアップ デバイスがマスターの役割を実行します。

（注） 優先度の低いマスターデバイスのプリエンプションは、オプションの遅延を使用してイネーブルにできます。

VRRP のアドバタイズメント

仮想デバイス マスターは、同じグループ内の他の VRRP デバイスに VRRP アドバタイズメントを送信します。アドバタイズメントでは、仮想デバイスマスターのプライオリティとステー

トを伝えます。VRRP アドバタイズメントは、（VRRP グループ設定に基づいて）IPv4 または IPv6 パケットにカプセル化され、VRRP グループに割り当てられた適切なマルチキャスト アドレスに送信されます。IPv4 では、マルチキャスト アドレスは 224.0.0.18 です。IPv6 では、マルチキャスト アドレスは FF02:0:0:0:0:0:0:12 です。アドバタイズメントは、デフォルトでは 1 秒に 1 回送信されますが、この間隔は設定可能です。

シスコ デバイスでは、VRRPv2 からの変更点であるミリ秒タイマーを設定できます。ミリ秒タイマー値は、プライマリ デバイスとバックアップ デバイスの両方に手動で設定する必要があります。バックアップ デバイス上の **showvrrp** コマンド出力に表示されるマスター アドバタイズメント値は、常に、1 秒です。これは、バックアップ デバイス上のパケットでミリ秒値が受け入れられないためです。

ミリ秒タイマーは、絶対に必要な場合以外は使用しないようにし、使用する場合は慎重な検討とテストが必要です。ミリ秒の値は望ましい状況でのみ動作します。ミリ秒のタイマー値の使用は、VRRPv3 も含めてサポートしている限り、サードパーティ ベンダーと互換性があります。タイマー値は 100 ～ 40000 ミリ秒の範囲で指定できます。

VRRPv3 プロトコル サポートについて

VRRPv3 の利点

IPv4 と IPv6 のサポート

VRRPv3 は、VRRPv2 が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレス ファミリをサポートしています。

（注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。VRRPv3 を設定可能にするには、**fhrpversionvrrpv3** コマンドをグローバル コンフィギュレーション モードで使用する必要があります

冗長性

VRRP により、複数のデバイスをデフォルト ゲートウェイ デバイスとして設定できるようになり、ネットワークに単一障害点が生じる可能性を低減できます。

ロード シェアリング

LAN クライアントとのトラフィックを複数のデバイスで共有するように VRRP を設定できるため、利用可能なデバイス間でより公平にトラフィックの負荷を共有できます。

複数の仮想デバイス

VRRP はデバイスの物理インターフェイス上で（拡張の制限に従って）最大 255 の仮想デバイス（VRRP グループ）をサポートします。複数の仮想デバイスをサポートすることで、LAN ト

ポロジ内で冗長化とロードシェアリングを実装できます。拡張環境では、VRRS 経路は VRRP 制御グループと組み合わせて使用する必要があります。

複数の IP アドレス

仮想デバイスは、セカンダリ IP アドレスを含め複数の IP アドレスを管理できます。そのため、イーサネット インターフェイスに複数のサブネットを設定した場合、サブネットごとに VRRP を設定できます。

（注） VRRP グループでセカンダリ IP アドレスを使用するには、プライマリ アドレスを同じグループで設定する必要があります。

プリエンプション

VRRP の冗長性スキームにより、仮想デバイス バックアップのプリエンプトが可能になり、より高いプライオリティが設定された仮想デバイス バックアップが、機能を停止した仮想デバイス マスターを引き継ぐようにできます。

（注） 優先度の低いマスターデバイスのプリエンプションは、オプションの遅延を使用してイネーブルにできます。

アドバタイズメント プロトコル

VRRP は、VRRP アドバタイズメント専用のインターネット割り当て番号局（IANA）標準マルチキャスト アドレスを使用します。IPv4 では、マルチキャスト アドレスは 224.0.0.18 です。IPv6 では、マルチキャスト アドレスは FF02:0:0:0:0:0:0:12 です。このアドレッシング方式によって、マルチキャストを提供するデバイス数が最小限になり、テスト機器でセグメント上の VRRP パケットを正確に識別できるようになります。IANA では VRRP に IP プロトコル番号 112 を割り当てていました。

VRRP デバイスのプライオリティおよびプリエンプション

VRRP 冗長性スキームの重要な一面に、VRRP デバイス プライオリティがあります。プライオリティにより、各 VRRP デバイスが実行する役割と、仮想マスター デバイスが機能を停止したときにどのようなことが起こるかが決定されます。

VRRP デバイス仮想デバイスの IP アドレスと物理インターフェイスの IP アドレスのオーナーである場合には、このデバイスが仮想マスター デバイスとして機能します。

VRRP デバイスが仮想バックアップ デバイスとして機能するかどうかや、仮想マスター デバイスが機能を停止した場合に仮想マスターデバイスを引き継ぐ順序も、プライオリティによって決定されます。各仮想バックアップ デバイスのプライオリティは、**priority** コマンドを使用して 1 ～ 254 の値に設定できます（**vrrpaddress-family** コマンドを使用して VRRP 設定モードに入り、**priority** オプションにアクセスします）。

たとえば、LAN トポロジのマスター仮想デバイスであるデバイス A が機能を停止した場合、選択プロセスが実行されて、仮想デバイス バックアップ B または C が引き継ぐかどうかが決定されます。デバイス B とデバイス C がそれぞれ プライオリティ 101 と 100 に設定されている場合、プライオリティの高いデバイス B が仮想デバイス マスターになります。デバイス B とデバイス C が両方ともプライオリティ 100 に設定されている場合、IP アドレスが高い方の仮想デバイス バックアップが選択されて仮想デバイス マスターになります。

デフォルトでは、プリエンプティブ設定はイネーブルになっています。この場合、仮想マスター デバイスになるように選択されている仮想バックアップ デバイスの中で、より高いプライオリティが設定されている仮想バックアップデバイスが仮想マスターデバイスになります。このプリエンプティブ設定は、**no preempt** コマンドを使用して無効にできます（**vrrpaddress-family** コマンドを使用して VRRP 設定モードに入り、**no preempt** コマンドを入力します）。プリエンプションがディセーブルになっている場合は、元の仮想マスターデバイスが回復して再びマスターになるまで、仮想マスターデバイスになるように選択されている仮想バックアップ デバイスがマスターの役割を実行します。

（注） 優先度の低いマスターデバイスのプリエンプションは、オプションの遅延を使用してイネーブルにできます。

VRRP のアドバタイズメント

仮想デバイス マスターは、同じグループ内の他の VRRP デバイスに VRRP アドバタイズメントを送信します。アドバタイズメントでは、仮想デバイスマスターのプライオリティとステートを伝えます。VRRP アドバタイズメントは、（VRRP グループ設定に基づいて）IPv4 または IPv6 パケットにカプセル化され、VRRP グループに割り当てられた適切なマルチキャスト アドレスに送信されます。IPv4 では、マルチキャスト アドレスは 224.0.0.18 です。IPv6 では、マルチキャスト アドレスは FF02:0:0:0:0:0:0:12 です。アドバタイズメントは、デフォルトでは 1 秒に 1 回送信されますが、この間隔は設定可能です。

シスコ デバイスでは、VRRPv2 からの変更点であるミリ秒タイマーを設定できます。ミリ秒タイマー値は、プライマリ デバイスとバックアップ デバイスの両方に手動で設定する必要があります。バックアップ デバイス上の **showvrrp** コマンド出力に表示されるマスター アドバタイズメント値は、常に、1 秒です。これは、バックアップ デバイス上のパケットでミリ秒値が受け入れられないためです。

ミリ秒タイマーは、絶対に必要な場合以外は使用しないようにし、使用する場合は慎重な検討とテストが必要です。ミリ秒の値は望ましい状況でのみ動作します。ミリ秒のタイマー値の使用は、VRRPv3 も含めてサポートしている限り、サードパーティ ベンダーと互換性があります。タイマー値は 100 ～ 40000 ミリ秒の範囲で指定できます。

VRRPv3 プロトコル サポートの設定方法

GLBP のイネーブル化と確認

インターフェイス上でGLBPをイネーブルにし、設定と動作を確認するには、次の作業を実行します。GLBP は、簡単に設定できる設計になっています。GLBP グループ内の各ゲートウェイは、同じグループ番号を使用して設定する必要があります。また、GLBP グループ内の少なくとも 1 つのゲートウェイは、そのグループで使う仮想 IP アドレスを使用して設定しなければなりません。その他のすべての必須パラメータは学習できます。

始める前に

インターフェイスで VLAN が使用されている場合、GLBP グループ番号は VLAN ごとに異なる値にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaddress** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.21.8.32 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group***ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# glbp 10 ip 10.21.8.10`	インターフェイス上でGLBPを設定し、仮想ゲートウェイのプライマリ IP アドレスを指定します。 • プライマリ IP アドレスの指定後は、**secondary** キーワードを指定し

	コマンドまたはアクション	目的
		て **glbp** *group* **ip** コマンドを再度使用し、このグループでサポートする他の IP アドレスを指定できます。
ステップ 6	**end** 例： `Device(config-if)# end`	インターフェイスコンフィギュレーション モードを終了して、デバイスが特権 EXEC モードに戻ります。
ステップ 7	**showglbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**] 例： `Device(config)# show glbp GigabitEthernet 1/0/1 10`	（任意）デバイス上の GLBP グループに関する情報を表示します。 • オプションの **brief** キーワードを使用すると、各仮想ゲートウェイまたは仮想フォワーダに関する情報が 1 行表示されます。

例

次に、デバイス上の GLBP グループ 10 のステータスに関する出力例を示します。

```
Device# show glbp GigabitEthernet 1/0/1 10
GigabitEthernet1/0/1 - Group 10
  State is Active
    1 state change, last state change 00:04:52
  Virtual IP address is 10.21.8.10
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.608 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption disabled
  Active is local
  Standby is unknown
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    ac7e.8a35.6364 (10.21.8.32) local
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:04:41
    MAC address is 0007.b400.0a01 (default)
    Owner ID is ac7e.8a35.6364
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
```

VRRP グループの作成とカスタマイズ

VRRP グループを作成するには、次の手順を実行します。ステップ 6 ～ 14 はそのグループのカスタマイズ オプションで、これらは省略可能です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**fhrpversionvrrpv3** 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。
ステップ 4	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**vrrp** *group-id***address-family** {**ipv4** | **ipv6**} 例： `Device(config-if)# vrrp 3 address-family ipv4`	VRRP グループを作成し、VRRP コンフィギュレーションモードを開始します。
ステップ 6	**address** *ip-address* [**primary** | **secondary**] 例： `Device(config-if-vrrp)# address 100.0.1.10 primary`	VRRP グループのプライマリ アドレスまたはセカンダリ アドレスを指定します。

	コマンドまたはアクション	目的
		（注） IPv6 の VRRPv3 では、グループを動作可能にするため、プライマリ仮想リンクローカル IPv6 アドレスが設定されている必要があります。プライマリ リンク ローカル IPv6 アドレスがグループに確立されると、セカンダリ グローバル アドレスを追加できます。
ステップ 7	**description** *group-description* 例： `Device(config-if-vrrp)# description group 3`	（任意）VRRP グループの説明を指定します。
ステップ 8	**match-address** 例： `Device(config-if-vrrp)# match-address`	（任意）アドバタイズメントパケットのセカンダリアドレスを設定したアドレスと照合します。 • セカンダリアドレスの照合は、デフォルトで有効になっています。
ステップ 9	**preemptdelayminimum** *seconds* 例： `Device(config-if-vrrp)# preempt delay minimum 30`	（任意）プライオリティの低いマスターデバイスのプリエンプションをオプションの延期期間でイネーブルにします。 • プリエンプションはデフォルトでイネーブルです。
ステップ 10	**priority** *priority-level* 例： `Device(config-if-vrrp)# priority 3`	（任意）VRRP グループのプライオリティを指定します。 • VRRP グループの優先度はデフォルトで 100 です。
ステップ 11	**timersadvertise** 間隔 例： `Device(config-if-vrrp)# timers advertise 1000`	（任意）アドバタイズメントタイマーをミリ秒で設定します。 • アドバタイズメントタイマーはデフォルトで 1000 ミリ秒に設定されています。
ステップ 12	**vrrpv2** 例：	（任意）VRRPv2 のみをサポートするデバイスと相互運用するため、VRRPv2

	コマンドまたはアクション	目的
	`Device(config-if-vrrp)# vrrpv2`	のサポートを同時にイネーブルにします。 • VRRPv2はデフォルトで無効になっています。
ステップ 13	**vrrsleader** *vrrs-leader-name* 例： `Device(config-if-vrrp)# vrrs leader leader-1`	（任意）VRRSに登録され、フォロワーに使用されるリーダーの名前を指定します。 • 登録済みの VRRS 名はデフォルトで使用不可になっています。
ステップ 14	**shutdown** 例： `Device(config-if-vrrp)# shutdown`	（任意）VRRP グループの VRRP 設定をディセーブルにします。 • VRRP の設定は、VRRP グループに対してはデフォルトでイネーブルになっています。
ステップ 15	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

FHRP クライアントの初期化前の遅延時間の設定

インターフェイス上のすべてのFHRPクライアントの初期化の前に遅延期間を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**fhrpversionvrrpv3** 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。
ステップ 4	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**fhrpdelay** {[**minimum**] [**reload**] *seconds*} 例： `Device(config-if)# fhrp delay minimum 5`	インターフェイスの起動後に、FHRP クライアントの初期化の遅延期間を指定します。 • 範囲は 0 ～ 3600 秒です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

VRRPv3 プロトコル サポートの設定例

例：デバイス上の VRRPv3 のイネーブル化

次の例は、デバイスで VRRPv3 をイネーブルにする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config-if-vrrp)# end
```

例：VRRP グループの作成とカスタマイズ

次に、VRRP グループを作成およびカスタマイズする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# vrrp 3 address-family ipv4
Device(config-if-vrrp)# address 100.0.1.10 primary
Device(config-if-vrrp)# description group 3
Device(config-if-vrrp)# match-address
Device(config-if-vrrp)# preempt delay minimum 30
```

```
Device(config-if-vrrp)# end
```

（注） 上記の例では、グローバル コンフィギュレーション モードで **fhrpversionvrrpv3** コマンドが使用されています。

例：FHRP クライアントの初期化前の遅延時間の設定

次の例は、FHRP クライアントの初期化前の遅延時間の設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# fhrp delay minimum 5
Device(config-if-vrrp)# end
```

（注） 上記の例では、インターフェイスが表示されてから FHRP クライアントの初期化に 5 秒間の遅延時間が指定されています。遅延時間は 0 ～ 3600 秒の範囲で指定できます。

例：VRRP ステータス、設定、および統計情報の詳細

以下は、VRRP グループのステータス、設定、および統計情報の詳細の出力例です。

```
Device> enable
Device# show vrrp detail

 GigabitEthernet1/0/1 - Group 3 - Address-Family IPv4
  Description is "group 3"
  State is MASTER
  State duration 53.901 secs
  Virtual IP address is 100.0.1.10
  Virtual MAC address is 0000.5E00.0103
  Advertisement interval is 1000 msec
  Preemption enabled, delay min 30 secs (0 msec remaining)
  Priority is 100
  Master Router is 10.21.0.1 (local), priority is 100
  Master Advertisement interval is 1000 msec (expires in 832 msec)
  Master Down interval is unknown
  VRRPv3 Advertisements: sent 61 (errors 0) - rcvd 0
  VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
  Group Discarded Packets: 0
    VRRPv2 incompatibility: 0
    IP Address Owner conflicts: 0
    Invalid address count: 0
    IP address configuration mismatch : 0
    Invalid Advert Interval: 0
    Adverts received in Init state: 0
    Invalid group other reason: 0
  Group State transition:
```

```
    Init to master: 0
    Init to backup: 1 (Last change Sun Mar 13 19:52:56.874)
    Backup to master: 1 (Last change Sun Mar 13 19:53:00.484)
    Master to backup: 0
    Master to init: 0
    Backup to init: 0

Device# exit
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』
FHRP コマンド	『First Hop Redundancy Protocols Command Reference』
VRRPv2 の設定	『*Configuring VRRP*』

標準および RFC

標準/RFC	Title
RFC5798	『*Virtual Router Redundancy Protocol*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VRRPv3 プロトコルのサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *29 : VRRPv3* プロトコルのサポートの機能情報

機能名	リリース	機能情報
VRRPv3 プロトコルのサポート	Cisco IOS XE 3.6E	VRRP は、デバイスのグループを使用して単一の仮想デバイスを形成し、冗長性を実現します。これにより、仮想デバイスをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。デバイスのグループを表す仮想デバイスは、「VRRP グループ」とも呼ばれます。VRRPv3 プロトコルのサポート機能は、IPv4 と IPv6 アドレスをサポートするための機能を提供します。 Cisco IOS Release Cisco IOS XE Release 3.6E では、この機能は以下のプラットフォームでサポートされるようになりました。 **fhrpdelay**、**showvrrp**、**vrrpaddress-family** の各コマンドが導入または修正されました。

用語集

VirtualIPaddressowner：仮想デバイスの IP アドレスを所有する VRRP デバイス。仮想デバイスアドレスを物理インターフェイスアドレスとして持っているデバイスが所有者になります。

Virtualdevice：1 つのグループを形成する 1 台または複数台の VRRP デバイス。仮想デバイスは、LAN クライアントのデフォルト ゲートウェイ デバイスとして動作します。仮想デバイスは、VRRP グループとも呼ばれます。

Virtualdevicebackup：仮想デバイス マスターが機能を停止したときにパケット転送のロールを引き受けられる 1 台または複数台の VRRP デバイス。

Virtualdevicemaster：仮想デバイスの IP アドレスに送信されるパケットの転送を現在行っている VRRP デバイス。通常、仮想デバイス マスターは IP アドレス所有者としても機能します。

VRRPdevice：VRRP を実行しているデバイス。

第 26 章

GLBP の設定

- 『Configuring GLBP』 （471 ページ）

『Configuring GLBP』

ゲートウェイ ロード バランシング プロトコル（GLBP）は、ホットスタンバイ ルータ プロトコル（HSRP）や仮想ルータ冗長プロトコル（VRRP）のように、機能を停止したデバイスや回路からデータ トラフィックを保護します。このとき、冗長化されたデバイスのグループ間でパケットのロード シェアリングを行うことができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

GLBP の制限事項

拡張オブジェクト トラッキング（EOT）はステートフル スイッチオーバー（SSO）を認識しないため、SSO モードで GLBP と併用することはできません。

GLBP の前提条件

GLBP を設定する前に、デバイスが物理インターフェイス上の複数の MAC アドレスをサポートできることを確認してください。設定している GLBP フォワーダごとに、追加の MAC アドレスが使用されます。

GLBP に関する情報

GLBP の概要

GLBP は、IEEE 802.3 LAN 上でデフォルト ゲートウェイを 1 つだけ指定して設定された IP ホストの自動デバイス バックアップを行います。LAN 上の複数のファーストホップ デバイスを連結し、IP パケットの転送負荷を共有しながら単一の仮想ファーストホップ IP デバイスを提供します。LAN 上にあるその他のデバイスは、冗長化された GLBP デバイスとして動作できます。このデバイスは、既存のフォワーディング デバイスが機能しなくなった場合にアクティブになります。

GLBP は、ユーザに対しては HSRP や VRRP と同様の機能を実行します。HSRP および VRRP は、仮想 IP アドレスを指定して設定された仮想デバイス グループに、複数のデバイスを参加させます。グループの仮想 IP アドレスに送信されたパケットを転送するアクティブ デバイスとして、1 つのメンバが選択されます。グループ内の他のデバイスは、アクティブ デバイスで障害が発生するまでは冗長デバイスです。これらのスタンバイ デバイスには、プロトコルによって使用されていない未使用帯域幅があります。同じデバイス セットに対して複数の仮想デバイス グループを設定できますが、ホストは異なるデフォルト ゲートウェイに対して設定する必要があります。その結果、管理上の負担が大きくなります。GLBP には、単一の仮想 IP アドレスと複数の仮想 MAC アドレスを使用して、複数のデバイス（ゲートウェイ）上でのロードバランシングを提供するというメリットがあります。転送負荷は、GLBP グループ内のすべてのデバイス間に分散されるため、単一のデバイスだけが処理して残りのデバイスがアイドルのままになるようなことはありません。各ホストは、同じ仮想 IP アドレスで設定され、仮想デバイス グループ内のすべてのデバイスが参加してパケットの転送を行います。GLBP メンバは、Hello メッセージを使用して相互に通信します。このメッセージは 3 秒ごとにマルチキャスト アドレス 224.0.0.102、UDP ポート 3222（送信元と宛先）に送信されます。

GLBP パケット タイプ

GLBP は実行に 3 つの異なるパケット タイプを使用します。そのパケット タイプは、Hello、要求、および応答です。Hello パケットはプロトコル情報をアドバタイズするために使用されます。Hello パケットはマルチキャストで、仮想ゲートウェイまたはバーチャル フォワーダが Speak、Standby、Active のいずれかの状態のときに送信されます。要求パケットと応答パケットは、仮想 MAC アドレスの割り当てに使用されます。これらはどちらもアクティブ仮想ゲートウェイ（AVG）間のユニキャスト メッセージです。

GLBP アクティブ仮想ゲートウェイ

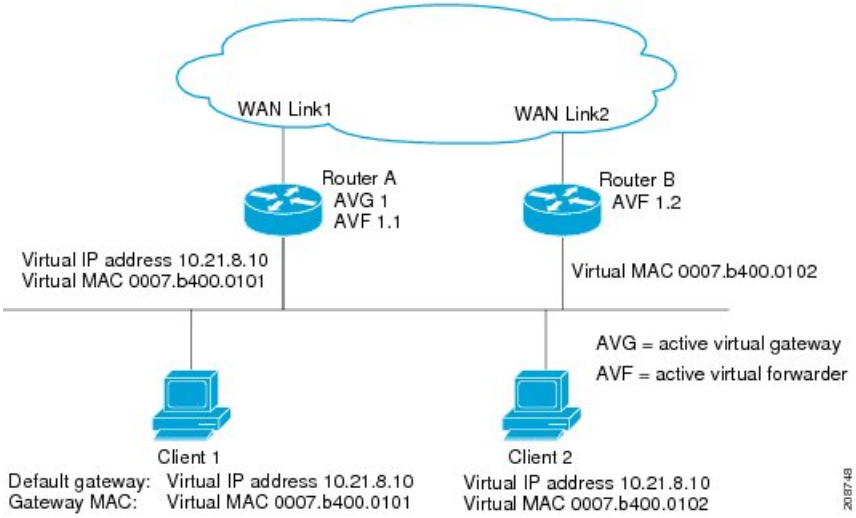
GLBP グループのメンバは、1 つのゲートウェイをそのグループのアクティブ仮想ゲートウェイ（AVG）として選択します。他のグループ メンバは、AVG が使用できなくなった場合のバックアップとなります。AVG は GLBP グループの各メンバに仮想 MAC アドレスを割り当てます。各ゲートウェイは、AVG によって割り当てられている仮想 MAC アドレスに送信されたパケットを転送する役割を引き継ぎます。これらのゲートウェイは、仮想 MAC アドレスのアクティブ仮想フォワーダ（AVF）と呼ばれます。

AVG は、仮想 IP アドレスのアドレス解決プロトコル（ARP）要求への応答も行います。ロード シェアリングは、AVG が異なる仮想 MAC で ARP 要求に応答することによって行われます。

noglbpload-balancing コマンドが設定されている場合は、AVG が AVF を備えていなければ、先頭のバーチャル フォワーダ（VF）の MAC アドレスで ARP 要求に応答します。そのため、その VF が現在の AVG に戻るまでは、トラフィックが別のゲートウェイ経由でルーティングされる可能性があります。

下の図では、ルータ A（またはデバイス A）は GLBP グループの AVG で、仮想 IP アドレス 10.21.8.10 に関する処理を行います。ルータ A は、仮想 MAC アドレス 0007.b400.0101 の AVF でもあります。ルータ B（またはデバイス B）は同じ GLBP グループのメンバであり、仮想 MAC アドレス 0007.b400.0102 の AVF として指定されています。クライアント 1 のデフォルト ゲートウェイ IP アドレスは 10.21.8.10、ゲートウェイ MAC アドレスは 0007.b400.0101 です。クライアント 2 は、同じデフォルト ゲートウェイ IP アドレスを共有しますが、ルータ B がルータ A とトラフィック負荷を分担するため、ゲートウェイ MAC アドレス 0007.b400.0102 が与えられます。

図 *19 : GLBP* トポロジ



ルータ A が使用できなくなった場合でも、クライアント 1 は WAN にアクセスできます。これは、ルータ B がルータ A の仮想 MAC アドレスに送信されたパケットの転送を引き継ぎ、ルータ B 自身の仮想 MAC アドレスに送信されたパケットに応答するからです。ルータ B は、GLBP グループ全体の AVG の役割も引き継ぎます。GLBP グループ内のデバイスで障害が発生しても、GLBP メンバの通信は継続されます。

GLBP 仮想 MAC アドレスの割り当て

GLBP グループごとに最大 4 つの仮想 MAC アドレスを設定できます。AVG は、仮想 MAC アドレスをグループの各メンバに割り当てます。他のグループ メンバは、hello メッセージを通じて AVG を検出したあとで仮想 MAC アドレスを要求します。ゲートウェイには、シーケンスにおける次の MAC アドレスが割り当てられます。AVG によって仮想 MAC アドレスが割り当てられた仮想フォワーダは、プライマリ仮想フォワーダと呼ばれます。GLBP グループの他

のメンバは、hello メッセージから仮想 MAC アドレスを学習します。仮想 MAC アドレスを学習した仮想フォワーダは、セカンダリ仮想フォワーダと呼ばれます。

GLBP 仮想ゲートウェイの冗長性

GLBP では、HSRP と同じ方法で仮想ゲートウェイの冗長性が実現されます。1 つのゲートウェイが AVG として選択され、もう 1 つのゲートウェイがスタンバイ仮想ゲートウェイとして選択されます。残りのゲートウェイはリッスン状態になります。

AVG の機能が停止すると、スタンバイ仮想ゲートウェイが該当する仮想 IP アドレスの処理を担当します。その後、リッスン状態のゲートウェイから新しいスタンバイ仮想ゲートウェイが選択されます。

GLBP 仮想フォワーダの冗長性

仮想フォワーダの冗長化は、AVF で使用する仮想ゲートウェイの冗長化に類似しています。AVF で障害が発生すると、リッスン状態のセカンダリ仮想フォワーダの 1 つが仮想 MAC アドレスの役割を引き継ぎます。

新しい AVF は、別のフォワーダ番号のプライマリ仮想フォワーダでもあります。GLBP は、ゲートウェイがアクティブ仮想フォワーダ状態に変わるとすぐに始動する 2 つのタイマーを使用して、古いフォワーダ番号からホストを移行します。GLBP は hello メッセージを使用してタイマーの現在の状態を通信します。

リダイレクト時間は、AVG がホストを古い仮想フォワーダ MAC アドレスにリダイレクトし続ける時間です。リダイレクト時間が経過すると、仮想フォワーダが、古い仮想フォワーダ MAC アドレスに送信されたパケットを転送し続けても、AVG は、ARP 応答で古い仮想フォワーダ MAC アドレスの使用を停止します。

仮想フォワーダが有効である時間は、セカンダリ ホールド時間になります。セカンダリ ホールド時間が経過すると、GLBP グループのすべてのゲートウェイから仮想フォワーダが削除されます。期限切れになった仮想フォワーダ番号は、AVG による再割り当てが可能になります。

GLBP ゲートウェイのプライオリティ

各 GLBP ゲートウェイが果たすロールと、AVG の機能が停止したときにどのようなことが発生するかについては、GLBP ゲートウェイ プライオリティによって決まります。

また、GLBP デバイスがバックアップ仮想ゲートウェイとして機能するかどうか、および現在の AVG で障害が発生した場合に AVG になる順番も決まります。各バックアップ仮想ゲートウェイのプライオリティには、**glbppriority** コマンドを使用して 1 ～ 255 の値を設定できます。

「GLBP トポロジ」の図では、LAN トポロジ内の AVG であるルータ A（またはデバイス A）で障害が発生すると、選択プロセスが実行され、処理を引き継ぐバックアップ仮想ゲートウェイが決定されます。この例では、ルータ B（またはデバイス B）がグループ内の唯一の他のメンバであるため、ルータ B（またはデバイス B）が自動的に新しい AVG になります。同じ GLBP グループ内にプライオリティの高い別のデバイスが存在していた場合は、そのプライオリティの高いデバイスが選択されます。両方のデバイスのプライオリティが同じである場合

は、IP アドレスが大きい方のバックアップ仮想ゲートウェイが選択され、アクティブ仮想ゲートウェイになります。

デフォルトでは、GLBP 仮想ゲートウェイのプリエンプティブ方式はディセーブルになっています。バックアップ仮想ゲートウェイが AVG になるのは、仮想ゲートウェイに割り当てられているプライオリティにかかわらず、現在の AVG で障害が発生した場合だけです。**glbppreempt** コマンドを使用すると、GLBP 仮想ゲートウェイのプリエンプティブ方式をイネーブルにすることができます。プリエンプションを使用すると、バックアップ仮想ゲートウェイに現在の AVG よりも高いプライオリティが割り当てられている場合に、そのバックアップ仮想ゲートウェイを AVG にすることができます。

GLBP ゲートウェイの重み付けとトラッキング

GLBP では、重み付けによって GLBP グループ内の各デバイスの転送容量を決定します。GLBP グループ内のデバイスに割り当てられた重み付けを使用して、そのルータがパケットを転送するかどうか、転送する場合はパケットを転送する LAN 内のホストの比率を決定できます。しきい値は、GLBP の重み付けが一定の値を下回ったときに転送を無効化し、別のしきい値を上回ったときには自動的に転送を再度有効化にするように設定できます。

GLBP グループの重み付けは、デバイス内のインターフェイス状態のトラッキングによって自動的に調整できます。追跡対象のインターフェイスがダウンした場合、GLBP グループの重み付けは指定された値だけ小さくなります。GLBP の重み付けの減少値は、追跡対象のインターフェイスごとに変えることができます。

デフォルトでは、GLBP 仮想フォワーダのプリエンプティブ方式はイネーブルになっており、遅延は 30 秒です。現在の AVF の重み付けが下限しきい値を下回り、その状態で 30 秒経過すると、バックアップ仮想フォワーダが AVF になります。**noglbpforwarderpreempt** コマンドを使用して GLBP 転送のプリエンプティブ方式を無効化するか、**glbpforwarderpreemptdelayminimum** コマンドを使用して遅延を変更することができます。

GLBP MD5 認証

GLBP MD5 認証は、信頼性とセキュリティを向上させるために業界標準の MD5 アルゴリズムを採用しています。MD5 認証を使用すると、別のプレーン テキスト認証方式よりもセキュリティを強化でき、スプーフィング ソフトウェアから保護できます。

MD5 認証では、各 GLBP グループ メンバが秘密キーを使用して、発信パケットに含まれるキー付き MD5 ハッシュを生成できます。着信パケットのキー付きハッシュが生成され、着信パケット内のハッシュが生成されたハッシュに一致しない場合、そのパケットは無視されます。

MD5 ハッシュのキーは、キーストリングを使用して設定で直接指定するか、またはキーチェーンを使用して間接的に指定できます。キーストリングは、100 文字の長さを超えることはできません。

デバイスは、GLBP グループに対する認証設定と異なる設定を持つデバイスからの着信 GLBP パケットを無視します。GLBP には、次の 3 つの認証方式があります。

- 認証なし
- プレーン テキスト認証

- MD5 認証

GLBP パケットは、次のいずれかの場合に拒否されます。

- 認証方式がデバイスと着信パケットの間で異なっている。
- MD5 ダイジェストがデバイスと着信パケットで異なる。
- テキスト認証文字列がデバイスと着信パケットで異なる。

ISSU-GLBP

GLBP はインサービス ソフトウェア アップグレード（ISSU）をサポートします。ISSU を使用すると、アクティブおよびスタンバイのルート プロセッサ（RP）またはライン カード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムをステートフル スイッチオーバー（SSO）モードで実行できるようになります。

ISSU は、サポートされる Cisco IOS Release から別のリリースへアップグレードまたはダウングレードする機能を提供します。この場合、パケット転送は継続して行われ、セッションは維持されるため、予定されるシステムの停止時間を短くすることができます。アップグレードまたはダウングレードする機能は、アクティブ RP およびスタンバイ RP 上で異なるバージョンのソフトウェアを実行することで実現します。これにより、RP 間でステート情報を維持する時間が短くなります。この機能により、システムをアップグレード対象（またはダウングレード対象）のソフトウェアを実行するセカンダリ RP に切り替えることができ、セッションを切断することなく、またパケットの損失も最小限に抑えながら、継続してパケットを転送できます。この機能は、デフォルトでイネーブルにされています。

GLBP SSO

GLBP SSO 機能が導入されたため、GLBP はステートフル スイッチオーバー（SSO）を認識するようになりました。GLBP は、デバイスがセカンダリ ルータ プロセッサ（RP）にフェールオーバーしたことを検出し、グループの現在の状態を継続することができます。

SSO は、デュアル RP をサポートするネットワーキング デバイス（通常はエッジ デバイス）で機能します。1 台の RP をアクティブ プロセッサとして設定し、他の RP をスタンバイ プロセッサとして設定することで、RP 冗長化を実現します。また、RP 間の重要なステート情報を同期するため、ネットワーク ステート情報は RP 間でダイナミックに維持されます。

SSO を認識せずに RP が冗長化されたデバイスに GLBP を展開した場合、アクティブ RP とスタンバイ RP 間のロールがスイッチオーバーされると、デバイスの GLBP グループ メンバとしてのアクティビティは破棄され、デバイスはリロードされた場合と同様にグループに再び参加することになります。GLBP SSO 機能により、スイッチオーバーが行われても、GLBP は継続してグループ メンバとしてのアクティビティを継続できます。冗長化された RP 間の GLBP ステート情報は維持されるため、スタンバイ RP はスイッチオーバーの実行中も実行後も GLBP 内で引き続きデバイスのアクティビティを実行できます。

この機能は、デフォルトでイネーブルにされています。この機能をディセーブルにするには、グローバル コンフィギュレーション モードで **noglbpsso** コマンドを使用します。

GLBP の利点

ロード シェアリング

LAN クライアントからのトラフィックを複数のデバイスで共有するように GLBP を設定できるため、利用可能なデバイス間でより公平にトラフィックの負荷を共有できます。

複数の仮想デバイス

GLBP では、デバイスの各物理インターフェイス上に最大 1024 台の仮想デバイス（GLBP グループ）とグループごとに最大 4 つの仮想フォワーダがサポートされます。

プリエンプション

GLBP の冗長性スキームにより、使用可能になっているプライオリティの高いバックアップ仮想ゲートウェイをアクティブ仮想ゲートウェイ（AVG）にすることができます。フォワーダ プリエンプションも同じように機能しますが、フォワーダ プリエンプションはプライオリティの代わりに重み付けを使用し、デフォルトでイネーブルになっている点が異なります。

認証

GLBP は、信頼性やセキュリティを向上させて GLBP スプーフィング ソフトウェアからの保護を強化するための業界標準のメッセージ ダイジェスト 5（MD5）アルゴリズムをサポートしています。GLBP グループ内のデバイスの認証文字列が他のデバイスとは異なる場合、そのデバイスは他のグループ メンバによって無視されます。GLBP グループ メンバ間で簡単なテキスト パスワード認証方式を使用して、設定エラーを検出することもできます。

GLBP の設定方法

GLBP のカスタマイズ

GLBP 動作のカスタマイズは任意です。GLBP グループをイネーブルにすると、そのグループはすぐに動作します。GLBP グループをイネーブルにしてから GLBP をカスタマイズすると、機能のカスタマイズを完了する前にデバイスがグループの制御を引き継ぎ、AVG になる可能性があります。したがって、GLBP をカスタマイズする場合は、GLBP をイネーブルにする前に行うことを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプおよび番号を指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 4	**ipaddress** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.21.8.32 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group***timers** [**msec**] *hellotime* [**msec**] *holdtime* 例： `Device(config-if)# glbp 10 timers 5 18`	GLBP グループ内の AVG によって連続的に送信される hello パケットの間隔を設定します。 • *holdtime* 引数には、hello パケット内の仮想ゲートウェイと仮想フォワーダの情報が無効と見なされるまでの時間を秒数で指定します。 • オプションの **msec** キーワードは、そのあとに続く引数がデフォルトの秒単位ではなくミリ秒単位であることを指定します。
ステップ 6	**glbp** *group***timersredirect** *redirect timeout* 例： `Device(config-if)# glbp 10 timers redirect 1800 28800`	AVG がクライアントを AVF にリダイレクトし続ける時間を設定します。デフォルトは 600 秒（10 分）です。 • *timeout* 引数には、セカンダリ仮想フォワーダが無効になるまでの時間を秒数で指定します。デフォルトは 14,400 秒（4 時間）です。

	コマンドまたはアクション	目的
		（注） *redirect* 引数のゼロ（0）値は、指定できる値の範囲から除外することはできません。Cisco IOS ソフトウェアの事前設定でゼロ（0）値を使用しているため、アップグレードに悪影響を及ぼすことになります。ただし、ゼロ（0）値に設定することは推奨しません。この値を使用すると、リダイレクトタイマーが期限切れになりません。リダイレクトタイマーが期限切れにならず、デバイスに障害が発生すると、新しいホストがバックアップへリダイレクトされずに、障害が発生したデバイスに引き続き割り当てられます。
ステップ 7	**glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**] 例： `Device(config-if)# glbp 10 load-balancing host-dependent`	GLBP AVG で使用するロードバランシングの方式を指定します。
ステップ 8	**glbp** *group* **priority** *level* 例： `Device(config-if)# glbp 10 priority 254`	GLBP グループ内のゲートウェイのプライオリティ レベルを設定します。 • デフォルト値は 100 です。
ステップ 9	**glbp** *group* **preempt** [**delay minimum** *seconds*] 例： `Device(config-if)# glbp 10 preempt delay minimum 60`	デバイスのプライオリティが現在の AVG よりも高い場合に、GLBP グループの AVG として処理を引き継ぐようにルータを設定します。 • このコマンドは、デフォルトでディセーブルになっています。 • AVG の交替が行われるまでの最小遅延インターバルを秒数で指定するには、オプションの **delay** キーワードおよび **minimum** キーワー

	コマンドまたはアクション	目的
		ドおよび *seconds* 引数を指定します。
ステップ 10	**glbp** *group* **client-cachemaximum** *number* [**timeout** *minutes*] 例： `Device(config-if)# glbp 10 client-cache maximum 1200 timeout 245`	（任意）GLBP クライアント キャッシュをイネーブルにします。 • このコマンドは、デフォルトでディセーブルになっています。 • *number* 引数を使用して、キャッシュがこの GLBP グループのためにホールドするクライアントの最大数を指定します。範囲は 8 ～ 2000 です。 • オプションの **timeout** *minutes* キーワードと引数のペアを使用して、クライアント情報が最後に更新されてから、クライアントエントリが GLBP クライアント キャッシュに保管される最大時間を設定します。範囲は、1 ～ 1440 分（1 日）です。 （注） IPv4 ネットワークには、予測されるエンド ホストの Address Resolution Protocol（ARP）キャッシュの最大タイムアウト値よりも若干長い GLBP クライアント キャッシュのタイムアウト値を設定することを推奨します。
ステップ 11	**glbp** *group* **name** *redundancy-name* 例： `Device(config-if)# glbp 10 name abc123`	GLBP グループに名前を割り当てることによって、IP 冗長性をイネーブルにします。 • 冗長クライアントと GLBP グループを接続できるように、GLBP 冗長クライアントに同じ GLBP グループ名を設定する必要があります。
ステップ 12	**exit** 例：	インターフェイス コンフィギュレーションモードを終了し、デバイスをグ

	コマンドまたはアクション	目的
	`Device(config-if)# exit`	ローバル コンフィギュレーション モードに戻します。
ステップ 13	**noglbpsso** 例： `Device(config)# no glbp sso`	（任意）SSO の GLBP サポートをディセーブルにします。

キー ストリングを使用した GLBP MD5 認証の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaddress** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group-number* **authenticationmd5key-string** [**0** | **7**] *key* 例： `Device(config-if)# glbp 1 authentication md5 key-string d00b4r987654321a`	GLBP MD5 認証の認証キーを設定します。 • キー ストリングは、100 文字の長さを超えることはできません。 • *key* 引数にはプレフィックスを指定しません。**0** を指定すると、キーは暗号化されていないことを示します。

	コマンドまたはアクション	目的
		• **7** を指定すると、キーは暗号化されます。**servicepassword-encryption** グローバル コンフィギュレーション コマンドがイネーブルになっている場合、key-string 認証キーは自動的に暗号化されます。
ステップ 6	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# glbp 1 ip 10.0.0.10`	インターフェイス上でGLBPを設定し、仮想ゲートウェイのプライマリ IP アドレスを指定します。
ステップ 7	通信する各デバイスに対してステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**showglbp** 例： `Device# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。設定されている場合はキー ストリングと認証タイプが表示されます。

キー チェーンを使用した GLBP MD5 認証の設定

キー チェーンを使用したGLBP MD5認証を設定するには、次の作業を実行します。キー チェーンを使用すると、キー チェーン設定に従って異なる時点で異なるキー ストリングを使用できます。GLBP は、適切なキー チェーンを照会して、指定されたキー チェーンの現在アクティブなキーとキー ID を取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**keychain** *name-of-chain* 例： `Device(config)# key chain glbp2`	ルーティング プロトコルの認証をイネーブルにし、認証キーのグループを識別し、キー チェーン キー コンフィギュレーション モードを開始します。
ステップ 4	**key** *key-id* 例： `Device(config-keychain)# key 100`	キー チェーンの認証キーを識別します。 • *key-id* 引数の値には数値を指定する必要があります。
ステップ 5	**key-string** *string* 例： `Device(config-keychain-key)# key-string abc123`	キーの認証文字列を指定し、キー チェーン キー コンフィギュレーション モードを開始します。 • *string* 引数の値は、1 ～ 80 文字の大文字または小文字の英数字を指定できます。最初の文字には数字を使用できません。
ステップ 6	**exit** 例： `Device(config-keychain-key)# exit`	キー チェーン キー コンフィギュレーション モードに戻ります。
ステップ 7	**exit** 例： `Device(config-keychain)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイスタイプを設定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 9	**ipaddress** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.21.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 10	**glbp** *group-number* **authentication md5 key-chain** *name-of-chain* 例： `Device(config-if)# glbp 1 authentication md5 key-chain glbp2`	GLBP MD5 認証の認証 MD5 キーチェーンを設定します。 • キーチェーン名は、ステップ 3 で指定した名前に一致する必要があります。
ステップ 11	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# glbp 1 ip 10.21.0.12`	インターフェイス上で GLBP を設定し、仮想ゲートウェイのプライマリ IP アドレスを指定します。
ステップ 12	通信する各デバイスに対してステップ 1 ～ 10 を繰り返します。	—
ステップ 13	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 14	**showglbp** 例： `Device# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。設定されている場合はキーチェーンと認証タイプが表示されます。
ステップ 15	**showkeychain** 例： `Device# show key chain`	（任意）認証キー情報を表示します。

GLBP テキスト認証の設定

テキスト認証は最小限のセキュリティを提供します。セキュリティが必須の場合は、MD5 認証を使用してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaddress** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group-number* **authenticationtext** *string* 例： `Device(config-if)# glbp 10 authentication text stringxyz`	グループ内の他のデバイスから受信した GLBP パケットを認証します。 • 認証を設定する場合は、GLBP グループ内のすべてのデバイスで同じ認証文字列を使用する必要があります。
ステップ 6	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# glbp 1 ip 10.0.0.10`	インターフェイス上でGLBPを設定し、仮想ゲートウェイのプライマリ IP アドレスを指定します。
ステップ 7	通信する各デバイスに対してステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**showglbp** 例： `Device# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。

GLBP の重み付けの値とオブジェクト トラッキング

GLBP 重み付けにより、GLBP グループが仮想フォワーダとして動作できるかどうかが決定されます。重み付けの初期値を設定したり、オプションのしきい値を指定したりできます。インターフェイスの状態を追跡し、インターフェイスがダウンした場合に重み付けの値を減らすための減少値を設定できます。GLBP グループの重み付けが指定の値を下回ると、グループはアクティブ仮想フォワーダでなくなります。重み付けが指定の値を上回ると、グループは再びアクティブ仮想フォワーダとしてのロールを実行できるようになります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number***interface** *type number* {**line-protocol** |{**ip** | **ipv6**} **routing**} 例： `Device(config)# track 2 interface GigabitEthernet 1/0/1 ip routing`	GLBP ゲートウェイの重み付けに影響する状態変化を追跡するインターフェイスを設定し、トラッキング コンフィギュレーション モードを開始します。 • このコマンドは、**glbpweightingtrack** コマンドで使用されるインターフェイスと対応するオブジェクトの数を設定します。 • **line-protocol** キーワードを指定すると、インターフェイスがアップ状態かどうかが追跡されます。**iprouting** キーワードを指定すると、インターフェイス上でIPルーティングがイネーブルであり、IP アドレスが設定されているかどうかもチェックされます。
ステップ 4	**exit** 例： `Device(config-track)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*] 例： `Device(config-if)# glbp 10 weighting 110 lower 95 upper 105`	GLBP ゲートウェイの重み付けの初期値、上限しきい値、および下限しきい値を指定します。
ステップ 7	**glbp** *group* **weightingtrack** *object-number* [**decrement** *value*] 例： `Device(config-if)# glbp 10 weighting track 2 decrement 5`	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。 • *value* 引数には、追跡対象のオブジェクトで障害が発生した場合に GLBP ゲートウェイの重み付けを減らす量を指定します。
ステップ 8	**glbp** *group* **forwarderpreempt** [**delayminimum** *seconds*] 例： `Device(config-if)# glbp 10 forwarder preempt delay minimum 60`	GLBP グループの現在の AVF の値が重みしきい値よりも低くなった場合に、GLBP グループの AVF としてのロールを引き継ぐデバイスを設定します。 • このコマンドは、デフォルトでイネーブルになっており、遅延は 30 秒です。 • AVF の交替が行われるまでの最小遅延インターバルを秒数で指定するには、オプションの **delay** キーワードおよび **minimum** キーワードおよび *seconds* 引数を指定します。
ステップ 9	**exit** 例： `Device(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 10	**showtrack** [*object-number* | **brief**] [**interface** [**brief**] | **iproute** [**brief**] | **resolution** | **timers**]	トラッキング情報を表示します。

	コマンドまたはアクション	目的
	例： `Device# show track 2`	

GLBP のトラブルシューティング

GLBP には、GLBP 動作に関する各種イベントに関連する診断出力を可視化する 5 つの特権 EXEC モード コマンドが導入されています。**debugconditionglbp**、**debugglbperrors**、**debugglbpevents**、**debugglbppackets**、**debugglbpterse** の各コマンドは、トラブルシューティング専用です。これはソフトウェアによって生成される出力のボリュームが、デバイスの深刻なパフォーマンスの低下を引き起こす可能性があるためです。**debugglbp** コマンドを使用した場合の影響を最小限に抑えるには、次の作業を実行します。

この手順により、コンソール ポートが文字単位のプロセッサ割り込みを行わなくなるため、**debugconditionglbp** コマンドまたは **debugglbp** コマンドを使用することでデバイスにかかる負荷が最小限に抑えられます。直接コンソールに接続できない場合は、ターミナルサーバを介してこの手順を実行できます。ただし、Telnet 接続を切断しなければならない場合は、デバッグ出力の生成でプロセッサに負荷がかかりデバイスが応答できないことに起因して、再接続できないことがあります。

始める前に

この作業では、コンソールに直接接続された GLBP を実行しているデバイスが必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**nologgingconsole** 例： `Device(config)# no logging console`	コンソール端末へのすべてのロギングをディセーブルにします。 • コンソールへのロギングを再度イネーブルにするには、グローバル コンフィギュレーション モードで **loggingconsole** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	Telnet を使用してデバイス ポートにアクセスし、ステップ 1 と 2 を繰り返します。	再帰 Telnet セッションでグローバル コンフィギュレーション モードを開始します。これにより、出力をコンソール ポートからリダイレクトできます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**terminalmonitor** 例： `Device# terminal monitor`	仮想端末でのロギング出力をイネーブルにします。
ステップ 7	**debugconditionglbp** *interface-type interface-number group* [*forwarder*] 例： `Device# debug condition glbp GigabitEthernet 0/0/0 1`	GLBP 状態に関するデバッグ メッセージを表示します。 • 特定の **debugconditionglbp** または **debugglbp** コマンドだけを入力して、出力を特定のサブコンポーネントに分離し、プロセッサの負荷を最小限に抑えます。適切な引数とキーワードを使用して、指定したサブコンポーネント上に詳細なデバッグ情報を生成します。 • 終了したら、特定の **nodebugconditionglbp** または **nodebugglbp** コマンドを入力します。
ステップ 8	**terminalnomonitor** 例： `Device# terminal no monitor`	仮想端末でのロギングをディセーブルにします。

GLBP の設定例

例：GLBP 設定のカスタマイズ

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 timers 5 18
```

```
Device(config-if)# glbp 10 timers redirect 1800 28800
Device(config-if)# glbp 10 load-balancing host-dependent
Device(config-if)# glbp 10 priority 254
Device(config-if)# glbp 10 preempt delay minimum 60

Device(config-if)# glbp 10 client-cache maximum 1200 timeout 245
```

例：キー ストリングを使用した GLBP MD5 認証の設定

次に、キー ストリングを使用して GLBP MD5 認証を設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-string ThisStringIsTheSecretKey
Device(config-if)# glbp 2 ip 10.0.0.10
```

例：キー チェーンを使用した GLBP MD5 認証の設定

次に、GLBP がキー チェーン「AuthenticateGLBP」を照会して、指定されたキー チェーンの現在アクティブなキーとキー ID を取得する例を示します。

```
Device(config)# key chain AuthenticateGLBP
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASecretKey
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
Device(config-if)# glbp 2 ip 10.0.0.10
```

例：GLBP テキスト認証の設定

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 authentication text stringxyz
Device(config-if)# glbp 10 ip 10.21.8.10
```

例：GLBP 重み付けの設定

次に、デバイスを POS インターフェイス 5/0/0 と 6/0/0 の IP ルーティング状態を追跡するように設定し、GLBP の重み付けの初期値、上限しきい値、下限しきい値、および重み付けの減少値 10 を設定する例を示します。POS インターフェイス 5/0/0 と 6/0/0 がダウンすると、デバイスの重み付けの値が小さくなります。

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1 decrement 10
Device(config-if)# glbp 10 weighting track 2 decrement 10
```

例：GLBP 設定のイネーブル化

次の例では、デバイスは GLBP をイネーブルにするように設定されています。GLBP グループ 10 には、仮想 IP アドレス 10.21.8.10 が指定されています。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 ip 10.21.8.10
```

GLBP に関する追加情報

関連資料

関連項目	マニュアル タイトル
GLBP コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例。	『Cisco IOS IP Application Services Command Reference』
インサービス ソフトウェア アップグレード（ISSU）の設定	『*Cisco IOS High Availability Configuration Guide*』の「In Service Software Upgrade Process」のモジュール
キーチェーンおよびキー管理用コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Routing Protocol-Independent Command Reference*』
オブジェクト トラッキング	「Configuring Enhanced Object Tracking」のモジュール
『Stateful Switchover』	『*Cisco IOS High Availability Configuration Guide*』の「Stateful Switchover」のモジュール
VRRP	「Configuring VRRP」のモジュール
HSRP	「Configuring HSRP」のモジュール
GLBP の IPv6 サポート	「FHRP - GLBP Support for IPv6」のモジュール

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GLBP の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *30 : GLBP* の機能情報

機能名	リリース	機能の設定情報
Gateway Load Balancing Protocol		GLBP は、冗長化されたルータ グループ間でパケットのロード シェアリングを行う一方、タ トラフィックを保護します。 Cisco IOS Release Cisco IOS XE Release 3.6E では、この機能は以下のプラットフォームでサ • Cisco 5760 Wireless LAN Controller 次のコマンドがこの機能によって導入、または変更されました： **glbpforwarderpreemptglbpipglbpload-balancingglbpnameglbppreemptglbppriorityglbpssoglbp**

機能名	リリース	機能の設定情報
GLBP MD5 認証	Cisco IOS XE 3.6E	MD5 認証を使用すると、別のプレーン テキスト認証方式よりもセキュリティを強化で して、発信パケットに含まれるキー付きMD5ハッシュを生成できます。着信パケットの れたハッシュに一致しない場合、そのパケットは無視されます。 Cisco IOS Release Cisco IOS XE Release 3.6E では、この機能は以下のプラットフォームで • Cisco 5760 Wireless LAN Controller **glbpauthentication** および **showglbp** の各コマンドがこの機能により変更されました。
ISSU と GLBP		GLBP はインサービス ソフトウェア アップグレード（ISSU）をサポートします。ISSU （RP）またはライン カード上で異なるバージョンの Cisco IOS ソフトウェアが実行され フル スイッチオーバー（SSO）モードで実行できるようになります。 この機能は、ソフトウェア アップグレード中に予定されたシステム停止中も同じレベル SSO を使用できます。つまり、システムをセカンダリ RP に切り替えることができ、セッ がら、継続してパケットを転送できます。 この機能は、デフォルトでイネーブルにされています。 この機能により、新規追加または変更されたコマンドはありません。
SSO：GLBP		GLBP が SSO を認識するようになりました。GLBP は、ルータがセカンダリ RP にフェ することができます。 別の RP がインストールされ、プライマリ RP が機能を停止した場合にはその処理を引き これを認識できません。プライマリが機能を停止すると、GLBP デバイスは GLBP グル 内の他のルータにアクティブ ルータとしてのロールが引き継がれます。このように機能 出できるようになったため、GLBP グループに何ら変化は生じません。セカンダリ RP 態であると、GLBP グループはこの状態を検出して新たなアクティブ GLBP ルータを再 この機能は、デフォルトでイネーブルにされています。 **debugglbpevents**、**glbpsso**、**showglbp** の各コマンドがこの機能によって導入または修正

用語集

アクティブ RP：ルート プロセッサ（RP）はシステムの制御、ネットワーク サービスの提供、ルーティング プロトコルの実行、システム管理インターフェイスの有効化を実行します。

AVF：Active Virtual Forwarder（アクティブ仮想フォワーダ）。GLBP グループ内の 1 つの仮想フォワーダが、指定の仮想 MAC アドレスのアクティブ仮想フォワーダとして選定されます。選定されたフォワーダは、指定の MAC アドレスに対するパケットの転送を処理します。1 つの GLBP グループに複数のアクティブ仮想フォワーダを存在させることができます。

AVG：Active Virtual Gateway（アクティブ仮想ゲートウェイ）。アクティブ バーチャル ゲートウェイとして選択され、プロトコルの動作を担当する、GLBP グループ内の 1 つのバーチャル ゲートウェイ。

GLBP ゲートウェイ：Gateway Load Balancing Protocol ゲートウェイ。GLBP を実行するルータまたはゲートウェイ。各 GLBP ゲートウェイは、1 つまたは複数の GLBP グループに参加できます。

GLBP グループ：Gateway Load Balancing Protocol グループ。接続されたイーサネットインターフェイス上で同じ GLBP グループ番号を持つ、1 つまたは複数の GLBP ゲートウェイ。

ISSU：In Service Software Upgrade（インサービス ソフトウェア アップグレード）。パケット転送の実行中に Cisco IOS XE ソフトウェアの更新や変更を可能にするプロセス。ほとんどのネットワークでは、計画的なソフトウェアアップグレードがダウンタイムの大きな原因になっています。ISSU を使用すると、パケット転送中にソフトウェアを変更できるため、ネットワークのアベイラビリティが向上し、計画的なソフトウェアアップグレードによるダウンタイムを短縮できます。

NSF：Nonstop Forwarding（ノンストップ フォワーディング）。機能停止状態からの回復処理を行っているルータに対してトラフィックの転送を継続するルータの機能。また、障害からの回復中であるルータは、自身に送信されたトラフィックをピアによって正しく転送することができます。

RP：ルート プロセッサ。シャーシに搭載される、集中化されたコントロール ユニットの総称です。一般に、プラットフォーム固有の用語が使用されます（Cisco 7500 では RSP、Cisco 10000 では PRE、Cisco 7600 では SUP+MSFC など）。

RPR：Route Processor Redundancy。RPR は、High System Availability（HSA）機能に代替方法を提供します。HSA を使用すると、システムはアクティブ RP が機能を停止したときにスタンバイ RP をリセットして使用できます。RPR を活用すると、アクティブ RP に致命的なエラーが発生したときにアクティブ RP とスタンバイ RP の間で迅速なスイッチオーバーが行われるため、不測のダウンタイムを減らすことができます。

RPR+：RPR の拡張。スタンバイ RP が完全に初期化されます。

SSO：Stateful Switchover（ステートフル スイッチオーバー）。アクティブ装置とスタンバイ装置間のステート情報を保持するためのアプリケーションおよび機能をイネーブルにします。

スタンバイ RP：完全に初期化され、アクティブ RP から制御を引き受ける準備が整った RP。手動または機能停止によってスイッチオーバーが発生します。

スイッチオーバー：システム制御とルーティング プロトコルの実行がアクティブ RP からスタンバイ RP に移行するイベント。スイッチオーバーは、手動操作によって、またはハードウェア/ソフトウェアの機能停止によって発生します。スイッチオーバーには、個々のユニットのシステム制御とパケット転送を組み合わせるシステムでのパケット転送機能の移行が含まれることがあります。

vIP：仮想 IP アドレス。IPv4 アドレス。設定された各 GLBP グループには、必ず 1 つの仮想 IP アドレスがあります。仮想 IP アドレスは、少なくとも 1 つの GLBP グループ メンバに設定する必要があります。他の GLBP グループ メンバは、Hello メッセージを通して仮想 IP アドレスを学習します。

第 VII 部

IP マルチキャスト ルーティング

- IP マルチキャスト ルーティング テクノロジーの概要 （497 ページ）
- IGMP の設定 （507 ページ）
- IGMP プロキシの設定 （579 ページ）
- スイッチド イーサネットでの IP マルチキャストの抑制 （591 ページ）
- PIM の設定 （601 ページ）
- IP マルチキャストに対する PIM MIB 拡張の設定 （679 ページ）
- MSDP の設定 （685 ページ）
- ワイヤレス マルチキャストの設定 （729 ページ）
- SSM の設定 （745 ページ）
- GRE トンネルを介するマルチキャスト ルーティングの設定 （765 ページ）
- サービス検出ゲートウェイの設定 （771 ページ）
- IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパース モードの最適化 （789 ページ）
- IP マルチキャストの最適化：マルチキャスト サブセカンド コンバージェンス （799 ページ）
- IP マルチキャストの最適化：等コスト パス間での IP マルチキャスト ロード スプリッティング （809 ページ）
- IP マルチキャストの最適化：マルチキャスト向け SSM チャネル ベース フィルタリング （835 ページ）
- IP マルチキャストの最適化：PIM デンス モード ステート リフレッシュ （843 ページ）
- IP マルチキャストの最適化：IGMP ステート制限 （851 ページ）

第 27 章

IP マルチキャスト ルーティング テクノロジーの概要

- 機能情報の確認 （497 ページ）
- IP マルチキャスト テクノロジーに関する情報 （497 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IP マルチキャスト テクノロジーに関する情報

情報配信における IP マルチキャストの役割

IP マルチキャストは、単一の情報ストリームを何千もの潜在的な企業および家庭に同時に配信することによってトラフィックを削減する帯域幅節約テクノロジーです。マルチキャストを利用するアプリケーションには、ビデオ会議、企業コミュニケーション、通信教育、およびソフトウェア、株価情報、ニュースの配信などが含まれます。

IP マルチキャスト ルーティングにより、ホスト（ソース）は、IP マルチキャスト グループ アドレスと呼ばれる特別な形式の IP アドレスを使用して、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。ソースのホストは、マルチキャスト グループ アドレスをパケットの宛先 IP アドレス フィールドに挿入します。IP マルチキャスト ルー

タおよびマルチレイヤ スイッチは、受信した IP マルチキャスト パケットを、マルチキャスト グループのメンバにつながるすべてのインターフェイスから転送します。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。

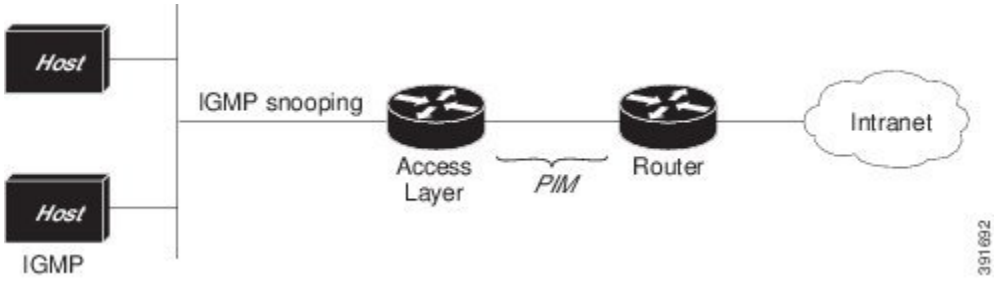
IP マルチキャスト ルーティング プロトコル

ソフトウェアでは、IPマルチキャストルーティングを実装するため、次のプロトコルがサポートされています。

- IGMP を LNA 上のホストとその LAN上のルータ（およびマルチレイヤ デバイス）間で使用して、ホストがメンバになっているマルチキャスト グループを追跡します。IP マルチキャスティングに参加するには、マルチキャスト ホスト、ルータ、およびマルチレイヤ デバイスで Internet Group Management Protocol（IGMP）が動作している必要があります。
- PIM（Protocol Independent Multicast）は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにルータ間で使用されます。
- IGMP スヌーピングは、レイヤ 2 スイッチング環境でのマルチキャストに使用します。レイヤ 2 インターフェイスを動的に設定し、マルチキャスト トラフィックが IP マルチキャストデバイスと関連付けられたインターフェイスにだけ転送されるようにすることによって、マルチキャスト トラフィックのフラッディングを削減します。

次の図に、これらのプロトコルが IP マルチキャスト環境内のどの部分で動作するかを示します。

図 *20 : IP* マルチキャスト ルーティング プロトコル



IPv4 マルチキャスト標準に従い、MAC 宛先マルチキャスト アドレスは 0100:5e で始まり、IP アドレスの末尾 23 ビットが付加されます。たとえば、IP 宛先アドレスが 239.1.1.39 の場合、MAC 宛先アドレスは 0100:5e01:0127 となります。

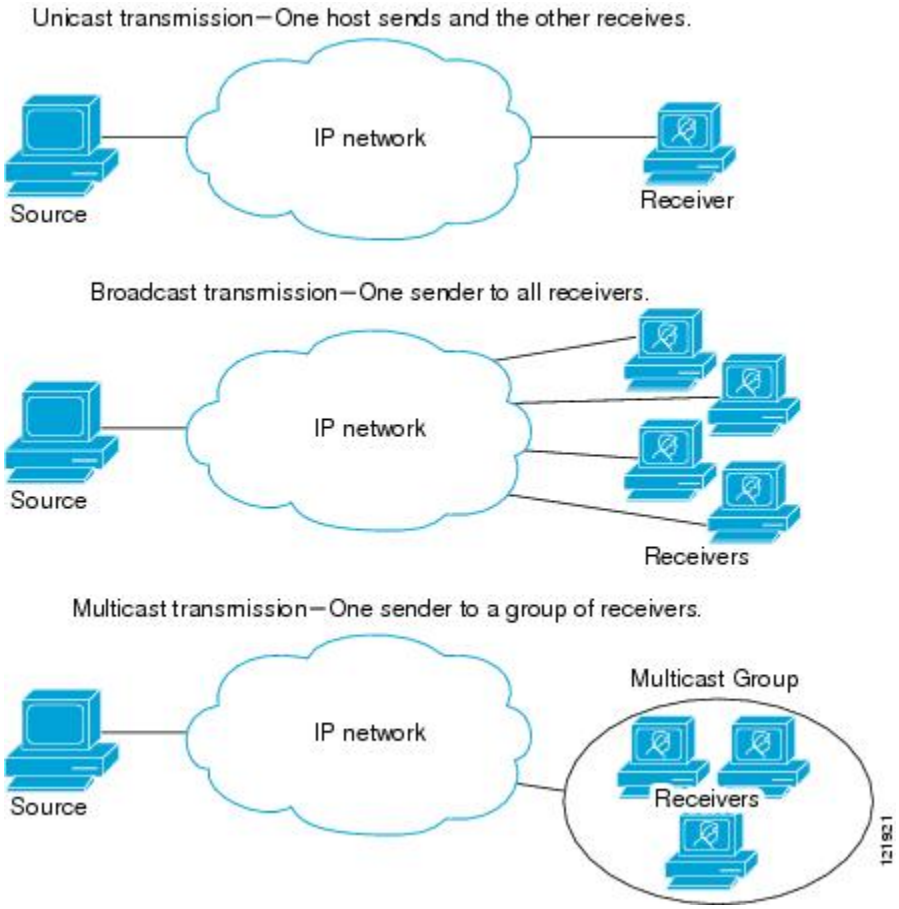
IPv4宛先アドレスとMAC宛先アドレスが一致しない場合、マルチキャスト パケットは一致しません。デバイスは、ハードウェア内の一致しないパケットをMACアドレス テーブルに基づいて転送します。MAC 宛先アドレスが MAC アドレス テーブルにない場合、デバイスは受信したポートと同じ VLAN 内のすべてのポートにパケットをフラッディングします。

マルチキャスト グループ伝送方式

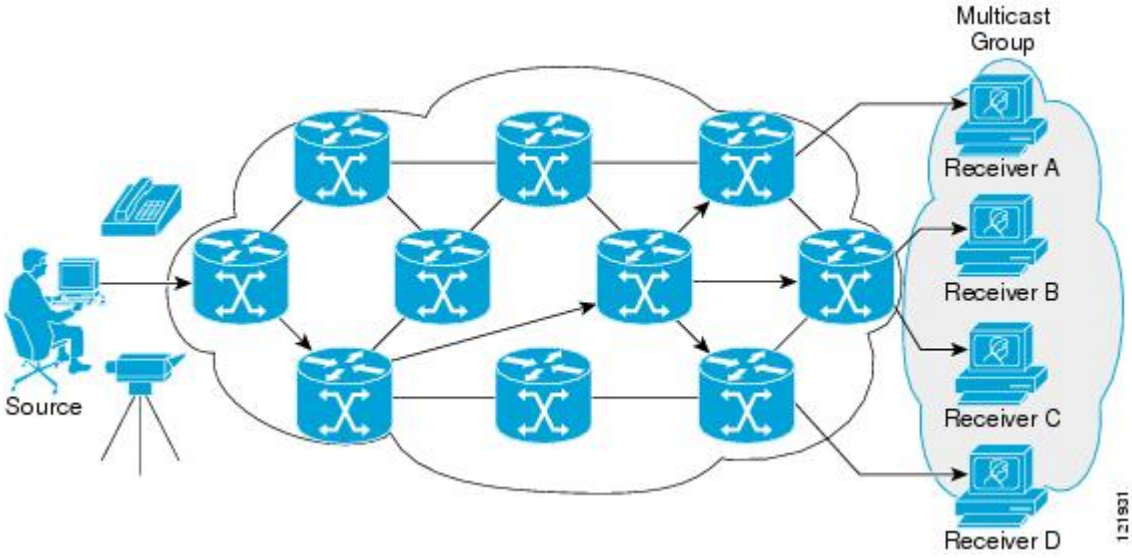
IP 通信は、最初の図に示すように、トラフィックの送信者として機能するホストと、レシーバとして機能するホストで構成されます。送信者はソースと呼ばれます。従来の IP 通信は、単一のホスト ソースがパケットを別の単一ホスト（ユニキャスト伝送）またはすべてのホスト（ブロードキャスト伝送）に送信することによって行われます。IP マルチキャストは第三の方式を提供するものであり、ホストはすべてのホストのサブセットにパケットを送信できます（マルチキャスト伝送）。受信側のホストのこのサブセットをマルチキャスト グループと呼びます。マルチキャスト グループに属するホストは、グループ メンバと呼ばれます。

マルチキャストは、このグループの概念に基づいています。マルチキャスト グループは、特定のデータ ストリームを受信するためにグループに加入する任意の数のレシーバです。このマルチキャスト グループには、物理的境界または地理的境界はありません。ホストは、インターネット上または任意のプライベート ネットワーク上のどこにでも配置できます。ソースから特定のグループに対するデータを受信する必要があるホストはそのグループに加入する必要があります。グループに加入するには、ホスト レシーバで Internet Group Management Protocol（IGMP）を使用します。

マルチキャスト環境では、どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、そのグループに送信されたパケットはグループのメンバだけが受信できます。IP ユニキャスト パケットと同様、マルチキャスト パケットは、ベストエフォート型の信頼性を使用してグループに配信されます。



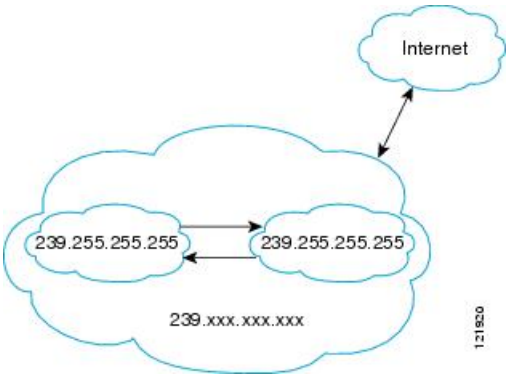
次の図では、レシーバ（指定したマルチキャスト グループ）がソースからのビデオ データ ストリームを受信する必要があります。これらのレシーバは、ネットワーク内のルータに IGMP ホスト レポートを送信することによってその意思を示します。この場合、ルータがソースからレシーバへのデータの配信を担います。ルータは、Protocol Independent Multicast（PIM）を使用して、マルチキャスト配信ツリーを動的に作成します。その後、ソースとレシーバ間のパスにあるネットワーク セグメントにのみ、ビデオ データ ストリームが配信されます。



IP マルチキャスト境界

図に示すように、アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界を定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

図 *21 :* 境界でのアドレス スコーピング



マルチキャスト グループ アドレッシングのインターフェイスに管理スコープの境界を設定するには、**ipmulticastboundary** コマンドと *access-list* 引数を使用します。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。境界が設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

Internet Assigned Numbers Authority（IANA）は、マルチキャスト アドレス範囲 239.0.0.0 ～ 239.255.255.255 を管理スコープ アドレスとして指定しています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。これらは、グローバルに一意ではなくローカルとみなされます。

filter-autorp キーワードを設定して、管理用スコープの境界で Auto-RP 検出と通知メッセージを検査し、フィルタできます。境界のアクセス コントロール リスト（ACL）に拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

IP マルチキャスト グループ アドレッシング

マルチキャスト グループは、マルチキャスト グループ アドレスによって識別されます。マルチキャスト パケットは、そのマルチキャスト グループ アドレスに配信されます。単一のホストを独自に識別するユニキャスト アドレスとは異なり、マルチキャスト IP アドレスは特定のホストを識別しません。マルチキャストアドレスに送信されるデータを受信するには、アドレスが識別するグループにホストが参加する必要があります。データは、マルチキャストアドレスに送信され、そのグループに送信されたトラフィックを受信する意思を示してグループに加入しているすべてのホストによって受信されます。マルチキャスト グループ アドレスは、送信元でグループに割り当てられます。マルチキャスト グループ アドレスを割り当てるネットワーク管理者は、Internet Assigned Numbers Authority（IANA）で予約されるマルチキャスト アドレスの範囲にアドレスが準拠していることを確認する必要があります。

IP クラス D アドレス

IP マルチキャスト アドレスは、IANA によって IPv4 クラス D アドレス空間に割り当てられました。クラス D アドレスの上位 4 ビットは 1110 です。したがって、ホスト グループ アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 であると考えられます。マルチキャスト アドレスは送信元（送信者）でマルチキャスト グループの受信先として選択されます。

（注） クラス D アドレスの範囲は、IP マルチキャスト トラフィックのグループ アドレスまたは宛先アドレスにだけ使用されます。マルチキャストデータグラムの送信元アドレスは常にユニキャスト送信元アドレスになります。

IP マルチキャスト アドレスのスコーピング

さまざまなアドレス範囲の予測可能な動作を提供したり、より小規模なドメイン内でアドレスを再利用したりできるよう、マルチキャストアドレスの範囲はさらに分割されます。表に、マルチキャスト アドレスの範囲を要約します。それに続いて、各範囲について簡単に説明します。

表 *31* : マルチキャスト アドレス範囲の割り当て

名前	範囲	説明
予約済みリンクローカル アドレス	224.0.0.0 ～ 224.0.0.255	ローカル ネットワーク セグメントのネットワーク プロトコルで使用するために予約されています。

名前	範囲	説明
グローバル スコープ アドレス	224.0.1.0 ～ 238.255.255.255	組織間およびインターネット上でマルチキャストデータを送信するために予約されています。
Source Specific Multicast	232.0.0.0 ～ 232.255.255.255	明示的にグループに参加している受信者だけにデータを転送する SSM データグラム配信モデル用に予約されています。
GLOP アドレス	233.0.0.0 ～ 233.255.255.255	割り当て済みの自律システム（AS）ドメイン番号をすでに持つ組織によって静的に定義されるアドレス用に予約されています。
限定スコープ アドレス	239.0.0.0 ～ 239.255.255.255	管理スコープ アドレスまたはプライベート マルチキャスト ドメインで使用するための限定スコープアドレスとして予約されています。

予約済みリンクローカル アドレス

IANA では、ローカル ネットワーク セグメントのネットワーク プロトコルで使用するために 224.0.0.0 ～ 224.0.0.255 の範囲を予約しています。この範囲のアドレスを持つパケットはスコープ内ローカルであり、IP ルータによって転送されません。通常、リンク ローカル宛先アドレスを持つパケットは存続可能時間（TTL）値 1 を使用して送信されるため、ルータによって転送されません。

この範囲内の予約済みリンクローカル アドレスは、それぞれに予約されたネットワーク プロトコル機能を提供します。ネットワーク プロトコルは、これらのアドレスをルータの自動検出および重要なルーティング情報の伝達用に使用します。たとえば、Open Shortest Path First（OSPF）は、IP アドレスの 224.0.0.5 と 224.0.0.6 を使用してリンクステート情報を交換します。

IANA では、ネットワーク プロトコルやネットワーク アプリケーションに対する単一マルチキャスト アドレス要求を 224.0.1.xxx のアドレス範囲外に割り当てています。マルチキャスト ルータはこれらのマルチキャスト アドレスを転送します。

グローバル スコープ アドレス

224.0.1.0 ～ 238.255.255.255 の範囲のアドレスは、グローバル スコープ アドレスと呼ばれます。これらのアドレスは、組織間およびインターネット上でのマルチキャストデータの送信に使用します。これらのアドレスの一部はマルチキャスト アプリケーションで使用するよう IANA によって予約されています。たとえば、IPアドレス 224.0.1.1 は、Network Time Protocol（NTP）用に予約されています。

Source Specific Multicast アドレス

232.0.0.0/8 のアドレス範囲は、Source Specific Multicast（SSM）用に予約されています。Cisco IOS ソフトウェアでは、**ippimssm** コマンドを使用して任意の IP マルチキャスト アドレス用の SSM も設定できます。SSM は、1 対多通信での効率的なデータ配信メカニズムを可能にする

Protocol Independent Multicast（PIM）の拡張版です。SSM については、IP マルチキャスト配信モード （505 ページ）の項を参照してください。

GLOP アドレス

GLOP アドレッシングでは（233/8 の RFC 2770、GLOP アドレッシングで提案されているように）、AS 番号をすでに予約している組織による静的に定義されたアドレス用に 233.0.0.0/8 の範囲を予約することを提案しています。これは、GLOP アドレッシングと呼ばれます。ドメインの AS 番号は 233.0.0.0/8 アドレス範囲の 2 番目と 3 番目のオクテットに組み込まれます。たとえば、AS 62010 は 16 進数形式で F23A と表されます。この 2 つのオクテット F2 および 3A を分割すると、結果は 10 進数でそれぞれ 242 および 58 となります。これらの値は、AS 62010 に使用するようにグローバルに予約される 233.242.58.0/24 のサブネットとなります。

限定スコープ アドレス

239.0.0.0 ～ 239.255.255.255 の範囲は、管理スコープ アドレス、またはプライベート マルチキャスト ドメインで使用する限定スコープ アドレスとして予約されています。これらのアドレスは、ローカル グループまたは組織に使用するように制限されています。会社、大学および他の組織は、限定スコープ アドレスを使用すると、ドメイン外に転送されないローカル マルチキャストアプリケーションを使用できます。通常、ルータは、このアドレス範囲のマルチキャスト トラフィックが自律システム（AS）またはユーザ定義のドメイン外にフローしないようにするフィルタを使用して設定されます。AS またはドメイン内では、ローカル マルチキャスト境界を定義できるように、限定スコープ アドレス範囲を細分化することもできます。

（注） ネットワーク管理者はこの範囲内のマルチキャストアドレスを使用できます。これによって、インターネット内の他の場所と競合することはありません。

レイヤ 2 マルチキャスト アドレス

従来、LAN セグメントのネットワーク インターフェイス カード（NIC）が受信できるのは、Burned-In MAC Address またはブロードキャスト MAC アドレスに指定されたパケットだけでした。IP マルチキャストでは、複数のホストが共通の宛先 MAC アドレスを使用した単一のデータ ストリームを受信する必要があります。複数のホストが同じパケットを受信する場合、複数のマルチキャスト グループを区別できるように、何らかの方法を考案する必要があります。そのための 1 つの方法は、IP マルチキャスト クラス D アドレスを MAC アドレスに直接マッピングすることです。この方法を使用すると、NIC は多くの異なる MAC アドレスを宛先とするパケットを受信できます。

Cisco グループ管理プロトコル（CGMP）は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたルータ上で使用されます。IP マルチキャスト データ パケットと IGMP レポート メッセージ（いずれも MAC レベルで同じグループ アドレスにアドレス指定されます）を区別できない Catalyst スイッチの場合、CGMP が必要になります。

IP マルチキャスト配信モード

IP マルチキャスト配信のモードは、送信元ホストではなく、受信側ホストのみによって異なります。送信元ホストは、パケットの IP 送信元アドレスとしての固有の IP アドレスと、パケットの IP 宛先アドレスとしてのグループ アドレスを使用して、IP マルチキャスト パケットを送信します。

Source Specific Multicast

Source Specific Multicast（SSM）は、ブロードキャスト アプリケーションとしても知られる 1 対多アプリケーションをサポートする最善のデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャストアプリケーション環境を対象としたシスコの IP マルチキャストのコア ネットワーク テクノロジーです。

SSM 配信モードの場合、IP マルチキャスト レシーバ ホストは IGMP バージョン3（IGMPv3）を使用してチャネル（S, G）を登録する必要があります。このチャネルに登録することによって、ソース ホストがグループ G に送信した IP マルチキャスト トラフィックの受信をレシーバ ホストが要求していることを示します。ネットワークは、ソース ホスト S からグループ G に送信された IP マルチキャスト パケットを、チャネル (S, G) に登録したネットワーク内のすべてのホストに配信します。

SSM では、ネットワーク内でグループ アドレスを割り当てる必要はありません。各ソース ホスト内で割り当てるだけです。同じソースホストで実行している各アプリケーションはそれぞれ異なる SSM グループを使用する必要があります。異なるソース ホストで実行しているアプリケーションは、SSM グループアドレスを再利用できます。ネットワークに大量のトラフィックを発生させることはありません。

第 28 章

IGMP の設定

- 機能情報の確認 （507 ページ）
- IGMP および IGMP スヌーピングの前提条件 （507 ページ）
- IGMP および IGMP スヌーピングの制約事項 （508 ページ）
- IGMP に関する情報 （510 ページ）
- IGMP の設定方法 （523 ページ）
- IGMP のモニタリング （568 ページ）
- IGMP の設定例 （571 ページ）
- その他の参考資料 （577 ページ）
- IGMP の機能履歴と情報 （578 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IGMP および IGMP スヌーピングの前提条件

IGMP のの前提条件

- このモジュールの作業を実行する前に、『IP Multicast Routing Technology Overview』モジュールで説明している概念をよく理解しておく必要があります。

- このモジュールの作業では、IP マルチキャストがイネーブルに設定され、「Configuring Basic IP Multicast Routing」モジュールで説明されている作業を使用して、Protocol Independent Multicast（PIM）インターフェイスが設定されていることを前提とします。

IGMP スヌーピングの前提条件

IGMP スヌーピング クエリアを設定するときには、次の注意事項を順守します。

- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。IGMP スヌーピング クエリアは、イネーブルの場合この IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN デバイス仮想インターフェイス（SVI）IP アドレス（存在する場合）の使用を試みます。SVI IP アドレスが存在しない場合、デバイスはデバイス上で設定された利用可能な最初の IP アドレスを使用します。利用可能な最初の IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。IGMP スヌーピング クエリアはデバイス上で利用可能な IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
- IGMP スヌーピング クエリアは IGMP バージョン 1 および 2 をサポートします。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアはネットワークにマルチキャスト ルータの存在を検出すると、非クエリア ステートになります。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアは操作上、次の状況でディセーブル ステートになります。
  - IGMP スヌーピングが VLAN でディセーブルの場合
  - PIM が、VLAN に対応する SVI でイネーブルの場合

IGMP および IGMP スヌーピングの制約事項

IGMP 設定の制約事項

次に、IGMP を設定する際の制約事項を示します。

- デバイスは、IGMP バージョン 1、2、および 3 をサポートします。

（注） IGMP バージョン 3 の場合、IGMP バージョン 3 BISS（基本的な IGMPv3 スヌーピング サポート）のみがサポートされます。

- IGMP バージョン 3 では新しいメンバーシップ レポート メッセージを使用しますが、これらは以前の IGMP スヌーピング デバイスが正しく認識しない可能性があります。
- IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、exclude と include の両方のモードのレポートを適用できます。SSM では、ラストホップ ルータは include モードのレポートだけを受け入れます。exclude モードのレポートは無視されます。
- IGMP フィルタリングおよびスロットリングは WLAN ではサポートされません。
- Catalyst 3850 および Catalyst 3650 デバイスの組み合わせを含むデバイス スタックを含めることはできません。

関連トピック

IGMP バージョンの変更（CLI） （528 ページ）
IGMP のバージョン （511 ページ）

IGMP スヌーピングの制約事項

次に、IGMP スヌーピングの制約事項を示します。

- デバイスは、宛先マルチキャスト IP アドレスのみに基づいて IGMPv3 スヌーピングをサポートします。送信元 IP アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。
- IGMP フィルタリングまたはマルチキャスト VLAN レジストレーション（MVR）が実行されているデバイスは、IGMPv3 Join および Leave メッセージをサポートしません。
- IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。
- IGMP の脱退時間の設定は、IGMP バージョン 2 が稼働しているホストでのみサポートされます。IGMP バージョン 2 はデバイスのデフォルト バージョンです。

  ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間を前後することがあります。
- IGMP スロットリング アクションの制約事項は、レイヤ 2 ポートにだけ適用されます。**ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドは論理 EtherChannel インターフェイスで使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups action {deny | replace}** コマンドを入力しても効果はありません。

インターフェイスによりマルチキャスト エントリが転送テーブルに追加されてから、スロットリング アクションを設定し、グループの最大数の制限を設定すると、転送テーブルのエントリは、スロットリング アクションに応じて期限切れになるか削除されます。

関連トピック

IGMP バージョンの変更（CLI） （528 ページ）
IGMP のバージョン （511 ページ）

IGMP に関する情報

Internet Group Management Protocol の役割

IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。インターフェイスで PIM をイネーブルにすると、IGMP もイネーブルになります。IGMP は、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャスト トラフィックのフローを自動的に制御および制限する手段を提供します。

- クエリアは、クエリー メッセージを送信して、特定のマルチキャスト グループのメンバであるネットワーク デバイスを検出するネットワーク デバイス（ルータなど）です。
- ホストは、クエリアにホスト メンバーシップを通知するためのレポート メッセージ（クエリー メッセージに応答するメッセージ）を送信するレシーバで、ルータも含まれます。ホストでは、IGMP メッセージを使用して、マルチキャスト グループに加入し、マルチキャスト グループを脱退します。

ホストは、そのローカル マルチキャスト デバイスに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、デバイスは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

IGMP マルチキャスト アドレス

IP マルチキャスト トラフィックには、グループ アドレス（クラス D IP アドレス）が使用されます。クラス D アドレスの上位 4 ビットは 1110 です。したがって、ホスト グループ アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 であると考えられます。

224.0.0.0 ～ 224.0.0.255 のマルチキャスト アドレスは、ルーティング プロトコルおよびその他のネットワーク制御トラフィックが使用するために予約されています。アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは IP マルチキャスト グループ アドレスを使用して次のように送信されます。

- IGMP 汎用クエリーは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリーは、クエリー対象デバイスのグループ IP アドレスを宛先とします。
- IGMP グループ メンバーシップ レポートは、レポート対象デバイスのグループ IP アドレスを宛先とします。
- IGMPv2 グループ脱退メッセージは、アドレス 224.0.0.2（サブネット上のすべてのデバイス）を宛先とします。
- IGMPv3 メンバーシップ レポートはアドレス 224.0.0.22 を宛先とします。すべての IGMPv3 対応マルチキャスト デバイスはこのアドレスをリッスンする必要があります。

関連トピック

グループのメンバとしてのデバイスの設定（CLI） （523 ページ）
例：マルチキャスト グループのメンバとしてのデバイスの設定 （571 ページ）

IGMP のバージョン

デバイスは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしています。これらのバージョンは、デバイス上で相互運用できます。たとえば、IGMP スヌーピングがイネーブルになっており、クエリーのバージョンが IGMPv2 で、デバイスがホストから IGMPv3 レポートを受信している場合、デバイスは IGMPv3 レポートをマルチキャスト ルータに転送できます。

IGMPv3 デバイスは、Source Specific Multicast（SSM）機能を実行しているデバイスとメッセージの送受信を行うことができます。

関連トピック

IGMP バージョンの変更（CLI） （528 ページ）
IGMP 設定の制約事項 （508 ページ）
IGMP スヌーピングの制約事項 （509 ページ）

IGMPv1

IGMP Version 1（IGMPv1）にはクエリー応答モデルが使用されているため、マルチキャスト ルータおよびマルチレイヤ デバイスは、ローカル サブネット上のどのマルチキャスト グループがアクティブであるか（マルチキャスト グループに関係するホストが 1 台または複数存在するか）を判別できます。IGMPv1 では別のプロセスを使用して、ホストをマルチキャスト グループに加入および脱退させることができます。詳細については、RFC 1112 を参照してください。

IGMPv2

IGMPv2 は IGMP 機能の拡張版です。IGMP 脱退処理などの機能を提供して、脱退遅延を短縮し、グループ固有のクエリー数を削減し、明示的な最大クエリー応答時間を短縮します。ま

た、この作業を実行するために、マルチキャスト プロトコルに依存することなく IGMP クエリアを選択する機能もルータに追加されます。詳細については、RFC 2236 を参照してください。

（注） IGMP バージョン 2 はデバイスのデフォルト バージョンです。

IGMP バージョン 3

デバイスは IGMP バージョン 3 をサポートしています。

IGMPv3 デバイスは、Basic IGMPv3 Snooping Support（BISS）をサポートしています。BISS は、IGMPv1 および IGMPv2 スイッチでのスヌーピング機能と、IGMPv3 メンバーシップ レポート メッセージをサポートしています。ネットワークに IGMPv3 ホストがある場合、BISS によりマルチキャスト トラフィックのフラッディングは抑制されます。トラフィックは、IGMPv2 または IGMPv1 ホストの IGMP スヌーピング機能の場合とほぼ同じポート セットに抑制されます。

IGMPv3 デバイスは、Source Specific Multicast（SSM）機能を実行しているデバイスとメッセージの送受信を行うことができます。

IGMPv3 ホスト シグナリング

IGMPv3 は、ホストがマルチキャスト グループのラスト ホップ デバイスにメンバーシップを伝える IETF 標準トラック プロトコルの第 3 バージョンです。IGMPv3 は、グループ メンバーシップを伝える能力をホストに与えます。これによってソースに関するフィルタリングが可能になります。ホストは、特定のソースを除いて、グループに送信するすべてのソースからトラフィックを受信したい（EXCLUDE と呼ばれるモード）、またはグループに送信する特定のソースからのみトラフィックを受信したい（INCLUDE と呼ばれるモード）と伝えることができます。

IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、EXCLUDE モードと INCLUDE モードの両方のレポートがラスト ホップ ルータによって受け入れられます。SSM では、INCLUDE モード レポートのみがラスト ホップ ルータによって受け入れられます。

IGMP のバージョンの違い

Internet Engineering Task Force（IETF）の Request for Comments（RFC）ドキュメントで定義されているように、IGMP には 3 種類のバージョンがあります。IGMPv2 は IGMPv1 の強化版で、ホストがマルチキャスト グループからの脱退を通知する機能が追加されていいます。IGMPv3 は IGMPv2 の強化版で、あるソース IP アドレスのセットから送信されたマルチキャストだけをリッスンする機能が追加されています。

表 *32 : IGMP* のバージョン

IGMP Version	説明
IGMPv1	どのマルチキャスト グループがアクティブであるかをマルチキャストデバイスが判断できる基本的なクエリー応答メカニズムと、ホストがマルチキャスト グループに加入および脱退できるようにするためのその他のプロセスを提供します。RFC 1112 で、IP マルチキャスト用の IGMPv1 ホスト拡張が定義されています。
IGMPv2	IGMP の拡張で、IGMP の脱退処理、グループ固有のクエリーおよび明示的な最大応答時間フィールドなどの機能が可能になっています。また、IGMPv2 ではこの作業を実行するために、マルチキャスト プロトコルに依存することなく IGMP クエリアを選択する機能もデバイスに追加されます。IGMPv2 は RFC 2236 で定義されています。

（注） デフォルトでは、インターフェイスで PIM をイネーブルにすると、そのデバイスで IGMPv2 がイネーブルになります。IGMPv2 は、可能な限り IGMPv1 と下位互換性を保つよう設計されました。この下位互換性を実現するために、RFC 2236 は特別な相互運用性ルールを定義しています。ネットワークにレガシー IGMPv1 ホストが含まれている場合は、これらの運用性ルールをよく知っておく必要があります。IGMPv1 と IGMPv2 の相互運用性の詳細については、RFC 2236『Internet Group Management Protocol, Version 2』を参照してください。

IGMPv1 を実行するデバイス

IGMPv1 デバイスは、「全ホスト」へのマルチキャスト アドレスである 224.0.0.1 に IGMP クエリーを送信して、アクティブ マルチキャスト レシーバが存在するマルチキャスト グループを求めます。マルチキャスト レシーバも、デバイスに IGMP レポートを送信して、特定のマルチキャスト ストリームの受信を待機していることを通知できます。ホストは非同期に、またはデバイスによって送信される IGMP クエリーに対応して、レポートを送信できます。同じマルチキャスト グループに複数のマルチキャスト レシーバが存在する場合、これらのホストの 1 つのみで、IGMP レポート メッセージが送信されます。他のホストでは、レポート メッセージが抑制されます。

IGMPv1 では、IGMP クエリア選択はありません。セグメント内に複数のデバイスがある場合、すべてのデバイスが定期的に IGMP クエリーを送信します。IGMPv1 には、ホストがグループから脱退できる特別なメカニズムはありません。ホストで、特定のグループに対するマルチキャスト パケットを受信する必要がなくなった場合は、デバイスから送信される IGMP クエリー パケットに対する応答を行わないだけです。デバイスはクエリー パケットを送信し続けます。デバイスが 3 回 IGMP クエリーの応答を受信しないと、グループはタイムアウトし、デバイスはグループのセグメントへのマルチキャスト パケットの送信を停止します。ホストがタイムアウト期間後にマルチキャスト パケットを受信する場合、そのホストは新しい IGMP join

をデバイスに送信するだけです。これにより、デバイスはマルチキャスト パケットの転送を再開します。

LAN 上に複数のデバイスが存在する場合は、指定ルータ（DR）を選択して、接続されているホストに対するマルチキャスト トラフィックの重複を回避する必要があります。PIM デバイスは DR を選択する選定プロセスに従います。最も大きい IP アドレスを持つ PIM デバイスが DR になります。

DR は、次のタスクを担当します。

- PIM 登録メッセージ、PIM 加入メッセージ、および PIM プルーニング メッセージをランデブー ポイント（RP）に送信し、ホスト グループ メンバーシップに関する情報を通知する。
- IGMP ホスト クエリー メッセージを送信する。
- IGMP オーバーヘッドをホストおよびネットワークでできるだけ低く維持するために、ホスト クエリー メッセージをデフォルトで 60 秒ごとに送信する。

IGMPv2 を実行するデバイス

IGMPv2 では、IGMPv1 のクエリー メッセージング機能が改善されました。

IGMPv2 のクエリーおよびメンバーシップ レポート メッセージは、次の 2 つの例外を除き、IGMPv1 メッセージと同じです。

- IGMPv2 クエリー メッセージは、一般クエリー（IGMPv1 クエリーと同じ）とグループ固有クエリーの 2 つのカテゴリに分かれる。
- IGMPv1 メンバーシップ レポートと IGMPv2 メンバーシップ レポートの IGMP タイプ コードが異なる。

IGMPv2 では、次の機能に対するサポートを追加することにより、IGMP の機能の強化も行われました。

- クエリア選択プロセス：IGMPv2 デバイスが、プロセスを実行するマルチキャスト ルーティング プロトコルに依存せずに、IGMP クエリアを選択できる機能を提供します。
- [Maximum Response Time] フィールド：IGMP クエリアを使用して最大クエリー応答時間を指定できる、クエリー メッセージの新しいフィールド。このフィールドで、応答のバースト性を制御し、脱退遅延を調整するクエリー応答プロセスの調整ができます。
- グループ固有クエリー メッセージ：すべてのグループではなく特定の 1 つのグループでクエリー操作を実行する目的で、IGMP クエリアを使用することができます。
- グループ脱退メッセージ：グループから脱退することをネットワーク上のデバイスに通知する手段をホストに提供します。

DR と IGMP クエリアが通常同じデバイスである IGMPv1 とは異なり、IGMPv2 では 2 つの機能は分離されます。DR と IGMP クエリアは異なる基準で選択され、同じサブネット上の異な

るデバイスである場合があります。DR はサブネットで IP アドレスが最大のデバイスで、IGMP クエリアは最小の IP アドレスを持つデバイスです。

次のように、クエリー メッセージは IGMP クエリアの選択に使用されます。

1. 各 IGMPv2 デバイスは起動時に、そのインターフェイス アドレスを一般クエリー メッセージのソース IP アドレス フィールドに使用して、当該メッセージを全システムのグループ アドレス 224.0.0.1 にマルチキャスト送信します。
2. IGMPv2 デバイスが一般クエリー メッセージを受信すると、デバイスは自分のインターフェイス アドレスとメッセージのソース IP アドレスを比較します。サブネット上の最下位 IP アドレスが使用されているデバイスにより、IGMP クエリアが選択されます。
3. すべてのデバイス（クエリアは除く）でクエリー タイマーが開始されます。IGMP クエリアから一般クエリー メッセージを受信するたびに、タイマーはリセットされます。クエリー タイマーが切れると、IGMP クエリアがダウンしたと見なされ、新しい IGMP クエリアを選択するために選択プロセスが再度実行されます。

デフォルトでは、タイマーはクエリー インターバルの 2 倍です。

IGMP の加入および脱退処理

IGMP の加入処理

ホストがマルチキャスト グループに加入するとき、ホストは、加入するマルチキャスト グループに 1 つ以上の送信要求されていないメンバーシップ レポートを送信します。IGMP 加入処理は、IGMPv1 ホストと IGMPv2 ホストで同じです。

IGMPv3 では、ホストの加入処理は次のように処理されます。

- ホストがグループに加入する場合は、空の EXCLUDE リストを使用して、224.0.0.22 に IGMPv3 メンバーシップ レポートを送信します。
- ホストが特定のチャネルに加入する場合は、特定のソース アドレスを含む INCLUDE リストを使用して、224.0.0.22 に IGMPv3 メンバーシップ レポートを送信します。
- ホストが特定のソースを除くグループに加入する場合は、これらのソースを EXCLUDE リストで除外して、224.0.0.22 に IGMPv3 メンバーシップ レポートを送信します。

（注） LAN 上にある一部の IGMPv3 ホストでソースが除外され、その他のホストで同じソースが含まれている場合、デバイスは LAN 上でそのソースのトラフィックを送信します（つまり、この場合、包含が除外より優先されます）。

IGMP の脱退処理

ホストがグループから脱退するために使用する方法は、動作中の IGMP のバージョンによって異なります。

IGMPv1 の脱退処理

IGMPv1には、ホストがあるグループからのマルチキャストトラフィックを受信しないことをそのサブネットのデバイスに通知するグループ脱退メッセージはありません。ホストでは、マルチキャストグループに対するトラフィックの処理が停止するだけで、そのグループに対するIGMP メンバーシップ レポートを使用したIGMP クエリーへの応答が終了します。その結果、IGMPv1デバイスがサブネットの特定のマルチキャストグループにアクティブなレシーバがなくなったことを認識する唯一の方法は、デバイスがメンバーシップ レポートを受信しなくなったときになります。このプロセスを容易にするために、IGMPv1 デバイスは、サブネットのIGMP グループとカウントダウンタイマーを関連付けます。サブネットのグループがメンバーシップ レポートを受信すると、タイマーがリセットされます。IGMPv1デバイスでは、このタイム アウト間隔は通常クエリー間隔の3倍（3分）です。このタイムアウト間隔は、すべてのホストがマルチキャストグループから脱退した後最大3分間、デバイスがサブネットにマルチキャスト トラフィックを転送し続ける可能性があることを意味します。

IGMPv2 の脱退処理

IGMPv2には、特定のグループのマルチキャストトラフィックの受信を停止することをホストが提示する手段を提供するグループ脱退メッセージが組み込まれています。IGMPv2 ホストがマルチキャスト グループから脱退するとき、そのホストがそのグループのメンバーシップ レポートでクエリーに応答する最後のホストである場合、デバイス全体のマルチキャストグループ（224.0.0.2）にグループ脱退メッセージを送信します。

IGMPv3 の脱退処理

IGMPv3 は、IGMPv3 メンバーシップ レポートにソース、グループ、またはチャネルを含めるか除外することによって、ホストが特定のグループ、ソース、またはチャネルからのトラフィックの受信を停止できる機能を導入することで、脱退処理を拡張しています。

IGMP スヌーピング

レイヤ2デバイスはIGMP スヌーピングを使用して、レイヤ2インターフェイスを動的に設定し、マルチキャスト トラフィックがIP マルチキャスト デバイスと対応付けられたインターフェイスにのみ転送されるようにすることによって、マルチキャスト トラフィックのフラッディングを制限できます。名称が示すとおり、IGMPスヌーピングの場合は、LANデバイスでホストとルータ間の IGMP 伝送をスヌーピングし、マルチキャスト グループとメンバ ポートを追跡する必要があります。特定のマルチキャストグループについて、デバイスがホストからIGMP レポートを受信すると、そのデバイスはホストのポート番号を転送テーブルエントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブル エントリからホスト ポートを削除します。マルチキャスト クライアントから IGMP メンバーシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。

（注） IP マルチキャストおよびIGMP の詳細については、RFC 1112 およびRFC 2236 を参照してください。

マルチキャストルータ（アクティブなデバイスのIPサービス機能のあるデバイスを含む）は、すべての VLAN に一般的なクエリーを定期的に送信します。このマルチキャスト トラフィックに関心のあるホストはすべてJoin要求を送信し、転送テーブルのエントリに追加されます。デバイスは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ごとに 1 つずつエントリを作成します。

デバイスは、MAC アドレスに基づくグループではなく、IP マルチキャスト グループに基づくブリッジングをサポートしています。マルチキャスト MAC アドレスに基づくグループの場合、設定されているIPアドレスを設定済みのMACアドレス（エイリアス）または予約済みのマルチキャスト MAC アドレス（224.0.0.xxx の範囲内）に変換すると、コマンドがエラーになります。デバイスでは IP マルチキャスト グループを使用するので、アドレス エイリアスの問題は発生しません。

IGMP スヌーピングによって、IP マルチキャスト グループは動的に学習されます。ただし、**ip igmp snooping vlan** *vlan-id* **static** *ip_address***interface** *interface-id* グローバル コンフィギュレーション コマンドを使用すると、マルチキャスト グループを静的に設定できます。グループ メンバーシップをマルチキャスト グループ アドレスに静的に指定すると、その設定値は IGMP スヌーピングによる自動操作より優先されます。マルチキャスト グループ メンバーシップのリストは、ユーザが定義した設定値およびIGMPスヌーピングによって学習された設定値の両方で構成できます。

マルチキャストトラフィックはルーティングする必要がないのでマルチキャストインターフェイスを使用せずに、サブネットの IGMP スヌーピングをサポートするよう IGMP スヌーピング クエリーを設定できます。

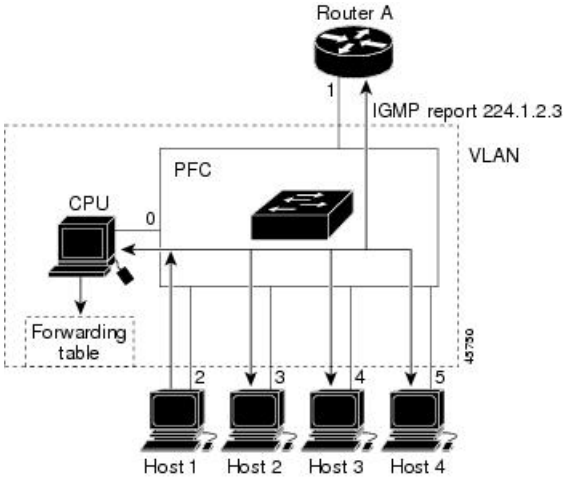
ポート スパニングツリー、ポート グループ、または VLAN ID が変更された場合、VLAN 上のこのポートから IGMP スヌーピングで学習されたマルチキャスト グループは削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

マルチキャスト グループへの加入

図 *22 :* 最初の *IGMP Join* メッセージ

デバイスに接続したホストが IP マルチキャスト グループに加入し、なおかつそのホストが IGMP バージョン 2 クライアントの場合、ホストは加入する IP マルチキャスト グループを指定した非送信請求 IGMP Join メッセージを送信します。別の方法として、ルータから一般クエリーを受信したデバイスは、そのクエリーを VLAN 内のすべてのポートに転送します。IGMP バージョン 1 またはバージョン 2 のホストがマルチキャスト グループに加入する場合、ホストはデバイスに Join メッセージを送信することによって応答します。デバイスの CPU は、そのグループのマルチキャスト転送テーブルエントリがまだ存在していないのであれば、エントリを作成します。CPU はさらに、Join メッセージを受信したインターフェイスを転送テーブルエントリに追加します。そのインターフェイスと対応付けられたホストが、そのマルチキャスト グループ用のマルチキャスト トラフィックを受信します。



ルータ A がデバイスに一般クエリーを送信し、スイッチがそのクエリーを同じ VLAN のすべてのメンバであるポート 2 ～ 5 に転送します。ホスト 1 はマルチキャスト グループ 224.1.2.3 に加入するために、グループに IGMP メンバーシップ レポート（IGMP Join メッセージ）をマルチキャストします。デバイスの CPU は IGMP レポートの情報を使用して、転送テーブルのエントリを設定します。転送テーブルにはホスト 1 およびルータに接続しているポート番号が含まれます。

表 *33 : IGMP* スヌーピング転送テーブル

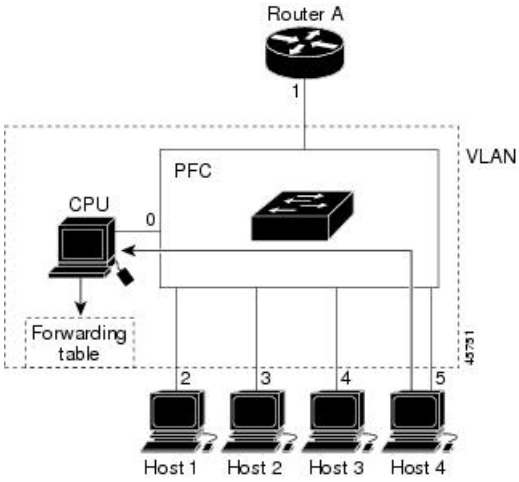
Destination Address	パケットのタイプ	ポート
224.1.2.3	IGMP	1、2

デバイスのハードウェアは、IGMP 情報パケットをマルチキャスト グループの他のパケットと区別できます。テーブルの情報は、224.1.2.3 マルチキャスト IP アドレス宛ての、IGMP パケットではないフレームを、ルータおよびグループに加入したホストに対して送信するように、スイッチング エンジンに指示します。

図 *23 : 2* 番目のホストのマルチキャスト グループへの加入

別のホスト（たとえば、ホスト 4）が、同じグループ用に非送信請求 IGMP Join メッセージを送信する場合、CPU がそのメッセージを受け取り、ホスト 4 のポート番号を転送テーブルに追加します。転送テーブルは CPU 宛てだけに IGMP メッセージを送るので、メッセージはデバ

イスの他のポートへフラッディングされません。認識されているマルチキャスト トラフィック



は、CPU宛てではなくグループ宛てに転送されます。

表 *34*：更新された *IGMP* スヌーピング転送テーブル

Destination Address	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2, 5

関連トピック

グループのメンバとしてのデバイスの設定（CLI） （523 ページ）
例：マルチキャスト グループのメンバとしてのデバイスの設定 （571 ページ）

マルチキャスト グループからの脱退

ルータは定期的にマルチキャスト一般クエリーを送信し、デバイスはそれらのクエリーをVLAN内のすべてのポート経由で転送します。関心のあるホストがクエリーに応答します。VLAN内の少なくとも1つのホストがマルチキャスト トラフィックを受信するようなら、ルータは、その VLAN へのマルチキャスト トラフィックの転送を続行します。デバイスは、その IGMP スヌーピングによって維持された IP マルチキャスト グループの転送テーブルで指定されたホストに対してだけ、マルチキャスト グループ トラフィックを転送します。

ホストがマルチキャスト グループから脱退する場合、何も通知せずに脱退することも、Leave メッセージを送信することもできます。ホストから Leave メッセージを受信したデバイスは、グループ固有のクエリーを送信して、そのインターフェイスに接続された他のデバイスが所定のマルチキャストグループのトラフィックに関与しているかどうかを学習します。デバイスはさらに、転送テーブルでその MAC グループの情報を更新し、そのグループのマルチキャスト トラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。ルータがVLANからレポートを受信しなかった場合、そのVLAN用のグループはIGMPキャッシュから削除されます。

即時脱退

デバイスはIGMPスヌーピングの即時脱退を使用して、先にデバイスからインターフェイスにグループ固有のクエリーを送信しなくても、Leave メッセージを送信するインターフェイスを

転送テーブルから削除できるようにします。VLAN インターフェイスは、最初の Leave メッセージで指定されたマルチキャスト グループのマルチキャスト ツリーからプルーニングされます。即時脱退によって、複数のマルチキャスト グループが同時に使用されている場合でも、スイッチド ネットワークのすべてのホストに最適な帯域幅管理が保証されます。

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。IGMP バージョン 2 はデバイスのデフォルト バージョンです。

（注） 即時脱退機能を使用するのは、各ポートに接続されているホストが 1 つだけの VLAN に限定してください。ポートに複数のホストが接続されている VLAN 上で即時脱退をイネーブルにすると、一部のホストが誤ってドロップされる可能性があります。

関連トピック

IGMP 即時脱退のイネーブル化（CLI） （555 ページ）

IGMP 設定可能脱退タイマー

特定のマルチキャスト グループへの参加がまだ必要かどうかを確認するために、グループ固有のクエリーを送信した後のデバイスの待機時間を設定できます。IGMP 脱退応答時間は、100 ～ 32767 ミリ秒の間で設定できます。

関連トピック

IGMP 脱退タイマーの設定（CLI） （556 ページ）

IGMP レポート抑制

（注） IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

デバイス は IGMP レポート抑制を使用して、1 つのマルチキャスト ルータ クエリごとに 1 つの IGMP レポートのみをマルチキャスト デバイスに転送します。IGMP レポート抑制がイネーブル（デフォルト）である場合、デバイスは最初の IGMP レポートをグループのすべてのホストからすべてのマルチキャスト ルータに送信します。デバイス は、グループの残りの IGMP レポートをマルチキャスト ルータに送信しません。この機能により、マルチキャスト デバイスにレポートが重複して送信されることを防ぎます。

マルチキャスト ルータ クエリに IGMPv1 および IGMPv2 レポートに対する要求だけが含まれている場合、デバイスは最初の IGMPv1 レポートまたは IGMPv2 レポートだけを、グループのすべてのホストからすべてのマルチキャスト ルータに送信します。

マルチキャスト ルータ クエリに IGMPv3 レポートに対する要求も含まれる場合、デバイス は グループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送します。

IGMP レポート抑制をディセーブルにすると、すべての IGMP レポートはマルチキャスト ルータに転送されます。

関連トピック

IGMP レポート抑制のディセーブル化（CLI）（567 ページ）

IGMP スヌーピングとデバイス スタック

IGMP スヌーピング機能はデバイス スタック間で機能します。つまり、1 つのデバイスからの IGMP 制御情報は、スタック内のすべてのデバイスに配信されますスタック メンバが、どの IGMP マルチキャスト データ経由でスタックに入ったかに関係なく、データは、そのグループで登録されたホストに到達します。

スタック内のデバイスに障害が発生した、またはスタックから削除された場合、そのデバイス上にあるマルチキャスト グループのメンバのみが、マルチキャスト データを受信しません。スタック内のその他のデバイス上のマルチキャスト グループの他のすべてのメンバでは、マルチキャスト データ ストリームを継続して受信します。ただし、アクティブなデバイスが削除された場合、レイヤ 2 およびレイヤ 3（IP マルチキャスト ルーティング）の両方に共通のマルチキャスト グループでは、収束するために、より長い時間を要する場合があります。

IGMP フィルタリングおよびスロットリング

都市部や集合住宅（MDU）などの環境では、デバイス ポート上のユーザが属する一連のマルチキャスト グループを制御する必要があります。この機能を使用することにより、IP/TV などのマルチキャスト サービスの配信を、特定タイプの契約またはサービス計画に基づいて制御できます。また、マルチキャスト グループの数を、デバイス ポート上でユーザが所属できる数に制限することもできます。

IGMP フィルタリング機能を使用すると、IP マルチキャスト プロファイルを設定し、それらを各デバイス ポートに関連付けて、ポート単位でマルチキャスト加入をフィルタリングできます。IGMP プロファイルにはマルチキャスト グループを 1 つまたは複数格納して、グループへのアクセスを許可するか拒否するかを指定できます。マルチキャスト グループへのアクセスを拒否する IGMP プロファイルがデバイス ポートに適用されると、IP マルチキャスト トラフィックのストリームを要求する IGMP Join レポートが廃棄され、ポートはそのグループからの IP マルチキャスト トラフィックを受信できなくなります。マルチキャスト グループへのアクセスがフィルタリング アクションで許可されている場合は、ポートからの IGMP レポートが転送されて、通常の処理が行われます。レイヤ 2 インターフェイスが加入できる IGMP グループの最大数も設定できます。

IGMP フィルタリングで制御されるのは、グループ固有のクエリーおよびメンバーシップ レポート（Join および Leave レポートを含む）だけです。一般 IGMP クエリーは制御されません。IGMP フィルタリングは、IP マルチキャスト トラフィックの転送を指示する機能とは無関係です。フィルタリング機能は、マルチキャスト トラフィックの転送に CGMP が使用されているか、または MVR が使用されているかに関係なく、同じように動作します。

IGMP フィルタリングが適用されるのは、IP マルチキャスト グループ アドレスを動的に学習する場合だけです。静的な設定には適用されません。

IGMP スロットリング機能を使用すると、レイヤ2インターフェイスが加入できる IGMP グループの最大数を設定できます。IGMP グループの最大数が設定され、IGMP スヌーピング転送テーブルに最大数のエントリが登録されていて、インターフェイスで IGMP Join レポートを受信する場合、インターフェイスを設定することにより、IGMP レポートを廃棄するか、あるいは受信した IGMP レポートでランダムに選択されたマルチキャスト エントリを上書きします。

（注） IGMP フィルタリングが実行されているデバイスは、IGMPv3 Join および Leave メッセージをサポートしていません。

IGMP のデフォルト設定

次の表に、デバイス の IGMP のデフォルト設定を示します。

表 *35 : IGMP* のデフォルト設定

機能	デフォルト設定
マルチキャスト グループのメンバとしてのマルチレイヤ デバイス	グループ メンバーシップは未定義
マルチキャスト グループへのアクセス	インターフェイスのすべてのグループを許可
IGMP のバージョン	すべてのインターフェイスでバージョン 2
IGMP ホストクエリー メッセージ インターバル	すべてのインターフェイスで 60 秒
IGMP クエリー タイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒
静的に接続されたメンバとしてのマルチレイヤ デバイス	ディセーブル

IGMP スヌーピングのデフォルト設定

次の表に、デバイスの IGMP スヌーピングのデフォルト設定を示します。

表 *36 : IGMP* スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位でイネーブル
マルチキャスト ルータ	未設定
IGMP スヌーピング即時脱退	ディセーブル

機能	デフォルト設定
スタティック グループ	未設定
TCN[1]フラッド クエリ カウント	2
TCN クエリー送信要求	ディセーブル
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	イネーブル

[1] (1) TCN = トポロジ変更通知

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

次の表に、デバイスの IGMP フィルタリングおよびスロットリングのデフォルト設定を示します。

表 *37 : IGMP* フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用なし
IGMP グループの最大数	最大数の設定なし （注） 転送テーブルに登録されているグループが最大数に達していると、デフォルトの IGMP スロットリング アクションは IGMP レポートを拒否します。
IGMP プロファイル	未定義
IGMP プロファイル アクション	範囲で示されたアドレスを拒否

IGMP の設定方法

グループのメンバとしてのデバイスの設定（CLI）

デバイスをマルチキャスト グループのメンバとして設定し、マルチキャストがネットワークに到達可能かどうかを検出できます。管理しているすべてのマルチキャスト対応ルータおよびマルチレイヤ デバイスがマルチキャスト グループのメンバである場合、グループに ping を送信すると、これらのすべてのデバイスが応答します。デバイスは、所属グループにアドレス指定

されたICMPエコー要求パケットに応答します。もう1つの例は、ソフトウェア付属のマルチキャスト トレースルート ツールです。

⚠

注意 この手順を実行すると、グループ アドレス用のデータ トラフィックがすべてCPUに送られるため、CPUのパフォーマンスが低下する場合があります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ3インターフェイスを指定し、インターフェイスコンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ3ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスのIP PIMスパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスをIGMPスタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成されたVLANインターフェイスです。また、VLAN

	コマンドまたはアクション	目的
		上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp join-group** *group-address* 例： `Device(config-if)# ip igmp join-group 225.2.2.2`	デバイスをマルチキャスト グループに参加するように設定します。 デフォルトで、グループのメンバーシップは定義されていません。 *group-address* には、マルチキャスト IP アドレスをドット付き 10 進表記で指定します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

マルチキャスト グループへの加入 （517 ページ）
例：マルチキャスト グループのメンバとしてのデバイスの設定 （571 ページ）
IGMP マルチキャスト アドレス （510 ページ）

IP マルチキャスト グループへのアクセスの制御（CLI）

デバイス は IGMP ホストクエリ メッセージを送信し、接続されたローカル ネットワーク上のメンバーが属しているマルチキャスト グループを判別します。次に、デバイスは、マルチキャスト グループにアドレス指定されたすべてのパケットをこれらのグループ メンバーに転送します。インターフェイスごとにフィルタを適用し、インターフェイスで処理されるサブネット上のホストが加入可能なマルチキャスト グループを制限できます。

インターフェイスで参加数を制限するには、IGMP プロファイルと関連付けるフィルタ用のポートを設定します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**ip igmp profile**
	例：
	`Device(config)# ip igmp profile 10`
	`Device(config-igmp-profile)# ?`
		1 ～ 4294967295 の範囲で、IGMP フィルタ プロファイル番号を入力します。
		IGMP フィルタ プロファイルの設定の詳細については、IGMP プロファイルの設定（CLI）（537 ページ）を参照してください。

ステップ 4	**permit** 例： `Device(config-igmp-profile)# permit 229.9.9.0`	IGMP プロファイル設定操作を開始します。次の IGMP プロファイル設定操作がサポートされています。 • **deny**：一致する IP アドレスが拒否されます。 • **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。 • **no**：コマンドを無効にするか、そのデフォルトに設定します。

	コマンドまたはアクション	目的
		• **permit**：一致するアドレスが許可されます。 • **range**：設定に範囲を追加します。
ステップ 5	**exit** 例： `Device(config-igmp-profile)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip igmp filter** *filter_number* 例： `Device(config-if)# ip igmp filter 10`	IGMP フィルタ プロファイル番号を指定します。 IGMP フィルタ プロファイルの適用の詳細については、IGMP プロファイルの適用（CLI）（539ページ）を参照してください。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP バージョンの変更（CLI）

スイッチでは、IGMP クエリータイムアウトや最大クエリー応答時間などの機能を使用できる IGMP バージョン 2 がデフォルトで使用されます。

サブネット上のすべてのシステムで、同じバージョンをサポートする必要があります。スイッチは自動的にバージョン 1 のシステムを検出せず、バージョン 1 へのスイッチングも行いません。バージョン 2 のルータまたはスイッチは、常に IGMPv1 ホストと正しく連動しているため、バージョン 1 とバージョン 2 のホストはサブネット上で混在できます。

使用しているホストでバージョン 2 がサポートされていない場合は、スイッチをバージョン 1 に設定してください。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip igmp version** {**1** | **2** | **3** } 例： `Device(config-if)# ip igmp version 2`	スイッチで使用する IGMP バージョンを指定します。 （注） バージョン 1 に変更すると、**ip igmp query-interval** または **ip igmp query-max-response-time** インターフェイス コンフィギュレーション コマンドを設定できません。

	コマンドまたはアクション	目的
		デフォルトの設定に戻すには、 **no ip igmp version** インターフェイス コンフィギュレーションコマンドを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP のバージョン （511 ページ）
IGMP 設定の制約事項 （508 ページ）
IGMP スヌーピングの制約事項 （509 ページ）

IGMP ホストクエリー メッセージ インターバルの変更（CLI）

デバイスは、IGMP ホストクエリー メッセージを定期的に送信し、接続されたネットワーク上にあるマルチキャスト グループを検出します。これらのメッセージは、TTL が 1 の全ホスト マルチキャスト グループ（224.0.0.1）に送信されます。デバイスはホストクエリー メッセージを送信し、ネットワーク上に存在するメンバーシップに関する情報をリフレッシュします。クエリーをいくつか実行したあとで、マルチキャスト グループのメンバーであるローカルホストが存在しないことをソフトウェアが検出した場合、そのグループのリモート送信元からローカル ネットワークへのマルチキャスト パケット転送が停止され、プルーニング メッセージが送信元のアップストリーム方向へ送信されます。

デバイスは LAN（サブネット）用の PIM DR を選択します。DR は、LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。SM の場合、DR は PIM 登録メッセージおよび PIM Join メッセージも RP ルータに向けて送信します。IGMPv2 では、DR は IP アドレスが最大である、ルータまたはマルチレイヤデバイスです。IGMPv1 では、DR は LAN 上で動作するマルチキャスト ルーティング プロトコルに従って選択されます。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ3インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。

	コマンドまたはアクション	目的
		これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp query-interval** *seconds* 例： `Device(config-if)# ip igmp query-interval 75`	DR が IGMP ホストクエリー メッセージを送信する頻度を設定します。 デフォルトでは、DR は IGMP ホストクエリー メッセージを 60 秒ごとに送信し、ホストおよびネットワークでの IGMP オーバーヘッドを抑制します。 指定できる範囲は 1 ～ 65535 です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMPv2 の IGMP クエリー タイムアウトの変更（CLI）

IGMPv2 を使用している場合、デバイスがインターフェイスのクエリアとして引き継ぐまでの時間を指定できます。デフォルトでは、デバイスは **ip igmp query-interval** インターフェイス コンフィギュレーション コマンドによって制御されるクエリー インターバルの 2 倍の時間だけ待機します。この時間を経過しても、デバイスがクエリーを受信しない場合は、スイッチがクエリアになります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ3インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。

	コマンドまたはアクション	目的
		これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp querier-timeout** *seconds* 例： `Device(config-if)# ip igmp querier-timeout 120`	IGMP クエリータイムアウトを指定します。 デフォルトは 60 秒です（クエリー インターバルの 2 倍）。指定できる範囲は 60 ～ 300 です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMPv2 の最大クエリー応答時間の変更（CLI）

IGMPv2 を使用している場合は、IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更できます。デバイスは最大クエリー応答時間を使用し、LAN 上に直接接続されたグループ メンバが存在しないことを短時間で検出します。値を小さくすると、デバイスによるグループのプルーニング速度が向上します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ3インターフェイスを指定し、インターフェイスコンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp query-max-response-time** *seconds* 例： `Device(config-if)# ip igmp`	IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更します。 デフォルトは 10 秒です。指定できる範囲は 1 ～ 25 秒です。

	コマンドまたはアクション	目的
	query-max-response-time 15	
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

静的に接続されたメンバとしてのデバイスの設定（CLI）

ネットワーク セグメント上にグループ メンバが存在しなかったり、ホストで IGMP を使用してグループ メンバーシップを報告できないことがあります。しかし、そのネットワーク セグメントに対して、マルチキャスト トラフィックの送信が必要な場合もあります。マルチキャスト トラフィックをネットワーク セグメントに送り込むには、次のコマンドを使用します。

- **ip igmp join-group**：デバイス はマルチキャスト パケットの転送だけでなく、マルチキャスト パケットを受け入れます。マルチキャスト パケットを受信すると、デバイスは高速スイッチングを実行できません。
- **ip igmp static-group**：デバイス は、パケットを転送するだけで、パケット自体は受け入れません。この方法を使用すると、高速スイッチングが可能です。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャスト ルート エントリに「L」（ローカル）フラグが付かないことからも明らかなように、デバイス自体はメンバではありません。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ3インターフェイスを指定し、インターフェイスコンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp static-group** *group-address* 例：	デバイスを静的に接続されたグループのメンバとして設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip igmp static-group 239.100.100.101`	デフォルトでは、この機能はディセーブルになっています。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP プロファイルの設定（CLI）

IGMP プロファイルを作成するには、次の手順を実行します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip igmp profile** *profile number* 例： `Device(config)# ip igmp profile 3`	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。指定できるプロファイル番号の範囲は 1 ～ 4294967295 です。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。 • **deny**：一致するアドレスを拒否します。デフォルトで設定されています。 • **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。 • **no**：コマンドを否定するか、または設定をデフォルトに戻します。 • **permit**：一致するアドレスを許可するように指定します。 • **range**：プロファイルの IP アドレスの範囲を指定します。単一の IP アドレス、または開始アドレスと終了アドレスで指定された IP アドレス範囲を入力できます。 デフォルトでは、デバイスには IGMP プロファイルが設定されていません。 （注） プロファイルを削除するには、**no ip igmp profile** *profile number* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**permit** | **deny** 例： `Device(config-igmp-profile)# permit`	（任意）IP マルチキャスト アドレスへのアクセスを許可または拒否するアクションを設定します。アクションを設定しないと、プロファイルのデフォルト設定はアクセス拒否になります。
ステップ 5	**range** *ip multicast address* 例：	アクセスを制御する IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を入力します。範囲を入力す

	コマンドまたはアクション	目的
	`Device(config-igmp-profile)# range 229.9.9.0`	る場合は、IP マルチキャスト アドレスの下限値、スペースを 1 つ、IP マルチキャスト アドレスの上限値を入力します。 **range** コマンドを複数回入力すると、複数のアドレスまたはアドレス範囲を入力できます。 （注） IP マルチキャスト アドレスまたはIPマルチキャスト アドレス範囲を削除するには、**no range** *ip multicast address* IGMP プロファイル コンフィギュレーション コマンドを使用します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip igmp profile** *profile number* 例： `Device# show ip igmp profile 3`	プロファイルの設定を確認します。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP プロファイルの適用（CLI）

IGMP プロファイルで定義されているとおりにアクセスを制御するには、プロファイルを該当するインターフェイスに適用する必要があります。IGMP プロファイルを適用できるのは、レ

イヤ 2 アクセス ポートだけです。ルーテッド ポートや SVI には適用できません。EtherChannel ポート グループに所属するポートに、プロファイルを適用することはできません。1 つのプロファイルを複数のインターフェイスに適用できますが、1 つのインターフェイスに適用できるプロファイルは 1 つだけです。

スイッチ ポートに IGMP プロファイルを適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属していないレイヤ 2 ポートでなければなりません。
ステップ 4	**ip igmp filter** *profile number* 例： `Device(config-if)# ip igmp filter 321`	インターフェイスに指定された IGMP プロファイルを適用します。指定できる範囲は 1 ～ 4294967295 です。 （注） インターフェイスからプロファイルを削除するには、**no ip igmp filter** *profile number* インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP グループの最大数の設定（CLI）

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定するには、次の手順を実行します。

始める前に

この制限が適用されるのはレイヤ 2 ポートだけです。ルーテッド ポートや SVI には IGMP グループの最大数を設定できません。このコマンドは、論理 EtherChannel インターフェイスでも使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または

	コマンドまたはアクション	目的
		EtherChannel インターフェイスのいずれかにできます。
ステップ 4	**ip igmp max-groups** *number* 例： `Device(config-if)# ip igmp max-groups 20`	インターフェイスが加入できる IGMP グループの最大数を設定します。指定できる範囲は 0 ～ 4294967294 です。デフォルトでは最大数は設定されません。 （注） デバイスはレイヤ 2 IGMP グループの最大数（4096）とレイヤ 3 IGMP グループの最大数（2048）をサポートします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP スロットリング アクションの設定（CLI）

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定した後、受信した IGMP レポートの新しいグループで、既存のグループを上書きするようにインターフェイスを設定できます。

転送テーブルに最大数のエントリが登録されているときにスロットリングアクションを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定する物理インターフェイスを指定し、インターフェイスコンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。トランク ポートをインターフェイスにすることはできません。
ステップ 4	**ip igmp max-groups action** {**deny** | **replace**} 例： `Device(config-if)# ip igmp max-groups action replace`	インターフェイスが IGMP レポートを受信したときに、転送テーブルに最大数のエントリが登録されている場合は、次のいずれかのアクションをインターフェイスに指定します。 • **deny**：レポートを破棄します。このスロットリング アクションを設定すると、すでに転送テーブルに登録されていたエントリは、削除されることはありませんが期限切れになります。エントリが期限切れになり、最大数のエントリが転送テーブルに登録されていると、デバイスは、インターフェイスで受信した次の IGMP レポートを廃棄します。 • **replace**：既存のグループを、IGMP レポートを受信した新しいグループで上書きします。このスロットリング アクションを設定すると、すでに転送テーブルに登録されていたエントリは削除されます。転送テーブ

	コマンドまたはアクション	目的
		ルのエントリが最大数まで達したら、デバイスはランダムに選択したエントリを受信したIGMPレポートで上書きします。 デバイスが転送テーブルのエントリを削除しないようにするには、インターフェイスにより転送テーブルにエントリが追加される前に、IGMPスロットリングアクションを設定します。 （注） レポートの廃棄というデフォルトのアクションに戻すには、**no ip igmp max-groups action** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

直接接続の IGMP ホストがない場合にマルチキャスト トラフィックが転送されるようにデバイスを設定する方法

直接接続されたIGMPホストがない場合に、マルチキャストトラフィックを転送するようにデバイスを設定するには、次のオプション作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1`	インターフェイス コンフィギュレーション モードを開始します。 • *type* 引数および *number* 引数に、ホストに接続されているインターフェイスを指定します。

ステップ 4	次のいずれかを実行します。
	• **ipigmpjoin-group** *group-address*
	• **ipigmpstatic-group** {***** | *group-address* [**source** *source-address*]}
	例：
	`Device(config-if)# ip igmp join-group 225.2.2.2`
	例：
	`Device(config-if)# ip igmp static-group 225.2.2.2`
		最初の例では、指定したグループに加入するデバイスのインターフェイスを設定する例を示します。
		• この方法では、デバイスは、マルチキャストパケットの転送に加えて、マルチキャスト パケットを受信します。マルチキャスト パケットを受信する場合は、高速スイッチングを実行できません。
		
		2 番目の例では、インターフェイスでスタティック グループ メンバーシップ エントリを設定する例を示します。
		• この方法の場合、デバイスはパケットそのものを受信せず、転送だけを実行します。したがって、この方法では、高速スイッチングを実行できます。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャスト ルート エントリに「L」（ローカル）フラグが付かないことからも明らかなように、デバイス自体はメンバではありません。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showipigmpinterface** [*interface-type interface-number*] 例： `Device# show ip igmp interface`	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。

IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御する方法

ソース アドレス、グループ アドレス、またはその両方に基づいて SSM トラフィックをフィルタする IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御するには、次のオプション作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipmulticast-routing** [**distributed**] 例： `Device(config)# ip multicast-routing distributed`	IP マルチキャスト ルーティングをイネーブルにします。 • **distributed** キーワードは、IPv4 マルチキャストの場合に必要です。
ステップ 4	**ippimssm** {**default** | **range** *access-list*} 例： `Device(config)# ip pim ssm default`	SSM サービスを設定します。 • **default** キーワードは SSM 範囲のアクセス リストを 232/8 と定義します。 • **range** キーワードは標準の IP アクセス リスト番号または SSM 範囲を定義する名前を指定します。
ステップ 5	**ipaccess-listextended** *access-list*-name 例： `Device(config)# ip access-list extended mygroup`	名前付き拡張 IP アクセス リストを指定します。
ステップ 6	**denyigmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# deny igmp host 10.1.2.3 any`	（任意）IGMP レポートから指定したソースアドレスまたはグループアドレスをフィルタリングすることで、サブネットのホストをメンバーシップから (S, G) チャネルに制限します。 • サブネット メンバーシップから他の (S, G) チャネルにホストを制限するには、この手順を繰り返します。（特に許可されないソースまたはグループは拒否されるため、これらのソースは後続の **permit** ステートメントより限定的になります）。 • アクセス リストは、暗黙の **deny** ステートメントで終了することに注意してください。 • 次に、ソース 10.1.2.3 に対してすべてのグループをフィルタリングして、効果的にソースを拒否する deny ステートメントを作成する例を示します。

	コマンドまたはアクション	目的
ステップ 7	**permitigmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit igmp any any`	IGMP レポートのソース アドレスまたはグループ アドレスが IP アクセス リストを渡すことができます。 • アクセス リストには少なくとも 1 つの **permit** ステートメントが必要です。 • 他のソースが IP アクセス リストを渡せるようにする場合は、この手順を繰り返します。 • この例では、前の **deny** ステートメントによって拒否されていないソースおよびグループに対するメンバーシップを許可する方法を示します。
ステップ 8	**exit** 例： `Device(config-ext-nacl)# exit`	現在のコンフィギュレーション セッションを終了し、グローバルコンフィギュレーション モードに戻ります。
ステップ 9	interface type number 例： `Device(config)# interface ethernet 0`	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 10	**ipigmpaccess-group** *access-list* 例： `Device(config-if)# ip igmp access-group mygroup`	IGMP レポートに指定されたアクセス リストが適用されます。
ステップ 11	**ippimsparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	インターフェイスで PIM-SM をイネーブルにします。 （注） スパースモードを使用する必要があります。
ステップ 12	SSM チャネル メンバーシップのアクセス コントロールを必要とするすべてのインターフェイスでステップ 1 ～ 11 を繰り返します。	--

	コマンドまたはアクション	目的
ステップ 13	**ipigmpversion3** 例： `Device(config-if)# ip igmp version 3`	このインターフェイス上で IGMPv3 をイネーブルにします。デフォルトの IGMP バージョンは IGMP バージョン 2 です。SSM にはバージョン 3 が必要です。
ステップ 14	ホスト方向のインターフェイスすべてでステップ 13 を繰り返します。	--
ステップ 15	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

IGMP スヌーピングを設定する方法

IGMP スヌーピングのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping** 例： `Device(config)# ip igmp snooping`	ディセーブルにした後で、IGMP スヌーピングをグローバルにイネーブルにします。
ステップ 4	**bridge-domain** *bridge-id* 例： `Device(config)# bridge-domain 100`	（任意）ブリッジ ドメイン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**ip igmp snooping** 例： `Device(config-bdomain)# ip igmp snooping`	（任意）設定されたブリッジ ドメイン インターフェイス上でIGMPスヌーピングをイネーブルにします。 • 指定されたブリッジ ドメインでIGMPスヌーピングが明示的にディセーブルにされた場合にだけ必要です。
ステップ 6	**end** 例： `Device(config-bdomain)# end`	特権 EXEC モードに戻ります。

VLAN インターフェイスでの IGMP スヌーピングのイネーブル化またはディセーブル化（CLI）

VLANインターフェイス上でIGMPスヌーピングを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan** *vlan-id* 例： `Device(config)# ip igmp snooping vlan 7`	VLAN インターフェイス上で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 VLANスヌーピングをイネーブルにするには、IGMPスヌーピングをグローバルにイネーブルに設定しておく必要があります。

	コマンドまたはアクション	目的
		（注） 特定の VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、**no ip igmp snooping vlan** *vlan-id* グローバル コンフィギュレーション コマンドを、指定した VLAN 番号に対して使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スヌーピング方法の設定（CLI）

マルチキャスト対応のルータ ポートは、レイヤ 2 マルチキャスト エントリごとに転送テーブルに追加されます。デバイス は、次のいずれかの方法でポートを学習します。

- IGMP クエリ、Protocol-Independent Multicast（PIM）パケット、のスヌーピング
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによるマルチキャスト ルータ ポートへの静的な接続

VLAN インターフェイスがマルチキャスト ルータにアクセスする方法を変更するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**ip igmp snooping vlan** *vlan-id* **mrouterinterface {GigabitEthernet | Port-Channel | TenGigabitEthernet}** 例： `Device(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet1/0/3`	VLAN 上で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

マルチキャスト ルータ ポートの設定（CLI）

デバイスにマルチキャスト ルータ ポートを追加する（マルチキャスト ルータへのスタティック接続を有効にする）には、次の手順を実行します。

（注） マルチキャスト ルータへのスタティック接続は、デバイス ポートに限りサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan** *vlan-id***mrouter interface** *interface-id* 例： `Device(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet1/0/1`	マルチキャスト ルータの VLAN ID およびマルチキャスト ルータに対するインターフェイスを指定します。 • 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 128 です。 （注） マルチキャスト ルータ ポートを VLAN から削除するには、**no ip igmp snooping vlan** *vlan-id***mrouter interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping mrouter** [**vlan** *vlan-id*] 例： `Device# show ip igmp snooping mrouter vlan 5`	VLAN インターフェイス上で IGMP スヌーピングが有効になっていることを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

グループに加入するホストの静的な設定（CLI）

ホストまたはレイヤ 2 ポートは通常、マルチキャスト グループに動的に加入しますが、インターフェイス上にホストを静的に設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ2ポートを追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan** *vlan-id***static** *ip_address***interface** *interface-id* 例： `Device(config)# ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1`	マルチキャスト グループのメンバとしてレイヤ2ポートを静的に設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。 • *ip-address* は、グループの IP アドレスです。 • *interface-id* は、メンバ ポートです。物理インターフェイスまたはポート チャネル（1 ～ 128）に設定できます。

	コマンドまたはアクション	目的
		（注） マルチキャスト グループからレイヤ 2 ポートを削除するには、**no ip igmp snooping vlan** *vlan-id***static** *mac-address***interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping groups** 例： `Device# show ip igmp snooping groups`	メンバ ポートおよび IP アドレスを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP 即時脱退のイネーブル化（CLI）

IGMP 即時脱退をイネーブルに設定すると、デバイスはポート上で IGMP バージョン 2 の Leave メッセージを検出した場合、ただちにそのポートを削除します。即時脱退機能は、VLAN の各ポートにレシーバが 1 つ存在する場合にだけ使用してください。

（注） 即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。IGMP バージョン 2 はデバイスのデフォルト バージョンです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan** *vlan-id***immediate-leave** 例： `Device(config)# ip igmp snooping vlan 21 immediate-leave`	VLANインターフェイス上で、IGMP即時脱退をイネーブルにします。 （注） VLAN 上で IGMP 即時脱退をディセーブルにするには、 **no ip igmp snooping vlan** *vlan-id***immediate-leave** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping vlan** *vlan-id* 例： `Device# show ip igmp snooping vlan 21`	VLANインターフェイス上で即時脱退がイネーブルになっていることを確認します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

即時脱退 （519 ページ）

IGMP 脱退タイマーの設定（CLI）

脱退時間はグローバルまたはVLAN単位で設定できます。IGMP脱退タイマーの設定をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping last-member-query-interval** *time* 例： `Device(config)# ip igmp snooping last-member-query-interval 1000`	IGMP 脱退タイマーをグローバルに設定します。指定できる範囲は 100 ～ 32767 ミリ秒です。 デフォルトの脱退時間は 1000 ミリ秒です。 （注） IGMP 脱退タイマーをグローバルにリセットしてデフォルト設定に戻すには、 **no ip igmp snooping last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**ip igmp snooping vlan** *vlan-id***last-member-query-interval** *time* 例： `Device(config)# ip igmp snooping vlan 210 last-member-query-interval 1000`	（任意）VLAN インターフェイス上で IGMP 脱退時間を設定します。有効値は 100 ～ 32767 ミリ秒です。 （注） VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。 （注） 特定の VLAN から IGMP 脱退タイマーの設定を削除するには、 **no ip igmp snooping vlan** *vlan-id***last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	（任意）設定された IGMP 脱退時間を表示します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP 設定可能脱退タイマー （520 ページ）

IGMP 堅牢性変数の設定（CLI）

デバイス で IGMP 堅牢性変数を設定するには、次の手順を使用します。

堅牢性変数は、IGMP メッセージの計算時に IGMP スヌーピングで使用される整数です。堅牢性変数により、想定されるパケット損失を考慮した微調整を実施できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip igmp snooping robustness-variable** *count* 例： `Device(config)# ip igmp snooping robustness-variable 3`	IGMP 堅牢性変数を設定します。範囲は、1 ～ 3 回です。 堅牢性変数の推奨値は 2 です。IGMP スヌーピングの堅牢性変数の値をデフォルトの 2 から指定した値に変更するには、このコマンドを使用します。
ステップ 4	**ip igmp snooping vlan** *vlan-id* **robustness-variable** *count* 例： `Device(config)#ip igmp snooping vlan 100 robustness-variable 3`	（任意）VLAN インターフェイス上で IGMP 堅牢性変数を設定します。範囲は、1 ～ 3 回です。堅牢性変数の推奨値は 2 です。 （注） VLAN で堅牢性変数カウントを設定すると、グローバルに設定された値が上書きされます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	（任意）設定された IGMP 堅牢性変数カウントを表示します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP 最終メンバー クエリ回数の設定（CLI）

グループ固有またはグループ ソース固有の leave メッセージの受信に応答して、IGMP グループ固有またはグループ ソース固有の（IGMP バージョン 3 で）クエリ メッセージを デバイスが送信する回数を設定するには、次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping last-member-query-count** *count* 例： `Device(config)# ip igmp snooping last-member-query-count 3`	IGMP 最終メンバー クエリ回数を設定します。指定できる範囲は 1 ～ 7 です。デフォルト値は 2 メッセージです。
ステップ 4	**ip igmp snooping vlan** *vlan-id* **last-member-query-count** *count* 例： `Device(config)#ip igmp snooping vlan 100 last-member-query-count 3`	（任意）VLAN インターフェイス上で IGMP 最終メンバー クエリ回数を設定します。指定できる範囲は 1 ～ 7 です。 （注） VLAN で最終メンバー クエリ回数を設定すると、グローバルに設定されたタイマーが上書きされます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	（任意）設定された IGMP 最終メンバー クエリ回数を表示します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

TCN 関連コマンドの設定

TCN イベント後のマルチキャスト フラッディング時間の制御（CLI）

トポロジ変更通知（TCN）イベント後にフラッディングするマルチキャストデータのトラフィックに対し、一般クエリー数を設定できます。TCN フラッド クエリ カウントを 1 に設定した場合は、1 つの一般クエリーを受信した後にフラッディングが停止します。カウントを 7 に設定した場合、一般クエリーを 7 つ受信するまでフラッディングが続きます。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

クライアント ロケーションが変更され、ブロックされていた後に現在は転送中の受信者が同じポートに存在する場合や、ポートが脱退メッセージを送信せずにダウンした場合などに TCN イベントが発生します。

TCN フラッド クエリー カウントを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping tcn flood query count** *count* 例： `Device(config)# ip igmp snooping tcn flood query count 3`	マルチキャスト トラフィックがフラッディングする IGMP の一般クエリー数を指定します。 指定できる範囲は 1 ～ 10 です。デフォルトのフラッディング クエリー カウントは 2 です。

	コマンドまたはアクション	目的
		（注） デフォルトのフラッディング クエリー カウントに戻すには、**no ip igmp snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	TCN の設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

フラッディング モードからの回復（CLI）

トポロジの変更が発生した場合、スパニングツリーのルートは特別な IGMP Leave メッセージ（グローバル Leave メッセージ）をグループ マルチキャスト アドレス 0.0.0.0. に送信します。ただし、スパニングツリーのルートであるかどうかにかかわらず、グローバルな Leave メッセージを送信するようにデバイスを設定できます。ルータはこの特別な Leave メッセージを受信した場合、即座に一般クエリーを送信して、TCN 中のフラッディング モードからできるだけ早く回復するようにします。デバイスがスパニングツリーのルートであれば、このコンフィギュレーションに関係なく、Leave メッセージが常に送信されます。

Leave メッセージを送信できるようにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping tcn query solicit** 例： `Device(config)# ip igmp snooping tcn query solicit`	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ（グローバル脱退）を送信します。デフォルトでは、クエリー送信要求はディセーブルに設定されています。 （注） デフォルトのクエリー送信要求に戻すには、 **no ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	TCN の設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

TCN イベント中のマルチキャスト フラッディングのディセーブル化（CLI）

デバイスは TCN を受信すると、一般クエリーを 2 つ受信するまで、すべてのポートに対してマルチキャスト トラフィックをフラッディングします。異なるマルチキャスト グループのホストに接続しているポートが複数ある場合、リンク範囲を超えてデバイスによるフラッディングが行われ、パケット損失が発生する可能性があります。TCN フラッディングを制御するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	**no ip igmp snooping tcn flood** 例： `Device(config-if)# no ip igmp snooping tcn flood`	スパニングツリーの TCN イベント中に発生するマルチキャスト トラフィックのフラッディングをディセーブルにします。 デフォルトでは、インターフェイス上のマルチキャストフラッディングはイネーブルです。 （注） インターフェイス上でマルチキャスト フラッディングを再度イネーブルにするには、 **ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping** 例：	TCN の設定を確認します。

	コマンドまたはアクション	目的
	`Device# show ip igmp snooping`	
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP スヌーピング クエリアの設定（CLI）

特定の VLAN で IGMP スヌーピング クエリア機能をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping querier** 例： `Device(config)# ip igmp snooping querier`	IGMP スヌーピング クエリアをイネーブルにします。
ステップ 4	**ip igmp snooping querier address** *ip_address* 例： `Device(config)# ip igmp snooping querier address 172.16.24.1`	（任意）IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。

	コマンドまたはアクション	目的
		（注） IGMP スヌーピング クエリアはデバイス上で IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
ステップ 5	**ip igmp snooping querier query-interval** *interval-count* 例： `Device(config)# ip igmp snooping querier query-interval 30`	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
ステップ 6	**ip igmp snooping querier tcn query** [**count** *count* | **interval** *interval*] 例： `Device(config)# ip igmp snooping querier tcn query interval 20`	（任意）トポロジ変更通知（TCN）クエリーの間隔を設定します。指定できる count の範囲は 1 ～ 10 です。指定できる interval の範囲は 1 ～ 255 秒です。
ステップ 7	**ip igmp snooping querier timer expiry** *timeout* 例： `Device(config)# ip igmp snooping querier timer expiry 180`	（任意）IGMP クエリアが期限切れになる時間を設定します。指定できる範囲は 60 ～ 300 秒です。
ステップ 8	**ip igmp snooping querier version** *version* 例： `Device(config)# ip igmp snooping querier version 2`	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip igmp snooping vlan** *vlan-id* 例： `Device# show ip igmp snooping vlan 30`	（任意）VLAN インターフェイス上で IGMP スヌーピング クエリアがイネーブルになっていることを確認します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

	コマンドまたはアクション	目的
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

IGMP レポート抑制のディセーブル化（CLI）

IGMP レポート抑制をディセーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ip igmp snooping report-suppression** 例： `Device(config)# no ip igmp snooping report-suppression`	IGMP レポート抑制をディセーブルにします。IGMP レポート抑制がディセーブルの場合、すべての IGMP レポートがマルチキャスト ルータに転送されます。 IGMP レポート抑制はデフォルトでイネーブルです。 IGMP レポート抑制がイネーブルの場合、デバイスはマルチキャスト ルータクエリーごとに IGMP レポートを 1 つだけ転送します。

	コマンドまたはアクション	目的
		（注） IGMP レポート抑制を再びイネーブルにするには、**ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	IGMP レポート抑制がディセーブルになっていることを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP レポート抑制 （520 ページ）

IGMP のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

（注） このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

次の表に示す特権EXECコマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 *38 :* システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
ping [*group-name* | *group-address*]	マルチキャスト グループ アドレスにインターネット制御メッセージプロトコル（ICMP）エコー要求を送信します。
show ip igmp filter	IGMP フィルタ情報を表示します。
show ip igmp groups [*type-number* | *detail*]	デバイスに直接接続され、IGMPによって取得されたマルチキャスト グループを表示します。
show ip igmp interface [*type number*]	インターフェイスのマルチキャスト関連情報を表示します。
show ip igmp membership [*name/group address* | **all** | **tracked**]	転送に関する IGMP メンバーシップ情報を表示します。
show ip igmp profile [*profile_number*]	IGMP プロファイル情報を表示します。
show ip igmp ssm-mapping [*hostname/IP address*]	IGMP SSM マッピング情報を表示します。
show ip igmp static-group {**class-map** [**interface** [*type*]]	スタティック グループ情報を表示します。
show ip igmp vrf	選択したVPNルーティング/転送インスタンスを名前別に表示します。

IGMP スヌーピング情報の監視

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの IGMP スヌーピング情報を表示できます。また、IGMP スヌーピング用に設定された VLAN の IP アドレス マルチキャスト エントリを表示することもできます。

表 *39 : IGMP* スヌーピング情報を表示するためのコマンド

コマンド	目的
show ip igmp snooping detail	動作状態情報を表示します。

コマンド	目的
show ip igmp snooping groups [**count** | [**vlan** *vlan-id* [*A.B.C.D* | **count**]]	デバイスまたは特定のパラメータに関して、マルチキャスト テーブル情報を表示します。 • **count**：グループの合計数を表示します。 • **vlan**：VLAN ID によるグループ情報を表示します。
show ip igmp snooping igmpv2-tracking	IGMP スヌーピング トラッキングを表示します。 （注） このコマンドでは、ワイヤレスマルチキャスト IGMP 加入のみに関するグループおよび IP アドレス エントリが表示され、有線 IGMP 加入については表示されません。このコマンドで表示させるには、ワイヤレス IP マルチキャストを有効にしておく必要があります。
show ip igmp snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習され、手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。 （注） IGMP スヌーピングを有効にすると、デバイスはマルチキャスト ルータの接続先インターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。
show ip igmp snooping querier [**detail** | **vlan** *vlan-id*]	IP アドレス、および VLAN で受信した最新の IGMP クエリ メッセージの受信ポートに関する情報を表示します。 （任意）VLAN の詳細な IGMP クエリア情報を表示するには、**detail** を入力します。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。

コマンド	目的
show ip igmp snooping [**vlan** *vlan-id* [**detail**]]	デバイス上のすべての VLAN または特定の VLANのスヌーピング設定情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ip igmp snooping wireless mgid	ワイヤレス関連イベントを表示します。

IGMP フィルタリングおよび IGMP スロットリングの設定のモニタリング

IGMP プロファイルの特性を表示したり、デバイス上のすべてのインターフェイスまたは指定されたインターフェイスのIGMPプロファイルや最大グループ設定を表示したりできます。また、デバイス上のすべてのインターフェイスまたは指定したインターフェイスに関する IGMP スロットリング設定を表示することもできます。

表 *40 : IGMP* フィルタリングおよび *IGMP* スロットリング設定を表示するためのコマンド

コマンド	目的
show ip igmp profile [*profile number*]	特定の IGMP プロファイルまたはデバイス上で定義されているすべての IGMP プロファイルを表示します。
show running-config [**interface** *interface-id*]	インターフェイスが所属できる IGMP グループの最大数（設定されている場合）や、インターフェイスに適用される IGMP プロファイルを含む、特定のインターフェイスまたはデバイス上のすべてのインターフェイスの設定を表示します。

IGMP の設定例

例：マルチキャスト グループのメンバとしてのデバイスの設定

次に、マルチキャスト グループ 255.2.2.2 へのデバイスの加入を許可する例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip igmp join-group 255.2.2.2
```

```
Device(config-if)#
```

関連トピック

グループのメンバとしてのデバイスの設定（CLI）（523 ページ）
マルチキャスト グループへの加入（517 ページ）
IGMP マルチキャスト アドレス（510 ページ）

例：マルチキャスト グループへのアクセスの制御

インターフェイスで参加数を制限するには、IGMPプロファイルと関連付けるフィルタ用のポートを設定します。

```
Device# configure terminal
Device(config)# ip igmp profile 10
Device(config-igmp-profile)# ?

IGMP profile configuration commands:
deny matching addresses are denied
exit Exit from igmp profile configuration mode
no Negate a command or set its defaults
permit matching addresses are permitted
range add a range to the set

Device(config-igmp-profile)# range 172.16.5.1
Device(config-igmp-profile)# exit
Device(config)#
Device(config)# interface gigabitEthernet 2/0/10
Device(config-if)# ip igmp filter 10
```

例：IGMP スヌーピングの設定

次に、マルチキャスト ルータへの静的な接続をイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Device(config)# end
```

次に、ポート上のホストを静的に設定する例を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/0/1
Device(config)# end
```

次に、VLAN 130 上で IGMP 即時脱退をイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping vlan 130 immediate-leave
Device(config)# end
```

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping querier 10.0.0.64
Device(config)# end
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping querier query-interval 25
Device(config)# end
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping querier timer expiry 60
Device(config)# end
```

次に、IGMP スヌーピング クエリア機能をバージョン 2 に設定する例を示します。

```
Device# configure terminal
Device(config)# no ip igmp snooping querier version 2
Device(config)# end
```

例：IGMP プロファイルの設定

次に、単一の IP マルチキャスト アドレスへのアクセスを許可する IGMP プロファイル 4 を作成して、設定を確認する例を示します。アクションが拒否（デフォルト）である場合は、**show ip igmp profile** の出力には表示されません。

```
Device(config)# ip igmp profile 4
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 229.9.9.0
Device(config-igmp-profile)# end
Device# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

例：IGMP プロファイルの適用

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip igmp filter 4
Device(config-if)# end
```

例：IGMP グループの最大数の設定

次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip igmp max-groups 25
Device(config-if)# end
```

例：ルーテッド ポートとしてのインターフェイス設定

次に、デバイスのインターフェイスをルーテッド ポートとして設定する例を示します。**no switchport** コマンドを実行する必要がある複数の IP マルチキャスト ルーティングの設定手順の場合に、この設定をインターフェイスで行う必要があります。

```
Device configure terminal
Device(config)#  interface GigabitEthernet1/0/9
Device(config-if)# description interface to be use as routed port
Device(config-if)# no switchport
Device(config-if)# ip address 20.20.20.1 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# ip igmp join-group 224.1.2.3 source 15.15.15.2
Device(config-if)# end
Device# configure terminal
Device# show run interface gigabitEthernet 1/0/9

Current configuration : 166 bytes
!
interface GigabitEthernet1/0/9
 no switchport
 ip address 20.20.20.1 255.255.255.0
 ip pim sparse-dense-mode
 ip igmp static-group 224.1.2.3 source 15.15.15.2
end
```

例：SVI としてのインターフェイスの設定

次に、デバイス のインターフェイスを SVI として設定する例を示します。**no switchport** コマンドを実行する必要がある複数の IP マルチキャスト ルーティングの設定手順の場合に、この設定をインターフェイスで行う必要があります。

```
Device(config)# interface vlan 150
Device(config-if)# ip address 20.20.20.1 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# ip igmp join-group 224.1.2.3 source 15.15.15.2
Device(config-if)# end
Device# configure terminal
Device(config)#  ip igmp snooping vlan 20 static 224.1.2.3
interface gigabitEthernet 1/0/9
Device# show run interface vlan 150

Current configuration : 137 bytes
!
interface Vlan150
```

```
 ip address 20.20.20.1 255.255.255.0
 ip pim sparse-dense-mode
 ip igmp static-group 224.1.2.3 source 15.15.15.2
end
```

例：直接接続された IGMP ホストがない場合に、マルチキャスト トラフィックを転送するようにデバイスを設定

次に、**ipigmpjoin-group** コマンドを使用して、直接接続された IGMP ホストがない場合に、マルチキャスト トラフィックを転送するようデバイスを設定する例を示します。この方法では、デバイスは、マルチキャスト パケットの転送に加えて、マルチキャスト パケットを受信します。マルチキャスト パケットを受信する場合は、高速スイッチングを実行できません。

この例では、グループ 225.2.2.2 に加入するように、デバイスでファストイーサネット インターフェイス 0/0/0 が設定されています。

```
interface FastEthernet0/0/0
 ip igmp join-group 225.2.2.2
```

次に、 **ip igmp static-group** コマンドを使用して、直接接続された IGMP ホストがない場合に、マルチキャスト トラフィックを転送するようデバイスを設定する例を示します。この方法の場合、デバイスはパケットそのものを受信せず、転送だけを実行します。したがって、この方法では、高速スイッチングを実行できます。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャスト ルート エントリに「L」（ローカル）フラグが付かないことからも明らかなように、デバイス自体はメンバではありません。

この例では、グループ 225.2.2.2 のスタティック グループ メンバーシップ エントリがファストイーサネット インターフェイス 0/1/0 で設定されます。

```
interface FastEthernet0/1/0
 ip igmp static-group 225.2.2.2
```

IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御する方法

ここでは、IGMP 拡張アクセス リストを使用して SSM ネットワーク上でアクセスを制御する、次の設定例について説明します。

（注） アクセス リストは非常に柔軟が高いことに留意してください。マルチキャスト トラフィックのフィルタリングに使用できる permit ステートメントと deny ステートメントの組み合わせは多数あります。この項では、少しの例を示します。

例：グループ G のすべての状態を拒否

次に、グループ G のすべての状態を拒否する方法の例を示します。この例では、IGMPv3 レポートの SSM グループ 232.2.2.2 のすべての送信元がフィルタリングされるよう、ファスト イーサネット インターフェイス 0/0/0 が設定されます。これにより、このグループが効率的に拒否されます。

```
ip access-list extended test1
 deny igmp any host 232.2.2.2
 permit igmp any any
!
interface FastEthernet0/0/0
 ip igmp access-group test1
```

例：ソース S のすべての状態を拒否

次に、ソース S ですべての状態を拒否する方法の例を示します。この例では、IGMPv3 レポートの送信元の 10.2.1.32 のグループがフィルタリングされるよう、ギガビット イーサネット インターフェイス 1/1/0 が設定されます。これにより、このソースが効果的に拒否されます。

```
ip access-list extended test2
 deny igmp host 10.2.1.32 any
 permit igmp any any
!
interface GigabitEthernet1/1/0
 ip igmp access-group test2
```

例：グループ G のすべての状態を許可

次に、グループ G ですべての状態を許可する例を示します。この例では、IGMPv3 レポートの SSM グループ 232.1.1.10 に対するすべてのソースが受け付けられるよう、ギガビット イーサネット インターフェイス 1/2/0 が設定されます。これにより、このグループ全体が効果的に受け付けられます。

```
ip access-list extended test3
 permit igmp any host 232.1.1.10
!
interface GigabitEthernet1/2/0
 ip igmp access-group test3
```

例：ソース S のすべての状態を許可

次に、ソース S ですべての状態を許可する例を示します。この例では、IGMPv3 レポートのソース 10.6.23.32 に対するすべてのグループが受け付けられるよう、ギガビット イーサネット インターフェイス 1/2 が設定されます。これにより、このソース全体が効果的に受け付けられます。

```
ip access-list extended test4
 permit igmp host 10.6.23.32 any
!
interface GigabitEthernet1/2/0
 ip igmp access-group test4
```

例：グループ G のソース S をフィルタリング

次に、グループ G の特定のソース S のフィルタリング例を示します。この例では、IGMPv3 レポートの SSM グループ 232.2.30.30 のソース 232.2.2.2 をフィルタリングするよう、ギガビット イーサネット インターフェイス 0/3/0 が設定されます。

```
ip access-list extended test5
 deny igmp host 10.4.4.4 host 232.2.30.30
 permit igmp any any
!
interface GigabitEthernet0/3/0
 ip igmp access-group test5
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*IP Multicast Routing Command Reference*（*Catalyst 3850 Switches*）
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP Multicast Command Reference』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
RFC 1112	『Host Extensions for IP Multicasting』
RFC 2236	『Internet Group Management Protocol, Version 2』
RFC 3376	『*Internet Group Management Protocol, Version 3*』

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IGMP の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 29 章

IGMP プロキシの設定

- 機能情報の確認 （579 ページ）
- IGMP プロキシの前提条件 （579 ページ）
- IGMP プロキシの情報 （580 ページ）
- IGMP プロキシの設定方法 （582 ページ）
- IGMP プロキシの設定例 （587 ページ）
- その他の参考資料 （588 ページ）
- IGMP プロキシの機能履歴と情報 （589 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IGMP プロキシの前提条件

- IGMP UDL 上のすべてのデバイスに、同じサブネット アドレスがあること。UDL 上のすべてのデバイスで、同じサブネットアドレスを持つことができない場合、アップストリーム デバイスは、ダウンストリーム デバイスが接続されているすべてのサブネットに一致するセカンダリ アドレスで設定される必要があります。
- IP マルチキャストがイネーブルになり、PIM インターフェイスが設定されます。

（注） IGMP プロキシの PIM インターフェイスを設定する際は、次のガイドラインに従ってください。

- インターフェイスがスパース モード領域で実行中で、スタティック RP、ブートストラップ（BSR）、または自動 RP リスナー機能ありで自動RPを実行している場合は、PIMスパース モード（PIM-SM）を使用します。
- インターフェイスがスパース-デンスモード領域で実行中で、自動RPリスナー機能なしで自動RPを実行している場合は、PIM スパース-デンス モードを使用します。
- インターフェイスがデンスモードで実行されているときに、デンス モード領域に加入する場合は、PIM デンス モード（PIM-DM）を使用します。
- インターフェイスが、スパースモード領域のレシーバに到達する必要があるトラフィックをデンスモード領域から受信する場合は、プロキシ登録機能ありのPIM-DMを使用します。

IGMP プロキシの情報

IGMP プロキシ

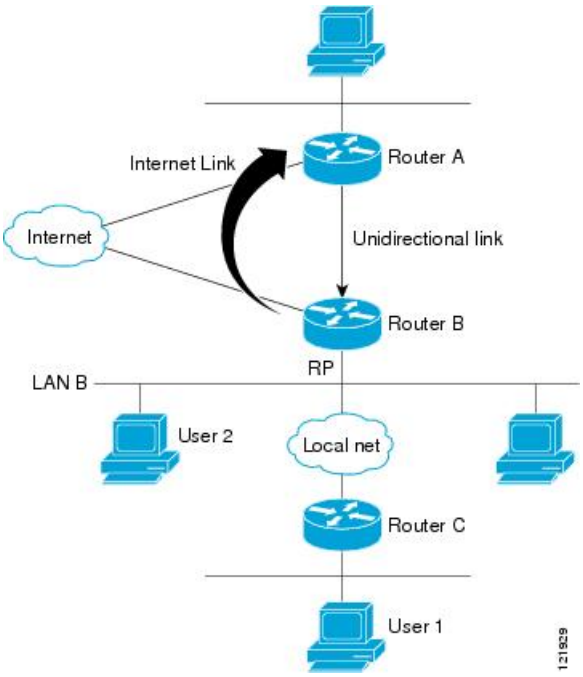
IGMPプロキシは、アップストリーム ネットワークがソースのマルチキャスト グループに、ダウンストリーム ルータに直接接続されていない単方向リンク ルーティング（UDLR）環境のホストが加入できるようにします。

次の図に、2 つの UDLR シナリオを示すトポロジ例を図示します。

- 従来型の UDL ルーティングのシナリオ：直接接続されたレシーバがある UDL デバイス。
- IGMP プロキシのシナリオ：直接接続されたレシーバのない UDL デバイス。

（注） IGMP UDL は、アップストリームおよびダウンストリーム デバイス上にある必要はありません。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。



シナリオ 1：従来型の UDLR のシナリオ（直接接続されたレシーバがある UDL デバイス）

シナリオ 1 では、IGMP プロキシ メカニズムは必要ありません。このシナリオでは、次の一連のイベントが発生します。

1. ユーザ 2 がグループ G の対象を要求する IGMP メンバーシップ レポートを送信します。
2. ルータ B は、IGMP メンバーシップ レポートを受信し、LAN B のグループ G の転送エントリを追加し、UDLR アップストリーム デバイスであるルータ A に IGMP レポートをプロキシします。
3. IGMP レポートは、インターネット リンク間でプロキシされます。
4. ルータ A は IGMP プロキシを受信し、単方向リンクの転送エントリを保持します。

シナリオ 2：IGMP プロキシのシナリオ（直接接続されたレシーバのない UDL デバイス）

シナリオ 2 の場合、アップストリーム ネットワークがソースのマルチキャスト グループに、ダウンストリームデバイスに直接接続されていないホストが加入できるように、IGMP プロキシ メカニズムが必要です。このシナリオでは、次の一連のイベントが発生します。

1. ユーザ 1 がグループ G の対象を要求する IGMP メンバーシップ レポートを送信します。
2. ルータ C が RP（ルータ B）に PIM Join メッセージをホップバイホップで送信します。
3. ルータ B で PIM 加入メッセージを受信し、LAN B 上のグループ G に対する転送エントリが追加されます。

4. ルータ B では、その mroute テーブルが定期的にチェックされ、インターネット リンクを介してアップストリーム UDL デバイスに IGMP メンバーシップ レポートがプロキシされます。

5. ルータ A は単方向リンク（UDL）転送エントリを作成し、維持します。

エンタープライズ ネットワークでは、サテライトを介して IP マルチキャスト トラフィックを受信し、ネットワーク中にトラフィックを転送することができる必要があります。シナリオ 2 は、受信ホストがダウンストリーム デバイスのルータ B に直接接続する必要があるため、単方向リンク ルーティング（UDLR）だけでは不可能です。IGMP プロキシ メカニズムを使用すると、マルチキャスト転送テーブル内の (*, G) エントリに対し IGMP レポートを作成することで、この制限が取り除かれます。そのため、このシナリオを機能させるには、インターフェイスでプロキシされた (*, G) マルチキャスト スタティック ルート（mroute）エントリの IGMP レポートの転送をイネーブルにして（**ipigmpmroute-proxy** コマンドを使用）、mroute プロキシ サービスをイネーブルにし、（**ipigmpproxy-service** コマンドを使用）、PIM 対応ネットワークと可能性があるメンバーに導く必要があります。

（注） PIM メッセージはアップストリームに転送されないため、各ダウンストリーム ネットワークとアップストリーム ネットワークのドメインは別になります。

関連トピック

IGMP UDLR に対するアップストリーム UDL デバイスの設定 （582 ページ）
IGMP プロキシ サポート付きの IGMP UDLR に対するダウンストリーム UDL デバイスの設定 （583 ページ）
例：IGMP プロキシ設定 （587 ページ）

IGMP プロキシの設定方法

IGMP UDLR に対するアップストリーム UDL デバイスの設定

IGMP UDLR に対するアップストリーム UDL デバイスを設定するには、この作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	インターフェイスコンフィギュレーション モードを開始します。 • *type* および *number* 引数に、アップストリームデバイスの UDL として使用するインターフェイスを指定します。
ステップ 4	**ipigmpunidirectional-link** 例： `Device(config-if)# ip igmp unidirectional-link`	インターフェイス上の IGMP を、IGMP UDLR に対して単方向になるよう設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

関連トピック

IGMP プロキシ （580 ページ）
例：IGMP プロキシ設定 （587 ページ）

IGMP プロキシ サポート付きの IGMP UDLR に対するダウンストリーム UDL デバイスの設定

IGMP プロキシ サポート付きの IGMP UDLR に対するダウンストリーム UDL デバイスを設定するには、この作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイス コンフィギュレーション モードを開始します。 • *type* および *number* 引数に、IGMP UDLR に対するダウンストリーム デバイスの UDL として使用するインターフェイスを指定します。
ステップ 4	**ipigmpunidirectional-link** 例： `Device(config-if)# ip igmp unidirectional-link`	インターフェイス上の IGMP を、IGMP UDLR に対して単方向になるよう設定します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	インターフェイス コンフィギュレーション モードを開始します。 • *type* および *number* 引数で、間接的に接続されているホストの方向に向いているインターフェイスを選択します。
ステップ 7	**ipigmpmroute-proxy** *type number* 例： `Device(config-if)# ip igmp mroute-proxy loopback 0`	プロキシされた (*, G) マルチキャスト スタティック ルート（mroute）エントリの IGMP レポートの転送をイネーブルにします。 • この手順は、マルチキャスト転送テーブルにあるすべての (*, G) 転送エントリに対するプロキシサービスインターフェイスへの、IGMP レポートの転送をイネーブルにするために実行されます。 • この例では、ギガビット イーサネットインターフェイス 1/0/0 で、

	コマンドまたはアクション	目的
		ギガビットイーサネットインターフェイス 1/0/0 に転送される mroute テーブルのすべてのグループのループバック インターフェイス 0 に IGMP レポートを送信するように要求する **ipigmpmroute-proxy** コマンドが設定されます。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	**interface** *type number* 例： `Device(config)# interface loopback 0`	指定したインターフェイスに対してインターフェイスコンフィギュレーション モードを開始します。 • この例では、ループバック インターフェイス 0 が指定されます。
ステップ 10	**ipigmphelper-addressudl** *interface-type interface-number* 例： `Device(config-if)# ip igmp helper-address udl gigabitethernet 0/0/0`	UDLR で IGMP ヘルパーを設定します。 • このステップで、ダウンストリームデバイスが受信したホストから *interface-type* および *interface-number* 引数で指定されたインターフェイスに関連付けられた UDL に接続されているアップストリーム デバイスへの IGMP レポートをヘルパー処理できるようになります。 • トポロジ例では、IGMP ヘルパーはダウンストリーム デバイスのループバック インターフェイス 0 に設定されます。そのため、ループバック インターフェイス 0 が、ホストからギガビットイーサネット インターフェイス 0/0/0 に接続されているアップストリームデバイスへの IGMP レポートをヘルパー処理するように設定されます。

	コマンドまたはアクション	目的
ステップ 11	**ipigmpproxy-service** 例： `Device(config-if)# ip igmp proxy-service`	mroute プロキシ サービスをイネーブルにします。 • mroute プロキシ サービスがイネーブルのときに、IGMP クエリ インターバルに基づいて **ipigmpmroute-proxy** コマンド（ステップ 7 を参照）で設定されたインターフェイスに一致する、(*, G) 転送エントリのスタティック mroute テーブルが、デバイスによって定期的にチェックされます。一致が存在する場合、1 つの IGMP レポートがこのインターフェイスで作成され、受信されます。 （注） **ipigmpproxy-service** コマンドは、**ipigmphelper-address**（UDL）コマンドと共に使用するように意図されています。 • この例では、**ipigmpmroute-proxy** コマンドで登録されているインターフェイスに対するすべてのグループのインターフェイスに対して IGMP レポートの転送をイネーブルにするように、ループバック インターフェイス 0 で **ipigmpproxy-service** コマンドが設定されます（ステップ 7 を参照してください）。
ステップ 12	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。
ステップ 13	**showipigmpinterface** 例： `Device# show ip igmp interface`	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。

	コマンドまたはアクション	目的
ステップ 14	**showipigmpudlr** 例： `Device# show ip igmp udlr`	（任意）設定された UDL ヘルパー アドレスがあるインターフェイス上で、マルチキャスト グループに直接接続されている UDLR 情報を表示します。

関連トピック

IGMP プロキシ （580 ページ）
例：IGMP プロキシ設定 （587 ページ）

IGMP プロキシの設定例

例：IGMP プロキシ設定

次に、IGMP UDLR に対してアップストリーム UDL デバイスを設定し、IGMP プロキシ サポート付きの IGMP UDLR に対してダウンストリーム UDL デバイスを設定する例を示します。

アップストリーム デバイスの設定

```
interface gigabitethernet 0/0/0
ip address 10.1.1.1 255.255.255.0
ip pim dense-mode
!
interface gigabitethernet 1/0/0
ip address 10.2.1.1 255.255.255.0
ip pim dense-mode
ip igmp unidirectional-link
!
interface gigabitethernet 2/0/0
ip address 10.3.1.1 255.255.255.0
```

ダウンストリーム デバイスの設定

```
ip pim rp-address 10.5.1.1 5
access-list 5 permit 239.0.0.0 0.255.255.255
!
interface loopback 0
ip address 10.7.1.1 255.255.255.0
ip pim dense-mode
ip igmp helper-address udl ethernet 0
ip igmp proxy-service
!
interface gigabitethernet 0/0/0
ip address 10.2.1.2 255.255.255.0
ip pim dense-mode
ip igmp unidirectional-link
!
interface gigabitethernet 1/0/0
ip address 10.5.1.1 255.255.255.0
ip pim sparse-mode
```

```
ip igmp mroute-proxy loopback 0
!
interface gigabitethernet 2/0/0
ip address 10.6.1.1 255.255.255.0
```

関連トピック

IGMP UDLR に対するアップストリーム UDL デバイスの設定 （582 ページ）
IGMP プロキシ サポート付きの IGMP UDLR に対するダウンストリーム UDL デバイスの設定 （583 ページ）
IGMP プロキシ （580 ページ）

その他の参考資料

ここでは、IGMP のカスタマイズに関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP Multicast Command Reference』
IP マルチキャスト テクノロジー分野の概要	「IP Multicast Technology Overview」モジュール
基本的な IP マルチキャストの概念、設定作業、および例	「Configuring Basic IP Multicast」または「Configuring IP Multicast in IPv6 Networks」モジュール

標準および RFC

標準/RFC	タイトル
RFC 1112	『*Host extensions for IP multicasting*』
RFC 2236	『*Internet Group Management Protocol, Version 2*』
RFC 3376	『*Internet Group Management Protocol, Version 3*』

MIB

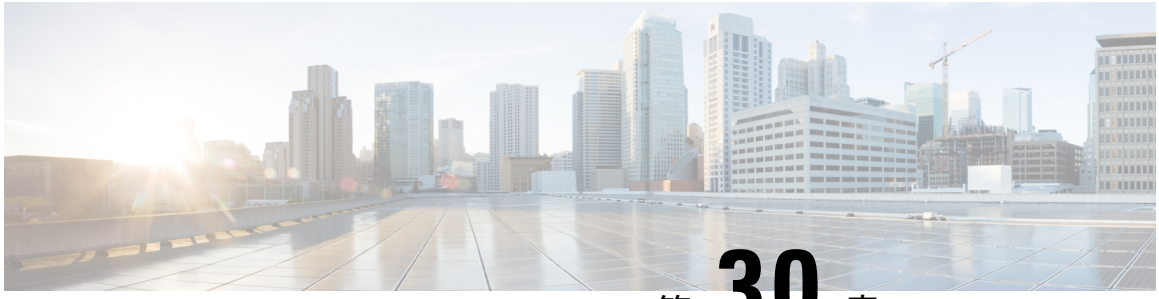
MIB	MIB のリンク
これらの機能によってサポートされる新しい MIB または変更された MIB はありません。またこれらの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右のURLにアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IGMP プロキシの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。



第 30 章

スイッチド イーサネットでの IP マルチキャストの抑制

- 機能情報の確認 （591 ページ）
- スイッチド イーサネット ネットワークで IP マルチキャストを抑制するための前提条件 （592 ページ）
- スイッチド イーサネット ネットワークでの IP マルチキャストについての情報 （592 ページ）
- スイッチド イーサネット ネットワークでマルチキャストを抑制する例 （594 ページ）
- スイッチド イーサネット ネットワークで IP マルチキャストを抑制する設定例 （597 ページ）
- その他の参考資料 （598 ページ）
- スイッチド イーサネット ネットワークでの IP マルチキャストの抑制に関する機能履歴と情報 （599 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

スイッチド イーサネット ネットワークで IP マルチキャストを抑制するための前提条件

このモジュールの作業を実行する前に、「IP Multicast Technology Overview」モジュールで説明している概念をよく理解しておく必要があります。

スイッチドイーサネットネットワークでのIPマルチキャストについての情報

IP マルチキャスト トラフィックとレイヤ 2 スイッチ

レイヤ 2 スイッチのデフォルト動作では、スイッチ上の宛先 LAN に属する各ポートに、すべてのマルチキャスト トラフィックが転送されます。この動作では、スイッチの効率が低下します。その目的は、データを受信する必要があるポートへのトラフィックを制限することです。この動作では、不要なマルチキャスト トラフィックを減らす抑制メカニズムが必要です。これによって、スイッチのパフォーマンスが改善されます。

Cisco Group Management Protocol（CGMP）、Router Group Management Protocol（RGMP）、および IGMP スヌーピングは、レイヤ 2 スイッチング環境で IP マルチキャストを効果的に抑制します。

- CGMP および IGMP スヌーピングは、エンド ユーザまたはレシーバ クライアントが含まれているサブネットで使用されます。
- RGMP は、コラプスト バックボーンなどのルータのみに含まれているルーティング対象セグメントで使用されます。
- RGMP と CGMP は相互運用できません。ただし、インターネット グループ管理プロトコル（IGMP）は、CGMP および RGMP スヌーピングと相互運用できます。

IP マルチキャスト用の Catalyst スイッチの CGMP

CGMP は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたデバイスで使用される、シスコが開発したプロトコルです。IP マルチキャスト データ パケットと IGMP レポート メッセージ（いずれも MAC レベルで同じグループ アドレスにアドレス指定されます）を区別しない Catalyst スイッチの場合、CGMP が必要になります。スイッチはIGMPパケットを区別できますが、スイッチ上でソフトウェアを使用する必要があり、これがパフォーマンスに大きな影響を与えます。

マルチキャスト デバイスとレイヤ 2 スイッチで CGMP を設定する必要があります。結果的に CGMP では、該当するレシーバに接続されている Catalyst スイッチのポートにだけ IP マルチ

キャスト トラフィックが提供されます。トラフィックを明示的に要求していない他のすべてのポートは、これらのポートがマルチキャスト ルータに接続されていない限り、トラフィックを受信しません。マルチキャスト ルータ ポートは、すべての IP マルチキャスト データ パケットを受信する必要があります。

マルチキャスト グループに加入するとき、ホストは CGMP を使用して、送信要求されなくてもターゲット グループへの IGMP メンバーシップ レポート メッセージをマルチキャストします。通常の IGMP 処理では、IGMP レポートが、スイッチを介してルータに渡されます。ルータ（このインターフェイス上で CGMP がイネーブルにされている必要がある）では、IGMP レポートを受信し、通常どおりに処理されますが、CGMP 加入メッセージも作成され、スイッチに送信されます。Join メッセージには、エンド ステーションの MAC アドレスと加入したグループの MAC アドレスが含まれます。

スイッチは、CGMP Join メッセージを受信し、そのマルチキャスト グループ用の連想メモリ（CAM）テーブルにポートを追加します。以後、このマルチキャスト グループに対するすべての後続のトラフィックは、そのホストのポートに転送されます。

レイヤ 2 スイッチは、いくつかの宛先 MAC アドレスを 1 つの物理ポートに割り当てることができるよう、設計されています。この設計により、スイッチを階層構造で接続できるようになります。また、多数のマルチキャスト宛先アドレスを単一ポートに転送できます。

デバイス ポートは、マルチキャスト グループのエントリにも追加されます。IGMP コントロール メッセージもマルチキャスト トラフィックとして送信されるため、マルチキャスト デバイスは、各グループに対するすべてのマルチキャスト トラフィックをリッスンします。その他のマルチキャスト トラフィックは、CGMP で作成された新しいエントリを含む CAM テーブルを使用して転送されます。

関連トピック

CGMP のイネーブル化 （595 ページ）
例：CGMP の設定 （597 ページ）

IGMP スヌーピング

IGMP スヌーピングは、レイヤ 2 LAN スイッチで実行される IP マルチキャスト抑制メカニズムです。IGMP スヌーピングでは、ホストとルータとの間で送信される IGMP パケットで、一部のレイヤ 3 情報（IGMP Join/Leave メッセージ）を調査、すなわち「スヌープ」します。スイッチでは、特定のマルチキャスト グループに対するホストから IGMP ホスト レポートを受信するときに、関連付けられているマルチキャスト テーブル エントリにホストのポート番号が追加されます。スイッチがホストから IGMP グループ脱退メッセージを受信すると、スイッチはホストのテーブル エントリを削除します。

IGMP 制御メッセージはマルチキャスト パケットとして送信されるので、レイヤ 2 ではマルチキャスト データと区別できません。IGMP スヌーピングを実行しているスイッチでは、各マルチキャスト データ パケットを検査し、永続的な IGMP コントロール情報が含まれているかどうかを特定できます。低速の CPU を搭載したローエンドのスイッチに IGMP スヌーピングを実装すると、データが高速で送信される場合に、パフォーマンスに重大な影響を与える可能性があります。解決策として、ハードウェアで IGMP チェックを実行できる特別な ASIC（特定

用途向け集積回路）を備えたハイエンドのスイッチにIGMPスヌーピングを実装します。CGMPは特別なハードウェアを使用しない、ローエンドのスイッチのための新しいオプションです。

Router-Port Group Management Protocol（RGMP）

CGMP および IGMP スヌーピングは、アクティブなレシーバがあるルーティング対象ネットワーク セグメントで動作するように設計されている、IP マルチキャスト抑制メカニズムです。両方とも、ホストとルータとの間で送信される IGMP コントロール メッセージに依存して、該当する受信先に接続されているスイッチ ポートが特定されます。

スイッチドイーサネット バックボーン ネットワーク セグメントは、通常、そのセグメント上にホストなしでスイッチに接続されているいくつかのルータで構成されています。ルータでは IGMP ホスト レポートが生成されないため、CGMP および IGMP スヌーピングによって、マルチキャスト トラフィックを抑制することができず、VLAN 上の各ポートにフラッディングされます。ルータでは、代わりに、Protocol Independent Multicast（PIM）メッセージが生成され、レイヤ 3 レベルで、マルチキャスト トラフィック フローに加入またはマルチキャスト トラフィック フローがプルーニングされます。

Router-Port Group Management Protocol（RGMP）は、ルータのみのネットワーク セグメントに対する、IP マルチキャスト抑制メカニズムです。RGMP は、ルータ上およびレイヤ 2 スイッチ上でイネーブルにする必要があります。マルチキャスト ルータは、特定のグループに RGMP Join メッセージを送信することによって、データ フローを受信したいことを示します。次に、CGMP Join メッセージの処理方法と同様に、スイッチによって、そのマルチキャスト グループに対する転送テーブルに、適切なポートが追加されます。IP マルチキャスト データ フローは、関連するルータ ポートにのみ転送されます。ルータがそのデータ フローを必要としなくなった場合、RGMP Leave メッセージを送信し、スイッチは転送エントリを削除します。

RGMP 対応されていないルータがある場合は、すべてのマルチキャスト データを受信し続けます。

関連トピック

レイヤ 2 スイッチド イーサネット ネットワークでの IP マルチキャストの設定 （596 ページ）
RGMP の設定例 （598 ページ）

スイッチドイーサネットネットワークでマルチキャストを抑制する例

IP マルチキャスト用のスイッチの設定

マルチキャスト ネットワークにスイッチングがある場合、IP マルチキャストの設定方法の詳細について、使用しているスイッチのマニュアルを参照してください。

IGMP スヌーピングの設定

ルータ上での設定は不要です。使用しているスイッチでIGMPスヌーピングをイネーブルにする方法についてはドキュメントを参照し、提示された手順に従ってください。

CGMP のイネーブル化

CGMP は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたデバイス上で使用されるプロトコルです。CGMP が必要となるのは、Catalyst スイッチで IP マルチキャスト データ パケットと IGMP レポート メッセージを区別できないためです。これらはともに MAC レベルで、同じグループ アドレスにアドレス指定されます。

（注）

- CGMP は 802 または ATM メディア、または ATM 経由の LAN エミュレーション（LANE）でのみイネーブルにする必要があります。
- CGMP は、Catalyst スイッチに接続されているデバイス上でのみ、イネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface ethernet 1`	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 4	**ipcgmp** [**proxy** | **router-only**] 例： `Device(config-if)# ip cgmp proxy`	Cisco Catalyst 5000 ファミリ スイッチに接続されているデバイスのインターフェイス上でCGMPをイネーブルにします。 • **proxy** キーワードは、CGMP プロキシ機能をイネーブルにします。イネーブルにすると、CGMP 対応でないデバイスがプロキシ ルータに

	コマンドまたはアクション	目的
		よってアドバタイズされます。プロキシ ルータでは、非 CGMP 対応デバイスの MAC アドレスおよびグループ アドレス 0000.0000.0000 が使用されている CGMP Join メッセージを送信することによって、他の非 CGMP 対応デバイスの存在がアドバタイズされます。
ステップ 5	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、EXEC モードに戻ります。
ステップ 6	**clearipcgmp** [*interface-type interface-number*] 例： `Device# clear ip cgmp`	（任意）Catalyst スイッチのキャッシュからすべてのグループ エントリをクリアします。

関連トピック

IP マルチキャスト用の Catalyst スイッチの CGMP （592 ページ）
例：CGMP の設定 （597 ページ）

レイヤ 2 スイッチド イーサネット ネットワークでの IP マルチキャストの設定

RGMP を使用してレイヤ 2 スイッチド イーサネット ネットワークで IP マルチキャストを設定するには、この作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**interface** *type number* 例： `Device(config)# interface ethernet 1`	ホストに接続されているインターフェイスを選択します。
ステップ 4	**iprgmp** 例： `Device(config-if)# ip rgmp`	イーサネット インターフェイス、ファスト イーサネット インターフェイス、およびギガビット イーサネット インターフェイスで、RGMP をイネーブルにします。
ステップ 5	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、EXEC モードに戻ります。
ステップ 6	**debugiprgmp** 例： `Device# debug ip rgmp`	（任意）RGMP 対応デバイスによって送信されたデバッグ メッセージを記録します。
ステップ 7	**showipigmpinterface** 例： `Device# show ip igmp interface`	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。

関連トピック

Router-Port Group Management Protocol（RGMP） （594 ページ）
RGMP の設定例 （598 ページ）

スイッチド イーサネット ネットワークで IP マルチキャストを抑制する設定例

例：CGMP の設定

次の例は、マルチキャスト ソースとマルチキャスト レシーバが同じ VLAN にある基本的なネットワーク環境向けです。目的とする動作は、スイッチ上でのマルチキャストの転送を、そのマルチキャスト ストリームを要求しているポート宛てに限定することです。

4908G-L3 ルータは、VLAN 50 のポート 3/1 で Catalyst 4003 に接続されます。次の設定は、GigabitEthernet1 インターフェイスに適用されます。ルータがインターフェイスでマルチキャスト トラフィックをルーティングしないため、**ipmulticast-routing** コマンドが設定されないことに注意してください。

```
interface GigabitEthernet1
 ip address 192.168.50.11 255.255.255.0
 ip pim dense-mode
 ip cgmp
```

関連トピック

CGMP のイネーブル化 （595 ページ）
IP マルチキャスト用の Catalyst スイッチの CGMP （592 ページ）

RGMP の設定例

次に、ルータ上で RGMP を設定する方法の例を示します。

```
ip multicast-routing
ip pim sparse-mode
interface ethernet 0
 ip rgmp
```

関連トピック

レイヤ 2 スイッチド イーサネット ネットワークでの IP マルチキャストの設定 （596 ページ）
Router-Port Group Management Protocol（RGMP） （594 ページ）

その他の参考資料

ここでは、スイッチド イーサネット ネットワークでの IP マルチキャストの抑制に関連する参考資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP Multicast Command Reference』
IGMP スヌーピング	『*IP Multicast: IGMP Configuration Guide*』の「IGMP Snooping」モジュール
RGMP	『*IP Multicast: IGMP Configuration Guide*』の「Configuring Router-Port Group Management Protocol」モジュール

MIB

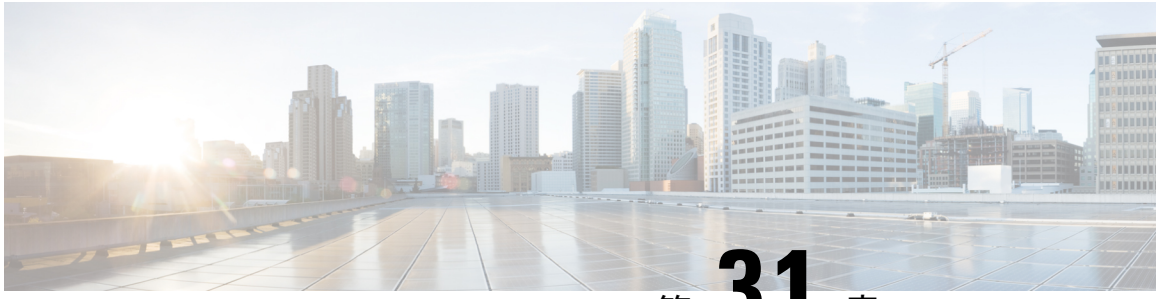
MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
Technical Assistance Center（TAC）ホーム ページ：多数の技術関連の記事と、製品、テクノロジー、ソリューション、テクニカルティップス、ツールへのリンクを提供する Web サイトです。必要な記事は検索して見つけることができます。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/public/support/tac/home.shtml

スイッチドイーサネットネットワークでのIPマルチキャストの抑制に関する機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。



第 31 章

PIM の設定

- 機能情報の確認 （601 ページ）
- PIM の前提条件 （601 ページ）
- PIM に関する制約事項 （602 ページ）
- PIM に関する情報 （606 ページ）
- PIM の設定方法 （625 ページ）
- PIM の動作の確認 （659 ページ）
- PIM のモニタリングとトラブルシューティング （669 ページ）
- PIM の設定例 （671 ページ）
- その他の参考資料 （675 ページ）
- PIM の機能履歴と情報 （677 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

PIM の前提条件

- PIM設定プロセスを開始する前に、使用するPIMモードを決定します。この決定は、ネットワーク上でサポートするアプリケーションに基づきます。次の注意事項に従ってください。
  - 一般に、本質的に 1 対多または多対多アプリケーションでは PIM-SM を正常に使用できます。

- 1 対多アプリケーションで最適なパフォーマンスを得るには、SSM が適しています。ただし、IGMP バージョン 3 サポートが必要です。

- PIM スタブ ルーティングを設定する前に、次の条件を満たしていることを確認します。
  - スタブ ルータと中央のルータの両方に IP マルチキャスト ルーティングが設定されている必要があります。さらに、スタブ ルータのアップリンク インターフェイスに PIM モード（デンス モード、スパース モード、または スパース - デンス モード）が設定されている必要があります。
  - また、デバイスに Enhanced Interior Gateway Routing Protocol（EIGRP）スタブ ルーティングか Open Shortest Path First（OSPF）スタブ ルーティングのいずれかが設定されている必要があります。
  - PIM スタブ ルータは、ディストリビューション ルータ間の伝送トラフィックのルーティングは行いません。ユニキャスト（EIGRP）スタブ ルーティングではこの動作が強制されます。PIM スタブ ルータの動作を支援するためにユニキャスト スタブ ルーティングを設定する必要があります。

（注） EIGRP または OSPF の設定については、『*Catalyst 3850 Routing Configuration Guide, Release 3SE*』を参照してください。

PIM に関する制約事項

次に、PIM を設定する際の制約事項を示します。

- PIM は、LAN Base フィーチャ セットを実行している場合はサポートされません。
- 双方向 PIM はサポートされていません。

PIMv1 および PIMv2 の相互運用性

デバイス上でのマルチキャスト ルーティングの設定ミスを回避するには、ここに記載する情報を確認してください。

シスコの PIMv2 実装を使用すると、バージョン 1 とバージョン 2 間での相互運用性および変換が可能となります。ただし、若干の問題が発生する場合もあります。

PIMv2 に差分的にアップグレードできます。PIM バージョン 1 および 2 を、1 つのネットワーク内の異なるルータおよびマルチレイヤ デバイスに設定できます。内部的には、共有メディア ネットワーク上のすべてのルータおよびマルチレイヤ デバイスで同じ PIM バージョンを実行する必要があります。したがって、PIMv2 デバイスが PIMv1 デバイスを検出した場合は、バージョン 1 デバイスがシャットダウンするかアップグレードされるまで、バージョン 2 デバイスはバージョン 1 にダウングレードされます。

PIMv2 は BSR を使用して各グループ プレフィックスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータおよびマルチレイヤ デバイスにアナウンスします。自動 RP 機能を組み合わせることにより、PIMv2 BSR と同じ作業を PIMv1 で実行できます。ただし、自動 RP は PIMv1 から独立している、スタンドアロンのシスコ独自のプロトコルで、PIMv2 は IETF 標準の追跡プロトコルです。

（注） したがって、PIMv2 の使用を推奨します。BSR 機能は、Cisco ルータおよびマルチレイヤ デバイス上の Auto-RP と相互運用します。

PIMv2 デバイスを PIMv1 デバイスと相互運用させる場合は、自動 RP を事前に導入しておく必要があります。自動 RP マッピング エージェントでもある PIMv2 BSR は、自動 RP で選択された RP を自動的にアドバタイズします。つまり、自動 RP によって、グループ内のルータまたはマルチレイヤ デバイスごとに 1 つの RP が設定されます。ドメイン内のルータおよびデバイスの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

PIMv1 と PIMv2 が混在する領域内の DM グループは、特殊な設定を行わなくても自動的に相互運用します。

PIMv1 の自動 RP 機能は PIMv2 RP 機能と相互運用するため、PIMv1 と PIMv2 が混在する領域内に SM グループを設定できます。すべての PIMv2 デバイスで PIMv1 を使用できますが、RP を PIMv2 にアップグレードすることを推奨します。PIMv2 への移行を簡単に行うには、以下を推奨します。

- 領域全体で Auto-RP を使用します。
- 領域全体でスパース - デンス モードを設定します。

自動 RP がまだ PIMv1 領域に設定されていない場合は、自動 RP を設定してください。

関連トピック

PIM のバージョン （609 ページ）

PIM スタブ ルーティングの設定に関する制約事項

- IP Services イメージには完全なマルチキャスト ルーティングが含まれています。
- 直接接続されたマルチキャスト（IGMP）レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。アクセス ドメインでは、PIM プロトコルはサポートされません。
- PIM スタブ ルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、PIM スタブ ルーティングを設定しているデバイス経由です。
- 冗長 PIM スタブ ルータ トポロジーはサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけがサポートされます。
- IP Base および IP Services の機能セットを実行している場合は、PIM スタブ ルーティングがサポートされます。

関連トピック

PIM スタブ ルーティングのイネーブル化（CLI） （625 ページ）
PIM スタブ ルーティング （610 ページ）

Auto-RP および BSR の設定に関する制約事項

Auto-RP および BSR を設定する場合は、ネットワーク設定と次の制約事項を考慮してください。

Auto-RP の制約事項

次に、Auto-RP の設定に関する制約事項を示します（ネットワーク設定で使用する場合）。

- Auto-RP は、LAN Base フィーチャ セットを実行している場合はサポートされません。
- PIM をスパース モードまたはデンス モードに設定し、Auto-RP を設定しない場合は、RP を手動で設定する必要があります。
- ルーテッド インターフェイスが SM に設定されていると、すべてのデバイスが自動 RP グループの手動 RP アドレスによって設定されている場合も、自動 RP を使用できます。
- ルーテッド インターフェイスが SM で設定され、**ip pim autorp listener** グローバル コンフィギュレーション コマンドを入力する場合、すべてのデバイスが Auto-RP グループの手動 RP アドレスを使用して設定されていなくても、Auto-RP は引き続き使用できます。

BSR 設定の制約事項

次に、BSR の設定に関する制約事項を示します（ネットワーク設定で使用する場合）。

- 候補 BSR を自動 RP 用の RP マッピング エージェントとして設定します。
- グループ プレフィックスが自動 RP によってアドバタイズされた場合は、異なる RP セットによって処理されたこれらのグループ プレフィックスのサブ範囲が、PIMv2 BSR メカニズムによってアドバタイズされないようにする必要があります。PIMv1 および PIMv2 ドメインが混在する環境では、バックアップ RP で同じグループ プレフィックスが処理されるように設定します。このようにすると、RP マッピング データベースの最長一致検索によって、PIMv2 DR はこれらの PIMv1 DR から異なる RP を選択できなくなります。

Auto-RP および BSR の注意事項と制限事項

次に、Auto-RP および BSR の設定に関する制約事項を示します（ネットワーク設定で使用する場合）。

- 使用しているネットワークがすべて Cisco ルータおよびマルチレイヤ デバイスである場合は、Auto-RP または BSR のいずれかを使用できます。
- ネットワークに他社製のルータがある場合は、BSR を使用する必要があります。

- Cisco PIMv1 および PIMv2 ルータとマルチレイヤ デバイス、および他社製のルータがある場合は、自動 RP と BSR の両方を使用する必要があります。ネットワークに他のベンダー製のルータが含まれる場合には、シスコの PIMv2 デバイス上に自動 RP マッピング エージェントと BSR を設定します。BSR と他社製の PIMv2 デバイス間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。

（注） PIMv2 は 2 つの方法で使用できます。1 つはバージョン 2 をネットワーク内で排他的に使用する方法、もう 1 つは PIM バージョンの混在環境を採用してバージョン 2 に移行する方法です。

- ブートストラップ メッセージはホップ単位で送信されるため、PIMv1 デバイスの場合、これらのメッセージはネットワーク内の一部のルータおよびマルチレイヤデバイスに到達しません。このため、ネットワーク内に PIMv1 デバイスがあり、Cisco ルータおよびマルチレイヤ デバイスだけが存在する場合は、Auto-RP を使用してください。
- ネットワーク内に他社製のルータが存在する場合は、Cisco PIMv2 ルータまたはマルチレイヤ デバイスに Auto-RP マッピング エージェントおよび BSR を設定します。BSR と他社製の PIMv2 ルータ間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。
- シスコ PIMv1 ルータおよびマルチレイヤ デバイスと他社製の PIMv2 ルータを相互運用させる場合は、Auto-RP と BSR の両方が必要です。シスコ PIMv2 デバイスを、自動 RP マッピング エージェントと BSR の両方に設定してください。

関連トピック

新規インターネットワークでの Auto-RP の設定（CLI） （631 ページ）
Auto-RP （612 ページ）
候補 BSR の設定（CLI） （645 ページ）
PIMv2 ブートストラップ ルータ （616 ページ）

Auto-RP 拡張の制約事項

Auto-RP とブートストラップ ルータ（BSP）の同時配備はサポートされていません。

関連トピック

新規インターネットワークでの Auto-RP の設定（CLI） （631 ページ）
Auto-RP （612 ページ）

PIM に関する情報

Protocol Independent Multicast の概要

PIM（Protocol Independent Multicast）プロトコルは、受信側が開始したメンバーシップの現在の IP マルチキャスト サービス モードを維持します。PIM は、特定のユニキャスト ルーティング プロトコルに依存しません。つまり、IP ルーティング プロトコルに依存せず、ユニキャスト ルーティング テーブルへの入力に使用されるユニキャスト ルーティング プロトコル（Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Border Gateway Protocol（BGP）、およびスタティック ルート）のいずれも利用できます。PIM は、ユニキャスト ルーティング情報を使用してマルチキャスト転送機能を実行します。

PIM はマルチキャスト ルーティング テーブルと呼ばれていますが、実際には完全に独立したマルチキャスト ルーティング テーブルを作成する代わりに、ユニキャスト ルーティング テーブルを使用してリバース パス フォワーディング（RPF）チェック機能を実行します。他のルーティング プロトコルとは異なり、PIM はルータ間のルーティング アップデートを送受信しません。

PIMは、RFC 4601 の Protocol Independent Multicast - Sparse Mode（PIM-SM）で定義されています。

PIM は、デンス モードまたはスパース モードで動作します。ルータは、スパース グループとデンス グループの両方を同時に処理できます（スパース - デンス モード）。これらのモードは、ルータによるマルチキャスト ルーティング テーブルの書き込み方法と、ルータが直接接続された LAN から受信したマルチキャスト パケットの転送方法を決定します。

PIM 転送（インターフェイス）モードについては、次の項を参照してください。

PIM デンス モード（PIM-DM）

PIM デンス モード（PIM-DM）は、プッシュ モデルを使用してマルチキャスト トラフィックをネットワークの隅々にまでフラッディングします。このプッシュ モデルは、データを要求するレシーバを使用せずにデータをレシーバに配信するための方式です。この方式は、ネットワークのあらゆるサブネットにアクティブなレシーバが存在する特定の配置には効率的です。

デンスモードでは、ルータは、他のすべてのルータが特定のグループのマルチキャストパケットの転送を求めていると想定します。あるルータがマルチキャストパケットを受信した場合、直接接続されたメンバまたは PIM ネイバーが存在しないときは、ソースにプルーニング メッセージが返送されます。後続のマルチキャストパケットは、このプルーニング済みのブランチのこのルータにはフラッディングされません。PIM は、ソース ベースのマルチキャスト配信ツリーを構築します。

PIM-DM は最初に、ネットワーク全体にマルチキャスト トラフィックをフラッディングします。ダウンストリーム ネイバーを持たないルータは、不要なトラフィックをプルーニングします。このプロセスは 3 分ごとに繰り返されます。

ルータは、フラッディングとプルーニングのメカニズムを介してデータ ストリームを受信することでステート情報を累積します。これらのデータ ストリームには送信元およびグループの情報が含まれているため、ダウンストリーム ルータがマルチキャスト転送テーブルを構築できます。PIM-DM ではソース ツリー、つまり（S, G）エントリしかサポートしていないため、共有配信ツリーの構築に使用できません。

（注） デンスモードはほとんど使用されておらず、また、その使用もお勧めしません。このため、関連モジュールの設定作業では指定しません。

PIM スパース モード（PIM-SM）

PIM スパース モード（PIM-SM）は、プル モデルを使用してマルチキャスト トラフィックを配信します。明示的にデータを要求したアクティブなレシーバを含むネットワーク セグメントだけがトラフィックを受信します。

デンス モードのインターフェイスと異なり、スパース モードのインターフェイスは、ダウンストリームのルータから定期的に加入メッセージを受信する場合またはインターフェイスに直接接続のメンバがある場合のみマルチキャスト ルーティング テーブルに追加されます。LAN から転送する場合、グループが認識している RP があれば、SM 動作が行われます。その場合、パケットはカプセル化され、その RP に送信されます。認識している RP がなければ、パケットは DM 方式でフラッディングされます。特定のソースからのマルチキャスト トラフィックが十分である場合、レシーバのファースト ホップ ルータは、ソース ベースのマルチキャスト配信ツリーを構築するために加入メッセージをソースに向けて送信できます。

PIM-SM は、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SM は少なくとも最初は共有ツリーを使用するので、ランデブー ポイント（RP）を使用する必要があります。RP は管理上メットワークで設定されている必要があります。詳細については、ランデブー ポイント（611 ページ）を参照してください。

スパース モードでは、ルータは、トラフィックに対する明示的な要求がない限り、他のルータはグループのマルチキャスト パケットを転送しないと見なします。ホストがマルチキャスト グループに加入すると、直接接続されたルータは RP に PIM 加入メッセージを送信します。RP はマルチキャスト グループを追跡します。マルチキャスト パケットを送信するホストは、そのホストのファースト ホップ ルータによって RP に登録されます。その後、RP は、ソースに加入メッセージを送信します。この時点で、パケットが共有配信ツリー上で転送されます。特定のソースからのマルチキャスト トラフィックが十分である場合、ホストのファースト ホップ ルータは、ソース ベースのマルチキャスト配信ツリーを構築するために加入メッセージをソースに向けて送信できます。

送信元が RP に登録され、データは共有ツリーを下ってレシーバに転送されます。エッジ ルータは、RP を介してソースから共有ツリーでデータ パケットを受信するときに、そのソースについて学習します。次に、エッジ ルータは、そのソースに向けて PIM (S, G)加入メッセージを送信します。リバース パスに沿った各ルータは、RP アドレスのユニキャスト ルーティング メトリックをソース アドレスのメトリックと比較します。送信元アドレスのメトリックの方が良い場合は、ソースに向けて PIM（S, G）加入メッセージを転送します。RP のメトリックと同

じ、または RP のメトリックの方が良い場合は、RP と同じ方向に PIM (S, G)加入メッセージが送信されます。この場合、共有ツリーとソース ツリーは一致すると見なされます。

共有ツリーがソースとレシーバの間の最適なパスでない場合、ルータは動的にソース ツリーを作成し、共有ツリーの下方向へのトラフィック フローを停止します。この動作は、ソフトウェアのデフォルトの動作です。ネットワーク管理者は、**ip pim spt-threshold infinity** コマンドを使用して、トラフィックを強制的に共有ツリー上で保持することができます。

PIM-SM は、WAN リンク付きのネットワークを含む、任意のサイズのネットワークに合わせて拡大または縮小します。明示的な加入メカニズムによって、不要なトラフィックが WAN リンクでフラッディングするのを防ぎます。

Multicast Source Discovery Protocol（MSDP）

Multicast Source Discovery Protocol（MSDP）は、PIM SM を使用する場合のドメイン間送信元検出に使用されます。各 PIM 管理ドメインには独自の RP があります。あるドメイン内の RP が他のドメイン内の RP に新しい送信元を信号で伝えるために、MSDP が使用されます。

MSDP が設定されている状態で、あるドメイン内の RP が新しい送信元の PIM 登録メッセージを受信すると、その RP は、新しい Source-Active（SA）メッセージを他のドメイン内のすべての MSDP ピアに送信します。それぞれの中間 MSDP ピアは、この SA メッセージを発信側の RP から離してフラッディングします。MSDP ピアは、この SA メッセージを自身の MSDP sa-cache にインストールします。他のドメイン内の RP が SA メッセージに記述されているグループへの加入要求を持っている場合（空でない発信インターフェイス リストで (*,G) エントリが存在することで示される）、そのグループはドメインの対象となり、RP から送信元方向に (S,G) Join メッセージが送信されます。

スパース-デンス モード

インターフェイス上でスパース モードまたはデンス モードを設定すると、そのインターフェイス全体にスパース性またはデンス性が適用されます。ただし、環境によっては、単一リージョン内の一部のグループについては PIM をスパース モードで実行し、残りのグループについてはデンス モードで実行しなければならない場合があります。

デンス モードだけ、またはスパース モードだけをイネーブルにする代わりに、スパース-デンス モードをイネーブルにできます。この場合、グループがデンス モードであればインターフェイスはデンス モードとして処理され、グループがスパース モードであればインターフェイスはスパース モードとして処理されます。インターフェイスがスパース-デンス モードである場合にグループをスパース グループとして処理するには、RP が必要です。

スパース-デンス モードを設定すると、ルータがメンバになっているグループにスパース性またはデンス性の概念が適用されます。

スパース - デンス モードのもう 1 つの利点は、Auto-RP 情報をデンス モードで配信しながら、ユーザ グループのマルチキャスト グループをスパース モード方式で使用できることです。したがって、リーフ ルータ上にデフォルト RP を設定する必要はありません。

インターフェイスがデンス モードで処理される場合、次のいずれかの条件が満たされると、そのインターフェイスはマルチキャスト ルーティング テーブルの発信インターフェイス リストに追加されます。

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する。
- PIM ネイバーが存在し、グループがプルーニングされていない。

インターフェイスがスパースモードで処理される場合、次のいずれかの条件が満たされると、そのインターフェイスはマルチキャスト ルーティング テーブルの発信インターフェイス リストに追加されます。

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する。
- インターフェイス上の PIM ネイバーが明示的な加入メッセージを受信した。

PIM のバージョン

PIMv2 は、PIMv1 と比べて次の点が改善されています。

- マルチキャスト グループごとに、複数のバックアップ ランデブー ポイント（RP）を持つアクティブな RP が 1 つ存在します。この単一の RP で、PIMv1 内の同じグループにアクティブな RP が複数ある場合と同様の処理を行います。
- ブートストラップ ルータ（BSP）は耐障害性のある、自動化された RP ディスカバリ メカニズム、および配信機能を提供します。これらの機能により、ルータおよびマルチレイヤ デバイスはグループ/RP マッピングを動的に取得できます。
- スパース モード（SM）およびデンス モード（DM）は、インターフェイスではなく、グループに関するプロパティです。

（注） SM または DM のいずれか一方だけでなく、SM-DM（スパース/デンス モード）を使用してください。

- PIM の Join メッセージおよびプルーニング メッセージを使用すると、複数のアドレス ファミリを柔軟に符号化できます。
- 現在以降の機能オプションを符号化するため、クエリー パケットではなく、より柔軟な hello パケット形式が使用されています。
- RP に送信される登録メッセージが、境界ルータによって送信されるか、あるいは指定ルータによって送信されるかを指定します。
- PIM パケットは IGMP パケット内に格納されず、独立したパケットとして処理されます。

関連トピック

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング （671 ページ）
PIMv1 および PIMv2 の相互運用性 （602 ページ）

PIM スタブ ルーティング

PIM スタブ ルーティング機能は、すべてのデバイス ソフトウェア イメージで使用でき、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの使用状況を低減させます。

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。サポート対象の PIM インターフェイスは、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類です。PIM パッシブ モードに設定されているルーテッド インターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過させたり転送したりするのは IGMP トラフィックだけです。

PIM スタブ ルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、PIM スタブ ルーティングを設定しているデバイス経由です。PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセス ドメイン、または他のレイヤ 2 デバイスに接続されているインターフェイスに接続されます。直接接続されたマルチキャスト（IGMP）レシーバおよび送信元だけが、レイヤ2アクセスドメインで許可されます。PIM受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

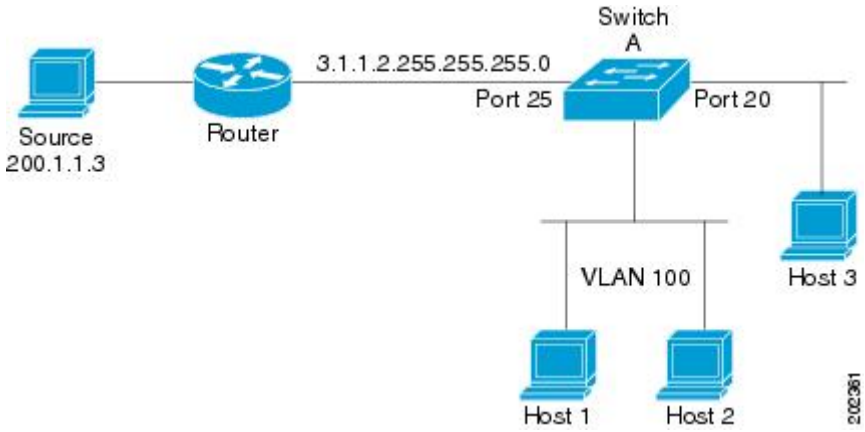
PIM スタブ ルーティングを使用しているときは、IP マルチキャスト ルーティングを使用し、デバイスだけを PIM スタブ ルータとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。デバイスは分散ルータ間の伝送トラフィックをルーティングしません。デバイスのルーテッドアップリンク ポートも設定する必要があります。SVI の場合は、デバイスのアップリンク ポートを使用できません。SVI アップリンク ポートの PIM が必要な場合は、IP Services フィーチャ セットにアップグレードする必要があります。

（注） また、PIM スタブ ルーティングをデバイスに設定するときは、EIGRP スタブ ルーティングも設定する必要があります。

冗長 PIM スタブ ルータ トポロジーはサポートされません。単一のアクセス ドメインにマルチキャスト トラフィックを転送している複数の PIM ルータがある場合、冗長トポロジーが存在します。PIM メッセージはブロックされ、PIM 資産および指定ルータ検出メカニズムは、PIM 受動インターフェイスでサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけがサポートされます。非冗長トポロジーを使用することで、PIM受動インターフェイスはそのアクセス ドメインで唯一のインターフェイスおよび指定ルータであると想定します。

図 *24 : PIM* スタブ ルータ設定

次の図では、デバイス A ルーテッド アップリンク ポート 25 がルータに接続され、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 で有効になっています。この設定により、直接接続されたホストはマルチキャスト発信元 200.1.1.3 からトラフィックを受信できます。



関連トピック

PIM スタブ ルーティングのイネーブル化（CLI） （625 ページ）
例：PIM スタブ ルーティングのイネーブル化 （671 ページ）
例：PIM スタブ ルーティングの確認 （672 ページ）
PIM スタブ ルーティングの設定に関する制約事項 （603 ページ）

IGMP ヘルパー

PIM スタブ ルーティングはルーティングされたトラフィックをエンド ユーザの近くに移動させ、ネットワーク トラフィックを軽減します。スタブ ルータ（スイッチ）に IGMP ヘルパー機能を設定する方法でもトラフィックを軽減できます。

ip igmp helper-address *ip-address* インターフェイス コンフィギュレーション コマンドを使用してスタブ ルータ（スイッチ）を設定すると、スイッチによるネクストホップ インターフェイスへのレポート送信をイネーブルにできます。ダウンストリーム ルータに直接接続されていないホストはアップストリーム ネットワークの送信元マルチキャスト グループに加入できます。この機能が設定されていると、マルチキャスト ストリームへの加入を求めるホストからの IGMP パケットはアップストリームのネクストホップ デバイスに転送されます。アップストリームのセントラル ルータは、ヘルパー IGMP レポートまたは leave を受信すると、そのグループの発信インターフェイス リストからインターフェイスの追加または削除を行います。

ランデブー ポイント

ランデブー ポイント（RP）は、デバイスが PIM（Protocol Independent Multicast）スパース モード（SM）で動作している場合にデバイスが実行するロールです。RP が必要になるのは、PIM SM を実行しているネットワークだけです。PIM-SM モデルでは、マルチキャスト データを明示的に要求したアクティブなレシーバを含むネットワーク セグメントだけにトラフィックが転送されます。マルチキャスト データの配信方法は、PIM デンス モード（PIM DM）とは対照的です。PIM DM では、マルチキャスト トラフィックが最初にネットワークのすべてのセグメントにフラッディングされます。ダウンストリーム ネイバーを持たないルータ、または直接レシーバに接続されているルータは、不要なトラフィックをプルーニングします。

RP は、マルチキャスト データのソースとレシーバの接点として機能します。PIM SIM ネットワークでは、ソースが RP にトラフィックを送信する必要があります。このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。デフォルトでは、レシーバのファースト ホップ デバイスがソースを認識すると、ソースに Join メッセージを直接送信し、ソースからレシーバへのソース ベースの配信ツリーを作成します。ソースとレシーバ間の最短パス内に RP が配置されていない限り、このソース ツリーに RP は含まれません。

ほとんどの場合、ネットワークにおける RP の配置は複雑な判断を必要としません。デフォルトでは、RP が必要になるのは、ソースおよびレシーバとの新しいセッションを開始する場合だけです。その結果、RP では、トラフィックのフローまたは処理によるオーバーヘッドはほとんど発生しません。PIM バージョン 2 で実行される処理は PIM バージョン 1 よりも少なくなっています。これは、ソースを定期的に RP に登録するだけでステートを作成できるためです。

関連トピック

候補 RP の設定（CLI） （647 ページ）
ランデブー ポイントの設定 （627 ページ）
例：候補 RP の設定 （675 ページ）

Auto-RP

PIM-SMの最初のバージョンでは、すべてのリーフルータ（ソースまたはレシーバに直接接続されたルータ）は、RP の IP アドレスを使用して手動で設定する必要がありました。このような設定は、スタティック RP 設定とも呼ばれます。スタティック RP の設定は、小規模のネットワークでは比較的容易ですが、大規模で複雑なネットワークでは困難を伴う可能性があります。

PIM-SM バージョン 1 の導入に続き、シスコは、Auto-RP 機能を備えた PIM-SM のバージョンを実装しました。Auto-RP は、PIM ネットワークにおけるグループから RP へのマッピングの配信を自動化します。Auto-RP には、次の利点があります。

- さまざまなグループにサービスを提供するために、ネットワーク内で複数の RP を設定することが比較的容易です。
- Auto-RP では、複数の RP 間で負荷を分散し、グループに加入するホストの場所に従って RP を配置できます。
- Auto-RP により、接続の問題の原因となる、矛盾した手動 RP 設定を回避できます。

複数の RP を使用して、異なるグループ範囲にサービスを提供したり、互いにバックアップとしての役割を果たしたりできます。Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。その場合、RP マッピング エージェントは、グループから RP への一貫したマッピングを他のすべてのルータに送信します。これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。

（注） PIM をスパース モードまたはデンス モードに設定し、Auto-RP を設定しない場合は、RP を静的に設定する必要があります。

（注） ルータ インターフェイスがスパース モードに設定されている場合、Auto-RP グループに対してすべてのルータが 1 つのスタティック アドレスで設定されているときは、引き続き Auto-RP グループを使用できます。

Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。その後、RP マッピング エージェントは、デンスモードフラッディングにより、グループから RP への一貫したマッピングを他のすべてのルータに送信するようになります。これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。インターネット割り当て番号局（IANA）は、224.0.1.39 と 224.0.1.40 という 2 つのグループ アドレスを Auto-RP 用に割り当てています。Auto-RP の利点の 1 つは、指定した RP に対するすべての変更は、RP であるルータ上で設定するだけで、リーフ ルータ上で設定する必要がないことです。Auto-RP のもう 1 つの利点は、ドメイン内で RP アドレスのスコープを設定する機能を提供することです。スコーピングを設定するには、Auto-RP アドバタイズメントに許容されている存続可能時間（TTL）値を定義します。

RP の各設定方式には、それぞれの長所、短所、および複雑度のレベルがあります。従来の IP マルチキャスト ネットワーク シナリオにおいては、Auto-RP を使用して RP を設定することを推奨します。Auto-RP は、設定が容易で、十分にテストされており、安定しているためです。代わりの方法として、スタティック RP、Auto-RP、およびブートストラップ ルータを使用して RP を設定することもできます。

関連トピック

新規インターネットワークでの Auto-RP の設定（CLI） （631 ページ）
例：Auto-RP の設定 （673 ページ）
例：Auto-RP でのスパース モード （673 ページ）
Auto-RP および BSR の設定に関する制約事項 （604 ページ）
Auto-RP 拡張の制約事項 （605 ページ）

PIM ネットワークでの Auto-RP の役割

Auto-RP は、PIM ネットワークにおけるグループからランデブー ポイント（RP）へのマッピングの配信を自動化します。Auto-RP が機能するためには、RP アナウンスメント メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてデバイスが指定されている必要があります。その後、RP マッピング エージェントは、デンス モード フラッディングにより、一貫した group-to-RP マッピングを他のすべてのデバイスに送信します。

これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。インターネット割り当て番号局（IANA）は、224.0.1.39 と 224.0.1.40 という 2 つのグループ アドレスを Auto-RP 用に割り当てています。

マッピング エージェントは、Candidate-RP から RP になる意図の通知を受信します。その後、マッピング エージェントが RP 選定の結果を通知します。この通知は、他のマッピング エージェントによる決定とは別に行われます。

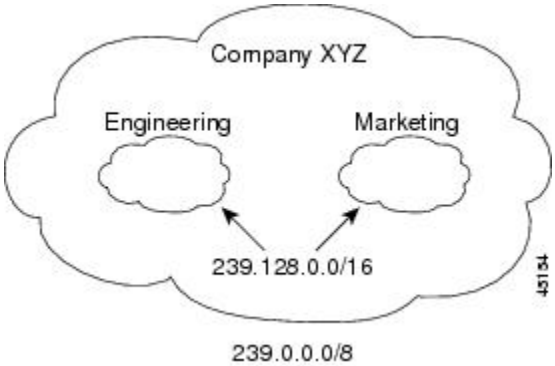
マルチキャスト境界

管理用スコープの境界を使用し、ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限できます。この方法では、「管理用スコープのアドレス」と呼ばれる特殊なマルチキャストアドレス範囲が境界のメカニズムとして使用されます。管理用スコープの境界をルーテッド インターフェイスに設定すると、マルチキャスト グループ アドレスがこの範囲内にあるマルチキャスト トラフィックは、このインターフェイスに出入りできず、このアドレス範囲内のマルチキャスト トラフィックに対するファイアウォール機能が提供されます。

（注） マルチキャスト境界および TTL しきい値は、マルチキャスト ドメインの有効範囲を制御しますが、TTL しきい値はこの デバイス でサポートされていません。ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限するには、TTL しきい値でなくマルチキャスト境界を使用する必要があります。

図 *25*：管理用スコープの境界

次の図に、XYZ 社が自社ネットワーク周辺にあるすべてのルーテッドインターフェイス上で、管理用スコープの境界をマルチキャスト アドレス範囲 239.0.0.0/8 に設定した例を示します。この境界では、239.0.0.0 ～ 239.255.255.255 の範囲のマルチキャスト トラフィックはネットワークに入ったり、外へ出ることができません。同様に、エンジニアリング部およびマーケティング部では、各自のネットワークの周辺で、管理用スコープの境界を 239.128.0.0/16 に設定しました。この境界では、239.128.0.0 ～ 239.128.255.255 の範囲のマルチキャスト トラフィックは、それぞれのネットワークに入ったり、外部に出ることができません。



マルチキャスト グループ アドレスに対して、ルーテッド インターフェイス上に管理用スコープの境界を定義できます。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。この境界が定義されている場合、マルチキャスト データ パケットはいずれの方向で

あっても境界を通過できません。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

IANA は、マルチキャスト アドレス範囲 239.0.0.0 ～ 239.255.255.255 を管理用スコープのアドレスとして指定しました。このアドレス範囲は、異なる組織によって管理されたドメイン内で再利用できます。このアドレスはグローバルではなく、ローカルで一意であると見なされます。

filter-autorp キーワードを設定して、管理用スコープの境界で Auto-RP 検出と通知メッセージを検査し、フィルタできます。境界のアクセス コントロール リスト（ACL）に拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

関連トピック

IP マルチキャスト境界の定義（CLI）（643 ページ）
例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義（673 ページ）

Auto-RP のスパース - デンス モード

Auto-RP の前提条件として、**ip pim sparse-dense-mode** インターフェイス コンフィギュレーション コマンドを使用してすべてのインターフェイスをスパース-デンス モードで設定する必要があります。スパース-デンス モードで設定されたインターフェイスは、マルチキャスト グループの動作モードに応じてスパース モードまたはデンス モードで処理されます。マルチキャスト グループ内に既知の RP が存在する場合、インターフェイスはスパース モードで処理されます。グループ内に既知の RP が存在しない場合、デフォルトでは、インターフェイスはデンス モードで処理され、このインターフェイス上にデータがフラッディングされます（デンス モード フォールバックを回避することもできます。「Configuring Basic IP Multicast」モジュールを参照してください）。

Auto-RP を正常に実装し、224.0.1.39 および 224.0.1.40 以外のグループがデンス モードで動作することを回避するには、「シンク RP」（「ラストリゾート RP」とも呼ばれます）を設定することを推奨します。シンク RP は、ネットワーク内に実際に存在するかどうかわからない静的に設定された RP です。デフォルトでは、Auto-RP メッセージはスタティック RP 設定よりも優先されるため、シンク RP の設定は Auto-RP の動作と干渉しません。未知のソースや予期しないソースをアクティブにできるため、ネットワーク内の可能なすべてのマルチキャスト グループにシンク RP を設定することを推奨します。ソースの登録を制限するように設定された RP がない場合は、グループがデンス モードに戻り、データがフラッディングされる可能性があります。

関連トピック

既存のスパース モード クラウドへの Auto-RP の追加（CLI）（634 ページ）

Auto-RP の利点

Auto-RP は IP マルチキャストを使用し、グループ/RP マッピングを PIM ネットワーク内のすべてのシスコ ルータおよびマルチレイヤ デバイス に自動配信します。Auto-RP には次の利点があります。

- ネットワーク内で複数の RP を使用し、複数のグループ範囲を処理する作業が簡単になります。
- 複数の RP 間で負荷を分散し、グループに加入するホストの場所に従って RP を配置できます。
- PIM ネットワーク内のすべてのルータおよびマルチレイヤ デバイス で矛盾が発生しなくなり、手動による RP 設定が不要になります。この結果、接続問題を引き起こす要因が取り除かれます。

PIM ネットワークでの Auto-RP の利点

- Auto-RP では、RP 指定に対するすべての変更を、RP であるデバイス上でのみ設定されるようにし、リーフ ルータ上では設定されないようにすることができます。
- Auto-RP には、ドメイン内の RP アドレスのスコープを設定する機能があります。

PIMv2 ブートストラップ ルータ

PIMv2 ブートストラップ ルータ（BSR）は、グループ/RP マッピング情報をネットワーク内のすべての PIM ルータおよびマルチレイヤ デバイス に配信する別の方法です。これにより、ネットワーク内のルータまたは デバイス ごとに RP 情報を手動で設定する必要がなくなります。ただし、BSR は IP マルチキャストを使用してグループ/RP マッピング情報を配信する代わりに、特殊な BSR メッセージをホップ単位でフラッディングしてマッピング情報を配信します。

BSR は、BSR として機能するように設定されたドメイン内の一連の候補ルータおよび デバイス から選択されます。選択メカニズムは、ブリッジングされた LAN で使用されるルートブリッジ選択メカニズムと類似しています。BSR の選択メカニズムの基準は、ネットワークを経由してホップ単位で送信される BSR メッセージに格納されている、デバイスの BSR プライオリティです。各 BSR デバイスは BSR メッセージを調べ、自身の BSR プライオリティよりも BSR プライオリティが同等以上で、BSR IP アドレスが大きなメッセージだけを、すべてのインターフェイスから転送します。この方法によって、BSR が選択されます。

選択された BSR によって、TTL 値が 1 である BSR メッセージが送信されます。隣接する PIMv2 ルータまたはマルチレイヤ デバイス は BSR メッセージを受信し、TTL 値が 1 である他のすべてのインターフェイス（BSR メッセージの着信インターフェイスを除く）にマルチキャストします。この方法で、BSR メッセージは PIM ドメイン内をホップ単位で移動します。BSR メッセージには現在の BSR の IP アドレスが格納されているため、候補 RP はフラッディング メカニズムを使用し、どのデバイスが選択された BSR であるかを自動的に学習します。

候補 RP は候補 RP アドバタイズメントを送信し、対象となるグループ範囲を BSR に指示します。この情報は、ローカルな候補 RP キャッシュに格納されます。BSR はドメイン内の他のす

べての PIM デバイスに、BSR メッセージ内のこのキャッシュの内容を定期的にアドバタイズします。これらのメッセージはネットワークをホップ単位で移動し、すべてのルータおよびデバイス に送信されます。BSR メッセージ内の RP 情報は、ローカルの RP キャッシュに格納されます。すべてのルータおよび デバイス には一般的な RP ハッシュ アルゴリズムが使用されるため、指定されたグループには同じ RP が選択されます。

関連トピック

候補 BSR の設定（CLI） （645 ページ）
PIMv2 BSR の設定 （640 ページ）
例：候補 BSR の設定 （674 ページ）
Auto-RP および BSR の設定に関する制約事項 （604 ページ）

PIM ドメイン境界

IP マルチキャストの普及に伴い、PIMv2 ドメインと別の PIMv2 ドメインが境界を挟んで隣接する場合が増えています。2 つのドメインは同じ RP、BSR、候補 RP、候補 BSR のセットを共有していないことが多いため、PIMv2 BSR メッセージがドメインの内外に流れないようにする必要があります。メッセージのドメイン境界通過を許可すると、通常の BSR 選択メカニズムに悪影響が及んだり、境界に位置するすべてのドメインで単一の BSR が選択されたり、候補 RP アドバタイズメントが混在し、間違ったドメイン内で RP が選択されたりします。

関連トピック

PIM ドメイン境界の定義（CLI） （641 ページ）

マルチキャスト転送

マルチキャスト トラフィックの転送は、マルチキャスト対応ルータによって行われます。このようなルータは、すべてのレシーバにトラフィックを配信するために、IP マルチキャストがネットワーク上でたどるパスを制御する配信ツリーを作成します。

マルチキャスト トラフィックは、すべてのソースをグループ内のすべてのレシーバに接続する配信ツリー上で、ソースからマルチキャスト グループに流れます。このツリーは、すべてのソースで共有できます（共有ツリー）。または、各ソースに個別の配信ツリーを作成することもできます（ソース ツリー）。共有ツリーは一方向または双方向です。

ソース ツリーと共有ツリーの構造を説明する前に、マルチキャスト ルーティング テーブルで使用する表記について触れておきます。これらの表記には次のものが含まれます。

- (S, G) = (マルチキャスト グループ G のユニキャスト ソース, マルチキャスト グループ G)
- (*, G) = (マルチキャスト グループ G のすべてのソース, マルチキャスト グループ G)

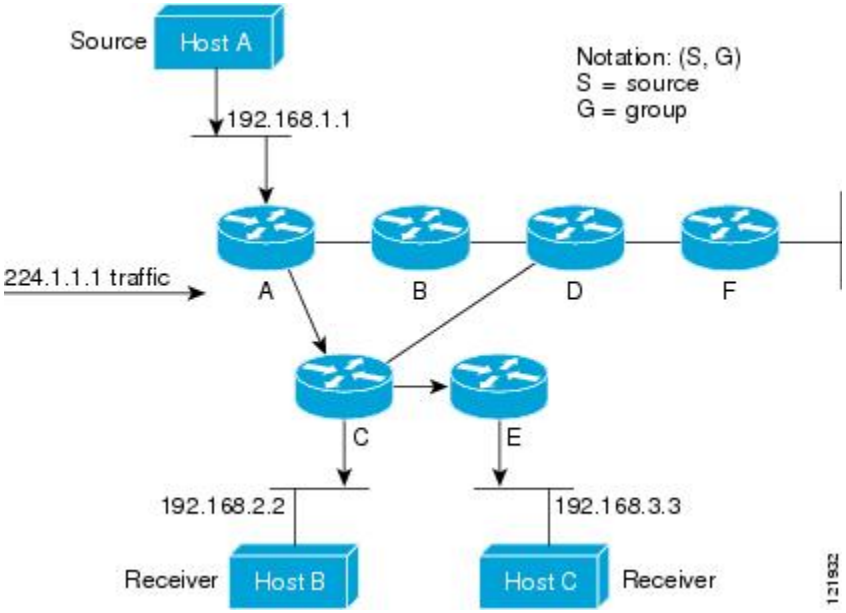
(S, G) という表記（「S カンマ G」と読みます）は、最短パス ツリーの列挙です。S はソースの IP アドレス、G はマルチキャスト グループ アドレスを表します。

共有ツリーは (*, G) で表されます。ソース ツリーは (S, G) で表され、常にソースでルーティングされます。

マルチキャスト配信のソース ツリー

マルチキャスト配信ツリーの最も単純な形式は、ソース ツリーです。ソース ツリーは、ソースホストをルートとし、ネットワークを介してレシーバに接続するスパニングツリーを形成するブランチを持ちます。このツリーはネットワーク上での最短パスを使用するため、最短パスツリー（SPT）とも呼ばれます。

次の図に、ソース（ホスト A）をルートとし、2 つのレシーバ（ホスト B およびホスト C）に接続するグループ 224.1.1.1 の SPT の例を示します。



標準表記を使用すると、図の例の SPT は（192.168.1.1, 224.1.1.1）となります。

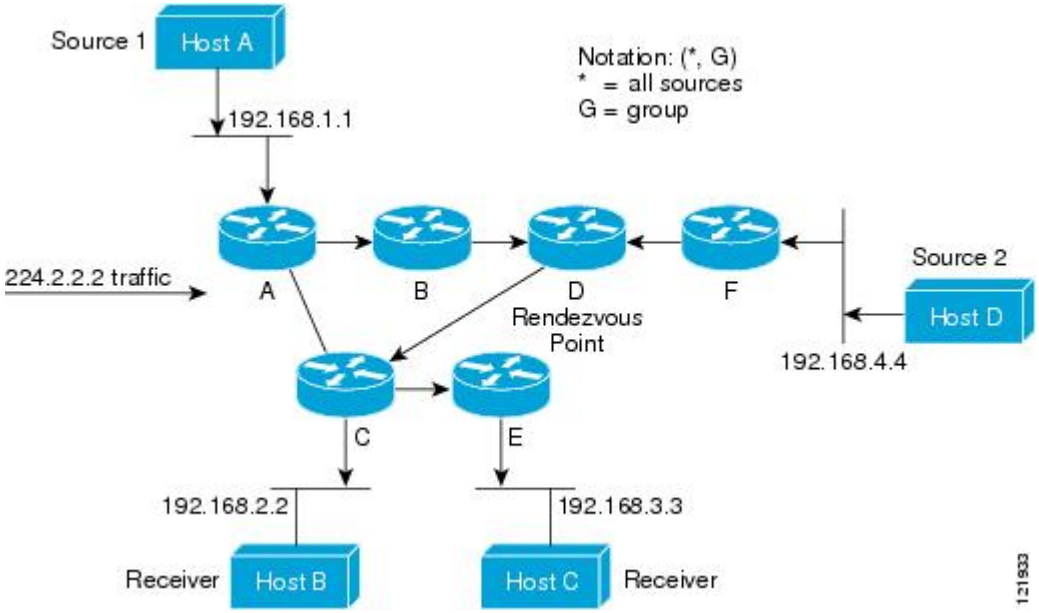
(S, G) という表記は、各グループに送信する個々のソースに個別の SPT が存在することを意味します。

マルチキャスト配信の共有ツリー

ソースをルートとするソースツリーとは異なり、共有ツリーはネットワーク内の選択されたポイントに配置された単一の共通ルートを使用します。この共有されたルートは、ランデブーポイント（RP）と呼ばれます。

次の図に、ルータ D にルートが配置されたグループ 224.2.2.2 の共有ツリーを示します。この共有ツリーは単方向です。ソーストラフィックは、ソースツリー上の RP に向けて送信されます。このトラフィックは、次に RP から共有ツリーを下方向に転送され、すべてのレシーバに到達します（レシーバがソースと RP の間に配置されていない場合は、直接サービスが提供されます）。

図 *26 :* 共有ツリー



この例では、ソース（ホスト A およびホスト D）からのマルチキャスト トラフィックがルート（ルータ D）に移動した後に共有ツリーから 2 つのレシーバ（ホスト B およびホスト C）へと到達します。マルチキャスト グループ内のすべての送信元が一般的な共有ツリーを使用するため、(*, G) というワイルドカード表記（「アスタリスク、カンマ、G」と読みます）でそのツリーを表します。この場合、* はすべてのソースを意味し、G はマルチキャスト グループを表します。したがって、図の共有ツリーは (*, 224.2.2.2) と表記します。

ソース ツリーと共有ツリーは、どちらもループフリーです。ツリーが分岐する場所でのみ、メッセージが複製されます。マルチキャスト グループのメンバは常に加入または脱退する可能性があるため、配信ツリーを動的に更新する必要があります。特定のブランチに存在するすべてのアクティブ レシーバが特定のマルチキャスト グループに対してトラフィックを要求しなくなると、ルータは配信ツリーからそのブランチをプルーニングし、そのブランチから下方向へのトラフィック転送を停止します。そのブランチの特定のレシーバがアクティブになり、マルチキャストトラフィックを要求すると、ルータは配信ツリーを動的に変更し、トラフィック転送を再開します。

ソース ツリーの利点

ソースツリーには、ソースとレシーバの間に最適なパスを作成するという利点があります。この利点により、マルチキャストトラフィックの転送におけるネットワーク遅延を最小限に抑えることができます。ただし、この最適化は代償を伴います。ルータがソースごとにパス情報を維持する必要があるのです。何千ものソース、何千ものグループが存在するネットワークでは、このオーバーヘッドがすぐにルータ上でのリソースの問題につながる可能性があります。ネットワーク設計者は、マルチキャスト ルーティング テーブルのサイズによるメモリ消費について考慮する必要があります。

共有ツリーの利点

共有ツリーには、各ルータにおいて要求されるステートの量が最小限に抑えられるという利点があります。この利点により、共有ツリーだけが許容されるネットワークの全体的なメモリ要件が緩和されます。共有ツリーの欠点は、特定の状況でソースとレシーバの間のパスが最適パスではなくなり、パケット配信に遅延を生じる可能性があることです。たとえば、上の図のホスト A（ソース 1）とホスト 2（レシーバ）間の最短パスはルータ A とルータ B です。共有ツリーのルートとしてルータ D を使用するため、トラフィックはルータ A、B、D、そして次に C を通過する必要があります。ネットワーク設計者は、共有ツリー専用環境を実装する際にランデブー ポイント（RP）の配置を慎重に考慮する必要があります。

ユニキャスト ルーティングでは、トラフィックは、ネットワーク上でソースから宛先ホストまでの単一パスに沿ってルーティングされます。ユニキャスト ルータは、ソース アドレスを考慮せず、宛先アドレスおよびその宛先へのトラフィックの転送方法だけを考慮します。ルータは、ルーティング テーブル全体をスキャンして宛先アドレスを取得し、適正なインターフェイスから宛先の方向へユニキャスト パケットのコピーを転送します。

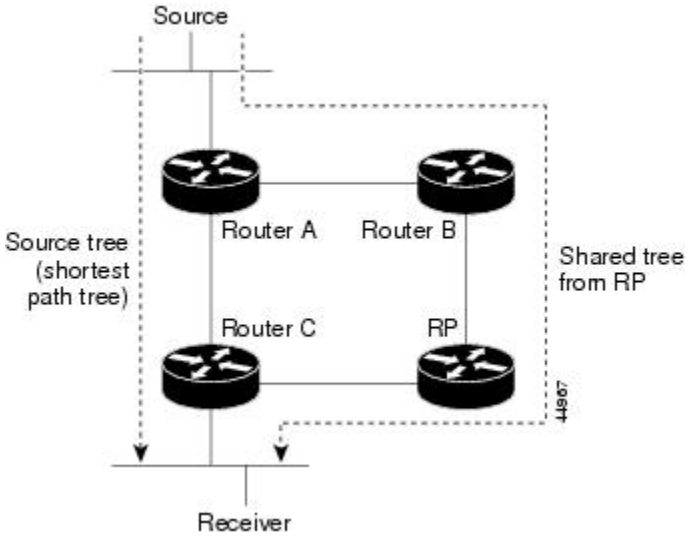
マルチキャスト転送では、ソースは、マルチキャスト グループ アドレスによって表される任意のホスト グループにトラフィックを送信します。マルチキャスト ルータは、どの方向が（ソースへ向かう）アップストリーム方向で、どの方向（1 方向または複数の方向）が（レシーバへ向かう）ダウンストリーム方向であるかを決定する必要があります。複数のダウンストリームパスがある場合、ルータはパケットを複製し、それを適切なダウンストリームパス（最善のユニキャスト ルート メトリック）で下方向に転送します。これらのパスがすべてであるとは限りません。レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャスト トラフィック転送は、Reverse Path Forwarding（RPF）と呼ばれます。RPF については、次の項を参照してください。

PIM 共有ツリーおよびソース ツリー

デフォルトでは、グループのメンバーで受信されるデータは、RP でルーティングされた単一のデータ配信ツリーを経由して、送信側からグループに送られます。

図 *27*: 共有ツリーおよびソース ツリー（最短パスツリー）

次の図に、このタイプの共有配信ツリーを示します。送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。



データ レートによって保証されている場合は、送信元でルーティングされるデータ配信ツリーを、共有ツリーのリーフ ルータ（ダウンストリーム接続がないルータ）で使用できます。このタイプの配信ツリーは、SPT または送信元ツリーと呼ばれます。デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、ソース ツリーにデバイスします。

共有ツリーから送信元ツリーへの移動プロセスは、次のとおりです。

1. レシーバがグループに加入します。リーフ ルータ C は Join メッセージを RP に向けて送信します。
2. RP はルータ C とのリンクを発信インターフェイス リストに格納します。
3. 送信元がデータを送信します。ルータ A はデータをカプセル化して登録メッセージに格納し、RP に送信します。
4. RP はデータをルータ C に向けて共有ツリーの下方向に転送し、送信元に向けて Join メッセージを送信します。この時点で、データはルータ C に 2 回着信する可能性があります（カプセル化されたデータ、およびネイティブ状態のデータ）。
5. データがネイティブ状態（カプセル化されていない状態）で着信すると、RP は登録停止メッセージをルータ A に送信します。
6. デフォルトでは、最初のデータ パケット受信時に、ルータ C が Join メッセージを送信元に送信するよう要求します。
7. ルータ C が（S, G）でデータを受信すると、ルータ C は共有ツリーの上位方向にある送信元に prune メッセージを送信します。
8. RP が（S, G）の発信インターフェイスからルータ C へのリンクを削除します。RP は送信元に向けてプルーニング メッセージを送信します。

送信元および RP に join および prune メッセージが送信されます。これらのメッセージはホップ単位で送信され、送信元または RP へのパス上にある各 PIM デバイスで処理されます。register および register-stop メッセージは、ホップバイホップで送信されません。これらのメッセージは、送信元に直接接続されている指定ルータによって送信され、グループの RP によって受信されます。

グループへ送信する複数の送信元で、共有ツリーが使用されます。共有ツリー上に存在するように、PIM デバイスを設定できます。

最初のデータ パケットがラスト ホップ ルータに着信すると、共有ツリーからソース ツリーへと変更されます。この変更は、**ip pim spt-threshold** グローバル コンフィギュレーション コマンドを使用して設定したしきい値によって異なります。

SPT には共有ツリーよりも多くのメモリが必要ですが、遅延が短縮されます。SPT の使用を延期することもできます。リーフ ルータを SPT にすぐ移動せず、トラフィックがしきい値に最初に到達したあとで移動するように指定できます。

PIM リーフ ルータが、指定グループの SPT に加入する時期を設定できます。送信元の送信速度が指定速度（キロビット/秒）以上の場合、マルチレイヤ スイッチは PIM Join メッセージを送信元に向けて送信し、送信元ツリー（SPT）を構築します。送信元からのトラフィック速度がしきい値を下回ると、リーフルータは共有ツリーに再び切り替わり、プルーニング メッセージを送信元に送信します。

SPT しきい値を適用するグループを指定するには、グループ リスト（標準アクセス リスト）を使用します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。

関連トピック

PIM 最短パス ツリーの使用の延期（CLI）（655 ページ）

Reverse Path Forwarding

ユニキャスト ルーティングでは、トラフィックは、ネットワーク上でソースから宛先ホストまでの単一パスに沿ってルーティングされます。ユニキャスト ルータは、ソース アドレスを考慮せず、宛先アドレスおよびその宛先へのトラフィックの転送方法だけを考慮します。ルータは、ルーティング テーブル全体をスキャンして宛先ネットワークを取得し、適正なインターフェイスから宛先の方向へユニキャスト パケットのコピーを転送します。

マルチキャスト転送では、ソースは、マルチキャスト グループ アドレスによって表される任意のホスト グループにトラフィックを送信します。マルチキャスト ルータは、どの方向が（ソースへ向かう）アップストリーム方向で、どの方向（1 方向または複数の方向）が（レシーバへ向かう）ダウンストリーム方向であるかを決定する必要があります。複数のダウンストリームパスがある場合、ルータはパケットを複製し、それを適切なダウンストリームパス（最善のユニキャスト ルート メトリック）で下方向に転送します。これらのパスがすべてであるとは限りません。レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャスト トラフィック転送は、Reverse Path Forwarding（RPF）と呼ばれます。RPF は、マルチキャスト データグラムの転送に使用されるアルゴリズムです。

Protocol Independent Multicast（PIM）は、ユニキャスト ルーティング情報を使用して、レシーバからソースへ向かうリバース パスに沿って配信ツリーを作成します。その後、マルチキャス

トルータは、その配信ツリーに沿ってソースからレシーバにパケットを転送します。RPFは、マルチキャスト転送における重要な概念です。RPFにより、ルータは、配信ツリーの下方向へ正しくマルチキャスト トラフィックを転送できます。RPF は、既存のユニキャスト ルーティング テーブルを使用して、アップストリーム ネイバーとダウンストリーム ネイバーを決定します。ルータは、アップストリームインターフェイスで受信した場合にのみ、マルチキャスト パケットを転送します。この RPF チェックにより、配信ツリーがループフリーであることを保証できます。

RPF チェック

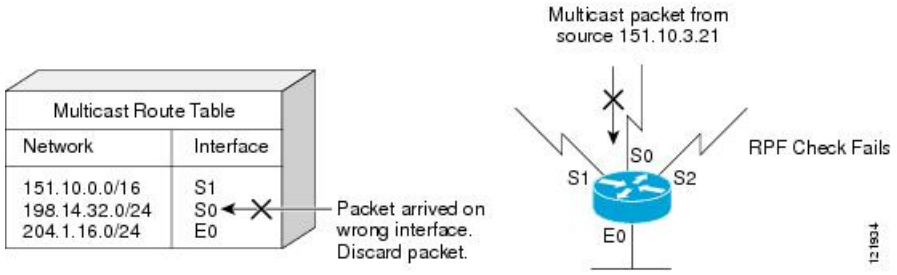
マルチキャスト パケットがルータに到達すると、ルータはそのパケットに対して RPF チェックを実行します。RPFチェックが成功すると、パケットが転送されます。そうでない場合、パケットはドロップされます。

ソース ツリーを下方向へ流れるトラフィックに対する RPF チェック手順は次のとおりです。

1. ルータは、ユニキャスト ルーティング テーブルでソース アドレスを検索して、ソースへのリバースパス上にあるインターフェイスにパケットが到達したかどうかを判定します。
2. ソースに戻すインターフェイスにパケットが到達した場合、RPF チェックは成功し、マルチキャスト ルーティング テーブル エントリの発信インターフェイス リストに示されているインターフェイスからパケットが転送されます。
3. ステップ 2 で RPF チェックに失敗した場合は、パケットがドロップされます。

図に、RPF チェックの失敗例を示します。

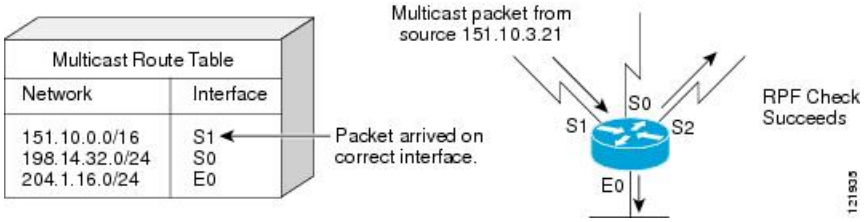
図 *28 : RPF* チェックの失敗



図に示すように、ソース 151.10.3.21 からのマルチキャスト パケットはシリアル インターフェイス 0（S0）上で受信されています。ユニキャスト ルート テーブルのチェック結果は、このルータが 151.10.3.21 にユニキャスト データを転送するために使用するインターフェイスは S1 であることを示しています。パケットはインターフェイス S0 に到達しているため、このパケットは廃棄されます。

図に RPF チェックの成功例を示します。

図 *29 : RPF* チェックの成功



この例では、マルチキャスト パケットはインターフェイス S1 に到達しています。ルータはユニキャスト ルーティング テーブルを参照し、S1 が適正なインターフェイスであることを知ります。RPF チェックが成功し、パケットが転送されます。

PIM はソース ツリーと RP でルーティングされた共有ツリーを使用して、データグラムを転送します。RPF チェックは、それぞれ異なる方法で実行されます。

- PIM ルータまたはマルチレイヤデバイスがソース ツリー ステートである場合（つまり（S, G）エントリがマルチキャスト ルーティング テーブル内にある場合）、マルチキャスト パケットの送信元の IP アドレスに対して RPF チェックが実行されます。
- PIM ルータまたはマルチレイヤ デバイスが共有ツリー ステートである場合（およびソース ツリー ステートが明示されていない場合）、（メンバがグループに加入している場合は既知である）RP アドレスについて RPF チェックが実行されます。

DVMRP およびデンス モードの PIM ではソース ツリーだけが使用され、RPF が使用されます。

（注） デバイスでは DVMRP はサポートされません。

PIM SM は RPF 参照機能を使用し、加入およびプルーニング メッセージを送信する必要があるかどうかを決定します。

- （S, G）join（送信元ツリー ステート）は送信元に向けて送信されます。
- （*,G）Join メッセージ（共有ツリー ステート）は RP に向け送信されます。

PIM ルーティングのデフォルト設定

次の表に、デバイスの PIM ルーティングのデフォルト設定を示します。

表 *41 :* マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義

機能	デフォルト設定
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル
PIM マルチキャスト境界	なし。
候補 BSR	ディセーブル
候補 RP	ディセーブル
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

PIM の設定方法

PIM スタブ ルーティングのイネーブル化（CLI）

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	PIM スタブ ルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
		次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip pim passive** 例： `Device(config-if)# ip pim passive`	インターフェイスに PIM スタブ機能を設定します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip pim interface** 例：	（任意）各インターフェイスで有効になっている PIM スタブを表示します。

	コマンドまたはアクション	目的
	`Device# show ip pim interface`	
ステップ 7	**show ip igmp groups detail** 例： `Device# show ip igmp groups detail`	（任意）特定のマルチキャスト送信元グループに参加した対象クライアントを表示します。
ステップ 8	**show ip mroute** 例： `Device# show ip mroute`	（任意）IPマルチキャストルーティング テーブルを表示します。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

PIM スタブ ルーティング （610 ページ）
例：PIM スタブ ルーティングのイネーブル化 （671 ページ）
例：PIM スタブ ルーティングの確認 （672 ページ）
PIM スタブ ルーティングの設定に関する制約事項 （603 ページ）

ランデブー ポイントの設定

インターフェイスがスパース - デンス モードで、グループをスパース グループとして扱う場合には、ランデブー ポイント（RP）を設定する必要があります。次の方法を使用できます。

- RP をマルチキャスト グループに手動で割り当てる
- PIMv1 から独立した、以下を含むスタンドアロンとしてのシスコ独自のプロトコル
  - 新規インターネットワークでの自動 RP の設定
  - 既存のスパースモード クラウドへの自動 RP の追加

- 問題のある RP への Join メッセージの送信禁止
- 着信 RP アナウンスメント メッセージのフィルタリング

- Internet Engineering Task Force（IETF）の標準追跡プロトコルの使用（PIMv2 BSR の設定を含む）

（注） 動作中の PIM バージョン、およびネットワーク内のルータ タイプに応じて、自動 RP、BSR、またはこれらを組み合わせて使用できます。ネットワーク内の異なるバージョンの PIM を利用する方法については、PIMv1 および PIMv2 の相互運用性 （602 ページ）を参照してください。

関連トピック

候補 RP の設定（CLI） （647 ページ）
ランデブー ポイント （611 ページ）

マルチキャスト グループへの RP の手動割り当て（CLI）

ダイナミック メカニズム（自動 RP や BSR など）を使用してグループのランデブー ポイント（RP）を取得する場合、RP を手動で割り当てる必要はありません。

マルチキャスト トラフィックの送信側は、送信元の先頭ホップ ルータ（指定ルータ）から受信して RP に転送される登録メッセージを通し、自身の存在をアナウンスします。マルチキャストパケットの受信側はRPを使用し、マルチキャスト グループに加入します。この場合は、明示的な Join メッセージが使用されます。

（注） RP はマルチキャスト グループのメンバーではなく、マルチキャスト送信元およびグループ メンバーの合流地点として機能します。

アクセス リストで定義される複数のグループに、単一の RP を設定できます。グループに RP が設定されていない場合、マルチレイヤ デバイスはデンスとしてグループに応答し、デンス モードの PIM 技術を使用します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim rp-address** *ip-address* [*access-list-number*] [**override**] 例： `Device(config)# ip pim rp-address 10.1.1.1 20 override`	PIM RP のアドレスを設定します。 デフォルトで、PIM RP アドレスは設定されていません。すべてのルータおよびマルチレイヤ デバイス（RP を含む）で、RP の IP アドレスを設定する必要があります。 （注） グループに RP が設定されていない場合、デバイスは PIM DM 技術を使用し、グループをデンスとして処理します。 1 台の PIM デバイスを、複数のグループの RP にできます。1 つの PIM ドメイン内で一度に使用できる RP アドレスは、1 つだけです。アクセス リスト条件により、デバイスがどのグループの RP であるかを指定します。 • *ip-address* には、RP のユニキャスト アドレスをドット付き 10 進表記で入力します。 • （任意）*access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • （任意）**override** キーワードを指定すると、このコマンドによって設定された RP と、自動 RP または BSR で取得された RP との間に矛盾が生じた場合に、このコマンドによって設定された RP が優先されます。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例：	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。

	コマンドまたはアクション	目的
	`Device(config)# access-list 25 permit 10.5.0.1 255.224.0.0`	• *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、RP が使用されるマルチキャスト グループのアドレスを入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：マルチキャスト グループへの RP の手動割り当て （672 ページ）

新規インターネットワークでの Auto-RP の設定（CLI）

新規インターネットワーク内に自動 RP を設定している場合は、すべてのインターフェイスが SM-DM に設定されるため、デフォルトの RP は不要です。

（注） PIM ルータをローカル グループの RP として設定する場合は、次の手順のステップ 3 を省略します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show running-config** 例： `Device# show running-config`	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内にあることを確認します。RP は、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって設定済みです。 （注） SM-DM 環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。この RP は、グローバル グループ（224.x.x.x やその他のグローバル グループなど）に対して使用されます。この RP で処理されるグループ アドレス範囲は再設定しないでください。自動 RP によって動的に検出された RP は、静的に設定された RP よりも優先されます。ローカル グループ用に 2 番めの RP を使用することもできます。
ステップ 3	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds* 例： `Device(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120`	別の PIM デバイスをローカル グループの候補 RP として設定します。 • *interface-id* には、RP アドレスを識別するインターフェイスタイプおよび番号を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • **scope** *ttl* には、ホップの存続可能時間の値を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。 • **group-list** *access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • **interval** *seconds* には、アナウンスメント メッセージを送信する頻度を指定します。デフォルトは 60 秒です。指定できる範囲は 1 ～ 16383 です。
ステップ 5	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit 10.10.0.0`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。

	コマンドまたはアクション	目的
		• *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 （注） アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 6	**ip pim send-rp-discovery scope** *ttl* 例： `Device(config)# ip pim send-rp-discovery scope 50`	接続が中断される可能性がないデバイスを検索し、RP マッピング エージェントの役割を割り当てます。 **scope** *ttl* には、ホップの存続可能時間の値を指定し、RPディスカバリ パケットを制限します。ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリ メッセージを受信します。これらのメッセージは他のデバイスに対し、矛盾（グループ/RP 範囲の重なりなど）を回避するために使用されるグループ/RP マッピングを通知します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 9	**show ip pim rp mapping** 例： `Device# show ip pim rp mapping`	関連するマルチキャストルーティングエントリとともに保管されているアクティブな RP を表示します。
ステップ 10	**show ip pim rp** 例： `Device# show ip pim rp`	ルーティングテーブルに保管されている情報を表示します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

Auto-RP （612 ページ）
例：Auto-RP の設定 （673 ページ）
例：Auto-RP でのスパース モード （673 ページ）
Auto-RP および BSR の設定に関する制約事項 （604 ページ）
Auto-RP 拡張の制約事項 （605 ページ）

既存のスパース モード クラウドへの Auto-RP の追加（CLI）

ここでは、最初に自動 RP を既存の SM クラウドに導入し、既存のマルチキャスト インフラストラクチャができるだけ破壊されないようにする方法について説明します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show running-config** 例：	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内にあることを

	コマンドまたはアクション	目的
	`Device# show running-config`	確認します。RP は、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって設定済みです。 （注） SM-DM 環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。この RP は、グローバル グループ（224.x.x.x やその他のグローバル グループなど）に対して使用されます。この RP で処理されるグループ アドレス範囲は再設定しないでください。自動 RP によって動的に検出された RP は、静的に設定された RP よりも優先されます。ローカル グループ用に 2 番めの RP を使用することもできます。
ステップ 3	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds* 例： `Device(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120`	別の PIM デバイスをローカル グループの候補 RP として設定します。 • *interface-id* には、RP アドレスを識別するインターフェイス タイプおよび番号を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • **scope** *ttl* には、ホップの存続可能時間の値を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。 • **group-list** *access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。

	コマンドまたはアクション	目的
		アクセスリストが設定されていない場合は、すべてのグループにRPが使用されます。 • **interval** *seconds* には、アナウンスメントメッセージを送信する頻度を指定します。デフォルトは60秒です。指定できる範囲は1～16383です。
ステップ 5	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit 224.0.0.0 15.255.255.255`	標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 6	**ip pim send-rp-discovery scope** *ttl* 例： `Device(config)# ip pim send-rp-discovery scope 50`	接続が中断される可能性がないデバイスを検索し、RP マッピング エージェントの役割を割り当てます。 **scope** *ttl* には、ホップの存続可能時間の値を指定し、RPディスカバリ パケットを制限します。ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリ メッセージを

	コマンドまたはアクション	目的
		受信します。これらのメッセージは他のデバイスに対し、矛盾（グループ/RP 範囲の重なりなど）を回避するために使用されるグループ/RP マッピングを通知します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。 （注） RP マッピング エージェントとして設定されたデバイスを削除するには、**no ip pim send-rp-discovery** グローバル コンフィギュレーション コマンドを使用します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**show ip pim rp mapping** 例： `Device# show ip pim rp mapping`	関連するマルチキャスト ルーティング エントリとともに保管されているアクティブな RP を表示します。
ステップ 10	**show ip pim rp** 例： `Device# show ip pim rp`	ルーティング テーブルに保管されている情報を表示します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

Auto-RP のスパース - デンス モード （615 ページ）

問題のある RP への Join メッセージの送信禁止（CLI）

ip pim accept-rp コマンドがネットワーク全体に設定されているかどうかを判別するには、**show running-config** 特権 EXEC コマンドを使用します。**ip pim accept-rp** コマンドが設定されていないデバイスがある場合は、後でこの問題を解決できます。ルータまたはマルチレイヤデバイスが **ip pim accept-rp** コマンドによってすでに設定されている場合は、このコマンドを再入力し、新規にアドバタイズされる RP を許可する必要があります。

自動 RP によってアドバタイズされるすべての RP を許可し、他のすべての RP をデフォルトで拒否するには、**ip pim accept-rp auto-rp** グローバル コンフィギュレーション コマンドを使用します。

この手順は任意です。

関連トピック

例：問題のある RP への Join メッセージの送信禁止 （674 ページ）

着信 RP アナウンスメント メッセージのフィルタリング（CLI）

マッピング エージェントにコンフィギュレーション コマンドを追加すると、故意に不正設定されたルータが候補 RP として動作し問題を引き起こさないようにできます。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim rp-announce-filter rp-list** *access-list-number***group-list** *access-list-number* 例： `Device(config)# ip pim`	着信RPアナウンスメントメッセージをフィルタリングします。 ネットワーク内のマッピング エージェントごとに、このコマンドを入力します。このコマンドを使用しないと、すべ

	コマンドまたはアクション	目的
	`rp-announce-filter rp-list 10 group-list 14`	ての着信RPアナウンスメントメッセージがデフォルトで許可されます。 **rp-list** *access-list-number* には、候補 RP アドレスのアクセス リストを設定します。アクセス リストが許可されている場合は、**group-list** *access-list-number* 変数で指定されたグループ範囲に対してアクセス リストを使用できます。この変数を省略すると、すべてのマルチキャスト グループにフィルタが適用されます。 複数のマッピング エージェントを使用する場合は、グループ/RPマッピング情報に矛盾が生じないようにするため、すべてのマッピングエージェント間でフィルタを統一する必要があります。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit 10.8.1.0 255.255.224.0`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • どのルータおよびマルチレイヤ デバイスからの候補 RP アナウンスメント（rp-list アクセス コントロール リスト（ACL））がマッピングエージェントによって許可されるかを指定するアクセス リストを作成します。 • 許可または拒否するマルチキャスト グループの範囲を指定するアクセス リスト（グループリスト ACL）を作成します。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。

	コマンドまたはアクション	目的
		• （任意）*source-wildcard* には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：着信 RP アナウンスメント メッセージのフィルタリング （674 ページ）

PIMv2 BSR の設定

PIMv2 BSR を設定するプロセスには、次のオプションの作業が含まれることがあります。

- PIM ドメイン境界の定義
- IP マルチキャスト境界の定義
- 候補 BSR の設定
- 候補 RP の設定

関連トピック

候補 BSR の設定（CLI） （645 ページ）
PIMv2 ブートストラップ ルータ （616 ページ）

PIM ドメイン境界の定義（CLI）

PIM ドメイン境界を設定するには、次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイスコンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェ

	コマンドまたはアクション	目的
		イスでIGMPスヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip pim bsr-border** 例： `Device(config-if)# ip pim bsr-border`	PIM ドメイン用の PIM ブートストラップ メッセージ境界を定義します。 境界に位置する他の PIM ドメインに接続されているインターフェイスごとに、このコマンドを入力します。このコマンドを実行すると、デバイスは、このインターフェイス上で PIMv2 BSR メッセージを送受信しないように指示されます。 （注） PIM 境界を削除するには、 **no ip pim bsr-border** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

PIM ドメイン境界 （617 ページ）

IP マルチキャスト境界の定義（CLI）

自動 RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。自動 RP 情報を伝達する 224.0.1.39 および 224.0.1.40 宛てのパケットを拒否するアクセス リストを作成します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**access-list** *access-list-number* **deny** *source* [*source-wildcard*]
	例：
	`Device(config)#`
	`access-list 12 deny 224.0.1.39`
	`access-list 12 deny 224.0.1.40`
		標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。
		• *access-list-number* の範囲は 1 ～ 99 です。
		• **deny** キーワードは、条件が一致した場合にアクセスを拒否します。
		• *source* には、自動 RP 情報を伝達するマルチキャスト アドレス 224.0.1.39 および 224.0.1.40 を入力します。
		• （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。
		アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。

	コマンドまたはアクション	目的
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 5	**ip multicast boundary** *access-list-number* 例： `Device(config-if)# ip multicast boundary 12`	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

マルチキャスト境界 （614 ページ）
例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義 （673 ページ）

候補 BSR の設定（CLI）

候補 BSR を、1 つまたは複数設定できます。候補 BSR として機能するデバイスは、他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim bsr-candidate** *interface-id hash-mask-length* [*priority*] 例： `Device(config)# ip pim bsr-candidate gigabitethernet 1/0/3 28 100`	候補 BSR となるようにデバイスを設定します。 • *interface-id* には、スイッチを候補 BSR に設定するときに BSR アドレスの取得元となるデバイス上のインターフェイスを入力します。このイ

	コマンドまたはアクション	目的
		ンターフェイスは PIM を使用してイネーブルにする必要があります。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • *hash-mask-length* には、ハッシュ機能を呼び出す前にグループ アドレスとの AND 条件となるマスク長（最大 32 ビット）を指定します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。 • （任意）*priority* を指定する場合は、0 ～ 255 の番号を入力します。プライオリティが大きな BSR が優先されます。このプライオリティ値が同じである場合は、大きな IP アドレスを持つデバイスが BSR として選択されます。デフォルトは 0 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

PIMv2 ブートストラップ ルータ （616 ページ）
PIMv2 BSR の設定 （640 ページ）

例：候補 BSR の設定 （674 ページ）
Auto-RP および BSR の設定に関する制約事項 （604 ページ）

候補 RP の設定（CLI）

候補 RP を、1 つまたは複数設定できます。BSR と同様、RP は他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。RP は IP マルチキャスト アドレス空間全体、またはその一部を処理します。候補 RP は候補 RP アドバタイズを BSR に送信します。

この手順は任意です。

始める前に

RP となるデバイスを決定するときは、次の可能性を考慮してください。

- 自動RPだけが使用されているCiscoルータおよびマルチレイヤデバイスで構成されるネットワークでは、すべてのデバイスを RP として設定できます。
- シスコの PIMv2 ルータおよびマルチレイヤ デバイスと、他のベンダーのルータだけで構成されるネットワークでは、すべてのデバイスを RP として使用できます。
- シスコの PIMv1 ルータ、PIMv2 ルータ、および他のベンダーのルータで構成されるネットワークでは、シスコ PIMv2 ルータおよびマルチレイヤデバイスを RP として設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim rp-candidate** *interface-id* [**group-list** *access-list-number*] 例： `Device(config)# ip pim rp-candidate gigabitethernet 1/0/5 group-list 10`	候補RP となるようにデバイスを設定します。 • *interface-id* には、対応する IP アドレスが候補RP アドレスとしてアドバタイズされるインターフェイスを指定します。有効なインターフェイ

	コマンドまたはアクション	目的
		スは、物理ポート、ポート チャネル、VLAN などです。 • （任意）**group-list** *access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。group-list を指定しない場合は、デバイスがすべてのグループの候補 RP となります。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit 239.0.0.0 0.255.255.255`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ランデブー ポイント （611 ページ）
ランデブー ポイントの設定 （627 ページ）
例：候補 RP の設定 （675 ページ）

Auto-RP によるスパース モードの設定（CLI）

始める前に

- スパース - デンス モードで設定されたインターフェイスは、マルチキャスト グループの動作モードに応じてスパース モードまたはデンス モードで処理されます。インターフェイスを設定する方法を決定する必要があります。
- Auto-RP を設定するときに必要なすべてのアクセス リストは、設定作業を開始する前に設定しておく必要があります。

（注）

- グループ内に既知の RP がなく、インターフェイスがスパース - デンス モードに設定されている場合、インターフェイスはデンス モードであるように扱われ、データはインターフェイスを介してフラッディングされます。このデータのフラッディングを避けるために、Auto-RP リスナーを設定してから、インターフェイスをスパース モードとして設定します。
- Auto-RP を設定するには、Auto-RP リスナーの機能を設定し（ステップ 5）、スパース モードを指定するか（ステップ 7）、またはスパース - デンス モードを指定する（ステップ 8）必要があります。
- スパース-デンス モードを指定する場合、デンス モードのフェールオーバーがネットワークのデンス モードのフラッディングを引き起こす可能性があります。この状況を避けるため、Auto-RP リスナー機能で PIM スパース モードを使用します。

自動ランデブー ポイント（Auto-RP）を設定するには、次の手順に従います。Auto-RP は任意でエニーキャスト RP でも使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmulticast-routing** [**distributed**] 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。 • **distributed** キーワードを使用して、マルチキャスト分散スイッチングをイネーブルにします。
ステップ 4	ステップ 5 ～ 7 を実行するか、またはステップ 6 および 8 を実行します。	--
ステップ 5	**ippimautorplistener** 例： `Device(config)# ip pim autorp listener`	2 つの Auto-RP グループ 224.0.1.39 と 224.0.1.40 の IP マルチキャスト トラフィックを PIM スパース モードで動作しているインターフェイスでフラッディングされる PIM デンス モードにします。 • ステップ 8 でスパース-デンス モードを設定している場合、このステップはスキップします。
ステップ 6	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 7	**ippimsparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	インターフェイスで PIM スパース モードをイネーブルにします。スパース モードで Auto-RP を設定している場合、次のステップで Auto-RP リスナーも設定する必要があります。

	コマンドまたはアクション	目的
		• ステップ 8 でスパース-デンス モードを設定している場合、このステップはスキップします。
ステップ 8	**ippimsparse-dense-mode** 例： `Device(config-if)# ip pim sparse-dense-mode`	インターフェイスで PIM スパース-デンス モードをイネーブルにします。 • ステップ 7 でスパース モードを設定している場合は、このステップをスキップします。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 10	すべての PIM インターフェイス上でステップ 1 ～ 9 を繰り返します。	--
ステップ 11	**ippimsend-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**] 例： `Device(config)# ip pim send-rp-announce loopback0 scope 31 group-list 5`	RP アナウンスメントをすべての PIM 対応インターフェイスに送信します。 • RP デバイスでのみこのステップを実行します。 • RP アドレスとして使用する IP アドレスを定義するには、*interface-type* 引数と *interface-number* 引数を使用します。 • 直接接続されている IP アドレスを RP アドレスとして指定するには、*ip-address* 引数を使用します。 （注） このコマンドに *ip-address* 引数が設定されている場合、RP 通知メッセージがこのアドレスが接続されているインターフェイスによって送信されます（つまり、RP 通知メッセージの IP ヘッダーのソース アドレスがそのインターフェイスの IP アドレスです）。

	コマンドまたはアクション	目的
		• 次の例は、最大ホップ数が 31 でインターフェイスがイネーブルであることを示します。デバイスは、ループバック インターフェイス 0 に関連付けられた IP アドレスによって RP として識別されることを望みます。アクセス リスト 5 はこのデバイスが RP として機能しているグループを示しています。
ステップ 12	**ippimsend-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*] 例： `Device(config)# ip pim send-rp-discovery loopback 1 scope 31`	デバイスを RP マッピング エージェントとして設定します。 • RP マッピング エージェント デバイス上、または RP/RP マッピング エージェント複合デバイス上で、このステップを実行します。 （注） Auto-RP によって、RP 機能は 1 台のデバイス上で単独で実行でき、RP マッピング エージェントは 1 台または複数のデバイス上で実行できます。RP/RP マッピング エージェント複合デバイス上で、RP および RP マッピング エージェントを展開することができます。 • RP マッピング エージェントのソース アドレスとして使用する IP アドレスを定義するには、オプションの *interface-type* 引数と *interface-number* 引数を使用します。 • Auto-RP 検出メッセージの IP ヘッダーで存続可能時間（TTL）値を指定するには、**scope** キーワードと *ttl-value* 引数を使用します。 • Auto-RP 検出メッセージが送信される間隔を指定するには、オプションの **interval** キーワードと *seconds* 引数を使用します。

	コマンドまたはアクション	目的
		（注） Auto-RP 検出メッセージが送信される間隔をデフォルト値の 60 秒から減らすと、group-to-RP マッピングのより頻繁なフラッディングが発生します。一部のネットワーク環境では、間隔を短縮する欠点（コントロール パケット オーバーヘッドの増加）が利点（グループと RP のマッピングのより頻繁な更新）を上回る場合があります。 • 例では、ループバック インターフェイス 1 で Auto-RP 検出メッセージを 31 ホップに制限していることを示しています。
ステップ 13	**ippimrp-announce-filterrp-list** *access-list* **group-list** *access-list* 例： `Device(config)# ip pim rp-announce-filter rp-list 1 group-list 2`	候補 RP（C-RP）から RP マッピング エージェントに送信された着信 RP アナウンスメント メッセージをフィルタリングします。 • このステップは、RP マッピング エージェントでのみ実行します。
ステップ 14	**noippimdm-fallback** 例： `Device(config)# no ip pim dm-fallback`	（任意）PIM デンス モード フォールバックを防ぎます。 • すべてのインターフェイスが PIM スパース モードで動作するよう設定されている場合、このステップはスキップします。 （注） （**ippimsparse-mode** コマンドを使用して）すべてのインターフェイスが PIM スパース モードで動作するよう設定されている場合、**noippimdm-fallback** コマンド動作がデフォルトでイネーブルになります。

	コマンドまたはアクション	目的
ステップ 15	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 16	**ipmulticastboundary** *access-list* [**filter-autorp**] 例： `Device(config-if)# ip multicast boundary 10 filter-autorp`	管理用スコープの境界を設定します。 • このステップは、他のデバイスとの境界であるインターフェイス上で実行します。 • この作業ではアクセスリストは表示されません。 • **deny** キーワードを使用するアクセスリストエントリはそのエントリに一致するパケットのマルチキャスト境界を作成します。
ステップ 17	**end** 例： `Device(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 18	**showippimautorp** 例： `Device# show ip pim autorp`	（任意）Auto-RP 情報を表示します。
ステップ 19	**showippimrp** [**mapping**] [*rp-address*] 例： `Device# show ip pim rp mapping`	（任意）ネットワークで既知の RP を表示し、デバイスが各 RP について学習する方法を示します。
ステップ 20	**showipigmpgroups** [*group-name* | *group-address*|*interface-type interface-number*] [**detail**] 例： `Device# show ip igmp groups`	（任意）デバイスに直接接続されている、インターネット グループ管理プロトコル（IGMP）を通じて学習されたレシーバを持つマルチキャスト グループを表示します。 • レシーバ情報が結果の画面に表示されるには、レシーバがこのコマンドが発行された時点でネットワーク上でアクティブである必要があります。

	コマンドまたはアクション	目的
ステップ 21	**showipmroute**[*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*] 例： `Device# show ip mroute cbone-audio`	（任意）IPマルチキャストルーティング（mroute）テーブルの内容を表示します。

PIM 最短パス ツリーの使用の延期（CLI）

マルチキャストルーティングが送信元ツリーから最短パスツリーに切り替わる前に到達する必要があるトラフィック レートしきい値を設定するには、次の手順を実行します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 16 permit 225.0.0.0 0.255.255.255`	標準アクセス リストを作成します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、しきい値が適用されるマルチキャスト グループを指定します。

	コマンドまたはアクション	目的
		• （任意）*source-wildcard* には、sourceに適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 4	**ip pim spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list-number*] 例： `Device(config)# ip pim spt-threshold infinity group-list 16`	最短パスツリー（SPT）に移行するまでに到達する必要があるしきい値を指定します。 • *kbps* を指定する場合は、トラフィック レートをキロビット/秒で指定します。デフォルト値は 0 キロビット/秒です。 （注） 有効範囲は 0 ～ 4294967 ですが、デバイス ハードウェアの制限により、0キロビット/秒以外は無効です。 • **infinity** を指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。 • （任意）**group-list** *access-list-number* には、ステップ 2 で作成したアクセス リストを指定します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

PIM 共有ツリーおよびソース ツリー （620 ページ）

PIM ルータクエリー メッセージ間隔の変更（CLI）

PIM ルータおよびマルチレイヤ デバイスでは、各 LAN セグメント（サブネット）の指定ルータ（DR）になるデバイスを検出するため、PIM ルータクエリー メッセージが送信されます。DR は、直接接続された LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。

PIM DM 動作では、IGMPv1 が使用中の場合だけ、DR は意味を持ちます。IGMPv1 には IGMP クエリア選択プロセスがないため、選択された DR は IGMP クエリアとして機能します。PIM-SM 動作では、マルチキャスト送信元に直接接続されたデバイスが DR になります。DR は PIM 登録メッセージを送信し、送信元からのマルチキャスト トラフィックを共有ツリーの下方向へ転送する必要があることを RP に通知します。この場合、DR は最大の IP アドレスを持つデバイスです。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip pim query-interval** *seconds* 例： `Device(config-if)# ip pim query-interval 45`	デバイスが PIM ルータクエリー メッセージを送信する頻度を設定します。 デフォルトは 30 秒です。指定できる範囲は 1 ～ 65535 です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM の動作の確認

PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト動作の確認

PIM-SM ネットワーク環境または PIM-SSM ネットワーク環境で IP マルチキャストの動作を確認する際、まずラストホップルータから検証を開始し、SPTに沿って次々にルータの検証を続け、最後にファースト ホップ ルータの検証を行う方法が効果的です。この確認の目的は、IP マルチキャスト ネットワークを介して IP マルチキャスト トラフィックが適切にルーティングされていることを確認することです。

PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト動作を確認するには、次の作業を実行します。これらの作業は、ソースとレシーバが想定どおりに動作しない場合に障害のあるホップを検出するのに役立ちます。

（注） パケットが想定された宛先に到達しない場合は、IP マルチキャストのファスト スイッチングをディセーブルにすることを検討してください。ディセーブルにすると、ルータがプロセス スイッチング モードになります。IP マルチキャストのファスト スイッチングをディセーブルにした後、パケットが正しい宛先に到達するようになった場合、問題はIPマルチキャストのファスト スイッチングに関連している可能性があります。

ファースト ホップ ルータでの IP マルチキャストの確認

ファーストホップルータでのIPマルチキャスト動作を確認するには、ファーストホップルータに次のコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

ステップ 2	**showipmroute** [*group-address*]
	例：
	`Device# show ip mroute 239.1.2.3`
	`(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF`
	`  Incoming interface: Serial1/0, RPF nbr 172.31.200.2`
	`  Outgoing interface list: Null`
	
	`(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT`
	`  Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0`
	
	`  Outgoing interface list:`
	`  Serial1/0, Forward/Sparse-Dense, 00:18:10/00:03:19`
		ファースト ホップ ルータの mroute に F フラグが設定されていることを確認します。

ステップ 3	**showipmrouteactive**[*kb/s*]
	例：
	`Device# show ip mroute active`
	`Active IP Multicast Sources - sending >= 4 kbps`
	
	`Group: 239.1.2.3, (?)`
		グループに送信しているアクティブなマルチキャスト送信元に関する情報を表示します。このコマンドの出力では、アクティブなソースのマルチキャストパケット レートに関する情報が示されます。

	コマンドまたはアクション	目的
	`Source: 10.0.0.1 (?)` `Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)`	（注） デフォルトでは、**showipmroute** コマンドと **active** キーワードによる出力では、4 kb/s 以上のレートでグループにトラフィックを送信するアクティブな送信元の情報が表示されます。より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

SPT 上のルータでの IP マルチキャストの確認

PIM-SM または PIM-SSM ネットワーク内の SPT 上のルータでの IP マルチキャスト動作を確認するには、SPT 上のルータに次のコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

ステップ 2	**showipmroute** [*group-address*]
	例：
	`Device# show ip mroute 239.1.2.3`
	`(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S`
	`Incoming interface: Null, RPF nbr`
		特定のグループの送信元に対する RPF ネイバーを確認します。

	コマンドまたはアクション	目的

	0.0.0.0
	  Outgoing interface list:
	  GigabitEthernet0/0/0,
	Forward/Sparse-Dense, 00:17:56/00:03:02
	
	(10.0.0.1, 239.1.2.3),
	00:15:34/00:03:28, flags: T
	  Incoming interface: Serial1/0, RPF
	nbr 172.31.200.1
	  Outgoing interface list:
	  GigabitEthernet0/0/0,
	Forward/Sparse-Dense, 00:15:34/00:03:02	

ステップ 3	**showipmrouteactive**
	
	例：
	
	Device# **show ip mroute active**
	Active IP Multicast Sources - sending
	 >= 4 kbps
	
	Group: 239.1.2.3, (?)
	  Source: 10.0.0.1 (?)
	  Rate: 20 pps/4 kbps(1sec), 4
	kbps(last 30 secs), 4 kbps(life avg)
		グループに送信しているアクティブなマルチキャスト送信元に関する情報を表示します。このコマンドの出力では、アクティブなソースのマルチキャストパケット レートに関する情報が示されます。
		
		（注） デフォルトでは、**showipmroute** コマンドと **active** キーワードによる出力では、4 kb/s 以上のレートでグループにトラフィックを送信するアクティブな送信元の情報が表示されます。より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

ラスト ホップ ルータでの IP マルチキャスト動作の確認

ラスト ホップ ルータでの IP マルチキャスト動作を確認するには、ラスト ホップ ルータで次のコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

ステップ 2	**showipigmpgroups**
	例：
	`Device# show ip igmp groups`
	`IGMP Connected Group Membership`
	`Group Address  Interface  Uptime  Expires  Last Reporter`
	`239.1.2.3  GigabitEthernet1/0/0  00:05:14  00:02:14  10.1.0.6`
	`224.0.1.39  GigabitEthernet0/0/0  00:09:11  00:02:08  172.31.100.1`
		ラスト ホップ ルータの IGMP メンバーシップを確認します。この情報によって、ラスト ホップ ルータに直接接続され、IGMP を介して認識されるレシーバが使用されているマルチキャスト グループが確認されます。

ステップ 3	**showippimrpmapping**
	例：
	`Device# show ip pim rp mapping`
	`PIM Group-to-RP Mappings`
	
	`Group(s) 224.0.0.0/4`
	`  RP 172.16.0.1 (?), v2v1`
	`  Info source: 172.16.0.1 (?), elected via Auto-RP`
	`  Uptime: 00:09:11, expires: 00:02:47`
		グループと RP 間のマッピングがラスト ホップ ルータで正しく生成されていることを確認します。
		（注） PIM/SSM ネットワークでラスト ホップ ルータを確認する場合は、この手順を無視してください。PIM-SSM ではランデブー ポイント（RP）が使用されないため、**showippimrpmapping** コマンドは PIM/SSM ネットワーク内のルータでは動作しません。さらに、正しく設定されている場合は、PIM/SSM グループは **showippimrpmapping** コマンドの出力には表示されません。

ステップ 4	**showipmroute**
	例：
	`Device# show ip mroute`
	`(*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC`
		mroute テーブルがラスト ホップ ルータに正しく入力されていることを確認します。

	コマンドまたはアクション	目的

	`  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1`
	`  Outgoing interface list:`
	`  GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:10/00:03:04`
	
	`(10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T`
	`  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1`
	`  Outgoing interface list:`
	`  GigabitEthernet1/0, Forward/Sparse-Dense, 00:02:49/00:03:04`
	
	`(*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC`
	`  Incoming interface: Null, RPF nbr 0.0.0.0`
	`  Outgoing interface list:`
	`  GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:15/00:00:00`
	
	`  GigabitEthernet0/0, Forward/Sparse-Dense, 00:10:05/00:00:00`
	
	`(172.16.0.1, 224.0.1.39), 00:02:00/00:01:33, flags: PTX`
	`  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1`	

ステップ 5	**showipinterface** [*type number*]
	
	例：
	
	`Device# show ip interface GigabitEthernet 0/0/0`
	`GigabitEthernet0/0 is up, line protocol is up`
	`  Internet address is 172.31.100.2/24`
	`  Broadcast address is 255.255.255.255`
	
	`  Address determined by setup command`
	`  MTU is 1500 bytes`
	`  Helper address is not set`
	`  Directed broadcast forwarding is disabled`
	`  Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13 224.0.0.5 224.0.0.6`
	`  Outgoing access list is not set`
	`  Inbound  access list is not set`
	`  Proxy ARP is enabled`
	`  Local Proxy ARP is disabled`
	`  Security level is default`
	`  Split horizon is enabled`
	`  ICMP redirects are always sent`
		マルチキャスト高速スイッチングがイネーブルになっており、ラスト ホップ ルータの発信インターフェイスでのパフォーマンスが最適化されていることを確認します。
		
		（注） **noipmroute-cache** インターフェイス コマンドを使用すると IP マルチキャスト高速スイッチングがディセーブルになります。IP マルチキャスト高速スイッチングがディセーブルになると、プロセス スイッチド パスを介してパケットが転送されます。

	コマンドまたはアクション	目的
	```ICMP unreachables are always sent ICMP mask replies are never sent IP fast switching is enabled IP fast switching on the same interface is disabled IP Flow switching is disabled IP CEF switching is disabled IP Fast switching turbo vector IP multicast fast switching is enabled IP multicast distributed fast switching is disabled IP route-cache flags are Fast Router Discovery is disabled IP output packet accounting is disabled IP access violation accounting is disabled TCP/IP header compression is disabled RTP/IP header compression is disabled Policy routing is disabled Network address translation is disabled WCCP Redirect outbound is disabled WCCP Redirect inbound is disabled WCCP Redirect exclude is disabled BGP Policy Mapping is disabled```	
ステップ 6	**showipmfib** 例： Device# **show ip mfib**	IP マルチキャスト転送情報ベース（MFIB）の転送エントリとインターフェイスが表示されます。
ステップ 7	**showippiminterfacecount** 例： Device# **show ip pim interface count** State: * - Fast Switched, D - Distributed Fast Switched H - Hardware Switching Enabled Address Interface FS Mpackets In/Out 172.31.100.2 GigabitEthernet0/0/0 * 4122/0 10.1.0.1 GigabitEthernet1/0/0 * 0/3193	マルチキャスト トラフィックがラスト ホップ ルータに転送されることを確認します。
ステップ 8	**showipmroutecount** 例： Device# **show ip mroute count** IP Multicast Statistics 6 routes using 4008 bytes of memory 3 groups, 1.00 average sources per group Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per	マルチキャスト トラフィックがラスト ホップ ルータに転送されることを確認します。

	コマンドまたはアクション	目的

	second
	Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
	
	Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165
	  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
	  Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0
	
	Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120
	  Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99
	
	Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10
	  Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0	

ステップ 9	**showipmrouteactive**[*kb/s*]
	
	例：
	
	Device# **show ip mroute active**
	Active IP Multicast Sources - sending >= 4 kbps
	
	Group: 239.1.2.3, (?)
	  Source: 10.0.0.1 (?)
	  Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg)
		ラスト ホップ ルータ上のグループにトラフィックを送信しているアクティブなマルチキャスト ソースに関する情報を表示します。このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。

	コマンドまたはアクション	目的
		（注） デフォルトでは、**showipmroute** コマンドと **active** キーワードによる出力では、4 kb/s 以上のレートでグループにトラフィックを送信するアクティブな送信元の情報が表示されます。より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

PIM 対応ルータを使用した IP マルチキャストの到達可能性のテスト

管理しているすべての PIM 対応ルータおよびアクセス サーバが、マルチキャスト グループのメンバで、すべてのルータが応答する原因となる ping が送信されます。これは、効果的な管理およびデバッグのツールです。

PIM 対応ルータを使用して IP マルチキャストの到達可能性をテストするには、次の作業を実行します。

マルチキャスト ping に応答するルータの設定

ルータがマルチキャスト ping に応答するように設定するには、次の手順を実行します。1 つのルータ上のすべてのインターフェイスと、マルチキャスト ネットワーク内のすべてのルータ上のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	インターフェイスコンフィギュレーション モードを開始します。 *type* 引数および *number* 引数には、ホストに直接接続されているインターフェイス、またはホストに対応しているインターフェイスを指定します。
ステップ 4	**ipigmpjoin-group** *group-address* 例： `Device(config-if)# ip igmp join-group 225.2.2.2`	（任意）指定したグループに加入するようにルータ上のインターフェイスを設定します。 この作業の目的として、マルチキャスト ネットワークに加入しているルータ上のすべてのインターフェイス上で、*group-address* 引数に同じグループ アドレスを設定します。 （注） この方法では、ルータは、マルチキャスト パケットの転送に加えて、マルチキャスト パケットを受信します。マルチキャスト パケットを受信することにより、ルータの高速スイッチングは行われません。
ステップ 5	マルチキャスト ネットワークに加入しているルータ上のインターフェイスで、ステップ 3 とステップ 4 を繰り返します。	--
ステップ 6	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

マルチキャスト ping に応答するように設定されたルータへの ping

マルチキャスト ping に応答するように設定されているルータに対して ping テストを開始するには、ルータで次の手順を実行します。このタスクは、ネットワーク内の IP マルチキャストの到達可能性のテストに使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**ping** *group-address* 例： `Device# ping 225.2.2.2`	IP マルチキャスト グループ アドレスを ping します。 正常な応答は、グループ アドレスが機能していることを示します。

PIM のモニタリングとトラブルシューティング

PIM 情報のモニタリング

PIM 設定をモニタするには、次の表に記載された特権 EXEC コマンドを使用します。

表 *42 : PIM* モニタリング コマンド

コマンド	目的
show ip pim all-vrfs tunnel [**tunnel** *tunnel_number* | **verbose**]	すべての VRF を表示します。
show ip pim autorp	グローバル Auto-RP 情報を表示します。
show ip pim boundary	インターフェイスに設定された、管理スコープ IPv4 マルチキャスト境界によってフィルタリングされた mroute に関する情報を表示します。
show ip pim interface	Protocol Independent Multicast（PIM）のために設定されているインターフェイスに関する情報を表示します。
show ip pim neighbor	PIM ネイバー情報を表示します。

コマンド	目的
show ip pim rp[*group-name* | *group-address*]	スパース モードのマルチキャスト グループに関連付けられた RP ルータを表示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
show ip pim tunnel [**tunnel** | **verbose**]	Protocol Independent Multicast（PIM）トンネル インターフェイスに関する情報を表示します。
show ip pim vrf { **word** { **all-vrfs** | **autorp** | **boundary** | **bsr-router** | **interface** | **mdt** | **neighbor** | **rp** | **rp-hash** | **tunnel** } }	VPN ルーティング/転送インスタンスを表示します。
show ip igmp groups detail	特定のマルチキャスト グループを結合した対象クライアントを表示します。

RP マッピングおよび BSR 情報のモニタリング

次の表に示す特権 EXEC モードを使用して、グループ/RP マッピングの一貫性を確認します。

表 *43 : RP* マッピングのモニタリング コマンド

コマンド	目的
show ip pim rp [*hostname* or *IP address* | **mapping** [*hostname* or *IP address* | **elected** | **in-use**] | **metric** [*hostname* or *IP address*]]	使用可能なすべての RP マッピングおよびメトリックを表示します。これにより、（BSR または Auto-RP メカニズムを通じて）デバイスがどのように RP を学習するかがわかります。 • （任意）*hostname* を指定する場合は、RP を表示するグループの IP 名を指定します。 • （任意）*IP address* を指定する場合は、RP を表示するグループの IP アドレスを指定します。 • （任意）シスコ デバイスによって認識されている（設定されている、または Auto-RP によって取得されている）すべてのグループ/RP マッピングを表示するには、**mapping** キーワードを使用します。 • （任意）**metric** キーワードを使用して、RP RPF メトリックを表示します。

コマンド	目的
show ip pim rp-hash *group*	指定したグループに選択されている RP を表示します。つまり、PIMv2 ルータまたはマルチレイヤ デバイス上で、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。*group* には、RP 情報を表示するグループ アドレスを入力します。

BSR の情報をモニタするには、次の表に示す特権 EXEC コマンドを使用します。

表 *44 : VTP* モニタリング コマンド

コマンド	目的
show ip pim bsr	選択された BSR に関する情報を表示します。
show ip pim bsr-router	BSRv2 に関する情報を表示します。

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング

PIMv1 および PIMv2 間の相互運用性に関する問題をデバッグするには、次の点を順にチェックします。

1. **show ip pim rp-hash** 特権 EXEC コマンドを使用して RP マッピングを確認し、すべてのシステムが同じグループの同じ RP に同意していることを確認します。
2. DR と RP の各バージョン間の相互運用性を確認し、RP が DR と適切に相互作用していることを確認します（この場合は、登録停止に応答し、カプセル化が解除されたデータ パケットをレジスタから転送します）。

関連トピック

PIM のバージョン （609 ページ）

PIM の設定例

例：PIM スタブ ルーティングのイネーブル化

次の例では、IP マルチキャスト ルーティングがイネーブルになっており、スイッチ A の PIM アップリンク ポート 25 はルーテッド アップリンク ポートとして設定されています（**spare-dense-mode** がイネーブル）。VLAN 100 インターフェイスとギガビット イーサネット ポート 20 で PIM スタブ ルーティングがイネーブルに設定されています。

```
Device(config)# ip multicast-routing distributed
Device(config)# interface GigabitEthernet3/0/25
```

```
Device(config-if)# no switchport
Device(config-if)# ip address 3.1.1.2 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# exit
Device(config)# interface vlan100
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface GigabitEthernet3/0/20
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface vlan100
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface GigabitEthernet3/0/20
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip pim passive
Device(config-if)# end
```

関連トピック

PIM スタブ ルーティングのイネーブル化（CLI） （625 ページ）
PIM スタブ ルーティング （610 ページ）

例：PIM スタブ ルーティングの確認

各インターフェイスの PIM スタブがイネーブルになっていることを確認するには、**show ip pim interfac** 特権 EXEC コマンドを使用します。

```
Device# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet3/0/25 v2/SD 1 30 1 3.1.1.2
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet3/0/20 v2/P 0 30 1 10.1.1.1
```

関連トピック

PIM スタブ ルーティングのイネーブル化（CLI） （625 ページ）
PIM スタブ ルーティング （610 ページ）

例：マルチキャスト グループへの RP の手動割り当て

次に、マルチキャスト グループ 225.2.2.2 の場合だけ、RP のアドレスを 147.106.6.22 に設定する例を示します。

```
Device(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Device(config)# ip pim rp-address 147.106.6.22 1
```

関連トピック

マルチキャスト グループへの RP の手動割り当て（CLI） （628 ページ）

例：Auto-RP の設定

次に、最大ホップ数が 31 であるすべての PIM 対応インターフェイスから RP アナウンスメントを送信する例を示します。ポート 1 の IP アドレスが RP です。アクセス リスト 5 には、このデバイスが RP として機能するグループが記述されています。

```
Device(config)# ip pim send-rp-announce gigabitethernet1/0/1 scope 31 group-list 5
Device(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

関連トピック

新規インターネットワークでの Auto-RP の設定（CLI）（631 ページ）
Auto-RP（612 ページ）

例：Auto-RP でのスパース モード

次の例では、Auto-RP でスパース モードを設定しています。

```
ip multicast-routing
ip pim autorp listener
ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery Loopback1 scope 16
no ip pim dm-fallback
access-list 1 permit 239.254.2.0 0.0.0.255
access-list 1 permit 239.254.3.0 0.0.0.255
.
.
.
access-list 10 permit 224.0.1.39
access-list 10 permit 224.0.1.40
access-list 10 permit 239.254.2.0 0.0.0.255
access-list 10 permit 239.254.3.0 0.0.0.255
```

関連トピック

新規インターネットワークでの Auto-RP の設定（CLI）（631 ページ）
Auto-RP（612 ページ）

例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義

次に、自動 RP 情報を拒否する IP マルチキャスト境界のコンフィギュレーション例の一部を示します。

```
Device(config)# access-list 1 deny 224.0.1.39
Device(config)# access-list 1 deny 224.0.1.40
Device(config)# access-list 1 permit all
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip multicast boundary 1
```

関連トピック

IP マルチキャスト境界の定義（CLI）（643 ページ）

マルチキャスト境界 （614 ページ）

例：着信 RP アナウンスメント メッセージのフィルタリング

次に、候補 RP アナウンスメントが不正な候補 RP から許可されないようにするために使用される自動 RP マッピング エージェントの設定例を示します。

```
Device(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Device(config)# access-list 10 permit host 172.16.5.1
Device(config)# access-list 10 permit host 172.16.2.1
Device(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Device(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

マッピング エージェントは 2 つのデバイス（172.16.5.1 および 172.16.2.1）からの候補 RP アナウンスだけを許可します。マッピング エージェントは 2 つのデバイスからの候補 RP アナウンスメントのうち、グループ範囲が 224.0.0.0 ～ 239.255.255.255 であるマルチキャスト グループ宛てのアナウンスメントだけを許可します。マッピングエージェントは、ネットワーク内の他のデバイスからの候補 RP アナウンスメントを許可しません。さらに、候補 RP アナウンスメントが 239.0.0.0 ～ 239.255.255.255 の範囲のグループに宛てたものである場合、マッピング エージェントは 172.16.5.1 または 172.16.2.1 からの候補 RP アナウンスメントを許可しません。この範囲は、管理の有効範囲付きアドレス範囲です。

関連トピック

着信 RP アナウンスメント メッセージのフィルタリング（CLI） （638 ページ）

例：問題のある RP への Join メッセージの送信禁止

すべてのインターフェイスが SM の場合はデフォルト設定の RP を使用し、既知のグループ 224.0.1.39 および 224.0.1.40 をサポートします。自動 RP はこれら 2 つの既知のグループを使用し、RP マッピング情報を収集、配信します。**ip pim accept-rp auto-rp** コマンドが設定されている場合は、RP を許可する別の **ip pim accept-rp** コマンドを次のように設定してください。

```
Device(config)# ip pim accept-rp 172.10.20.1 1
Device(config)# access-list 1 permit 224.0.1.39
Device(config)# access-list 1 permit 224.0.1.40
```

関連トピック

問題のある RP への Join メッセージの送信禁止（CLI） （638 ページ）

例：候補 BSR の設定

次に、候補 BSR の設定例を示します。この例では、アドバタイズ済み BSR アドレスとしてポートの IP アドレス 172.21.24.18 を、hash-mask-length として 30 ビットを使用します。プライオリティは 10 です。

```
Device(config)# interface gigabitethernet1/0/2
```

```
Device(config-if)# ip address 172.21.24.18 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# ip pim bsr-candidate gigabitethernet1/0/2 30 10
```

関連トピック

候補 BSR の設定（CLI）（645 ページ）
PIMv2 ブートストラップ ルータ（616 ページ）

例：候補 RP の設定

次に、デバイスが自身を候補 RP として PIM ドメイン内の BSR にアドバタイズするよう設定する例を示します。標準アクセス リスト番号 4 により、ポートで識別されるアドレスを持つ RP に対応するグループ プレフィックスが指定されます。この RP は、プレフィックスが 239 であるグループを処理します。

```
Device(config)# ip pim rp-candidate gigabitethernet1/0/2 group-list 4
Device(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

関連トピック

候補 RP の設定（CLI）（647 ページ）
ランデブー ポイント（611 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	『*IP Multicast Routing Command Reference（Catalyst 3850 Switches）*』
IGMP ヘルパー コマンドの構文および使用方法の詳細。	『*IP Multicast Routing Command Reference（Catalyst 3850 Switches）*』
Multicast Source Discovery Protocol（MSDP）	『*IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE Release 3E（Catalyst 3850 Switches）*』
Enhanced Interior Gateway Routing Protocol (EIGRP) スタブ ルーティング	『*IP Routing: EIGRP Configuration Guide, Cisco IOS XE Release 3E （Catalyst 3850 Switches）*』
Open Shortest Path First（OSPF）スタブ ルーティング	『*IP Routing: OSPF Configuration Guide, Cisco IOS XE 3E（Catalyst 3850 Switches）*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
Cisco IOS IP SLA コマンド	『Cisco IOS IP Multicast Command Reference』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
PIM については、RFC 4601 および次に示す Internet Engineering Task Force（IETF）インターネット ドラフトを参照してください。	• 『*Protocol Independent Multicast (PIM): Motivation and Architecture*』 • 『*Protocol Independent Multicast (PIM), Dense Mode Protocol Specification*』 • 『*Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification*』 • 『*draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2*』 • 『*draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode*』

MIB

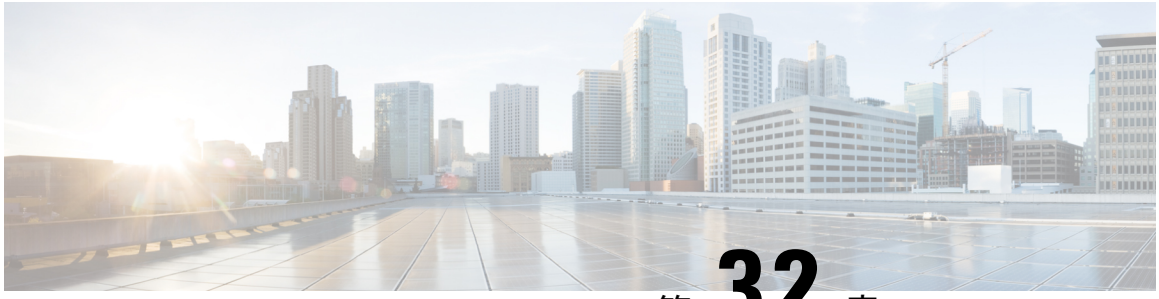
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

PIM の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。



第 32 章

IP マルチキャストに対する PIM MIB 拡張の設定

- 機能情報の確認 （679 ページ）
- IP マルチキャストに対する PIM MIB 拡張について （679 ページ）
- IP マルチキャストに対する PIM MIB 拡張の設定方法 （680 ページ）
- PIM MIB 拡張の設定例 （682 ページ）
- その他の参考資料 （682 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IP マルチキャストに対する PIM MIB 拡張について

IP マルチキャストに対する SNMP トラップの PIM MIB 拡張

Protocol Independent Multicast（PIM）は、マルチキャスト データ パケットをマルチキャスト グループにルーティングするために使用される IP マルチキャスト ルーティング プロトコルです。RFC 2934 は、IPv4 用の PIM MIB を定義します。PIM MIB は、Simple Network Management Protocol（SNMP）を使用してユーザがリモートに PIM を監視および設定できるようにする管理対象オブジェクトを記述したものです。

PIM MIB 拡張では、次の新しいクラスの PIM 通知を導入しています。

- neighbor-change：この通知は、次の条件により発生します。
  - ルータの PIM インターフェイスが（インターフェイス コンフィギュレーション モードで **ip pim** コマンドを使用して）無効化、または有効化されている。
  - ルータの PIM ネイバーの隣接関係が失効している（RFC 2934 の定義による）。
- rp-mapping-change：この通知は、自動RPメッセージまたはブートストラップルータ（BSP）メッセージのいずれかが原因で、ランデブー ポイント（RP）マッピング情報が変更された場合に、発生します。
- invalid-pim-message：この通知は、次の条件により発生します。
  - 無効な (*, G) Join または Prune メッセージがデバイスで受信された（たとえば、パケットで指定された RP がマルチキャスト グループの RP でない Join または Prune メッセージをルータが受信した場合）
  - 無効な PIM 登録メッセージがデバイスで受信された（たとえば、RP ではないマルチキャスト グループから登録メッセージをルータが受信した場合）

関連トピック

IP マルチキャストに対する PIM MIB 拡張のイネーブル化 （680 ページ）
IP マルチキャストに対する PIM MIB 拡張のイネーブル化の例 （682 ページ）

PIM MIB 拡張の利点

PIM MIB 拡張：

- ユーザは、RP マッピングの変更を検出することで、ネットワークのマルチキャスト トポロジの変更を確認できます。
- PIM 対応インターフェイスで PIM プロトコルをモニタするトラップが提供されます。
- マルチキャストの隣接関係がマルチキャスト インターフェイスで期限切れになったときに、ユーザがルーティングの問題を特定するのを支援します。
- ユーザが RP 設定エラー（たとえば、Auto-RP などのダイナミック RP 割り当てプロトコルのフラッピングによるエラーなど）をモニタできるようにします。

IP マルチキャストに対する PIM MIB 拡張の設定方法

IP マルチキャストに対する PIM MIB 拡張のイネーブル化

IP マルチキャストに対する PIM MIB 拡張を有効にするには、次のタスクを実行します。

（注）

- pimInterfaceVersion オブジェクトは RFC 2934 から削除されたので、ソフトウェアではサポートされていません。
- 次の MIB テーブルは、シスコ ソフトウェアでサポートされていません。
  - pimIpMRouteTable
  - pimIpMRouteNextHopTable

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-serverenabletrapspim** [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**] 例： `Device(config)# snmp-server enable traps pim neighbor-change`	デバイスが PIM 通知を送信できるようにします。 • **neighbor-change**：このキーワードは、デバイスの PIM インターフェイスがディセーブル、またはイネーブルである、あるいはデバイスの PIM 隣接関係が失効していることを示す通知をイネーブル化します。 • **rp-mapping-change**：このキーワードは、Auto-RP メッセージまたは BSR メッセージによる RP マッピング情報の変更を示す通知をイネーブル化します。 • **invalid-pim-message**：このキーワードは、無効な PIM プロトコル操作のモニタリングに関する通知をイネーブル化します（たとえば、パケットに指定された RP がマルチキャスト グループの RP ではない Join または Prune メッセージをデバイスが受信する場合、または RP で

	コマンドまたはアクション	目的
		はないマルチキャスト グループから登録メッセージをデバイスが受信する場合）。
ステップ 4	**snmp-serverhost** *host-address* [**traps** | **informs**] *community-string* **pim** 例： `Device(config)# snmp-server host 10.10.10.10 traps public pim`	PIM SNMP 通知操作の受信者を指定します。

関連トピック

IP マルチキャストに対する SNMP トラップの PIM MIB 拡張 （679 ページ）
IP マルチキャストに対する PIM MIB 拡張のイネーブル化の例 （682 ページ）

PIM MIB 拡張の設定例

IP マルチキャストに対する PIM MIB 拡張のイネーブル化の例

次の例に、ルータの PIM インターフェイスが有効になっていることを示す通知を生成するようにルータを設定する方法を示します。最初の行では、IP アドレスが 10.0.0.1 のホストに SNMP v2c トラップとして送信されるよう、PIM トラップが設定されます。2 行目では、トラップ通知の neighbor-change クラスをホストに送信するよう、ルータが設定されます。

```
snmp-server host 10.0.0.1 traps version 2c public pim
snmp-server enable traps pim neighbor-change
interface ethernet0/0
 ip pim sparse-dense-mode
```

関連トピック

IP マルチキャストに対する PIM MIB 拡張のイネーブル化 （680 ページ）
IP マルチキャストに対する SNMP トラップの PIM MIB 拡張 （679 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

標準および RFC

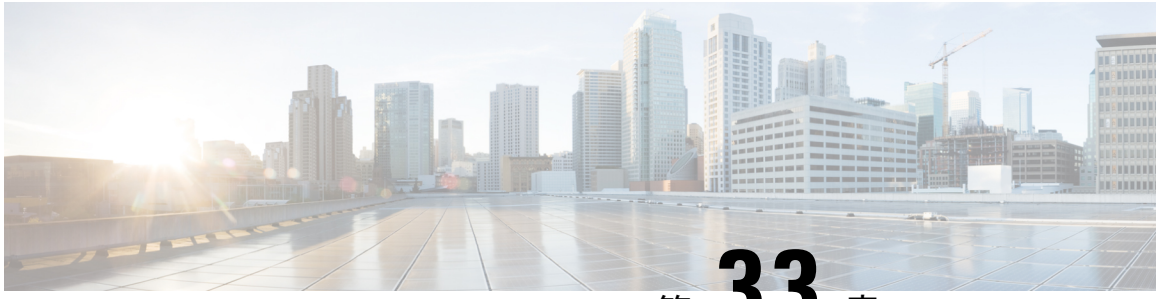
標準/RFC	タイトル
draft-kouvelas-pim-bidir-new-00.txt	『A New Proposal for Bi-directional PIM』
RFC 1112	『Host Extensions for IP Multicasting』
RFC 1918	『Address Allocation for Private Internets』
RFC 2770	『GLOP Addressing in 233/8』
RFC 3569	『An Overview of Source-Specific Multicast (SSM)』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html



第 33 章

MSDP の設定

- 機能情報の確認 （685 ページ）
- （685 ページ）
- MSDP を使用して複数の PIM-SM ドメインを相互接続するための情報 （685 ページ）
- MSDP を使用して複数の PIM-SM ドメインを相互接続する方法 （701 ページ）
- MSDP を使用して複数の PIM-SM ドメインを相互接続する設定例 （724 ページ）
- その他の参考資料 （727 ページ）
- Multicast Source Discovery Protocol の機能履歴と情報 （728 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

MSDP を使用して複数の PIM-SM ドメインを相互接続するための情報

MSDP を使用した複数の PIM-SM ドメインの相互接続の利点

- ランデブー ポイント(RP)が動的にドメイン外のアクティブな送信元を検出できます。

- 複数のドメイン間でマルチキャスト配信ツリーを構築するための、より管理しやすいアプローチが導入されます。

MSDP は複数の PIM-SM ドメインを接続するメカニズムです。MSDP は、他の PIM ドメイン内のマルチキャスト送信元を検出することを目的としています。MSDP の主な利点は、（一般的な共有ツリーではなく）ドメイン間ソース ツリーを PIM-SM ドメインで使用できるようにし、複数の PIM-SM ドメインを相互接続する複雑性を軽減することです。MSDP がネットワークで設定されている場合、RP は他のドメイン内の RP と送信元情報を交換します。RP は、レシーバがいるグループに送信するソースのドメイン間ソース ツリーに参加できます。RP は、そのドメイン内の共有ツリーのルートであり、アクティブ レシーバが存在するドメイン内のすべてのポイントへのブランチがあるため、これを行うことができます。PIM-SM ドメイン外の新しい送信元を（共有ツリーの送信元からのマルチキャストパケットの到着によって）ラストホップ デバイスが認識すると、その送信元に加入要求を送信してドメイン間ソース ツリーに参加できます。

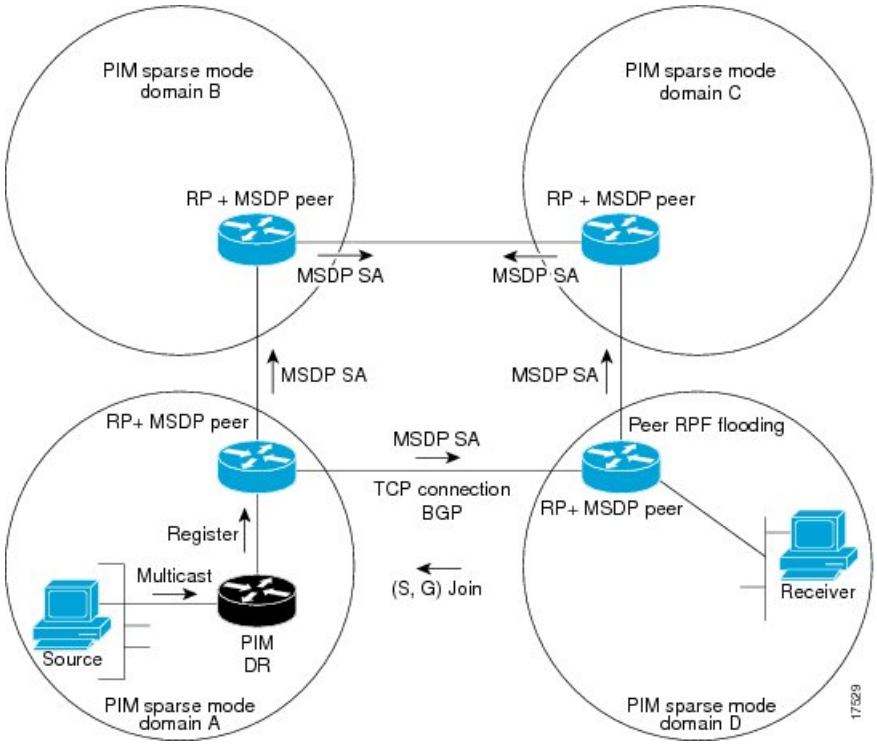
（注） RP に特定グループの共有ツリーがないか、発信インターフェイス リストがヌルの共有ツリーがある場合は、別のドメインの発信元に加入要求を送信しません。

MSDP がイネーブルになっている場合、PIM-SM ドメインの RP は、他のドメインの MSDP 対応デバイスとの MSDP ピアリング関係を維持します。このピアリング関係は TCP 接続を通じて発生します。交換されるのは主にマルチキャスト グループを送信する送信元のリストです。MSDP はピアリング接続に TCP（ポート 639）を使用します。BGP と同様に、ポイントツーポイント TCP ピアリングを使用する場合は、各ピアを明示的に設定する必要があります。さらに、RP 間の TCP 接続は基本的なルーティング システムによって実現されます。受信側の RP では、送信元リストを使用して送信元のパスが確立されます。マルチキャスト ソースがレシーバがいるドメインの対象である場合、マルチキャスト データは PIM-SM で提供される通常のソース ツリー構築メカニズムを使用して配信されます。MSDP は、グループを送信する送信元のアナウンスにも使用されます。これらのアナウンスは、ドメインの RP で発信する必要があります。

図に、2 つの MSDP ピア間の MSDP の動作を示します。PIM では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP が使用されます。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *30 : RP* ピア間で動作する *MSDP*



MSDP が実装されている場合、次のイベント シーケンスが発生します。

1. 図に示すように、PIM 指定デバイス（DR）が送信元を RP に登録すると、その RP が Source-Active（SA）メッセージをすべての MSDP ピアに送信します。

（注） DR は、（ソースがアクティブになると）カプセル化されたデータをソースごとに 1 回だけ RP に送信します。ソースがタイムアウトした場合、ソースが再度アクティブになるとこのプロセスが実行されます。これは、発信元 RP に登録されているすべての発信元を含んでいる定期的な SA メッセージの場合とは異なります。これらの SA メッセージは MSDP 制御パケットであるため、アクティブな送信元からのカプセル化されたデータを含んでいません。

1. SA メッセージでは、ソース アドレス、ソースの送信先グループ、および RP のアドレスまたは発信者 ID が識別されます（設定されている場合）。

2. SA メッセージを受信する各 MSDP ピアは、発信者からのダウンストリームのすべてのピアに SA メッセージをフラッディングします。場合によっては（図の PIM-SM ドメイン B および C 内の RP の場合など）、RP は複数の MSDP ピアからの SA メッセージのコピーを受信することがあります。ループが作成されないように、RP は BGP ネクスト ホップ データベースに問い合わせて、SA メッセージの発信者へのネクスト ホップを識別します。MBGP とユニキャスト BGP の両方が設定されている場合、MBGP が最初に確認されてからユニキャスト BGP が確認されます。そのネクストホップ ネイバーが発信元の RPF ピアです。RPF ピアへのインターフェイス以外のインターフェイスにある発信元から受信した

SA メッセージはドロップされます。そのため、SA メッセージ フラッディング プロセスはピア RPF フラッディングと呼ばれます。ピア RPF フラッディング メカニズムにより、BGP または MBGP は MSDP とともに実行する必要があります。

1. SA メッセージを受信した RP は、グループの (*, G) 送信インターフェイス リストにインターフェイスが存在するかどうかを確認することによって、そのドメイン内にアドバタイズされたグループのメンバが存在するかどうかを確認します。グループ メンバが存在しない場合、RP は何も実行しません。グループ メンバが存在する場合、RP は（S, G）加入要求を送信元に送信します。その結果、ドメイン間ソースツリーのブランチが自律システムの RP との境界に構築されます。マルチキャスト パケットは、RP に着信すると、その共有ツリーを経由して RP のドメイン内のグループ メンバに転送されます。メンバの DR は、標準的な PIM-SM 手順を使用してソースへのランデブー ポイント ツリー（RPT）に加入することもできます。
2. 発信元 RP は、送信元がグループにパケットを送信し続ける限り、60 秒ごとに（S, G）ステートに関する SA メッセージを定期的に送信し続けます。RP は SA メッセージを受信すると、SA メッセージをキャッシュします。たとえば、発信元 RP 10.5.4.3 から (172.16.5.4, 228.1.2.3) に対する SA メッセージを受信したとします。RP は mroute テーブルを確認し、グループ 228.1.2.3 にアクティブなメンバが存在しないことを検出すると、SA メッセージを 10.5.4.3 のダウンストリームにあるピアに渡します。次に、ドメイン内のホストが加入要求をグループ 228.1.2.3 の RP に送信した場合、その RP はホストへのインターフェイスを (*, 224.1.2.3) エントリの発信インターフェイス リストに追加します。RP は SA メッセージをキャッシュするため、デバイスは (172.16.5.4, 228.1.2.3) のエントリを持ち、ホストが加入を要求するとすぐにソース ツリーに加入できます。

（注） 現行のすべてのサポート対象のソフトウェア リリースでは、MSDP SA メッセージのキャッシュは必須であり、手動でイネーブルまたはディセーブルにすることはできません。デフォルトでは、MSDP ピアが設定されると、**ipmulticastcache-sa-state** コマンドが自動的に実行コンフィギュレーションに追加されます。

MSDP メッセージ タイプ

MSDP メッセージには 4 つの基本タイプがあり、それぞれが固有の Type、Length、および Value（TLV）データ フォーマットでエンコードされています。

SA メッセージ

SA メッセージを使用して、ドメイン内のアクティブなソースをアドバタイズします。また、これらの SA メッセージには送信元によって送信された最初のマルチキャスト データ パケットが含まれていることがあります。

SA メッセージには、発信元 RP の IPアドレスと、アドバタイズされる 1 つ以上の（S, G）ペアが含まれています。また、SA メッセージにカプセル化されたデータ パケットが含まれていることがあります。

（注） SA メッセージの詳細については、SA メッセージの発信、受信および処理 （689 ページ）を参照してください。

SA 要求メッセージ

SA 要求メッセージを使用して、特定のグループにアクティブなソースのリストを要求します。これらのメッセージは、SA キャッシュにアクティブな（S, G）ペアのリストを保持する MSDP SA キャッシュに送信されます。グループ内のすべてのアクティブなソースが発信元の RP によって再アドバタイズされるまで待つ代わりに、SA 要求メッセージを使用してアクティブなソースのリストを要求すると、加入遅延を短縮できます。

SA 応答メッセージ

SA 応答メッセージは SA 要求メッセージに応答する MSDP ピアによって送信されます。SA 応答メッセージには、発信元の RP の IP アドレスと、キャッシュに保存されている発信元 RP のドメイン内のアクティブなソースの 1 つ以上の（S, G）ペアが含まれています。

キープアライブ メッセージ

キープアライブ メッセージは 60 秒ごとに送信され、MSDP セッションをアクティブに保ちます。キープアライブ メッセージまたは SA メッセージを 75 秒間受信しなかった場合、MSDP セッションがリセットされます。

SA メッセージの発信、受信および処理

ここでは、SA メッセージの発信、受信、および処理について詳しく説明します。

SA メッセージの発信

SA メッセージは、ローカル PIM-SM ドメイン内で新しいソースがアクティブになると、RP によってトリガーされます（MSDP が設定されている場合）。ローカル送信元は、RP に直接接続された送信元であるか、または RP に登録済みのファーストホップ DR です。RP は、PIM-SM ドメイン内のローカル送信元（つまり、RP に登録しているローカル送信元）に対してのみ SA メッセージを発信します。

（注） ローカル送信元は、RP の (S, G) mroute エントリに設定されている A フラグによって示されます（**show ip mroute** コマンドの出力で確認できます）。このフラグは、送信元が他の MSDP ピアに対する RP によるアドバタイズメントの候補であることを示します。

送信元がローカルの PIM-SM ドメインにある場合、RP で (S, G) ステートが作成されます。登録メッセージを受信するか、または直接接続された送信元から最初の (S, G) パケットが到着することによって、新しい送信元は RP によって検出されます。ソースから送信された最初のマ

ルチキャストパケット（登録メッセージにカプセル化されるか、直接接続されているソースから受信します）は、最初の SA メッセージにカプセル化されます。

SA メッセージの受信

SA メッセージは、送信元に戻るベスト パスにある MSDP RPF ピアからのみ受け入れられます。他の MSDP ピアから到着する同じ SA メッセージは無視する必要があり、そうしないと SA ループが発生する可能性があります。到着した SA メッセージの MSDP RPF ピアを確定的に選択するには、MSDP トポロジの知識が必要です。ただし、MSDP はルーティング アップデートの形式でトポロジ情報を配信しません。MSDP は、SA RPF チェック機能に関する MSDP トポロジの最良近似として (M)BGP ルーティング データを使用することで、この情報を推測します。したがって、MSDP トポロジは BGP ピア トポロジと同じ汎用トポロジに従う必要があります。わずかな例外（MSDP メッシュ グループ内のデフォルトの MSDP ピアおよび MSDP ピア）を除き、MSDP ピアは一般的に (M)BGP ピアでもあります。

RPF チェック ルールが SA メッセージに適用される仕組み

SA メッセージの RPF チェックに適用されるルールは、MSDP ピア間の BGP ピアリングに依存します。

- ルール 1：送信側の MSDP ピアが Interior (M)BGP（i（M）BGP）ピアでもある場合に適用されます。
- ルール 2：送信側の MSDP ピアが exterior (M)BGP ピアでもある場合に適用されます。
- ルール 3：送信側の MSDP ピアが (M)BGP ピアでない場合に適用されます。

RPF チェックは、次の場合は実行されません。

- 送信側の MSDP ピアが唯一の MSDP ピアであり、唯一の単一の MSDP ピアまたはデフォルトの MSDP ピアが設定されている状況の場合。
- 送信側の MSDP ピアがメッシュ グループのメンバーである場合。
- 送信側の MSDP ピアのアドレスが SA メッセージに含まれる RP アドレスである場合

RPF チェックに適用するルールをソフトウェアが決定する仕組み

ソフトウェアは、次のロジックを使用して、RPF チェックに適用される RPF ルールを決定します。

- 送信側の MSDP ピアと同じ IP アドレスを持つ (M)BGP ネイバーを見つけます。
  - 一致した (M)BGP ネイバーが Internal BGP（iBGP）ピアである場合、ルール 1 を適用します。
  - 一致した（M）BGP ネイバーが External BGP（eBGP）ピアである場合、ルール 2 を適用します。
  - 一致するネイバーが見つからなかった場合、ルール 3 を適用します。

RPF チェック ルール選択の影響は次のとおりです。デバイスで MSDP ピアの設定に使用される IP アドレスは、同じデバイスで (M)BGP ピアの設定に使用される IP アドレスと一致する必要があります。

MSDP における SA メッセージの RPF チェックのルール 1

送信側の MSDP ピアが i(M)BGP ピアでもある場合、MSDP における RPF チェックのルール 1 が適用されます。ルール 1 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP マルチキャスト ルーティング情報ベース（MRIB）を検索して SA メッセージを発信した RP への最適パスを探します。MRIB でパスが検出されなかった場合、ピアはユニキャスト ルーティング情報ベース（URIB）を検索します。それでもパスが検出されなかった場合は、RPF チェックは失敗します。
2. 前の検索が成功した（つまり、ベスト パスが見つかった）場合、ピアは、このベスト パスに対する BGP ネイバーのアドレスを判別します。このアドレスは、BGP 更新メッセージでピアにパスを送信した BGP ネイバーのアドレスです。

（注） BGP ネイバーアドレスは、パス内のネクストホップアドレスと同じではありません。i(M)BGP ピアはパスのネクストホップ属性を更新しないので、ネクストホップアドレスは通常、シスコにパスを送信した BGP ピアのアドレスと同じではありません。

（注） BGP ネイバー アドレスは、ピアにパスを送信したピアの BGP ID と必ずしも同じとは限りません。

1. 送信側の MSDP ピアの IP アドレスが BGP ネイバー アドレス（ピアにパスを送信した BGP ピアのアドレス）と同じである場合、RPF チェックは正常に終了します。同じでない場合は、RPF チェックは失敗します。

MSDP に対する RPF チェック ルール 1 の影響

MSDP トポロジでは、（M）BGP トポロジをミラーリングする必要があります。通常、2 つのデバイス間に i(M)BGP ピア接続がある場合は、MSDP ピア接続を設定する必要があります。つまり、遠端 MSDP ピア接続の IP アドレスは、遠端 i（M）BGP ピア接続と同じにする必要があります。自律システム内の i(M)BGP ピア間の BGP トポロジは AS パスによって記述されないため、アドレスは同じである必要があります。別の i（M）BGP ピアへのアップデートの送信時に i（M）BGP ピアがパス内のネクストホップ アドレスをアップデートした場合、ピアはネクスト ホップ アドレスを使用して i（M）BGP トポロジ（したがって MSDP トポロジ）を表すことができます。ただし、i(M)BGP ピアのデフォルトの動作ではネクストホップ アドレスがアップデートされないため、ピアは (M)BGP トポロジ（MSDP トポロジ）の記述にネクストホップ アドレスを当てにすることができません。その代わりに、i（M）BGP ピアは、パスを送信した i（M）BGP ピアのアドレスを使用して、自律システム内の i（M）BGP トポロジ（MSDP トポロジ）を表します。

ヒント　i(M)BGP と MSDP の両方のピア アドレスに同じアドレスが使用されるように、MSDP ピア アドレスの設定時は注意を払う必要があります。

MSDP における SA メッセージの RPF チェックのルール 2

送信側の MSDP ピアが e(M)BGP ピアでもある場合、MSDP における RPF チェックのルール 2 が適用されます。ルール 2 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP MRIB を検索して SA メッセージを発信した RP への最適パスを探します。MRIB でパスが検出されなかった場合、ピアは URIB を検索します。それでもパスが検出されなかった場合は、RPF チェックは失敗します。
2. 前の検索が成功した（つまり、ベストパスが見つかった）場合、ピアはパスを調べます。RP へのベスト パス内の最初の自律システムが e(M)BGP ピア（送信側の MSDP ピアでもある）の自律システムと同じである場合、RPF チェックは正常に終了します。同じでない場合は失敗します。

MSDP に対する RPF チェック ルール 2 の影響

MSDP トポロジでは、（M）BGP トポロジをミラーリングする必要があります。通常、2 つのデバイス間に e(M)BGP ピア接続がある場合は、MSDP ピア接続を設定する必要があります。ルール 1 とは対照的に、遠端 MSDP ピア接続の IP アドレスは遠端 e（M）BGP ピア接続と同じである必要はありません。その理由は、2 つの e（M）BGP ピア間の BGP トポロジが AS パスで記述されないためです。

MSDP における SA メッセージの RPF チェックのルール 3

送信側の MSDP ピアが (M)BGP ピアではない場合、RPF チェックのルール 3 が適用されます。ルール 3 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP MRIB を検索して SA メッセージを発信した RP への最適パスを探します。MRIB でパスが検出されなかった場合、ピアは URIB を検索します。それでもパスが検出されなかった場合は、RPF チェックは失敗します。
2. 前の検索が成功した（つまり、SA メッセージを発信した RP へのベスト パスが見つかった）場合、ピアは、SA メッセージを送信した MSDP ピアへのベスト パスの BGP MRIB を検索します。MRIB でパスが検出されなかった場合、ピアは URIB を検索します。それでもパスが検出されなかった場合は、RPF チェックは失敗します。

（注）　SA メッセージを送信した MSDP ピアの自律システムは発信元自律システムで、これは MSDP ピアへの AS パス内にある最後の自律システムです。

1. RP への最適パス内の最初の自律システムが送信側の MSDP ピアの自律システムと同じである場合、RPF チェックは正常に終了します。同じでない場合は、RPF チェックは失敗します。

SA メッセージの処理

次の手順は、MSDP ピアが SA メッセージを処理するときに実行されます。

1. ピアは SA メッセージの (S, G) ペアのグループ アドレス G を使用して、mroute テーブル内の関連する (*, G) エントリを見つけます。(*, G) エントリが見つかり、その発信インターフェイスのリストがヌルでない場合は、SA メッセージでアドバタイズされる送信元用の PIM-SM ドメインにアクティブな受信者がいます。
2. その後、MSDP ピアは、アドバタイズされた送信元用に (S, G) エントリを作成します。
3. (S, G) エントリがない場合、MSDP ピアはソース ツリーに加入するためにソースへの (S, G) 加入をただちにトリガーします。
4. ピアは SA メッセージをその他のすべての MSDP ピアにフラッディングします。ただし、次を除きます。
   - SA メッセージが受信された MSDP ピア。
   - このデバイスと同じ MSDP メッシュ グループにある MSDP ピア（ピアがメッシュ グループのメンバーである場合）。

（注） SA メッセージは、デバイスの SA キャッシュにローカルに保存されます。

MSDP ピア

BGP と同様に、MSDP は他の MSDP ピアとのネイバー関係を確立します。MSDP ピアは、TCP ポート 639 を使用して接続します。下位の IP アドレス ピアは、TCP 接続のオープンにおいてアクティブな役割を果たします。上位の IP アドレス ピアは、もう一方が接続を行うまで LISTEN ステートで待機します。MSDP ピアは、60 秒ごとにキープアライブ メッセージを送信します。データが着信すると、キープアライブ メッセージと同じ機能が実行され、セッションがタイムアウトにならないようにします。キープアライブ メッセージまたはデータを 75 秒間受信しなかった場合、TCP 接続がリセットされます。

関連トピック

MSDP ピアの設定 （701 ページ）
MSDP ピアのシャットダウン （703 ページ）
例：MSDP ピアの設定 （724 ページ）

MSDP MD5 パスワード認証

MSDP MD5 パスワード認証機能は、2 つの MSDP ピア間の TCP 接続上で Message Digest 5（MD5）シグネチャの保護を提供するための拡張です。この機能は、TCP 接続ストリームに導入されるスプーフィングされた TCP セグメントの脅威に対して MSDP を保護することにより、追加のセキュリティを提供します。

関連トピック

MSDP ピア間の MSDP MD5 パスワード認証の設定 （704 ページ）
例：MSDP MD5 パスワード認証の設定 （724 ページ）

MSDP MD5 パスワード認証の動作

RFC 2385 に従って開発された、MSDP MD5 パスワード認証機能は、MSDP ピア間の TCP 接続上で送信された各セグメントを検証するために使用されます。**ip msdp password peer** コマンドは、2 つの MSDP ピア間の TCP 接続の MD5 認証をイネーブルにするために使用されます。2 つの MSDP ピア間で MD5 認証がイネーブルになると、ピア間の TCP 接続で送信された各セグメントが確認されます。どちらの MSDP ピアでも同じパスワードを使用して MD5 認証を設定する必要があります。そうしない場合は、これらの間の接続が確立されません。MD5 認証を設定すると、Cisco IOS ソフトウェアにより、TCP 接続上で送信される各セグメントについて MD5 ダイジェストが生成され、検証されるようになります。

MSDP MD5 パスワード認証の利点

- TCP 接続ストリームに導入されるスプーフィングされた TCP セグメントの脅威に対して MSDP を保護します。
- 業界標準の MD5 アルゴリズムを使用して信頼性およびセキュリティを向上させます。

SA メッセージの制限

デバイスが特定の MSDP ピアから受け入れることができる SA メッセージの総数を制限するには、**ipmsdpsa-limit** コマンドを使用します。**ipmsdpsa-limit** コマンドが設定されている場合、デバイスは SA キャッシュに保存された SA メッセージの数をピアごとに維持し、そのピアに設定された SA メッセージの制限に達した場合は、ピアからの新しいメッセージを無視します。

MSDP 対応デバイスをサービス妨害（DoS）攻撃から保護する手段として、**ipmsdpsa-limit** コマンドが導入されました。デバイスですべての MSDP ピアリングに対する SA メッセージの制限を設定することを推奨します。適度に低い SA 制限をスタブ MSDP リージョンとのピアリングに設定する必要があります（たとえば、さらにダウンストリーム ピアを持つが、インターネットの残りの部分で SA メッセージの中継として動作しないピアなど）。インターネット上の SA メッセージの中継として動作するすべての MSDP ピアリングに高い SA 制限を設定する必要があります。

MSDP キープアライブ インターバルおよび保留時間インターバル

ip msdp keepalive コマンドは、MSDP ピアがキープアライブ メッセージを送信する間隔、および MSDP ピアが他のピアがダウンしたと宣言するまでに他のピアからのキープアライブ メッセージを待機する間隔を調整するために使用します。

MSDP のピアリング セッションが確立されると、接続の各サイドでキープアライブ メッセージを送信し、キープアライブ タイマーを設定します。キープアライブ タイマーの期限が切れ

ると、ローカル MSDP ピアはキープアライブ メッセージを送信し、キープアライブ タイマーを再開します。この間隔をキープアライブ インターバルといいます。*keepalive-interval* 引数は、キープアライブ メッセージの送信間隔を調整するために使用されます。キープアライブ タイマーは、ピアがアップ状態のときに *keepalive-interval* 引数に指定された値に設定されます。MSDP キープアライブ メッセージがピアに送信され、タイマーが期限切れになったときにリセットされると、キープアライブ タイマーは *keepalive-interval* 引数の値にリセットされます。キープアライブ タイマーは、MSDP ピアリング セッションがクローズすると削除されます。デフォルトでは、keepalive タイマーは 60 秒に設定されます。

（注） *keepalive-interval* 引数に指定される値は、*holdtime-interval* 引数に指定される値未満にしなければならず、また、1 秒以上に設定する必要があります。

保留時間タイマーは、MSDP ピアリング接続が確立されると *hold-time-interval* 引数の値に初期化され、MSDP キープアライブ メッセージが受信されると *hold-time-interval* 引数の値にリセットされます。保留時間タイマーは、MSDP ピアリング接続がクローズすると削除されます。デフォルトでは、保留時間インターバルは 75 秒に設定されています。

MSDP ピアが他のピアがダウンしたと宣言するまで他のピアからのキープアライブ メッセージを待機する間隔を調整するには、*hold-time-interval* 引数を使用します。

MSDP 接続再試行インターバル

ピアリング セッションがリセットされてからピアリング セッションの再確立が試行されるまですべての MSDP ピアが待機する間隔を調整できます。この間隔は、接続再試行間隔と呼ばれます。デフォルトでは、ピアリングセッションがリセットされてから他のピアとのピアリングセッションの再確立が試行されるまで MSDP ピアは 30 秒間待機します。変更設定された接続再試行間隔は、デバイス上のすべての MSDP ピアリング セッションに適用されます。

デフォルト MSDP ピア

スタブ自律システムには、冗長性を実現するために複数の RP との MSDP ピアリングが必要な場合もあります。たとえば、RPF チェック メカニズムがないため、SA メッセージは複数のデフォルト ピアから受け入れられません。その代わりに、SA メッセージは 1 つのピアからだけ受け入れられます。そのピアに障害が発生した場合、SA メッセージは別のピアから受け入れられます。もちろん、デフォルトのピアが両方とも同じ SAメッセージを送信することがこの基本的な前提となっています。

下の図に、デフォルトの MSDP ピアが使用されるシナリオを示します。この図では、デバイス B を所有するカスタマーが 2 つのインターネット サービス プロバイダー（ISP）を介してインターネットに接続されています。一方の ISP はデバイス A を所有し、もう一方の ISP はデバイス C を所有しています。どちらもそれらの間で BGP も MBGP も実行していません。カスタマーが ISP ドメインまたは他のドメイン内のソースについて学習するために、デバイス B はデバイス A をデフォルト MSDP ピアとして識別します。デバイス B はデバイス A とデバイス C の両方に SA メッセージをアドバタイズしますが、デバイス A だけまたはデバイス C だけから

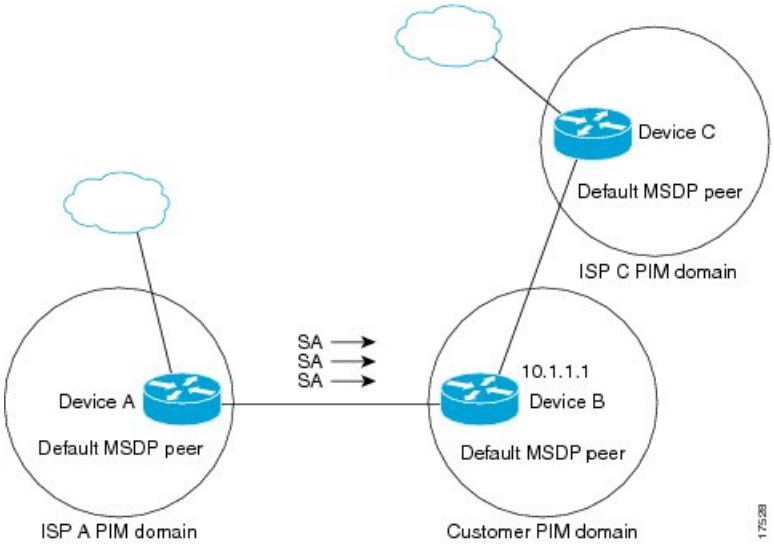
SA メッセージを受け入れます。デバイス A が設定内の最初のデフォルト ピアである場合、デバイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス C からの SA メッセージを受け入れます。

ISP は、プレフィックス リストを使用して、カスタマーのデバイスから受け入れるプレフィックスを定義する場合もあります。カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

カスタマーは 2 つの ISP を使用しています。カスタマーはこの 2 つの ISP をデフォルト ピアとして定義します。設定内で最初のデフォルト ピアとして特定されているピアが稼働している限り、このピアがデフォルト ピアになり、カスタマーはそのピアから受信するすべての SA メッセージを受け入れます。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *31 :* デフォルト *MSDP* ピアのシナリオ



デバイス B はデバイス A およびデバイス C に SA をアドバタイズしますが、デバイス A またはデバイス C だけを使用して SA メッセージを受け入れます。デバイス A が設定内の最初のデバイスである場合、デバイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス C から SA メッセージを受け入れます。これは、プレフィックス リストを使用しない動作です。

プレフィックス リストを指定すると、リスト内のプレフィックスに対してだけピアはデフォルト ピアになります。プレフィックス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。プレフィックス リストがない場合も、複数のデフォルト ピアを設定できますが、アクティブなデフォルト ピアになるのは最初のピアだけです（このピアにデバイスが接続されていて、ピアがアクティブの場合に限ります）。最初に設

定されたピアがダウンするか、このピアとの接続がダウンした場合、2 番目に設定されたピアがアクティブなデフォルト ピアになります。以下同様です。

関連トピック

デフォルトの MSDP ピアの設定 （709 ページ）
例：デフォルト MSDP ピアの設定 （725 ページ）

MSDP メッシュ グループ

MSDP メッシュ グループは、MSDP によってフル メッシュ型に相互接続された MSDP スピーカーのグループです。つまり、グループの各 MSDP ピアには、グループ内の他のすべての MSDP ピアとの MSDP ピアリング関係（MSDP 接続）が必要です。MSDP メッシュ グループが MSDP ピアのグループ間に設定されている場合、SA メッセージのフラッディングが削減されます。グループ内の MSDP ピアがグループ内の別の MSDP ピアから SA メッセージを受信すると、この SA メッセージはグループ内のその他のすべての MSDP ピアに送信されたとみなされるためです。その結果、受信側の MSDP ピアがグループ内の他の MSDP ピアに SA メッセージをフラッディングする必要はありません。

関連トピック

MSDP メッシュ グループの設定 （710 ページ）
例：MSDP メッシュ グループの設定 （727 ページ）

MSDP メッシュ グループの利点

- SA フラッディングの最適化：グループ内に複数のピアがある場合、SA フラッディングを最適化するために MSDP メッシュ グループは特に有用です。
- インターネットを通過する SA トラフィック量の削減：MSDP メッシュ グループを使用すると、SA メッセージは他のメッシュ グループ ピアにフラッディングされません。
- 着信 SA メッセージの RPF チェックの省略：MSDP メッシュ グループが設定されていると、メッシュ グループ ピアからの SA メッセージは常に受け入れられます。

SA 発信フィルタ

デフォルトでは、MSDP を実行するように設定されている RP は、それが RP であるすべてのローカル ソースの SA メッセージを発信します。そのため、RP に登録されているローカル ソースは SA メッセージでアドバタイズされますが、これが望ましくない場合もあります。たとえば、PIM-SM ドメイン内のソースがプライベートアドレス（たとえば、ネットワーク 10.0.0.0/8）を使用している場合、SA 発信フィルタを設定してこれらのアドレスがインターネット上の他の MSDP ピアにアドバタイズされないようにする必要があります。

SA メッセージでアドバタイズされるソースを制御するには、RP に SA 発信フィルタを設定します。SA 発信フィルタを作成すると、SA メッセージでアドバタイズされるソースを次のように制御できます。

- デバイスが SA メッセージでローカル ソースをアドバタイズしないように RP を設定できます。この場合もデバイスは通常の方法で他の MSDP ピアからの SA メッセージを転送します。ローカル ソースの SA メッセージは発信しません。
- 拡張アクセス リストで定義されている（S, G）ペアと一致する、特定のグループに送信するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- AS パス アクセス リストで定義されている AS パスと一致する、特定のグループに送信するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- ルート マップで定義されている基準と一致するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- 拡張アクセス リスト、AS パス アクセス リスト、およびルート マップ（またはそれらのその組み合わせ）を含む SA 発信フィルタを設定します。この場合、ローカル ソースが SA メッセージでアドバタイズされる前に、すべての条件を満たしている必要があります。

MSDP での発信フィルタ リストの使用

デフォルトでは、MSDP 対応デバイスは、受信したすべての SA メッセージをその MSDP ピアすべてに転送します。ただし、発信フィルタ リストを作成することで、SA メッセージが MSDP ピアに転送されないようにできます。発信フィルタ リストは、ローカルに発信されたか別の MSDP ピアから受信したかに関係なくすべての SA メッセージに適用されますが、SA 発信フィルタはローカルに発信された SA メッセージだけに適用されます。ローカル デバイスから発信される MSDP SA メッセージのフィルタをイネーブルにする方法の詳細については、「ローカル ソースの RP によって発信された SA メッセージの制御」の項を参照してください。

発信フィルタ リストを作成すると、デバイスがピアへ転送する SA メッセージを次のように制御できます。

- 指定した MSDP ピアへ転送したすべての発信 SAメッセージをフィルタリングするには、MSDP ピアへの SA メッセージの転送を停止するようにデバイスを設定します。
- 指定した MSDP ピアへ転送した発信 SA メッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアに基づいてフィルタリングするには、拡張アクセス リストで許可されている（S, G）ペアに一致する MSDP ピアへの SA メッセージだけを転送するようにデバイスを設定します。その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- 指定した MSDP へ転送した発信 SA メッセージのサブセットをルート マップに定義された一致基準に基づいてフィルタリングするには、ルート マップに定義された基準に一致する SA メッセージだけを転送するようにデバイスを設定します。その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- 指定したピアからの発信 SA メッセージのサブセットを SA メッセージに含まれているアナウンス側 RP アドレスに基づいてフィルタリングするには、SA メッセージが1 つ以上の

MSDP ピアに送信されていても、それらの発信元に基づいて発信 SA メッセージをフィルタリングするようにデバイスを設定します。その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。

- 拡張アクセス リスト、ルート マップ、および RP アクセス リストまたは RP ルート マップのいずれかを含む発信フィルタ リストを設定できます。この場合、MSDP ピアで発信 SA メッセージを転送するにはすべての条件を満たしている必要があります。

⚠

注意 SA メッセージの任意のフィルタリングを実行すると、ダウンストリーム MSDP ピアで正当なアクティブソースの SA メッセージを受信できなくなることがあります。そのため、このタイプのフィルタを使用する場合は注意が必要です。通常、発信フィルタ リストは、プライベートアドレスを使用するソースなど、望ましくないソースを拒否するためだけに使用します。

MSDP での着信フィルタ リストの使用

デフォルトでは、MSDP 対応デバイスは MSDP ピアからそのデバイスに送信されたすべての SA メッセージを受信します。ただし、着信フィルタ リストを作成することによって、MSDP ピアからデバイスが受信する送信元情報を制御できます。

着信フィルタ リストを作成すると、デバイスがピアから受信する着信 SA メッセージを次のように制御できます。

- 指定した MSDP ピアからのすべての着信 SAメッセージをフィルタリングするには、指定した MSDP ピアから送信されたすべての SAメッセージを無視するようにデバイスを設定します。
- 指定したピアからの着信 SA メッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアに基づいてフィルタリングするには、拡張アクセス リストに定義された（S, G）ペアに一致する MSDP ピアからの SA メッセージだけを受信するようにデバイスを設定します。MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 指定したピアからの着信 SA 要求メッセージのサブセットをルート マップに定義された一致基準に基づいてフィルタリングするには、ルート マップに指定された基準に一致する SA メッセージだけを受信するようにデバイスを設定します。MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 指定したピアからの着信 SA メッセージのサブセットを拡張アクセス リストに定義された（S,G）ペアと、ルートマップに定義された基準の両方に基づいてフィルタリングするには、拡張アクセス リストに定義された（S, G）ペアと、ルート マップに定義された基準の両方に一致する着信 SA メッセージだけを受信するようにデバイスを設定します。MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 指定したピアからの着信 SA メッセージのサブセットを SA メッセージに含まれているアナウンス側 RP アドレスに基づいてフィルタリングするには、SA メッセージがすでに1 つ以上の MSDP ピア全体に送信されている可能性がある場合でも、それらの発信元に基づいて着信 SA メッセージをフィルタリングするようにデバイスを設定します。

- 拡張アクセス リスト、ルート マップ、および RP アクセス リストまたは RP ルート マップのいずれかを含む着信フィルタ リストを設定できます。この場合、MSDP ピアで着信 SA メッセージを受信するにはすべての条件を満たしている必要があります。

⚠

注意 SA メッセージの任意のフィルタリングを実行すると、ダウンストリーム MSDP ピアで正当なアクティブソースの SA メッセージを受信できなくなることがあります。そのため、このタイプのフィルタを使用する場合は注意が必要です。通常、着信フィルタ リストは、プライベート アドレスを使用するソースなど、望ましくないソースを拒否するためだけに使用されます。

MSDP の TTL しきい値

存続可能時間（TTL）値を使用して、ドロップされる前にパケットが取得できるホップの数を制限できます。特定の MSDP ピアに送信された、データがカプセル化された SA メッセージの TTL を指定するには、**ip multicast ttl-threshold** コマンドを使用します。デフォルトでは、パケットの TTL 値が 0（標準 TTL 動作）より大きい場合は、SA メッセージのマルチキャスト データ パケットは MSDP ピアに送信されます。

一般に、TTL しきい値の問題は、SA メッセージ内でソースの初期マルチキャスト パケットがカプセル化されることによって発生することがあります。マルチキャスト パケットはユニキャスト SA メッセージ内部でカプセル化されるため（TTL は 255）、SA メッセージが MSDP ピアに送信されるときに TTL は減少しません。さらに、マルチキャスト トラフィックおよびユニキャスト トラフィックは MSDP ピア、したがってリモート PIM-SM ドメインへのまったく異なるパスに従うため、SA メッセージが通過するホップの総数は、通常のマルチキャスト パケットとは大きく異なります。その結果、カプセル化されたパケットは TTL しきい値に違反することになります。この問題を解決するには、**ip multicast ttl-threshold** コマンドを使用して、特定の MSDP ピアに送信された SA メッセージにカプセル化されているマルチキャスト パケットに関連付けられた TTL しきい値を設定します。**ip msdp ttl-threshold** コマンドを使用すると、IP ヘッダーの TTL が *ttl-value* 引数に指定されている TTL 値未満であるマルチキャスト パケットが、ピアに送信される SA メッセージにカプセル化されないようにすることができます。

SA 要求メッセージ

1 つ以上の指定した MSDP ピアに SA 要求メッセージを送信するように非キャッシュ デバイスを設定できます。

非キャッシュ RP に SA をキャッシュする MSDP ピアがある場合、非キャッシュ ピアが SA 要求メッセージを送信できるようにすると非キャッシュ ピアの参加遅延を低減できます。ホストが特定のグループに対して加入を要求すると、非キャッシュ RP は SA 要求メッセージをキャッシュ ピアに送信します。ピアがこの特定のグループのソース情報をキャッシュしている場合、SA 応答メッセージで要求側の RP に情報を送信します。要求側の RP は SA 応答内の情報を使用しますが、他のピアにメッセージを転送しません。非キャッシュ RP が SA 要求を受信すると、要求者にエラー メッセージを返します。

（注） 現行のすべてのサポート対象のソフトウェア リリースでは、MSDP SA メッセージのキャッシュは必須であり、手動でイネーブルまたはディセーブルにすることはできません。デフォルトでは、MSDP ピアが設定されると、設定コマンドが自動的に実行コンフィギュレーションに追加されます。

SA 要求フィルタ

デフォルトでは、デバイスはその MSDP ピアからのすべての発信 SA 要求メッセージを受け入れます。つまり、デバイスはキャッシュされたソース情報を要求側の MSDP ピアに SA 応答メッセージで送信します。デバイスが特定のピアから受け入れる発信 SA 要求メッセージを制御するには、SA 要求フィルタを作成します。SA 要求フィルタは、デバイスが MSDP ピアから受け入れる発信 SA 要求を次のように制御します。

- 指定したピアからのすべての SA 要求メッセージをフィルタリングするには、指定した MSDP ピアからのすべての SA 要求を無視するようにデバイスを設定します。
- 指定したピアからの SA 要求メッセージのサブセットを標準アクセス リストに定義されたグループに基づいてフィルタリングするには、標準アクセスリストに定義されたグループに一致する MSDP ピアからの SA 要求メッセージだけを受け入れるようにデバイスを設定します。その他のグループの指定されたピアからの SA 要求メッセージは無視されます。

MSDP を使用して複数の PIM-SM ドメインを相互接続する方法

最初の作業は必須で、他の作業はすべて任意です。

MSDP ピアの設定

（注） MSDP ピアをイネーブルにすることで、MSDP は暗黙的にイネーブルになります。

始める前に

- IP マルチキャスト ルーティングをイネーブルにし、PIM-SM を設定する必要があります。
- 単一の MSDP ピア、デフォルトの MSDP ピア、および MSDP メッシュ グループの場合を除き、すべての MSDP ピアは MSDP に設定される前に BGP を実行するように設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdppeer** {*peer-name*|*peer-address*} [*connect-source type number*] [**remote-as** *as-number*] 例： `Device(config)# ip msdp peer 192.168.1.2 connect-source loopback0`	MSDP をイネーブルにし、DNS 名または IP アドレスで指定される MSDP ピアを設定します。 （注） MSDP ピアとして設定するように選択されたデバイスは、通常は BGP ネイバーでもあります。そうでない場合は、デフォルトの MSDP ピアの設定（709 ページ）または MSDP メッシュ グループの設定（710ページ）を参照してください。 • **connect-source** キーワードを指定した場合、指定されたローカル インターフェイスの *type* と *number* の値で示されるプライマリ アドレスは TCP 接続の送信元 IP アドレスとして使用されます。リモート ドメイン内のデバイスとのピアを確立している境界上の MSDP ピアの場合は特に、**connect-source** キーワードを推奨します。
ステップ 4	**ipmsdpdescription** {*peer-name*|*peer-address*} *text* 例： `Device(config)# ip msdp description 192.168.1.2 router at customer a`	（任意）設定内で、または **show** コマンド出力内で簡単に識別できるように、指定されたピアの説明を設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

関連トピック

MSDP ピア （693 ページ）
例：MSDP ピアの設定 （724 ページ）

MSDP ピアのシャットダウン

MSDP ピアをシャットダウンするには、次の任意の作業を実行します。

複数の MSDP ピアを設定し、そのすべての設定が終了するまではどのピアもアクティブにしない場合は、それぞれのピアをシャットダウンし、ピアごとに設定して、後からそれぞれのピアを起動することができます。その MSDP ピアの設定を失うことなく、MSDP セッションをシャットダウンすることもできます。

（注） MSDP ピアをシャットダウンすると、TCP 接続が終了します。**no ip msdp shutdown** コマンドを（指定したピアに対して）使用し、ピアを起動するまではこの接続は再開されません。

始める前に

MSDP が動作していて、MSDP ピアを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpshutdown** {*peer-name* | *peer-address*} 例：	指定された MSDP ピアを管理シャットダウンします。

	コマンドまたはアクション	目的
	`Device(config)# ip msdp shutdown 192.168.1.3`	
ステップ 4	別の MSDP ピアをシャットダウンするには、ステップ 3 を繰り返します。	--
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

関連トピック

MSDP ピア （693 ページ）
例：MSDP ピアの設定 （724 ページ）

MSDP ピア間の MSDP MD5 パスワード認証の設定

MSDP ピア間の MSDP Message Digest 5（MD5）パスワード認証を設定するには、次の任意の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdppassword peer** {*peer-name* | *peer-address*} [*encryption-type*] *string* 例： `Device(config)# ip msdp password peer 10.32.43.144 0 test`	2 つの MSDP ピア間の TCP 接続の MD5 パスワード暗号化をイネーブルにします。 （注） どちらの MSDP ピアでも同じパスワードを使用して MD5 認証を設定する必要があります。そうしない場合は、これらの間の接続が確立されません。

	コマンドまたはアクション	目的
		• 2 つの MSDP ピアの間で MD5 認証に使用されるパスワードやキーを設定または変更した場合、パスワードの設定後にローカル デバイスの既存のセッションは切断されません。新しいパスワードまたは変更されたパスワードをアクティブにするには、手動でセッションを切断する必要があります。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**showipmsdppeer**[peer-address | peer-name] 例： `Device# show ip msdp peer`	（任意）MSDP ピアに関する詳細情報を表示します。 （注） このコマンドを使用して、MSDP ピアで MD5 パスワード認証がイネーブルになっているかどうかを確認します。

関連トピック

MSDP MD5 パスワード認証 （693 ページ）
例：MSDP MD5 パスワード認証の設定 （724 ページ）

トラブルシューティングのヒント

デバイスにMSDP ピア用のパスワードが設定されているが、MSDP ピアには設定されていない場合、デバイスがそれらの間でMSDP セッションを確立しようとすると、次のようなメッセージがコンソールに表示されます。

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

同様に、2 台のデバイスに異なるパスワードが設定されている場合、次のようなメッセージがコンソールに表示されます。

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

debug ip tcp transactions コマンドを使用すると、ステートの変更、再送、重複するパケットなどの重要な TCP トランザクションに関する情報が表示されます。MSDP MD5 パスワード認証のモニタリングまたはトラブルシューティングでは、**debug ip tcp transactions** コマンドを使用

して、MD5 パスワードが有効かどうか、およびキープアライブ メッセージが MSDP ピアで受信されるかどうかを確認します。

SA キャッシュ内で許可される特定の MSDP ピアからの SA メッセージ数の制限によるサービス拒絶（DoS）攻撃の防止

デバイスが指定された MSDP ピアから受け入れることができる SA メッセージの総数を制限するには、このオプションの（しかし強く推奨されます）タスクを実行します。この作業を実行することで、MSDP 対応デバイスを分散型サービス妨害（DoS）攻撃から保護します。

（注） デバイス上のすべての MSDP ピアリングに対してこの作業を実行することを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpsa-limit** {*peer-address* | *peer-name*} *sa-limit* 例： `Device(config)# ip msdp sa-limit 192.168.10.1 100`	SA キャッシュ内で許可される特定の MSDP ピアからの SA メッセージの数を制限します。
ステップ 4	別の MSDP ピアの SA 制限を設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**showipmsdpcount** [*as-number*] 例：	（任意）MSDP SA メッセージ内で発信されたソースおよびグループの数、およ

	コマンドまたはアクション	目的
	`Device# show ip msdp count`	びSA キャッシュ内の MSDP ピアからの SA メッセージの数を表示します。
ステップ 7	**showipmsdppeer** [*peer-address* | *peer-name*] 例： `Device# show ip msdp peer`	（任意）MSDP ピアに関する詳細情報を表示します。 （注） このコマンドの出力には、キャッシュに格納されている MSDP ピアから受信した SA メッセージの数が表示されます。
ステップ 8	**showipmsdpsummary** 例： `Device# show ip msdp summary`	（任意）MSDP ピアのステータスを表示します。 （注） このコマンドの出力には、キャッシュに格納されている SA の数を表示するピアごとの「SA Count」フィールドが表示されます。

MSDP キープアライブ インターバルおよび保留時間インターバルの調整

MSDP ピアがキープアライブ メッセージを送信する間隔、および MSDP ピアが他のピアがダウンしたと宣言するまでに他のピアからのキープアライブ メッセージを待機する間隔を調整するには、次の任意の作業を実行します。デフォルトでは、MSDP ピアが別の MSDP ピアとのピアリング セッションのダウンを検出するまでに 75 秒かかる場合があります。冗長 MSDP ピアが設定されたネットワーク環境では、保持時間間隔を短縮すると、MSDP ピアの障害発生時に MSDP ピアの再コンバージェンス時間を短縮できます。

（注） コマンドのデフォルトは RFC 3618、*Multicast Source Discovery Protocol* に従うため、**ipmsdpkeepalive** コマンドのデフォルトを変更しないことを推奨します。デフォルトの変更が必要なネットワーク環境の場合は、MSDP ピアリングセッションの終了時の *keepalive-interval* と *hold-time-interval*の両方の引数に同じ時刻値を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpkeepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval* 例： `Device(config)# ip msdp keepalive 10.1.1.3 40 55`	MSDP ピアがキープアライブ メッセージを送信する間隔、および MSDP ピアが他のピアがダウンとしたと宣言するまでに他のピアからのキープアライブメッセージを待機する間隔を設定します。
ステップ 4	別の MSDP ピアのキープアライブ メッセージの間隔を調整するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP 接続再試行インターバルの調整

ピアリング セッションがリセットされてからピアリング セッションの再確立が試行されるまで MSDP ピアが待機する間隔を調整するには、次のオプション タスクを実行します。取引フロアのネットワーク環境など、SA メッセージの高速リカバリが必要なネットワーク環境では、接続再試行間隔をデフォルト値の 30 秒未満の時間値に減らすことができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdptimer** *connection-retry-interval* 例： `Device# ip msdp timer 45`	ピアリング セッションがリセットされてからピアリング セッションの再確立が試行されるまで MSDP ピアが待機する間隔を設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

デフォルトの MSDP ピアの設定

デフォルト MSDP ピアを設定するには、次の任意の作業を実行します。

始める前に

デフォルト MSDP ピアは、事前に設定されている MSDP ピアでなければなりません。デフォルト MSDP ピアを設定する前に、まず MSDP ピアを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpdefault-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*] 例： `Device(config)# ip msdp default-peer 192.168.1.3`	すべての MSDP SA メッセージの受信元となるデフォルト ピアを設定します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

関連トピック

デフォルト MSDP ピア （695 ページ）
例：デフォルト MSDP ピアの設定 （725 ページ）

MSDP メッシュ グループの設定

MSDP メッシュ グループを設定するには、次の任意の作業を実行します。

（注） デバイスごとに複数のメッシュ グループを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*} 例：	MSDP メッシュ グループを設定し、MSDP ピアがそのメッシュ グループに属することを指定します。

	コマンドまたはアクション	目的
	`Device(config)# ip msdp mesh-group peermesh`	（注） メッシュ グループに参加しているデバイス上のすべての MSDP ピアは、そのグループ内の他のすべての MSDP ピアと完全にメッシュ構造になっている必要があります。 各デバイスの各 MSDP ピアは、**ip msdp peer** コマンドを使用してピアとして、また、 **ip msdp mesh-group** コマンドを使用してそのメッシュ グループのメンバとしても設定されている必要があります。
ステップ 4	MSDP ピアをメッシュ グループのメンバとして追加するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

関連トピック

MSDP メッシュ グループ （697 ページ）
例：MSDP メッシュ グループの設定 （727 ページ）

ローカル ソースの RP によって発信された SA メッセージの制御

SA メッセージでアドバタイズされる登録ソースを制限するフィルタをイネーブルにして、RP によって発信された SA メッセージを制御するには、次の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpredistribute**[**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*] 例： `Device(config)# ip msdp redistribute route-map customer-sources`	ローカル デバイスによって発信される MSDP SA メッセージのフィルタをイネーブルにします。 （注） **ipmsdpredistribute** コマンドは、RP で認識されているが登録されていないソースをアドバタイズするために使用することもできます。ただし、RP に登録されていないソースのアドバタイズメントは発信しないことを強く推奨します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

発信フィルタ リストを使用した SA メッセージの MSDP ピアへの転送の制御

発信フィルタ リストを設定して SA メッセージの MSDP ピアへの転送を制御するには、次の任意の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpsa-filterout** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] 例： `Device(config)# ip msdp sa-filter out 192.168.1.5 peerone`	発信 MSDP メッセージのフィルタをイネーブルにします。
ステップ 4	別の MSDP ピアの発信フィルタ リストを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

着信フィルタ リストを使用した MSDP ピアからの SA メッセージの受信の制御

MSDP ピアからの着信 SA メッセージの受信を制御するには、次の任意の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpsa-filterin** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] 例： `Device(config)# ip msdp sa-filter in 192.168.1.3`	着信 MSDP SA メッセージのフィルタをイネーブルにします。
ステップ 4	別の MSDP ピアの着信フィルタ リストを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

TTL しきい値を使用した SA メッセージで送信されたマルチキャスト データの制限

SA メッセージで送信されるマルチキャスト データを制限するために存続可能時間（TTL）しきい値を確立するには、次の任意の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipmsdpttl-threshold** {*peer-address* | *peer-name*} *ttl-value* 例： 例： `Device(config)# ip msdp ttl-threshold 192.168.1.5 8`	ローカル デバイスにより発信される MSDP メッセージの TTL 値を設定します。 • デフォルトでは、パケットの TTL 値が 0（標準 TTL 動作）より大きい場合は、SA メッセージのマルチキャスト データ パケットは MSDP ピアに送信されます。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP ピアへの送信元情報の要求

デバイスが MSDP ピアから送信元情報を要求できるようにするには、次の任意の作業を実行します。

（注） シスコの以前のソフトウェア リリースでは SA キャッシングはデフォルトでイネーブルになっており、明示的にイネーブルまたはディセーブルにすることはできないため、この作業はほとんど必要ありません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpsa-request** {*peer-address* | *peer-name*} 例：	デバイスが指定された MSDP ピアに SA 要求メッセージを送信するように指定します。

	コマンドまたはアクション	目的
	`Device(config)# ip msdp sa-request 192.168.10.1`	
ステップ 4	デバイスが別の MSDP キャッシュ ピアに SA 要求メッセージを送信するように指定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SA 要求フィルタを使用した MSDP ピアからの発信 SA 要求メッセージに対する応答の制御

デバイスが MSDP ピアから受け入れる発信 SA 要求メッセージを制御するには、次の任意の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpfilter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*] 例： `Device(config)# ip msdp filter sa-request 172.31.2.2 list 1`	発信 SA 要求メッセージのフィルタをイネーブルにします。 （注） MSDP ピアには SA 要求フィルタを 1 つだけ設定できます。
ステップ 4	別の MSDP ピアの SA 要求フィルタを設定するには、ステップ 3 を繰り返します。	--

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

境界 PIM デンス モード領域の MSDP への包含

PIM デンス モード（PIM-DM）リージョンでアクティブなソースの SA メッセージを送信するように境界デバイスを設定するには、次の任意の作業を実行します。

PIM-SM リージョンと PIM-DM リージョンの境界にデバイスを設定できます。デフォルトでは、PIM-DM ドメインのソースは MSDP に含まれません。PIM-DM ドメインでアクティブなソースの SA メッセージを送信するようにこの境界デバイスを設定できます。その場合、**ipmsdpredistribute** コマンドを設定してアドバタイズする PIM-DM ドメインのローカル ソースを制御することも非常に重要です。このコマンドを設定しないと、PIM-DM ドメインのソースが送信を停止した後も長時間(S, G)ステートのままになります。設定の詳細については、「ローカル ソースの RP によって発信された SA メッセージの制御 （711 ページ）」の項を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpbordersa-address** *type number* 例： `Device(config)# ip msdp border sa-address gigabitethernet0/0/0`	PIM-DM ドメインでアクティブなソースの SA メッセージを発信するように、PIM-SM および PIM-DM ドメイン間の境界にデバイスを設定します。 • インターフェイスの IP アドレスは、SA メッセージの RP フィールドに示されるソース ID として使用されます。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RP アドレス以外の発信元アドレスの設定

SA メッセージを発信する MSDP スピーカーがそのインターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用できるようにするには、次の任意の作業を実行します。

また、次のいずれかの理由により、発信元 ID を変更できます。

- Anycast RP の MSDP メッシュ グループに複数のデバイスを設定する場合。
- デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にある場合。デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にあり、PIM-DM ドメイン内のアクティブなソースをアドバタイズする場合は、SA メッセージ内の RP アドレスが発信元デバイスのインターフェイスのアドレスになるように設定します。

始める前に

MSDP がイネーブルになり、MSDP ピアが設定されます。MSDP ピアの設定の詳細については、MSDP ピアの設定 （701 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdporiginator-id** *type number* 例： `Device(config)# ip msdp originator-id ethernet 1`	発信元デバイスのインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP のモニタリング

MSDP の SA メッセージ、ピア、ステート、およびピアのステータスをモニタリングするには、次の任意の作業を実行します。

手順

ステップ 1 **enable**

例：

```
Device# enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **debugipmsdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]

このコマンドを使用して、MSDP アクティビティをデバッグします。

オプションの *peer-address* または *peer-name* 引数を使用して、デバッグ イベントをログに記録するピアを指定します。

次に、**debugipmsdp** コマンドの出力例を示します。

例：

```
Device# debug ip msdp
MSDP debugging is on
Device#
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.254: Received 1028-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1028, ec: 85, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1028-byte SA to peer
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.250: Received 56-byte message from peer
MSDP: 224.150.44.250: SA TLV, len: 56, ec: 4, RP: 192.168.76.241
MSDP: 224.150.44.250: Peer RPF check passed for 192.168.76.241, used EMBGP peer
MSDP: 224.150.44.254: Forward 56-byte SA to peer
```

```
MSDP: 224.150.44.254: Received 116-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 116, ec: 9, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 116-byte SA to peer
MSDP: 224.150.44.254: Received 32-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 32, ec: 2, RP: 172.31.3.78
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.78, used EMBGP peer
MSDP: 224.150.44.250: Forward 32-byte SA to peer
```

ステップ 3 **debugipmsdpresets**

このコマンドを使用して、MSDP ピアのリセット理由をデバッグします。

例：

```
Device# debug ip msdp resets
```

ステップ 4 **showipmsdpcount** [*as-number*]

このコマンドを使用して、MSDP SA メッセージ内で発信したソースおよびグループの数、および SA キャッシュ内の MSDP ピアからの SA メッセージの数を表示します。**ipmsdpcache-sa-state** コマンドは、このコマンドによって出力が生成されるように設定する必要があります。

次に、**showipmsdpcount** コマンドの出力例を示します。

例：

```
Device# show ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
    192.168.4.4: 8
SA State per ASN Counters, <asn>: <# sources>/<# groups>
    Total entries: 8
    ?: 8/8
```

ステップ 5 **showipmsdppeer** [*peer-address* | *peer-name*]

このコマンドを使用して、MSDP ピアに関する詳細情報を表示します。

オプションの *peer-address* 引数または *peer-name* 引数を使用して、特定のピアに関する情報を表示します。

次に、**showipmsdppeer** コマンドの出力例を示します。

例：

```
Device# show ip msdp peer 192.168.4.4
MSDP Peer 192.168.4.4 (?), AS 64512 (configured AS)
  Connection status:
    State: Up, Resets: 0, Connection source: Loopback0 (2.2.2.2)
    Uptime(Downtime): 00:07:55, Messages sent/received: 8/18
    Output messages discarded: 0
    Connection and counters cleared 00:08:55 ago
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
```

```
  Peer ttl threshold: 0
  SAs learned from this peer: 8
  Input queue size: 0, Output queue size: 0
  MD5 signature protection on MSDP TCP connection: not enabled
```

ステップ 6 **showipmsdpsa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]

このコマンドを使用して、MSDP ピアから学習した (S, G) ステートを表示します。

次に、**showipmsdpsa-cache** コマンドの出力例を示します。

例：

```
Device# show ip msdp sa-cache
MSDP Source-Active Cache - 8 entries
(10.44.44.5, 239.232.1.0), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer
192.168.4.4
(10.44.44.5, 239.232.1.1), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer
192.168.4.4
(10.44.44.5, 239.232.1.2), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer
192.168.4.4
(10.44.44.5, 239.232.1.3), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer
192.168.4.4
(10.44.44.5, 239.232.1.4), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer
192.168.4.4
(10.44.44.5, 239.232.1.5), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer
192.168.4.4
(10.44.44.5, 239.232.1.6), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer
192.168.4.4
(10.44.44.5, 239.232.1.7), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer
192.168.4.4
```

ステップ 7 **showipmsdpsummary**

このコマンドを使用して、MSDP ピアのステータスを表示します。

次に、**showipmsdp summary** コマンドの出力例を示します。

例：

```
Device# show ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
192.168.4.4      4     Up       00:08:05 0     8     ?
```

MSDP 接続統計情報および SA キャッシュ エントリの消去

MSDP 接続、統計情報または SA キャッシュ エントリを消去するには、次の任意の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clearipmsdppeer** [*peer-address* | *peer-name*] 例： `Device# clear ip msdp peer`	指定された MSDP ピアへの TCP 接続をクリアし、すべての MSDP メッセージ カウンタをリセットします。
ステップ 3	**clearipmsdpstatistics** [*peer-address* | peer-name] 例： `Device# clear ip msdp statistics`	指定された MSDP ピアの統計カウンタをクリアし、すべての MSDP メッセージ カウンタをリセットします。
ステップ 4	**clearipmsdpsa-cache** [*group-address*] 例： `Device# clear ip msdp sa-cache`	SA キャッシュ エントリを消去します。 • **clearipmsdpsa-cache** コマンドにオプションの *group-address* 引数または *source-address* 引数を指定した場合、すべての SA キャッシュ エントリが消去されます。 • 特定のグループに関連付けられたすべての SA キャッシュ エントリを消去するには、オプションの *group-address* 引数を使用します。

MSDPの簡易ネットワーク管理プロトコル（SNMP）モニタリングのイネーブル化

MSDP の簡易ネットワーク管理プロトコル（SNMP）モニタリングをイネーブルにするには、次の任意の作業を実行します。

始める前に

- SNMP および MSDP はデバイスに設定されています。
- 各 PIM-SM ドメインには、MSDP スピーカーとして設定されているデバイスが必要です。このデバイスは、SNMP と MSDP MIB がイネーブルに設定されている必要があります。

（注）
- すべての MSDP-MIB オブジェクトは読み取り専用として実装されます。
- 要求テーブルは、シスコの MSDP MIB の実装ではサポートされていません。
- msdpEstablished 通知は、シスコの MSDP MIB の実装ではサポートされていません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**snmp-serverenabletrapsmsdp** 例： `Device# snmp-server enable traps msdp`	SNMP で使用される MSDP 通知の送信をイネーブルにします。 （注） **snmp-serverenabletraps msdp** コマンドは、トラップと応答要求の両方をイネーブルにします。
ステップ 3	**snmp-serverhost** *host* [**traps** | **informs**] [**version** {**1** |**2c** | **3** [**auth**|**priv** | **noauth**]}] *community-string* [**udp-port** *port-number*] **msdp** 例： `Device# snmp-server host examplehost msdp`	MSDP トラップまたは応答要求の受信者（ホスト）を指定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

MSDP MIB 通知の結果とソフトウェアの出力を比較するには、適切なデバイスで **showipmsdpsummary** コマンドおよび **showipmsdppeer** コマンドを使用します。また、これらのコマンドの結果と SNMP GET 操作の結果を比較することもできます。SA キャッシュ テーブル エントリを確認するには、**showipmsdpsa-cache** コマンドを使用します。接続のローカル アドレス、ローカル ポート、リモート ポートなどのその他のトラブルシューティング情報は、**debugipmsdp** コマンドの出力を使用して取得できます。

MSDP を使用して複数の PIM-SM ドメインを相互接続する設定例

例：MSDP ピアの設定

次に、3 つの MSDP ピア間で MSDP ピアリング接続を確立する例を示します。

デバイス A

```
!
interface Loopback 0
 ip address 10.220.8.1 255.255.255.255
!
ip msdp peer 10.220.16.1 connect-source Loopback0
ip msdp peer 10.220.32.1 connect-source Loopback0
!
```

デバイス B

```
!
interface Loopback 0
 ip address 10.220.16.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect connect-source Loopback0
ip msdp peer 10.220.32.1 connect connect-source Loopback0
!
```

デバイス C

```
!
interface Loopback 0
 ip address 10.220.32.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect 10.220.8.1 connect-source Loopback0
ip msdp peer 10.220.16.1 connect 10.220.16.1 connect-source Loopback0
!
```

関連トピック

MSDP ピア （693 ページ）
MSDP ピアの設定 （701 ページ）
MSDP ピアのシャットダウン （703 ページ）

例：MSDP MD5 パスワード認証の設定

次に、2 つの MSDP ピア間の TCP 接続の MD5 パスワード認証をイネーブルにする例を示します。

デバイス A

```
!
ip msdp peer 10.3.32.154
ip msdp password peer 10.3.32.154 0 test
!
```

デバイス B

```
!
ip msdp peer 10.3.32.153
ip msdp password peer 10.3.32.153 0 test
!
```

関連トピック

MSDP ピア間の MSDP MD5 パスワード認証の設定 （704 ページ）
MSDP MD5 パスワード認証 （693 ページ）

例：デフォルト MSDP ピアの設定

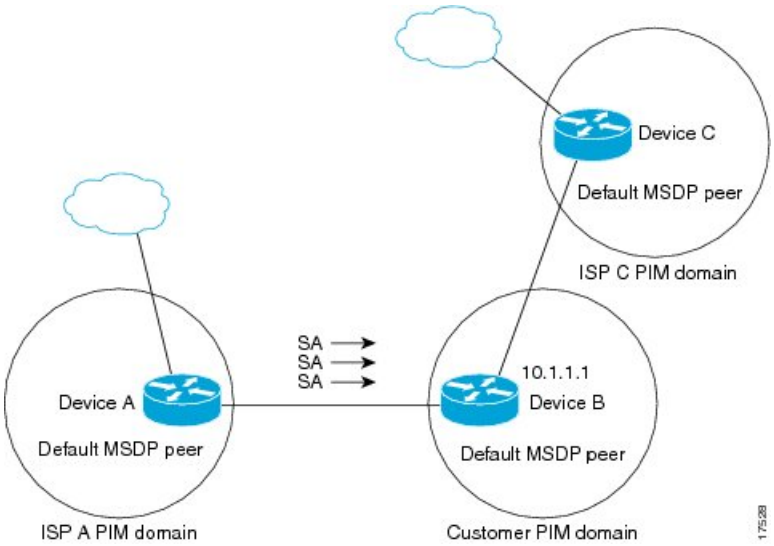
下の図に、デフォルトの MSDP ピアが使用されるシナリオを示します。この図では、デバイス B を所有するカスタマーが 2 つの ISP を介してインターネットに接続されています。一方の ISP はデバイス A を所有し、もう一方の ISP はデバイス C を所有しています。どちらもそれらの間で (M)BGP を実行していません。カスタマーが ISP ドメインまたは他のドメイン内のソースについて学習するために、デバイス B はデバイス A をデフォルト MSDP ピアとして識別します。デバイス B はデバイス A とデバイス C の両方に SA メッセージをアドバタイズしますが、デバイス A だけまたはデバイス C だけから SA メッセージを受け入れます。デバイス A が設定内の最初のデフォルト ピアである場合、デバイス A が稼働していれば デバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス C からの SA メッセージを受け入れます。

ISP は、プレフィックス リストを使用して、カスタマーのデバイスから受け入れるプレフィックスを定義する場合もあります。カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

カスタマーは 2 つの ISP を使用しています。カスタマーはこの 2 つの ISP をデフォルト ピアとして定義します。設定内で最初のデフォルト ピアとして特定されているピアが稼働している限り、このピアがデフォルト ピアになり、カスタマーはそのピアから受信するすべての SA メッセージを受け入れます。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *32*：デフォルト *MSDP* ピアのシナリオ



デバイス B はデバイス A およびデバイス C に SA をアドバタイズしますが、デバイス A またはデバイス C だけを使用して SA メッセージを受け入れます。デバイス A が設定ファイル内の最初のデバイスである場合、デバイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス C から SA メッセージを受け入れます。これは、プレフィックス リストを使用しない動作です。

プレフィックスリストを指定すると、リスト内のプレフィックスに対してだけピアはデフォルト ピアになります。プレフィックス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。プレフィックス リストがない場合も、複数のデフォルト ピアを設定できますが、アクティブなデフォルト ピアになるのは最初のピアだけです（このピアにデバイスが接続されていて、ピアがアクティブの場合に限ります）。最初に設定されたピアがダウンするか、このピアとの接続がダウンした場合、2 番目に設定されたピアがアクティブなデフォルト ピアになります。以下同様です。

次に、図に示されているデバイス A およびデバイス C の部分的な設定例を示します。これらの ISP にはそれぞれ、図に示すカスタマーのような、デフォルト ピアリングを使用している複数のカスタマーがいる可能性があります。そのようなカスタマーの設定は類似しています。つまり、SA が対応するプレフィックス リストによって許可される場合、デフォルト ピアからの SA だけを受け入れます。

デバイス A の設定

```
ip msdp default-peer 10.1.1.1
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

デバイス C の設定

```
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

関連トピック

デフォルトの MSDP ピアの設定 （709 ページ）
デフォルト MSDP ピア （695 ページ）

例：MSDP メッシュ グループの設定

次に、3 台のデバイスを MSDP メッシュ グループのフル メッシュ メンバになるように設定する例を示します。

デバイス A の設定

```
ip msdp peer 10.2.2.2
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.2.2.2
ip msdp mesh-group test-mesh-group 10.3.3.3
```

デバイス B の設定

```
ip msdp peer 10.1.1.1
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.3.3.3
```

デバイス C の設定

```
ip msdp peer 10.1.1.1
ip msdp peer 10.2.2.2
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.2.2.2
```

関連トピック

MSDP メッシュ グループの設定 （710 ページ）
MSDP メッシュ グループ （697 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』

関連項目	マニュアル タイトル
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

MIB

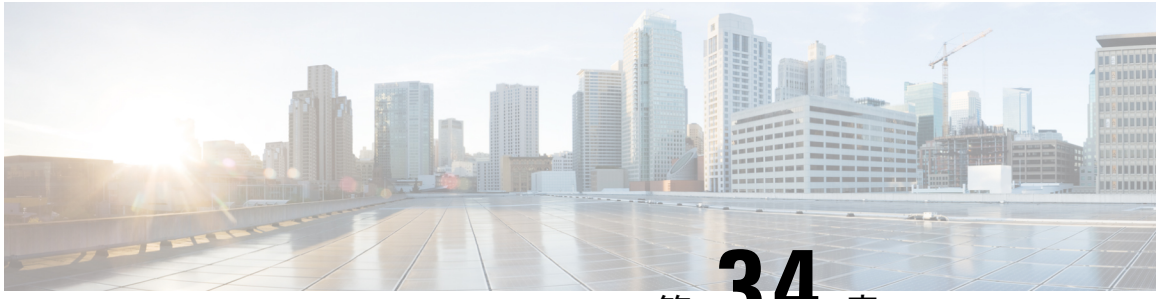
MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Multicast Source Discovery Protocol の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。



第 34 章

ワイヤレス マルチキャストの設定

- 機能情報の確認 （729 ページ）
- ワイヤレス マルチキャスト設定の前提条件 （729 ページ）
- ワイヤレス マルチキャスト設定の制約事項 （730 ページ）
- ワイヤレス マルチキャストに関する情報 （731 ページ）
- ワイヤレス マルチキャストの設定方法 （736 ページ）
- ワイヤレス マルチキャストのモニタリング （743 ページ）
- ワイヤレス マルチキャストの次の作業 （743 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ワイヤレス マルチキャスト設定の前提条件

- IP マルチキャスト ルーティングをイネーブルにし、PIM バージョンと PIM モードを設定する必要があります。デフォルト ルートをデバイスで使用できるようにする必要があります。これらのタスクを実行した後、デバイスはマルチキャスト パケットを転送し、マルチキャスト ルーティング テーブルに読み込むことができるようになります。
- IP マルチキャスティングに加入するには、マルチキャスト ホスト、ルータ、およびマルチレイヤ スイッチで IGMP が動作している必要があります。

- 上でマルチキャスト モードを有効にする場合は、CAPWAP マルチキャスト グループ アドレスも設定する必要があります。アクセス ポイントは、IGMP を使用して CAPWAP マルチキャスト グループをリッスンします。

ワイヤレス マルチキャスト設定の制約事項

次は、IP マルチキャスト ルーティングの設定の制約事項です。

- 監視モード、スニファ モード、または不正検出モードのアクセス ポイントは、CAPWAP マルチキャスト グループ アドレスには加入しません。
- 上で設定されている CAPWAP マルチキャスト グループは、デバイス ごとに異なっている必要があります。
- マルチキャスト ルーティングは、管理インターフェイスには有効にしないでください。

IPv6 スヌーピングの制限

IPv6 スヌーピング機能は、EtherChannel ポートではサポートされません。

IPv6 RA ガードの制限

- IPv6 RA ガード機能は、IPv6 トラフィックがトンネリングされる環境では保護を行いません。
- この機能は、TCAM（Ternary Content Addressable Memory）がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスで設定できます。
- この機能は、ホスト モードとルータ モードをサポートしています。
- この機能は、入力方向だけでサポートされます。出力方向ではサポートされません。
- この機能は、EtherChannel および EtherChannel ポート メンバーではサポートされません。
- この機能は、マージ モードのトランク ポートではサポートされません。
- この機能は、補助 VLAN およびプライベート VLAN（PVLAN）でサポートされています。PVLAN の場合、プライマリ VLAN の機能が継承され、ポート機能とマージされます。
- IPv6 RA ガード機能によってドロップされたパケットはスパニングできます。
- **platform ipv6 acl icmp optimize neighbor-discovery command** コマンドが設定されている場合、IPv6 RA ガード機能は設定できず、エラー メッセージが表示されます。このコマンドは、RA ガードの ICMP エントリを上書きするデフォルトのグローバル Internet Control Message Protocol（ICMP）エントリを追加します。

ワイヤレス マルチキャストに関する情報

ネットワークがパケットのマルチキャストをサポートしている場合は、デバイスが使用するマルチキャストの方法を設定できます。デバイスは次の2つのモードでマルチキャストを実行します。

- ユニキャスト モード：デバイス は、デバイス にアソシエートしているすべてのアクセス ポイントに、すべてのマルチキャスト パケットをユニキャストします。このモードは非効率的ですが、マルチキャストをサポートしないネットワークでは必要な場合があります。
- マルチキャスト モード：デバイス は、マルチキャスト パケットを CAPWAP マルチキャスト グループに送信します。この方法では、デバイス プロセッサのオーバーヘッドが軽減され、パケット レプリケーションの作業はネットワークに移されます。これは、ユニキャストを使った方法より、はるかに効率的です。

マルチキャスト モードが有効な場合に、デバイス がマルチキャスト パケットを有線 LAN から受信すると、デバイス は CAPWAP を使用してパケットをカプセル化し、CAPWAP マルチキャスト グループ アドレスへ転送します。デバイス は、必ず管理 VLAN を使用してマルチキャスト パケットを送信します。マルチキャスト グループのアクセス ポイントはパケットを受け取り、クライアントがマルチキャスト トラフィックを受信する LAN にマップされたすべての BSSID にこれを転送します。

デバイス は、マルチキャスト リスナー検出（MLD)v1 スヌーピングを含む v1 のすべての機能をサポートしていますが、v2 および v3 の機能は制限されます。この機能により、IPv6 マルチキャスト フローが追跡され、フローを要求したクライアントにそれらが配信されます。IPv6 マルチキャストをサポートするには、グローバル マルチキャスト モードを有効にする必要があります。

マルチキャスト パケットのダイレクトを向上させるために、インターネット グループ管理プロトコル（IGMP）スヌーピングを導入しています。この機能が有効になっている場合、デバイス スヌーピングは IGMP レポートをクライアントから収集して処理し、レイヤ 3 マルチキャスト アドレスと VLAN 番号に基づいて一意なマルチキャスト グループ ID（MGID）を作成し、その IGMP レポートを IGMP クエリアへ送信します。次に、デバイス は、アクセス ポイント上のアクセス ポイント MGID テーブルを、クライアント MAC アドレスを使用して更新します。デバイス が特定のマルチキャスト グループのマルチキャスト トラフィックを受信した場合、それをすべてのアクセス ポイントに転送します。ただし、アクティブなクライアントでリッスンしているアクセス ポイント、またはそのマルチキャスト グループへ加入しているアクセス ポイントだけは、その特定の WLAN 上でマルチキャスト トラフィックを送信します。IP パケットは、入力 VLAN および宛先マルチキャスト グループの一意の MGID を使用して転送されます。レイヤ 2 マルチキャスト パケットは、入力 VLAN の一意の MGID を使用して転送されます。

MGID は、CAPWAP ヘッダー内のワイヤレス情報の 16 ビットの予約済みフィールドに入力された 14 ビットの値です。残りの 2 ビットはゼロに設定する必要があります。

関連トピック

ワイヤレス マルチキャスト MCMC モードの設定（CLI）　（736 ページ）

ワイヤレス マルチキャスト MCUC モードの設定（CLI）　（736 ページ）

マルチキャスト最適化について

マルチキャストは、マルチキャスト アドレスと VLAN を 1 つのエンティティ（MGID）としてグループ化することを基本としていました。VLAN グループで、重複したパケットが増加する可能性があります。VLAN グループ機能を使用して、すべてのクライアントがそれぞれ異なる VLAN 上でマルチキャスト ストリームをリッスンします。そのため、デバイスは、マルチキャスト アドレスと VLAN の組み合わせごとに異なる MGID を作成します。その結果、最悪の場合、アップストリーム ルータは VLAN ごとにコピーを 1 つ送信するため、グループ内に存在する VLAN の数だけコピーが作成されます。WLAN はすべてのクライアントに対して同じままなので、マルチキャスト パケットの複数のコピーがワイヤレス ネットワークで送信されます。デバイス とアクセス ポイント間のワイヤレス メディアでマルチキャスト ストリームの重複を抑制するには、マルチキャスト最適化機能を使用できます。

マルチキャスト最適化では、マルチキャスト トラフィック用に使用可能なマルチキャスト VLAN を作成できます。デバイス 内の VLAN の 1 つを、マルチキャスト グループが登録されるマルチキャスト VLAN として設定できます。クライアントは、マルチキャスト VLAN 上でマルチキャスト ストリームをリッスンできます。MGID は、マルチキャスト VLAN とマルチキャスト IP アドレスを使用して生成されます。同じ WLAN の異なる VLAN 上にある複数のクライアントが単一のマルチキャスト IP アドレスをリッスンしている場合、単一の MGID が生成されます。デバイス は、この VLAN グループ上のクライアントからのすべてのマルチキャスト ストリームが常にマルチキャスト VLAN 上に送出されるようにして、その VLAN グループのすべての VLAN に対し、アップストリーム ルータに登録されるエントリが 1 つになるようにします。クライアントが異なる VLAN 上にあっても、1 つのマルチキャスト ストリームだけが VLAN グループにヒットします。したがって、ネットワークで送信されるマルチキャスト パケットは、1 つのストリームだけになります。

関連トピック

WLAN の IP マルチキャスト VLAN の設定（CLI）　（742 ページ）

IPv6 グローバル ポリシー

IPv6 グローバル ポリシーは、ストレージおよびアクセス ポリシー データベースのサービスを提供します。IPv6 ND 検査と IPv6 RA ガードは、IPv6 グローバル ポリシー機能です。ND インスペクションまたは RA ガードをグローバルに設定するたびに、ポリシーの属性が、ソフトウェア ポリシー データベースに保存されます。その後ポリシーはインターフェイスに適用され、ポリシーが適用されたこのインターフェイスを含めるためにソフトウェア ポリシー データベース エントリが更新されます。

IPv6 RA ガード

IPv6 RA ガード機能は、ネットワーク デバイス プラットフォームに到着した不要または不正な RA ガード メッセージを、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。RA は、リンクで自身をアナウンスするためにデバイスによって使

用されます。IPv6 RA ガード機能は、それらの RA を分析して、承認されていないデバイスから送信された RA を除外します。ホスト モードでは、ポート上の RA とルータ リダイレクト メッセージはすべて許可されません。RA ガード機能は、レイヤ 2（L2）デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。L2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます。

IPv6 スヌーピングに関する情報

IPv6 ネイバー ディスカバリ ネイバー インスペクション

IPv6 ネイバー探索インスペクション、または IPv6「スヌーピング」機能によって、複数のレイヤ 2 IPv6 ファーストホップ セキュリティ機能（IPv6 アドレス収集と IPv6 デバイス トラッキングを含む）がバンドルされます。IPv6 ネイバー探索（ND）インスペクションは、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。この機能によって、Duplicate Address Detection（DAD）、アドレス解決、デバイス検出やネイバー キャッシュに対する攻撃といった、ネイバー探索メカニズムに固有のいくつかの脆弱性が軽減されます。

IPv6 ND インスペクションは、レイヤ 2 ネイバー テーブルのステートレス自動設定アドレスのバインディングを学習して保護し、信頼できるバインディング テーブルを構築するために ND メッセージを分析します。有効なバインディングのない IPv6 ND メッセージはドロップされます。ND メッセージは、その IPv6 から MAC へのマッピングが検証可能な場合に信頼できると見なされます。

ターゲット（プラットフォームのターゲット サポートによって異なり、デバイス ポート、スイッチ ポート、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、および VLAN が含まれることがある）に IPv6 ND インスペクションが設定されている場合、IPv6 トラフィックの ND プロトコルと Dynamic Host Configuration Protocol（DHCP）をルーティング デバイスのスイッチ統合セキュリティ機能（SISF）インフラストラクチャにリダイレクトするためのキャプチャ命令がハードウェアにダウンロードされます。ND トラフィックの場合、NS、NA、RS、RA、REDIRECT などのメッセージが SISF にリダイレクトされます。DHCP の場合、ポート 546 または 547 から送信された UDP メッセージがリダイレクトされます。

IPv6 ND インスペクションはその「キャプチャ ルール」を分類子に登録します。分類子では、特定のターゲットにあるすべての機能のルールがすべて集約され、対応する ACL がプラットフォーム依存モジュールにインストールされます。分類子は、リダイレクトされたトラフィックを受信すると、（トラフィックを受信しているターゲットに対して）登録されているすべての機能からすべてのエントリ ポイント（IPv6 ND インスペクションのエントリ ポイントを含む）を呼び出します。このエントリ ポイントは最後に呼び出されるため、他の機能によって行われた決定が IPv6 ND インスペクションの決定よりも優先されます。

IPv6 ND 検査

IPv6 ND 検査は、レイヤ 2 ネイバー テーブルでステートレス自動設定アドレスのバインディングを学習し、保護します。IPv6 ND 検査は、信頼できるバインディング テーブル データベー

スを構築するためにネイバー探索メッセージを分析します。有効なバインディングがないIPv6ネイバー探索メッセージはドロップされます。ネイバー探索メッセージは、その IPv6 から MAC へのマッピングが検証可能な場合に信頼できると見なされます。

この機能によって、Duplicate Address Detection（DAD）、アドレス解決、デバイス検出やネイバーキャッシュに対する攻撃といった、ネイバー探索メカニズムに固有のいくつかの脆弱性が軽減されます。

IPv6 デバイス トラッキング

IPv6 デバイス トラッキングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

IPv6 ファーストホップ セキュリティ バインディング テーブル

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズム機能を使用すると、デバイスのリブート時にバインディングテーブルをリカバリできます。デバイスに接続されている IPv6 ネイバーのデータベース テーブルは、ND スヌーピングなどの情報源から作成されます。このデータベース（またはバインディング）テーブルは、スプーフィングやリダイレクト攻撃を防止するために、リンク層アドレス（LLA）、IPv4 または IPv6 アドレス、およびネイバーのプレフィックス バインディングを検証するためにさまざまな IPv6 ガード機能によって使用されます。

このメカニズムにより、デバイスのリブート時にバインディング テーブルをリカバリできます。リカバリ メカニズムは、不明な送信元、（バインディング テーブルにまだ指定されていない送信元や、ND または DHCP グリーニングを使用して学習されていない送信元）からのデータ トラフィックをブロックします。この機能は、宛先ガードで宛先アドレスの解決に失敗したときに、不足しているバインディングテーブルのエントリをリカバリします。障害が発生すると、バインディングテーブルのエントリは、設定に応じて、DHCP サーバまたは宛先ホストにクエリを実行することでリカバリできます。

リカバリ プロトコルとプレフィックス リスト

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズム機能は、DHCP と NDP の両方でリカバリを試みる前に、一致するプレフィックス リストを提供する機能を導入します。

アドレスがプロトコルと関連付けられているプレフィックスリストと一致しない場合、そのプロトコルではバインディング テーブル エントリのリカバリは試行されません。プレフィックス リストは、プロトコルを使用してレイヤ2ドメインに割り当てられているアドレスに対して有効なプレフィックスに対応している必要があります。デフォルトではプレフィックスリストは存在せず、すべてのアドレスのリカバリが試行されます。プレフィクスリストとプロトコルを関連付けるコマンドは、**protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*] です。

IPv6 デバイス トラッキング

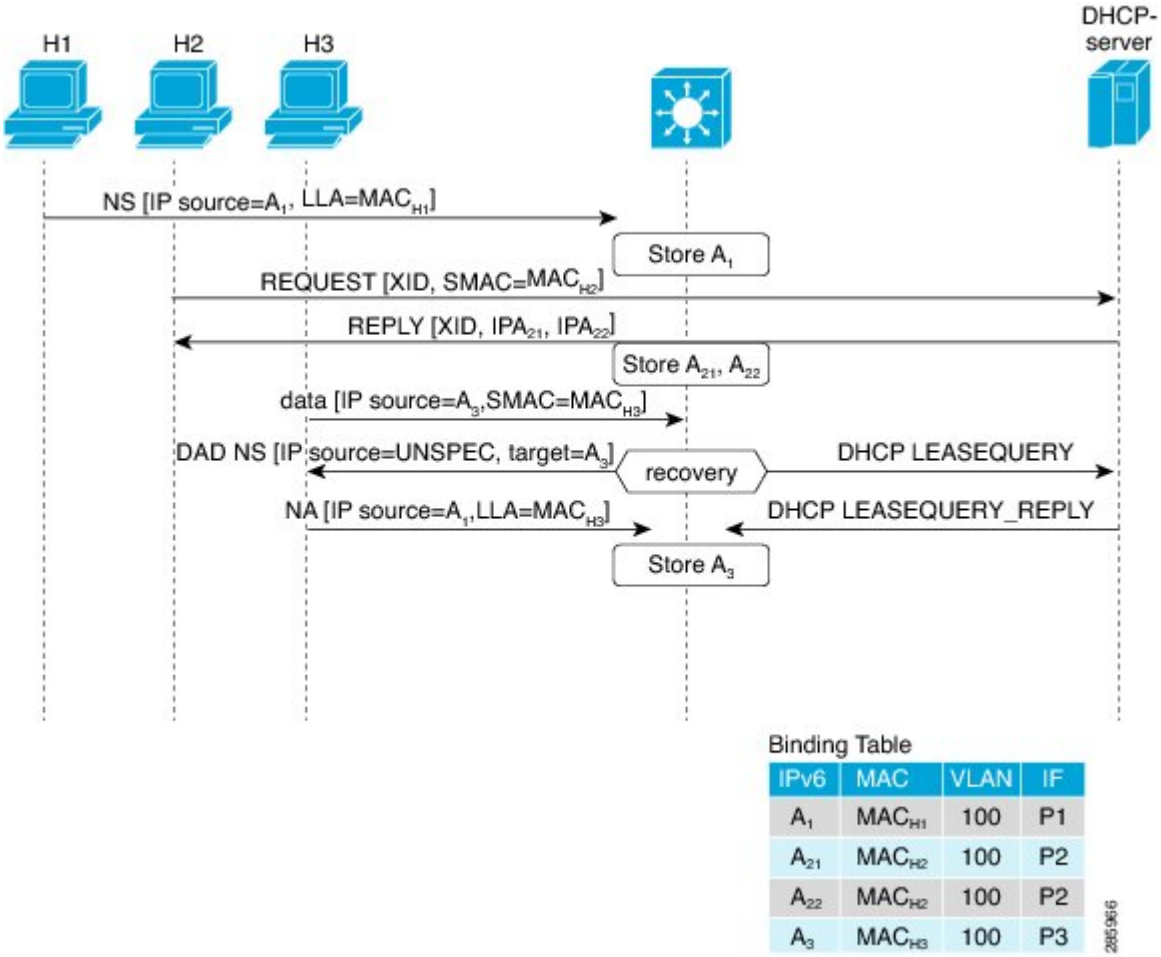
IPv6 デバイス トラッキングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

IPv6 アドレス収集

IPv6 アドレス収集は、正確なバインディング テーブルに依存するその他多くの IPv6 の機能の基盤です。この機能は、アドレス収集のためにリンク上の ND および DHCP メッセージを検査した後に、それらのアドレスをバインディングテーブルに入力します。また、この機能は、アドレスの所有権を強制し、特定のノードが要求可能なアドレスの数を制限します。

次の図は、IPv6 アドレス収集の仕組みを示しています。

図 *33 : IPv6* アドレス収集



ワイヤレス マルチキャストの設定方法

ワイヤレス マルチキャスト MCMC モードの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。

ステップ 3	**wireless multicast**
	例：
	`Device(config)# wireless multicast`
	`Device(config)# no wireless multicast`
		ワイヤレスクライアントへのマルチキャスト トラフィックを有効にします。デフォルト値は disable です。ワイヤレスクライアントへのマルチキャスト トラフィックを無効にするには、コマンドに **no** を追加します。

ステップ 4	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押してコンフィギュレーション モードを終了します。

関連トピック

ワイヤレス マルチキャストに関する情報 （731 ページ）

ワイヤレス マルチキャスト MCUC モードの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 3	**wireless multicast** 例： `Device(config)# wireless multicast`	ワイヤレスクライアントへのマルチキャストトラフィックを有効にして、mDNS ブリッジングを有効にします。デフォルト値は disable です。ワイヤレス クライアントへのマルチキャスト トラフィックを無効にして、mDNS ブリッジングを無効にするには、コマンドに **no** を追加します。
ステップ 4	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押してコンフィギュレーション モードを終了します。

関連トピック

ワイヤレス マルチキャストに関する情報 （731 ページ）

IPv6 スヌーピングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 3	**ipv6 mld snooping** 例： `Device(config)# ipv6 mld snooping`	MLD スヌーピングをイネーブルにします。

IPv6 スヌーピング ポリシーの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 3	**ipv6 snooping policy** *policy-name* 例： `Device(config)# ipv6 snooping policy mypolicy`	名前付きの IPv6 スヌーピング ポリシーを設定します。
ステップ 4	**security-level guard** 例： `Device(config-ipv6-snooping)# security-level guard`	未承認のメッセージを検査してドロップするためのセキュリティ レベルを設定します。
ステップ 5	**device-role node** 例： `Device(config-ipv6-snooping)# device-role node`	接続されたポートに、デバイスのロール（それはノードです）を設定します。
ステップ 6	**protocol** {**dhcp** | **ndp**} 例： `Device(config-ipv6-snooping)# protocol ndp`	DHCP または NDP パケット内のアドレスを収集するためのプロトコルを設定します。

マルチキャスト ルータ ポートとしてのレイヤ 2 ポートの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id***mrouter interface Port-channel** *port-channel-interface-number* 例： `Device(config)# ipv6 mld snooping vlan 2 mrouter interface Port-channel 22`	レイヤ 2 ポートをマルチキャスト ルータ ポートとして設定します。VLAN はクライアント VLAN です。

IPv6 RA ガードの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 3	**ipv6 nd raguard policy** *policy-name* 例： `Device(config)# ipv6 nd raguard policy myraguardpolicy`	RA ガードのポリシーを設定します。
ステップ 4	**trusted-port** 例： `Device(config-nd-raguard)# trusted-port`	信頼できるポートを設定します。
ステップ 5	**device-role** {**host** | **monitor** | **router** | **switch**} 例：	ポートに接続されているデバイスのロールを設定します。

	コマンドまたはアクション	目的
	`Device(config-nd-raguard)# device-role router`	

非 IP ワイヤレス マルチキャストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。

ステップ 3	**wireless multicast non-ip**
	例：
	`Device(config)# wireless multicast non-ip`
	`Device(config)# no wireless multicast non-ip`
		すべての VLAN で非 IP マルチキャストを有効にします。デフォルト値は **enable** です。トラフィックが通過できるように、ワイヤレス マルチキャストを有効にしておく必要があります。すべての VLAN で非 IP マルチキャストを無効にするには、コマンドに **no** を追加します。

ステップ 4	**wireless multicast non-ip** *vlanid*
	例：
	`Device(config)# wireless multicast non-ip 5`
	`Device(config)# no wireless multicast non-ip 5`
		VLAN ごとに非 IP マルチキャストを有効にします。デフォルト値は **enable** です。トラフィックが通過できるように、ワイヤレス マルチキャストおよびワイヤレス マルチキャスト非 IP の両方を有効にする必要があります。VLAN ごとに非IPマルチキャストを無効にするには、コマンドに **no** を追加します。

ステップ 5	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押してコンフィギュレーション モードを終了します。

ワイヤレス ブロードキャストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。

ステップ 3	**wireless broadcast**
	例：
	`Device(config)# wireless broadcast`
	`Device(config)# no wireless broadcast`
		ワイヤレス クライアントへのブロードキャスト パケットを有効にします。デフォルト値は、disable です。**wireless broadcast** を有効にすると、各 VLAN へのブロードキャスト トラフィックが有効になります。ブロードキャスティング パケットをディセーブルにするには、コマンドに「**no**」を追加します。

ステップ 4	**wireless broadcast vlan** *vlanid*
	例：
	`Device(config)# wireless broadcast vlan 3`
	`Device(config)# no wireless broadcast vlan 3`
		単一の VLAN へのブロードキャスト パケットを有効にします。デフォルト値は **enable** です。ワイヤレス ブロードキャストは、ブロードキャスティングに対し有効にする必要があります。各 VLAN へのブロードキャスト トラフィックを無効にするには、コマンドに **no** を追加します。

ステップ 5	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押してコンフィギュレーション モードを終了します。

WLAN の IP マルチキャスト VLAN の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 3	**wlan** *wlan_name* 例： `Device(config)# wlan test 1`	WLAN にさまざまなパラメータを設定するコンフィギュレーション モードを開始します。
ステップ 4	**shutdown** 例： `Device(config-wlan)# shutdown`	WLAN をディセーブルにします。

ステップ 5	**ip multicast vlan** {*vlan_name vlan_id*}
	例：
	`Device(config-wlan)# ip multicast vlan 5`
	`Device(config-wlan)# no ip multicast vlan 5`
		WLAN にマルチキャスト VLAN を設定します。WLAN のマルチキャスト VLAN を無効にするには、コマンドに **no** を追加します。

ステップ 6	**no shutdown** 例： `Device(config-wlan)# no shutdown`	無効になっている WLAN をイネーブルにします。
ステップ 7	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押してコンフィギュレーション モードを終了します。

関連トピック

マルチキャスト最適化について （732 ページ）

ワイヤレス マルチキャストのモニタリング

表 *45 :* ワイヤレス マルチキャストをモニタリングするためのコマンド

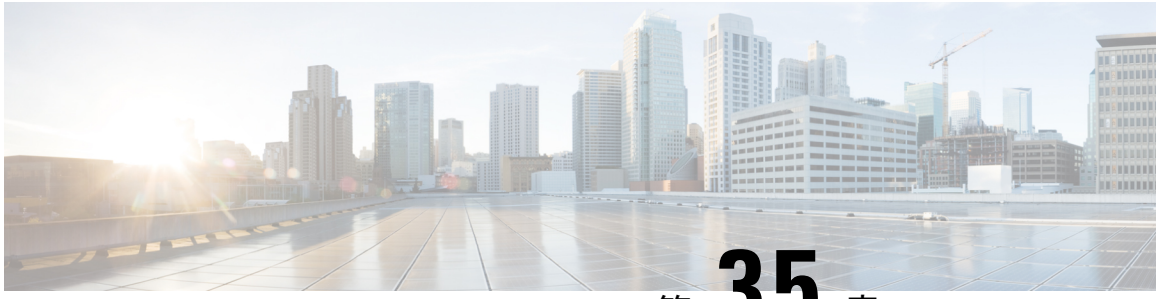
コマンド	説明
show wireless multicast	マルチキャスト ステータスと IP マルチキャスト モード、各 VLAN のブロードキャストおよび非 IP マルチキャスト ステータスを表示します。mDNS ブリッジング状態も表示されます。
show wireless multicast group summary	すべての（送信元、グループおよび VLAN）リストおよび対応する MGID 値を表示します。
show wireless multicast [**source** *source*] **group** *group***vlan** *vlanid*	所定の (S,G,V) の詳細を表示し、それに関連付けられているすべてのクライアントおよび MC2UC ステータスを示します。 .
show ip igmp snooping wireless mcast-spi-count	IOS とワイヤレス コントローラ モジュール間で送信される MGID ごとのマルチキャスト SPI 数の統計を表示します。
show ip igmp snooping wireless mgid	MGID マッピングを表示します。
show ip igmp snooping igmpv2-tracking	クライアントから SGV への間マッピングおよび SGV からクライアントへのマッピングを表示します。
show ip igmp snooping querier vlan *vlanid*	指定された VLAN の IGMP クエリア情報を表示します。
show ip igmp snooping querier detail	すべての VLAN の IGMP クエリアの詳細情報を表示します。
show ipv6 mld snooping querier vlan *vlanid*	指定された VLAN の MLD クエリア情報を表示します。
show ipv6 mld snooping wireless mgid	IPv6 マルチキャスト グループの MGID を表示します。

ワイヤレス マルチキャストの次の作業

次の設定を行えます。

- IGMP
- PIM
- SSM

- IP マルチキャスト ルーティング
- サービス検出ゲートウェイ



第 35 章

SSM の設定

- 機能情報の確認 （745 ページ）
- SSM の設定の前提条件 （745 ページ）
- SSM 設定の制約事項 （746 ページ）
- SSM に関する情報 （747 ページ）
- SSM の設定方法 （752 ページ）
- SSM のモニタリング （760 ページ）
- SSM の次の作業 （761 ページ）
- その他の参考資料 （761 ページ）
- SSM の機能履歴と情報 （763 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

SSM の設定の前提条件

次に、Source-Specific Multicast （SSM）および SSM マッピングを設定するための前提条件を示します。

- SSM マッピングを設定する前に、次の作業を実行する必要があります。
  - IP マルチキャスト ルーティングをイネーブルにします。
  - PIM スパース モードをイネーブルにします。

- SSM を設定します。

- スタティック SSM マッピングを設定する場合は、事前にアクセス コントロール リスト（ACL）を設定して、送信元アドレスにマッピングされるグループ範囲を定義する必要があります。
- SSMマッピングを設定し、DNSルックアップで使用できるようにするには、稼動中のDNSサーバにレコードを追加する必要があります。稼働中の DNS サーバがない場合は、DNS サーバをインストールする必要があります。

（注） 実行中の DNS サーバにレコードを追加するには、*Cisco Network Registrar* などの製品を使用できます。

SSM 設定の制約事項

次に、SSM を設定する際の制約事項を示します。

- IGMPv3 で SSM を使用するには、Cisco IOS ルータ、アプリケーションが稼働しているホスト、そしてアプリケーション自体が SSM をサポートしている必要があります。
- SSMにまだ対応していないネットワーク内の既存のアプリケーションは、（S,G）チャネルの加入登録をサポートするように変更していない限り、SSM範囲内では機能しません。そのため、既存のアプリケーションが指定のSSM範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題が発生することがあります。
- IGMP スヌーピング：IGMPv3 で使用される新しいメンバーシップ レポート メッセージは、旧型の IGMP スヌーピング デバイスでは正しく認識されない場合があります。
- SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。Cisco Group Management Protocol（CGMP）、IGMP スヌーピング、または Router-Port Group Management Protocol（RGMP）でサポートされるのはグループ固有のフィルタリングだけであり、（S, G）チャネル固有のフィルタリングはサポートされていません。同じスイッチドネットワーク内の異なるレシーバーが異なる（S,G）チャネルを要求し、これらのチャネルが同じグループを共有している場合、レシーバーは上記のような既存メカニズムの利点を活用できません。どちらのレシーバーも、すべての（S, G）チャネル トラフィックを受信し、不要なトラフィックを入力から除外します。SSM は、独立した多くのアプリケーションに SSM 範囲のグループ アドレスを再利用できるので、このような状況では、スイッチド ネットワークのトラフィック フィルタリング機能が低下する可能性があります。そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM範囲内の1つのアドレスがさまざまなアプリケーションに再利用される可能性を小さくすることが重要です。たとえば、TV チャネル セットを提供するアプリケーション サービスで、SSM を使用する場合は、各 TV（S, G）チャネルに異なるグループを使用する必要があります。このようにすれば、同じアプリケーション サー

ビス内の異なるチャネルに複数のレシーバが接続されていても、レイヤ2デバイスを含むネットワークでトラフィック エイリアシングが発生しなくなります。

- PIM-SSM では、ラストホップ ルータは、そのインターフェイス上に適切な（S, G）加入登録があると、定期的に（S, G）Join メッセージを送信し続けます。このため、レシーバが（S, G）加入を送信する限り、ソースが長時間（または二度と）トラフィックを送信しなくてもレシーバからソースへの最短パス ツリー（SPT）状態が維持されます。

  送信元がトラフィックを送信し、レシーバーがグループに加入している場合にだけ（S, G）ステートが維持される PIM-SM では、これとは対照的な状況が発生します。PIM-SM では、送信元がトラフィックの送信を 3 分以上停止すると、（S, G）ステートは削除され、その送信元からのパケットが RPT を通じて再度到達した場合のみに再確立されます。PI-SSM では、送信元がアクティブであることをレシーバに通知するメカニズムがないので、レシーバが（S, G）チャネルの受信を要求している限り、（S, G）ステートを維持する必要があります。

次に、SSM マッピングを設定する際の制約事項を示します。

- SSM マッピング機能は、完全な SSM の利点を共有しません。SSM マッピングでは、ホストからグループ G の加入が取得され、1 つまたは複数のソースに関連付けられているアプリケーションでこのグループを指定できるため、グループ G ごとにこのようなアプリケーション 1 つのみをサポートできます。それにもかかわらず、完全な SSM アプリケーションは、SSM マッピングにも使用される同じグループを共有することができます。

- 完全な SSM への移行ソリューションとして SSM マッピングだけを使用する場合は、ラストホップ ルータの IGMPv3 をイネーブルにする際に十分に注意してください。SSM マッピングと IGMPv3 を両方イネーブルにした場合、すでに IGMPv3 をサポートしている（SSM はサポートしていない）ホストは IGMPv3 グループ レポートを送信します。SSM マッピングは、このような IGMPv3 グループ レポートをサポートしていないので、ルータは送信元をこれらのレポートと正しく関連付けることができません。

SSM に関する情報

Source-Specific Multicast（SSM; 送信元特定マルチキャスト）機能は、IP マルチキャストの拡張機能であり、この機能を使用すると、受信者に転送されるデータグラム トラフィックは、その受信者が明示的に加入しているマルチキャスト送信元からのトラフィックだけになります。SSM 用にマルチキャスト グループを設定する場合、SSM 配信ツリー（共有ツリーはない）だけが作成されます。

ここでは、Source-Specific Multicast（SSM）の設定方法を説明します。この項の SSM コマンドの詳細な説明については、『*IP Multicast Command Reference*』を参照してください。この章で言及する他のコマンドについては、コマンド リファレンス マスター インデックス（オンライン検索）を使用して、該当するマニュアルを参照してください。

SSM コンポーネントの概要

SSMは、1対多のアプリケーション（ブロードキャストアプリケーション）に最適なデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャスト ソリューションの中核的なネットワーキングテクノロジーです。デバイス は、SSM の実装をサポートする次のコンポーネントをサポートしています。

- Protocol Independent Multicast Source-Specific Mode（PIM-SSM）

  PIM-SSM は、SSM の実装をサポートするルーティング プロトコルで、PIM Sparse Mode（PIM-SM）に基づいています。

- Internet Group Management Protocol version 3（IGMPv3）

SSM および Internet Standard Multicast（ISM）

インターネットの現行のIPマルチキャストインフラストラクチャや多くの企業のイントラネットは、PIM-SM プロトコルと Multicast Source Discovery Protocol（MSDP）に基づいています。これらのプロトコルには、Internet Standard Multicast（ISM）サービス モデルの限界があります。たとえば、ISM では、ネットワークは、実際にマルチキャスト トラフィックを送信しているホストについての情報を維持する必要があります。

ISM サービスは、任意の送信元からマルチキャスト ホスト グループと呼ばれるレシーバー グループへの IP データグラムの配信でなりたっています。マルチキャスト ホスト グループのデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス（S）と IP 宛先アドレスとしてのマルチキャスト グループ アドレス（G）のデータグラムで構成されます。システムは、ホスト グループのメンバーになることによって、このトラフィックを受信します。ホスト グループのメンバーシップには IGMP バージョン 1、2、または 3 によるホスト グループのシグナリングが必要です。

SSM では、データグラムは（S, G）チャネルに基づいて配信されます。SSM と ISM のどちらでも、ソースになるためにシグナリングは必要ありません。ただし、SSMでは、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために（S, G）への加入または脱退を行う必要があります。つまり、レシーバは加入した（S,G）チャネルからだけトラフィックを受信できます。一方、 ISM では、レシーバは受信するトラフィックの送信元の IP アドレスを知る必要はありません。チャネル加入シグナリングの標準的な方法として、IGMP を使用してモードメンバーシップ レポートを包含することが提案されていますが、この手法をサポートしているのは IGMP version 3 だけです。

SSM IP アドレスの範囲

IP マルチキャスト グループ アドレス範囲の設定済みのサブセットに SSM 配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。Cisco IOS ソフトウェアでは、224.0.0.0 ～ 239.255.255.255 の IP マルチキャスト アドレス範囲の SSM 設定が可能です。SSM

範囲が定義されている場合、既存の IP マルチキャスト受信アプリケーションが SSM 範囲のアドレスの使用を試行しても、トラフィックを受信できません。

SSM の動作

確立されているネットワークは、IP マルチキャスト サービスが PIM SM に基づいているので、SSM サービスをサポートできます。SSM サービスだけが必要な場合は、ドメイン間の PIM-SM に必要な全プロトコル範囲（MSDP、Auto-RP、またはブートストラップ ルータ（BSR））ではなく、SSM を単独でネットワークに配置することもできます。

PIM-SM 用に設定されているネットワークに SSM を配置する場合、SSM をサポートするのはラストホップ ルータだけです。レシーバーに直接接続されていないルータは SSM をサポートする必要はありません。一般的に、ラストホップ以外のルータに必要なのは、SSM 範囲内の PIM-SM だけです。このようなルータは SSM 範囲内での MSDP シグナリング、登録、PIM-SM 共有ツリー操作を抑制するために、ほかのアクセス コントロール設定が必要になる場合もあります。

SSM の範囲を設定し SSM をイネーブルにするには、 **ip pim ssm** グローバル コンフィギュレーション コマンドを使用します。この設定による影響は次のとおりです。

- SSM 範囲内のグループは、IGMPv3 include モード メンバーシップ レポートを通じて、（S, G）チャネルに加入できます。
- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、ルータで生成されるのは PIM（S, G）の join と prune のメッセージだけであり、（S, G）の Rendezvous Point Tree（RPT）や（*, G）の RPT メッセージは生成されません。RPT 動作に関連する着信メッセージは無視されるか拒否されます。着信 PIM 登録メッセージに対しては即座に register-stop メッセージで応答が行われます。ラストホップ ルータ以外のルータでは、PIM-SSM は PIM-SM と下位互換性を保ちます。したがって、ラストホップ ルータ以外のルータは SSM グループに PIM-SM を使用できます（SSM をサポートしていない場合など）。
- SSM 範囲内の Source-Active（SA）メッセージは、受け入れ、生成、転送のいずれも実行されません。

SSM マッピング

典型的なセットトップ ボックス（STB）配置では、各 TV チャネルは独立した 1 つの IP マルチキャスト グループを使用し、その TV チャネルの送信を行うアクティブなサーバは 1 つです。1 つのサーバから複数の TV チャネルへの送信は可能ですが、各チャネルのグループはそれぞれ異なります。このようなネットワーク環境で、ルータが特定のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信した場合、レポートの宛先は、そのマルチキャスト グループに関連付けられている TV チャネルの well-known TV サーバになります。

SSM マッピングが設定されている場合、特定グループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信したルータは、レポートを、このグループに関連付けられている well-known 送信元の 1 つ以上のチャネル メンバーシップに変換します。

ルータは、IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、SSM マッピングを使用して、そのグループ に 1 つ以上の送信元 IP アドレスを決定します。その後、SSM マッピングによって、そのメンバーシップ レポートが IGMPv3 レポートに変換され、IGMPv3 レポートを受信した場合と同様に処理が続行されます。IGMPv1 または IGMPv2 メンバーシップ レポートの受信が続き、そのグループの SSM マッピングが同じである限り、ルータは PIM join を送信し、グループに加入し続けます。

SSM マッピング機能を使用すると、ラストホップ ルータはスタティックに設定されたルータ上のテーブルまたは DNS サーバを通じて、送信元アドレスを決定できます。スタティックに設定されたテーブルまたは DNS マッピングが変更された場合、ルータは加入しているグループに関連付けられている現在の送信元から脱退します。

スタティック SSM マッピング

スタティック SSM マッピングでは、ラストホップ ルータは、グループへの送信を行う送信元を決定するために、継続的にスタティック マップを使用します。スタティック SSM マッピングを使用するには、グループ範囲を定義した ACL を設定する必要があります。グループ範囲を定義する ACL を設定した後、**ip igmp ssm-map static** グローバル コンフィギュレーション コマンドを使用して、ACL で許可されたグループを送信元にマッピングできます。

DNS が必要とされないか、またはローカルで DNS マッピングが変更される場合、小規模なネットワークではスタティック SSM マッピングを設定できます。設定されたスタティック SSM マッピングは、DNS マッピングよりも優先されます。

関連トピック

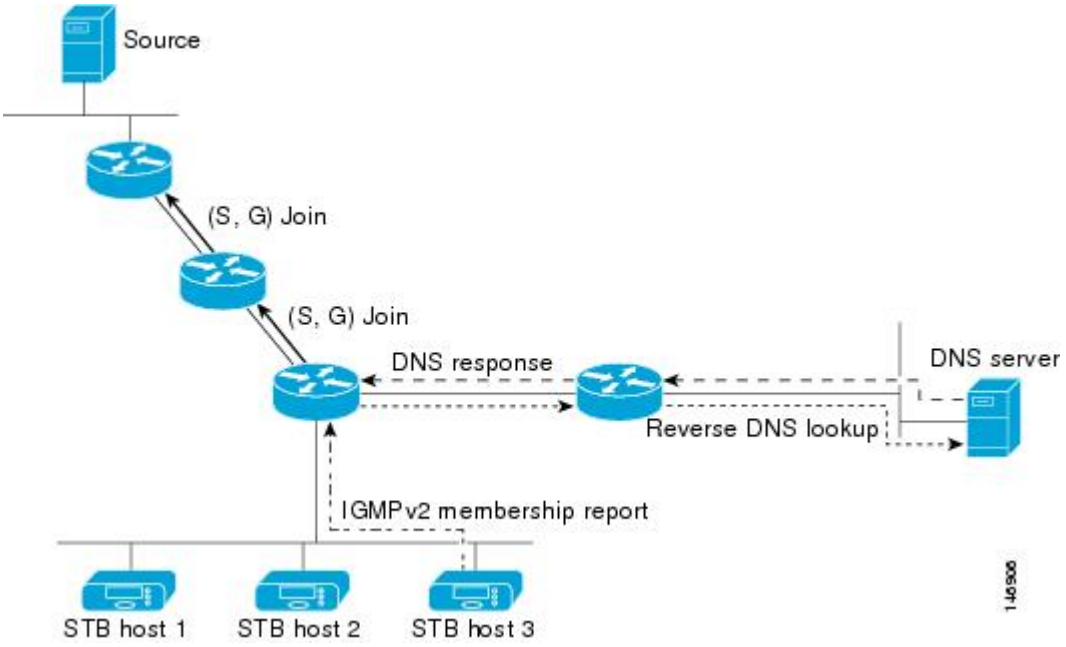
スタティック SSM マッピングの設定（CLI） （754 ページ）
SSM マッピングを使用したスタティック トラフィック転送の設定（CLI） （758 ページ）

DNS ベースの SSM マッピング

DNS ベースの SSM マッピングを使用して、ラストホップ ルータが継続的に逆 DNS ルックアップを実行し、グループに送信する送信元を決定するようにすることも可能です。DNS ベースの SSM マッピングが設定されると、ルータはグループ名を含むドメイン名を構築し、DNS への逆ルックアップを実行します。ルータは IP アドレス リソースを検索し、それらをグループに関連付けられた送信元アドレスとして使用します。SSM マッピングでサポートできる送信元の数は、グループごとに最大 20 です。ルータは各グループに設定されているすべてのソースに加入します。

図 *34 : DNS* ベースの *SSM* マッピング

次の図は、DNS ベースの SSM マッピングを示します。



ラスト ホップ ルータが 1 つのグループの複数の送信元に加入できるようにする SSM マッピング メカニズムによって、TV ブロードキャストの送信元に冗長性を持たせることができます。この場合、ラストホップ ルータは、SSM マッピングを使用し、同じ TV チャネルに対して 2 つのビデオ送信元に同時に加入することにより冗長性を提供します。ただし、ラストホップ ルータでのビデオ トラフィックの重複を防ぐため、ビデオ送信元がサーバ側でスイッチオーバー メカニズムを使用する必要があります。一方のビデオ送信元はアクティブ、もう一方のバックアップ ビデオ送信元はパッシブになります。パッシブの送信元は待機状態になり、アクティブな送信元の障害が検出された場合に、その TV チャネルにビデオ トラフィックを送信します。サーバ側のスイッチオーバー メカニズムによって、実際にその TV チャネルにビデオ トラフィックを送信するサーバは 1 つだけになります。

G1、G2、G3、G4 を含むグループの 1 つ以上の送信元アドレスを検索するには、DNS サーバに次のような DNS レコードを設定する必要があります。

```
G4.G3.G2.G1 [multicast-domain] [timeout] IN A source-address-1
 IN A source-address-2
 IN A source-address-n
```

DNS リソース レコードの設定の詳細については、DNS サーバのマニュアルを参照してください。

関連トピック

DNS ベースの SSM マッピングの設定（CLI） （756 ページ）

SSM の設定方法

この項の Source-Specific Multicast（SSM; 送信元特定マルチキャスト）コマンドの詳細な説明については、『*IP Multicast Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』を参照してください。この章で言及する他のコマンドについては、コマンド リファレンス マスター インデックス（オンライン検索）を使用して、該当するマニュアルを参照してください。

SSM の設定（CLI）

SSM を設定するには、次の手順を実行します。

この手順は任意です。

始める前に

Source Specific Multicast（SSM）範囲の定義にアクセス リストを使用する場合、**ip pim ssm** コマンドでアクセス リストを参照する前にアクセス リストを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim ssm** [**default** | **range** *access-list*] 例： `Device(config)# ip pim ssm range 20`	IP マルチキャスト アドレスの SSM 範囲を定義します。
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet`	IGMPv3 をイネーブルに設定可能なホストに接続されているインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	1/0/1	次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 5	**ip pim** {**sparse-mode** | **sparse-dense-mode**} 例： `Device(config-if)# ip pim sparse-dense-mode`	インターフェイスに対して PIM をイネーブルにします。スパース モードまたはスパース — デンス モードのどちらかを使用する必要があります。
ステップ 6	**ip igmp version 3** 例： `Device(config-if)# ip igmp version 3`	このインターフェイス上で IGMPv3 をイネーブルにします。デフォルトでは、IGMP のバージョン 2 が設定されます。
ステップ 7	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Source-Specific Multicast（SSM）マッピングの設定

Source Specific Multicast（SSM）マッピング機能は、管理上または技術上の理由からエンド システムで SSM をサポートできないかまたはサポートが望ましくない場合に SSM 移行手段として使用できます。SSM マッピングを使用すると、IGMPv3 をサポートしないレガシー STB へのビデオ配信や、IGMPv3 ホスト スタックを使用しないアプリケーションに SSM を活用できます。

スタティック SSM マッピングの設定（CLI）

スタティック SSM マッピングを設定するには、次の手順を実行します。

SSM マッピングの詳細については、『IP Multicast CG Library, Cisco IOS XE Release 3SE（Catalyst 3850 Switches）』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipigmpssm-mapenable** 例： `Device(config)# ip igmp ssm-map enable`	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。 （注） このコマンドでは、デフォルトで、DNS ベースの SSM マッピングがイネーブルにされます。
ステップ 4	**noipigmpssm-mapquerydns** 例： `Device(config)# no ip igmp ssm-map query dns`	（任意）DNS ベースの SSM マッピングをディセーブルにします。 （注） スタティック SSM マッピングだけを使用する場合は、DNS ベースの SSM マッピングをディセーブルにします。デフォルトでは、**ip igmp ssm-map** コマンドは DNS ベースの SSM マッピングをイネーブルにします。
ステップ 5	**ipigmpssm-mapstatic** *access-list source-address* 例： `Device(config)# ip igmp ssm-map static 11 172.16.8.11`	スタティック SSM マッピングを設定します。 • *access-list* 引数に入力した ACL によって、*source-address* 引数に入力したソース IP アドレスにマッピングされるグループが決まります。 （注） 追加のスタティック SSM マッピングを設定することもできます。SSM マッピングを追加設定した場合、ルータが SSM 範囲のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、デバイスは、設定されている各 **ipigmpssm-mapstatic** コマンドに基づいて、そのグループに関連付けられている送信元アドレスを決定します。デバイスは各グループに最大 20 の送信元を関連付けます。

	コマンドまたはアクション	目的
		必要な場合は、ステップを繰り返して、追加のスタティック SSM マッピングを設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

スタティック SSM マッピング （750 ページ）

DNS ベースの SSM マッピングの設定（CLI）

DNS ベースの SSM マッピングを設定するには、DNS サーバ ゾーンを作成するか、または既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用するルータが他の目的にも DNS を使用している場合は、通常の設定の DNS サーバを使用する必要があります。そのルータで使用されている DNS 実装が DNS ベースの SSM マッピングだけの場合は、ルート ゾーンが空であるか、またはそれ自身を指すようなフォールス DNS セットアップが可能です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipigmpssm-mapenable** 例： `Device(config)# ip igmp ssm-map enable`	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。
ステップ 4	**ipigmpssm-mapquerydns** 例： `Device(config)# ip igmp ssm-map query dns`	（任意）DNS ベースの SSM マッピングをイネーブルにします。 • デフォルトでは、**ip igmp ssm-map** コマンドは DNS ベースの SSM マッピングをイネーブルにします。実行コンフィギュレーションに保存されるのは、このコマンドを **no** 形式で使用した場合だけです。 （注） DNS ベースの SSM マッピングがディセーブルの場合、このコマンドを使用して DNS ベースの SSM マッピングを再度イネーブルにします。
ステップ 5	**ipdomainmulticast** *domain-prefix* 例： `Device(config)# ip domain multicast ssm-map.cisco.com`	（任意）DNS ベースの SSM マッピングに使用するドメインプレフィックスを変更します。 • デフォルトでは、ip-addr.arpa ドメインプレフィックスが使用されます。
ステップ 6	**ipname-server** *server-address1* [*server-address2...server-address6*] 例： `Device(config)# ip name-server 10.48.81.21`	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。
ステップ 7	冗長性のために追加の DNS サーバを設定する場合は、必要に応じて、ステップ 6 を繰り返します。	

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

DNS ベースの SSM マッピング （750 ページ）

SSM マッピングを使用したスタティック トラフィック転送の設定（CLI）

ラスト ホップ ルータ上の SSM マッピングでスタティック トラフィック転送を設定する場合は、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface`	SSM マッピングを使用してマルチキャスト グループにスタティックにトラフィックを転送するインターフェイスを

	コマンドまたはアクション	目的
	gigabitethernet 1/0/1	選択し、インターフェイスコンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。 （注） SSM マッピングを使用したトラフィックのスタティック転送は、DNS ベースの SSM マッピングとスタティックに設定された SSM マッピングのいずれかで機能します。
ステップ 4	**ip igmp static-group** *group-address* **source ssm-map** 例： `Device(config-if)# ip igmp static-group 239.1.2.1 source`	そのインターフェイスから（S, G）チャネルへのスタティック転送用の SSM マッピングを設定します。 このコマンドは、特定グループに SSM トラフィックをスタティックに転送する

	コマンドまたはアクション	目的
	ssm-map	場合に使用します。チャネルの送信元アドレスを決定するには DNS ベースの SSM マッピングを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

スタティック SSM マッピング （750 ページ）

SSM のモニタリング

SSM をモニタするには、次の表の特権 EXEC コマンドを使用します。

表 *46 : SSM* のモニタリング コマンド

コマンド	目的
show ip igmp groups detail	IGMPv3 による (S, G) チャネル加入登録を表示します。
show ip mroute	マルチキャスト グループが SSM サービスをサポートしているかどうか、または送信元固有のホスト レポートが受信されたかどうかを表示します。

SSM マッピングのモニタリング

SSM マッピングをモニタするには、次の表の特権 EXEC コマンドを使用します。

表 *47 : SSM* マッピングをモニタするコマンド

コマンド	目的
Device# **show ip igmp ssm-mapping**	SSMマッピングについての情報を表示します。
Device#**show ip igmp ssm-mapping** *group-address*	SSM マッピングが特定のグループに使用する送信元を表示します。
Device#**show ip igmp groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]	ルータに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。
Device#**show host**	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。
Device#**debug ip igmp** *group-address*	送受信された IGMP パケットと IGMP ホスト関連イベントを表示します。

SSM の次の作業

次の設定を行えます。

- IGMP
- ワイヤレス マルチキャスト
- PIM
- IP マルチキャスト ルーティング
- サービス検出ゲートウェイ

その他の参考資料

関連資料

関連項目	マニュアル タイトル
SSM、およびその他の使用可能なコマンド	『*IP Multicast Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』

関連項目	マニュアル タイトル
プラットフォームに依存しない設定情報	• 『*IP Multicast: PIM Configuration Guide, Cisco IOS XE Release 3SE（Catalyst 3850 Switches）*』 • 『*IP Multicast: IGMP Configuration Guide, Cisco IOS XE Release 3SE（Catalyst 3850 Switches）*』 • *I*『*P Multicast: Multicast Optimization Configuration Guide, Cisco IOS XE Release 3SE（Catalyst 3850 Switches）*』

標準および RFC

標準/RFC	Title
RFC 4601	『*Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*』

MIB

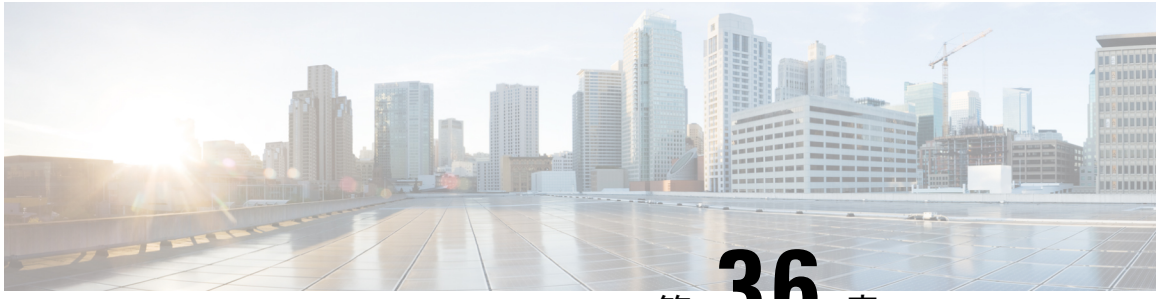
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

SSM の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。



第 36 章

GRE トンネルを介するマルチキャスト ルーティングの設定

- 機能情報の確認 （765 ページ）
- GRE トンネルを介するマルチキャスト ルーティングの設定の前提条件 （765 ページ）
- GRE トンネルを介するマルチキャスト ルーティングの設定の制約事項 （766 ページ）
- GRE トンネルを介するマルチキャスト ルーティングについて （766 ページ）
- GRE トンネルを介するマルチキャスト ルーティングの設定方法 （767 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GRE トンネルを介するマルチキャスト ルーティングの設定の前提条件

GRE を介するマルチキャスト ルーティングを設定する前に、IP マルチキャスト ルーティング テクノロジーと GRE トンネリングの概念についてよく理解しておく必要があります。

GRE トンネルを介するマルチキャスト ルーティングの設定の制約事項

次に、GRE トンネルを介するマルチキャスト ルーティングの設定の制約事項を示します。

- GRE トンネルを介する IPv6 マルチキャストはサポートされません。
- サポートされるマルチキャスト ルート（mroute）の総数は、すべてのトンネル全体で 2000 です。
- 双方向 PIM はサポートされていません。
- GRE トンネルを介するマルチキャストをサポートするには、マルチキャスト ルーティングを最初のホップ ルータ（FHR）、ランデブー ポイント（RP）および最後のホップ ルータ（LHR）で設定する必要があります。
- Catalyst 3850 および Catalyst 3650 シリーズ スイッチでは、トンネル送信元をループバック インターフェイス、物理インターフェイス、または L3 EtherChannel インターフェイスにできます。
- IPSec、ACL、トンネル カウンタ、暗号化サポート、フラグメンテーション、Cisco Discovery Protocol（CDP）、QoS、GRE キープアライブ、マルチポイント GRE などの機能の相互作用は、GRE トンネルでサポートされていません。

GRE トンネルを介するマルチキャスト ルーティングについて

この章では、非 IP マルチキャスト エリア間で IP マルチキャスト パケットをトンネリングするために、Generic Route Encapsulation（GRE）トンネルを設定する方法について説明します。その利点は、IP マルチキャストをサポートしないエリアを経由して、IP マルチキャスト トラフィックをソースからマルチキャスト グループに送信できることです。GRE トンネルを介するマルチキャスト ルーティングは、ip PIM デンス モード、スパース - デンス モード、スパース モード、および pim-ssm モードをサポートしています。また、スタティック RP および Auto-RP もサポートしています。スタティック RP と Auto-RP の設定の詳細については、ランデブー ポイントと Auto-RP を参照してください。

（注） Cisco IOS XE Denali 16.3.1 以降では、マルチキャスト ルーティングおよび NHRP が GRE トンネリングでサポートされています。トンネル エンド ポイントのダイナミック検出を促進するために、トンネル インターフェイス上のマルチキャスト設定とともに、NHRP をオプションで設定できます。トンネル インターフェイスに NHRP を設定する方法については、NHRP を参照してください。

非 IP マルチキャスト エリアを接続するトンネリングの利点

- 送信元とグループ メンバー（宛先）間のパスが IP マルチキャストをサポートしていない場合、それらの間のトンネルは IP マルチキャスト パケットを転送できます。

GRE トンネルを介するマルチキャスト ルーティングの設定方法

非 IP マルチキャスト エリアを接続する GRE トンネルの設定

マルチキャストルーティングをサポートしていないメディアで接続されている送信元と宛先の間の IP マルチキャスト パケットを転送するように GRE トンネルを設定できます。

手順

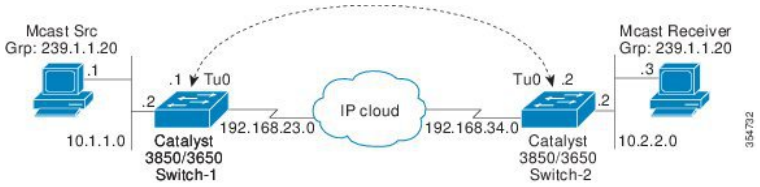
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**interfacetunnel** *number* 例： `Device(config)# interface tunnel 0`	トンネル インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address ip_address** *subnet_mask* 例： `Device(config-if)# ip address 192.168.24.1 255.255.255.252`	IP アドレスおよび IP サブネットを設定します。

	コマンドまたはアクション	目的
ステップ 6	**ippim** { **sparse-dense-mode** | **sparse-mode** | **dense-mode** } 例： `Device(config-if)# ip pim sparse-dense-mode`	次の動作モードのいずれかでトンネルインターフェイス上で Protocol Independent Multicast（PIM）を有効にします。 • **sparse-dense-mode** ：マルチキャスト グループの動作モードに応じて、インターフェイスをスパース動作モードまたはデンス動作モードで処理します。 • **sparse-mode** ：スパース動作モードをイネーブルにします。 • **dense-mode** ：デンス動作モードをイネーブルにします。
ステップ 7	**tunnelsource** { *ip-address* | *interface-name* } 例： `Device(config-if)# tunnel source 100.1.1.1`	トンネル送信元を設定します。
ステップ 8	**tunneldestination** { *hostname* | *ip-address* } 例： `Device(config-if)# tunnel destination 100.1.5.3`	トンネル宛先を設定します。
ステップ 9	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。
ステップ 10	**show interface** *type number* 例： `Device# show interface tunnel 0`	トンネルインターフェイスの情報を表示します。

非 IP マルチキャスト エリアを接続するトンネリングの例

次の例に、GRE トンネルを介した Catalyst 3650/3850 スイッチ間のマルチキャスト ルーティングを示します。

図 *35*：非 *IP* マルチキャスト エリアを接続するトンネル



上の図では、マルチキャスト送信元（10.1.1.1）は、Catalyst 3850/3650 スイッチ 1 に接続され、マルチキャスト グループ 239.1.1.20 に設定されています。マルチキャスト受信者（10.2.2.3）は、Catalyst 3850/3650 スイッチ 2 に接続され、グループ 239.1.1.20 のマルチキャスト パケットを受信するように設定されています。スイッチ 1 とスイッチ 2 は、マルチキャスト ルーティング用に設定されていない IP クラウドで分離されています。

GRE トンネルは、ループバック インターフェイスで送信元が特定されたスイッチ 1 とスイッチ 2 の間に設定されています。マルチキャスト ルーティングは、スイッチ 1 とスイッチ 2 で有効になっています。スパース モードまたはデンス モードで PIM をサポートするために、**ip pim sparse-dense-mode** コマンドがトンネル インターフェイスに設定されています。トンネル インターフェイスの sparse-dense-mode 設定により、スパース モード パケットまたはデンス モード パケットをグループのランデブー ポイント（RP）設定に応じて、トンネルを経由して転送できます。

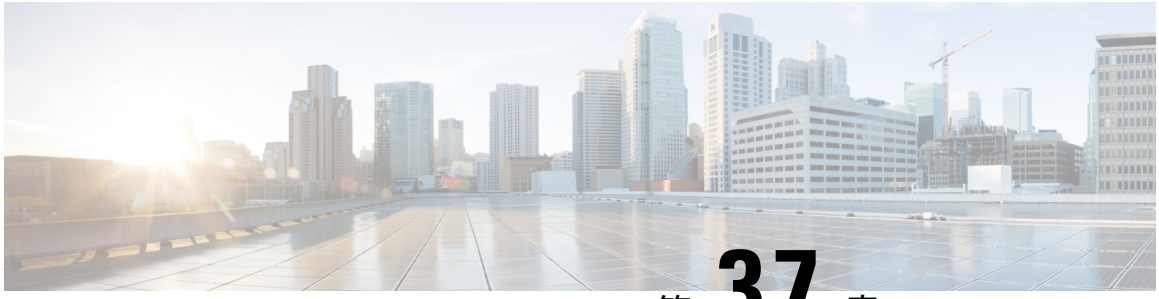
スイッチ 1 の設定：

```
Device(config)# ip multicast-routing
Device(config)# interface Loopback0   //Tunnel source interface
Device(config-if)# ip address 2.2.2.2 255.255.255.255

Device(config)# interface Tunnel 10    //Tunnel interface configured for PIM
traffic
Device(config-if)# ip address 192.168.24.1 255.255.255.252
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# ip nhrp map 192.168.24.3  4.4.4.4  //NHRP may optionally be
configured to dynamically discover tunnel end points.
Device(config-if)# ip nhrp map multicast 4.4.4.4
Device(config-if)# ip nhrp network-id 1
Device(config-if)# ip nhrp nhs 192.168.24.3
Device(config-if)# tunnel source Loopback0
Device(config-if)# tunnel destination 4.4.4.4

Device(config)# interface GigabitEthernet 0/0/0      //Source interface
Device(config-if)# ip address 10.1.1.2 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
```

スイッチ 2 の設定：

```
Device(config)# ip multicast-routing
Device(config)# interface Loopback0    //Tunnel source interface
Device(config-if)# ip address 4.4.4.4 255.255.255.255

Device(config)# interface Tunnel 10     //Tunnel interface configured for PIM
```

```
 traffic
Device(config-if)# ip address 192.168.24.2 255.255.255.252
Device(config-if)# ip nhrp map 192.168.24.4 2.2.2.2  //NHRP may optionally be
configured to dynamically discover tunnel end points.
Device(config-if)# ip nhrp map multicast 2.2.2.2
Device(config-if)# ip nhrp network-id 1
Device(config-if)# ip nhrp nhs 192.168.24.4
Device(config-if)# ip pim sparse-dense mode
Device(config-if)# tunnel source Loopback0
Device(config-if)# tunnel destination 2.2.2.2

Device(config)# interface GigabitEthernet 0/0/0      //Receiver interface
Device(config-if)# ip address 10.2.2.2 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
```



第 37 章

サービス検出ゲートウェイの設定

- 機能情報の確認 （771 ページ）
- サービス検出ゲートウェイの設定に関する制約事項 （771 ページ）
- サービス検出ゲートウェイおよび mDNS に関する情報 （772 ページ）
- サービス検出ゲートウェイの設定方法 （776 ページ）
- サービス検出ゲートウェイのモニタリング （782 ページ）
- 設定例 （783 ページ）
- サービス検出ゲートウェイの設定の次の作業 （785 ページ）
- その他の参考資料 （786 ページ）
- サービス検出ゲートウェイの機能履歴と情報 （787 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

サービス検出ゲートウェイの設定に関する制約事項

サービス検出ゲートウェイの設定に関する制約事項は次のとおりです。

- サービス検出ゲートウェイは、複数のホップによるトポロジをサポートしていません。すべてのネットワーク セグメントを直接接続する必要があります。サービス検出ゲートウェイは、接続されているすべてのセグメントからサービスを学習して、キャッシュを構築し、プロキシとして動作する要求に応答できます。

- サードパーティ mDNS サーバまたはアプリケーションの使用は、この機能ではサポートされていません。
- mDNS を実行している Cat4500sup8e MC (3.7) では、iOS7.0 を実行している iPhone と ipad で、mDNS を介してプリントサービスにアクセスすると問題が発生する場合があります。

サービス検出ゲートウェイおよび mDNS に関する情報

mDNS

mDNS は設定不要を実現するために定義され、設定不要は次の機能を提供するものとして定義されています。

- アドレッシング：ホストへの IP アドレスの割り当て
- ネーミング：IP アドレスの代わりに名前を使用したホストの参照
- サービス検出：ネットワークでの自動的なサービスの検索

mDNS を使用すると、ネットワーク ユーザは、ネットワーク上のサービスにアクセスするために IP アドレスを割り当てたり、ホスト名を割り当てたり、名前を入力する必要がなくなります。ユーザが行うことは、利用可能なネットワーク サービスの表示を要求し、リストから選択することだけです。

mDNS では、DHCP/DHCPv6 または IPv4 および IPv6 リンク ローカル スコープ アドレスの使用を通じてアドレッシングが実行されます。設定不要の利点が生じるのは、DHCP や DNS のようなインフラストラクチャ サービスが存在せず、自分で割り当てたリンクローカルアドレッシングを使用できる場合です。その結果、クライアントは、リンクローカル範囲（169.254.0.0/24）内でランダムな IPv4 アドレスを選択するか、またはその IPv6 リンクローカル アドレス（FE80::/10）を使用して通信を行うことができます。

mDNS では、ネーミング（mDNS を使用したローカル ネットワークでの名前/アドレス変換）クエリはリンクローカル スコープ IP マルチキャストを使用してローカル ネットワークを介して送信されます。これらの DNS クエリはマルチキャスト アドレス（IPv4 アドレス 224.0.0.251 または IPv6 アドレス FF02::FB）に送信されるため、クエリへの応答にグローバルな知識を持つ単一の DNS サーバは必要ありません。サービスまたはデバイスは、認識しているサービスに関するクエリを確認すると、キャッシュからの情報が含まれた DNS 応答を提供します。

mDNS では、サービス検出はブラウジングによって実行されます。mDNS クエリは、特定のサービス タイプとドメインに応じて送信され、一致するサービスを認識しているデバイスがサービス情報を返します。その結果は利用可能なサービスのリストからなり、ユーザはそのリストから選択できます。

mDNS プロトコル（mDNS-RFC）を DNS サービス検出（DNS-SD-RFC）とともに使用すると、アドレッシング、ネーミング、およびサービス検出の設定が不要になります。

mDNS-SD

マルチキャスト DNS サービス検出（mDNS-SD）は、DNS プロトコル セマンティックおよびウェルノウン マルチキャスト アドレス経由のマルチキャストを使用して、設定不要のサービス検出を実現します。DNS パケットは、マルチキャスト アドレス 224.0.0.251 とその IPv6 相当の FF02::FB を使用してポート 5353 上で送受信されます。

mDNS はリンクローカル マルチキャスト アドレスを使用するため、その範囲は 1 つの物理 LAN または論理的 LAN に制限されます。ネットワーキングの範囲を分散したキャンパス、またはさまざまな多数のネットワークテクノロジーで構成される広域環境に拡張する必要がある場合は、mDNS ゲートウェイが実装されます。mDNS ゲートウェイでは、1 つのレイヤ 3 ドメインから別のドメインへのサービスのフィルタリング、キャッシング、および再配布を行うことで、レイヤ 3 境界間での mDNS パケットの転送を行うことができます。

ワイヤレス クライアントの mDNS-SD の検討事項

- mDNS パケットは、IP アドレスがない可能性があるレイヤ 3 インターフェイスから送信できます。
- multicast-multicast モードが有効になっている場合、mDNS マルチキャスト IP およびマルチキャスト MAC を持つパケットは、マルチキャスト CAPWAP トンネルで送信されます。マルチキャスト CAPWAP トンネルは、各 AP CAPWAP トンネル用に生成される必要があるマルチキャスト パケットのコピー数を減らすために使用される特別な CAPWAP トンネルです。マルチキャスト CAPWAP トンネル上でパケットを送信するには、外部の IP ヘッダーをすべての AP が登録しているマルチキャスト CAPWAP トンネルのアドレス宛てにする必要があります。
- すべての mDNS パケット処理は、ローミングされたクライアント用の外部スイッチで実行されます。外部スイッチは、ローミングされたワイヤレスクライアントが実際に接続されている新しいスイッチであり、接続ポイントと呼ばれます。

サービス検出ゲートウェイ

サービス検出ゲートウェイ機能により、マルチキャスト ドメイン ネーム システム（mDNS）は、レイヤ 3の境界を越えて（異なるサブネットで）動作します。mDNS ゲートウェイでは、1 つのレイヤ 3 ドメイン（サブネット）から別のドメインへのサービスのフィルタリング、キャッシング、および再配布を行うことで、レイヤ 3 境界間でのサービス検出の転送を行うことができます。この機能が実装される前は、リンクローカル スコープのマルチキャスト アドレスを使用していたため、mDNS は 1 サブネット内に範囲が制限されていました。この機能により、Bring Your Own Device（BYOD）が強化されます。

関連トピック

サービス リストの設定（CLI） （776 ページ）
例：サービス リストの作成、フィルタの適用およびパラメータの設定 （784 ページ）
mDNS ゲートウェイの有効化とサービスの再配布（CLI） （779 ページ）
例：発信 mDNS パケットに対する代替送信元インターフェイスの指定 （783 ページ）
例：サービス アナウンスメントの再配布 （783 ページ）

例：ワイヤレス クライアントに対する mDNS パケットのブリッジングの無効化 （783 ページ）
例：mDNS ゲートウェイの有効化とサービスの再配布 （784 ページ）
例：グローバル mDNS 設定 （784 ページ）
例：インターフェイス mDNS 設定 （785 ページ）

mDNS ゲートウェイとサブネット

サービス検出をサブネット間で動作させるには、mDNS ゲートウェイを有効にする必要があります。mDNS ゲートウェイは、デバイスまたはインターフェイスに対してイネーブルにできます。

（注） インターフェイス レベルで設定する前に、グローバルにサービスを設定する必要があります。

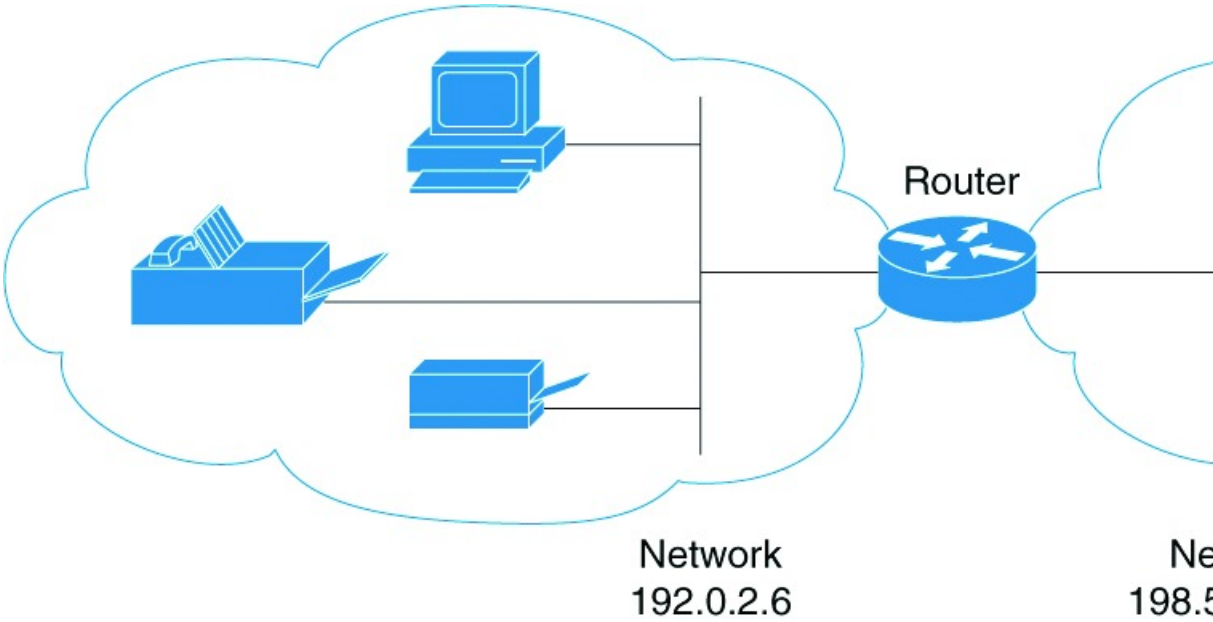
デバイスまたはインターフェイスを有効にした後、サブネット間にサービス検出情報を再配布できます。サービス ポリシーを作成し、着信サービス検出情報（インバウンド（IN）フィルタリングと呼ぶ）または発信サービス検出情報（アウトバウンド（OUT）フィルタリングと呼ぶ）に対してフィルタを適用できます。

（注） 再配布がグローバルに有効になっている場合は、グローバル コンフィギュレーションがインターフェイス コンフィギュレーションよりも優先順位が高くなります。

図 *36*：サンプルのネットワーク シナリオ

たとえば、mDNS ゲートウェイ機能がこの図のルータで有効になっている場合は、サービス情報を 1 つのサブネットから別のサブネットに送信することができ、その逆も同様です。たとえば、IP アドレス 192.0.2.6 のネットワークでアドバタイズされているプリンタとファクスのサービス情報は、IP アドレス 198.51.100.4 のネットワークに再配布されます。IP アドレス 192.0.2.6 のネットワーク内のプリンタとファクスのサービス情報は、他のネットワーク内の mDNS 対

応ホストとデバイスによって学習されます。



フィルタリング

mDNS ゲートウェイとサブネットを設定した後、再配布するサービスをフィルタリングできます。サービス リストを作成するときは、**permit** または **deny** コマンド オプションが使用されます。

- **permit** コマンド オプションを使用すると、特定のサービス リスト情報を許可したり転送したりできます。
- **deny** オプションを使用すると、他のサブネットに転送可能なサービス リスト情報を拒否することができます。

permit または **deny** コマンド オプションを使用する場合は、シーケンス番号を含める必要があります。同じサービス リスト名を複数のシーケンス番号に関連付けることができ、各シーケンス番号はルールにマッピングされます。

（注） フィルタが設定されていない場合、デフォルトのアクションは、デバイスまたはインターフェイスを通して転送されるサービス リスト情報を拒否することです。

クエリは、サービス リストを作成する際に提供される別のオプションです。サービス リストを使用してクエリを作成できます。サービスについて参照する場合は、アクティブなクエリを使用できます。この機能は、キャッシュ内で更新されたレコードを保持するのに役立ちます。

（注） アクティブなクエリはグローバルでのみ使用でき、インターフェイス レベルでは使用できません。

サービスが起動すると、サービスエンドポイント（プリンタ、ファックスなど）は非請求アナウンスメントを送信します。その後、ネットワーク変更イベント（インターフェイスの表示や消去など）が発生するたびに、非請求アナウンスメントを送信します。デバイスは必ずクエリに応答します。

サービス リストを作成し、**permit** または **deny** コマンド オプションを使用した後、*service-instance*、*service-type* または *message-type* に基づいて、match ステートメント（コマンド）を使用してフィルタリングできます（アナウンスメントまたはクエリ）。

関連トピック

サービス リストの設定（CLI） （776 ページ）
例：サービス リストの作成、フィルタの適用およびパラメータの設定 （784 ページ）
mDNS ゲートウェイの有効化とサービスの再配布（CLI） （779 ページ）
例：発信 mDNS パケットに対する代替送信元インターフェイスの指定 （783 ページ）
例：サービス アナウンスメントの再配布 （783 ページ）
例：ワイヤレス クライアントに対する mDNS パケットのブリッジングの無効化 （783 ページ）
例：mDNS ゲートウェイの有効化とサービスの再配布 （784 ページ）
例：グローバル mDNS 設定 （784 ページ）
例：インターフェイス mDNS 設定 （785 ページ）

サービス検出ゲートウェイの設定方法

サービス リストの設定（CLI）

次の手順では、サービス リストを作成し、サービス リストにフィルタを適用して、サービス リスト名のパラメータを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**service-list mdns-sd** *service-list-name* {**deny** *sequence-number* | **permit** *sequence-number* | **query**}
	例：
	`Device(config)# service-list mdns-sd sl1 permit 3`
	`Device(config)# service-list mdns-sd sl4 query`
		mDNS サービス検出サービス リスト モードを開始します。このモードでは、次の操作を実行できます。
		• サービス リストを作成し、シーケンス番号に適用された **permit** または **deny** オプションに従って、サービス リストにフィルタを適用します。
		• **query** オプションを使用している場合は、サービス リストを作成し、サービス リスト名のクエリを関連付けます。
		（注） シーケンス番号は、ルールの優先順位を設定するものです。低いシーケンス番号を持つルールが最初に選択され、サービス アナウンスメントまたはクエリがそれに応じて許可または拒否されます。ネットワーク要件によってシーケンス番号を定義します。

ステップ 4	**match message-type** {**announcement** | **any** | **query**} 例： `Device(config-mdns-sd-sl)# match message-type announcement`	（任意）照合するメッセージ タイプを設定します。次のメッセージ タイプを照合できます。 • announcement • any • query これらのコマンドでは、ステップ 2 で作成されたサービス リスト名に対するパラメータが設定されます。 **match message-type** がアナウンスメントの場合、サービス リストのルールで

	コマンドまたはアクション	目的
		は、デバイスに対するサービス アドバタイズメントまたはアナウンスメントのみが許可されます。**match message-type** がクエリの場合は、ネットワーク内の特定のサービスに対するクライアントからのクエリのみが許可されます。 異なるシーケンス番号を持つ同じ名前の複数のサービス マップを作成することができ、フィルタの評価順序はシーケンス番号に基づきます。サービス リストは、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。サービス リストの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクション permit または deny が実行されると停止します。リスト全体をスキャンした後のデフォルトのアクションは deny です。 （注） 前のステップで **query** オプションを使用していた場合は、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションでのみ使用できます。
ステップ 5	**match service-instance** { *LINE* } 例： `Device(config-mdns-sd-sl)## match service-instance servInst 1`	（任意）照合するサービス インスタンスを設定します。 このコマンドでは、ステップ 2 で作成されたサービス リスト名に対するパラメータが設定されます。 （注） 前のステップで **query** オプションを使用していた場合は、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションでのみ使用できます。

	コマンドまたはアクション	目的
ステップ 6	**match service-type** {*LINE* } 例： `Device(config-mdns-sd-sl)# match service-type _ipp._tcp`	（任意）照合する mDNS サービス タイプ文字列の値を設定します。 このコマンドでは、ステップ 2 で作成されたサービス リスト名に対するパラメータが設定されます。 （注） 前のステップで **query** オプションを使用していた場合は、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションでのみ使用できます。
ステップ 7	**end** 例： `Device(config-mdns-sd-sl)# end`	特権 EXEC モードに戻ります。

次のタスク

mDNS ゲートウェイを有効にして、サービスの再配布に進みます。

関連トピック

サービス検出ゲートウェイ （773 ページ）
フィルタリング （775 ページ）
例：サービス リストの作成、フィルタの適用およびパラメータの設定 （784 ページ）

mDNS ゲートウェイの有効化とサービスの再配布（CLI）

デバイスに対して mDNS ゲートウェイをイネーブルにしたら、フィルタ（インバウンド（IN）フィルタリングまたはアウトバウンド（OUT）フィルタリングを適用）およびアクティブなクエリを、それぞれ **service-policy** コマンドと **service-policy-query** コマンドを使用して適用できます。**redistribute mdns-sd** コマンドを使用して、サービスおよびサービス アナウンスメントを再配布でき、**cache-memory-max** コマンドを使用して、システム メモリの一部をキャッシュ用に設定できます。

（注） デフォルトでは、mDNS ゲートウェイはすべてのインターフェイスでディセーブルです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service-routing mdns-sd** 例： `Device (config)# service-routing mdns-sd`	デバイスに対して mDNS ゲートウェイ機能をイネーブルにし、マルチキャスト DNS コンフィギュレーション（config-mdns）モードを開始します。 （注） このコマンドは、mDNS 機能をグローバルに有効にします。 （注） 発信インターフェイスに何も設定されていない場合にその IP アドレスを使用できるように、発信 mDNS パケットに代替送信元インターフェイスを指定するには、グローバルコンフィギュレーションモードまたはインターフェイスコンフィギュレーションモードで **service-routing mdns-sd source-interface** *if-name* コマンドを入力します。
ステップ 4	**service-policy** *service-policy-name* {**IN** | **OUT**} 例： `Device (config-mdns)# service-policy serv-poll IN`	（任意）サービスリストで、フィルタを着信サービス検出情報（インバウンド（IN）フィルタリング）または発信サービスディスカバリ情報（アウトバウンド（OUT）フィルタリング）に対して適用します。

	コマンドまたはアクション	目的
ステップ 5	**redistribute mdns-sd** 例： `Device (config-mdns)# redistribute mdns-sd`	（任意）サブネット全体にサービスやサービス アナウンスメントを再配布します。 （注） 再配布がグローバルに有効になっている場合は、グローバル コンフィギュレーションがインターフェイス コンフィギュレーションよりも優先順位が高くなります。
ステップ 6	**cache-memory-max** *cache-config-percentage* 例： `Device (config-mdns)# cache-memory-max 20`	（任意）システム メモリの一部を（パーセンテージ単位で）キャッシュ用に設定します。 （注） デフォルトでは、システム メモリの 10% がキャッシュ用に取り分けられます。デフォルト値は、次のコマンドを使用してオーバーライドできます。
ステップ 7	**service-policy-query** *service-list-query-name service-list-query-periodicity* 例： `Device (config-mdns)# service-policy-query sl-query1 100`	（任意）サービス リスト クエリの周期性を設定します。
ステップ 8	**exit** 例： `Device (config-mdns)#exit`	（任意）グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**wireless multicast** 例： `Device (config)# wireless multicast`	（任意）ワイヤレス イーサネット マルチキャストのサポートを有効にします。

	コマンドまたはアクション	目的
ステップ 10	**no wireless mdns-bridging** 例： `Device (config)# no wireless mdns-bridging`	（任意）ワイヤレスクライアントへの mDNS パケットのブリッジングを無効にします。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

サービス検出ゲートウェイ （773 ページ）
フィルタリング （775 ページ）
例：発信 mDNS パケットに対する代替送信元インターフェイスの指定 （783 ページ）
例：サービス アナウンスメントの再配布 （783 ページ）
例：ワイヤレス クライアントに対する mDNS パケットのブリッジングの無効化 （783 ページ）
例：mDNS ゲートウェイの有効化とサービスの再配布 （784 ページ）
例：グローバル mDNS 設定 （784 ページ）
例：インターフェイス mDNS 設定 （785 ページ）

サービス検出ゲートウェイのモニタリング

表 *48*：サービス検出ゲートウェイのモニタリング

コマンド	目的
show mdns requests [**detail** | **name** *record-name*| **type** *record-type* [**name** *record-name*]]	このコマンドは、レコード名とレコード タイプ情報を含む、未処理の mDNS 要求についての情報を表示します。
show mdns cache [**interface** *type number* | **name** *record-name* [**type** *record-type*]| **type** *record-type*]	このコマンドにより、mDNS キャッシュ情報が表示されます。
show mdns statistics {**all** | **service-list** *list-name* | **service-policy** {**all** | **interface** *type number* }}	次のコマンドでは、mDNS の統計情報が表示されます。

設定例

例：発信 mDNS パケットに対する代替送信元インターフェイスの指定

次の例に、発信インターフェイスに何も設定されていない場合にその IP アドレスを使用できるように、発信 mDNS パケットに代替送信元インターフェイスを指定する方法を示します。

```
Device(config)# service-routing mdns-sd
Device(config-mdns)# source-interface if-name
```

関連トピック

mDNS ゲートウェイの有効化とサービスの再配布（CLI） （779 ページ）
サービス検出ゲートウェイ （773 ページ）
フィルタリング （775 ページ）

例：サービス アナウンスメントの再配布

次の例に、1 つのインターフェイスで受信されたサービス アナウンスメントをすべてのインターフェイスまたは特定のインターフェイスに再配布する方法を示します。

```
Device(config)# service-routing mdns-sd
Device(config-mdns)# Redistribute mdns-sd if-name
```

関連トピック

mDNS ゲートウェイの有効化とサービスの再配布（CLI） （779 ページ）
サービス検出ゲートウェイ （773 ページ）
フィルタリング （775 ページ）

例：ワイヤレス クライアントに対する mDNS パケットのブリッジングの無効化

次の例では、ワイヤレス クライアントに対する mDNS パケットのブリッジングを無効にする方法について説明します。

```
Device(config)# wireless multicast
Device(config)# no wireless mdns-bridging
```

関連トピック

mDNS ゲートウェイの有効化とサービスの再配布（CLI） （779 ページ）
サービス検出ゲートウェイ （773 ページ）
フィルタリング （775 ページ）

例：サービスリストの作成、フィルタの適用およびパラメータの設定

以下の例は、サービス リスト sl1 の作成を示しています。**permit** コマンド オプションはシーケンス番号 3 で適用され、メッセージ タイプがアナウンスメントであるすべてのサービスがフィルタ処理され、デバイスに関連するさまざまなサブネット間で転送できるようになります。

```
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)#match message-type announcement
Device(config-mdns)# exit
```

関連トピック

サービス リストの設定（CLI） （776 ページ）
サービス検出ゲートウェイ （773 ページ）
フィルタリング （775 ページ）

例：mDNS ゲートウェイの有効化とサービスの再配布

次の例に、デバイスの mDNS ゲートウェイを有効にして、サブネット間のサービスの再配布を有効にする方法を示します。インバウンド フィルタリングは、サービス リスト serv-pol1 に適用されます。システム メモリの 20% をキャッシュに使用でき、サービス リスト クエリの周期性は 100 秒に設定されています。

```
Device# configure terminal
Device# service-routing mdns-sd
Device(config-mdns)# service-policy serv-pol1 IN
Device(config-mdns)# redistribute mdns-sd
Device(config-mdns)# cache-memory-max 20
Device(config-mdns)# service-policy-query sl-query1 100
Device(config-mdns)# exit
```

関連トピック

mDNS ゲートウェイの有効化とサービスの再配布（CLI） （779 ページ）
サービス検出ゲートウェイ （773 ページ）
フィルタリング （775 ページ）

例：グローバル mDNS 設定

次に、mDNS をグローバルに設定する例を示します。

```
Device# configure terminal
Device(config)# service-list mdns-sd mypermit-all permit 10
Device(config-mdns-sd-s1)# exit
Device(config)# service-list mdns-sd querier query
Device(config-mdns-sd-s1)# service-type _dns._udp
Device(config-mdns-sd-s1)# end
```

```
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# service-policy mypermit-all IN
Device(config-mdns)# service-policy mypermit-all OUT
```

関連トピック

mDNS ゲートウェイの有効化とサービスの再配布（CLI） （779 ページ）
サービス検出ゲートウェイ （773 ページ）
フィルタリング （775 ページ）

例：インターフェイス mDNS 設定

次に、インターフェイスに mDNS を設定する例を示します。

```
Device(config)#interface Vlan136
Device(config-if)# description *** Mgmt VLAN ***
Device(config-if)# ip address 9.7.136.10 255.255.255.0
Device(config-if)# ip helper-address 9.1.0.100
Device(config-if)# service-routing mdns-sd
Device(config-if-mdns-sd)#  service-policy mypermit-all IN
Device(config-if-mdns-sd)# service-policy mypermit-all OUT
Device(config-if-mdns-sd)#  service-policy-query querier 60
```

関連トピック

mDNS ゲートウェイの有効化とサービスの再配布（CLI） （779 ページ）
サービス検出ゲートウェイ （773 ページ）
フィルタリング （775 ページ）

サービス検出ゲートウェイの設定の次の作業

次の設定を行えます。

- IGMP
- ワイヤレス マルチキャスト
- PIM
- SSM
- IP マルチキャスト ルーティング

その他の参考資料

関連資料

関連項目	マニュアル タイトル
DNS の設定	*IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3SE*
DNS の概念情報	『*IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3SE*』の「Information About DNS」の項
プラットフォームに依存しない設定情報	*IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3SE*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
RFC 6763	『*DNS-Based Service Discovery*』
マルチキャストDNSインターネット（ドラフト）	マルチキャスト

MIB

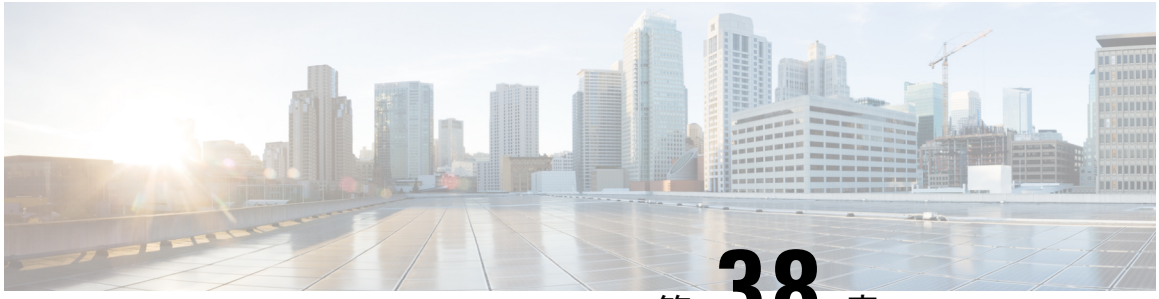
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

サービス検出ゲートウェイの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。



第 38 章

IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパース モードの最適化

- 機能情報の確認 （789 ページ）
- 大規模な IP マルチキャスト展開での PIM スパース モードの最適化の前提条件 （790 ページ）
- 大規模な IP マルチキャスト展開での PIM スパース モードの最適化について （790 ページ）
- 大規模な IP マルチキャスト展開で PIM スパース モードを最適化する方法 （794 ページ）
- 大規模なマルチキャスト展開での PIM スパース モードの最適化の設定例 （796 ページ）
- その他の参考資料 （797 ページ）
- 大規模な IP マルチキャスト展開での PIM スパース モードの最適化の機能履歴と情報 （798 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

大規模な IP マルチキャスト展開での PIM スパース モードの最適化の前提条件

- PIM スパース モードがネットワークで実行されている必要があります。
- どのグループに最短パスツリー（SPT）しきい値を適用するかを制御するのにグループ リストを使用することを計画している場合は、この作業を実行する前にアクセス リストを設定する必要があります。

大規模な IP マルチキャスト展開での PIM スパース モードの最適化について

PIM 登録プロセス

IP マルチキャスト ソースは、その存在をアナウンスするのにシグナリング メカニズムを使用しません。送信元は接続ネットワークにデータを送信するだけなのに対し、受信者は Internet Group Management Protocol（IGMP）を使用して、自身の在席状態を示します。ソースが PIM スパースモード（PIM-SM）で設定されているマルチキャストグループにトラフィックを送信すると、ソースにつながる指定ルータ（DR）は、このソースの存在についてランデブー ポイント（RP）に知らせなければなりません。この送信元からマルチキャスト トラフィックを（ネイティブに）受信するダウンストリーム受信者がRPにいて、RPが送信元につながる最短パスに加入していない場合、DRはトラフィックを送信元からRPに送信する必要があります。PIM 登録プロセスは、各 (S, G) エントリに対し個別に実行されますが、DR と RP 間のこれらのタスクを実行します。

登録プロセスは、DR が新しい (S, G) ステートを作成すると開始されます。DR は、(S, G) ステートに一致するすべてのデータ パケットを PIM 登録メッセージにカプセル化し、それらの登録メッセージを RP にユニキャストします。

RP が新しいソースからの登録メッセージを受信したいダウンストリーム レシーバを持っている場合は、RP は、登録メッセージを DR を通じて受信し続けることも、ソースにつながる最短パスに加入することもできます。デフォルトでは、ネイティブ マルチキャスト トラフィックの配信が最も高いスループットを実現するため、RP は最短パスに加入します。最短パス経由でネイティブに到着した最初のパケットを受信後、RP は DR に登録停止メッセージを送り返します。DRは、この登録停止メッセージを受信したら、RPへの登録メッセージの送信を停止します。

RP に新しい送信元からの登録メッセージを受信するダウンストリーム受信者がいない場合、RP は最短パスに加入しません。その代わり、RP は、ただちに DR に登録停止メッセージを送り返します。DRは、この登録停止メッセージを受信したら、RPへの登録メッセージの送信を停止します。

いったんソースへのルーティング エントリが確立されたら、DR と RP の間で定期的な再登録が発生します。DR が RP から登録停止メッセージを受信するまでは、ソースがアクティブであれば、マルチキャスト ルーティング テーブル ステートがタイムアウトする 1 分前に DR が 1 つのデータのない登録メッセージを RP に送信します。このアクションがマルチキャスト ルーティング テーブル エントリのタイムアウト時間をリスタートさせ、通常は、2 分ごとに 1 つの登録交換が行われることになります。登録は、ステートを維持するため、ステート損失から回復するため、および RP 上でソースを追跡するために必要です。これは、RP の最短パスへの加入からは独立して発生します。

PIM バージョン 1 の互換性

RP が PIM バージョン 1 を実行している場合、それはデータのない登録メッセージは理解しません。この場合、DR は RP にデータのない登録メッセージを送信しません。代わりに、RP から登録停止メッセージを受信後約 3 分おきに、DR は送信元からの着信データ パケットを登録メッセージにカプセル化し、それを RP に送信します。DR は RP から別の登録停止メッセージを受信するまで、登録メッセージを送信し続けます。DR が PIM バージョン 1 を実行している場合、同じ動作が起こります。

PIM バージョン 1 を実行している DR が特定の (S, G) エントリ向けの登録メッセージにデータ パケットをカプセル化すると、エントリではプロセス スイッチングが行われます（高速スイッチングやハードウェア スイッチングではない）。これらの高速パスをサポートしているプラットフォームでは、PIM バージョン 1 を実行している RP または DR の PIM 登録プロセスが、定期的で不適切なパケット配信の原因となる可能性があります。そのため、ネットワークを PIM バージョン 1 から PIM バージョン 2 にアップグレードすることを推奨しています。

PIM 指定ルータ

IP マルチキャスト用に設定されているデバイスは、PIM ハロー メッセージを送信して、どのデバイスが各 LAN セグメント（サブネット）の指定ルータ（DR）であるかを調べます。ハロー メッセージにはデバイスの IP アドレスが含まれており、最も大きい IP アドレスを持つデバイスが DR になります。

DR は、直接接続された LAN 上のすべてのホストに Internet Group Management Protocol（IGMP）ホスト クエリ メッセージを送信します。スパース モードで稼働している場合は、DR は、ソース登録メッセージをランデブー ポイント（RP）に送信します。

デフォルトでは、マルチキャスト デバイスは、30 秒ごとに PIM ルータ クエリ メッセージを送信します。デバイスがより頻繁に PIM ハロー メッセージを送信できるようにすることにより、デバイスは、応答しないネイバーをより迅速に検出できるようになります。その結果、デバイスは、より効率的なフェールオーバー手順または回復手順を実装できます。この変更は、ネットワークのエッジ上の冗長デバイスに対してのみ行うことが推奨されます。

PIM スパース モード登録メッセージ

データのない登録メッセージは、1 秒に 1 メッセージのレートで送信されます。DR が集中的なソース（データ レートの高いソース）を登録しており、RP が PIM バージョン 2 を実行していない場合は、連続的に高いレートの登録メッセージが発生する可能性があります。

デフォルトでは、PIM スパース モード登録メッセージは、レート制限なしで送信されます。登録メッセージのレートを制限すると、設定された制限を超えた登録メッセージはドロップされるという代償を伴いますが、DR および RP にかかる負荷が制限されます。レシーバは、パケットが集中的なソースから送信されてから最初の 1 秒間に、データ パケット損失を経験する可能性があります。

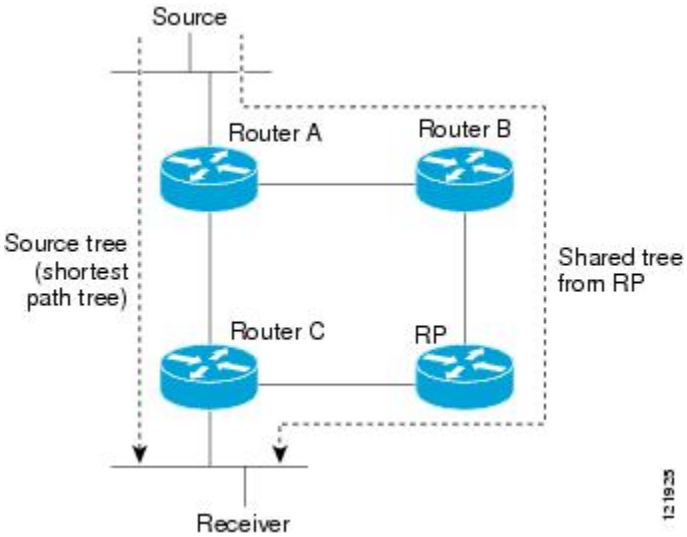
メモリ要件を減らすために最短パス ツリーの使用を回避する

PIM 共有ツリーとソース ツリーを理解しておくと、最短パス ツリーの使用を回避することでどのようにメモリ要件を減らせるかについて理解しやすくなります。

PIM 共有ツリーおよびソース ツリー（最短パス ツリー）

デフォルトでは、Rendezvous Point（RP）がルートになる単一のデータ配信ツリー全体にわたって、マルチキャスト グループのメンバが送信者からグループへのデータを受信します。このタイプの配布ツリーは、図に示すように、共有ツリーと呼ばれます。送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。

図 *37*：共有ツリーとソース ツリー（最短パス ツリー）



データ レートで保証される場合、共有ツリー上のリーフ ルータは、送信元をルートとするデータ配布ツリーへの切り替えを開始できます。このタイプの配信ツリーは、最短パス ツリー（SPT）またはソース ツリーと呼ばれます。デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

次に、共有ツリーから送信元ツリーに切り替わるプロセスの詳細を示します。

1. レシーバがグループに加入します。リーフルータであるルータ C が、RP に向けて加入メッセージを送信します。
2. RP がルータ C へのリンクを発信インターフェイス リストに登録します。
3. 送信元がデータを送信します。ルータ A はデータをカプセル化して登録メッセージに格納し、RP に送信します。
4. RP が、データを共有ツリーの下流に向けて、ルータ C に転送し、ソースに向けて加入メッセージを送信します。この時点で、データはルータ C に 2 回（カプセル化された状態で 1 回、ネイティブの状態で 1 回）着信する可能性があります。
5. データがネイティブに（マルチキャストを通じて）RP に到着すると、RP は、ルータ A に登録停止メッセージを送信します。
6. デフォルトでは、最初のデータ パケットの受信で、ルータ C のソースへの加入メッセージ送信が促されます。
7. ルータ C は、(S, G) でデータを受信すると、共有ツリーの上流に向けて、ソースのプルーニング メッセージを送信します。
8. RP が（S, G）の発信インターフェイスからルータ C へのリンクを削除します。RP は、ソースに向けてプルーニング メッセージをトリガーします。

加入メッセージとプルーニング メッセージが、ソースと RP に送信されます。これらのメッセージはホップバイホップで送信され、送信元または RP に向かうパス上の各 PIM ルータによって処理されます。register および register-stop メッセージは、ホップバイホップで送信されません。これらのメッセージは、送信元に直接接続されている指定ルータによって送信され、グループの RP によって受信されます。

グループへ送信する複数の送信元で、共有ツリーが使用されます。

最短パスツリーの使用を回避または延期する利点

共有ツリーからソース ツリーへのスイッチは、最初のデータ パケットがラスト ホップ デバイス（PIM 共有ツリーおよびソース ツリー（最短パス ツリー） （792 ページ） でのルータ C）に到着すると発生します。このスイッチが発生するのは、**ippimspt-threshold** コマンドがタイミングを制御しているためで、そのデフォルト設定は 0 kbps です。

最短パスツリーは共有ツリーより多くのメモリを必要としますが、遅延は低減します。この使用を回避または延期して、メモリの要件を減らすことができます。リーフデバイスがただちに最短パスツリーに移動できるようにする代わりに、SPT の使用を防止したり、まずトラフィックがしきい値に到達しなければならないように指定したりできます。

PIM リーフ デバイスが、指定グループの SPT に加入する時期を設定できます。送信元の送信速度が指定速度（キロビット/秒）以上の場合、デバイスは PIM Join メッセージを送信元に向けて送信し、ソース ツリー（SPT）を構築します。**infinity** キーワードを指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。

大規模な IP マルチキャスト展開で PIM スパース モードを最適化する方法

大規模な展開での PIM スパース モードの最適化

IP マルチキャストの展開が大規模な場合には、この作業を行うことを検討してください。

このタスクのステップ 3、5、および 6 は相互に依存せず、オプションと見なされます。これらの手順はいずれも、PIM スパース モードの最適化に役立ちます。ステップ 5 または 6 を実行する場合は、ステップ 4 を実行する必要があります。ステップ 6 は、指定ルータにしか適用されません。PIM クエリーの間隔の変更は、PIM ドメインのエッジにある冗長ルータに対してしか適切ではありません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ippimregister-rate-limit** *rate* 例： `Router(config)# ip pim register-rate-limit 10`	（任意）各 (S, G) ルーティング エントリについて、1 秒当たりに送信される PIM スパース モード登録メッセージの最大数の制限を設定します。 • このコマンドは、指定ルータ（DR）が各 (S, G) エントリに許可する登録メッセージ数を制限する場合に使用します。 • デフォルトでは、最大レートは設定されていません。 • このコマンドを設定すると、設定された制限を超えた登録メッセージはドロップされるという代償を伴いま

	コマンドまたはアクション	目的
		すが、DR および RP への負荷は制限されます。 • レシーバは、登録メッセージが集中的なソースから送信されてから最初の 1 秒間に、データ パケット損失を経験する可能性があります。
ステップ 4	**ippimspt-threshold**{*kbps*| **infinity**}[**group-list** *access-list*] 例： `Router(config)# ip pim spt-threshold infinity group-list 5`	（任意）最短パス ツリーに移行するには超えなければならないしきい値を指定します。 • デフォルト値は**0**です。この場合、ルータは、最初のデータ パケットを受信したらただちに SPT に加入します。 • **infinity** キーワードを指定すると、最短パス ツリーへの移行は一切行われなくなり、共有ツリーのままとなります。このキーワードは、「多対多」通信のマルチキャスト環境に適用されます。 • グループ リストは、SPT のしきい値がどのグループに適用されるかを制御する標準アクセスリストです。0 の値を指定するか、またはグループ リストを指定しなかった場合、しきい値はすべてのグループに適用されます。 • この例では、グループ リスト 5 は、すでにマルチキャスト グループ 239.254.2.0 および 239.254.3.0 を許可するように設定されています（access-list 5 permit 239.254.2.0 0.0.0.255 access-list 5 permit 239.254.3.0 0.0.0.255）。
ステップ 5	**interface** *type number* 例： `Router(config)# interface ethernet 0`	インターフェイスを設定します。 • PIM SPT しきい値または PIM クエリー間隔のデフォルト値を変更したくない場合は、このステップは実行

	コマンドまたはアクション	目的
		しないでください。このステップで変更が行われます。
ステップ 6	**ippimquery-interval** *period* [**msec**] 例： `Router(config-if)# ip pim query-interval 1`	（任意）マルチキャスト ルータが PIM ルータ クエリー メッセージを送信する頻度を設定します。 • この手順は、PIM ドメインのエッジにある冗長ルータに対してだけ実行してください。 • デフォルトのクエリー間隔は 30 秒です。 • **msec** キーワードが指定されないかぎり、*period* 引数の単位は秒です。 • クエリー間隔を少ない秒数に設定するとコンバージェンスを高速化できますが、コンバージェンスの高速化と引き換えに CPU と帯域幅の使用量が大きくなります。

関連トピック

大規模な IP マルチキャスト展開での PIM スパース モードの最適化の例 （796 ページ）

大規模なマルチキャスト展開での PIM スパース モードの最適化の設定例

大規模な IP マルチキャスト展開での PIM スパース モードの最適化の例

次の例は、下記のことを行う方法を示します。

- クエリー間隔を 1 秒に設定して、コンバージェンスを高速化する。
- ルータが一切 SPT に移行せず、共有ツリーに留まるように設定する。
- 各 (S, G) ルーティング エントリについて、1 秒当たりに送信される PIM スパース モード登録メッセージの制限を 10 個に設定する。

```
interface ethernet 0
```

```
 ip pim query-interval 1
.
.
.
!
ip pim spt-threshold infinity
ip pim register-rate-limit 10
!
```

関連トピック

大規模な展開での PIM スパース モードの最適化 （794 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP Multicast Command Reference』
PIM スパース モードの概念と設定	「Configuring Basic IP Multicast」モジュールまたは「Configuring IP Multicast in IPv6 Networks」モジュール

MIB

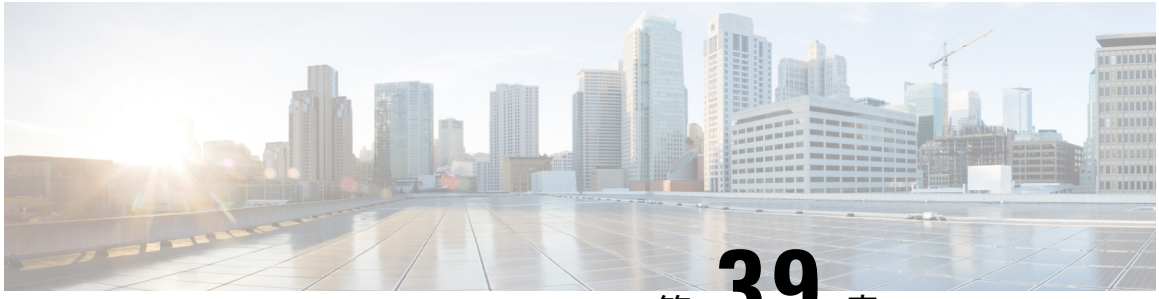
MIB	MIB のリンク
これらの機能によってサポートされる新しい MIB または変更された MIB はありません。またこれらの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

大規模な IP マルチキャスト展開での PIM スパース モードの最適化の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。



第 39 章

IP マルチキャストの最適化：マルチキャスト サブセカンド コンバージェンス

- 機能情報の確認 （799 ページ）
- マルチキャスト サブセカンド コンバージェンスの前提条件 （799 ページ）
- マルチキャスト サブセカンド コンバージェンスの制約事項 （800 ページ）
- マルチキャスト サブセカンド コンバージェンスについて （800 ページ）
- マルチキャスト サブセカンド コンバージェンスの設定方法 （803 ページ）
- マルチキャスト サブセカンド コンバージェンスの設定例 （806 ページ）
- その他の参考資料 （807 ページ）
- マルチキャスト サブセカンド コンバージェンスの機能履歴と情報 （808 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

マルチキャストサブセカンドコンバージェンスの前提条件

サービス プロバイダーは、シスコ マルチキャスト サブセカンド コンバージェンス機能を使用するには、マルチキャスト対応コアが必要です。

マルチキャストサブセカンドコンバージェンスの制約事項

サブセカンド指定ルータ（DR）フェールオーバー拡張機能を使用するデバイスは、到着したHelloインターバル情報をミリ秒単位で処理できる必要があります。輻輳しているデバイス、またはHelloインターバルを処理するための十分なCPUサイクルがないデバイスは、それが事実でない可能性があっても、Protocol Independent Multicast（PIM）ネイバーが切断されていると見なす可能性があります。

マルチキャストサブセカンドコンバージェンスについて

マルチキャスト サブセカンド コンバージェンスの利点

- スケーラビリティコンポーネントは、サービスユーザ（レシーバ）とサービス負荷（ソースまたはコンテンツ）の増加（または減少）を処理する際の効率を向上させます。
- 新しいアルゴリズムとプロセス（最大 1000 個の個別メッセージを 1 つのパケットに入れて配信する、集約された加入メッセージなど）が、コンバージェンスに達するまでの時間を 10 分の 1 にも低減します。
- マルチキャスト サブセカンド コンバージェンスが、大規模なマルチキャスト ネットワークのサービス可用性を向上させます。
- マルチキャスト機能は以前に必要とした何分の1かの時間で元に戻せるため、金融サービス会社や証券会社などのマルチキャスト ユーザは、Quality of Service（QoS）の向上が得られます。

マルチキャスト サブセカンド コンバージェンス スケーラビリティ拡張機能

マルチキャスト サブセカンド コンバージェンス機能は、サービス ユーザ（レシーバ）とサービス負荷（ソースまたはコンテンツ）の増加（または減少）を処理する際の効率を向上させるスケーラビリティ拡張機能を提供します。このリリースのスケーラビリティ拡張機能に含まれているものは次のとおりです。

- 新しいタイマー管理テクニックによる、インターネット グループ管理プロトコル（IGMP）と PIM ステート メンテナンスの向上
- Multicast Source Discovery Protocol（MSDP）Source-Active（SA）キャッシュの規模拡張の向上

スケーラビリティ拡張機能には、以下のメリットがあります。

- 可能な PIM マルチキャスト ルート（mroute）、IGMP、および MSDP SA キャッシュ ステート容量の増加
- CPU 使用率の減少

PIM ルータ クエリ メッセージ

マルチキャストサブセカンドコンバージェンスによって、PIM ルータ クエリ メッセージ（PIM hello）を数ミリ秒ごとに送信できます。PIM hello メッセージは、隣接する PIM デバイスを探すために使用されます。この機能の導入前は、デバイスは PIM hello を数秒単位でしか送信できませんでした。デバイスがより頻繁に PIM ハロー メッセージを送信できるようにすることにより、デバイスは、この機能を使用して応答しないネイバーをより迅速に検出できるようになります。その結果、デバイスは、より効率的なフェールオーバー手順または回復手順を実装できます。

関連トピック

PIM ルータ クエリ メッセージ間隔の変更 （804 ページ）
PIM ルータ クエリ メッセージ インターバルの変更例 （807 ページ）

Reverse Path Forwarding

ユニキャスト リバース パス転送（RPF）機能は、裏付けのない IP ソース アドレスを持つ IP パケットを廃棄することにより、ネットワークに変形または偽造（スプーフィング）された IP ソース アドレスが注入されて引き起こされる問題の緩和に役立ちます。変形または偽造（スプーフィング）された送信元アドレスは、送信元 IP アドレスのスプーフィングに基づいたサービス拒絶（DoS）攻撃を示す場合があります。

RPF はアクセス コントロール リスト（ACL）を使用して、不正なまたは偽造の IP 送信元アドレスを持つデータ パケットをドロップまたは転送するかどうかを判断します。ACL コマンドのオプションを使用して、システム管理者は、ドロップまたは転送されたパケットに関する情報をログに記録できます。偽装パケットに関する情報をログに記録しておくと、可能性のあるネットワーク攻撃に関する情報の発見に役立てることができます。

インターフェイスごとの統計情報を使用して、システム管理者は、ネットワーク攻撃のエントリ ポイントとなっているインターフェイスを迅速に検出できます。

RPF チェック

PIM は、標準的なユニキャストルーティングテーブルを使用して IP マルチキャストトラフィックを転送するように設計されています。PIM は、IP マルチキャストパケットのソースが、ソースから最適なパスで到着したかどうかを判断するためにユニキャスト ルーティング テーブルを使用します。RPF チェックのこのプロセスは、特定のルーティング プロトコルではなくユニキャスト ルーティング テーブルの内容に基づいているため、プロトコルに依存しません。

関連トピック

定期的な RPF チェック間隔の変更 （803 ページ）

定期的な RPF チェック間隔の変更例 （806 ページ）

トリガード RPF チェック

マルチキャスト サブセカンド コンバージェンスは、mroute ステートの RPF 変更のチェックをトリガーする機能を提供します。このチェックは、ユニキャストルーティングの変更によってトリガーされます。トリガードRPFチェックを実行することで、ユーザは定期的なRPFチェックを比較的高い値（たとえば、10秒）に設定でき、フェールオーバーは引き続き迅速に行うことができます。

トリガード RPF チェックの拡張機能によって、単一のサービス イベント（たとえば、送信元が 1 つと受信者が 1 つの状況の場合）またはパラメータに沿ったサービス規模（たとえば、多数の送信元、多数の受信者、多数のインターフェイス）などで、中断後にサービスが復元するのに必要な時間が短縮されます。この機能拡張によって、time-to-converge PIM（mroute）、IGMP、および MSDP（SA キャッシュ）状態が減少します。

RPF フェールオーバー

トリガードRPFチェックを使用する不安定なユニキャストルーティング環境では、頻繁にRPFチェックがトリガーされ、デバイスのリソースに負担がかかる可能性があります。この問題を避けるため、**ipmulticastrpfbackoff** コマンドを使用して、2 番目のトリガード RPF チェックが設定された期間の間発生しないようにします。つまり、ユーザが設定した最小限のミリ秒の間、PIM は別のトリガード RPF チェックを撤回します。

追加のルーティング テーブルの変更が行われずバックオフ期間が切れると、PIM はルーティング変更をスキャンし、それに応じてマルチキャスト RPF の変更を確立します。ただし、追加のルーティング変更がバックオフ期間中に発生すると、PIMはバックオフ期間を繰り返し、ルーティングテーブルの統合がまだ行われている間、PIM RPF変更でデバイスがオーバーロードするのを防ぎます。

関連トピック

PIM RPF フェールオーバー間隔の設定 （804 ページ）
PIM RPF フェールオーバー間隔の設定例 （807 ページ）

トポロジの変更とマルチキャスト ルーティングのリカバリ

マルチキャスト サブセカンド コンバージェンス フィーチャ セットは、ユニキャスト ルーティングのリカバリの後にほぼ瞬時に完了するマルチキャスト パス リカバリを提供することにより、企業とサービス プロバイダー両方のネットワーク バックボーンを強化します。

ネットワーク トポロジの変更が発生すると、PIM は RPF の計算をユニキャスト ルーティング テーブルに依存するため、ユニキャスト プロトコルは最初にトラフィックのベスト パスのオプションを計算する必要があり、その後、マルチキャストはベストパスを決定できるようになります。

マルチキャスト サブセカンド コンバージェンスは、ユニキャストの計算が完了した後の、ほぼ瞬時のマルチキャストプロトコル計算完了を可能にします。その結果、トポロジの変更後、マルチキャスト トラフィックの転送は大幅に速く復元されます。

マルチキャストサブセカンドコンバージェンスの設定方法

定期的な RPF チェック間隔の変更

定期的な RPF チェックの発生間隔を変更するには、次の任意の作業を実行します。

（注） シスコでは、**iprpfinterval** コマンドのデフォルト値を変更しないことを推奨しています。デフォルト値を使用すると、サブセカンド RPF フェールオーバーが有効になります。定期的な RPF チェックが発生するデフォルトの間隔は 10 秒です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmulticastrpfinterval** *seconds*[**list** *access-list* | **route-map** *route-map*] 例： `Device(config)# ip multicast rpf interval 10`	指定したインターバルでチェックが発生するように、定期的な RPF チェックのインターバルを秒単位で設定します。

関連トピック

RPF チェック （801 ページ）
定期的な RPF チェック間隔の変更例 （806 ページ）

PIM RPF フェールオーバー間隔の設定

PIM RPF フェールオーバーがルーティング テーブルの変更によってトリガーされる間隔を設定するには、次のオプション作業を実行します。

（注） シスコでは、**ipmulticastrpfbackoff** コマンドのデフォルト値を変更しないことを推奨しています。デフォルト値を使用すると、サブセカンド RPF フェールオーバーが有効になります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmulticastrpfbackoff** *minimum maximum* [**disable**] 例： `Device(config)# ip multicast rpf backoff 100 2500`	最小および最大のバックオフ インターバルを設定します。

関連トピック

RPF フェールオーバー （802 ページ）
PIM RPF フェールオーバー間隔の設定例 （807 ページ）

PIM ルータ クエリ メッセージ間隔の変更

PIM ルータ クエリ メッセージ間隔を変更するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot / subslot / port* 例： `Device(config)# interface gigabitethernet 1/0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ippimquery-interval** *period* [**msec**] 例： `Device(config-if)# ip pim query-interval 45`	マルチキャスト ルータが PIM ルータ クエリー メッセージを送信する頻度を設定します。

関連トピック

PIM ルータ クエリ メッセージ （801 ページ）
PIM ルータ クエリ メッセージ インターバルの変更例 （807 ページ）

マルチキャスト サブセカンド コンバージェンス設定の確認

マルチキャスト サブセカンド コンバージェンス機能に関する詳細情報を表示し、確認するには、次のタスクを実行します。

手順

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **showippiminterface** *type number*

このコマンドを使用して、PIM に設定されているインターフェイスに関する情報を表示します。

次に、**showippiminterface** コマンドの出力例を示します。

例：

```
Device# show ip pim interface GigabitEthernet 1/0/0
Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
172.16.1.4       GigabitEthernet1/0/0     v2/S   1      100 ms 1      172.16.1.4
```

ステップ 3 showippimneighbor

Cisco IOS XE ソフトウェアによって検出された PIM ネイバーを表示するには、このコマンドを使用します。

次に、**showippimneighbor** コマンドの出力例を示します。

例：

```
Device# show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
172.16.1.3        GigabitEthernet1/0/0     00:03:41/250 msec v2    1 / S
```

マルチキャストサブセカンドコンバージェンスの設定例

定期的な RPF チェック間隔の変更例

次の例では、**ip multicast rpf interval** が 10 秒に設定されています。このコマンドは、間隔値がデフォルト以外の値になるように設定されていない限り、**show running-config** 出力に表示されません。

```
!
ip multicast-routing
ip multicast rpf interval 10
.
.
.
interface Ethernet0/0
 ip address 172.16.2.1 255.255.255.0
.
.
.
ip pim sparse-mode
!
```

関連トピック

定期的な RPF チェック間隔の変更 （803 ページ）
RPF チェック （801 ページ）

PIM RPF フェールオーバー間隔の設定例

次に、**ip multicast rpf backoff** コマンドを、バックオフ間隔の最小値を 100、バックオフ間隔の最高値を 2500 で設定した例を示します。このコマンドは、間隔値がデフォルト以外の値になるように設定されていない限り、**show running-config** コマンド出力に表示されません。

```
!
ip multicast-routing
.
.
.
ip multicast rpf backoff 100 2500
!
!
interface Ethernet0/0
 ip address 172.16.2.1 255.255.255.0
.
.
.
ip pim sparse-mode
!
```

関連トピック

PIM RPF フェールオーバー間隔の設定 （804 ページ）
RPF フェールオーバー （802 ページ）

PIM ルータ クエリ メッセージ インターバルの変更例

次の例では、**ip pim query-interval** コマンドが 100 ミリ秒に設定されています。このコマンドは、間隔値がデフォルト以外の値になるように設定されていない限り、**show running-config** コマンド出力に表示されません。

```
!
interface gigabitethernet0/0/1
 ip address 172.16.2.1 255.255.255.0
ip pim query-interval 100 msec
ip pim sparse-mode
```

関連トピック

PIM ルータ クエリ メッセージ間隔の変更 （804 ページ）
PIM ルータ クエリ メッセージ （801 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
Cisco IOS IP SLA コマンド	『Cisco IOS IP Multicast Command Reference』
PIM スパース モードの概念と設定	「Configuring Basic IP Multicast」モジュールまたは「Configuring IP Multicast in IPv6 Networks」モジュール

MIB

MIB	MIB のリンク
これらの機能によってサポートされる新しい MIB または変更された MIB はありません。またこれらの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右のURLにアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

マルチキャストサブセカンドコンバージェンスの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 40 章

IP マルチキャストの最適化：等コスト パス間での IP マルチキャスト ロード スプリッティング

- 機能情報の確認 （809 ページ）
- 等コスト パス間での IP マルチキャスト ロード スプリットの前提条件 （810 ページ）
- 等コスト パス間での IP マルチキャスト ロード スプリッティングについて （810 ページ）
- ECMP を介して IP マルチキャスト トラフィックをロード スプリットする方法 （822 ページ）
- ECMP を介した IP マルチキャスト トラフィックのロード スプリットの設定例 （831 ページ）
- その他の参考資料 （832 ページ）
- ECMP を介した IP マルチキャスト トラフィックのロード スプリットの機能履歴と情報 （833 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

等コスト パス間での IP マルチキャスト ロード スプリットの前提条件

IP マルチキャストをデバイスで有効にするには、『*IP Multicast: PIM Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。

等コスト パス間での IP マルチキャスト ロード スプリッティングについて

ロード スプリットとロード バランシング

ロード スプリットとロード バランシングは同じではありません。ロード スプリットでは、複数の等コスト リバース パス フォワーディング（RPF）パスを介して (*, G) および (S, G) トラフィック ストリームをランダムに分散する手段が提供され、必ずしもそれらの等コスト RPF パス上で平衡のとれた IP マルチキャスト トラフィック負荷が得られるわけではありません。IP マルチキャスト トラフィックのロード スプリットに使用される方法は、(*, G) および (S, G) トラフィック ストリームをランダムに分散させることによって、フローをカウントしてではなく、むしろ疑似乱数判定を作成して、使用可能な各 RPF パスに等価な量のトラフィック フローを分散させようとします。これらの方法は総称して等コスト マルチパス（ECMP）マルチキャスト ロード スプリットと呼ばれ、ほぼ同量の帯域幅を使用する多くのトラフィック ストリームがあるネットワークでのロード シェアリングを向上させます。

一連の等コスト リンクにわたってわずか 2、3 の (S, G) または (*, G) ステート フローしかない場合は、それらの良好なバランスが得られる可能性は非常に低くなります。この制限を克服するため、(S, G) ステートの場合は事前に計算された発信元アドレス、または (*, G) ステートの場合はランデブー ポイント（RP）アドレスを使用して、合理的な形式のロード バランシングを実現できます。この制限は、Cisco Express Forwarding（CEF）または EtherChannel でのフロー単位のロードスプリットに同様に適用されます。わずかなフローがある限り、それらの方法でロード スプリットを行っても、何らかの形式の手動によるエンジニアリングなしでは良好なロード分散は得られません。

複数の等コスト パスが存在する場合の IP マルチキャストのデフォルト動作

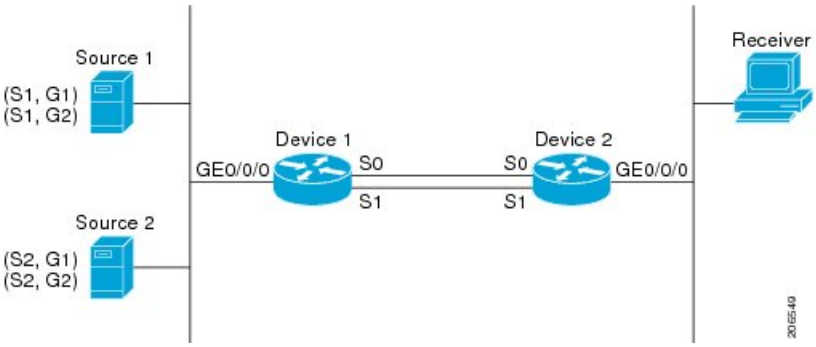
デフォルトでは、Protocol Independent Multicast スパース モード（PIM-SM）、Source Specific Multicast（PIM-SSM）、双方向 PIM（Bidir-PIM）、および PIM デンス モード（PIM-DM）グループについては、複数の等コスト パスが使用可能な場合、リバース パス転送（RPF）for IPv4 マルチキャスト トラフィックは、最も大きい IP アドレスを持つ PIM ネイバーに基づきます。

この方法は、最高 PIM ネイバー動作と呼ばれます。この動作は、PIM-SM の RFC 2362 に基づいていますが、PIM-SSM、PIM-DM、および bidir-PIM にも適用されます。

次の図に、複数の等コスト パスが存在する場合の IP マルチキャストのデフォルト動作を説明するためにここで使用するサンプル トポロジを示します。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *38 :* 複数の等コスト パスが存在する場合の *IP* マルチキャストのデフォルト動作



この図では、2 つの送信元 S1 および S2 が、トラフックを IPv4 マルチキャスト グループ G1 および G2 に送信しています。PIM-SM、PIM-SSM、PIM-DM のいずれかが、このトポロジに使用できます。PIM-SM が使用される場合は、**ippimspt-threshold** コマンドのデフォルト 0 がデバイス 2 で使用中で、内部ゲートウェイ プロトコル（IGP）が実行中で、S1 および S2 向け（デバイス 2 で入力された場合）の **showiproute** コマンドの出力に、デバイス 1 でのシリアル インターフェイス 0 およびシリアル インターフェイス 1 がデバイス 2 の等コスト ネクストホップ PIM ネイバーとして表示されると仮定します。

追加の設定を行うことなく、図に示すトポロジ内の IPv4 マルチキャスト トラフィックは、どちらのインターフェイスがより高い IP アドレスを持っているかに応じて、常に 1 つのシリアル インターフェイス（シリアル インターフェイス 0 またはシリアル インターフェイス 1）を経由して移動します。たとえば、デバイス 1 上のシリアル インターフェイス 0 とシリアル インターフェイス 1 で設定されている IP アドレスが、それぞれ 10.1.1.1 と 10.1.2.1 であるものとします。このシナリオが与えられているとして、PIM-SM と PIM-SSM の場合、デバイス 2 は、図に示されるすべてのソースおよびグループについて、常に PIM 加入メッセージを 10.1.2.1 に送信し、常にシリアル インターフェイス 1 上で IPv4 マルチキャスト トラフィックを受信します。PIM-DM の場合は、デバイス 2 は、常に IP マルチキャスト トラフィックをシリアル インターフェイス 1 上で受信し、その場合にだけ、PIM 加入メッセージが PIM-DM で使用されず、代わりにデバイス 2 はシリアル インターフェイス 0 を通る IP マルチキャスト トラフィックをプルーニングし、それをシリアル インターフェイス 1 を通じて受信します。これは、デバイス 1 上ではシリアル インターフェイス 1 が最も大きい IP アドレスを持つためです。

IPv4 RPF ルックアップが中継マルチキャスト デバイスによって実行され、IPv4 (*,G) および (S, G) マルチキャスト ルート（ツリー）のための RPF インターフェイスと RPF ネイバーが決定されます。RPF ルックアップは、RPF ルート選択とルート パス選択によって構成されます。

RPF ルート選択は、マルチキャスト ツリーのルートを特定するために、IP ユニキャスト アドレスだけで動作します。(*, G) ルート（PIM-SM および Bidir-PIM）の場合、マルチキャスト ツリーのルートはグループ G の RP アドレスです。(S, G) ツリー（PIM-SM、PIM-SSM および PIM-DM）の場合、マルチキャスト ツリーのルートは送信元 S です。RPF ルート選択では、ルーティング情報ベース（RIB）で、また設定済みの場合（または使用可能な場合）は、ディスタンス ベクター マルチキャスト ルーティング プロトコル（DVMRP）ルーティング テーブル、マルチプロトコル ボーダー ゲートウェイ プロトコル（MBGP）ルーティング テーブルまたは設定済みの静的マルチキャスト ルータで、RP または送信元に対する最適なルートが検索されます。得られたルートが使用可能な 1 つのパスだけだった場合は、RPF ルックアップが完了し、ルートのネクストホップ デバイスおよびインターフェイスが、このマルチキャスト ツリーの RPF ネイバーと RPF インターフェイスになります。そのルートに使用可能な複数のパスがある場合は、ルート パス選択を使用して、どのパスを選択するかが決定されます。

IP マルチキャストでは、ルート パス選択に次の方法が使用できます。

（注） IP マルチキャストで使用可能なルート パス選択のデフォルトの方法以外のすべての方法で、いくつかの形式の ECMP マルチキャスト ロード スプリッティングが可能です。

- 最も高い PIM ネイバー：これはデフォルトの方法です。したがって、設定は不要です。複数の等コスト パスが使用できる場合は、RPF for IPv4 マルチキャスト トラフィックは、最も大きい IP アドレスを持つ PIM ネイバーに基づき、その結果、設定しなければ、ECMP マルチキャスト ロード スプリットはデフォルトでディセーブルになります。

- ECMP マルチキャスト ロード スプリットの発信元アドレスに基づいた方法：**ipmulticastmultipath** コマンドにを使用して、ECMP マルチキャスト ロード スプリットを設定できます。この形式の **ipmulticastmultipath** コマンドを入力すると、S ハッシュ アルゴリズムを使用する、発信元アドレスに基づいた ECMP マルチキャスト ロード スプリットがイネーブルになります。詳細については、「S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード スプリット （813 ページ）」の項を参照してください。

- ECMP マルチキャスト ロード スプリットのソースおよびグループ アドレスに基づいた方法：**ipmulticastmultipath** コマンドに **s-g-hash** キーワードと **basic** キーワードを指定して、ECMP マルチキャスト ロード スプリットを設定できます。この形式の **ipmulticastmultipath** コマンドを入力すると、基本 S-G ハッシュ アルゴリズムを使用する、ソースとグループ アドレスに基づいた ECMP マルチキャスト ロード ススプリットがイネーブルになります。詳細については、「基本 S-G ハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリット （814 ページ）」の項を参照してください。

- ECMP マルチキャスト ロード スプリットのソース、グループ、およびネクストホップ アドレスに基づいた方法：**ipmulticastmultipath** コマンドに **s-g-hash** キーワードと **next-hop-based** キーワードを指定して、ECMP マルチキャスト ロード スプリットを設定できます。この形式のコマンドを入力すると、ネクストホップ ベースの S-G ハッシュ アルゴリズムを使用した、ソース アドレス、グループ アドレス、およびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットが可能になります。詳細について

は、「ソース グループとネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリッティング （816 ページ）」の項を参照してください。

デフォルト動作（最高 PIM ネイバー動作）は、IP マルチキャストでのどのような形の ECMP ロード スプリットにもならず、使用可能なパスのネクスト ホップ PIM ネイバーの中から最も大きい IP アドレスを持つ PIM ネイバーを選択します。ネクスト ホップは **showippimneighbor** コマンドの出力に表示された場合に PIM ネイバーとみなされます。これは、それからの PIM のハローメッセージが受信され、タイムアウトしていない場合です。使用可能なネクストホップのいずれも PIM ネイバーでない場合は、そのまま最も高い IP アドレスを持つネクスト ホップが選択されます。

IP マルチキャスト トラフィックをロード スプリットする方法

一般に、IPマルチキャスト トラフィックのロードスプリットには、次の方法が使用できます。

- ソース アドレス、ソース アドレスとグループ アドレス、またはソース アドレスとグループ アドレスとネクスト ホップ アドレスに基づいて、ECMP マルチキャスト ロード スプリッティングをイネーブルにできます。等コスト パスが認識された後、ECMP マルチキャスト ロードスプリットは、ユニキャスト トラフィックと同様に、パケットごとではなく、(S, G) ごとに動作します。
- IP マルチキャストをロード スプリットする別の方法としては、2 つ以上の等コスト パスを Generic Routing Encapsulation（GRE）トンネルに統合して、ユニキャスト ルーティング プロトコルがロード スプリットを実行できるようにするか、または Fast または Gigabit EtherChannel インターフェイス、マルチリンク PPP（MLPPP）リンク バンドル、またはマルチリンク フレーム リレー（FR.16）リンク バンドルなどのバンドル インターフェイスを介してロード スプリットできるようにします。

ECMP マルチキャスト ロード スプリットの概要

デフォルトでは、IPv4 マルチキャスト トラフィックの ECMP マルチキャスト ロード スプリットはディセーブルになっています。ECMP マルチキャスト ロード スプリットは、**ip multicast multipath** コマンドを使用してイネーブルにできます。

S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード スプリット

発信元アドレスに基づく ECMP マルチキャスト ロード スプリットのトラフィックは、S ハッシュ アルゴリズムを使用して、各 (*, G) または (S, G) ステートの RPF インターフェイスが、ステートの解決される RPF アドレスに応じて、使用可能な等コスト パスの中から選択されるようにします。(S, G) ステートの場合、RPF アドレスはステートの発信元アドレスです。(*, G) ステートの場合、RPF アドレスはステートのグループ アドレスに関連付けられた RP のアドレスです。

発信元アドレスに基づいて ECMP マルチキャスト ロード スプリットを設定すると、さまざまなステートのマルチキャスト トラフィックを等コスト インターフェイスのうち複数を介して

受信できます。原則として、IPv4 マルチキャストによって適用される方法は、IPv4 CEF でのデフォルトのフロー単位のロード スプリットまたは Fast および Gigabit EtherChannel で使用されるロード スプリットとかなり似ています。しかし、ECMP マルチキャスト ロード スプリットのこの方法は、局在化の影響を受けます。

関連トピック

ソース アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 （824 ページ）
例：ソース アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 （831 ページ）

基本 S-G ハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリット

送信元アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリットでは、送信元アドレスとグループ アドレスに基づいた基本 S-G ハッシュ アルゴリズムと呼ばれる、単純なハッシュが使用されます。基本 S-G ハッシュ アルゴリズムは、ハッシュ値を出すためにランダム化を一切使用しないため、予測可能です。ただし、S-G ハッシュ アルゴリズムは、特定のソースとグループについて、どのデバイス上でそのハッシュが計算されたかに関係なく常に同じハッシュが得られるため、局在化する傾向があります。

（注） 基本の S-G ハッシュ アルゴリズムでは、Bidir-PIM グループは無視されます。

関連トピック

ソース アドレスおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 （827 ページ）
ソース アドレスおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化の例 （831 ページ）

S ハッシュおよび基本 S-G ハッシュ アルゴリズムを使用した場合の副産物としての予測可能性

IPv4 マルチキャストの ECMP マルチキャスト ロード スプリットで使用される方法では、同じ数の等コストパスがトポロジ内の複数の場所に存在するネットワークにおいて、一貫したロード スプリットが可能です。フローを N パスを通過して分割させるために RP アドレスまたは送信元アドレスが計算されると、フローはトポロジ内のすべての場所で同じようにそれらの N パスを通過して分割されます。一貫したロードスプリットによって予測可能性を考慮でき、それにより、IPv4 マルチキャスト トラフィックのロード スプリットを手動で操作できるようになります。

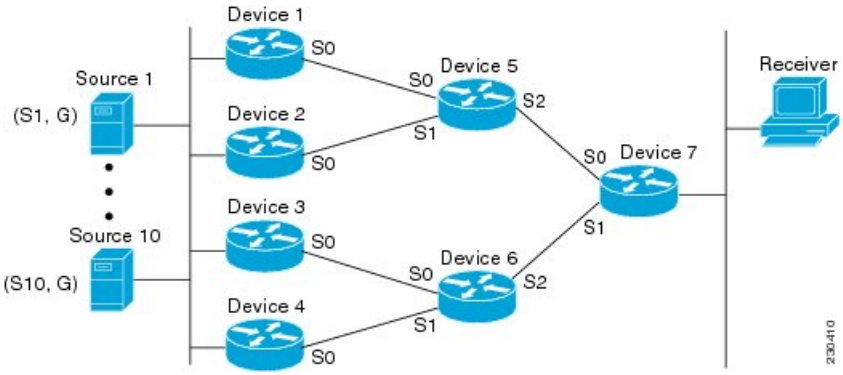
S ハッシュおよび基本 S-G ハッシュ アルゴリズムを使用した場合の副産物としての局在化

ソース アドレスまたはソースおよびグループ アドレスによってマルチキャスト トラフィックをロード スプリットするために IPv4 マルチキャストで使用されるハッシュ機能には通常、局在化と呼ばれる問題があります。ソース アドレスまたはソースおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットの副産物として、局在化は、一部のトポロジ内のルータがロードスプリットに使用可能なすべてのパスを効果的に使用できないという問題です。

次の図に、ソース アドレスに基づく、またはソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリットを設定した場合の局在化の問題を説明するために、ここで使用するトポロジを示します。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *39 :* 局在化トポロジ



図に示すトポロジでは、ルータ 7 がルータ 5 およびルータ 6 を経由してソース S1 ～ S10 に向かう 2 つの等コスト パスがあることに注目してください。このトポロジでは、ECMP マルチキャスト ロード スプリッティングが **ipmulticastmultipath** コマンドを使用してトポロジ内のすべてのルータで有効になっていると仮定します。このシナリオでは、ルータ 7 は、10 個の (S, G) ステートに等コスト ロード スプリットを適用します。このシナリオにおける局在化の問題は、ルータ 7 に影響します。そのルータがソース S1 ～ S5 についてはルータ 5 でシリアル インターフェイス 0 を選択し、ソース S6 ～ S10 についてはルータ 6 でシリアル インターフェイス 1 を選択することになるからです。さらに、このトポロジでは、局在化の問題による影響はルータ 5 とルータ 6 にも及びます。ルータ 5 には、ルータ 1 上のシリアル インターフェイス 0 およびルータ 2 上のシリアル インターフェイス 1 を経由する S1 ～ S5 への 2 つの等コスト パスがあります。ルータ 5 は、2 つのパスのどちらを使用するかの選択に同じハッシュ アルゴリズムを適用するため、ソース S1 ～ S5 には 2 つのアップストリーム パスのうちの片方だけを使用することになります。つまり、すべてのトラフィックがルータ 1 とルータ 5 を流れるか、またはルータ 2 とルータ 5 を流れるかのいずれかになります。このトポロジでは、ロード スプリットにルータ 1 とルータ 5 およびルータ 2 とルータ 5 を使用することはできません。同様

に、局在化問題は、ルータ 3 とルータ 6 およびルータ 4 とルータ 6 に当てはまります。つまり、このトポロジでは、ロード スプリットにルータ 3 とルータ 6 およびルータ 4 とルータ 6 の両方を使用することはできません。

ソース グループとネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリッティング

ソース、グループ、およびネクストホップ アドレスに基づいて ECMP マルチキャスト ロード スプリットを設定すると、ソース、グループ、およびネクストホップアドレスに基づくより複雑なハッシュ、ネクストホップ ベースの S-G ハッシュ アルゴリズムが有効になります。ネクスト ホップ ベースの S-G ハッシュ アルゴリズムは、ハッシュ値の計算にランダム化を一切使用しないため、予測可能です。S ハッシュ アルゴリズムや基本 S-G ハッシュ アルゴリズムと違って、ネクスト ホップ ベースの S-G ハッシュ アルゴリズムに使用されるハッシュ メカニズムは、局在化の傾向がありません。

（注） IPv4 マルチキャストにおけるネクストホップ ベースの S-G ハッシュ アルゴリズムは、IPv6 ECMPマルチキャスト ロードスプリットで使用されるものと同じアルゴリズムであり、PIM-SM ブートストラップ デバイス（BSR）に使用されるものと同じハッシュ機能を活用できます。

ネクストホップベースのハッシュ機能では局在化は生成されず、パスで障害が発生した場合により良い RPF の安定性が維持されます。これらの利点には、ソース アドレスまたは RP IP アドレスを使用して信頼性を持って予測したり、ネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用した場合にロードスプリットの成果をエンジニアリングしたりすることができないという代償が伴います。多くのカスタマー ネットワークは等コスト マルチパス トポロジを実装しているため、ロードスプリットの手動操作は多くの場合必須ではありません。むしろ、IP マルチキャストのデフォルトの動作が IP ユニキャストと類似している必要があります。つまり、IP マルチキャストはベストエフォート ベースで複数の等コスト パスを使用すると期待されます。そのため、局在化の異常により、IPv4マルチキャストのロードスプリットはデフォルトで有効にできません。

（注） また、CEF ユニキャストのロード スプリットは局在化を示さない方法を使用し、同様にロード スプリットの結果を予測したりロード スプリットの結果を操作するために使用することはできません。

ネクストホップ ベースのハッシュ機能では、PIM ネイバーの実際のネクストホップ IP アドレスが計算に取り込まれるため、局在化を回避できます。そのため、ハッシュの結果は各デバイスで異なり、実質的に局在化の問題はありません。局在化の回避に加えて、このハッシュ機能は、パスの障害に直面して選択された RPF パスの安定性も向上させます。4 つの等コスト パスを持つデバイスと、これらのパス間でロードスプリットされる多数のステートを考えます。これらのパスの 1 つに障害が発生し、残りの 3 つのパスが使用可能な状態になったとします。ハッシュ機能の二極化によって使用されるハッシュ機能（S ハッシュおよび基本の S-G ハッシュ アルゴリズムによって使用されるハッシュ機能）を使用して、すべてのステートの RPF

パスは再コンバージェンスされるため、それら 3 つのパスの間（特にそれら 3 つのパスのいずれかをすでに使用していたパス）で変更される可能性があります。したがって、これらのステートは、その RPF インターフェイスとネクスト ホップ ネイバーが不必要に変更されることになります。この問題が発生するのは、このアルゴリズムでは、選択されるパスが、考慮できるすべてのパスの総数を取ることにより決定されるためです。このため、いったんパスが変わると、すべてのステートの RPF 選択も変更の対象となります。ネクスト ホップ ベースのハッシュ アルゴリズムでは、RPF の変更されたパスを使用していたステートだけが、残る 3 つのパスのいずれかへと再コンバージェンスする必要があります。すでにこれらのパスのいずれかを使用しているステートは、変更されません。4 つ目のパスが再び稼働し始めると、最初はそれを使用していたステートが、ただちに再コンバージェンスしてそのパスに戻ります。他のステートは、一切影響を受けません。

（注） ネクスト ホップ ベースの S-G ハッシュ アルゴリズムでは、Bidir-PIM グループは無視されます。

関連トピック

ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 （829 ページ）
ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化の例 （832 ページ）

RPF パス選択のための PIM ネイバー クエリおよびハロー メッセージへの ECMP マルチキャスト ロード スプリットの影響

ECMP を介する IP マルチキャスト トラフィックのロード スプリットがイネーブルになっておらず、RP またはソースに向けて複数の等コスト パスが存在する場合、IPv4 マルチキャストは、まず最も大きい IP アドレスの PIM ネイバーを選択します。PIM ネイバーとは、受信した PIM ハロー（または PIMv1 クエリ）メッセージのソース デバイスです。たとえば、IGP で学習された、または 2 つのスタティック ルート経由で設定された 2 つの等コスト パスを持つデバイスを考えてみます。これら 2 つのパスのネクスト ホップは、10.1.1.1 と 10.1.2.1 です。これらのネクスト ホップ デバイスの両方が PIM ハロー メッセージを送信した場合、10.1.2.1 が最も IP アドレスの大きい PIM ネイバーとして選択されます。10.1.1.1 だけが PIM ハロー メッセージを送信した場合は、10.1.1.1 が選択されます。これらのデバイスのどちらも PIM ハロー メッセージを送信しない場合は、10.1.2.1 が選択されます。PIM ハロー メッセージへのこの違いが、スタティック マルチキャスト ルート（mroute）しか持たない特定のタイプのダイナミック フェールオーバー シナリオの構築を可能にします。それ以外では、これはあまり有用ではありません。

（注） スタティック mroute の設定の詳細については、ftp://ftpeng.cisco.com/ipmulticast/config-notes/static-mroutes.txt で Cisco IOS IP マルチキャスト FTP サイトにある『Configuring Multiple Static Mroutes in Cisco IOS』設定ノートを参照してください。

ECMP を介する IP マルチキャスト トラフィックのロード スプリットがイネーブルになっている場合、ネイバーからの PIM ハロー メッセージの存在は考慮されません。つまり、選択される RPF ネイバーは、そのネイバーからの PIM ハロー メッセージを受信したかどうかに左右されません。選択は、等コスト ルート エントリの有無にだけ依存します。

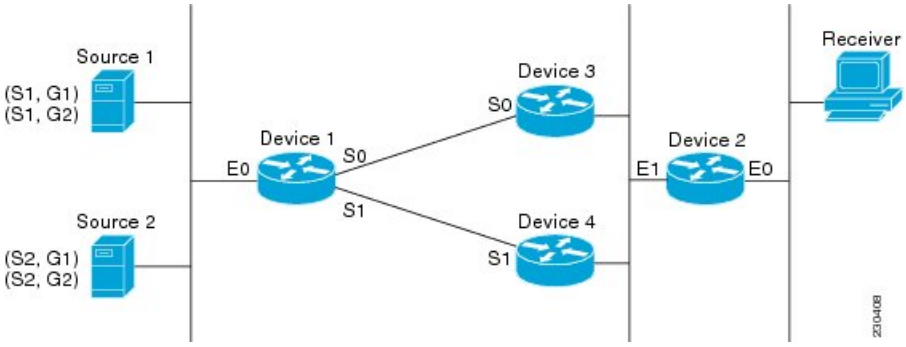
PIM-DM および Bidir-PIM での DF 選定でのアサート処理に対する ECMP マルチキャスト ロード スプリットの影響

ipmulticastmultipath コマンドが変更するのは、ダウンストリーム デバイスの RPF 選択だけです。Bidir-PIM での指定フォワーダ（DF）選定や、PIM-DM でのアップストリーム デバイスへのアサート処理には影響しません。

次の図に、ECMP マルチキャスト ロード スプリットの PIM-DM におけるアサート処理および Bidir-PIM における DF 選定に与える影響を説明するために、ここで使用するトポロジを示します。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *40 : ECMP* マルチキャスト ロード スプリットと *PIM-DM* におけるアサート処理および *Bidir-PIM* における *DF* 選定



図では、デバイス 2 が S1 と S2 およびデバイス 1 上の RP アドレスへの 2 つの等コスト パスを持っています。両方のパスが、ギガビット イーサネット インターフェイス 1/0/0 を通ります。片方のパスはデバイス 3、他方のパスはデバイス 4 に向かいます。PIM-SM と PIM-SSM (*, G) および (S, G) RPF 選択の場合は、このトポロジでのデバイス 2 の動作と図に示したトポロジでのデバイス 2 の動作に違いはありません。一方、PIM-DM または Bidir-PIM を使用する場合は、違いがあります。

図に示したトポロジで PIM-DM を使用する場合は、デバイス 3 とデバイス 4 がギガビット イーサネット インターフェイス 1/0/0 へのステートのトラフィックのフラッディングを開始させ、トラフィックを転送してトラフィックの重複を回避するために、PIM アサート処理を使用してそれらの中から 1 つのデバイスを選定します。デバイス 3 とデバイス 4 は両方とも同じルート コストを持つため、常にギガビット イーサネット インターフェイス 1/0/0 上で最も大きい IP アドレスを持つデバイスがアサート処理で選択されます。この結果、このトポロジで PIM-DM

を使用した場合は、トラフィックは、デバイス 3 とデバイス 4 の間でロード スプリットされません。

図に示されているトポロジで Bidir-PIM を使用すると、ギガビット イーサネット インターフェイス 1/0/0 上のデバイス 2、デバイス 3、およびデバイス 4 の間で DF 選定と呼ばれる処理が発生します。DF 選定の処理では、特定の RP を使用する任意のグループについてギガビット イーサネット インターフェイス 1/0/0 を介してトラフィックを転送するために、そのインターフェイスに設定されている最も大きい IP アドレスを持つデバイスに基づいて各 RP に 1 つのデバイスが選定されます。複数の RP が使用されている場合でも（たとえば、G1 に 1 つ、G2 に別の 1 つなど）、それらの RP の DF 選定では、常にギガビット イーサネット インターフェイス 1/0/0 に設定されている最も大きい IP アドレスを持つデバイスが選定されます（このトポロジでは、デバイス 3 またはデバイス 4）。DF 選定に使用される選定ルールは、実質的には PIM アサート処理に使用される選定ルールと同じで、唯一異なるのは、ネゴシエーションに使用されるプロトコル メカニズムが DF 選定の方が洗練されているという点だけです（より理にかなった結果を返すために）。結果として、このトポロジで Bidir-PIM を使用した場合、ギガビット イーサネット インターフェイス 1/0/0 で常にロード スプリットが発生します。

ECMP マルチキャスト ロード スプリットが RPF 選択には影響し、Bidir-PIM での PIM-DM または DF 選定のアサート処理には影響しないのは、アサート処理と DF 選定の両方が、参加するデバイス間で一貫性を保つように実装されている必要がある連携処理であるためです。これらを変更すると、何らかの形でのプロトコルの変更が必要になり、それについて、参加しているデバイスによる合意が必要になります。RPF 選択は、純粋にデバイス ローカル ポリシーであるため、各デバイスでの個別のプロトコル変更を伴わずにイネーブルにしたりディセーブルにしたりできます。

等コスト パスが同一 LAN 上でのアップストリーム PIM ネイバーではなく、異なる LAN またはポイントツーポイント リンク上のネイバーであるトポロジでは、PIM-DM と Bidir-PIM には **ipmulticastmultipath** コマンドで ECMP マルチキャスト ロード スプリットを設定するのが唯一の効果的な方法です。

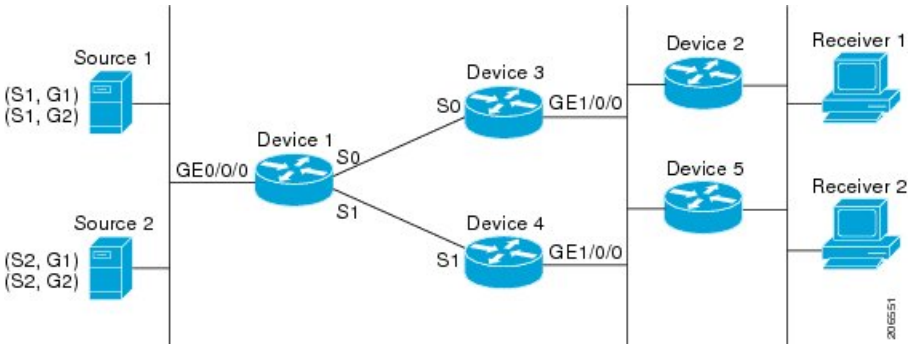
PIM-SM および PIM-SSM での PIM アサート処理に対する ECMP マルチキャスト ロード スプリットの影響

PIM-SM を (*, G) または (S, G) 転送で使用していた場合、または PIM-SSM を (S, G) 転送で使用していた場合でも、PIM アサート処理が発生したことが原因で **ipmulticastmultipath** コマンドでの ECMP マルチキャスト ロード スプリットが有効でなくなる場合もあります。

次の図に、PIM-SM および PIM-SSM での ECMP マルチキャスト ロード スプリットの PIM アサート処理への影響を説明するためにここで使用するサンプル トポロジを示します。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *41 : PIM-SM* および *PIM-SSM* での *ECMP* マルチキャスト ロード スプリットと *PIM* アサート処理



図に示すトポロジでは、デバイス 2 とデバイス 5 の両方がシスコ デバイスで、**ipmulticastmultipath** コマンドを使用して ECMP マルチキャスト ロード スプリット用に一貫性を持って設定されており、ロード スプリットが期待どおりに動作し続けるようになっています。つまり、両方のデバイスがデバイス 3 とデバイス 4 を等コスト ネクスト ホップとして持ち、等コスト パスのリストを同じ方法で（IP アドレスにより）ソートします。各 (S, G) ステートまたは (*, G) ステートに対してマルチパス ハッシュ関数を適用すると、それらは同じ RPF ネイバー（デバイス 3 またはデバイス 4）を選択し、その PIM 加入をこのネイバーに送信するようになります。

デバイス 5 とデバイス 2 が **ipmulticastmultipath** コマンドで一貫性のないように設定されている場合、またはデバイス 5 がサードパーティ製デバイスの場合は、デバイス 2 とデバイス 5 が、一部の (*, G) ステートまたは (S, G) ステートに対して異なる RPF ネイバーを選択する可能性があります。たとえば、デバイス 2 は、特定の (S, G) ステートに対してデバイス 3 を選択し、デバイス 5 は特定の (S, G) ステートに対してデバイス 4 を選択したりします。このシナリオでは、デバイス 3 とデバイス 4 が両方ともそのステートのトラフィックのギガビット イーサネット インターフェイス 1/0/0 への転送を開始し、お互いの転送したトラフィックを見て、トラフィックの重複を回避するためにアサート処理を開始します。その結果、その (S, G) ステートについては、ギガビット イーサネット インターフェイス 1/0/0 に最も大きい IP アドレスを持つデバイスがトラフィックを転送します。ところが、デバイス 2 とデバイス 5 は両方ともアサート選定での選択結果を追跡し、このアサートで選択されたデバイスが自分がその RPF 選択で計算して得たデバイスと同じでなくても、そのステートのための PIM 加入をこのアサートで選択されたデバイスに送信します。このため、PIM-SM と PIM-SSM では、ECMP マルチキャスト ロード スプリットの動作が保証されるのは、LAN 上のすべてのダウンストリーム デバイスが一貫性を持って設定されたシスコ デバイスである場合だけです。

ユニキャスト ルーティングが変わった場合の ECMP マルチキャスト ロード スプリットと再コンバージェンス

ユニキャスト ルーティングが変わると、すべての IP マルチキャスト ルーティング ステートが、利用可能なユニキャスト ルーティング情報を元にしてただちに再コンバージェンスされます。特に、1 つのパスが停止した場合、残りのパスがただちに再コンバージェンスされ、そのパスが再び稼働し始めた場合、それ以降は、マルチキャスト転送は、そのパスが停止する前に使用されていた同じ RPF パスに再コンバージェンスされます。再コンバージェンスは、ECMP

上の IP マルチキャスト トラフィックのロード スプリットが設定されているかどうかにかかわらず発生します。

ECMP マルチキャスト ロード スプリットでの BGP の使用

ECMP マルチキャスト ロード スプリットは、BGP を通じて学習した RPF 情報とも、その他のプロトコルから学習した RPF 情報と同じ方法で一緒に動作します。このプロトコルによりインストールされた複数のパスの中から 1 つのパスを選択します。BGP での主な違いは、デフォルトでは単一のパスしかインストールされないことです。たとえば、BGP スピーカーがプレフィックスに 2 つの同一外部 BGP（eBGP）パスを学習した場合、最も小さいデバイス ID を持つパスが最良パスとして選択されます。この最良パスが IP ルーティング テーブルにインストールされます。BGP マルチパス サポートがイネーブルになっており、隣接する同一の AS から複数の eBGP パスが学習された場合、単一の最良パスが選ばれるのではなく、複数のパスが IP ルーティング テーブルにインストールされます。デフォルトでは、BGP は IP ルーティング テーブルに 1 つのパスしかインストールしません。

BGP に学習されるプレフィックスに ECMP マルチキャスト ロード スプリットを使用するには、BGP マルチパスをイネーブルにする必要があります。一度設定されると、BGP によりリモート ネクスト ホップ情報がインストールされた場合、その BGP ネクスト ホップに対して（ユニキャストとして）最良のネクスト ホップを検出するため、RPF ルックアップが再帰的に実行されます。たとえば、与えられたプレフィックスに対して単一の BGP パスしかないのに、その BGP ネクスト ホップに到達する IGP パスが 2 つあった場合、マルチキャスト RPF は、この異なる 2 つの IGP パス間で正しくロード スプリットします。

スタティック mroute での ECMP マルチキャスト ロード スプリットの使用

特定のソースまたは RP に対して IGP を使用して等コスト ルートをインストールすることが可能でない場合、スタティック ルートを設定して、ロード スプリットのための等コスト パスを指定することができます。ソフトウェアは、プレフィックスに対し 1 つのスタティック mroute という設定をサポートしていないため、等コスト パスの設定にスタティック mroute は使用できません。再帰的なルート ルックアップを使用した場合のこの制限にはいくつかの回避策がありますが、その回避策は等コスト マルチパス ルーティングには適用できません。

（注） スタティック mroute の設定の詳細については、ftp://ftpeng.cisco.com/ipmulticast/config-notes/static-mroutes.txt で Cisco IOS IP マルチキャスト FTP サイトにある『Configuring Multiple Static Mroutes in Cisco IOS』設定ノートを参照してください。

IPv4 マルチキャストでは等コスト マルチパスにスタティック mroute のみを指定できます。しかし、それらのスタティック mroute はマルチキャストにのみ適用できます。または、等コスト マルチパスがユニキャストおよびマルチキャスト ルーティングの両方に適用されるように指定できます。IPv6 マルチキャストでは、このような制限はありません。等コスト マルチパス mroute を、ユニキャスト ルーティングのみ、マルチキャスト ルーティングのみ、またはこの双方に適用するスタティック IPv6 mroute に設定することができます。

IP マルチキャスト トラフィックのロード スプリッティングの代替方法

IP マルチキャスト トラフィックのロード スプリットは、複数のパラレル リンクを単一のトンネルに統合し、マルチキャスト トラフィックがそのトンネルを介してルーティングされるようにすることによっても達成できます。ロード スプリッティングのこの方法は、ECMP マルチキャスト ロード スプリッティングよりも設定が複雑です。GRE リンクを使用した等コスト パスを介したロード スプリットを設定するのが有利である例として、(S, G) ステートまたは (*, G) ステートの合計数が非常に小さく、各ステートによって伝送される帯域幅の変動が大きいため、ソースまたはRPアドレスの手動でのエンジニアリングでさえトラフィックの適切なロード スプリットを保証できない場合が挙げられます。

（注） ECMP マルチキャスト ロード スプリットの可用性があるため、通常は、パケットごとのロード シェアリングが必要な場合にしかトンネルを使用する必要はありません。

IP マルチキャスト トラフィックは、ファストまたはギガビット EtherChannel インターフェイス、MLPPP リンク バンドル、マルチリンク フレーム リレー（FRF.16）バンドルなどのバンドル インターフェイスを介したロード スプリットにも使用できます。GRE またはその他のタイプのトンネルも、このような形態のレイヤ2リンク バンドルを構成できます。このようなレイヤ2メカニズムを使用する場合は、ユニキャストとマルチキャストのトラフィックがどのようにロード スプリットされるかを理解しておく必要があります。

トンネルを介した等コスト パス間で IP マルチキャスト トラフィックをロード スプリットするには、その前に CEF のパケットごとのロード バランシングを設定しておく必要があります。これをしなければ、GRE パケットにパケットごとのロード バランシングが行われません。

ECMP を介して IP マルチキャスト トラフィックをロード スプリットする方法

ECMP マルチキャスト ロード スプリットのイネーブル化

発信元アドレスに基づいて複数の等コスト パス間で IP マルチキャスト トラフィックの負荷を分割するには、次のタスクを実行します。

ソースから 2 つ以上の等コスト パスが使用できる場合は、ユニキャスト トラフィックはそれらのパスの間でロード スプリットされます。一方、マルチキャスト トラフィックは、デフォルトでは、複数の等コスト パスの間でロード スプリットすることはありません。一般に、マルチキャスト トラフィックは、RPF ネイバーから下流に流れます。PIM 仕様によると、複数のネイバーが同じメトリックを持つ場合、このネイバーは最も大きい IP アドレスを持っていなければなりません。

ipmulticastmultipath コマンドでロード スプリッティングを設定すると、システムは、S ハッシュ アルゴリズムを使用して、ソース アドレスに基づいて、複数の等コスト パスの間でマル

チキャスト トラフィックをロード スプリットします。**ipmulticastmultipath** コマンドを設定していて、複数の等コスト パスが存在する場合、マルチキャスト トラフィックを伝送するパスは、ソース IP アドレスに基づいて選択されます。異なる複数のソースからのマルチキャスト トラフィックが、異なる複数の等コスト パスの間でロード スプリットされます。同一ソースから異なる複数のマルチキャスト グループに送信されたマルチキャスト トラフィックについては、複数の等コスト パスの間でロード スプリットは行われません。

（注） **ipmulticastmultipath** コマンドは、トラフィックのロードバランシングではなくロード スプリットを行います。ソースからのトラフィックは、そのトラフィックがその他のソースからのトラフィックよりはるかに多い場合でも、1 つのパスしか使用しません。

IP マルチキャスト ロード スプリットの前提条件：ECMP

- 発信元アドレスに基づいて ECMP マルチキャスト ロード スプリットを有効にするには、十分な数の送信元（少なくとも 3 つの送信元）が必要です。
- ECMP マルチキャスト ロード スプリットを設定するには、RP が使用できる複数のパスが必要です。

（注） 送信元または RP がそれぞれ使用できるパスが複数あることを確認するには、*ip-address* 引数に送信元の IP アドレスまたは RP の IP アドレスを指定して、**showiproute** コマンドを使用します。コマンドの出力に複数のパスが表示されない場合は、ECMP マルチキャスト ロード スプリットを設定することはできません。

- 最短パス ツリー（SPT）フォワーディングで PIM-SM を使用する場合は、すべての (S, G) ステートのフォワーディングに T ビットを設定する必要があります。
- ECMP マルチキャスト ロード スプリットを設定する前に、**showiprpf** コマンドを使用して、ソースが IP マルチキャスト マルチパス機能を利用できるかどうかを確認しておくことをベスト プラクティスとして推奨します。
- BGP は、デフォルトでは複数の等コスト パスをインストールしません。**maximum-paths** コマンドを使用して（たとえば BGP での）マルチパスを設定してください。詳細については、「ECMP マルチキャスト ロード スプリットでの BGP の使用 （821 ページ）」の項を参照してください。

機能制限

- ソースから 2 つ以上の等コスト パスが使用できる場合は、ユニキャスト トラフィックはそれらのパスの間でロードスプリットされます。一方、マルチキャスト トラフィックは、デフォルトでは、複数の等コスト パスの間でロード スプリットすることはありません。一般に、マルチキャスト トラフィックは、RPF ネイバーから下流に流れます。PIM 仕様

によると、複数のネイバーが同じメトリックを持つ場合、このネイバーは最も大きい IP アドレスを持っていなければなりません。

- **ipmulticastmultipath** コマンドは、同一の PIM ネイバー IP アドレスに複数の等コスト パスを介して到達できるような設定はサポートしていません。この状況は、通常、番号付けされていないインターフェイスを使用している場合に発生します。**ipmulticastmultipath** コマンドを設定する場合は、すべてのインターフェイスに異なる IP アドレスを使用してください。
- **ip multicast multipath** コマンドは、トラフィックのロードバランシングではなくロード スプリットを行います。ソースからのトラフィックは、そのトラフィックがその他のソースからのトラフィックよりはるかに多い場合でも、1 つのパスしか使用しません。

ソース アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化

ソース アドレスに基づいたマルチキャスト トラフィックの ECMP マルチキャスト ロード スプリット（S ハッシュ アルゴリズムを使用）をイネーブルにして、ネットワーク上にある複数のパスの利点を活かすには、次の作業を実行します。S ハッシュ アルゴリズムは、ハッシュ値の計算にランダム化を一切使用しないため、予測可能です。ただし、S ハッシュ アルゴリズムは、特定のソースについて、ハッシュが計算されたデバイスに関係なく常に同じハッシュが得られるため、局在化する傾向があります。

（注） 複数の着信インターフェイスからのトラフィックのレシーバになるデバイスで ECMP マルチキャスト ロート スプリットをイネーブルにします。これは、ユニキャスト ルーティングと反対です。ユニキャストの視点からすると、複数の発信インターフェイスに接続されている送信デバイス上でマルチキャストがアクティブになっています。

始める前に

- 発信元アドレスに基づいて ECMP マルチキャスト ロード スプリットを有効にするには、十分な数の送信元（少なくとも 3 つの送信元）が必要です。
- ECMP マルチキャスト ロード スプリットを設定するには、RP が使用できる複数のパスが必要です。

  （注） 送信元または RP がそれぞれ使用できるパスが複数あることを確認するには、*ip-address* 引数に送信元の IP アドレスまたは RP の IP アドレスを指定して、**showiproute** コマンドを使用します。コマンドの出力に複数のパスが表示されない場合は、ECMP マルチキャスト ロード スプリットを設定することはできません。

- 最短パス ツリー（SPT）フォワーディングで PIM-SM を使用する場合は、すべての (S, G) ステートのフォワーディングに T ビットを設定する必要があります。

- ECMP マルチキャスト ロード スプリットを設定する前に、**showiprpf** コマンドを使用して、ソースが IP マルチキャスト マルチパス機能を利用できるかどうかを確認しておくことをベスト プラクティスとして推奨します。
- BGP は、デフォルトでは複数の等コスト パスをインストールしません。**maximum-paths** コマンドを使用して（たとえば BGP での）マルチパスを設定してください。詳細については、「ECMP マルチキャスト ロード スプリットでの BGP の使用 （821 ページ）」の項を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmulticastmultipath** 例： `Device(config)# ip multicast multipath`	S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード スプリットをイネーブルにします。 • このコマンドは RPF ネイバーが選択される方法を変更するため、ループを回避するために、冗長トポロジ内のすべてのデバイスに一貫性を持たせて設定しなければなりません。 • このコマンドは、同一の PIM ネイバー IP アドレスに複数の等コスト パスを介して到達できるような設定はサポートしていません。この状況は、通常、番号付けされていないインターフェイスを使用している場合に発生します。このコマンドが設定されるデバイスでは、各インターフェイスに異なる IP アドレスを使用します。 • このコマンドは、トラフィックのロード バランシングではなくロー

	コマンドまたはアクション	目的
		ド スプリットを行います。ソースからのトラフィックは、そのトラフィックがその他のソースからのトラフィックよりはるかに多い場合でも、1 つのパスしか使用しません。
ステップ 4	冗長トポロジ内のすべてのデバイスで、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**showiprpf** *source-address* [*group-address*] 例： `Device# show ip rpf 10.1.1.2`	（任意）IP マルチキャスト ルーティングが RPF チェックの実行に使用する情報を表示します。 • IP マルチキャスト トラフィックが正常にロード スプリットされるようにするために、このコマンドを使用して RPF 選択を確認します。
ステップ 7	**showiproute** *ip-address* 例： `Device# show ip route 10.1.1.2`	（任意）IP ルーティング テーブルの現在のステータスを表示します。 • このコマンドを使用して、ECMP マルチキャスト ロード スプリットのために、ソースまたは RP までに複数のパスが使用できることを確認します。 • *ip-address* 引数については、ソースまでに複数のパスが使用できることを確認するにはソースの IP アドレスを入力し（最短パス ツリーの場合）、RP までに複数のパスが使用できることを確認するには RP の IP アドレスを入力します（共有ツリーの場合）。

関連トピック

S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード スプリット （813 ページ）

例：ソース アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化（831 ページ）

ソースアドレスおよびグループアドレスに基づくECMPマルチキャストロードスプリットのイネーブル化

ソース アドレスとグループ アドレスに基づいたマルチキャスト トラフィックの ECMP マルチキャスト ロード スプリット（基本 S-G ハッシュ アルゴリズムを使用）をイネーブルにして、ネットワーク上にある複数のパスの利点を活かすには、次の作業を実行します。基本S-Gハッシュ アルゴリズムは、ハッシュ値の計算にランダム化を一切しようしないため、予測可能です。ただし、基本S-Gハッシュアルゴリズムは、特定のソースとグループについて、ハッシュが計算されているデバイスに関係なく常に同じハッシュが得られるため、局在化する傾向があります。

基本S-Gハッシュアルゴリズムは、ECMPマルチキャストロードスプリットに対して、Sハッシュアルゴリズムよりも柔軟なサポートを提供します。ロードスプリットに基本S-Gハッシュアルゴリズムを使用すると、特に、グループに多数のストリームを送信するデバイスや、IPTV サーバや MPEG ビデオ サーバのように多くのチャネルをブロードキャストするデバイスからのマルチキャスト トラフィックを、複数の等コスト パスの間でより効果的にロード スプリットすることが可能になります。

（注） 複数の着信インターフェイスからのトラフィックのレシーバになるデバイスで ECMP マルチキャスト ロート スプリットをイネーブルにします。これは、ユニキャスト ルーティングと反対です。ユニキャストの視点からすると、複数の発信インターフェイスに接続されている送信デバイス上でマルチキャストがアクティブになっています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmulticastmultipath s-g-hash basic** 例：	基本 S-G ハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト

	コマンドまたはアクション	目的
	`Device(config)# ip multicast multipath s-g-hash basic`	ロード スプリットをイネーブルにします。 • このコマンドは RPF ネイバーが選択される方法を変更するため、ループを回避するために、冗長トポロジ内のすべてのデバイスに一貫性を持たせて設定しなければなりません。
ステップ 4	冗長トポロジ内のすべてのデバイスで、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**showiprpf** *source-address* [*group-address*] 例： `Device# show ip rpf 10.1.1.2`	（任意）IP マルチキャスト ルーティングが RPF チェックの実行に使用する情報を表示します。 • IP マルチキャスト トラフィックが正常にロード スプリットされるようにするために、このコマンドを使用して RPF 選択を確認します。
ステップ 7	**showiproute** *ip-address* 例： `Device# show ip route 10.1.1.2`	（任意）IP ルーティング テーブルの現在のステータスを表示します。 • このコマンドを使用して、ECMP マルチキャスト ロード スプリットのために、ソースまたは RP までに複数のパスが使用できることを確認します。 • *ip-address* 引数については、ソースまでに複数のパスが使用できることを確認するにはソースの IP アドレスを入力し（最短パス ツリーの場合）、RP までに複数のパスが使用できることを確認するには RP の IP アドレスを入力します（共有ツリーの場合）。

関連トピック

基本 S-G ハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリット （814 ページ）
ソース アドレスおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化の例 （831 ページ）

ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化

ソース アドレス、グループ アドレス、およびネクスト ホップ アドレスに基づいたマルチキャスト トラフィックの ECMP マルチキャスト ロード スプリット（ネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用）をイネーブルにして、ネットワーク上にある複数のパスの利点を活かすには、次の作業を実行します。ネクスト ホップ ベースの S-G ハッシュ アルゴリズムは、ハッシュ値の計算にランダム化を一切使用しないため、予測可能です。S ハッシュ アルゴリズムや基本 S-G ハッシュ アルゴリズムと違って、ネクスト ホップ ベースの S-G ハッシュ アルゴリズムに使用されるハッシュ メカニズムは、局在化の傾向がありません。

ネクスト ホップ ベースの S-G ハッシュ アルゴリズムは、ECMP マルチキャスト ロード スプリットに対して、S ハッシュ アルゴリズムよりも柔軟なサポートを提供し、局在化の問題をなくします。ECMP マルチキャスト ロード スプリットにネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用すると、グループに多数のストリームを送信するデバイスや、IPTV サーバや MPEG ビデオ サーバのように多くのチャネルをブロードキャストするデバイスからのマルチキャスト トラフィックを、複数の等コスト パスの間でより効果的にロード スプリットすることが可能になります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmulticastmultipath s-g-hashnext-hop-based** 例： `Router(config)# ip multicast multipath s-g-hash next-hop-based`	ネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用した、ソース アドレス、グループ アドレス、およびネクスト ホップ アドレスに基づく ECMP マルチキャスト ロード スプリットをイネーブル化します。

	コマンドまたはアクション	目的
		• このコマンドは RPF ネイバーが選択される方法を変更するため、ループを回避するために、冗長トポロジ内のすべてのルータに一貫性を持たせて設定しなければなりません。 （注） 複数の着信インターフェイスからのトラフィックのレシーバになると想定されるルータ上で、**ip multicast multipath** コマンドをイネーブルにします。これは、ユニキャスト ルーティングと反対です。ユニキャストの視点からすると、複数の発信インターフェイスに接続されている送信ルータ上でマルチキャストがアクティブになっています。
ステップ 4	冗長トポロジ内のすべてのルータについて、ステップ 1 ～ 3 を繰り返します。	--
ステップ 5	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**showiprpf** *source-address* [*group-address*] 例： `Router# show ip rpf 10.1.1.2`	（任意）IP マルチキャスト ルーティングが RPF チェックの実行に使用する情報を表示します。 • IP マルチキャスト トラフィックが正常にロード スプリットされるようにするために、このコマンドを使用して RPF 選択を確認します。
ステップ 7	**showiproute** *ip-address* 例： `Router# show ip route 10.1.1.2`	（任意）IP ルーティング テーブルの現在のステータスを表示します。 • このコマンドを使用して、ECMP マルチキャスト ロード スプリットのために、ソースまたは RP までに複数のパスが使用できることを確認します。

	コマンドまたはアクション	目的
		• *ip-address* 引数については、ソースまでに複数のパスが使用できることを確認するにはソースの IP アドレスを入力し（最短パス ツリーの場合）、RP までに複数のパスが使用できることを確認するには RP の IP アドレスを入力します（共有ツリーの場合）。

関連トピック

ソース グループとネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリッティング （816 ページ）
ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化の例 （832 ページ）

ECMP を介した IP マルチキャスト トラフィックのロード スプリットの設定例

例：ソース アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化

次の例は、S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード スプリットをルータ上でイネーブルにする方法を示します。

```
ip multicast multipath
```

関連トピック

ソース アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 （824 ページ）
S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード スプリット （813 ページ）

ソース アドレスおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化の例

次の例は、基本 S-G ハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリットをルータ上でイネーブルにする方法を示します。

```
ip multicast multipath s-g-hash basic
```

関連トピック

ソース アドレスおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 （827 ページ）
基本 S-G ハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリット （814 ページ）

ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化の例

次の例は、ネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用した、ソース アドレス、グループ アドレス、およびネクスト ホップ アドレスに基づく ECMP マルチキャスト ロード スプリットをルータ上でイネーブルにする方法を示します。

```
ip multicast multipath s-g-hash next-hop-based
```

関連トピック

ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化 （829 ページ）
ソース グループとネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリッティング （816 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

標準および RFC

標準/RFC	Title
RFC 4601	『Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification』

MIB

MIB	MIB のリンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ECMP を介した IP マルチキャスト トラフィックのロード スプリットの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 41 章

IP マルチキャストの最適化：マルチキャスト向け SSM チャネル ベース フィルタリング

- 機能情報の確認 （835 ページ）
- マルチキャスト境界向け SSM チャネル ベース フィルタリングの前提条件 （836 ページ）
- マルチキャスト境界向け SSM チャネル ベース フィルタリング機能について （836 ページ）
- マルチキャスト境界向け SSM チャネル ベース フィルタリングの設定方法 （837 ページ）
- マルチキャスト境界向け SSM チャネル ベース フィルタリングの設定例 （838 ページ）
- その他の参考資料 （840 ページ）
- マルチキャスト境界向け SSM チャネル ベース フィルタリングの機能履歴と情報 （841 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

マルチキャスト境界向け SSM チャネル ベース フィルタリングの前提条件

IP マルチキャストをデバイスで有効にするには、『*IP Multicast: PIM Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。

マルチキャスト境界向け SSM チャネル ベース フィルタリング機能について

マルチキャスト境界のルール

マルチキャスト境界のための SSM チャネルベース フィルタリング機能は、**ip multicast boundary** コマンドを拡張して、コントロール プレーン フィルタリングをサポートします。複数の**ip multicast boundary** コマンドをインターフェイスに適用できます。

次のルールで、**ipmulticastboundary** コマンドは制御されます。

- 1 つのインターフェイスに設定できるのは、**in** および **out** キーワードの一方のインスタンスです。
- **in** および **out** キーワードは、標準アクセス リストまたは拡張アクセス リストに使用できます。
- **filter-autorp** キーワードまたは no キーワードを使用する場合、標準のアクセス リストだけが許可されます。
- コマンドの最大 3 つのインスタンスが 1 つのインターフェイスで許可されます。**in** の 1 つのインスタンス、**out** の 1 つのインスタンス、および **filter-autorp** または no キーワードの 1 つのインスタンスです。
- コマンドの複数のインスタンスを使用すると、フィルタリングは累積的になります。キーワードなしの境界ステートメントが、**in** キーワードが含まれる境界ステートメントと存在する場合、両方のアクセス リストが in 方向に適用され、どちらか一方での一致で十分です。
- コマンドのすべてのインスタンスは、制御トラフィックおよびデータ プレーン トラフィックの両方に適用されます。
- 拡張アクセス リストのプロトコル情報は解析され、一貫性の再利用とフィルタリングが許可されます。アクセス リストがすべてのプロトコルの（S,G）トラフィックをフィルタリングする場合、（S,G）オペレーションは、キーワードについて記述されたすべての条件で拡張アクセス リストによってフィルタリングされます。

関連トピック

マルチキャスト境界の設定 （837 ページ）
トラフィックを許可および拒否するマルチキャスト境界の設定例 （838 ページ）
トラフィックを許可するマルチキャスト境界の設定例 （839 ページ）
トラフィックを拒否するマルチキャスト境界の設定例 （839 ページ）

マルチキャスト境界向け SSM チャネル ベース フィルタリングの利点

- この機能によって、送信元インターフェイスでの入力が可能になります。
- アクセス制御機能は、SSM および Any Source Multicast（ASM）の場合と同じです。

マルチキャスト境界向け SSM チャネル ベース フィルタリングの設定方法

マルチキャスト境界の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipaccess-list** {**standard**|**extended**} *access-list-name* 例： `Device(config)# ip access-list 101`	標準または拡張のアクセス リストを設定します。
ステップ 4	**permit** *protocol* **host** *address* **host** *address* 例： `Device(config-ext-nacl)# permit ip host 181.1.2.201 host 232.1.1.11`	指定された ip ホスト トラフィックを許可します。

	コマンドまたはアクション	目的
ステップ 5	**deny** *protocol* **host** *address* **host** *address* 例： `Device(config-acl-nacl)# deny ip host 181.1.2.203 host 232.1.1.1`	指定されたマルチキャスト ip グループおよび送信元トラフィックを拒否します。
ステップ 6	必要に応じて、ステップ 4 またはステップ 5 を繰り返します。	指定されたホストおよび送信元トラフィックを許可および拒否します。
ステップ 7	**interface** *type* **interface-number** *port-number* 例： `Device(config)# interface gigabitethernet 2/3/0`	インターフェイスコンフィギュレーション モードをイネーブルにします。
ステップ 8	**ipmulticastboundary** *access-list-name* [**in**|**out** | **filter-autorp**] 例： `Device(config-if)# ip multicast boundary acc_grp1 out`	マルチキャスト境界を設定します。 （注） **filter-autorp** キーワードは、拡張アクセス リストをサポートしていません。

関連トピック

マルチキャスト境界のルール （836 ページ）
トラフィックを許可および拒否するマルチキャスト境界の設定例 （838 ページ）
トラフィックを許可するマルチキャスト境界の設定例 （839 ページ）
トラフィックを拒否するマルチキャスト境界の設定例 （839 ページ）

マルチキャスト境界向け SSM チャネル ベース フィルタリングの設定例

トラフィックを許可および拒否するマルチキャスト境界の設定例

次の例では、(181.1.2.201, 232.1.1.1) および (181.1.2.202, 232.1.1.1) への発信トラフィックを許可し、他のすべての (S,G) を拒否します。

```
configure terminal
 ip access-list extended acc_grp1
 permit ip host 0.0.0.0 232.1.1.1 0.0.0.255
 permit ip host 181.1.2.201 host 232.1.1.1
 permit udp host 181.1.2.202 host 232.1.1.1
 permit ip host 181.1.2.202 host 232.1.1.1
```

```
 deny igmp host 181.2.3.303 host 232.1.1.1
 interface gigabitethernet 2/3/0
 ip multicast boundary acc_grp1 out
```

関連トピック

マルチキャスト境界の設定 （837 ページ）
マルチキャスト境界のルール （836 ページ）

トラフィックを許可するマルチキャスト境界の設定例

次の例では、(192.168.2.201, 232.1.1.5) および (192.168.2.202, 232.1.1.5) への発信トラフィックを許可します。

```
configure terminal
ip access-list extended acc_grp6
 permit ip host 0.0.0.0 232.1.1.1 5.0.0.255
 deny udp host 192.168.2.201 host 232.1.1.5
 permit ip host 192.168.2.201 host 232.1.1.5
 deny pim host 192.168.2.201 host 232.1.1.5
 permit ip host 192.168.2.202 host 232.1.1.5
 deny igmp host 192.2.3.303 host 232.1.1.1
interface gigabitethernet 2/3/0
 ip multicast boundary acc_grp6 out
```

関連トピック

マルチキャスト境界の設定 （837 ページ）
マルチキャスト境界のルール （836 ページ）

トラフィックを拒否するマルチキャスト境界の設定例

次に、候補 RP でアナウンスされるグループ範囲を拒否する例を示します。グループ範囲が拒否されるため、pim auto-rp マッピングは作成されません。

```
configure terminal
ip access-list standard acc_grp10
 deny 225.0.0.0 0.255.255.255
 permit any
 access-list extended acc_grp12
 permit pim host 181.1.2.201 host 232.1.1.8
 deny udp host 181.1.2.201 host 232.1.1.8
 permit pim host 181.1.2.203 0.0.0.255 host 227.7.7.7
 permit ip host 0.0.0.0 host 227.7.7.7
 permit ip 181.1.2.203 0.0.0.255 host 227.7.7.7
 permit ip host 181.1.2.201 host 232.1.1.7
ip access-list extended acc_grp13
 deny ip host 181.1.2.201 host 232.1.1.8
 permit ip any any
interface gigabitethernet 2/3/0
 ip multicast boundary acc_grp10 filter-autorp
 ip multicast boundary acc_grp12 out
 ip multicast boundary acc_grp13 in
```

関連トピック

マルチキャスト境界の設定 （837 ページ）

マルチキャスト境界のルール （836 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

MIB

MIB	MIB のリンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

マルチキャスト境界向け SSM チャネル ベース フィルタリングの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 42 章

IP マルチキャストの最適化：PIM デンス モード ステート リフレッシュ

- 機能情報の確認 （843 ページ）
- PIM デンス モード ステート リフレッシュの前提条件 （843 ページ）
- PIM デンス モード ステート リフレッシュの制約事項 （844 ページ）
- PIM デンス モード ステート リフレッシュについて （844 ページ）
- PIM デンス モード ステート リフレッシュの設定方法 （845 ページ）
- PIM デンス モード ステート リフレッシュの設定例 （847 ページ）
- その他の参考資料 （848 ページ）
- PIM デンス モード ステート リフレッシュの機能履歴と情報 （849 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

PIM デンス モード ステート リフレッシュの前提条件

- PIM デンス モード ステート リフレッシュ機能を設定するには、その前にインターフェイス上で PIM デンス モードをイネーブルにしておく必要があります。

PIM デンス モード ステート リフレッシュの制約事項

- PIM デンス モード ネットワーク内のすべてのルータは、ステート リフレッシュ制御メッセージを処理して転送するためには、PIM デンス モード ステート リフレッシュ機能をサポートしているソフトウェア リリースを実行する必要があります。
- ステート リフレッシュ制御メッセージの発信間隔は、同じ LAN 上のすべての PIM ルータで同じである必要があります。具体的には、LAN に直接接続されている各ルータインターフェイスに同じ発信間隔を設定する必要があります。

PIM デンス モード ステート リフレッシュについて

PIM デンス モード ステート リフレッシュの概要

PIM デンス モード ステート リフレッシュ機能は、PIM バージョン 2 マルチキャスト ルーティング アーキテクチャの拡張機能です。

PIM デンス モードは、フラッディング/プルーニング原則で動作するソース ベースのマルチキャスト配信ツリーを構築します。ソースからのマルチキャストパケットは、PIM デンス モード ネットワークのすべてのエリアにフラッディングされます。マルチキャスト グループ メンバまたは PIM ネイバーに直接接続されていない PIM ルータは、マルチキャスト パケットを受信すると、ソース ベースの配信ツリーをバックアップするプルーニング メッセージをパケットのソースに向けて送信します。その結果、後続のマルチキャストパケットは、配信ツリーのプルーニング済みブランチにはフラッディングされません。ところが、PIM デンス モードでのプルーニングされたステートは、およそ 3 分間ごとにタイムアウトし、PIM デンス モード ネットワーク全体が、マルチキャスト パケットとプルーニング メッセージで再フラッディングされます。PIM デンス モード ネットワーク全体の望ましくないトラフィックの再フラッディングは、ネットワーク帯域幅を消費します。

PIM デンス モード ステート リフレッシュ機能は、定期的に制御メッセージをソース ベースの配信ツリーの下流へと転送することにより、PIM デンス モードのプルーニングされたステートをタイムアウトしないように維持します。制御メッセージによって、配信ツリー内の各ルータの発信インターフェイスのプルーニング状態が更新されます。

関連トピック

PIM デンス モード ステート リフレッシュの設定 （845 ページ）
PIM デンス モード ステート リフレッシュ制御メッセージの発信、処理、および転送の例 （847 ページ）
PIM デンス モード ステート リフレッシュ制御メッセージの処理および転送の例 （848 ページ）

PIM デンス モード ステート リフレッシュの利点

PIM デンス モード ステート リフレッシュ機能は、PIM デンス モードでのプルーニングされたステートをタイムアウトしないようにします。これは、PIM デンス モード ネットワークのプルーニングされたブランチへの不要なマルチキャスト トラフィックの再フラッディングを大幅に低減することにより、ネットワーク帯域幅を節約します。また、この機能によって、PIM デンス モード マルチキャスト ネットワーク内の PIM ルータは、デフォルトの 3 分間のステート リフレッシュ タイムアウト期間の前に、トポロジの変更（マルチキャスト グループに参加する送信元またはマルチキャスト グループから脱退した送信元）を認証することができます。

PIM デンス モード ステート リフレッシュの設定方法

PIM デンス モード ステート リフレッシュの設定

PIM デンス モード ステート リフレッシュ機能を有効にするための設定作業はありません。デフォルトでは、PIM デンス モード ステート リフレッシュ機能をサポートする Cisco IOS XE ソフトウェア リリースを実行するすべての PIM ルータが、ステート リフレッシュ制御メッセージを自動的に処理し、転送します。

PIM ルータ上でのステート リフレッシュ制御メッセージの処理と転送をディセーブルにするには、**ip pim state-refresh disable** グローバル コンフィギュレーション コマンドを使用します。無効になっているステート リフレッシュを再度有効にするには、**no ip pim state-refresh disable** グローバル コンフィギュレーション コマンドを使用します。

ステート リフレッシュ制御メッセージの発生はデフォルトで無効になっています。PIM ルータ上の制御メッセージの発生を設定するには、グローバル コンフィギュレーション モードで始めて、次のコマンドを使用します。

コマンド	目的
`Router(config)# interface type number`	インターフェイスを指定し、ルータをインターフェイス コンフィギュレーション モードにします。
`Router(config-if)# ip pim state-refresh origination-interval [interval]`	PIM デンス モード ステート リフレッシュ制御メッセージの発生を設定します。必要に応じて、*interval* 引数を使用して、制御メッセージ間の秒数を設定できます。デフォルト インターバルは 60 秒です。指定できる間隔の範囲は 1 ～ 100 秒です。

関連トピック

PIM デンス モード ステート リフレッシュの概要 （844 ページ）
PIM デンス モード ステート リフレッシュ制御メッセージの発信、処理、および転送の例 （847 ページ）

PIM デンス モード ステート リフレッシュ制御メッセージの処理および転送の例（848 ページ）

PIM デンス モード ステート リフレッシュの設定

PIM デンス モード ステート リフレッシュ機能が正しく設定されているかを確認するには、**show ip pim interface** [*type number*] **detail** および **show ip pim neighbor** [*interface*] コマンドを使用します。次の **show ip pim interface** [*type number*] **detail** コマンドの出力は、ステート リフレッシュ制御メッセージの処理、転送、および発信が有効になっていることを示します。

```
Router# show ip pim interface fastethernet 0/1/0 detail
FastEthernet0/1/0 is up, line protocol is up
  Internet address is 172.16.8.1/24
  Multicast switching:process
  Multicast packets in/out:0/0
  Multicast boundary:not set
  Multicast TTL threshold:0
  PIM:enabled
    PIM version:2, mode:dense
    PIM DR:172.16.8.1 (this system)
    PIM neighbor count:0
    PIM Hello/Query interval:30 seconds
 PIM State-Refresh processing:enabled
 PIM State-Refresh origination:enabled, interval:60 seconds
    PIM NBMA mode:disabled
    PIM ATM multipoint signalling:disabled
    PIM domain border:disabled
  Multicast Tagswitching:disabled
```

次の **show ip pim neighbor** [*interface*] コマンド出力の Mode フィールドに表示されている S は、ネイバーの PIM デンス モード ステート リフレッシュ機能が設定されていることを示します。

```
Router# show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                      Priority/Mode
172.16.5.1        Ethernet1/1        00:09:03/00:01:41 v2    1 / B S
```

PIM DM ステート リフレッシュのモニタリングと維持

以下に、**debug ip pim** 特権 EXEC コマンドをマルチキャスト グループ 239.0.0.1 に設定した後に PIM ルータで送受信される PIM デンス モード ステート リフレッシュ制御メッセージを示します。

```
Router# debug ip pim 239.0.0.1
*Mar  1 00:25:10.416:PIM:Originating refresh message for
(172.16.8.3,239.0.0.1)
*Mar  1 00:25:10.416:PIM:Send SR on GigabitEthernet1/1/0 for (172.16.8.3,239.0.0.1)
TTL=9
```

show ip mroute コマンドが表示する次の出力は、GigabitEthernet インターフェイス 1/0/0 およびマルチキャスト グループ 239.0.0.1 に得られたプルーニング タイマーの変更です。（次の出力は、**debug ip pim** 特権 EXEC コマンドがルータにすでに設定されていると仮定しています）。

show ip mroute コマンドからの最初の出力では、プルーニング タイマーは 00:02:06 と示しています。このデバッグ メッセージは、PIM デンス モード ステート リフレッシュ制御メッセージがイーサネット インターフェイス 1/0 で送受信され、他の PIM デンス モード ステート リフレッシュ ルータが検出されたことを示します。**show ip mroute** コマンドからの 2 番目の出力では、プルーニング タイマーが 00:02:55 にリセットされています。

```
Router# show ip mroute 239.0.0.1
(172.16.8.3, 239.0.0.1), 00:09:50/00:02:06, flags:PT
  Incoming interface:GigabitEthernet1/1/0, RPF nbr 172.16.5.2
  Outgoing interface list:
 GigabitEthernet1/0/0, Prune/Dense, 00:09:43/00:02:06
Router#
*Mar  1 00:32:06.657:PIM:SR on iif from 172.16.5.2 orig 172.16.8.1 for
(172.16.8.3,239.0.0.1)
*Mar  1 00:32:06.661:     flags:prune-indicator
*Mar  1 00:32:06.661:PIM:Cached metric is [0/0]
*Mar  1 00:32:06.661:PIM:Keep RPF nbr 172.16.5.2
*Mar  1 00:32:06.661:PIM:Send SR on Ethernet1/0 for (172.16.8.3,239.0.0.1)
TTL=8
*Mar  1 00:32:06.661:     flags:prune-indicator
Router# show ip mroute 239.0.0.1
(172.16.8.3, 239.0.0.1), 00:10:01/00:02:55, flags:PT
  Incoming interface:GigabitEthernet1/1/0, RPF nbr 172.16.5.2
  Outgoing interface list:
 GigabitEthernet1/0/0, Prune/Dense, 00:09:55/00:02:55
```

PIM デンス モード ステート リフレッシュの設定例

PIM デンス モード ステート リフレッシュ制御メッセージの発信、処理、および転送の例

次に、ファスト イーサネット インターフェイス 0/1/0 で PIM デンス モード ステート リフレッシュ制御メッセージを 60 秒ごとに発信、処理および転送している PIM ルータの例を示します。

```
ip multicast-routing distributed
interface FastEthernet0/1/0
 ip address 172.16.8.1 255.255.255.0
 ip pim state-refresh origination-interval 60
 ip pim dense-mode
```

関連トピック

PIM デンス モード ステート リフレッシュの設定 （845 ページ）
PIM デンス モード ステート リフレッシュの概要 （844 ページ）

PIM デンス モード ステート リフレッシュ制御メッセージの処理および転送の例

次に、ファスト イーサネット インターフェイス 1/1/0 で PIM デンス モード ステート リフレッシュ制御メッセージを処理および転送しているだけの PIM ルータの例を示します。

```
ip multicast-routing
interface FastEthernet1/1/0
 ip address 172.16.7.3 255.255.255.0
 ip pim dense-mode
```

関連トピック

PIM デンス モード ステート リフレッシュの設定 （845 ページ）
PIM デンス モード ステート リフレッシュの概要 （844 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
PIM デンス モード ステート リフレッシュ機能は、PIM バージョン 2 マルチキャスト ルーティング アーキテクチャの拡張機能です。	「Configuring Basic IP Multicast」モジュール
IP マルチキャスト コマンド：コマンド構文の詳細、コマンド モード、デフォルト設定、コマンド履歴、使用に関する注意事項、および例	『*Cisco IOS IP Multicast Command Reference*』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

PIM デンス モード ステート リフレッシュの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 43 章

IP マルチキャストの最適化：IGMP ステート制限

- 機能情報の確認 （851 ページ）
- IGMP ステート制限の前提条件 （851 ページ）
- IGMP ステート制限の制約事項 （852 ページ）
- IGMP ステート制限に関する情報 （852 ページ）
- IGMP ステート制限の設定方法 （853 ページ）
- IGMP ステート制限の設定例 （856 ページ）
- その他の参考資料 （857 ページ）
- IGMP ステート制限の機能履歴と情報 （858 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IGMP ステート制限の前提条件

- IP マルチキャストを有効にして、Protocol Independent Multicast（PIM）インターフェイスを設定するには、『*IP Multicast: PIM Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。

- すべての ACL を設定する必要があります。詳細については、『*Security Configuration Guide: Access Control Lists*』ガイドの「Creating an IP Access List and Applying It to an Interface」モジュールを参照してください。

IGMP ステート制限の制約事項

デバイスごとに 1 つのグローバル制限と、インターフェイスごとに 1 つの制限を設定できます。

IGMP ステート制限に関する情報

IGMP ステート制限

IGMP ステート制限機能を使用すると、IGMP ステート リミッタの設定が可能になり、この設定により、IGMP メンバーシップ レポート（IGMP 加入）により生成される mroute ステートの数がグローバルに、またはインターフェイスごとに制限されます。設定されている制限を超えたメンバーシップ レポートは、IGMP キャッシュに入れられません。この機能により、DoS（サービス拒絶）攻撃を防止したり、すべてのマルチキャスト フローがほぼ同量の帯域幅を使用するネットワーク環境でマルチキャスト CAC メカニズムを提供したりできます。

（注） IGMP ステート リミッタは、IGMP、IGMP v3lite、および URL Rendezvous Directory（URD）メンバーシップ レポートから生じる route ステートの数に、グローバルまたはインターフェイスごとに制限をかけます。

関連トピック

グローバルな IGMP ステート リミッタの設定 （854 ページ）
IGMP ステート リミッタの設定例 （856 ページ）

IGMP ステート制限機能の設計

- グローバル コンフィギュレーション モードで IGMP ステート リミッタを設定すると、キャッシュに格納できる IGMP メンバーシップ レポートの数に対してグローバルな制限を指定できます。
- インターフェイス コンフィギュレーション モードで IGMP ステート リミッタを設定すると、IGMP メンバーシップ レポートの数に対してインターフェイスごとの制限を指定できます。
- ACL を使用すれば、グループまたはチャネルがインターフェイス制限に対してカウントされることがなくなります。標準 ACL または拡張 ACL を指定できます。標準 ACL は、(*, G) ステートがインターフェイスへの制限から除外されるように定義するのに使用できま

す。拡張 ACL は、(S, G) ステートがインターフェイスへの制限から除外されるように定義するのに使用できます。拡張 ACL は、拡張アクセス リストを構成する許可文または拒否文の中でソース アドレスとソース ワイルドカードに 0.0.0.0 を指定することにより（(0, G) とみなされます）インターフェイスへの制限から除外される (*, G) ステートを定義するのにも使用できます。

- デバイスごとに 1 つのグローバル制限と、インターフェイスごとに 1 つの制限を設定できます。

IGMP ステート リミッタのメカニズム

IGMP ステート リミッタのメカニズムは、次のとおりです。

- ルータが特定のグループまたはチャネルに関する IGMP メンバーシップ レポートを受信するたびに、Cisco IOS ソフトウェアは、グローバル IGMP ステート リミッタまたはインターフェイスごとの IGMP ステート リミッタが制限に達したかどうかを確認します。
- グローバル IGMP ステート リミッタだけが設定されていて、その制限に達していない場合は、IGMP メンバーシップ レポートは受け入れられます。設定されている制限に達した場合は、以降の IGMP メンバーシップ レポートは無視され（ドロップされ）、次のいずれかの形式の警告メッセージが生成されます。
  - ```
    %IGMP-6-IGMP_GROUP_LIMIT: IGMP limit exceeded for <group (*, group address)> on
     <interface type number> by host <ip address>
    ```
  - ```
    %IGMP-6-IGMP_CHANNEL_LIMIT: IGMP limit exceeded for <channel (source address,
    group address)> on <interface type number> by host <ip address>
    ```
- インターフェイスごとの IGMP ステート リミッタだけに達した場合、各制限はそれが設定されているインターフェイスに対してだけカウントされます。
- グローバル IGMP ステート リミッタとインターフェイスごとの IGMP ステート リミッタの両方が設定されている場合、インターフェイスごとの IGMP ステート リミッタに設定されている制限も実施されますが、グローバル制限により制約されます。

IGMP ステート制限の設定方法

IGMP ステート リミッタの設定

（注） IGMP ステート リミッタは、IGMP、IGMP v3lite、および URD メンバーシップ レポートから生じる route ステートの数に、グローバルにかまたはインターフェイスごとに制限をかけます。

グローバルな IGMP ステート リミッタの設定

デバイスごとに 1 つのグローバルな IGMP ステート リミッタを設定するには、次の任意作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipigmplimit** *number* 例： `Device(config)# ip igmp limit 150`	IGMP メンバーシップ レポート（IGMP 加入）から生じる mroute ステートの数に対するグローバルな制限を設定します。
ステップ 4	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 5	**showipigmpgroups** 例： `Device# show ip igmp groups`	（任意）デバイスに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。

関連トピック

IGMP ステート制限 （852 ページ）
IGMP ステート リミッタの設定例 （856 ページ）

インターフェイスごとの IGMP ステート リミッタの設定

インターフェイスごとの IGMP ステート リミッタを設定するには、次の任意作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet0/0`	インターフェイス コンフィギュレーション モードを開始します。 • ホストに接続されているインターフェイスを指定します。
ステップ 4	**ipigmplimit** *number* [**except** *access-list*] 例： `Device(config-if)# ip igmp limit 100`	IGMP メンバーシップ レポート（IGMP 加入）の結果として作成される mroute ステートの数に対するインターフェイスごとの制限を設定します。

ステップ 5	次のいずれかを実行します。
	• **exit**
	• **end**
	例：
	`Device(config-if)# exit`
	`Device(config-if)# end`
		• （任意）現在のコンフィギュレーション セッションを終了して、グローバル コンフィギュレーション モードに戻ります。別のインターフェイスでインターフェイスごとのリミッタを設定するには、ステップ 3 および 4 を繰り返します。
		• 現在のコンフィギュレーションセッションを終了して、特権EXECモードに戻ります。

ステップ 6	**showipigmpinterface** [*type number*] 例： `Device# show ip igmp interface`	（任意）インターフェイス上の IGMP のステータスと設定およびマルチキャスト ルーティングに関する情報を表示します。
ステップ 7	**showipigmpgroups** 例： `Device# show ip igmp groups`	（任意）デバイスに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。

IGMP ステート制限の設定例

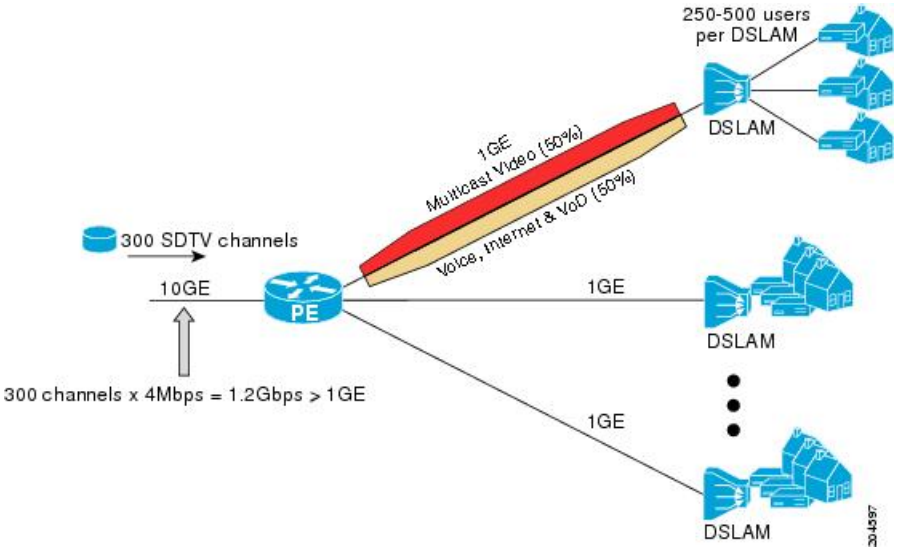
IGMP ステート リミッタの設定例

次の例は、すべてのマルチキャストフローがほぼ同量の帯域幅を使用するネットワーク環境でマルチキャストCACを提供するために、IGMPステートリミッタを設定する方法を示します。

この例では、図に示すトポロジを使用します。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *42 : IGMP* ステート制限のサンプル トポロジ



この例では、サービス プロバイダーは、300 の標準画質（SD）TV チャネルを提供しています。各 SD チャネルが、約 4 Mbps を使用します。

このサービスプロバイダーは、デジタル加入者回線アクセスマルチプレクサ（DSLAM）に接続されているPEルータ上のギガビットイーサネットインターフェイスを、リンクの帯域幅の 50%（500 Mbps）をインターネット、音声、およびビデオ オン デマンド（VoD）サービス提供の加入者が利用できるようにしたうえで、リンクの帯域幅の残りの 50%（500 Mbps）は SD チャネル提供の加入者が利用できるようにプロビジョニングしなければなりません。

各 SD チャネルが同量の帯域幅（4 Mbps）を使用するため、このサービス プロバイダーが提供するサービスのプロビジョニングに必要な CAC は、インターフェイスごとの IGMP ステートリミッタを使用して提供できます。インターフェイスごとに必要な必須CACを調べるために、チャネルの総数を 4 で割ります（各チャネルが 4 Mbps の帯域幅を使用するため）。したがって、インターフェイスごとに必要な必須 CAC は、次のようになります。

500Mbps / 4Mbps = 125 mroute

必須CACがわかったら、サービスプロバイダーは、その結果を使用して、PEルータ上でギガビットイーサネットインターフェイスをプロビジョニングするのに必要なIGMPごとのステートリミッタを設定します。このサービスプロバイダーは、ネットワークのCAC要件に基づいて、ギガビットイーサネットインターフェイスから外部へ転送できるSDチャネルを（常時）125に制限しなければなりません。SDチャネルのプロビジョンのためのインターフェイスごとのIGMPステート制限を125に設定すると、リンクの帯域幅の50%は常にSDチャネルの提供に確保しなければならない（しかし使用が50%を超えてはならない）500 Mbpsの帯域幅にインターフェイスをプロビジョニングできます。

次の設定は、サービス プロバイダーがインターフェイスごとのmrouteステート リミッタを使用して、加入者に提供するSDチャネルとインターネット、音声、およびVoDサービス用にインターフェイス ギガビット イーサネット0/0をプロビジョニングする方法を示します。

```
interface GigabitEthernet0/0/0
description --- Interface towards the DSLAM ---
.
.
.
ip igmp limit 125
```

関連トピック

グローバルな IGMP ステート リミッタの設定 （854 ページ）
IGMP ステート制限 （852 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

MIB

MIB	MIB のリンク
この機能がサポートする新しいMIBまたは変更されたMIBはありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットのMIBを検索してダウンロードするには、次のURLにあるCisco MIB Locatorを使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IGMP ステート制限の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 VIII 部

レイヤ 2/3

- スパニングツリー プロトコルの設定 （861 ページ）
- 複数のスパニング ツリー プロトコルの設定 （893 ページ）
- オプションのスパニングツリー機能の設定 （933 ページ）
- EtherChannel の設定 （959 ページ）
- Resilient Ethernet Protocol の設定 （1005 ページ）
- 単方向リンク検出の設定 （1023 ページ）

第 44 章

スパニングツリー プロトコルの設定

- 機能情報の確認 （861 ページ）
- STP の制約事項 （861 ページ）
- スパニング ツリー プロトコルに関する情報 （862 ページ）
- スパニングツリー機能の設定方法 （876 ページ）
- スパニングツリー ステータスのモニタリング （890 ページ）
- スパニング ツリー プロトコルに関する追加情報 （891 ページ）
- STP の機能情報 （892 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

STP の制約事項

- ルート デバイスとしてデバイスを設定しようとする場合、ルート デバイスにするために必要な値が 1 未満だと、失敗します。
- ネットワークが、拡張システム ID をサポートするデバイスとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするデバイスがルート デバイスになる可能性は低くなります。古いソフトウェアを実行している接続デバイスの優先度より VLAN 番号が大きい場合は常に、拡張システム ID によってデバイス 優先度の値が増加します。

- 各スパニングツリー インスタンスのルート デバイスは、バックボーンまたはディストリビューション デバイスでなければなりません。アクセス デバイスをスパニングツリー プライマリ ルートとして設定しないでください。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

関連トピック

ルート デバイスの設定（CLI） （879 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID （865 ページ）
スパニングツリー トポロジと BPDU （863 ページ）
接続を維持するためのエージング タイムの短縮 （872 ページ）

スパニング ツリー プロトコルに関する情報

スパニングツリー プロトコル

スパニングツリープロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ2リンク管理プロトコルです。レイヤ2イーサネット ネットワークが正常に動作するには、任意の2つのステーション間で存在できるアクティブ パスは1つだけです。エンドステーション間に複数のアクティブパスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着する可能性があります。デバイスは、複数のレイヤ 2 インターフェイスのエンド ステーション MAC アドレスを学習する可能性もあります。このような状況によって、ネットワークが不安定になります。スパニングツリーの動作は透過的であり、エンドステーション側で、単一LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STP は、スパニングツリーアルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のデバイスを1つ選択します。アルゴリズムは、次に基づき、各ポートに役割を割り当て、スイッチド レイヤ 2 ネットワークを介して最良のループフリー パスを算出します。 アクティブ トポロジでのポートの役割：

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているデバイス、またはバックアップの役割が指定されているスイッチはルート デバイスです。 少なくとも *1* つのポートに役割が指定されているデバイスは、指定デバイスを意味します。

冗長データ パスはスパニングツリーによって、強制的にスタンバイ（ブロックされた）ステートにされます。スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パ

スが存在する場合は、スパニングツリー アルゴリズムがスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。デバイスは、スパニングツリーフレーム（ブリッジ プロトコル データ ユニット（BPDU）と呼ばれる）を定期間隔で送受信します。デバイスはこのフレームを転送しませんが、このフレームを使用してループフリーパスを構築します。BPDU には、デバイスおよび MAC アドレス、デバイスの優先順位、ポートの優先順位、およびパス コストを含む、送信側デバイスとそのポートに関する情報が含まれます。スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート デバイスおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

デバイスの 2 つのポートがループの一部である場合、 spanning-tree および、パス コスト設定は、どのポートがフォワーディング ステートになるか、およびどのポートがブロッキング ステートになるかを制御します。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。The コスト値は、メディア速度を表します。

（注） デフォルトではデバイスは、Small Form-Factor Pluggable（SFP）モジュールを備えていないインターフェイスにだけ、（接続が稼働していることを確認するために）キープアライブ メッセージを送信します。[**no**] **keepalive** インターフェイス コンフィギュレーション コマンドをキーワードなしで入力すると、インターフェイスのデフォルトを変更できます。

スパニングツリー トポロジと BPDU

スイッチド ネットワーク内の安定したアクティブ スパニングツリー トポロジは、次の要素によって制御されます。

- デバイス上の各 VLAN に関連付けられた一意のブリッジ ID（デバイス優先度および MAC アドレス）。デバイス スタックでは、ある特定のスパニングツリー インスタンスに対して、すべてのデバイスが同一のブリッジ ID を使用します。
- ルート デバイスに対するスパニングツリー パス コスト。
- 各レイヤ 2 インターフェイスに対応付けられたポート ID（ポート プライオリティおよび MAC アドレス）。

ネットワーク内のデバイスに電源が入ると、各機能はルートデバイスとして機能します。各デバイスは、そのすべてのポートからコンフィギュレーション BPDU を送信します。BPDU によって通信が行われ、スパニングツリートポロジが計算されます。各設定BPDUには、次の情報が含まれています。

- 送信デバイスがルート デバイスとして識別するデバイスの一意のブリッジ ID
- ルートまでのスパニングツリー パス コスト
- 送信デバイスのブリッジ ID
- メッセージ エージ

- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

デバイスは、優位な情報（より小さいブリッジ ID、より低いパス コストなど）が含まれているコンフィギュレーション BPDU を受信すると、そのポートに対する情報を保存します。この BPDU をデバイスのルート ポート上で受信した場合、そのデバイスが指定デバイスとなっているすべての接続 LAN に、更新したメッセージを付けて BPDU を転送します。

デバイスは、そのポートに現在保存されている情報よりも下位の情報を含むコンフィギュレーション BPDU を受信した場合は、その BPDU を廃棄します。デバイスが下位 BPDU を受信した LAN の指定デバイスである場合、そのポートに保存されている最新情報を含む BPDU をその LAN に送信します。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- ネットワーク内の 1 つのデバイスがとして選択されます。ルート デバイス（スイッチドネットワークのスパニングツリー トポロジーの論理的な中心）。箇条書きの項目の下の図を参照してください。

  VLAN ごとに、デバイス優先度が最も高い（最も小さい数字の優先順位の値）デバイスがルート デバイスとして選択されます。すべてのデバイスがデフォルトの優先度（32768）で設定されている場合、VLAN 内で MAC アドレスの最も小さいデバイスがルート デバイスになります。デバイスの優先順位の値は、次の図のようにブリッジ ID の最上位ビットを占めます。

- デバイスごとに（ルートデバイスを除く）、ルート ポートが 1 つ選択されます。このポートは、デバイスからルートデバイスにパケットを転送するときに最適パス（最小コスト）を提供します。

  デバイス スタックのルート ポートを選択する場合には、スパニング ツリーは次の順序に従います。

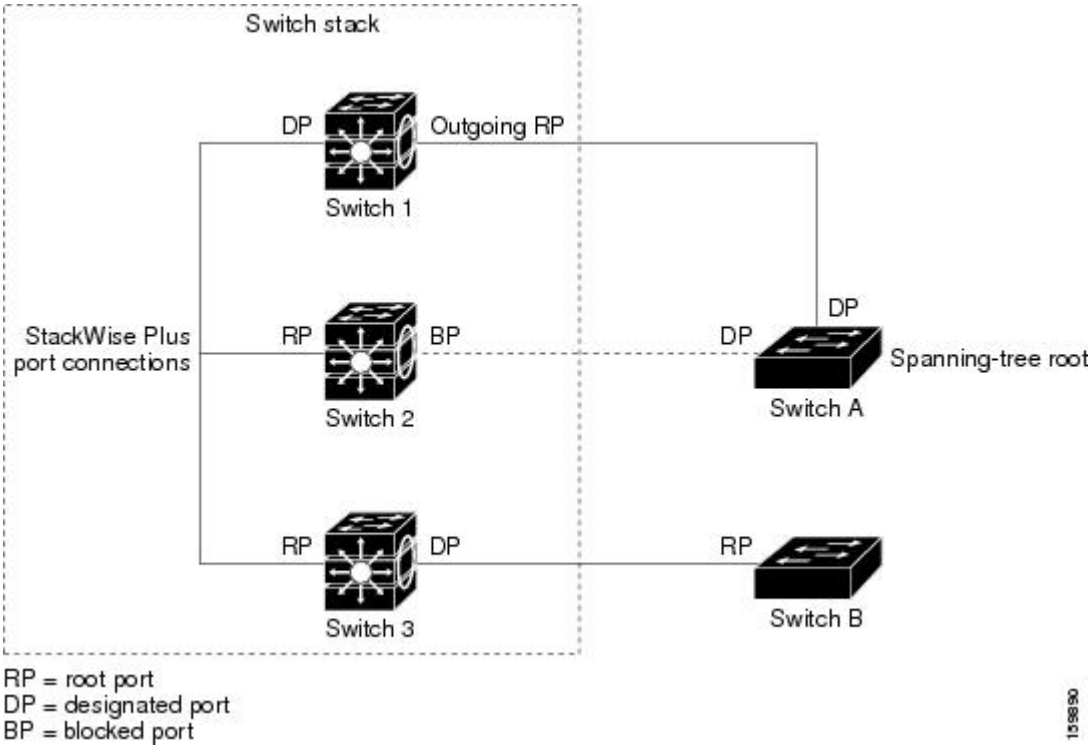
  - 最も低いルート ブリッジ ID を選択
  - ルート デバイスへの最も低いパス コストを選択
  - 最も低い代表ブリッジ ID を選択
  - 最も低い代表パス コストを選択
  - 最も低いポート ID を選択

- スタック ルート デバイス上の 1 つの発信ポートだけが、ルート ポートとして選択されます。スタック内の残りのデバイスは、次の図に示すように指定デバイスになります（デバイス 2 およびデバイス 3）。
- ルート デバイスへの最短距離は、パス コストに基づいてデバイスごとに計算されます。

- LAN セグメントごとに指定デバイスが選択されます。指定デバイスは、その LAN からルート デバイスにパケットを転送するときの最小パス コストを提供します。DP は、指定デバイスが LAN に接続されているポートです。

図 *43*：デバイス スタックのスパニング ツリー ポート ステート

1 つのスタック メンバーがスタック ルート デバイスとして選択されます。スタック ルート デバイスには出力ルート ポート（デバイス 1）が含まれます。



スイッチド ネットワーク上のいずれの地点からもルート デバイスに到達する場合に必要のないパスはすべて、スパニングツリー ブロッキング モードになります。

関連トピック

ルート デバイスの設定（CLI）（879 ページ）
STP の制約事項（861 ページ）

ブリッジ ID、デバイス プライオリティ、および拡張システム ID

IEEE 802.1D 標準では、それぞれのデバイスに固有のルートデバイスの選択を制御するブリッジ識別子（ブリッジ ID）が必要です。各 VLAN は PVST+ と Rapid PVST+ によって異なる論理ブリッジと見なされるので、同一のデバイスは設定された各 VLAN とは異なるブリッジ ID を保有している必要があります。デバイス上の各 VLAN には一意の 8 バイト ブリッジ ID が設定されます。上位の 2 バイトはデバイス プライオリティに使用され、残りの 6 バイトがデバイスの MAC アドレスから取得されます。

デバイスでは IEEE 802.1t スパニングツリー拡張機能がサポートされ、従来はデバイス プライオリティに使用されていたビットの一部が VLAN ID として使用されるようになりました。そ

の結果、デバイスに割り当てられる MAC アドレスが少なくなり、より広い範囲の VLAN ID をサポートできるようになり、しかもブリッジ ID の一意性を損なうこともありません。

従来はデバイス プライオリティに使用されていた 2 バイトが、4 ビットのプライオリティ値と 12 ビットの拡張システム ID 値（VLAN ID と同じ）に割り当てられています。

表 *49*：デバイス プライオリティ値および拡張システム *ID*

プライオリティ値				拡張システム ID（VLAN ID と同設定）											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニングツリーは、ブリッジ ID を VLAN ごとに一意にするために、拡張システム ID、デバイス プライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用します。デバイス スタックは他のネットワークからは単一のデバイスとして認識されるため、スタック内のすべてのデバイスは、指定のスパニングツリーに対して同一のブリッジ ID を使用します。スタック マスターに障害が発生した場合、スタック メンバは新しいスタック マスターの新しい MAC アドレスに基づいて、実行中のすべてのスパニングツリーのブリッジ ID を再計算します。

拡張システム ID のサポートにより、ルート デバイス、セカンダリ ルート デバイス、および VLAN のデバイス プライオリティの手動での設定方法に影響が生じます。たとえば、デバイスのプライオリティ値を変更すると、デバイスがルートデバイスとして選定される可能性も変更されることになります。大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。

指定された VLAN のルート デバイスに 24576 に満たないデバイス プライオリティが設定されている場合は、デバイスはその VLAN について、自身のプライオリティを最小のデバイス プライオリティより 4096 だけ小さい値に設定します4096 は、表に示すように 4 ビット デバイス スイッチ プライオリティ値の最下位ビットの値です。

関連トピック

ルート デバイスの設定（CLI）（879 ページ）
STP の制約事項（861 ページ）
ルート デバイスの設定（CLI）（916 ページ）
ルート スイッチ（897 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI）（913 ページ）

ポート プライオリティとパス コスト

ループが発生した場合、スパニングツリーはポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てることができます。すべてのインターフェイスに

同じプライオリティ値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

スパニングツリー パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、スパニングツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスに同じコスト値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

デバイスがデバイス スタックのメンバーの場合は、最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには（ポートプライオリティを調整せずに）大きいコスト値を与えます。詳細については、関連項目を参照してください。

関連トピック

ポート プライオリティの設定（CLI）（882 ページ）
パス コストの設定（CLI）（883 ページ）

スパニングツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジーの変化が発生します。インターフェイスがスパニングツリートポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成されることがあります。インターフェイスは新しいトポロジ情報がスイッチド LAN 上で伝播されるまで待機し、フレーム転送を開始する必要があります。インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

スパニングツリーを使用しているデバイスの各レイヤ 2 インターフェイスは、次のいずれかのステートになります。

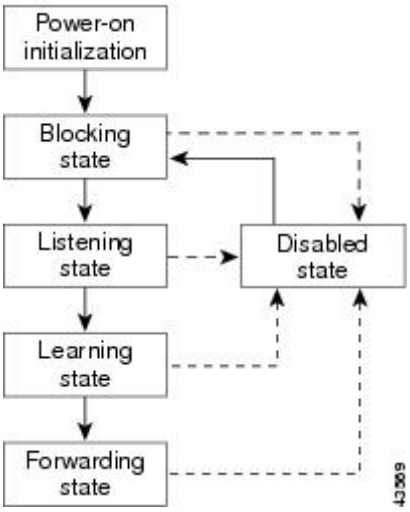
- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：インターフェイスをフレーム転送に関与させることをスパニングツリーが決定した場合、ブロッキング ステートから最初に移行するステートです。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニングツリーに含まれません。シャットダウンポートであるか、ポート上にリンクがないか、またはポート上でスパニングツリーインスタンスが稼働していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル

- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 *44 :* スパニングツリー インターフェイス ステート



インターフェイスはこれらのステート間を移動します。

デフォルト設定では、デバイスを起動するとスパニングツリーが有効になります。その後、デバイスの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。スパニングツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. スパニングツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニング ステートになります。
2. スパニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートの間、デバイスが転送データベースのエンド ステーションの位置情報を学習しているとき、インターフェイスはフレーム転送をブロックし続けます。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ2インターフェイスはフレームの転送に関与しません。初期化後、デバイスの各インターフェイスにBPDUが送信されます。デバイスは最初、他のデバイスとBPDUを交換するまで、ルートとして動作します。この交換により、ネットワーク内でどのデバイスがルートまたはルートデバイスになるかが確立されます。ネットワーク内にデバイス

が1つしかない場合は交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニング ステートになります。インターフェイスはデバイスの初期化後、必ずブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、ブロッキング ステートを経て、レイヤ 2 インターフェイスが最初に移行するステートです。インターフェイスがリスニング ステートになるのは、スパニングツリーによってそのインターフェイスのフレーム転送への関与が決定された場合です。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ2インターフェイスは、フレームの転送に関与できるように準備します。インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ2インターフェイスは、フレームを転送します。インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。

- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ブロッキング ステートのレイヤ2インターフェイスは、フレームの転送やスパニングツリーに関与しません。ディセーブル ステートのインターフェイスは動作不能です。

ディセーブル インターフェイスは、次の機能を実行します。

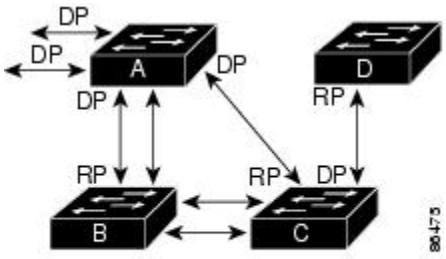
- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

デバイス またはポートがルート デバイスまたはルート ポートになる仕組み

ネットワーク上のすべてのデバイスがデフォルトのスパニングツリー設定で有効になっている場合、最小の MAC アドレスを持つデバイスがルート デバイスになります。

図 *45 :* スパニングツリー トポロジ

デバイス A はルート デバイスとして選択されます。すべてのデバイスのデバイスの優先度がデフォルト（32768）に設定されており、デバイス A の MAC アドレスが最も小さいためです。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、デバイス A が最適なルート デバイスとは限りません。ルート デバイスになるように、最適なデバイスの優先度を引き上げる（数値を引き下げる）と、スパニングツリーの再計算が強制的に行われ、最適なデバイスをルートとした新しいトポロジが形成されます。



RP = Root Port
DP = Designated Port

スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチドネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。たとえば、ルート ポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルート ポートが変更される可能性があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、デバイス B のあるポートがギガビット イーサネット リンクで、デバイス上の別のポート（10/100 リンク）がルート ポートであると仮定します。ネットワーク トラフィックは

ギガビット イーサネット リンクに流す方が効率的です。ギガビット イーサネット ポートのスパニングツリー ポート プライオリティをルート ポートより高くする（数値を小さくする）と、ギガビット イーサネット ポートが新しいルート ポートになります。

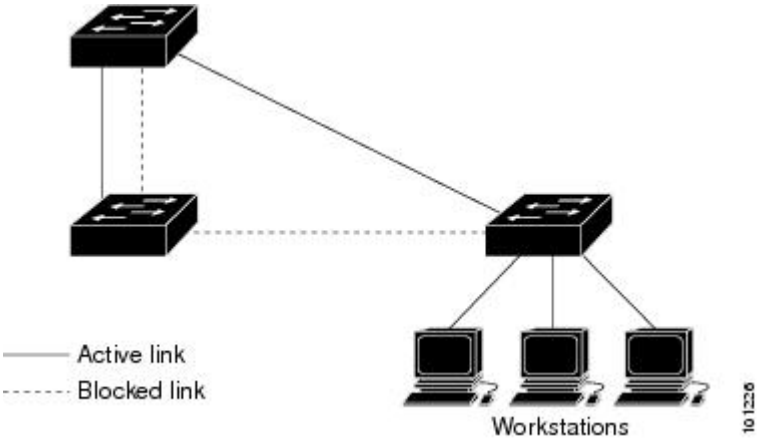
関連トピック

ポート プライオリティの設定（CLI）（882 ページ）

スパニングツリーおよび冗長接続

図 *46 :* スパニングツリーおよび冗長接続

2 つのデバイス インターフェイスを別の 1 台のデバイス、または 2 台の異なるデバイスに接続することにより、スパニングツリーを使用して冗長バックボーンを作成できます。スパニングツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合にはそのディセーブルにしていた方をイネーブルにします。一方のリンクが高速で、他方が低速の場合、必ず、低速の方のリンクがディセーブルになります。速度が同じ場合、ポート優先度とポート ID が加算され、最大値を持つリンクがスパニングツリーによって無効にされます。



EtherChannel グループを使用して、デバイス間に冗長リンクを設定することもできます。

スパニングツリー アドレスの管理

IEEE 802.1D では、各種ブリッジ プロトコルに使用させるために、0x00180C2000000 ～ 0x0180C2000010 の範囲で 17 のマルチキャスト アドレスが規定されています。これらのアドレスは削除できないスタティック アドレスです。

スパニングツリー ステートに関係なく、スタック内の各デバイスは 0x0180C2000000 ～ 0x0180C2000000 のアドレス宛てのパケットを受信しますが、転送は行いません。

スパニングツリーがイネーブルの場合、デバイスまたはスタック内の各デバイスの CPU は 0x0180C2000000 および 0x0180C2000010 宛てのパケットを受信します。スパニングツリーがディセーブルの場合は、デバイスまたはスタック内の各デバイスは、それらのパケットを不明のマルチキャスト アドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミック アドレスのエージング タイムはデフォルトで5分です。これは、**mac address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルトの設定です。ただし、スパニングツリーの再構成により、多数のステーションの位置が変更されることがあります。このようなステーションは、再構成中、5 分以上にわたって到達できないことがあるので、アドレステーブルからステーションアドレスを削除し、改めて学習できるように、アドレスエージング タイムが短縮されます。スパニングツリー再構成時に短縮されるエージング タイムは、転送遅延パラメータ値（**spanning-tree vlan** *vlan-id* **forward-time** *seconds* グローバル コンフィギュレーション コマンド）と同じです。

各 VLAN はそれぞれ独立したスパニングツリー インスタンスであるため、デバイスは VLAN 単位でエージング タイムを短縮します。ある VLAN でスパニングツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスがエージング タイム短縮の対象になります。他の VLAN のダイナミック アドレスは影響を受けず、デバイスで設定されたエージング間隔がそのまま保持されます。

関連トピック

ルート デバイスの設定（CLI）（879 ページ）
STP の制約事項（861 ページ）

スパニングツリー モードおよびプロトコル

このデバイスでサポートされるモードおよびプロトコルは、次のとおりです。

- PVST+：このスパニングツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。PVST+ はデバイス上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリー パスを提供します。

  PVST+ は、対象となる VLAN にレイヤ 2 ロード バランシングを提供します。ネットワーク上の VLAN を使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリンクを使用できるようにします。VLAN 上の PVST+ インスタンスごとに、それぞれ 1 つのルート デバイスがあります。このルート デバイスは、その VLAN に対応するスパニングツリー情報を、ネットワーク上の他のすべてのデバイスに伝送します。このプロセスにより、各デバイスがネットワークに関する共通の情報を持つため、ネットワーク トポロジが確実に維持されます。

- Rapid PVST+：Rapid PVST+ はデバイス上のデフォルトの STP モードです。このスパニングツリー モードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。。高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージング タイムが使用されます。

  Rapid PVST+ は PVST+ と同じ設定を使用しているので（特に明記する場合を除く）、デバイスで必要なことは最小限の追加設定のみです。Rapid PVST+ の利点は、大規模な PVST+ のインストール ベースを Rapid PVST+ に移行する際に、複雑なマルチ スパニングツリー プロトコル（MSTP）設定の学習やネットワーク再設定の必要がないことです。Rapid PVST+ モードでは、各 VLAN は独自のスパニングツリー インスタンスを最大数実行します。

- MSTP：このスパニングツリーモードはIEEE 802.1s標準に準拠しています。複数のVLANを同一のスパニングツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要となるスパニングツリーインスタンスの数を減らすことができます。MSTPはRapid Spanning-Tree Protocol（RSTP）（IEEE 802.1w 準拠）上で実行され、転送遅延を解消し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行することにより、スパニングツリーの高速コンバージェンスを可能にします。デバイス スタックでは、クロススタック高速移行（CSRT）機能が RSTP と同じ機能を実行します。RSTP または CSRT を使用しなければ、MSTP は稼働できません。

関連トピック

スパニングツリー モードの変更（CLI）（876 ページ）

サポートされるスパニングツリー インスタンス

PVST+ または Rapid PVST+ モードでは、デバイスまたはデバイス スタックは最大 128 のスパニングツリー インスタンスをサポートします。

MSTP モードでは、デバイスまたはデバイス スタックは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

関連トピック

スパニング ツリーのディセーブル化（CLI）（878 ページ）
スパニングツリー機能のデフォルト設定（875 ページ）
MSTP のデフォルト設定（913 ページ）

スパニングツリーの相互運用性と下位互換性

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree（CST）のルートは MST バックボーンの内側に配置する必要があり、PVST+ デバイスを複数の MST リージョンに接続することはできません。

ネットワーク内に Rapid PVST+ を実行しているデバイスと PVST+ を実行しているデバイスが存在する場合、Rapid PVST+ デバイスと PVST+ デバイスを別のスパニングツリー インスタンスに設定することを推奨します。Rapid PVST+ スパニングツリー インスタンスでは、ルートデバイスは Rapid PVST+ デバイスでなければなりません。PVST+ インスタンスでは、ルートデバイスは PVST+ デバイスでなければなりません。PVST+ デバイスはネットワークのエッジに配置する必要があります。

すべてのスタック メンバーが、同じバージョンのスパニングツリーを実行します（すべて PVST+、すべて Rapid PVST+、またはすべて MSTP）。

表 *50 : PVST+、MSTP、Rapid PVST+* の相互運用性と互換性

	PVST+	MSTP	Rapid PVST+
PVST+	Yes	あり（制限あり）	あり（PVST+に戻る）
MSTP	あり（制限あり）	Yes	あり（PVST+に戻る）

	PVST+	MSTP	Rapid PVST+
Rapid PVST+	あり（PVST+に戻る）	あり（PVST+に戻る）	Yes

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI） （913 ページ）
MSTP 設定時の注意事項 （896 ページ）
MST リージョン （898 ページ）

STP および IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニングツリー ストラテジに一定の制限を設けています。この規格では、トランク上で使用できるすべての VLAN に対して、1 つのスパニングツリー インスタンスしか認められません。ただし、IEEE 802.1Q トランクを介して接続される Cisco デバイスのネットワークにおいて、デバイスはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。

IEEE 802.1Q トランクを介して Cisco デバイスを他社製のデバイスに接続する場合、Cisco デバイスは PVST+ を使用してスパニングツリーの相互運用性を実現します。Rapid PVST+ がイネーブルの場合、デバイスは PVST+ ではなく Rapid PVST+ を使用します。デバイスは、トランクの IEEE 802.1Q VLAN のスパニングツリー インスタンスと他社の IEEE 802.1Q デバイスのスパニングツリー インスタンスを結合します。

ただし、PVST+ または Rapid PVST+ の情報はすべて、他社製の IEEE 802.1Q デバイスからなるクラウドにより分離された Cisco デバイスによって維持されます。Cisco デバイスを分離する他社製の IEEE 802.1Q クラウドは、デバイス間の単一トランク リンクとして扱われます。

PVST+ は IEEE 802.1Q トランクで自動的に有効になるので、ユーザ側で設定する必要はありません。アクセス ポートおよび ISL（スイッチ間リンク）トランク ポートでの外部スパニングツリーの動作は、PVST+ の影響を受けません。

VLAN ブリッジ スパニングツリー

シスコ VLAN ブリッジ スパニングツリーは、フォールバック ブリッジング機能（ブリッジ グループ）で使用し、DECnet などの IP 以外のプロトコルを 2 つ以上の VLAN ブリッジ ドメインまたはルーテッド ポート間で伝送します。VLAN ブリッジ スパニングツリーにより、ブリッジ グループは個々の VLAN スパニングツリーの上部にスパニングツリーを形成できるので、VLAN 間で複数の接続がある場合に、ループが形成されないようにします。また、ブリッジングされている VLAN からの個々のスパニングツリーが単一のスパニングツリーに縮小しないようにする働きもします。

VLAN ブリッジ スパニングツリーをサポートするには、一部のスパニングツリー タイマーを増やします。フォールバック ブリッジング機能を使用するには、デバイスで IP サービス フィーチャ セットをイネーブルにする必要があります。

スパニング ツリーとデバイス スタック

デバイス スタックが PVST+ または Rapid PVST+ モードで動作している場合：

- デバイス スタックは、ネットワークのその他の部分に対しては単一のスパニングツリーノードに見え、すべてのスタック メンバーが与えられたスパニングツリーに同一のブリッジ ID を使用します。ブリッジ ID は、アクティブ スイッチの MAC アドレスから取得されます。
- 新しいデバイスがスタックに加わると、そのスイッチは、アクティブ スイッチのブリッジ ID を自分のブリッジ ID として設定します。新しく追加されたデバイスの ID が最も小さく、ルート パス コストがすべてのスタック メンバー間で同じ場合は、新しく追加されたデバイスがスタック ルートになります。
- スタック メンバがスタックから除外されると、スタック内でスパニングツリーの再コンバージェンスが発生します（スタック外で発生する場合もあります）。残っているスタック メンバのうち最も低いスタック ポート ID を持つスタック メンバが、スタック ルートになります。
- デバイス スタックがスパニング ツリー ルートで、アクティブ スイッチで障害が発生した、またはスタックから外れた場合、スタンバイ スイッチが新しいアクティブ スイッチになり、ブリッジ ID は同じままで、スパニング ツリーの再コンバージェンスが発生する可能性があります。
- デバイス スタック外にあるネイバー デバイスに障害が発生したか、またはその電源が停止した場合、通常のスパニングツリー処理が発生します。スパニングツリーの再コンバージェンスは、アクティブなトポロジ内のデバイスが失われたことにより発生する場合もあります。
- デバイス スタック外にある新しい デバイスがネットワークに追加された場合、通常のスパニングツリー処理が発生します。スパニングツリーの再コンバージェンスは、ネットワークにデバイスが追加されたことにより発生する場合もあります。

スパニングツリー機能のデフォルト設定

表 *51 :* スパニングツリー機能のデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル
スパニングツリー モード	Rapid PVST+（PVST+ と MSTP はディセーブル）
デバイス priority	32768
スパニングツリー ポート プライオリティ（インターフェイス単位で設定可能）	128

機能	デフォルト設定
スパニングツリー ポート コスト（インターフェイス単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー VLAN ポート プライオリティ（VLAN 単位で設定可能）	128
スパニングツリー VLAN ポート コスト（VLAN 単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー タイマー	hello タイム：2 秒 転送遅延時間：15 秒 最大エージング タイム：20 秒 転送保留カウント：6 BPDU

（注） Cisco IOS Release 15.2(4)E 以降では、デフォルトの STP モードは Rapid PVST+ です。

関連トピック

スパニング ツリーのディセーブル化（CLI） （878 ページ）
サポートされるスパニングツリー インスタンス （873 ページ）

スパニングツリー機能の設定方法

スパニングツリー モードの変更（CLI）

スイッチは次の 3 つのスパニングツリー モードをサポートします。Per-VLAN Spanning-Tree Plus（PVST+）、Rapid PVST+、またはマルチ スパニングツリープロトコル（MSTP）。デフォルトでは、デバイスは Rapid PVST+ プロトコルを実行します。

デフォルト モード以外のモードをイネーブルにする場合、この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**} 例： `Device(config)# spanning-tree mode pvst`	スパニングツリーモードを設定します。すべてのスタック メンバーは、同じバージョンのスパニング ツリーを実行します。 • PVST+ をイネーブルにするには、**pvst** を選択します。 • MSTP をイネーブルにするには、**mst** を選択します。 • **rapid-pvst** を選択して、Rapid PVST+ をイネーブルにします。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。VLAN ID の範囲は 1 ～ 4094 です。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 5	**spanning-tree link-type point-to-point** 例： `Device(config-if)# spanning-tree link-type point-to-point`	このポートのリンク タイプがポイントツーポイントであることを指定します。 このポート（ローカル ポート）をポイントツーポイント リンクでリモート ポートと接続し、ローカル ポートが指定ポートになると、デバイスはリモート ポートとネゴシエーションし、ローカル ポートをフォワーディング ステートにすばやく変更します。
ステップ 6	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# end`	
ステップ 7	**clear spanning-tree detected-protocols** 例： `Device# clear spanning-tree detected-protocols`	デバイス上のいずれかのポートが IEEE 802.1D レガシー デバイス上のポートに接続されている場合は、このコマンドによりデバイス全体のプロトコル移行プロセスを再開します。 このステップは、このデバイスで Rapid PVST+ が稼働していることを指定デバイスが検出する場合のオプションです。

関連トピック

スパニングツリー モードおよびプロトコル （872 ページ）

スパニング ツリーのディセーブル化（CLI）

スパニングツリーはデフォルトで、VLAN 1 およびスパニングツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。スパニングツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。

⚠

注意 スパニングツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**no spanning-tree vlan** *vlan-id* 例： `Device(config)# no spanning-tree vlan 300`	*vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

サポートされるスパニングツリー インスタンス （873 ページ）
スパニングツリー機能のデフォルト設定 （875 ページ）

ルート デバイスの設定（CLI）

特定の VLAN でデバイスをルートとして設定するには、**spanning-tree vlan** *vlan-id***root** グローバル コンフィギュレーション コマンドを使用して、デバイス プライオリティをデフォルト値（32768）から、それより大幅に小さい値に変更します。このコマンドを入力すると、ソフトウェアが各 VLAN について、ルート デバイスのデバイス プライオリティを確認します。拡張システム ID をサポートするため、デバイスは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、このデバイスを指定された VLAN のルートに設定できます。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大デバイス ホップ カウント）を指定するには、**diameter** キーワードを使用します。ネットワーク直径を指定すると、デバイスはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id***root primary** [**diameter** *net-diameter* 例： `Device(config)# spanning-tree vlan 20-24 root primary diameter 4`	指定された VLAN のルートになるように、デバイスを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （オプション）**diameter** *net-diameter* には、任意の 2 つのエンド ステーション間の最大デバイス数を指定します。範囲は 2 ～ 7 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

次のタスク

デバイスをルート デバイスに設定した後に、hello タイム、転送遅延時間、最大エージング タイムを、**spanning-tree vlan** *vlan-id***hello-time**、**spanning-tree vlan** *vlan-id***forward-time**、および **spanning-tree vlan** *vlan-id***max-age** グローバル コンフィギュレーション コマンドを使用して手動で設定することは推奨しません。

関連トピック

ブリッジ ID、デバイス プライオリティ、および拡張システム ID （865 ページ）
スパニングツリー トポロジと BPDU （863 ページ）
接続を維持するためのエージング タイムの短縮 （872 ページ）
STP の制約事項 （861 ページ）

セカンダリ ルート デバイスの設定（CLI）

デバイスをセカンダリ ルートとして設定すると、デバイス プライオリティがデフォルト値（32768）から 28672 に変更されます。このプライオリティでは、デバイスがプライマリ ルートデバイスが失敗した場合の、指定された VLAN のルートデバイスになる可能性があります。

ここでは、その他のネットワーク デバイスが、デフォルトのデバイス プライオリティの 32768 を使用しているためにルート デバイスになる可能性が低いことが前提となっています。

このコマンドを複数のデバイスに対して実行すると、複数のバックアップ ルート デバイスを設定できます。**spanning-tree vlan** *vlan-id***root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート デバイスを設定したときと同じネットワーク直径および hello タイム値を使用してください。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id***root secondary** [**diameter** *net-diameter* 例： `Device(config)# spanning-tree vlan 20-24 root secondary diameter 4`	指定された VLAN のセカンダリ ルートになるように、デバイスを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （オプション）**diameter** *net-diameter* には、任意の 2 つのエンド ステーション間の最大デバイス数を指定します。指定できる範囲は 2 ～ 7 です。 プライマリ ルート デバイスを設定したときと同じネットワーク直径を使用してください。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	

ポート プライオリティの設定（CLI）

（注） デバイスがデバイス スタックのメンバである場合、**spanning-tree** [**vlan** *vlan-id*] **port-priority** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree** [**vlan** *vlan-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させるインターフェイスには、低いコスト値を割り当て、最後に選択させるインターフェイスには高いコスト値を割り当てます。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスは、物理ポートおよびポートチャネル論理インターフェイス（**port-channel** *port-channel-number*）です。
ステップ 4	**spanning-tree port-priority** *priority* 例：	インターフェイスのポート プライオリティを設定します。 *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128

	コマンドまたはアクション	目的
	`Device(config-if)# spanning-tree port-priority 0`	です。有効な値は0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 5	**spanning-treevlan** *vlan-id***port-priority** *priority* 例： `Device(config-if)# spanning-tree vlan 20-25 port-priority 0`	VLAN のポート プライオリティを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一のVLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 • *priority* に指定できる範囲は0～240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

ポート プライオリティとパス コスト （866 ページ）
デバイス またはポートがルート デバイスまたはルート ポートになる仕組み （870ページ）

パス コストの設定（CLI）

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスは、物理ポートおよびポートチャネル論理インターフェイス（**port-channel** *port-channel-number*）です。
ステップ 4	**spanning-tree cost** *cost* 例： `Device(config-if)# spanning-tree cost 250`	インターフェイスのコストを設定します。 ループが発生した場合、スパニングツリーはパスコストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**spanning-tree vlan** *vlan-id***cost** *cost* 例： `Device(config-if)# spanning-tree vlan 10,12-15,20 cost 300`	VLAN のコストを設定します。 ループが発生した場合、スパニングツリーはパスコストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 • *vlan-id* には、VLAN ID 番号で識別された単一のVLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。

	コマンドまたはアクション	目的
		• *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-treeinterface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティとパス コスト （866 ページ）

VLAN のデバイス プライオリティの設定（CLI）

デバイス プライオリティを設定して、スタンドアロン デバイスまたはスタックにあるデバイスがルート デバイスとして選択される可能性を高めることができます。

（注） このコマンドの使用には注意してください。多くの場合、**spanning-tree vlan** *vlan-id***root primary** および **spanning-tree vlan** *vlan-id***root secondary** グローバル コンフィギュレーション コマンドを使用して、デバイスのプライオリティを変更することを推奨します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree vlan** *vlan-id* **priority** *priority* 例： `Device(config)# spanning-tree vlan 20 priority 8192`	VLAN のデバイス プライオリティの設定 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。この値が低いほど、デバイスがルート デバイスとして選択される可能性が高くなります。 有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。その他の値はすべて拒否されます。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

hello タイムの設定（CLI）

hello タイムはルート デバイスによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**spanning-tree vlan** *vlan-id* **hello-time** *seconds* 例： `Device(config)# spanning-tree vlan 20-24 hello-time 3`	VLAN の hello タイムを設定します。hello タイムはルート デバイスによって設定メッセージが生成されて送信される時間の間隔です。このメッセージは、デバイスが活動中であることを表します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

VLAN の転送遅延時間の設定（CLI）

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **forward-time** *seconds* 例：	VLAN の転送時間を設定します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行

	コマンドまたはアクション	目的
	`Device(config)# spanning-tree vlan 20,25 forward-time 18`	するまでに、インターフェイスが待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

VLAN の最大エージング タイムの設定（CLI）

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **max-age** *seconds* 例： `Device(config)# spanning-tree vlan 20 max-age 30`	VLAN の最大エージング タイムを設定します。最大エージング タイムは、デバイスが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。

	コマンドまたはアクション	目的
		• *vlan-id* には、VLAN ID 番号で識別された単一のVLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 • *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

転送保留カウントの設定（CLI）

転送保留カウント値を変更することで、BPDU のバースト サイズを設定できます。

（注） このパラメータをより高い値に変更すると、（特に Rapid PVST+ モードで）CPU の使用率に大きく影響します。逆に、この値を低く設定すると、セッションによってはコンバージェンスを抑えることができます。この値は、デフォルト設定で使用することを推奨します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree transmit hold-count** *value* 例：	1 秒間停止する前に送信できる BPDU 数を設定します。

	コマンドまたはアクション	目的
	`Device(config)# spanning-tree transmit hold-count 6`	*value* に指定できる範囲は 1 ～ 20 です。デフォルト値は 6 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

スパニングツリー ステータスのモニタリング

表 *52*：スパニングツリー ステータス表示用のコマンド

show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree vlan *vlan-id*	指定した VLAN のスパニング ツリー情報を表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree interface *interface-id* **portfast**	指定したインターフェイスのスパニングツリー portfast 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。または STP ステート セクションのすべての行を表示します。

スパニングツリー カウンタをクリアするには、**clear spanning-tree** [**interface** i*nterface-id*] 特権 EXEC コマンドを使用します。

スパニング ツリー プロトコルに関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	*LAN Switching Command Reference, Cisco IOS XE Release 3SE（Catalyst 3850 Switches）*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

STP の機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 45 章

複数のスパニング ツリー プロトコルの設定

- 機能情報の確認 （893 ページ）
- MSTP の前提条件 （893 ページ）
- MSTP の制約事項 （894 ページ）
- MSTP について （895 ページ）
- MSTP 機能の設定方法 （913 ページ）
- MSTP に関する追加情報 （931 ページ）
- MSTP の機能情報 （932 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

MSTP の前提条件

- 2 つ以上のデバイスを同じマルチスパニングツリー（MST）リージョンに設定するには、その 2 つに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。
- 2 つ以上のスタックされたスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

- ネットワーク内の冗長パスでロード バランシングを機能させるには、すべての VLAN/インスタンスマッピングの割り当てが一致している必要があります。一致していないと、すべてのトラフィックが 1 つのリンク上で伝送されます。パス コストを手動で設定することで、デバイス スタック全体にわたりロード バランシングを実現できます。
- Per-VLAN Spanning-Tree Plus（PVST+）と MST クラウドの間、または Rapid- PVST+ と MST クラウドの間でロードバランシングが機能するためには、すべての MST 境界ポートがフォワーディングでなければなりません。MST クラウドの内部スパニングツリー（IST）マスターが共通スパニング ツリー（CST）のルートである場合、MST 境界ポートはフォワーディングです。MST クラウドが複数の MST リージョンから構成されている場合、いずれかの MST リージョンに CST ルートを含める必要があり、その他すべての MST リージョンに、PVST+ クラウドまたは高速 PVST+ クラウドを通るパスよりも、MST クラウド内に含まれるルートへのパスが良くする必要があります。クラウド内のデバイスを手動で設定しなければならない場合もあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI） （913 ページ）
MSTP 設定時の注意事項 （896 ページ）
MST リージョン （898 ページ）

MSTP の制約事項

- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。
- デバイス スタックは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。
- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは 1 つのバージョンだけです（たとえば、すべての VLAN で PVST+ を実行する、すべての VLAN で Rapid PVST+ を実行する、またはすべての VLAN で MSTP を実行します）。
- すべてのスタック メンバーは同一のスパニングツリー バージョンを実行する必要があります（すべての PVST+、Rapid PVST+、または MSTP）。
- MST コンフィギュレーションの VLAN トランキング プロトコル（VTP）伝搬はサポートされません。ただし、コマンドライン インターフェイス（CLI）または簡易ネットワーク管理プロトコル（SNMP）サポートを通じて、MST リージョン内の各デバイスで MST コンフィギュレーション（リージョン名、リビジョン番号、および VLAN とインスタンスのマッピング）を手動で設定することは可能です。
- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。
- リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバーで構成されます。リージョンの各メンバーは高速スパニングツリープロトコル（RSTP）ブリッ

ジ プロトコル データ ユニット（BPDU）を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリー インスタンスの数は 65 までです。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

- デバイスをルートデバイスとして設定した後に、**spanning-tree mst hello-time**、**spanning-tree mst max-age**、および **spanning-tree mst forward-time** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定することは推奨できません。

表 *53 : PVST+*、*MSTP*、*Rapid PVST+* の相互運用性と互換性

	PVST+	MSTP	Rapid PVST+
PVST+	Yes	あり（制限あり）	あり（PVST+に戻る）
MSTP	あり（制限あり）	Yes	あり（PVST+に戻る）
Rapid PVST+	あり（PVST+に戻る）	あり（PVST+に戻る）	Yes

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）（913 ページ）
MSTP 設定時の注意事項（896 ページ）
MST リージョン（898 ページ）
ルート デバイスの設定（CLI）（916 ページ）
ルート スイッチ（897 ページ）

MSTP について

MSTP の設定

高速コンバージェンスのために RSTP を使用する MSTP では、複数の VLAN をグループ化して同じスパニングツリーインスタンスにマッピングすることが可能で、多くの VLAN をサポートするのに必要なスパニングツリー インスタンスの数を軽減できます。MSTP は、データ トラフィックに複数の転送パスを提供し、ロード バランシングを実現して、多数の VLAN をサポートするのに必要なスパニングツリーインスタンスの数を減らすことができます。MSTP を使用すると、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）は影響を受けないので、ネットワークのフォールトトレランスが向上します。

（注） マルチ スパニングツリー（MST）実装は IEEE 802.1s 標準に準拠しています。

MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの導入です。MSTP の導入により、サービス プロバイダー環境に求められる高可用性ネットワークを実現できます。

デバイスが MST モードの場合、IEEE 802.1w 準拠の RSTP が自動的にイネーブルになります。RSTP は、IEEE 802.1D の転送遅延を軽減し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行する明示的なハンドシェイクによって、スパニングツリーの高速コンバージェンスを実現します。

MSTP と RSTP は、既存のシスコ独自の Multiple Instance STP（MISTP）、および既存の Cisco PVST+ と Rapid Per-VLAN Spanning-Tree plux（Rapid PVST+）を使用して、スパニングツリーの動作を改善し、（オリジナルの）IEEE 802.1D スパニング ツリーに準拠した機器との下位互換性を保持しています。

デバイス スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが同一のデバイス ID を使用します。

MSTP 設定時の注意事項

- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して、MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- UplinkFast、BackboneFast、クロススタック UplinkFast の設定のガイドラインについては、関連項目のセクションの該当するセクションを参照してください。
- デバイスが MST モードの場合は、パス コスト値の計算に、ロング パス コスト計算方式（32 ビット）が使用されます。ロング パス コスト計算方式では、次のパス コスト値がサポートされます。

速度	パス コスト値
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）（913 ページ）
MSTP の前提条件（893 ページ）
MSTP の制約事項（894 ページ）
スパニングツリーの相互運用性と下位互換性（873 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast（940 ページ）

UplinkFast （935 ページ）

ルート スイッチ

デバイスは、マッピングされている VLAN グループのスパニングツリー インスタンスを保持しています。デバイス ID は、デバイスのプライオリティおよびデバイスの MAC アドレスで構成されており、各インスタンスに関連付けられます。VLANのグループでは、最小のデバイス ID をもつデバイスがルート デバイスになります。

デバイスをルートとして設定する場合は、デバイス プライオリティをデフォルト値（32768）からそれより大幅に低い値に変更し、デバイスが、指定したスパニング ツリー インスタンスのルート デバイスになるようにします。このコマンドを入力すると、デバイスはルート デバイスのデバイス プライオリティをチェックします。拡張システム ID をサポートしているため、24576 という値でデバイスが指定したスパニングツリー インスタンスのルートとなる場合、そのデバイスは指定したインスタンスに対する自身のプライオリティを 24576 に設定します。

指定されたインスタンスのルート デバイスに 24576 に満たないデバイス プライオリティが設定されている場合は、デバイスは自身のプライオリティを最小のデバイス プライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット デバイス プライオリティの最下位ビットの値です）。詳細については、関連項目の「ブリッジ ID、スイッチ プライオリティ、および拡張システム IDデバイス」リンクを参照してください。

ネットワークが、拡張システム ID をサポートするデバイスとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするデバイスがルート デバイスになる可能性は低くなります。古いソフトウェアを実行している接続デバイスのプライオリティより VLAN 番号が大きい場合は常に、拡張システム ID によってスイッチ プライオリティ値が増加します。

各スパニングツリーインスタンスのルートデバイスは、バックボーンまたはディストリビューション デバイスでなければなりません。アクセス デバイスをスパニングツリー プライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大デバイス ホップ カウント）を指定するには、**diameter** キーワード（MST インスタンスが 0 の場合のみ使用できる）を指定します。ネットワーク直径を指定すると、デバイスはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

関連トピック

ルート デバイスの設定（CLI） （916 ページ）
MSTP の制約事項 （894 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID （865 ページ）

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して矛盾のないようにスイッチを設定する必要があります。同じ MST 設定の相互接続スイッチの集まりによって MST リージョンが構成されます。

MST 設定では、それぞれのデバイスが属する MST リージョンが制御されます。この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。その中で MST リージョンの設定を指定することにより、リージョンのデバイスを設定します。MST インスタンスに VLAN をマッピングし、リージョン名を指定して、リビジョン番号を設定できます。手順と例については、関連項目の「MST リージョン設定の指定と MSTP のイネーブル化」リンクをクリックします。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。さらに、各メンバは、RSTP ブリッジプロトコルデータユニット（BPDU）を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は 65 までです。インスタンスは、0 ～ 4094 の範囲の任意の番号で識別できます。VLAN には、一度に 1 つのスパニングツリーインスタンスのみ割り当てることができます。

関連トピック

MST リージョンの図 （901 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI） （913 ページ）
MSTP の前提条件 （893 ページ）
MSTP の制約事項 （894 ページ）
スパニングツリーの相互運用性と下位互換性 （873 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast （940 ページ）
UplinkFast （935 ページ）

IST、CIST、CST

すべてのスパニングツリー インスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の 2 つのタイプのスパニングツリーを確立して保持しています。

- Internal Spanning-Tree（IST）は、1 つの MST リージョン内で稼働するスパニングツリーです。

  各 MST リージョン内の MSTP は複数のスパニングツリー インスタンスを維持しています。インスタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。その他すべての MSTI には、1 ～ 4094 の番号が付きます。

  IST は、BPDU を送受信する唯一のスパニングツリー インスタンスです。他のスパニングツリーの情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されています。MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニングツリー インスタンスをサポートする処理が必要な BPDU の数を大幅に減少できます。

同一リージョン内のすべてのMSTインスタンスは同じプロトコルタイマーを共有しますが、各MSTインスタンスは独自のトポロジパラメータ（ルートデバイスID、ルートパスコストなど）を持っています。デフォルトでは、すべてのVLANがISTに割り当てられます。

MSTIはリージョンにローカルです。たとえばリージョンAおよびリージョンBが相互接続されていても、リージョンAのMSTI 1は、リージョンBのMSTI 1に依存しません。

- Common and Internal Spanning-Tree（CIST）は、各MSTリージョン内のISTと、MSTリージョンおよびシングルスパニングツリーを相互接続するCommon Spanning-Tree（CST）の集合です。

  1つのリージョン内で計算されたスパニングツリーは、スイッチドドメイン全体を網羅するCSTのサブツリーと見なされます。CISTは、IEEE 802.1w、IEEE 802.1s、およびIEEE 802.1D標準をサポートするスイッチ間で実行されるスパニングツリーアルゴリズムによって形成されます。MSTリージョン内のCISTは、リージョン外のCSTと同じです。

MST リージョン内の動作

ISTは1つのリージョン内のすべてのMSTPスイッチを接続します。ISTが収束すると、ISTのルートは、CISTリージョナルルート（IEEE 802.1s標準が実装される以前は*IST*マスターと呼ばれた）になります。これは、リージョン内で最も小さいデバイスID、およびCISTルートに対するパスコストをもつデバイスです。ネットワークに領域が1つしかない場合、CISTリージョナルルートはCISTルートにもなります。CISTルートがリージョンの外部にある場合、リージョンの境界に位置するMSTPスイッチの1つがCISTリージョナルルートとして選択されます。

MSTPデバイスは初期化時に、自身がCISTのルートおよびCISTリージョナルルートであることを主張するためにCISTルートとCISTリージョナルルートへのパスコストがいずれもゼロに設定されたBPDUを送信します。デバイスはすべてのMSTIを初期化し、そのすべてのルートであることを主張します。デバイスは、ポート用に現在保存されているものより上位のMSTルート情報（低いデバイスID、低いパスコストなど）を受信した場合、CISTリージョナルルートとしての主張を放棄します。

リージョンには、初期化中に多くのサブリージョンが含まれて、それぞれに独自のCISTリージョナルルートが含まれることがあります。スイッチは、優位のIST情報を受信すると、古いサブリージョンを脱退して、真のCISTリージョナルルートが含まれている新しいサブリージョンに加入します。真のCISTリージョナルルートが含まれている以外のサブリージョンは、すべて縮小します。

正常な動作のためには、MSTリージョン内のすべてのスイッチが同じCISTリージョナルルートを承認する必要があります。共通のCISTリージョナルルートに収束する場合、そのリージョン内にある2つのスイッチは、1つのMSTインスタンスに対するポートの役割のみを同期させます。

関連トピック

MST リージョンの図 （901 ページ）

MST リージョン間の動作

ネットワーク内に複数のリージョンまたはレガシー IEEE 802.1D デバイスが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP デバイスから構成される CST を構築して保持します。MSTI は、リージョンの境界にある IST と組み合わさり、CST になります。

IST はリージョン内のすべての MSTP デバイスを接続し、スイッチド ドメイン全体を囲む CIST のサブツリーとして認識されます。サブツリーのルートは CIST リージョナル ルートです。MST リージョンは、隣接する STP デバイスおよび MST リージョンへの仮想デバイスとして認識されます。

CST インスタンスのみが BPDU を送受信し、MST インスタンスはスパニングツリー情報を BPDU に追加して隣接するデバイスと相互作用し、最終的なスパニングツリー トポロジを算出します。したがって、BPDU 伝送に関連するスパニングツリー パラメータ（hello タイム、転送時間、最大エージング タイム、最大ホップ カウントなど）は、CST インスタンスだけで設定されますが、その影響はすべての MST インスタンスに及びます。スパニングツリー トポロジに関連するパラメータ（デバイス プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンスと MST インスタンスの両方で設定できます。

MSTP デバイスは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、レガシー IEEE 802.1D デバイスと通信します。MSTP デバイスは、MSTP BPDU を使用して MSTP デバイスと通信します。

関連トピック

MST リージョンの図 （901 ページ）

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部の MST 命名規則は、一部の内部パラメータまたはリージョンパラメータを識別するように変更されました。これらのパラメータは、ネットワーク全体に関連している外部パラメータと違い、MST リージョン内でのみ影響があります。CIST はネットワーク全体を網羅するスパニングツリー インスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル修飾子ではなく外部修飾子が必要です。

- CIST ルートは、ネットワーク全体を網羅する一意のインスタンスのためのルート デバイスです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。MST リージョンは、CIST への単一デバイスと見なすことに注意してください。CIST 外部ルート パス コストは、これらの仮想デバイス、およびどのリージョンにも属さないデバイスの間で算出されるルート パス コストです。
- CIST リージョナル ルートは、準規格の実装で IST マスターと呼ばれていました。CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。CIST ルートがリージョン内にない場合、CIST リージョナル ルートは、リージョン内の CIST ルートに最も近いデバイスです。CIST リージョナル ルートは、IST のルート デバイスとして動作します。

- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。このコストは、IST つまりインスタンス 0 だけに関連します。

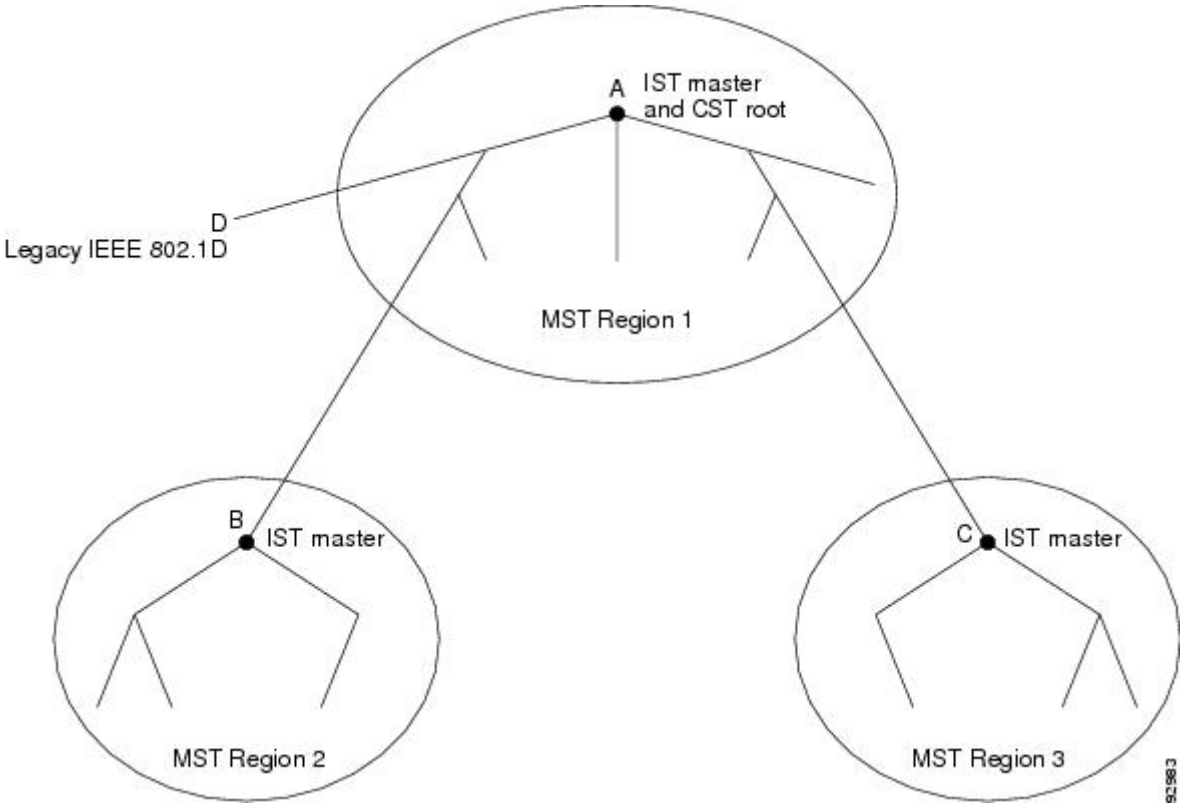
表 *54 :* 準規格と規格の用語

IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

MST リージョンの図

この図は、3 個の MST リージョンとレガシー IEEE 802.1D デバイス（D）を示しています。リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。リージョン 2 の CIST リージョナル ルート（B）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。RSTP はすべてのリージョンで稼働しています。

図 *47 : MST* リージョン、*CIST* マスター、および *CST* ルート



関連トピック

MST リージョン （898 ページ）
MST リージョン内の動作 （899 ページ）
MST リージョン間の動作 （900 ページ）

ホップ カウント

IST および MST インスタンスは、スパニングツリー トポロジの計算に、コンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報を使用しません。その代わりに、IP Time To Live（TTL）メカニズムに似た、ルートまでのパス コストおよびホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することにより、リージョン内の最大ホップを設定し、その値をリージョン内の IST インスタンスとすべての MST インスタンスに適用できます。ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。インスタンスのルート デバイスは、コストが 0 でホップ カウントが最大値に設定されている BPDU（M レコード）を常に送信します。デバイスは、この BPDU を受信すると、受信した残りのホップ カウントから 1 を引き、生成する BPDU で残りのホップ カウントとしてこの値を伝播します。カウントがゼロに達すると、デバイスは BPDU を廃棄し、ポート用に維持されている情報を期限切れにします。

BPDU の RSTP 部分に格納されているメッセージ有効期間と最大エージング タイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTP が稼働する単一のスパニングツリー リージョン、PVST+ または Rapid PVST+ が稼働する単一のスパニングツリー リージョン、または異なる MST コンフィギュレーションを持つ別の MST リージョンに MST リージョンを接続します。境界ポートは、LAN、単一のスパニングツリー デバイスまたは MST 設定が異なるデバイスの指定デバイスにも接続します。

IEEE 802.1s 標準では、境界ポートの定義はなくなりました。IEEE 802.1Q-2002 標準では、ポートが受信できる 2 種類のメッセージを識別します。

- 内部（同一リージョンから）
- 外部（別のリージョンから）

メッセージが内部の場合、CIST の部分は CIST によって受信されるので、各 MST インスタンスは個々の M レコードだけを受信します。

メッセージが外部である場合、CIST だけが受信します。CIST の役割がルートや代替ルートの場合、または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。

MST リージョンには、デバイスおよび LAN の両方が含まれます。セグメントは、DP のリージョンに属します。そのため、セグメントの指定ポートではなく異なるリージョンにあるポートは境界ポートになります。この定義では、リージョン内部の 2 つのポートが、別のリージョンに属するポートとセグメントを共有し、内部メッセージおよび外部メッセージの両方を 1 つのポートで受信できるようになります。

シスコ先行標準の実装との主な違いは、STP 互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。

（注） レガシー STP デバイスがセグメントに存在する場合、メッセージは常に外部と見なされます。

シスコ先行標準の実装から他に変更された点は、送信デバイス ID を持つ RSTP またはレガシー IEEE 802.1Q デバイスの部分に、CIST リージョナル ルート デバイス ID フィールドが加えられたことです。リージョン全体は、一貫した送信者デバイス ID をネイバー デバイスに送信し、単一仮想デバイスのように動作します。この例では、A または B がセグメントに指定されているかどうかに関係なく、ルートの一貫した送信者デバイス ID が同じである BPDU をデバイス C が受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標準には含まれていない一部の（要望されている）先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的に MST 標準に含まれませんでしたが、境界の概念自体はシスコの実装に投影されています。ただし、リージョン境界にある MST インスタンスのポートは、対応する CIST ポートのステートに必ずしも従うわけではありません。現在、2 つの境界の役割が存在しています。

- 境界ポートが CIST リージョナル ルートのルート ポートである場合：CIST インスタンスポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わった後であれば（その後フォワーディングします）、その場合のみ合意を返信してフォワーディング ステートに移行できます。MSTI ポートには、特別なマスターの役割があります。
- 境界ポートが CIST リージョナル ルートのルート ポートでない：MSTI ポートは、CIST ポートのステートおよび役割に従います。標準では提供される情報が少ないため、MSTI ポートが BPDU（M レコード）を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかりにくい場合があります。この場合、境界の役割自体は存在していませんが、**show** コマンドで見ると、出力される *type* カラムで、ポートが境界ポートとして認識されていることがわかります。

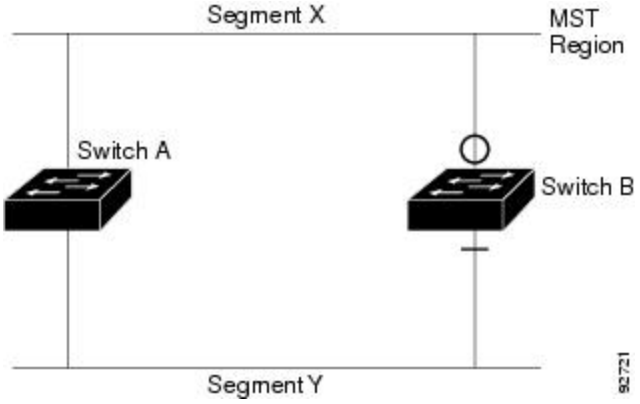
レガシーおよび規格デバイスの相互運用

準規格デバイスの自動検出はエラーになることがあるので、インターフェイス コンフィギュレーション コマンドを使用して準規格ポートを識別できます。デバイスの規格と準規格の間にリージョンを形成することはできませんが、CIST を使用して相互運用することができます。このような特別な方法を採用しても、失われる機能は、異なるインスタンス上のロードバランシングだけです。ポートが先行標準の BPDU を受信すると、CLI（コマンドライン インターフェイス）にはポートの設定に応じて異なるフラグが表示されます。デバイスが準規格BPDU送信用に設定されていないポートで準規格BPDUを初めて受信したときは、Syslogメッセージも表示されます。

図 *48*：規格および準規格のデバイスの相互運用

A が規格のデバイスで、B が準規格のデバイスとして、両方とも同じリージョンに設定されているとします。A はCIST のルートデバイスです。B のセグメント X にはルート ポート（BX）、セグメント Y には代替ポート（BY）があります。セグメント Y がフラップして BY のポートが代替になってから準規格 BPDU を 1 つ送信すると、AY は準規格デバイスが Y に接続されていることを検出できず、規格 BPDU の送信を続けます。ポート BY は境界に固定され、A と B との間でのロードランシングは不可能になります。セグメント X にも同じ問題がありますが、

B はトポロジの変更であれば送信する場合があります。



（注） 規格 MST 実装と準規格 MST 実装間の相互作用を最低限に抑えることを推奨します。

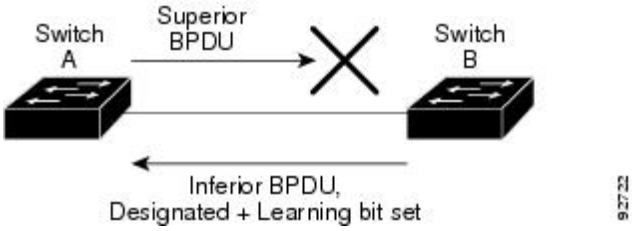
単一方向リンク障害の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

指定ポートは、矛盾を検出すると、その役割を維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジング ループを解決できるからです。

図 *49 :* 単一方向リンク障害の検出

次の図に、ブリッジング ループの一般的な原因となる単方向リンク障害を示します。デバイス A はルート デバイスであり、デバイス B へのリンクで BPDU は失われます。RSTP および MST BPDU には、送信側ポートの役割とステートが含まれます。デバイス A はこの情報を使用し、ルータ A が送信する上位 BPDU にデバイス B が反応しないこと、およびデバイス B がルート デバイスではなく指定ブリッジであることを検出できます。この結果、デバイス A は、そのポートをブロックし（またはブロックし続け）、ブリッジング ループが防止されます。



MSTP およびデバイス スタック

デバイス スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが与えられたスパニングツリーに同一のブリッジ ID を使用します。ブリッジ ID は、アクティブ スイッチの MAC アドレスから取得されます。

スタックがネットワークのルートで、スタック内でルートの選択が行われていない場合は、アクティブ スイッチがスタック ルートになります。

デバイス スタックがスパニング ツリー ルートで、アクティブ スイッチで障害が発生した、またはスタックから外れた場合、スタンバイ スイッチが新しいアクティブ スイッチになり、ブリッジ ID は同じままで、スパニング ツリーの再コンバージェンスが発生する可能性があります。

MSTP をサポートしていないデバイスが、MSTP またはリバースをサポートしているデバイス スタックに追加されると、デバイスはバージョンが不一致の状態になります。可能な場合、デバイスは、デバイス スタックで実行中のソフトウェアと同じバージョンに自動的にアップグレードまたはダウングレードされます。

IEEE 802.1D STP との相互運用性

MSTP が稼働しているデバイスは、IEEE 802.1D 準拠のレガシー デバイスとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このデバイスは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP デバイスは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、デバイスが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシー デバイスが指定デバイスでない限り、レガシー デバイスがリンクから削除されたかどうか検出できないためです。このデバイスが接続するデバイスがリージョンに加入していると、デバイスはポートに境界の役割を割り当て続ける場合があります。プロトコル移行プロセスを再開するには（強制的にネイバーデバイスと再びネゴシエーションするには）、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシーデバイスが RSTP デバイスであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。したがって、MSTP デバイスは、バージョン 0 コンフィギュレーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで送信します。境界ポートは、LAN、単一スパニングツリー デバイスまたは MST 設定が異なるデバイスのいずれかの指定のデバイスに接続します。

RSTP 概要

RSTP は、ポイントツーポイントの配線を利用して、スパニングツリーの高速コンバージェンスを実現します。また、1 秒未満の間に、スパニングツリーを再構成できます（IEEE 802.1D スパニングツリーのデフォルトに設定されている 50 秒とは異なります）。

ポートの役割およびアクティブ トポロジ

RSTP は、ポートに役割を割り当てて、アクティブ トポロジを学習することによって高速コンバージェンスを実現します。RSTP は デバイス をルート デバイスとして最も高いデバイス プライオリティ（プライオリティの数値が一番小さい）に選択するために、IEEE 802.1D STP 上

に構築されます。RSTP は、次のうちいずれかのポートの役割をそれぞれのポートに割り当てます。

- ルート ポート：デバイス がルートデバイス にパケットを転送するとき、最適なパス（最低コスト）を提供します。
- 指定ポート：指定デバイスに接続し、その LAN からルート デバイスにパケットを転送するとき、パス コストを最低にします。DP は、指定デバイスが LAN に接続されているポートです。
- 代替ポート：現在のルート ポートが提供したパスに代わるルート デバイスへの代替パスを提供します。
- バックアップ ポート：指定ポートが提供した、スパニングツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートは、2 つのポートがループバック内でポイントツーポイント リンクによって接続されるか、共有 LAN セグメントとの複数の接続がデバイスにある場合に限って存在できます。
- ディセーブル ポート：スパニングツリーの動作において何も役割が与えられていません。

ルート ポートまたは指定ポートのロールを持つポートは、アクティブなトポロジに含まれます。代替ポートまたはバックアップ ポートのロールがあるポートは、アクティブ トポロジから除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTP は、すべてのルート ポートおよび指定ポートがただちにフォワーディング ステートに移行し、代替ポートとバックアップ ポートが必ず廃棄ステート（IEEE 802.1D のブロッキング ステートと同じ）になるように保証します。ポートのステートにより、転送処理および学習処理の動作が制御されます。

表 *55 :* ポート ステートの比較

Operational Status	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	Blocking	廃棄	いいえ
イネーブル	リスニング	廃棄	いいえ
イネーブル	ラーニング	ラーニング	Yes
イネーブル	Forwarding	Forwarding	Yes
ディセーブル	ディセーブル	廃棄	いいえ

Cisco STP の実装との一貫性を保つため、このマニュアルでは、ポート ステートを廃棄ではなくブロッキングとして定義します。DP はリスニング ステートから開始します。

高速コンバージェンス

RSTPは、デバイス、デバイスポート、LANのうちいずれかの障害のあと、接続の高速回復を提供します。エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- エッジ ポート：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して RSTP デバイスでエッジ ポートとしてポートを設定した場合、エッジ ポートはフォワーディング ステートにすぐに移行します。エッジ ポートは Port Fast 対応ポートと同じであり、単一エンドステーションに接続しているポートだけでイネーブルにする必要があります。
- ルート ポート：RSTP は、新しいルート ポートを選択した場合、古いルート ポートをブロックし、新しいルート ポートをフォワーディング ステートにすぐに移行します。
- ポイントツーポイント リンク：ポイントツーポイント リンクによってあるポートと別のポートを接続することでローカルポートが指定ポートになると、提案合意ハンドシェイクを使用して他のポートと急速な移行がネゴシエートされ、トポロジにループがなくなります。

図 *50*：高速コンバージェンスの提案と合意のハンドシェイク

デバイス A がデバイス B にポイントツーポイント リンクで接続され、すべてのポートはブロッキング ステートになっています。デバイス A の優先度がデバイス B の優先度よりも数値的に小さいとします。デバイス A は提案メッセージ（提案フラグを設定した設定 BPDU）をデバイス B に送信し、指定デバイスとしてそれ自体を提案します。

デバイスBは、提案メッセージの受信後、提案メッセージを受信したポートを新しいルート ポートとして選択し、エッジ以外のすべてのポートを強制的にブロッキング ステートにして、新しいルートポートを介して合意メッセージ（合意フラグを設定したBPDU）を送信します。

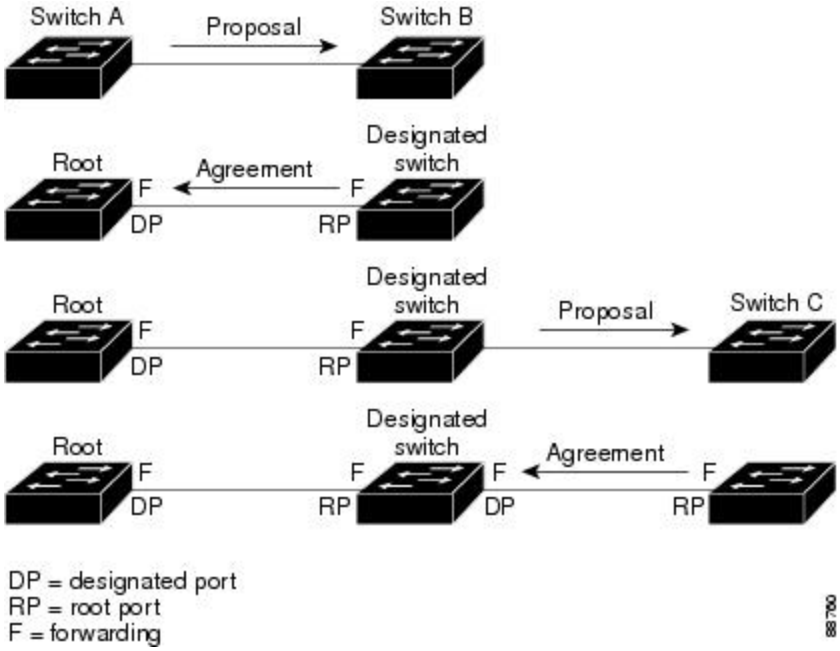
デバイス A も、デバイス B の合意メッセージの受信後、指定ポートをフォワーディング ステートにすぐに移行します。デバイスBはすべてのエッジ以外のポートをブロックし、デバイス A およびルータ B の間にポイントツーポイント リンクがあるので、ネットワークにループは形成されません。

デバイス C がデバイス B に接続すると、同様のセットのハンドシェーク メッセージが交換されます。デバイス C はデバイス B に接続されているポートをルート ポートとして選択し、両端がフォワーディングステートにすぐに移行します。このハンドシェーク処理を繰り返して、もう1つのデバイスがアクティブ トポロジーに加わります。ネットワークが収束すると、この提案/合意ハンドシェイクがルートからスパニングツリーのリーフへと進みます。

デバイス スタックでは、Cross-Stack Rapid Transition（CSRT）機能を使用すると、ポートがフォワーディング ステートに移行する前に、スタック メンバで、提案/合意ハンドシェイク中にすべてのスタック メンバーから確認メッセージを受信できます。デバイスがMSTモードの場合、CSRT は自動的に有効にされます。

デバイスはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。

spanning-tree link-type インターフェイス コンフィギュレーション コマンドを使用すると、デュプレックス設定によって制御されるデフォルト設定を無効にすることができます。



ポート ロールの同期

デバイスがそのルータのポートの 1 つで提案メッセージを受信し、そのポートが新しいルートポートとして選択されると、RSTP によってその他すべてのポートが新しいルートの情報と強制的に同期化します。

その他すべてのポートが同期化されている場合、デバイスはルート ポートで受信した上位ルート情報で同期化されます。デバイスのそれぞれのポートは、次のような場合に同期化します。

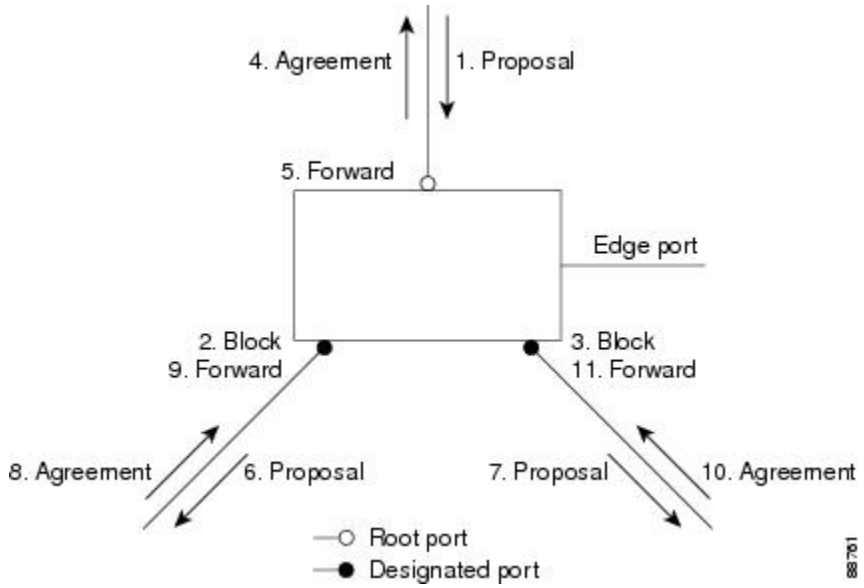
- ポートがブロッキング ステートである。
- エッジ ポートである（ネットワークのエッジに存在するように設定されたポート）。

指定ポートがフォワーディング ステートでエッジ ポートとして設定されていない場合、RSTP によって新しいルート情報と強制的に同期されると、その指定ポートはブロッキング ステートに移行します。一般的に RSTP がルート情報でポートを強制的に同期化し、ポートが上の条件を満たしていない場合、そのポート ステートはブロッキングに設定されます。

図 *51* : 高速コンバージェンス中のイベントのシーケンス

デバイスは、すべてのポートが同期化されたことを確認した後で、ルート ポートに対応する指定デバイスに合意メッセージを送信します。ポイントツーポイント リンクで接続されたデバイ

スがポートの役割で合意すると、RSTP はポート ステートをフォワーディングにすぐに移行します。



ブリッジ プロトコル データ ユニットの形式および処理

RSTP BPDU のフォーマットは、プロトコル バージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報がないことを示しています。

表 *56 : RSTP BPDU* フラグ

ビット	機能
0	トポロジーの変化（TC）
1	提案
2 ～ 3: 00 01 10 11	ポートの役割： 不明（Unknown） Alternate port Root port Designated port
4	ラーニング
5	Forwarding
6	合意
7	トポロジー変更確認応答（TCA）

送信側デバイスはRSTP BPDUの提案フラグを設定し、そのLANの指定デバイスとして自分自身を提案します。提案メッセージのポートの役割は、常に DP に設定されます。

送信側デバイスは、RSTP BPDUの合意フラグを設定して以前の提案を受け入れます。合意メッセージ内のポート ロールは、常にルート ポートに設定されます。

RSTPには個別のトポロジ変更通知（TCN）BPDUはありません。TCフラグが使用されて、TCが示されます。ただし、IEEE 802.1D デバイスとの相互運用性を保つために、RSTP デバイスは TCN BPDU の処理と生成を行います。

ラーニング フラグおよびフォワーディング フラグは、送信側ポートのステートに従って設定されます。

優位 BPDU 情報の処理

ポートに現在保存されているルート情報よりも優位のルート情報（小さいデバイス ID、低いパス コストなど）をポートが受け取ると、RSTP は再構成を開始します。ポートが新しいルート ポートとして提案されて選択されると、RSTP は強制的にその他すべてのポートを同期化します。

受信した BPDU が、提案フラグが設定されている RSTP BPDU である場合、デバイスはその他すべてのポートが同期化されてから合意メッセージを送信します。BPDU が IEEE 802.1D BPDU の場合、デバイスは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。新しいルート ポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

ポートで優位の情報が受信されたために、そのポートがバックアップ ポートまたは代替ポートになる場合、RSTP はそのポートをブロッキング ステートに設定し、合意メッセージは送信しません。DP は、転送遅延タイマーが失効するまで、提案フラグを設定して BPDU を送信し続け、転送遅延タイマーの失効時に、ポートはフォワーディング ステートに移行します。

下位 BPDU 情報の処理

指定ポートの役割を持つ下位BPDU（そのポートに現在保存されている値より大きいデバイス ID 、高いパス コストなど）を指定ポートが受信した場合、その指定ポートはただちに現在の自身の情報で応答します。

トポロジの変更

ここでは、スパニングツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出：IEEE 802.1D では、どのようなブロッキング ステートとフォワーディング ステートとの間の移行でもトポロジの変更が発生しますが、RSTP でトポロジの変更が発生するのは、ブロッキング ステートからフォワーディング ステートに移行する場合だけです（トポロジの変更と見なされるのは、接続数が増加する場合だけです）。エッジポートにおけるステート変更は、TC の原因になりません。RSTP デバイスは、TC を検出すると、TCN を受信したポートを除く、エッジ以外のすべてのポートで学習した情報を削除します。

- 通知：IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。ただし、IEEE 802.1D との相互運用性を保つために、RSTP デバイスは TCN BPDU の処理と生成を行います。
- 確認：RSTP デバイスは、指定ポートで IEEE 802.1D デバイスから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D デバイスに接続されたルート ポートで TC 時間タイマー（IEEE 802.1D のトポロジ変更タイマーと同じ）がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

  この処理は、IEEE 802.1D デバイスをサポートする目的でのみ必要とされます。RSTP BPDU は TCA ビットが設定されていません。
- 伝播：RSTP デバイスは、DP またはルート ポートを介して別のデバイスから TC メッセージを受信すると、エッジ以外のすべての DP、およびルート ポート（TC メッセージを受信したポートを除く）に変更を伝播します。デバイスはこのようなすべてのポートで TC-while タイマーを開始し、そのポートで学習した情報を消去します。
- プロトコルの移行：IEEE 802.1D デバイスとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU が送信される最低時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブである間、デバイスはそのポートで受信したすべての BPDU を処理し、プロトコルタイプを無視します。

  デバイスはポートの移行遅延タイマーが満了した後に IEEE 802.1D BPDU を受信した場合、IEEE 802.1D デバイスに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。ただし、RSTP デバイスが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了した後に RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用が開始されます。

プロトコル移行プロセス

MSTP が稼働しているデバイスは、IEEE 802.1D 準拠のレガシー デバイスとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このデバイスは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MST デバイスは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、デバイスが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシー デバイスが指定デバイスでない限り、レガシー デバイスがリンクから削除されたかどうか検出できないためです。また、接続するデバイスがリージョンに加入していると、デバイスはポートに境界の役割を割り当て続ける場合があります。

関連トピック

プロトコルの移行プロセスの再開（CLI）（930 ページ）

MSTP のデフォルト設定

表 *57 : MSTP* のデフォルト設定

機能	デフォルト設定
スパニングツリー モード	MSTP
デバイス プライオリティ（CIST ポートごとに設定可能）	32768
スパニングツリー ポート プライオリティ（CIST ポート単位で設定可能）	128
スパニングツリー ポート コスト（CIST ポート単位で設定可能）	1000 Mb/s：20000 100 Mb/s：20000 10 Mb/s：20000 1000 Mb/s：20000 100 Mb/s：20000 10 Mb/s：20000
hello タイム	3 秒
転送遅延時間	20 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

関連トピック

サポートされるスパニングツリー インスタンス（873 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI）（913 ページ）

MSTP 機能の設定方法

MST リージョン設定の指定と MSTP のイネーブル化（CLI）

2 つ以上のスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

リージョンには、MST設定が同一である、1つ以上のメンバーを含めることができます。各メンバーでは、RSTP BPDU を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は 65 までです。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst configuration** 例： `Device(config)# spanning-tree mst configuration`	MST コンフィギュレーション モードを開始します。
ステップ 4	**instance** *instance-id* **vlan** *vlan-range* 例： `Device(config-mst)# instance 1 vlan 10-20`	VLAN を MSTI にマップします。 • *instance-id* に指定できる範囲は、0 ～ 4094 です。 • vlan**vlan**に指定できる範囲は、1 ～ 4094 です。 VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN の範囲を指定するには、ハイフンを使用します。たとえば **instance 1 vlan 1-63** では、VLAN 1 ～ 63 が MST インスタンス 1 にマップされます。 一連の VLAN を指定するには、カンマを使用します。たとえば **instance 1 vlan 10, 20, 30** と指定すると、VLAN 10、

	コマンドまたはアクション	目的
		20、30 が MST インスタンス 1 にマップされます。
ステップ 5	**name** *name* 例： `Device(config-mst)# name region1`	コンフィギュレーション名を指定します。*name* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。
ステップ 6	**revision** *version* 例： `Device(config-mst)# revision 1`	設定リビジョン番号を指定します。指定できる範囲は 0 ～ 65535 です。
ステップ 7	**show pending** 例： `Device(config-mst)# show pending`	保留中の設定を表示し、設定を確認します。
ステップ 8	**exit** 例： `Device(config-mst)# exit`	すべての変更を適用し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	**spanning-tree mode mst** 例： `Device(config)# spanning-tree mode mst`	MSTP をイネーブルにします。RSTP もイネーブルになります。 スパニングツリー モードを変更すると、すべてのスパニングツリーインスタンスは以前のモードであるため停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。 MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MSTP 設定時の注意事項 （896 ページ）
MST リージョン （898 ページ）

MSTP の前提条件 （893 ページ）
MSTP の制約事項 （894 ページ）
スパニングツリーの相互運用性と下位互換性 （873 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast （940 ページ）
UplinkFast （935 ページ）
MSTP のデフォルト設定 （913 ページ）
ルート デバイスの設定（CLI） （916 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID （865 ページ）
セカンダリ ルート デバイスの設定（CLI） （917 ページ）
ポート プライオリティの設定（CLI） （919 ページ）
パス コストの設定（CLI） （920 ページ）
デバイス プライオリティの設定（CLI） （922 ページ）
hello タイムの設定（CLI） （924 ページ）
転送遅延時間の設定（CLI） （925 ページ）
最大エージング タイムの設定（CLI） （926 ページ）
最大ホップ カウントの設定（CLI） （926 ページ）
高速移行を確実にするためのリンク タイプの指定（CLI） （927 ページ）
ネイバー タイプの設定（CLI） （929 ページ）
プロトコルの移行プロセスの再開（CLI） （930 ページ）

ルート デバイスの設定（CLI）

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。この例のステップ 2 では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **root primary** 例： `Device(config)# spanning-tree mst 0 root primary`	ルート デバイスとしてデバイスを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ルート スイッチ （897 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI） （913 ページ）
MSTP の制約事項 （894 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID （865 ページ）
セカンダリ ルート デバイスの設定（CLI） （917 ページ）

セカンダリ ルート デバイスの設定（CLI）

拡張システム ID をサポートするデバイスをセカンダリ ルートとして設定する場合、デバイス プライオリティはデフォルト値（32768）から 28672 に修正されます。プライマリ ルート デバイスで障害が発生した場合は、このデバイスが指定インスタンスのルートデバイスになる可能性があります。ここでは、その他のネットワーク デバイスが、デフォルトのデバイス プライオリティの 32768 を使用しているためにルートデバイスになる可能性が低いことが前提となっています。

このコマンドを複数のデバイスに対して実行すると、複数のバックアップ ルート デバイスを設定できます。**spanning-tree mst** *instance-id***root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート デバイスを設定したときと同じネットワーク直径および hello タイム値を使用してください。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **root secondary** 例： `Device(config)# spanning-tree mst 0 root secondary`	セカンダリ ルート デバイスとしてデバイスを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（913 ページ）
ルート デバイスの設定（CLI）　（916 ページ）

ポート プライオリティの設定（CLI）

ループが発生した場合、MSTPはポートプライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、MSTPはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

（注） デバイスがデバイス スタックのメンバーの場合、**spanning-tree mst** [*instance-id*] **port-priority** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree mst** [*instance-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用し、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させたいポートには、より小さいコスト値を割り当て、最後に選択させたいポートには、より大きいコスト値を割り当てることができます。詳細については、関連項目の下に表示されるパスコストのトピックを参照してください。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定されたMSTインスタンスIDと使用されるインターフェイスも把握する必要があります。この例では、インスタンスIDとして0を使用し、インターフェイスとしてGigabitEthernet1/0/1を使用します。これは「関連トピック」で示されている手順によってインスタンスIDとインターフェイスがそのように設定されているためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree mst** *instance-id* **port-priority** *priority* 例： `Device(config-if)# spanning-tree mst 0 port-priority 64`	ポート プライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *priority* 値の範囲は 0 ～ 240 で、16 ずつ増加します。デフォルト値は 128 です。値が小さいほど、プライオリティが高くなります。 使用可能な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 だけです。その他の値はすべて拒否されます。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-tree mstinterface *interface-id* 特権 EXEC コマンドは、ポートがリンク アップ動作可能状態であるかどうかの情報のみ表示します。そうでない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）（913 ページ）
パス コストの設定（CLI）（920 ページ）

パス コストの設定（CLI）

MSTP パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。すべてのイン

ターフェイスに同じコスト値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連トピック」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。有効なインターフェイスには、物理ポートとポートチャネル論理インターフェイスがあります。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**spanning-tree mst** *instance-id* **cost** *cost* 例： `Device(config-if)# spanning-tree mst 0 cost 17031970`	コストを設定します。 ループが発生した場合、MSTP はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のイ

	コマンドまたはアクション	目的
		ンスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-tree mst interface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンク アップ動作可能状態のポートの情報だけです。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティの設定（CLI）（919 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI）（913 ページ）

デバイス プライオリティの設定（CLI）

デバイスのプライオリティを変更すると、スタンドアロンデバイスまたはスタック内のデバイスであるかに関係なく、ルートデバイスとして選択される可能性が高くなります。

（注） このコマンドの使用には注意してください。通常のネットワーク設定では、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** グローバル コンフィグレーション コマンドを使用し、デバイスをルートまたはセカンダリ ルート デバイスに指定することを推奨します。これらのコマンドが動作しない場合にのみデバイスプライオリティを変更する必要があります。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

使用する指定された MST インスタンス ID も把握する必要があります。この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **priority** *priority* 例： `Device(config)# spanning-tree mst 0 priority 40960`	デバイスのプライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。この値が低いほど、デバイスがルート デバイスとして選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。これらは唯一の許容値です。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（913 ページ）

hello タイムの設定（CLI）

hello タイムはルート デバイスによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst hello-time** *seconds* 例： `Device(config)# spanning-tree mst hello-time 4`	すべての MST インスタンスについて、hello タイムを設定します。hello タイムはルートデバイスによって設定メッセージが生成されて送信される時間の間隔です。このメッセージは、デバイスが活動中であることを表します。 *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 3 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（913 ページ）

転送遅延時間の設定（CLI）

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst forward-time** *seconds* 例： `Device(config)# spanning-tree mst forward-time 25`	すべての MST インスタンスについて、転送時間を設定します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、ポートが待機する秒数です。 *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（913 ページ）

最大エージング タイムの設定（CLI）

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst max-age** *seconds* 例： `Device(config)# spanning-tree mst max-age 40`	すべての MST インスタンスについて、最大経過時間を設定します。最大エージング タイムは、デバイスが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（913 ページ）

最大ホップ カウントの設定（CLI）

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst max-hops** *hop-count* 例： `Device(config)# spanning-tree mst max-hops 25`	BPDU を廃棄してポート用に保持していた情報を期限切れにするまでの、リージョンでのホップ数を設定します。 *hop-count* に指定できる範囲は 1 ～ 255 です。デフォルト値は 20 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（913 ページ）

高速移行を確実にするためのリンク タイプの指定（CLI）

ポイントツーポイント リンクでポート間を接続し、ローカル ポートが DP になると、RSTP は提案と合意のハンドシェークを使用して別のポートと高速移行をネゴシエーションし、ループがないトポロジを保証します。

デフォルトの場合、リンク タイプはインターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続、半二重ポートは共有接続と見なされます。MSTP を実行しているリモート デバイスの単一ポートに、半二重リンクを物理的にポイントツーポイントで接続した場合は、リンク タイプのデフォルト設定を無効にして、フォワーディング ステートへの高速移行をイネーブルにすることができます。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連トピック」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポート、VLAN、およびポート チャネル論理インターフェイスがあります。VLAN ID の範囲は 1 ～ 4094 です。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**spanning-tree link-type point-to-point** 例： `Device(config-if)# spanning-tree link-type point-to-point`	ポートのリンク タイプがポイントツーポイントであることを指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（913 ページ）

ネイバー タイプの設定（CLI）

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることができます。デフォルトの場合、ポートは準規格デバイスを自動的に検出できますが、規格 BPDU および準規格 BPDU の両方を受信できます。デバイスとそのネイバーの間に不一致がある場合は、CIST だけがインターフェイスで動作します。

準規格 BPDU だけを送信するようにポートを設定できます。ポートが STP 互換モードになっていても、すべての **show** コマンドで準規格フラグが表示されます。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**spanning-tree mst pre-standard** 例： `Device(config-if)# spanning-tree mst pre-standard`	ポートが準規格 BPDU だけを送信できることを指定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）（913 ページ）

プロトコルの移行プロセスの再開（CLI）

この手順では、プロトコル移行プロセスを再開し、ネイバーデバイスとの再ネゴシエーションを強制します。また、デバイスを MST モードに戻します。これは、IEEE 802.1D BPDU の受信後にデバイスがそれらを受信しない場合に必要です。

デバイスでプロトコルの移行プロセスを再開する（隣接するデバイスで再ネゴシエーションを強制的に行う）手順については、これらの手順に従ってください。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

コマンドのインターフェイス バージョンを使用する場合は、使用する MST インターフェイスが分かっている必要があります。この例では、インターフェイスとして GigabitEthernet1/0/1 を使用します。それが「関連項目」で示されている手順によって設定されたインターフェイスであるからです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかのコマンドを入力します。 • **clear spanning-tree detected-protocols** • **clear spanning-tree detected-protocolsinterface** *interface-id* 例： `Device# clear spanning-tree detected-protocols`	デバイスが MSTP モードに戻り、プロトコルの移行プロセスが再開されます。

	コマンドまたはアクション	目的
	または `Device# clear spanning-tree detected-protocols interface GigabitEthernet1/0/1`	

次のタスク

この手順は、デバイスでさらにレガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定された BPDU）を受信する場合に、繰り返しが必要なことがあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI） （913 ページ）
プロトコル移行プロセス （912 ページ）

MSTP に関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	*LAN Switching Command Reference, Cisco IOS XE Release 3SE（Catalyst 3850 Switches）*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

MSTP の機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 46 章

オプションのスパニングツリー機能の設定

- オプションのスパニングツリー機能について （933 ページ）
- オプションのスパニングツリー機能の設定方法 （944 ページ）
- スパニングツリー ステータスのモニタリング （956 ページ）
- オプションのスパニング ツリー機能に関する追加情報 （957 ページ）
- オプションのスパニングツリー機能の機能情報 （958 ページ）

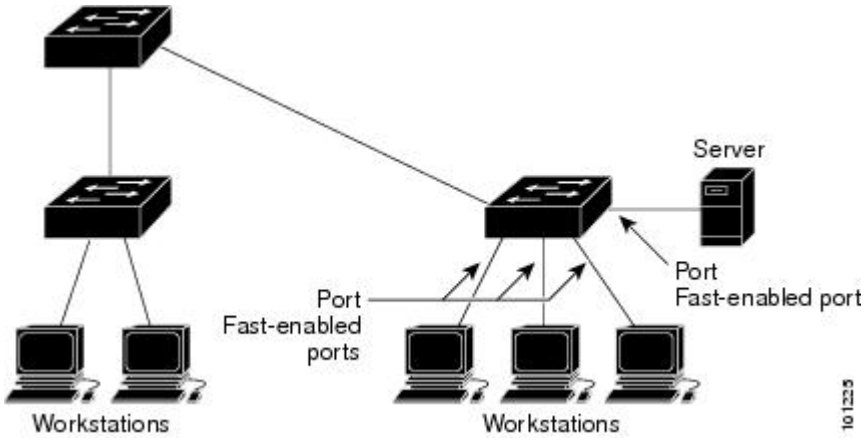
オプションのスパニングツリー機能について

PortFast

PortFast 機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートから直接フォワーディング ステートに移行します。

図 *52 : PortFast* が有効なインターフェイス

1 台のワークステーションまたはサーバに接続されているインターフェイス上で PortFast を使用すると、スパニングツリーが収束するのを待たずにデバイスをすぐにネットワークに接続できます。



1 台のワークステーションまたはサーバに接続されたインターフェイスがブリッジプロトコルデータ ユニット（BPDU）を受信しないようにする必要があります。スイッチを再起動すると、PortFast が有効に設定されているインターフェイスは通常のスパニングツリー ステータスの遷移をたどります。

インターフェイスまたはすべての非トランク ポートで有効にして、この機能を有効にできます。

関連トピック

PortFast のイネーブル化（CLI）（944 ページ）
オプションのスパニング ツリー機能の制約事項

BPDU ガード

ブリッジプロトコルデータ ユニット（BPDU）ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

PortFast エッジ対応ポート上でグローバル レベルで BPDU ガードをイネーブルにすると、スパニング ツリーは、BPDU が受信されると、PortFast エッジ動作ステートのポートをシャット ダウンします。有効な設定では、PortFast エッジ対応ポートは BPDU を受信しません。PortFast エッジ対応ポートが BPDU を受信した場合は、許可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは error-disabled ステートになります。この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

PortFast エッジ機能をイネーブルにせずにインターフェイス レベルでポート上の BPDU ガードをイネーブルにした場合、ポートが BPDU を受信すると、error-disabled ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

関連トピック

BPDU ガードのイネーブル化（CLI）（946 ページ）

BPDU フィルタリング

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルでは、PortFast エッジ対応インターフェイスで BPDU フィルタリングをイネーブルにすると、PortFast エッジ動作ステートにあるインターフェイスでの BPDU の送受信が防止されます。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。PortFast エッジ対応インター

フェイスでは、BPDU を受信すると、PortFast エッジ動作ステートが解除され、BPDU フィルタリングがディセーブルになります。

PortFastエッジ機能をイネーブルにせずに、インターフェイスでBPDUフィルタリングをイネーブルにすると、インターフェイスでの BPDU の送受信が防止されます。

注意 BPDUフィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチ全体または1つのインターフェイスでBPDUフィルタリング機能をイネーブルにできます。

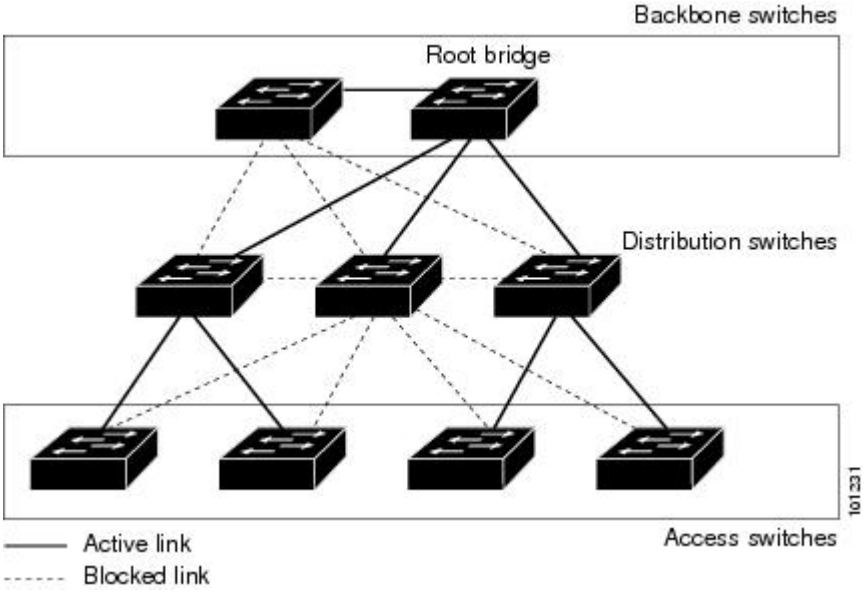
関連トピック

BPDU フィルタリングのイネーブル化（CLI）（948 ページ）

UplinkFast

図 *53*：階層型ネットワークのスイッチ

階層型ネットワークに配置されたスイッチは、バックボーン スイッチ、ディストリビューション スイッチ、およびアクセス スイッチに分類できます。この複雑なネットワークには、ディストリビューション スイッチとアクセス スイッチがあり、ループを防止するために、スパニング ツリーがブロックする冗長リンクが少なくとも 1 つあります。



スイッチの接続が切断されると、スイッチはスパニングツリーが新しいルート ポートを選択すると同時に代替パスの使用を開始します。リンクやスイッチに障害が発生した場合、またはスパニングツリーが UplinkFast の有効化によって自動的に再設定された場合に、新しいルート ポートを短時間で選択できます。ルート ポートは、通常のスパニングツリー手順とは異なり、

リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

スパニングツリーが新規ルート ポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッディングし、インターフェイス上で学習した各アドレスにパケットを送信します。max-update-rate パラメータの値を小さくすることで、これらのマルチキャスト トラフィックのバーストを制限できます（このパラメータはデフォルトで毎秒 150 パケットです）。ただし、0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。

（注） UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのスイッチで非常に有効です。バックボーン デバイスには適していません。他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロード バランシングを実行します。アップリンク グループは、（VLAN ごとの）レイヤ 2 インターフェイスの集合であり、いかなるときも、その中の 1 つのインターフェイスだけが転送を行います。つまり、アップリンク グループは、（転送を行う）ルート ポートと、（セルフループを行うポートを除く）ブロックされたポートの集合で構成されます。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

図 *54 :* 直接リンク障害が発生する前の *UplinkFast* の例

このトポロジにはリンク障害がありません。ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

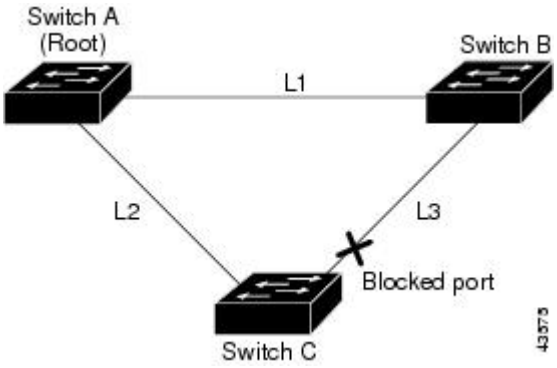
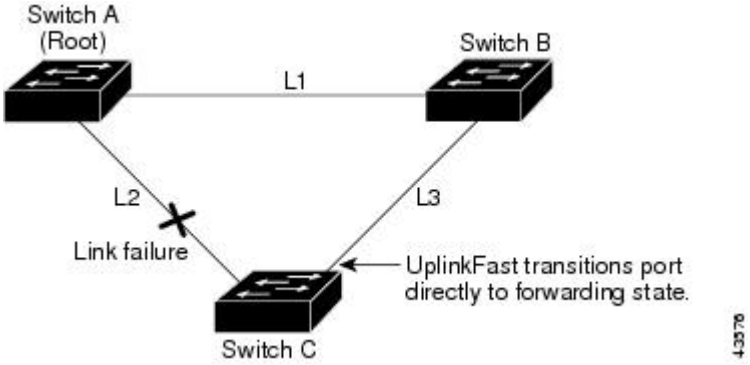


図 *55 :* 直接リンク障害が発生したあとの *UplinkFast* の例

スイッチ C が、ルート ポートの現在のアクティブ リンクである L2 でリンク障害（直接リンク障害）を検出すると、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、直接フォワー

ディング ステートに移行させます。この切り替えに必要な時間は、約 1 ～ 5 秒です。



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）（913 ページ）
MSTP 設定時の注意事項（896 ページ）
MST リージョン（898 ページ）
冗長リンクで使用するための UplinkFast のイネーブル化（CLI）（949 ページ）
高速コンバージェンスを発生させるイベント（939 ページ）

クロススタック UplinkFast

クロススタック UplinkFast（CSUF）は、スイッチ スタック全体にスパニングツリー高速移行（通常のネットワーク状態の下では1秒未満の高速コンバージェンス）を提供します。高速移行の間は、スタック上の代替冗長リンクがフォワーディング ステートになり、一時的なスパニングツリーループもバックボーンへの接続の損失も発生させません。一部の設定では、この機能により、冗長性と復元力を備えたネットワークが得られます。CSUF は UplinkFast 機能をイネーブルにすると、自動的にイネーブルになります。

CSUF で高速移行が得られない場合もあります。この場合は、通常のスパニングツリー移行が発生し、30 ～ 40 秒以内に完了します。詳細については、「関連項目」を参照してください。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化（CLI）（949 ページ）
高速コンバージェンスを発生させるイベント（939 ページ）

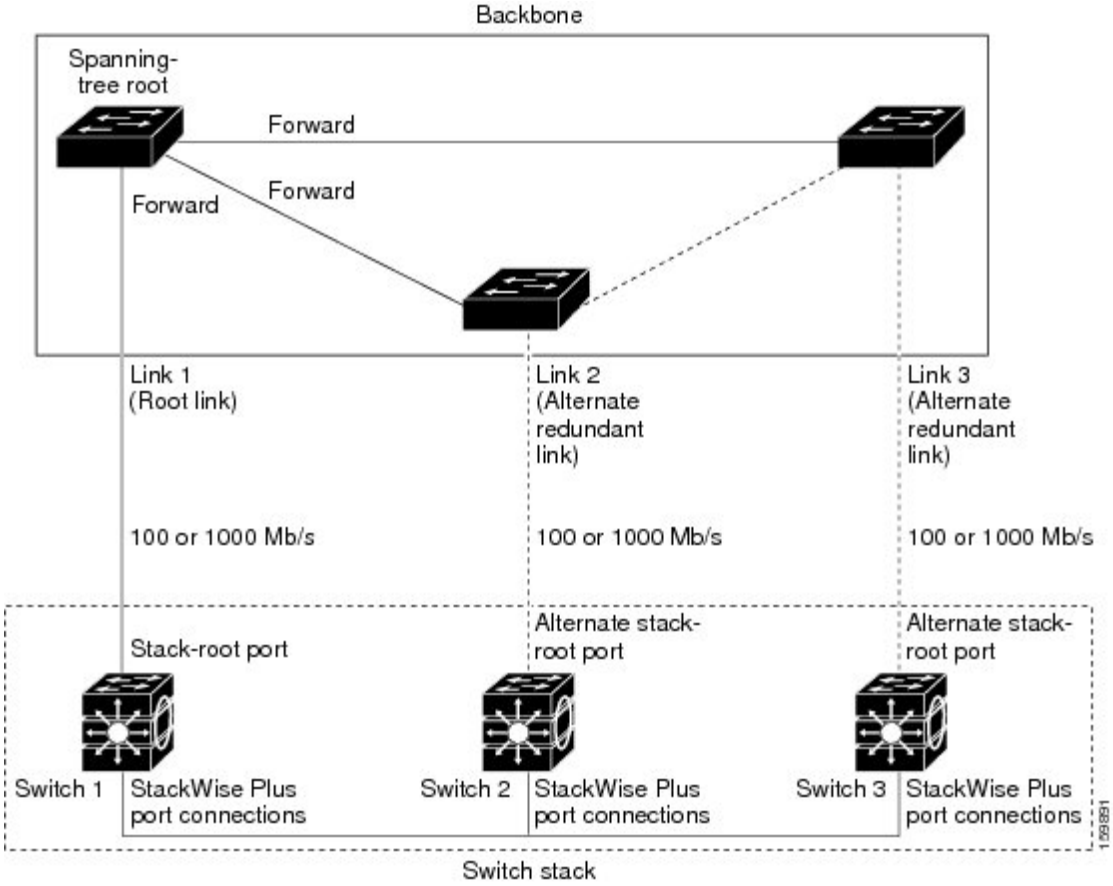
クロススタック UplinkFast の動作

クロススタック UplinkFast（CSUF）によって、ルートへのパスとしてスタック内で1つのリンクが確実に選択されます。

図 *56 :* クロススタック *UplinkFast* トポロジ

スイッチ1のスタックルート ポートは、スパニングツリーのルートへパスを提供しています。スイッチ 2 およびスイッチ 3 の代替スタックルート ポートは、現在のスタックルート スイッチに障害が発生したか、またはそのスパニングツリールートへのリンクに障害が発生した場合に、スパニングツリー ルートへの代替パスを提供できます。

ルート リンクである Link 1 は、スパニングツリー フォワーディング ステートになっています。Link 2 と Link 3 は、スパニングツリー ブロッキング ステートになっている代替冗長リンクです。スイッチ 1 に障害が発生したか、そのスタック ルート ポートに障害が発生したか、または Link 1 に障害が発生した場合には、CSUF が、1 秒未満でスイッチ 2 またはスイッチ 3 のいずれかにある代替スタックルート ポートを選択して、それをフォワーディング ステートにします。



特定のリンク損失またはスパニングツリーイベントが発生した場合（次のトピックを参照）、Fast Uplink Transition Protocol は、ネイバー リストを使用して、高速移行要求をスタック メンバーに送信します。

高速移行要求を送信するスイッチは、ルートポートとして選択されたポートをフォワーディングステートへ高速移行する必要があります。また、高速移行を実行するには、事前に各スタックから確認応答を取得しておく必要があります。

スタック内の各スイッチが、ルート、コスト、およびブリッジ ID を比較することにより、このスパニングツリー インスタンスのスタック ルートとなるよりも送信スイッチの方がよりよい選択肢であるかどうかを判断します。スタックルートとして送信スイッチが最も良い選択である場合は、スタック内の各スイッチが確認応答を返します。それ以外の場合は、高速移行要求を送信します。この時点では、送信スイッチは、すべてのスタック スイッチから確認応答を受け取っていません。

すべてのスタック スイッチから確認応答を受け取ると、送信スイッチの Fast Uplink Transition Protocol は代替スタックルート ポートをすぐにフォワーディング ステートに移行させます。送信スイッチがすべてのスタック スイッチからの確認応答を取得しなかった場合、通常のスパニングツリー移行（ブロッキング、リスニング、ラーニング、およびフォワーディング）が行われ、スパニングツリー トポロジが通常のレート（2 × 転送遅延時間 + 最大エージング タイム）で収束します。

Fast Uplink Transition Protocol は、VLAN ごとに実装されており、一度に 1 つのスパニングツリー インスタンスにしか影響しません。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化（CLI） （949 ページ）
高速コンバージェンスを発生させるイベント （939 ページ）

高速コンバージェンスを発生させるイベント

CSUF 高速コンバージェンスは、ネットワーク イベントまたはネットワーク障害に応じて、発生する場合もあれば発生しない場合もあります。

高速コンバージェンス（通常のネットワーク状態で 1 秒未満）は、次のような状況で発生します。

- スタック ルート ポート リンクに障害が発生した。

  スタック内の 2 つのスイッチがルートへの代替パスを持つ場合、それらのスイッチの片方だけが高速移行を行います。

- スタック ルートをスパニングツリー ルートに接続するリンクに障害が発生し、回復した。
- ネットワークの再設定により、新しいスタックルート スイッチが選択された。
- ネットワークの再設定により、現在のスタックルート スイッチ上で新しいポートがスタック ルート ポートとして選択された。

（注） 複数のイベントが同時に発生すると、高速移行が行われなくなる場合もあります。たとえば、スタック メンバの電源がオフになり、それと同時にスタック ルートをスパニングツリー ルートに接続しているリンクが回復した場合、通常のスパニングツリー コンバージェンスが発生します。

通常のスパニングツリー コンバージェンス（30 ～ 40 秒）は、次のような状況で発生します。

- スタック ルート スイッチの電源がオフになったか、またはソフトウェアに障害が発生した。
- 電源がオフになっていたか、または障害が発生していたスタック ルート スイッチの電源が入った。
- スタック ルートになる可能性のある新しいスイッチがスタックに追加された。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化（CLI）（949 ページ）
UplinkFast（935 ページ）
クロススタック UplinkFast（937 ページ）
クロススタック UplinkFast の動作（937 ページ）

BackboneFast

BackboneFast は、バックボーンのコアにおける間接障害を検出します。BackboneFast は、UplinkFast 機能を補完するテクノロジーです。UplinkFast は、アクセス スイッチに直接接続されたリンクの障害に対応します。BackboneFastは、最大エージング タイマーを最適化します。最大エージング タイマーによって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御されます。スイッチが別のスイッチの指定ポートから下位BPDUを受信した場合、BPDUは他のスイッチでルートまでのパスが失われた可能性を示すシグナルとなり、BackboneFast はルートまでの別のパスを見つけようとします。

スイッチのルート ポートまたはブロックされたインターフェイスが、指定スイッチから下位 BPDU を受け取ると、BackboneFast が開始します。下位 BPDU は、ルート ブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位BPDUを受信した場合、そのスイッチが直接接続されていないリンク（間接リンク）で障害が発生したことを意味します（指定スイッチとルート スイッチ間の接続が切断されています）。スパニングツリーのルールに従い、スイッチは最大エージング タイム（デフォルトは 20 秒）の間、下位 BPDU を無視します。

スイッチは、ルート スイッチへの代替パスの有無を判別します。下位 BPDU がブロック インターフェイスに到達した場合、スイッチ上のルート ポートおよび他のブロック インターフェイスがルート スイッチへの代替パスになります（セルフループ ポートはルート スイッチの代替パスとは見なされません）。下位 BPDU がルート ポートに到達した場合には、すべてのブロック インターフェイスがルート スイッチへの代替パスになります。下位 BPDU がルート ポートに到達し、しかもブロック インターフェイスがない場合、スイッチはルート スイッチへの接続が切断されたものと見なし、ルート ポートの最大エージング タイムが経過するまで待ち、通常のスパニングツリー ルールに従ってルート スイッチになります。

スイッチが代替パスでルート スイッチに到達できる場合、スイッチはその代替パスを使用して、Root Link Query（RLQ）要求を送信します。スイッチは、スタック メンバーがルート スイッチへの代替ルートを持つかどうかを学習するために、すべての代替パスに RLQ 要求を送信し、ネットワーク内およびスタック内の他のスイッチからのRLQ応答を待機します。スイッチは、すべての代替パスに RLQ 要求を送信し、ネットワーク内の他のスイッチからの RLQ 応答を待機します。

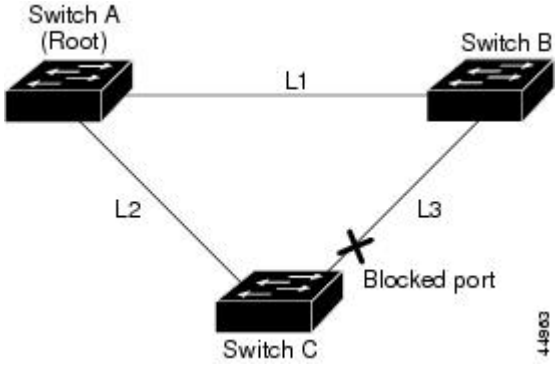
スタック メンバが、ブロック インターフェイス上の非スタック メンバから RLQ 応答を受信し、その応答が他の非スタック スイッチ宛てのものであった場合、そのスタック メンバは、スパニングツリー インターフェイス ステートに関係なく、その応答パケットを転送します。

スタック メンバが非スタック メンバから RLQ 応答を受信し、その応答がスタック宛てのものであった場合、そのスタック メンバは、他のすべてのスタック メンバがその応答を受信するようにその応答を転送します。

ルートへの代替パスがまだ存在していると判断したスイッチは、下位 BPDU を受信したインターフェイスの最大エージング タイムが経過するまで待ちます。ルート スイッチへのすべての代替パスが、スイッチとルート スイッチ間の接続が切断されていることを示している場合、スイッチは RLQ 応答を受信したインターフェイスの最大エージング タイムを満了させます。1 つまたは複数の代替パスからルート スイッチへ引き続き接続できる場合、スイッチは下位 BPDU を受信したすべてのインターフェイスを指定ポートにして、（ブロッキング ステートになっていた場合）ブロッキング ステートを解除し、リスニング ステート、ラーニング ステートを経てフォワーディング ステートに移行させます。

図 *57*：間接リンク障害が発生する前の *BackboneFast* の例

これは、リンク障害が発生していないトポロジ例です。ルート スイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング



ステートです。

図 *58*：間接リンク障害が発生したあとの *BackboneFast* の例

リンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、この障害を検出できません。一方スイッチ B は、L1 によってルート スイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。BackboneFast は、次に、スイッチ C のレイヤ2インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを提供します。ルートスイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に設定されていればその倍の時間です。BackboneFast がリンク L1 で発

生した障害に応じてトポロジを再設定します。

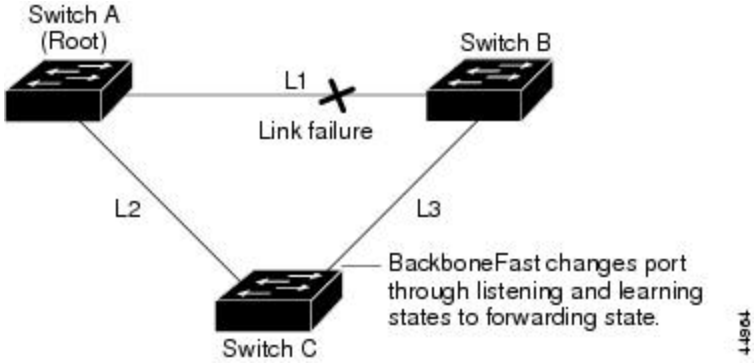
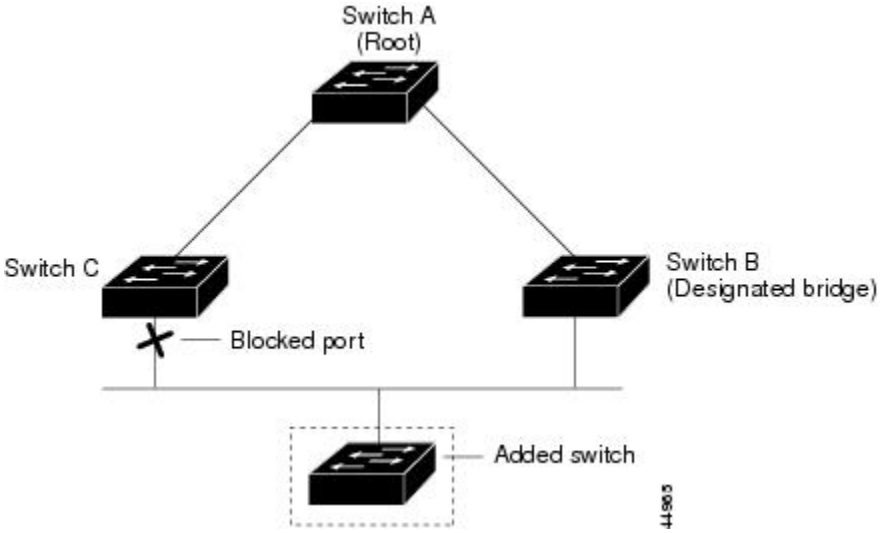


図 *59 :* メディア共有型トポロジにおけるスイッチの追加

新しいスイッチがメディア共有型トポロジに組み込まれた場合、認識された指定スイッチ（スイッチ B）から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。新しいスイッチは、自身がルート スイッチであることを伝える下位 BPDU の送信を開始します。ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定スイッチであることを学習します。



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI） （913 ページ）
MSTP 設定時の注意事項 （896 ページ）
MST リージョン （898 ページ）
BackboneFast をイネーブル化（CLI） （952 ページ）

EtherChannel ガード

EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾

が発生します。また、EtherChannel の両端でチャネルのパラメータが異なる場合にも、設定の矛盾が発生します。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのインターフェイスを errdisable ステートにし、エラー メッセージを表示します。

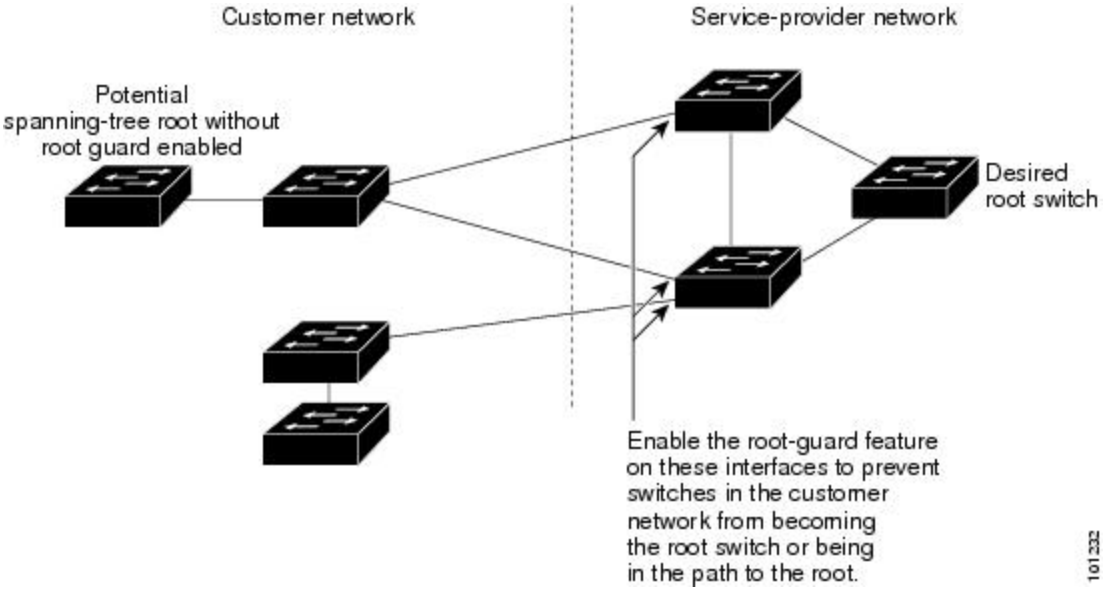
関連トピック

EtherChannel ガードのイネーブル化（CLI） （953 ページ）

ルート ガード

図 *60*：サービス プロバイダー ネットワークのルート ガード

サービス プロバイダー（SP）のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多く含まれている場合があります。このようなトポロジでは、スパニングツリーが再構成され、カスタマー スイッチをルート スイッチとして選択する可能性があります。この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルート ガード機能を有効に設定します。スパニングツリーの計算によってカスタマーネットワーク内のインターフェイスがルート ポートとして選択されると、ルート ガードがそのインターフェイスを root-inconsistent（ブロッキング）ステートにして、カスタマーのスイッチがルート スイッチにならないようにするか、ルートへのパスに組み込まれないようにします。



SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ（root-inconsistent ステートになり）、スパニングツリーが新しいルート スイッチを選択します。カスタマーのスイッチがルート スイッチになることはありません。ルートへのパスに組み込まれることもありません。

スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定ポートにします。また、境界ポートがルート ガードによって Internal Spanning-Tree（IST）インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インス

タンスでもブロックされます。境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。VLAN は、MST インスタンスに対してグループ化された後、マッピングされます。

⚠

注意 ルート ガード機能を誤って使用すると、接続が切断されることがあります。

関連トピック

ルート ガードのイネーブル化（CLI） （954 ページ）

ループ ガード

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチドネットワーク全体でイネーブルにした場合に最も効果があります。ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされている場合でのみ、非境界ポートで BPDU を送信しません。境界ポートでは、ループ ガードがすべての MST インスタンスでインターフェイスをブロックします。

関連トピック

ループ ガードのイネーブル化（CLI） （955 ページ）

オプションのスパニングツリー機能の設定方法

PortFast のイネーブル化（CLI）

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、すぐにスパニングツリー フォワーディング ステートに移行されます。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

⚠

注意 PortFast を使用するのは、1 つのエンド ステーションがアクセス ポートまたはトランク ポートに接続されている場合に限定されます。スイッチまたはハブに接続するインターフェイス上でこの機能をイネーブルにすると、スパニングツリーがネットワーク ループを検出または阻止できなくなり、その結果、ブロードキャスト ストームおよびアドレス ラーニングの障害が起きる可能性があります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree portfast** [**trunk**] 例： `Device(config-if)# spanning-tree portfast trunk`	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で PortFast をイネーブルにします。**trunk** キーワードを指定すると、トランク ポート上で PortFast をイネーブルにできます。

	コマンドまたはアクション	目的
		（注） トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランク ポート上では機能しないためです。 トランク ポート上で PortFast をイネーブルにする場合は、事前に、トランク ポートとワークステーションまたはサーバの間にループがないことを確認してください。 デフォルトでは、PortFast はすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

次のタスク

spanning-tree portfast default グローバル コンフィギュレーション コマンドを使用すると、すべての非トランク ポート上で PortFast 機能をグローバルにイネーブルにできます。

関連トピック

PortFast （933 ページ）
オプションのスパニング ツリー機能の制約事項

BPDU ガードのイネーブル化（CLI）

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU ガード機能をイネーブルにできます。

⚠

注意 PortFast エッジは、エンド ステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree portfast edge bpduguard default** 例： `Device(config)# spanning-tree portfast edge bpduguard default`	BPDU ガードをグローバルにイネーブルにします。 BPDU ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	エンドステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**spanning-tree portfast edge** 例： `Device(config-if)# spanning-tree portfast edge`	PortFast エッジ機能をイネーブルにします。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

次のタスク

ポートのシャットダウンを防ぐには、**errdisable detect cause bpduguard shutdown vlan** グローバル コンフィギュレーション コマンドを使用すると、違反の発生時にポートで問題になっている VLAN のみをシャットダウンできます。

PortFast エッジ機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにすることもできます。BPDU を受信したポートは、errdisable ステートになります。

関連トピック

BPDU ガード （934 ページ）

BPDU フィルタリングのイネーブル化（CLI）

PortFast エッジ機能をイネーブルにしなくても、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイスで BPDU フィルタリングをイネーブルにすることもできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。

⚠

注意 BPDUフィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU フィルタリング機能をイネーブルにできます。

⚠

注意 PortFast エッジは、エンド ステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree portfast edge bpdufilter default** 例： `Device(config)# spanning-tree portfast edge bpdufilter default`	BPDU フィルタリングをグローバルにイネーブルにします。 BPDU フィルタリングは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	エンドステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**spanning-tree portfast edge** 例： `Device(config-if)# spanning-tree portfast edge`	指定したインターフェイスで PortFast エッジ機能をイネーブルにします。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

BPDU フィルタリング （934 ページ）

冗長リンクで使用するための UplinkFast のイネーブル化（CLI）

（注） UplinkFast をイネーブルにすると、スイッチまたはスイッチ スタックのすべての VLAN に影響します。個々の VLAN について UplinkFast を設定することはできません。

Rapid PVST+ または MSTP に対して UplinkFast または Cross-Stack UplinkFast（CSUF）機能を設定できますが、この機能は、スパニングツリーのモードを PVST+ に変更するまではディセーブル（非アクティブ）になったままです。

この手順は任意です。UplinkFast および CSUF をイネーブルにするには、次の手順に従います。

始める前に

スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにすることはできません。スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにする場合は、最初に **no spanning-tree vlan** *vlan-id***priority** グローバル コンフィギュレーショ

ン コマンドを使用することによって、VLAN のスイッチ プライオリティをデフォルト値に戻す必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree uplinkfast** [**max-update-rate** *pkts-per-second*] 例： `Device(config)# spanning-tree uplinkfast max-update-rate 200`	UplinkFast をイネーブルにします。 （任意）*pkts-per-second* に指定できる範囲は毎秒 0 ～ 32000 パケットです。デフォルト値は 150 です。 0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。 このコマンドを入力すると、すべての非スタック ポート インターフェイス上で CSUF もイネーブルになります。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティは 49152 に設定されます。UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します（パス コストを 3000 以上の値に変更した場合、パス コストは変更されません）。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をイネーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにイネーブルになります。

関連トピック

UplinkFast （935 ページ）
クロススタック UplinkFast （937 ページ）
クロススタック UplinkFast の動作 （937 ページ）
高速コンバージェンスを発生させるイベント （939 ページ）

UplinkFast のディセーブル化（CLI）

この手順は任意です。

UplinkFast および Cross-Stack UplinkFast（SUF）をディセーブルにするには、次の手順に従います。

始める前に

UplinkFast を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree uplinkfast** 例： `Device(config)# no spanning-tree uplinkfast`	スイッチおよびそのスイッチのすべての VLAN で UplinkFast および CSUF をディセーブルにします。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をディセーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにディセーブルになります。

BackboneFast をイネーブル化（CLI）

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニングツリーの再構成をより早く開始できます。

Rapid PVST+ または MSTP に対して BackboneFast 機能を設定できます。ただし、スパニングツリーモードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

この手順は任意です。スイッチ上で BackboneFast をイネーブルにするには、次の手順に従います。

始める前に

BackboneFast を使用する場合は、ネットワーク上のすべてのスイッチでイネーブルする必要があります。BackboneFast は、トークンリング VLAN ではサポートされません。この機能は他社製スイッチでの使用にサポートされています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree backbonefast** 例：	BackboneFast をイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config)# spanning-tree backbonefast`	
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

BackboneFast （940 ページ）

EtherChannel ガードのイネーブル化（CLI）

デバイスで PVST+、Rapid PVST+、または MSTP が稼働している場合、EtherChannel の設定の矛盾を検出する EtherChannel ガード機能をイネーブルにできます。

この手順は任意です。

デバイスで EtherChannel ガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree etherchannel guard misconfig** 例： `Device(config)# spanning-tree etherchannel guard misconfig`	EtherChannel ガードをイネーブルにします。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	

次のタスク

show interfaces status err-disabled 特権 EXEC コマンドを使用することで、EtherChannel の設定矛盾が原因でディセーブルになっているデバイス ポートを表示できます。リモート デバイス上では、**show etherchannel summary** 特権 EXEC コマンドを使用して、EtherChannel の設定を確認できます。

設定を修正した後、誤って設定していたポート チャネル インターフェイス上で、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してください。

関連トピック

EtherChannel ガード （942 ページ）

ルート ガードのイネーブル化（CLI）

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロック ステートの）バックアップ インターフェイスがルート ポートになります。ただし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。

（注） ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。

スイッチ上でルート ガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree guard root** 例： `Device(config-if)# spanning-tree guard root`	インターフェイス上でルート ガードをイネーブルにします。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

ルート ガード （943 ページ）

ループ ガードのイネーブル化（CLI）

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチドネットワーク全体に設定した場合に最も効果があります。ループ ガードは、スパニングツリーがポイントツーポイントと見なすインターフェイス上でのみ動作します。

（注） ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。

デバイスで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。デバイスでループ ガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的

ステップ 1	次のいずれかのコマンドを入力します。
	• **show spanning-tree active**
	• **show spanning-tree mst**
	例：
	`Device# show spanning-tree active`
	または
	`Device# show spanning-tree mst`
		どのインターフェイスが代替ポートまたはルートポートであるかを確認します。

ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree loopguard default** 例： `Device(config)# spanning-tree loopguard default`	ループ ガードをイネーブルにします。 ループ ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ループ ガード （944 ページ）

スパニングツリー ステータスのモニタリング

表 *58 :* スパニングツリー ステータスをモニタリングするコマンド

コマンド	目的
show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。

コマンド	目的
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree mst interface *interface-id*	指定インターフェイスのMST情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。またはスパニングツリー ステート セクションのすべての行を表示します。
show spanning-tree mst interface *interface-id***portfast edge**	指定したインターフェイスのスパニングツリー portfast 情報を表示します。

オプションのスパニング ツリー機能に関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	『LAN Switching Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

オプションのスパニングツリー機能の機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 47 章

EtherChannel の設定

- 機能情報の確認 （959 ページ）
- EtherChannel の制約事項 （959 ページ）
- EtherChannel について （960 ページ）
- EtherChannel の設定方法 （979 ページ）
- EtherChannel、PAgP、および LACP ステータスのモニタ （999 ページ）
- EtherChannel の設定例 （1000 ページ）
- EtherChannels の追加リファレンス （1003 ページ）
- EtherChannels の機能情報 （1004 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

EtherChannel の制約事項

次に、EtherChannels の制約事項を示します。

- EtherChannel のすべてのポートは同じ VLAN に割り当てるか、またはトランク ポートとして設定する必要があります。
- LAN Base ライセンス フィーチャ セットを実行している場合は、レイヤ 3 EtherChannels はサポートされません。

- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

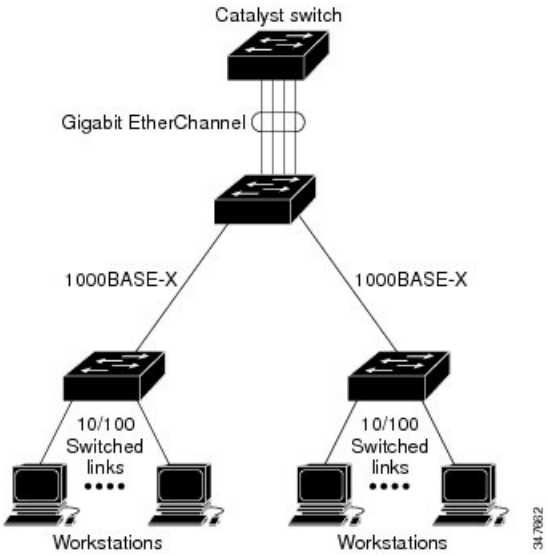
EtherChannel について

EtherChannel の概要

EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用して、ワイヤリング クローゼットとデータセンター間の帯域幅を増やすことができます。さらに、ボトルネックが発生しやすいネットワーク上のあらゆる場所に EtherChannel を配置できます。EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャネル内の他のリンクにトラフィックをリダイレクトします。

EtherChannel は、単一の論理リンクにバンドルする個別のイーサネット リンクで構成されます。

図 *61 :* 一般的な *EtherChannel* 構成



EtherChannel は、スイッチ間またはスイッチとホスト間に、最大 8 Gb/s（ギガビット EtherChannel）または 80 Gb/s（10 ギガビット EtherChannel）の全二重帯域幅を提供します。

各 EtherChannel は、互換性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

EtherChannel の最大数は 128 に制限されています。

LAN Base フィーチャ セットでは、最大 24 個の EtherChannel をサポートします。

各 EtherChannel 内のすべてのポートは、レイヤ 2 またはレイヤ 3 ポートのいずれかとして設定する必要があります。EtherChannel レイヤ 3 ポートは、ルーテッド ポートで構成されます。

ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ3モードに設定された物理ポートです。詳細については、「インターフェイス特性の設定」を参照してください。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （979 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）

EtherChannel のモード

EtherChannel は、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、または On のいずれかのモードに設定できます。EtherChannel の両端は同じモードで設定します。

- EtherChannel の一方の端を PAgP または LACP モードに設定すると、システムはもう一方の端とネゴシエーションし、アクティブにするポートを決定します。リモート ポートが EtherChannel とネゴシエーションができない場合、ローカル ポートは独立ステートになり、他の単一リンクと同様にデータ トラフィックを引き続き伝送します。ポート設定は変更されませんが、ポートは EtherChannel に参加しません。
- EtherChannel を **on** モードに設定すると、ネゴシエーションは実行されません。スイッチは EtherChannel 内で互換性のあるすべてのポートを強制的にアクティブにします。EtherChannel のもう一方の端（他のスイッチ上）も、同じように **on** モードに設定する必要があります。それ以外を設定した場合、パケットの損失が発生する可能性があります。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （979 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）

デバイス上の EtherChannel

デバイス上、スタックの単一デバイス上、またはスタックの複数デバイス上（クロススタック EtherChannel とも呼ぶ）で EtherChannel を作成できます。

図 *62*：単一スイッチ *EtherChannel*

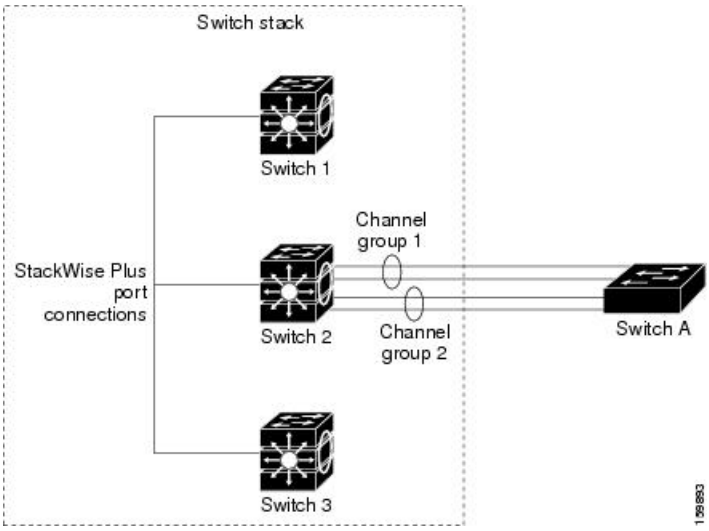
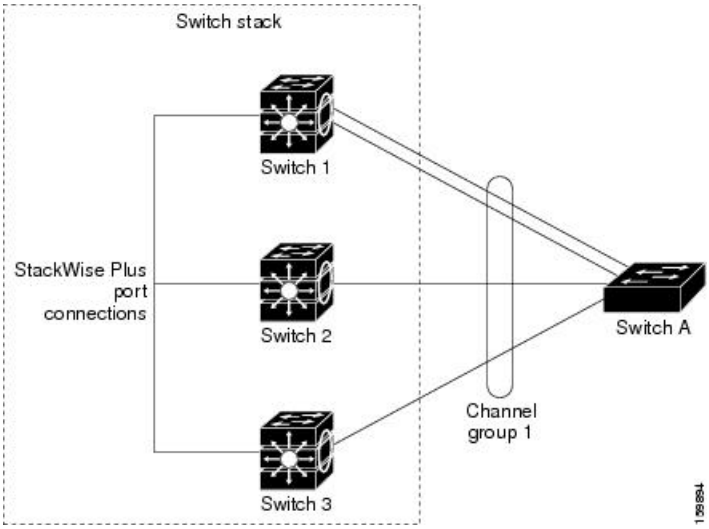


図 *63*：クロススタック *EtherChannel*



関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （979 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）

EtherChannel リンクのフェールオーバー

EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが EtherChannel 内の残りのリンクに切り替えられます。スイッチでトラップがイネーブルになっている場合、スイッチ、EtherChannel、および失敗したリンクを区別したトラップ

が送信されます。EtherChannel の 1 つのリンク上の着信ブロードキャストおよびマルチキャスト パケットは、EtherChannel の他のリンクに戻らないようにブロックされます。

関連トピック

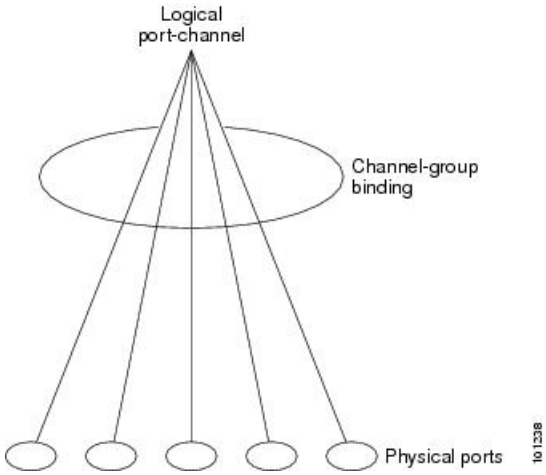
レイヤ 2 EtherChannel の設定 （CLI） （979 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）

チャネル グループおよびポートチャネル インターフェイス

EtherChannel は、チャネル グループとポートチャネル インターフェイスから構成されます。チャネル グループはポートチャネル インターフェイスに物理ポートをバインドします。ポートチャネル インターフェイスに適用した設定変更は、チャネル グループにまとめてバインドされるすべての物理ポートに適用されます。

図 *64 :* 物理ポート、チャネル グループおよびポートチャネル インターフェイスの関係

channel-group コマンドは、物理ポートおよびポートチャネル インターフェイスをまとめてバインドします。各 EtherChannel には 1 ～ 128 までの番号が付いたポートチャネル論理インターフェイスがあります。このポートチャネル インターフェイス番号は、**channel-group** インターフェイス コンフィギュレーション コマンドで指定した番号に対応しています。



- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル インターフェイスを動的に作成します。

  また、**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group** *channel-group-number* コマンドを使用する必要があります。*channel-group-number* は *port-channel-number* と同じ値に設定することも、違う値を使用することもできます。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。その後、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。
- レイヤ 3 ポートでレイヤ 3 インターフェイスとしてインターフェイスを設定するには、**no switchport** インターフェイス コマンドを使用した上で **channel-group** インターフェイス コンフィギュレーション コマンドを使用して動的にポートチャネル インターフェイスを作成します。

関連トピック

ポートチャネル論理インターフェイスの作成 （CLI）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）
物理インターフェイスの設定（CLI）

Port Aggregation Protocol; ポート集約プロトコル

ポート集約プロトコル（PAgP）はシスコ独自のプロトコルで、Cisco デバイスおよび PAgP をサポートするベンダーによってライセンス供与されたデバイスでのみ稼働します。PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。PAgP はクロススタック EtherChannel でイネーブルにできます。

デバイスまたはデバイス スタックは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似している（スタック内の単一デバイス上の）ポートを、単一の論理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、PAgP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクを EtherChannel にグループ化した後で、PAgP は単一デバイス ポートとして、スパニングツリーにそのグループを追加します。

PAgP モード

PAgP モードは、PAgP ネゴシエーションを開始する PAgP パケットをポートが送信できるか、または受信した PAgP パケットに応答できるかを指定します。

表 *59 : EtherChannel PAgP* モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。これにより、PAgP パケットの送信は最小限に抑えられます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。EtherChannel メンバが、スイッチ スタックにある異なるスイッチから（クロススタック EtherChannel）の場合、このモードがサポートされます。

スイッチ ポートは、**auto** モードまたは **desirable** モードに設定された相手ポートとだけ PAgP パケットを交換します。**on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

PAgP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **desirable** モードのポートは、**desirable** モードまたは **auto** モードの別のポートとともに EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートとともに EtherChannel を形成できます。

どのポートも PAgP ネゴシエーションを開始しないため、**auto** モードのポートは、**auto** モードの別のポートとは EtherChannel を形成できません。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （979 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
物理インターフェイスの設定（CLI）

サイレント モード

PAgP 対応のデバイスにスイッチを接続する場合、**non-silent** キーワードを使用すると、非サイレント動作としてスイッチ ポートを設定できます。**auto** モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレント モードが指定されていると見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにスイッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼働させると、このスイッチ ポートが動作しなくなります。ただし、サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （979 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
物理インターフェイスの設定（CLI）

PAgP 学習方式およびプライオリティ

ネットワーク デバイスは、PAgP 物理ラーナーまたは集約ポート ラーナーに分類されます。物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。集約（論理）ポートによってアドレスを学習するデバイスは、集約ポート ラーナーです。学習方式は、リンクの両端で同一の設定にする必要があります。

デバイスとそのパートナーが両方とも集約ポート ラーナーの場合、論理ポートチャネル上のアドレスを学習します。デバイスは EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポート ラーナーの場合には自動検出できません。したがって、物理ポートでアドレスを学習するには、ローカルデバイスに手動で学習方式を設定する必要があります。また、負荷の分散方式を送信元ベース分散に設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要もあります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホット スタンバイに使用することもできます。選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。パケット伝送用に常に選択されるようにポートを設定するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。

（注） CLI で **physical-port** キーワードを指定した場合でも、デバイスがサポートするのは、集約ポート上でのアドレス ラーニングのみです。**pagp learn-method** コマンドおよび **pagp port-priority** コマンドは、デバイスのハードウェアには作用しませんが、Catalyst 1900 スイッチなどの物理ポートによるアドレス ラーニングだけをサポートするデバイスと PAgP の相互運用性を確保するために必要です。

デバイスのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポート ラーナーとしてデバイスを設定することを推奨します。送信元 MAC アドレスに基づいて負荷の分散方式を設定するには、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用します。すると、デバイスは送信元アドレスを学習した EtherChannel 内の同じポートを使用して、物理ラーナーにパケットを送信します。**pagp learn-method** コマンドは、このような場合のみ使用してください。

関連トピック

PAgP 学習方式およびプライオリティの設定 （CLI） （988 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （999 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）

PAgP と他の機能との相互作用

ダイナミック トランキング プロトコル（DTP）および Cisco Discovery Protocol（CDP）は、EtherChannel の物理ポートを使用してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で PAgP プロトコル データ ユニット（PDU）を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。レイヤ 3 EtherChannel の場合は、（**interface port-channel** グローバル コンフィギュレーション コマンドを使用して）ポートが作成された直後に、アクティブなデバイスによって MAC アドレスが割り当てられます。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼働状態のポート上だけです。

Link Aggregation Control Protocol

LACP は IEEE 802.3ad で定義されており、Cisco デバイスが IEEE 802.3ad プロトコルに適合したデバイス間のイーサネット チャネルを管理できるようにします。LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

デバイスまたはデバイス スタックは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポー

トを単一の倫理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポートパラメータ制約です。たとえば、LACP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成した後で、LACP は単一デバイス ポートとして、スパニングツリーにそのグループを追加します。

ポート チャネル内のポートの独立モード動作が変更されます。CSCtn96950 では、デフォルトでスタンドアロン モードが有効になっています。LACP ピアから応答が受信されない場合、ポート チャネル内のポートは中断状態に移動されます。

LACP モード

LACP モードでは、ポートが LACP パケットを送信できるか、LACP パケットの受信のみができるかどうかを指定します。

表 *60 : EtherChannel LACP* モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。これにより、LACP パケットの送信を最小限に抑えます。

active モードおよび **passive LACP** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

LACP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** モードまたは **passive** モードの別のポートとともに EtherChannel を形成できます。
- 両ポートとも LACP ネゴシエーションを開始しないため、**passive** モードのポートは、**passive** モードの別のポートと EtherChannel を形成することはできません。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （979 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）

LACP とリンクの冗長性

LACP ポートチャネルの最小リンクおよびLACP の最大バンドルの機能を使用して、LACP ポートチャネル動作、帯域幅の可用性およびリンク冗長性をさらに高めることができます。

LACP ポートチャネルの最小リンク機能：

- LACP ポート チャネルでリンクし、バンドルする必要があるポートの最小数を設定します。
- 低帯域幅の LACP ポート チャネルがアクティブにならないようにします。
- 必要な最低帯域幅を提供する十分なアクティブ メンバ ポートがない場合、LACP ポートチャネルが非アクティブになるようにします。

LACP の最大バンドル機能：

- LACP ポート チャネルのバンドル ポートの上限数を定義します。
- バンドル ポートがより少ない場合のホット スタンバイ ポートを可能にします。たとえば、5 個のポートがある LACP ポート チャネルで、3 個の最大バンドルを指定し、残りの 2 個のポートをホット スタンバイ ポートとして指定できます。

関連トピック

LACP 最大バンドル機能の設定（CLI） （990 ページ）
LACP ホット スタンバイ ポートの設定：例 （1001 ページ）
LACP ポート チャネルの最小リンク機能の設定（CLI） （991 ページ）

LACP と他の機能との相互作用

DTP および CDP は、EtherChannel の物理ポートを介してパケットを送受信します。トランクポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。レイヤ 3 EtherChannel の場合は、**interface port-channel** グローバル コンフィギュレーション コマンドでインターフェイスが作成された直後に、アクティブなデバイスによって MAC アドレスが割り当てられます。

LACP が LACP PDU を送受信するのは、LACP が active モードまたは passive モードでイネーブルになっている稼働状態のポートとの間だけです。

EtherChannel の On モード

EtherChannel の **on** モードは、EtherChannel の手動設定に使用します。**on** モードを使用すると、ポートはネゴシエーションせずに強制的に EtherChannel に参加します。リモート デバイスが PAgP や LACP をサポートしていない場合にこの **on** モードが役立ちます。**on** モードでは、リンクの両端のデバイスが **on** モードに設定されている場合のみ EtherChannel を使用できます。

同じチャネル グループの **on** モードで設定されたポートは、速度やデュプレックスのようなポート特性に互換性を持たせる必要があります。**on** モードで設定されている場合でも、互換性のないポートは suspended ステートになります。

注意 **on** モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパニングツリー ループが発生することがあります。

ロードバランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル内の 1 つのリンクを選択する数値に縮小することによって、チャネル内のリンク間でトラフィックのロード バランシングを行います。MAC アドレス、IP アドレス、送信元アドレス、宛先アドレス、または送信元と宛先両方のアドレスに基づいた負荷分散など、複数の異なるロードバランシング モードから 1 つを指定できます。選択したモードは、デバイス上で設定されているすべての EtherChannel に適用されます。

（注） レイヤ 3 等コスト マルチ パス（ECMP）のロード バランシングは、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびレイヤ 4 プロトコルに基づいています。フラグメント化されたパケットは、これらのパラメータを使用して計算されたアルゴリズムに基づいて 2 つの異なるリンクで処理されます。これらのパラメータのいずれかを変更すると、ロード バランシングが実行されます。

グローバル コンフィギュレーション コマンド **port-channel load-balance** および **port-channel load-balance extended** を使用して、ロードバランシングおよび転送方式を設定します。

関連トピック

EtherChannel ロードバランシングの設定（CLI） （985 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （977 ページ）

MAC アドレス転送

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、ロード バランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャネル ポートを使用しますが、送信元ホストが同じパケットは同じチャネル ポートを使用します。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先ホストの MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、宛先が同

じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネルポートに転送されます。

送信元および宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャネル ポート間で分配されます。この転送方式は、負荷分散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のデバイスに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のどちらが適切であるかが不明な場合に使用できます。送信元および宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

EtherChannel ロードバランシングの設定（CLI） （985 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （977 ページ）

IP アドレス転送

送信元 IP アドレスベース転送の場合、パケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。ロード バランシングを行うために、IP アドレスが異なるパケットはチャネルでそれぞれ異なるポートを使用しますが、IP アドレスが同じパケットはチャネルで同じポートを使用します。

宛先 IP アドレスベース転送の場合、パケットは着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。ロード バランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、チャネルの異なるチャネル ポートに送信できます。異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常にチャネルの同じポートに送信されます。

送信元と宛先 IP アドレスベース転送の場合、パケットは着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたもので、特定のデバイスに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切であるか不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

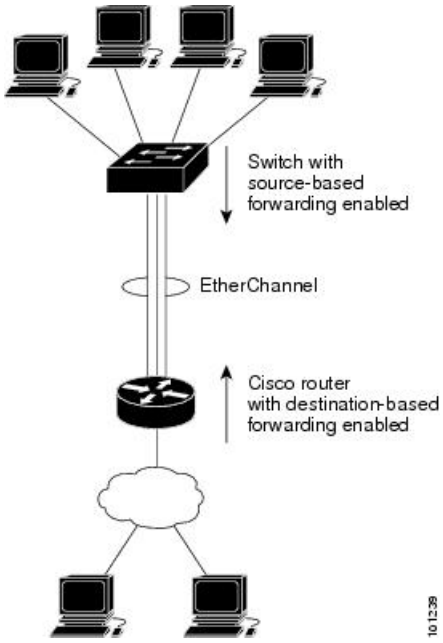
EtherChannel ロードバランシングの設定（CLI） （985 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （977 ページ）

ロードバランシングの利点

ロードバランシング方式には異なる利点があるため、ネットワーク内のデバイスの位置、および負荷分散が必要なトラフィックの種類に基づいて特定のロードバランシング方式を選択する必要があります。

図 *65 :* 負荷の分散および転送方式

次の図では、4 台のワーク ステーションの EtherChannel がルータと通信します。ルータは単一 MAC アドレス デバイスであるため、デバイス EtherChannel で送信元ベース転送を行うことにより、デバイスが、ルータで使用可能なすべての帯域幅を使用することが保証されます。ルータは、宛先アドレスベース転送を行うように設定されます。これは、多数のワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっているためです。



設定で一番種類が多くなるオプションを使用してください。たとえば、チャネル上のトラフィックが単一 MAC アドレスを宛先とする場合、宛先 MAC アドレスを使用すると、チャネル内の同じリンクが常に選択されます。ただし、送信元アドレスまたはIPアドレスを使用した方が、ロードバランシングの効率がよくなる場合があります。

関連トピック

EtherChannel ロードバランシングの設定（CLI） （985 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （977 ページ）

EtherChannel およびデバイス スタック

EtherChannel に加入しているポートが含まれているスタック メンバに障害が発生したり、スタックを離れると、アクティブなデバイスにより、障害が発生したスタック デバイス メンバポートが削除されます。EtherChannel に残っているポートがある場合、接続は引き続き確保されます。

デバイスが既存のスタックに追加されると、新しいデバイスがアクティブなデバイスから実行コンフィギュレーションを受信し、EtherChannel 関連のスタック コンフィギュレーションで更新されます。スタック メンバでは、動作情報（動作中で、チャネルのメンバであるポートのリスト）も受信します。

2 つのスタック間で設定されている EtherChannel がマージされた場合、セルフループ ポートになります。スパニングツリーにより、この状況が検出され、必要な動作が発生します。権利を獲得したデバイス スタックにある PAgP 設定または LACP 設定は影響を受けませんが、権利を失った デバイス スタックの PAgP 設定または LACP 設定は、スタックのリブート後に失われます。

デバイス スタックおよび PAgP

PAgP では、アクティブ デバイスに障害が発生するか、スタックを離れた場合、スタンバイ デバイスが新しいアクティブデバイスになります。EtherChannel 帯域幅に変更がない場合、スパニングツリーの再コンバージェンスはトリガーされません。新しいアクティブデバイスはアクティブデバイスの該当項目にスタック メンバの設定を同期します。PAgP 設定は、EtherChannel に古いアクティブ デバイス上にあるポートがない限り、アクティブ デバイスの変更後も影響を受けません。

デバイス スタックおよび LACP

LACP の場合、システム ID は、アクティブ デバイスから取得したスタック MAC アドレスが使用されます。アクティブ デバイスに障害が発生したり、スタックを離れ、スタンバイ デバイスが新しいアクティブ デバイスが変更になっても、LACP システム ID は変更されません。デフォルトでは、LACP 設定はアクティブ デバイスの変更後も影響を受けません。

EtherChannel のデフォルト設定

EtherChannel のデフォルト設定を、次の表に示します。

表 *61 : EtherChannel* のデフォルト設定

機能	デフォルト設定
チャネル グループ	割り当てなし
ポートチャネル論理インターフェイス	未定義
PAgP モード	デフォルトなし。

機能	デフォルト設定
PAgP 学習方式	すべてのポートで集約ポート ラーニング
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし。
LACP 学習方式	すべてのポートで集約ポート ラーニング
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768
LACP システム ID	LACP システムのプライオリティ、デバイスまたはスタックの MAC アドレス。
ロード バランシング	デバイス上での負荷分散は着信パケットの送信元MAC アドレスに基づきます。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （979 ページ）
EtherChannel の概要 （960 ページ）
EtherChannel のモード （961 ページ）
デバイス上の EtherChannel （961 ページ）
EtherChannel リンクのフェールオーバー （962 ページ）
LACP モード （968 ページ）
PAgP モード （965 ページ）
サイレント モード （966 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
チャネル グループおよびポートチャネル インターフェイス （963 ページ）
物理インターフェイスの設定（CLI）
EtherChannel ロードバランシングの設定（CLI） （985 ページ）
ロードバランシングおよび転送方式 （970 ページ）
MAC アドレス転送 （970 ページ）
IP アドレス転送 （971 ページ）
ロードバランシングの利点 （972 ページ）
PAgP 学習方式およびプライオリティの設定 （CLI） （988 ページ）
PAgP 学習方式およびプライオリティ （966 ページ）
LACP システム プライオリティの設定（CLI） （992 ページ）
LACP ポート プライオリティの設定（CLI） （993 ページ）

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワーク ループおよびその他の問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。設定上の問題を回避するために、次の注意事項に従ってください。

- デバイスまたはデバイス スタック上では、128 を超える EtherChannel を設定しないでください。
- PAgP EtherChannel は、同じタイプのイーサネット ポートを 8 つまで使用して設定します。
- 同じタイプのイーサネット ポートを最大で 16 個備えた LACP EtherChannel を設定してください。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックス モードで動作するように設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。**shutdown** インターフェイス コンフィギュレーション コマンドによってディセーブルにされた EtherChannel 内のポートは、リンク障害として扱われます。そのポートのトラフィックは、EtherChannel 内の他のポートの 1 つに転送されます。
- グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかで設定を変更した場合は、グループ内のすべてのポートでも変更する必要があります。
  - 許可 VLAN リスト
  - 各 VLAN のスパニングツリー パス コスト
  - 各 VLAN のスパニングツリー ポート プライオリティ
  - スパニングツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバになるように設定しないでください。
- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP を実行している EtherChannel グループはスタックの同一デバイス、または異なるデバイスで共存できます。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。
- EtherChannel の一部としてセキュア ポートを設定したり、セキュア ポートの一部として EtherChannel を設定したりしないでください。
- アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。
- EtherChannel がデバイス インターフェイス上に設定されている場合、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、IEEE 802.1x

をデバイス上でグローバルにイネーブルにする前に、EtherChannel の設定をインターフェイスから削除します。

- クロススタック EtherChannel が設定されていると、デバイス スタック パーティション、ループおよび転送の問題が発生する可能性があります。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （979 ページ）
EtherChannel の概要 （960 ページ）
EtherChannel のモード （961 ページ）
デバイス上の EtherChannel （961 ページ）
EtherChannel リンクのフェールオーバー （962 ページ）
LACP モード （968 ページ）
PAgP モード （965 ページ）
サイレント モード （966 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
チャネル グループおよびポートチャネル インターフェイス （963 ページ）
物理インターフェイスの設定（CLI）
EtherChannel ロードバランシングの設定（CLI） （985 ページ）
ロードバランシングおよび転送方式 （970 ページ）
MAC アドレス転送 （970 ページ）
IP アドレス転送 （971 ページ）
ロードバランシングの利点 （972 ページ）
PAgP 学習方式およびプライオリティの設定 （CLI） （988 ページ）
PAgP 学習方式およびプライオリティ （966 ページ）
LACP システム プライオリティの設定（CLI） （992 ページ）
LACP ポート プライオリティの設定（CLI） （993 ページ）

レイヤ 2 EtherChannel 設定時の注意事項

レイヤ 2 EtherChannels を設定する場合は、次の注意事項に従ってください。

- EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。
- EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。VLAN 許容範囲が一致していないと、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
- スパニングツリー パス コストが異なるポートは、設定上の矛盾がない限り、EtherChannel を形成できます。異なるスパニングツリー パス コストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （979 ページ）
EtherChannel の概要 （960 ページ）
EtherChannel のモード （961 ページ）
デバイス上の EtherChannel （961 ページ）
EtherChannel リンクのフェールオーバー （962 ページ）
LACP モード （968 ページ）
PAgP モード （965 ページ）
サイレント モード （966 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
チャネル グループおよびポートチャネル インターフェイス （963 ページ）
物理インターフェイスの設定（CLI）
EtherChannel ロードバランシングの設定（CLI） （985 ページ）
ロードバランシングおよび転送方式 （970 ページ）
MAC アドレス転送 （970 ページ）
IP アドレス転送 （971 ページ）
ロードバランシングの利点 （972 ページ）
PAgP 学習方式およびプライオリティの設定 （CLI） （988 ページ）
PAgP 学習方式およびプライオリティ （966 ページ）
LACP システム プライオリティの設定（CLI） （992 ページ）
LACP ポート プライオリティの設定（CLI） （993 ページ）

レイヤ 3 EtherChannel 設定時の注意事項

- レイヤ 3 EtherChannel の場合は、レイヤ 3 アドレスをチャネル内の物理ポートでなく、ポートチャネル論理インターフェイスに割り当ててください。

関連トピック

EtherChannel ロードバランシングの設定（CLI） （985 ページ）
ロードバランシングおよび転送方式 （970 ページ）
MAC アドレス転送 （970 ページ）
IP アドレス転送 （971 ページ）
ロードバランシングの利点 （972 ページ）

Auto-LAG

Auto-LAG 機能は、スイッチに接続されたポートで EtherChannel を自動的に作成できる機能です。デフォルトでは、Auto-LAG がグローバルに無効にされ、すべてのポート インターフェイスで有効になっています。Auto-LAG は、グローバルに有効になっている場合にのみ、スイッチに適用されます。

Auto-LAG をグローバルに有効にすると、次のシナリオが可能になります。

- パートナー ポート インターフェイス上に EtherChannel が設定されている場合、すべてのポートインターフェイスが自動 EtherChannel の作成に参加します。詳細については、次の表「アクターとパートナー デバイス間でサポートされる *Auto-LAG* 設定」を参照してください。
- すでに手動 EtherChannel の一部であるポートは、自動 EtherChannel の作成に参加することはできません。
- Auto-LAG がすでに自動で作成された EtherChannel の一部であるポート インターフェイスで無効になっている場合、ポートインターフェイスは自動 EtherChannel からバンドル解除されます。

次の表に、アクターとパートナー デバイス間でサポートされる Auto-LAG 設定を示します。

表 *62*：アクターとパートナー デバイス間でサポートされる *Auto-LAG* 設定

アクター/パートナー	**Active**	**Passive**	自動
Active	Yes	Yes	Yes
Passive	Yes	いいえ	Yes
自動	Yes	Yes	Yes

Auto-LAG をグローバルに無効にすると、自動で作成されたすべての Etherchannel が手動 EtherChannel になります。

既存の自動で作成された EtherChannel で設定を追加することはできません。追加するには、最初に **port-channel**<*channel-number*>**persistent** を実行して、手動 EtherChannel に変換する必要があります。

（注） Auto-LAG は自動 EtherChannel の作成に LACP プロトコルを使用します。一意のパートナー デバイスで自動的に作成できる EtherChannel は 1 つだけです。

Auto-LAG 設定時の注意事項

Auto-LAG 機能を設定するときには、次の注意事項に従ってください。

- Auto-LAG がグローバルで有効な場合、およびポート インターフェイスで有効な場合に、ポート インターフェイスを自動 EtherChannel のメンバーにしたくない場合は、ポート インターフェイスで Auto-LAG を無効にします。
- ポート インターフェイスは、すでに手動 EtherChannel のメンバーである場合、自動 EtherChannel にバンドルされません。自動 EtherChannel にバンドルされるようにするには、まずポート インターフェイスで手動 EtherChannel のバンドルを解除します。

- Auto-LAG が有効になり、自動 EtherChannel が作成されると、同じパートナー デバイスで複数の EtherChannel を手動で作成できます。ただし、デフォルトでは、ポートはパートナー デバイスで自動 EtherChannel の作成を試行します。
- Auto-LAG は、レイヤ 2 EtherChannel でのみサポートされています。レイヤ 3 インターフェイスおよびレイヤ 3 EtherChannel ではサポートされていません。
- Auto-LAG は、Cross-Stack EtherChannel でサポートされています。

EtherChannel の設定方法

EtherChannel の設定後、ポートチャネルインターフェイスに適用した設定変更は、そのポートチャネルインターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。

レイヤ 2 EtherChannel の設定 （CLI）

レイヤ 2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャネル グループにポートを割り当てます。このコマンドにより、ポートチャネル論理インターフェイスが自動的に作成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスは、物理ポートです。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。

	コマンドまたはアクション	目的
ステップ 3	**switchport mode** {**access** | **trunk**} 例： `Device(config-if)# switchport mode access`	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセス ポートとして設定する場合は、ポートを1つの VLANにのみ割り当ててください。指定できる範囲は 1 ～ 4094 です。
ステップ 4	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 22`	ポートをスタティックアクセス ポートとして設定する場合は、ポートを1つの VLANにのみ割り当ててください。指定できる範囲は 1 ～ 4094 です。
ステップ 5	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive**} 例： `Device(config-if)# channel-group 5 mode auto`	チャネルグループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 *channel-group-number* の範囲は 1 ～ 128 です。 **mode** には、次のキーワードのいずれか 1 つを選択します。 • **auto**–PAgP 装置が検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。このキーワードは、EtherChannel メンバがデバイス スタックの異なるデバイスのものである場合にはサポートされません。 • **desirable**–無条件に PAgP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。このキーワードは、EtherChannel メンバがデバイス ス

	コマンドまたはアクション	目的
		タックの異なるデバイスのものである場合にはサポートされません。 • **on**–PAgP または LACP を使用せずにポートが強制的にチャネル化されます。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**–（任意）デバイスが PAgP 対応のパートナーに接続されている場合、ポートが **auto** または **desirable** モードになると非サイレント動作を行うようにデバイスポートを設定します。**non-silent** を指定しないと、サイレントが想定されます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。 • **active**：LACP 装置が検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートはLACPパケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive**–ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーションステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 6	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# end`	

関連トピック

EtherChannel の概要 （960 ページ）
EtherChannel のモード （961 ページ）
デバイス上の EtherChannel （961 ページ）
EtherChannel リンクのフェールオーバー （962 ページ）
LACP モード （968 ページ）
PAgP モード （965 ページ）
サイレント モード （966 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）

レイヤ 3 EtherChannel の設定 （CLI）

レイヤ 3 EtherChannel にイーサネット ポートを割り当てるには、この手順を実行します。この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。

	コマンドまたはアクション	目的
		PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 4	**no ip address** 例： `Device(config-if)# no ip address`	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 5	**noswitchport** 例： `Device(config-if)# no switchport`	ポートをレイヤ 3 モードにします。
ステップ 6	**channel-group** *channel-group-number* **mode** {**auto** ［**non-silent**］ ｜ **desirable** ［**non-silent**］ ｜ **on**} ｜ {**active** ｜ **passive**} 例： `Device(config-if)# channel-group 5 mode auto`	チャネルグループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 **mode** には、次のキーワードのいずれか 1 つを選択します。 • **auto**：PAgP 装置が検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。このキーワードは、EtherChannel メンバがデバイス スタックの異なるデバイスのものである場合にはサポートされません。 • **desirable**：無条件に PAgP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開

	コマンドまたはアクション	目的
		始します。このキーワードは、EtherChannel メンバがデバイス スタックの異なるデバイスのものである場合にはサポートされません。 • **on**：PAgP や LACP を使用しないで、ポートを強制的にチャネル化します。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**：（任意）デバイスが PAgP 対応のパートナーに接続されている場合、ポートが **auto** または **desirable** モードになると非サイレント動作を行うようにデバイス ポートを設定します。**non-silent** を指定しないと、サイレントが想定されます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。 • **active**：LACP 装置が検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートはLACPパケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive**–ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーションステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

EtherChannel ロードバランシングの設定（CLI）

複数の異なる転送方式の 1 つを使用するように EtherChannel ロードバランシングを設定できます。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance** {**dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **extended** [**dst-ip** | **dst-mac** | **dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] | **src-dst-ip** | **src-dst-mac src-dst-mixed-ip-port src-dst-portsrc-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**} 例： `Device(config)# port-channel load-balance src-mac`	EtherChannel のロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **dst-mixed-ip-port**：ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **dst-port**：宛先 TCP/UDP ポートを指定します。 • **extended**：標準コマンドで使用可能なもの以外に、送信元および宛先の方式を組み合わせた、拡張ロードバランシング方式を指定します。

	コマンドまたはアクション	目的
		• **ipv6-label**：IPv6 フロー ラベルを指定します。 • **l3-proto**：レイヤ 3 プロトコルを指定します。 • **src-dst-ip**：送信元および宛先ホストの IP アドレスを指定します。 • **src-dst-mac**：送信元および宛先ホストの MAC アドレスを指定します。 • **src-dst-mixed-ip-port**：送信先および宛先ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **src-dst-port**：送信元および宛先 TCP/UDP ポートを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。 • **src-mac**：着信パケットの送信元 MAC アドレスを指定します。 • **src-mixed-ip-port**：送信元ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **src-port**：送信元 TCP/UDP ポートを指定します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ロードバランシングおよび転送方式 （970 ページ）
MAC アドレス転送 （970 ページ）
IP アドレス転送 （971 ページ）
ロードバランシングの利点 （972 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）
EtherChannel のデフォルト設定 （973 ページ）

レイヤ 3 EtherChannel 設定時の注意事項 （977 ページ）

EtherChannel 拡張ロードバランシングの設定（CLI）

ロードバランシング方式を組み合わせて使用する場合には、拡張ロードバランシングを設定します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance extended** ［**dst-ip** ｜ **dst-macdst-port** ｜ **ipv6-label** ｜ **l3-proto** ｜ **src-ip** ｜ **src-mac** ｜ **src-port** ］ 例： `Device(config)# port-channel load-balance extended dst-ip dst-mac src-ip`	EtherChannel 拡張ロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **dst-port**：宛先 TCP/UDP ポートを指定します。 • **ipv6-label**：IPv6 フロー ラベルを指定します。 • **l3-proto**：レイヤ 3 プロトコルを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。 • **src-mac**：着信パケットの送信元 MAC アドレスを指定します。 • **src-port**：送信元 TCP/UDP ポートを指定します。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

PAgP 学習方式およびプライオリティの設定 （CLI）

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	伝送ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**pagp learn-methodphysical-port** 例： `Device(config-if)# pagp learn-method physical port`	PAgP 学習方式を選択します。 デフォルトでは、**aggregation-port learning** が選択されています。つまり、EtherChannel 内のポートのいずれかを使用して、デバイスがパケットを送信元に送信します。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。 物理ポートラーナー `is`別のデバイスに接続する**physical-port**を選択します。**port-channel load-balance** グローバル コンフィギュレーション コマンドを **src-mac** に設定してください。 学習方式はリンクの両端で同じ方式に設定する必要があります。

	コマンドまたはアクション	目的
ステップ 4	**pagp port-priority** *priority* 例： `Device(config-if)# pagp port-priority 200`	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 *priority* に指定できる範囲は 0 ～ 255 です。デフォルト値は128 です。プライオリティが高いほど、ポートが PAgP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

PAgP 学習方式およびプライオリティ （966 ページ）
EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （999 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）

LACP ホット スタンバイ ポートの設定

LACP がイネーブルの場合、ソフトウェアはデフォルトで、チャネルにおける LACP 互換ポートの最大数（最大 16 個のポート）の設定を試みます。一度にアクティブにできる LACP リンクは 8 つだけです。残りの 8 個のリンクがホット スタンバイ モードになります。アクティブリンクの 1 つが非アクティブになると、ホット スタンバイ モードのリンクが代わりにアクティブになります。

チャネルでアクティブ ポートの最大数を指定することでデフォルト動作を上書きできます。この場合、残りのポートがホット スタンバイ ポートになります。たとえばチャネルで最大 5 個のポートを指定した場合、11 個までのポートがホット スタンバイ ポートになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリティに基づいてアクティブにするホット スタンバイ ポートを決定します。ソフトウェアは、LACP を操作するシステム間のすべてのリンクに、次の要素（プライオリティ順）で構成された一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID（デバイス MAC アドレス）
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。プライオリティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバイ モードにするポートを決定します。

アクティブ ポートかホット スタンバイ ポートかを判別するには、次の（2 つの）手順を使用します。まず、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。次に、ポートプライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートとホット スタンバイ ポートを決定します。他のシステムのポート プライオリティとポート番号の値は使用されません。

ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響を与えるように、LACP システムプライオリティおよびLACPポートプライオリティのデフォルト値を変更できます。

LACP 最大バンドル機能の設定（CLI）

ポート チャネルで許可されるバンドル化された LACP ポートの最大数を指定すると、ポート チャネル内の残りのポートがホット スタンバイ ポートとして指定されます。

ポート チャネルの LACP ポートの最大数を設定するには、特権 EXEC モードで開始して、次の手順に従います。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *channel-number* 例： `Device(config)# interface port-channel 2`	ポート チャネルのインターフェイス コンフィギュレーション モードを開始します。 指定できる範囲は 1 ～ 128 です。
ステップ 3	**lacp max-bundle** *max-bundle-number* 例： `Device(config-if)# lacp max-bundle 3`	ポートチャネル バンドルで LACP ポートの最大数を指定します。 指定できる範囲は 1 ～ 8 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

LACP とリンクの冗長性 （969 ページ）
LACP ホット スタンバイ ポートの設定：例 （1001 ページ）

LACP ポートチャネル スタンドアロン ディセーブルの設定

ポート チャネルのスタンドアロン EtherChannel メンバー ポート ステートをディセーブルにするには、ポート チャネル インターフェイスで次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *channel-group* 例： `Device(config)# interface port-channel channel-group`	設定するポート チャネル インターフェイスを選択します。
ステップ 3	**port-channel standalone-disable** 例： `Device(config-if)# port-channel standalone-disable`	ポートチャネル インターフェイスのスタンドアロン モードをディセーブルにします。
ステップ 4	**end** 例： `Device(config-if)# end`	設定モードを終了します。

ステップ 5	**show etherchannel**
	例：
	`Device# show etherchannel channel-group port-channel`
	`Device# show etherchannel channel-group detail`
		設定を確認します。

LACP ポート チャネルの最小リンク機能の設定（CLI）

リンク アップ状態で、リンク アップ ステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるアクティブ ポートの最小数を指定できます。EtherChannel の最小リンクを使用して、低帯域幅 LACP EtherChannel がアクティブになることを防止できます。また、LACP EtherChannel にアクティブ メンバー ポートが少なすぎて、必要な最低帯域幅を提供できない場合、この機能により LACP EtherChannel が非アクティブになります。

ポート チャネルに必要なリンクの最小数を設定する。次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel** *channel-number* 例： `Device(config)# interface port-channel 2`	ポートチャネルのインターフェイス コンフィギュレーション モードを開始します。 *channel-number* の範囲は 1 ～ 63 です。
ステップ 4	**port-channel min-links** *min-links-number* 例： `Device(config-if)# port-channel min-links 3`	リンク アップ状態で、リンク アップ ステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるメンバ ポートの最小数を指定できます。 *min-links-number* の範囲は 2 ～ 8 です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

LACP とリンクの冗長性 （969 ページ）
LACP ホット スタンバイ ポートの設定：例 （1001 ページ）

LACP システム プライオリティの設定（CLI）

lacp system-priority グローバル コンフィギュレーション コマンドを使用して、LACP をイネーブルにしているすべての EtherChannel に対してシステム プライオリティを設定できます。LACP を設定済みの各チャネルに対しては、システム プライオリティを設定できません。デフォルト

値を変更すると、ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響します。

show etherchannel summary 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが H になっています）。

LACP システム プライオリティを設定するには、次の手順に従います。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lacp system-priority** *priority* 例： `Device(config)# lacp system-priority 32000`	LACP システム プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。デフォルトは 32768 です。 値が小さいほど、システム プライオリティは高くなります。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （999 ページ）

LACP ポート プライオリティの設定（CLI）

デフォルトでは、すべてのポートは同じポート プライオリティです。ローカル システムのシステム プライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP

EtherChannel ポートのポートプライオリティをデフォルトよりも小さな値に変更して、最初にアクティブになるホットスタンバイ リンクを変更できます。ホット スタンバイ ポートは、番号が小さい方が先にチャネルでアクティブになります。**show etherchannel summary** 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが H になっています）。

（注） LACP がすべての互換ポートを集約できない場合（たとえば、ハードウェアの制約が大きいリモート システム）、EtherChannel 中でアクティブにならないポートはすべてホット スタンバイ ステートになり、チャネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP ポート プライオリティを設定するには、次の手順に従います。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lacp port-priority** *priority* 例： `Device(config-if)# lacp port-priority 32000`	LACP ポート プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。デフォルトは 32768 です。値が小さいほど、ポートが LACP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# end`	

関連トピック

EtherChannel 設定時の注意事項 （975 ページ）
EtherChannel のデフォルト設定 （973 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （976 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （999 ページ）

LACP 高速レート タイマーの設定

LACP タイマー レートを変更することにより、LACP タイムアウトの時間を変更することができます。**lacp rate** コマンドを使用すれば、LACP がサポートされているインターフェイスで受信される LACP 制御パケットのレートを設定できます。タイムアウト レートは、デフォルトのレート（30秒）から高速レート（1秒）に変更することができます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* 例： `Device(config)# interface gigabitEthernet 2/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**lacp rate**{**normal** | **fast**} 例： `Device(config-if)# lacp rate fast`	LACP がサポートされているインターフェイスで受信される LACP 制御パケットのレートを設定します。 • タイムアウト レートをデフォルトにリセットするには、**no lacp rate** コマンドを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 6	**show lacp internal**
	例：
	`Device# show lacp internal`
	`Device# show lacp counters`
		設定を確認します。

グローバルな Auto-LAG の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**] **port-channel auto** 例： `Device(config)# port-channel auto`	スイッチ上の Auto-LAG 機能をグローバルで有効にします。スイッチ上の Auto-LAG 機能をグローバルで無効にするには、このコマンドの no 形式を使用します。

	コマンドまたはアクション	目的
		（注） デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show etherchannel auto** 例： `Device# show etherchannel auto`	EtherChannel が自動的に作成されたことが表示されます。

ポート インターフェイスでの Auto-LAG の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	Auto-LAG を有効にするポート インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	[**no**] **channel-group auto** 例： `Device(config-if)# channel-group auto`	（任意）個々のポート インターフェイスで Auto-LAG 機能を有効にします。個々のポート インターフェイス上で Auto-LAG 機能を無効にするには、このコマンドの no 形式を使用します。 （注） デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show etherchannel auto** 例： `Device# show etherchannel auto`	EtherChannel が自動的に作成されたことが表示されます。

次のタスク

Auto-LAG での持続性の設定

自動で作成された EtherChannel を手動のものに変更し、既存の EtherChannel に設定を追加するには、persistence コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**port-channel** *channel-number***persistent** 例： `Device# port-channel 1 persistent`	自動で作成された EtherChannel を手動のものに変更し、EtherChannel に設定を追加することができます。
ステップ 3	**show etherchannel summary** 例： `Device# show etherchannel summary`	EtherChannel 情報を表示します。

EtherChannel、PAgP、および LACP ステータスのモニタ

この表に記載されているコマンドを使用して EtherChannel、PAgP、および LACP ステータスを表示できます。

表 *63 : EtherChannel、PAgP、および LACP* ステータスのモニタ用コマンド

コマンド	説明
clear lacp { *channel-group-number* **counters** | **counters**}	LACP チャネル グループ情報およびトラフィック カウンタをクリアします。
clear pagp { *channel-group-number* **counters** | **counters**}	PAgP チャネル グループ情報およびトラフィック カウンタをクリアします。
show etherchannel [*channel-group-number* {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}] [**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **auto** | **summary**]	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。負荷分散方式またはフレーム配布方式、ポート、ポート チャネル、プロトコル、および Auto-LAG 情報も表示されます。
show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 PAgP 設定、ネイバー情報などの PAgP 情報が表示されます。
show pagp [*channel-group-number*] **dual-active**	デュアルアクティブ検出ステータスが表示されます。
show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**}	トラフィック情報、内部 LACP 設定、ネイバー情報などの LACP 情報が表示されます。
show running-config	設定エントリを確認します。
show etherchannel load-balance	ポート チャネル内のポート間のロードバランシング、またはフレーム配布方式を表示します。

関連トピック

PAgP 学習方式およびプライオリティの設定 （CLI） （988 ページ）
PAgP 学習方式およびプライオリティ （966 ページ）
LACP システム プライオリティの設定（CLI） （992 ページ）
LACP ポート プライオリティの設定（CLI） （993 ページ）

EtherChannel の設定例

レイヤ 2 EtherChannel の設定：例

この例では、スタック内の 1 つのデバイスに EtherChannel を設定する例を示します。2 つのポートを VLAN 10 のスタティック アクセス ポートとして、PAgP モードが **desirable** であるチャネル 5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode desirable non-silent
Device(config-if-range)# end
```

この例では、スタック内の 1 つのデバイスに EtherChannel を設定する例を示します。2 つのポートは VLAN 10 のスタティックアクセス ポートとして、LACP モードが active であるチャネル 5 に割り当てられます。 **active：**

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

次の例では、クロススタック EtherChannel を設定する方法を示します。LACP パッシブ モードを使用して、VLAN 10 内のスタティックアクセス ポートとしてスタック メンバ 1 のポートを 2 つ、スタック メンバ 2 のポートを 1 つチャネル 5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/4 -5
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode passive
Device(config-if-range)# exit
Device(config)# interface gigabitethernet3/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 10
Device(config-if)# channel-group 5 mode passive
Device(config-if)# exit
```

PoE または LACP ネゴシエーションのエラーは、スイッチからアクセスポイント（AP）に 2 つのポートを設定した場合に発生する可能性があります。このシナリオは、ポートチャネルの設定をスイッチ側で行うと回避できます。詳細については、次の例を参照してください。

```
interface Port-channel1
  switchport access vlan 20
```

```
switchport mode access
 switchport nonegotiate
 no port-channel standalone-disable   <--this one
 spanning-tree portfast
```

（注） ポートがポートのフラッピングに関するLACPエラーを検出した場合は、次のコマンドも含める必要があります。 **no errdisable detect cause pagp-flap**

レイヤ 3 EtherChannel の設定：例

この例では、レイヤ 3 インターフェイスの設定方法を示します。2 つのポートは、LACP モードが **active** であるチャネル 5 に割り当てられます。

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# no ip address
Device(config-if-range)# no switchport
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

この例では、クロススタック レイヤ 3 EtherChannel の設定方法を示します。スタック メンバー 2 の 2 つのポートとスタック メンバー 3 の 1 つのポートは、LACP active モードでチャネル 7 に割り当てられます。

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/4 -5
Device(config-if-range)# no ip address
Device(config-if-range)# no switchport
Device(config-if-range)# channel-group 7 mode active
Device(config-if-range)# exit
Device(config)# interface gigabitethernet3/0/3
Device(config-if)# no ip address
Device(config-if)# no switchport
Device(config-if)# channel-group 7 mode active
Device(config-if)# exit
```

LACP ホット スタンバイ ポートの設定：例

この例では、少なくとも 3 個のアクティブ ポートがある場合にアクティブ化される EtherChannel を設定する例を示します（ポート チャネル 2）。これは、7 個のアクティブ ポートとホット スタンバイ ポートとしての最大 9 個の残りのポートから構成されます。

```
Device# configure terminal
Device(config)# interface port-channel 2
```

```
Device(config-if)# port-channel min-links 3
Device(config-if)# lacp max-bundle 7
```

次に、ポート チャネル 42 のスタンドアロン EtherChannel メンバ ポート ステートをディセーブルにする例を示します。

```
Device(config)# interface port-channel channel-group
Device(config-if)# port-channel standalone-disable
```

次に、設定を確認する例を示します。

```
Device# show etherchannel 42 port-channel | include Standalone
Standalone Disable  = enabled
Device# show etherchannel 42 detail | include Standalone
Standalone Disable  = enabled
```

関連トピック

LACP 最大バンドル機能の設定（CLI） （990 ページ）
LACP とリンクの冗長性 （969 ページ）
LACP ポート チャネルの最小リンク機能の設定（CLI） （991 ページ）

Auto-LAG の設定：例

次に、スイッチに Auto-LAG を設定する例を示します。

```
デバイス> enable
デバイス# configure terminal
デバイス (config)# port-channel auto
デバイス (config-if)# end
デバイス#  show etherchannel auto
```

次の例は、自動的に作成された EtherChannel の概要を示します。

```
デバイス# show etherchannel auto
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SUA)        LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

次の例は、**port-channel** 1 **persistent** コマンドを実行した後の自動 EtherChannel の概要を示します。

```
デバイス# port-channel 1 persistent
```

```
デバイス# show etherchannel summary
Switch# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

EtherChannels の追加リファレンス

関連資料

関連項目	マニュアル タイトル
レイヤ 2 コマンド リファレンス	『*Layer 2/3 Command Reference (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

EtherChannels の機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。
Cisco IOS XE 3.3SE	LACP 最大バンドル機能、ポート チャネルの最小リンク機能のサポートが追加されました。
Cisco IOS 15.2(3)E2、Cisco IOS XE 3.7.2E	Auto-LAG 機能が導入されました。

第 48 章

Resilient Ethernet Protocol の設定

- 機能情報の確認 （1005 ページ）
- REP の概要 （1005 ページ）
- REP の設定方法 （1011 ページ）
- REP のモニタリング （1022 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

REP の概要

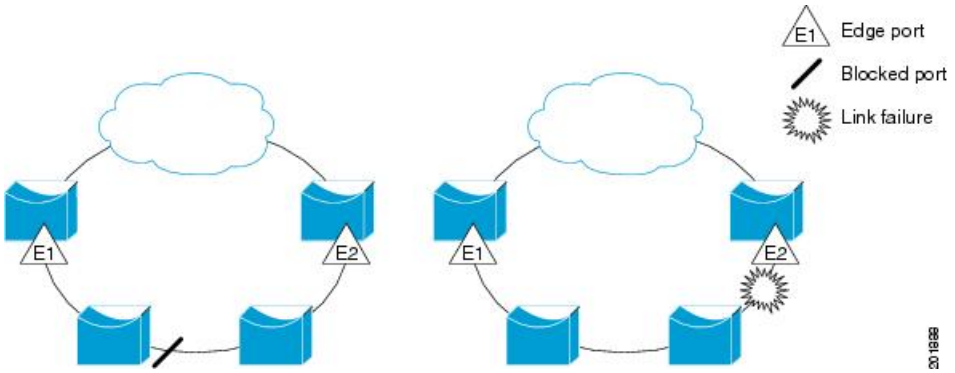
Resilient Ethernet Protocol（REP）はシスコ独自のプロトコルで、スパニングツリー プロトコル（STP）に代わるプロトコルとして、ネットワーク ループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジングループを作成するのを防ぎ、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。

（注） REP は IP Base および IP Services を実行している Catalyst スイッチでサポートされます。REP は LAN Base ライセンスではサポートされません。

REP セグメントは、相互接続されたポートのチェーンで、セグメント ID が設定されます。各セグメントは、標準（非エッジ）セグメント ポートと、2 つのユーザ設定エッジ ポートで構成されています。1 ルータは同じセグメントに属するポートを複数持たず、各セグメント ポートにある外部ネイバーは 1 つだけです。セグメントは共有メディアを通過できますが、どのリンクであっても同じセグメントに属することができるのは 2 ポートだけです。REP はトランクのイーサネット フロー ポイント（EFP）インターフェイスでのみサポートされます。

次の図に、4 つのスイッチにまたがる 6 つのポートで構成されているセグメントの例を示します。ポート E1 および E2 がエッジ ポートとして設定されています。（左側のセグメントのように）すべてのポートが動作可能の場合、斜線で表しているように単一ポートがブロックされます。ネットワークに障害が発生した場合、ブロックされたポートがフォワーディング ステートに戻り、ネットワークの中断を最小限に抑えます。

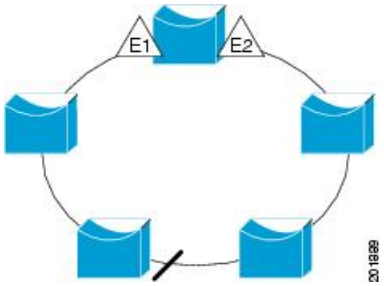
図 *66 : REP* オープン セグメント



上の図に示されたセグメントは、オープンセグメントで、2 つのエッジ ポート間は接続されていません。REP セグメントはブリッジング ループの原因とならないため、セグメント エッジを安全に任意のネットワークに接続できます。セグメント内のルータに接続されているすべてのホストには、エッジ ポートを通じて残りのネットワークに接続する方法が 2 つありますが、いつでもアクセス可能なのは 1 つだけです。いずれかのセグメントまたは REP セグメントのいずれかのポートに障害が発生した場合、REP はすべてのポートのブロックを解除し、他のゲートウェイ経由で接続できるようにします。

下の図に示すセグメントはリング セグメントであり、同じルータ上に両方のエッジ ポートがあります。この設定を使用すると、セグメント内の任意の 2 ルータ間で冗長接続を形成することができます。

図 *67 : REP* リング セグメント



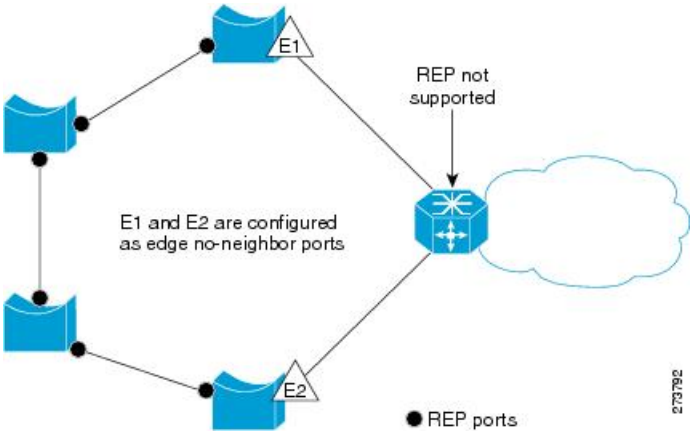
REP セグメントには、次のような特徴があります。

- セグメント内の全ポートが動作可能な場合、1 ポート（代替ポートと呼ばれる）が各 VLAN でブロック ステートとなります。VLAN ロード バランシングが設定されている場合は、セグメント内の 2 つのポートが VLAN のブロック ステートを制御します。
- セグメント内の 1 つまたは複数のポートが動作不能になると、リンク障害が発生して、すべてのポートがすべての VLAN トラフィックを転送して、接続性を確保します。
- リンク障害の場合、できるだけ早期に代替ポートのブロックが解除されます。障害リンクが復旧すると、ネットワークの中断を最小限に抑えるように VLAN 単位で論理的にブロックされたポートが選択されます。

REP セグメントに基づいて、ほとんどのネットワーク タイプを構成することができます。また REP はプライマリ エッジ ポートで制御され、セグメント内の任意のポートで発生する VLAN ロード バランシングをサポートします。

アクセス リング トポロジでは、下の図に示すように、ネイバー スイッチで REP がサポートされない場合があります。この場合、そのスイッチ側のポート（E1 と E2）を非ネイバー エッジ ポートとして設定できます。これらのポートは、エッジ ポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。たとえば、STP や REP のトポロジ変更通知を集約スイッチに送信するように設定することもできます。この場合、送信される STP トポロジ変更通知（TCN）は、Multiple Spanning-Tree（MST）STP メッセージです。

図 *68 :* 非ネイバー エッジ ポート



REP には次のような制限事項があります。

- 各セグメント ポートを設定する必要があります。設定を間違えると、ネットワーク内でフォワーディング ループが発生します。
- REP はセグメント内の単一障害ポートだけを管理できます。REP セグメント内の複数ポート障害の場合、ネットワークの接続が中断します。
- 冗長ネットワーク内だけに REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

リンク完全性

REP は、リンク完全性の確認にエッジ ポート間でエンドツーエンド ポーリング機能を使用しません。ローカル リンク障害検出を実装しています。REP リンク ステータス レイヤ（LSL）が REP 対応ネイバーを検出して、セグメント内の接続性を確立します。すべての VLAN は、ネイバーが検出されるまでインターフェイス上でブロックされます。ネイバーが特定されたあと、REP が代替ポートとなるネイバー ポートと、トラフィックを転送するポートを決定します。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポート ID フォーマットは、スパニングツリーアルゴリズムで使用されるものと類似しており、ポート番号（ブリッジ上で一意）と、関連 MAC アドレス（ネットワーク内で一意）から構成されます。セグメントポートが起動すると、ポートの LSL がセグメント ID およびポート ID を含むパケットの送信を開始します。ポートは、同じセグメント内のネイバーとのスリーウェイ ハンドシェイクを実行したあとで、動作可能と宣言されます。

次のような場合、セグメント ポートは動作可能になりません。

- ネイバーに同じセグメント ID がない
- 複数のネイバーに同じセグメント ID がある
- ネイバーがピアとして、ローカル ポートに確認応答しない

各ポートは、直近のネイバーと隣接関係を確立します。ネイバー関係が確立されると、ポートがセグメントの 1 つのブロックされたポート（代替ポート）を決定するようにネゴシエートします。その他のポートのブロックは解除されます。デフォルトで、REP パケットは BPDU クラス MAC アドレスに送信されます。パケットは、シスコ マルチキャスト アドレスにも送信できますが、セグメントに障害が発生した場合にブロックされたポートのアドバタイズ（BPA）メッセージの送信だけに使用されます。パケットは、REP が動作していない装置によって廃棄されます。

短時間でのコンバージェンス

REP は、物理リンク ベースで動作し、VLAN 単位ベースでは動作しません。すべての VLAN に対して 1 つの hello メッセージしか必要ないため、プロトコル上の負荷が軽減されます。指定セグメント内の全スイッチで継続的に VLAN を作成し、REP トランク ポート上に同じ許容 VLAN を設定することを推奨します。ソフトウェアでのメッセージのリレーによって発生する遅延を回避するために、REP ではいくつかのパケットを通常のマルチキャスト アドレスにフラッディングすることも可能です。これらのメッセージはハードウェア フラッド レイヤ（HFL）で動作し、REP セグメントだけではなくネットワーク全体にフラッディングされます。セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。ドメイン全体または特定のセグメントの管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

予想されるコンバージェンス復旧時間は、150 ～ 500 ms で、最大 1000 の MAC と 5 つの VLAN となります。マルチキャスト トラフィックの予想されるコンバージェンス復旧時間は、300 ～ 500 ms で、最大 100 のグループと 5 つの VLAN となります。

VLAN ロード バランシング

REP セグメント内の 1 つのエッジ ポートがプライマリ エッジ ポートとして機能し、もう一方がセカンダリ エッジ ポートとなります。セグメント内の VLAN ロード バランシングに常に参加しているのがプライマリ エッジ ポートです。REP VLAN バランシングは、設定された代替ポートでいくつかの VLAN をブロックし、プライマリ エッジ ポートでその他の全 VLAN をブロックすることで実行されます。VLAN ロード バランシングを設定する際に、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

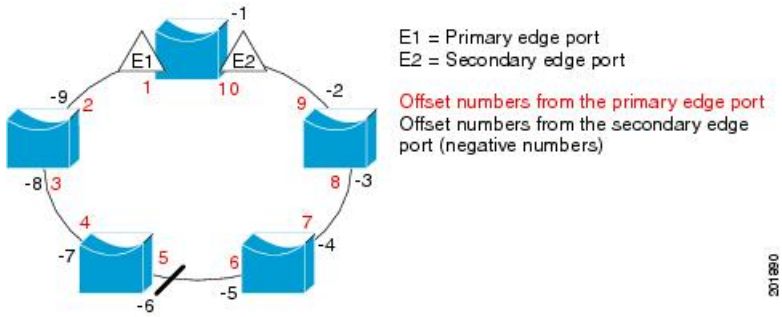
- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの **show interface rep** detail インターフェイス コンフィギュレーション コマンドを入力します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジ ポートのダウンストリーム ネイバー ポートを識別するものです。ネイバー オフセット番号の範囲は、-256 ～ +256 で、0 値は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負数は、セカンダリ エッジ ポート（オフセット番号 -1）とそのダウンストリーム ネイバーを示します。

（注） プライマリ（またはセカンダリ）エッジポートからポートのダウンストリーム位置を識別することで、プライマリ エッジ ポートのオフセット番号を設定します。番号 1 はプライマリ エッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

下の図に、E1 がプライマリ エッジ ポートで E2 がセカンダリ エッジ ポートの場合の、セグメントのネイバーオフセット番号を示します。リングの内側にある赤い番号は、プライマリエッジ ポートからのオフセット番号で、リングの外側にある黒い番号がセカンダリ エッジ ポートからのオフセット番号です。正のオフセット番号（プライマリ エッジ ポートからのダウンストリーム位置）または負のオフセット番号（セカンダリ エッジ ポートからのダウンストリーム位置）のいずれかにより、（プライマリ エッジ ポートを除く）全ポートを識別できます。E2 がプライマリ エッジ ポートになるとオフセット番号 1 となり、E1 のオフセット番号が -1 になります。

- **preferred** キーワードを入力します。これにより、**rep segment***segment-id***preferred** インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。

図 *69*：セグメント内のネイバー オフセット番号



REP セグメントが完了すると、すべての VLAN がブロックされます。VLAN ロード バランシングを設定する際には、次の 2 種類の方法のいずれかを使用してトリガーを設定する必要もあります。

- プライマリ エッジ ポートのあるスイッチ上で **rep preempt segment***segment-id* 特権 EXEC コマンドを入力することで、いつでも手動で VLAN ロード バランシングをトリガーすることができます。
- **rep preempt delay***seconds* インターフェイス コンフィギュレーション コマンドを入力すると、プリエンプション遅延時間を設定できます。リンク障害が発生して回復すると、設定されたプリエンプション期間の経過後に VLAN ロード バランシングが開始されます。設定時間が経過する前に別のポートで障害が発生した場合、遅延タイマーが再開されることに注意してください。

（注） VLAN ロード バランシングが設定されている場合、手動での介入またはリンク障害および回復によってトリガーされるまで、動作が開始されません。

VLAN ロード バランシングがトリガーされると、プライマリ エッジ ポートがメッセージを送信して、セグメント内の全インターフェイスにプリエンプションについて警告します。メッセージがセカンダリ ポートで受信されると、これがネットワークに反映され、メッセージ内で指定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジ ポートに通知します。

またすべての VLAN をブロックするために、セグメント内の特定ポートを設定できます。プライマリ エッジ ポートだけによって VLAN ロード バランシングが開始され、セグメントが各エンドでエッジ ポートによって終端されていない場合開始することができません。プライマリ エッジ ポートは、ローカル VLAN ロード バランシング設定を決定します。

ロード バランシングを再設定するには、プライマリ エッジ ポートを再設定します。ロード バランシング設定を変更すると、プライマリ エッジ ポートでは、再び **rep preempt segment** コマンドが実行されるか、ポート障害および復旧のあとで設定済みプリエンプト遅延期間が経過してから、新規設定が実行されます。エッジ ポートを通常セグメント ポートに変更しても、既存の VLAN ロード バランシング ステータスは変更されません。新規エッジ ポートを設定すると、新規トポロジ設定になる可能性があります。

スパニングツリー インタラクション

REP は、STP とも Flex Link 機能とも対話しませんが、どちらとも共存できます。セグメントに属しているポートはスパニングツリーの制御から削除されるため、セグメント ポートでは STP BPDU の送受信は行われません。したがって、STP はセグメント上で実行できません。

STP リング コンフィギュレーションから REP セグメント コンフィギュレーションに移行するには、まずリング内の単一ポートをセグメントの一部として設定し、次にセグメント数を最小限にするように隣接するポートを設定します。各セグメントには、常にブロックされたポートが含まれているので、セグメントが複数になるとブロックされたポートも複数になり、接続が失われる可能性があります。セグメントがエッジポートの場所まで両方向に設定されたら、次にエッジ ポートを設定します。

REP ポート

REP セグメントは、障害ポート、オープン ポート、および代替ポートで構成されます。

- 標準セグメント ポートとして設定されたポートは、障害ポートとして起動します。
- ネイバー との隣接関係が確立されると、ポートは代替ポート ステートに移行して、インターフェイス内の全 VLAN をブロックします。ブロックされたポートのネゴシエーションが発生して、セグメントが安定すると、ブロックされたポートのうちの 1 つが代替ロールのままになって他のすべてのポートがオープン ポートになります。
- リンク内に障害が発生すると、すべてのポートが障害ステートに移行します。代替ポートは、障害通知を受信すると、すべての VLAN を転送するオープン ステートに遷移します。

通常セグメント ポートをエッジ ポートに変換しても、エッジ ポートを通常セグメント ポートに変換しても、必ずトポロジ変更が発生するわけではありません。エッジポートを通常セグメント ポートに変更する場合、設定されるまで VLAN ロード バランシングは実装されません。VLAN ロード バランシングの場合、セグメント内に 2 つのエッジ ポートを設定する必要があります。

スパニングツリー ポートとして再設定されたセグメント ポートは、スパニングツリー設定に従って再起動します。デフォルトでは、これは指定ブロッキング ポートです。PortFast が設定されていたり、STP がディセーブルの場合、ポートはフォワーディング ステートになります。

REP の設定方法

セグメントは、チェーンで相互接続しているポートの集合で、セグメント ID が設定されています。REP セグメントを設定するには、REP 管理 VLAN を設定し（またはデフォルト VLAN 1 を使用し）、次にインターフェイス コンフィギュレーション モードを使用してセグメントにポートを追加します。2 つのエッジ ポートをセグメント内に設定して、1 つをプライマリ エッジ ポート、もう 1 つをデフォルトでセカンダリ エッジ ポートにします。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグ

メントのプライマリ エッジ ポートとして機能させます。オプションで、セグメント トポロジ変更通知（STCN）およびVLANロードバランシングを送信する場所を設定することもできます。

REP のデフォルト設定

REPはすべてのインターフェイス上でディセーブルです。イネーブルにする際に、エッジポートとして設定されていなければインターフェイスは通常セグメント ポートになります。

REPをイネーブルにする際に、STCNの送信はディセーブルで、すべてのVLANはブロックされ、管理 VLAN は VLAN 1 になります。

VLANロードバランシングがイネーブルの場合、デフォルトは手動でのプリエンプションで、遅延タイマーはディセーブルになっています。VLAN ロード バランシングが設定されていない場合、手動でのプリエンプション後のデフォルト動作は、プライマリ エッジ ポートで全 VLAN がブロックとなります。

REP 設定時の注意事項

REP の設定時には、次の注意事項に従ってください。

- まず1ポートの設定から始めて、セグメント数とブロックされたポートの数を最小限に抑えるように隣接するポートを設定することを推奨します。
- 外部ネイバーが設定されておらずセグメント内では3つ以上のポートに障害が発生した場合、1ポートがデータ パス用のフォワーディング ステートになり、設定中の接続性の維持に役立ちます。**showrepinterface** コマンド出力では、このポートのポート ロールは「Fail Logical Open」と表示され、他の障害ポートのポート ロールは「Fail No Ext Neighbor」と表示されます。障害ポートの外部ネイバーが設定されている場合、ポートは代替ポート ステートに移行して、代替ポート選択メカニズムに基づいて最終的にオープン ステートになるか、代替ポートのままになります。
- REP ポートは、レイヤ 2 IEEE 802.1Q またはトランク ポートのいずれかである必要があります。
- 同じ許可 VLAN のセットでセグメント内のすべてのトランク ポートを設定することを推奨します。
- Telnet接続を通じてREPを設定する際には注意してください。これは、別のREPインターフェイスがブロック解除のメッセージを送信するまで、REP はすべての VLAN をブロックするためです。同じインターフェイス経由でルータにアクセスする Telnet セッションで REP をイネーブルにすると、ルータへの接続が失われることがあります。
- REP と STP または REP と Flex Link を同じセグメントやインターフェイスで実行できません。
- STP ネットワークを REP セグメントに接続する場合、接続はセグメント エッジであることを確認してください。エッジで実行されていないSTP接続は、REPセグメントではSTP

が実行されないため、ブリッジング ループが発生する可能性があります。すべての STP BPDU は、REP インターフェイスで廃棄されます。

- 同じ許容 VLAN セットでセグメント内のすべてのトランク ポートを設定する必要があります。そうでない場合、設定ミスが発生します。
- REP がスイッチの 2 ポートでイネーブルの場合、両方のポートが通常セグメント ポートまたはエッジ ポートである必要があります。REP ポートは以下の規則に従います。
  - スイッチ上の REP ポートの数に制限はありませんが、同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
  - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジ ポートとなります。
  - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジポートであるか、両方のポートが通常セグメントポートであるか、一方が通常ポートでもう一方が非ネイバー エッジ ポートである必要があります。スイッチ上のエッジ ポートと通常セグメント ポートが同じセグメントに属することはできません。
  - スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジ ポートとして設定され、もう 1 つが通常セグメントポートに設定されている場合（設定ミス）、エッジ ポートは通常セグメント ポートとして扱われます。
- REPインターフェイスはブロックされた状態になり、ブロック解除できるようになるまでブロックされた状態のまま残ります。突然の接続切断を避けるために、このステータスを認識しておく必要があります。
- REP はネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。シスコ マルチキャスト アドレスに送信された BPA メッセージは、管理 VLAN で送信されます。これはデフォルトで VLAN 1 です。
- ネイバーからの hello が受信されないままどのくらいの時間が経過すると REP インターフェイスがダウンするかを設定できます。**rep lsl-age-timer** value インターフェイス コンフィギュレーション コマンドを使用して、120 ～ 10000 ミリ秒の時間を設定します。LSL hello タイマーは、このエージング タイマーの値を 3 で割った値に設定されます。通常の動作では、ピア スイッチのエージング タイマーが満了になって hello メッセージが確認されるまでに LSL hello が 3 回送信されます。
  - EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。ポート チャネルで 1000 ミリ秒未満の値を設定しようとすると、エラー メッセージが表示されてコマンドが拒否されます。
- REP ポートは、次のポート タイプのいずれかに設定できません。
  - スイッチド ポート アナライザ（SPAN）宛先ポート
  - トンネル ポート
  - Access port

- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別のポートではサポートされません。
- スイッチごとに最大 64 の REP セグメントを設定できます。

REP 管理 VLAN の設定

リンク障害によるソフトウェアでのメッセージのリレーやロード バランシング時の VLAN ブロッキング通知によって発生する遅延を回避するため、REP はハードウェア フラッド レイヤ（HFL）で通常のマルチキャストアドレスにパケットをフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。ドメイン全体または特定のセグメントの管理VLANを設定することで、これらのメッセージのフラッディングを制御することができます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- すべてのセグメントに対し 1 つの管理 VLAN をスイッチで設定するか、またはセグメントごとに管理 VLAN を設定できます。
- 管理 VLAN は RSPAN VLAN になりません。

REP 管理 VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**repadminvlan** *vlan-id***segment** *segment-id* 例： `Device(config)# rep admin vlan 2 segment 2`	管理 VLAN を指定します。指定できる範囲は 2 ～ 4094 です。デフォルトは VLAN 1 です。 セグメントごとに管理 VLAN を指定するには、グローバル コンフィギュレーション モードで **rep admin vlan** *vlan-id***segment** *segment-id* コマンドを入力します。 管理 VLAN を 1 に設定するには、**no rep admin vlan** グローバル コンフィギュレーション コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show interface** [*interface-id*] **rep detail** 例： `Device# show interface gigabitethernet1/1 rep detail`	REP インターフェイスのいずれか 1 つの設定を確認します。
ステップ 5	**copy running-config startup config** 例： `Device# copy running-config startup config`	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

REP インターフェイスの設定

REP 動作の場合、各セグメント インターフェイスで REP をイネーブルにして、セグメント ID を指定する必要があります。このタスクは必須で、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。その他のステップはすべて任意です。

インターフェイスで REP をイネーブルにし、設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。指定できるポートチャネルの範囲は 1 ～ 48 です。

	コマンドまたはアクション	目的
ステップ 4	**switchport mode trunk**	インターフェイスをレイヤ 2 トランクポートとして設定します。
ステップ 5	**repsegment** *segment-id* [**edge** [**no-neighbor**] [[**primary**]] [**preferred**]	インターフェイス上で REP をイネーブルにして、セグメント番号を特定します。指定できるセグメント ID の範囲は 1 ～ 1024 です。これらの任意のキーワードは利用可能です。 （注） 各セグメントに 1 つのプライマリ エッジ ポートを含めて、2 つのエッジ ポートを設定する必要があります。 • （任意）**edge**：エッジ ポートとしてポートを設定します。各セグメントにあるエッジ ポートは 2 つだけです。**primary** キーワードなしで **edge** を入力すると、ポートがセカンダリ エッジポートとして設定されます。 • （任意）**primary**：プライマリ エッジ ポート（VLAN ロードバランシングを設定できるポート）としてポートを設定します。 • （任意）**no-neighbor**：エッジ ポートとして外部 REP ネイバーを使用せずにポートを設定します。そのポートはエッジポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。

	コマンドまたはアクション	目的
		（注） 各セグメントにあるプライマリ エッジ ポートは 1 つだけですが、2 つの異なるスイッチにエッジポートを設定して **primary** キーワードを両方のスイッチに入力しても、その設定は有効です。ただし、REP ではセグメント プライマリ エッジ ポートとして 1 つのポートだけが選択されます。**showreptopology** 特権 EXEC コマンドを入力すると、セグメントのプライマリエッジポートを特定することができます。 • （任意）**preferred**：ポートが優先代替ポートであるか、VLAN ロードバランシングの優先ポートであるかを示します。 （注） ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。
ステップ 6	**repstcn** {**interface** *interface id*| **segment** *id-list* | **stp**}	（任意）STCN を送信するようにエッジ ポートを設定します。 • **interface** *interface -id*：物理インターフェイスまたはポート チャネルを指定して、STCN を受け取ります。 • **segment** *id-list*：STCN を受け取る 1 つ以上のセグメントを特定します。有効な範囲は 1 ～ 1024 です。 • **stp**：STCN を STP ネットワークに送信します。

	コマンドまたはアクション	目的
		（注） STCN を STP ネットワークに送信するために rep stcn stp を設定する場合は、スパニングツリーモード mst がネイバーなしのエッジノード上に必要です。
ステップ 7	**repblockport** {**id** *port-id*| *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}	（任意）プライマリ エッジ ポートに VLAN ロード バランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し、代替ポートでブロックされるように VLAN を設定します。 • **id***port-id*：ポート ID で代替ポートを特定します。セグメント内の各ポートにポート ID が自動的に生成されます。**showinterface** *type number* **rep** [**detail**] 特権 EXEC コマンドを入力し、インターフェイスポート ID を表示できます。 • *neighbor_offset*：エッジポートからのダウンストリーム ネイバーとして代替ポートを特定するための番号。有効範囲は -256 ～ 256 で、負数はセカンダリ エッジポートからのダウンストリーム ネイバーを示します。値 **0** は無効です。**-1** を入力して、セカンダリ エッジポートを代替ポートとして識別します。ネイバーオフセット番号付けの例については、図 69：セグメント内のネイバーオフセット番号（1010 ページ） を参照してください。 （注） プライマリ エッジ ポート（オフセット番号 1）にこのコマンドを入力するので、代替ポートを特定するのにオフセット値 1 を入力できません。 • **preferred**：すでに VLAN ロード バランシングの優先代替ポートと

	コマンドまたはアクション	目的
		して指定されている通常セグメント ポートを選択します。 • **vlan** *vlan-list*：1 つの VLAN または VLAN の範囲をブロックします。 • **vlan all**：すべての VLAN をブロックします。 （注） REP プライマリ エッジ ポート上にだけこのコマンドを入力します。
ステップ 8	**reppreemptdelay** *seconds*	（任意）プリエンプト遅延時間を設定します。 • リンク障害が発生して復旧した後に、VLAN ロード バランシングを自動的にトリガーするには、このコマンドを使用します。 • 遅延時間の範囲は 15 ～ 300 秒です。デフォルトは、遅延時間のない手動によるプリエンプションです。 （注） REP プライマリ エッジ ポート上にだけこのコマンドを入力します。
ステップ 9	**rep lsl-age-timer** *value*	（任意）ネイバーからの hello が受信されないままどのくらいの時間（ミリ秒）が経過すると REP インターフェイスがダウンするかを設定します。 指定できる範囲は 120 ～ 10000 ミリ秒（40 ミリ秒単位）です。デフォルト値は 5000 ミリ秒（5 秒）です。

	コマンドまたはアクション	目的
		（注） • EtherChannel ポート チャネルインターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。 • リンクのフラップを避けるため、リンクの両方のポートに同じ LSL エージが設定されている必要があります。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**showinterface** [*interface-id*] **rep** [**detail**]	（任意）REP インターフェイスの設定を表示します。
ステップ 12	**copyrunning-configstartup-config**	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

VLAN ロード バランシングの手動によるプリエンプションの設定

プライマリ エッジ ポートで **rep preempt delay***seconds* インターフェイス コンフィギュレーション コマンドを入力しないで、プリエンプション時間遅延を設定する場合、デフォルトではセグメントで VLAN ロード バランシングを手動でトリガーします。手動で VLAN ロード バランシングをプリエンプトする前に、他のすべてのセグメント設定が完了しているかどうか確認してください。**rep preempt delay segment** *segment-id* コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**rep preempt segment** *segment-id*	手動により、セグメント上の VLAN ロード バランシングをトリガーします。 実行前にコマンドを確認する必要があります。
ステップ 2	**show rep topology segment** *segment-id*	REP トポロジ情報を表示します。

REP の SNMP トラップ設定

REP 固有のトラップを送信して、簡易ネットワーク管理プロトコル（SNMP）サーバにリンクの動作状態の変更およびすべてのポート役割の変更を通知するようにルータを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmpmibreptrap-rate** *value* 例： `Switch(config)# snmp mib rep trap-rate 500`	スイッチでREPトラップの送信をイネーブルにして、1秒あたりのトラップの送信数を設定します。 • 1秒あたりのトラップの送信数を入力します。範囲は 0 ～ 1000 です。デフォルトは0（制限なし、発生するたびにトラップが送信される）です。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**showrunning-config** 例： `Switch# show running-config`	（任意）実行コンフィギュレーションを表示します。これを使用してREPトラップ コンフィギュレーションを検証できます。
ステップ 5	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

REP のモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	**show interface** [*interface-id*] **rep** [**detail**]	特定のインターフェイスまたはすべてのインターフェイスのREPの設定とステータスを表示します。 • （任意）**detail**：インターフェイス固有の REP 情報を表示します。
ステップ 2	**show rep topology** [**segment** *segment-_id*] [**archive**] [**detail**]	セグメント内のプライマリおよびセカンダリ エッジ ポートを含む、1 セグメントまたは全セグメントの REP トポロジ情報を表示します。 • （任意）**archive**：最後の安定したトポロジを表示します。 （注） アーカイブのトポロジは、スイッチをリロードすると保持されません。 • （任意）**detail**：詳細なアーカイブ情報を表示します。

第 49 章

単方向リンク検出の設定

- 機能情報の確認 （1023 ページ）
- UDLD 設定の制約事項 （1023 ページ）
- UDLD について （1024 ページ）
- UDLD の設定方法 （1028 ページ）
- UDLD のモニタおよびメンテナンス （1031 ページ）
- UDLD の追加リファレンス （1031 ページ）
- UDLD の機能情報 （1032 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

UDLD 設定の制約事項

次に、単方向リンク検出（UDLD）設定の制約事項を示します。

- UDLD 対応ポートが別のデバイスの UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。
- モード（通常またはアグレッシブ）を設定する場合、リンクの両側に同じモードを設定します。

⚠

注意 ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

UDLD について

UniDirectional Link Detection（UDLD）は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニタリングしたり、単一方向リンクの存在を検出できるようにするためのレイヤ2プロトコルです。このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。UDLD は単一方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。単一方向リンクは、スパニングツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。通常モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できます。アグレッシブ モードの UDLD は、光ファイバ リンクおよびツイストペア リンク上の片方向トラフィックと、光ファイバ リンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ 1 のメカニズムを使用して、リンクの物理ステータスを学習します。レイヤ1では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバー ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカルデバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカルデバイスが受信しない場合に、単一方向リンクが発生します。

通常モード

通常モードの UDLD は、光ファイバ ポートの光ファイバが誤って接続されている場合に単一方向リンクを検出しますが、レイヤ1メカニズムは、この誤った接続を検出しません。ポートが正しく接続されていてもトラフィックが片方向である場合、単一方向リンクを検出するはずのレイヤ1メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。この場合、論理リンクは不確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ1メカニズムがリンクの物理的な問題を検出するため、

リンクは稼働状態でなくなります。この場合は、UDLDは何のアクションも行わず、論理リンクは不確定と見なされます。

関連トピック

UDLD のグローバルなイネーブル化（CLI）（1028 ページ）
インターフェイスでの UDLD のイネーブル化（CLI）（1029 ページ）

アグレッシブ モード

アグレッシブ モードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイントリンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがトラフィックを送受信できない。
- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがダウンし、残りのインターフェイスが稼働している。
- ケーブルのうち 1 本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイントリンクでは、UDLD helloパケットをハートビートと見なすことができ、ハートビートがあればリンクは正常です。逆に、ハートビートがないということは、双方向リンクを再確立できない限り、リンクをシャットダウンする必要があることを意味しています。

レイヤ1の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブ モードの UDLD はそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは自動ネゴシエーションでは実行できません。

（注） Udld は、udld アグレッシブ モードでグローバルに有効になります。Rx ケーブルまたは Tx が switch1 からのケーブルである場合、switch1 と switch2 ポートは**Not connected**状態になります。これらのポートは **error disabled** ステートにはなりません。また、物理接続を確認する場合、ポートは点灯しません。

Switch1 (Tx)_____(Rx) Switch2

Switch1 (Rx)_____(Tx) Switch2

関連トピック

UDLD のグローバルなイネーブル化（CLI）（1028 ページ）
インターフェイスでの UDLD のイネーブル化（CLI）（1029 ページ）

単一方向の検出方法

UDLD は、2 つの方法で動作します。

- ネイバー データベース メンテナンス
- イベントドリブン検出およびエコー

関連トピック

UDLD のグローバルなイネーブル化（CLI）（1028 ページ）
インターフェイスでの UDLD のイネーブル化（CLI）（1029 ページ）

ネイバー データベース メンテナンス

UDLD は、アクティブな各ポート上で hello パケット（別名アドバタイズまたはプローブ）を定期的に送信して、他の UDLD 対応ネイバーに関して学習し、各デバイスがネイバーに関する情報を常に維持できるようにします。

デバイスが hello メッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、情報をキャッシュします。古いキャッシュ エントリの期限が切れる前に、デバイスが新しい hello メッセージを受信すると、デバイスが古いエントリを新しいエントリで置き換えます。

UDLD の実行中にポートがディセーブルになったり、ポート上で UDLD がディセーブルになったり、またはデバイスをリセットした場合、UDLD は設定変更の影響を受けるポートの既存のキャッシュ エントリをすべてクリアします。UDLD は、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを 1 つまたは複数送信します。このメッセージは、キャッシュを継続的に同期するためのものです。

イベントドリブン検出およびエコー

UDLD は検出動作としてエコーを利用します。UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続の UDLD デバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。この動作はすべての UDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブ モードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

関連トピック

UDLD のグローバルなイネーブル化（CLI）（1028 ページ）
インターフェイスでの UDLD のイネーブル化（CLI）（1029 ページ）

UDLD リセット オプション

インターフェイスが UDLD でディセーブル化された場合、次のオプションの 1 つを使用して UDLD をリセットできます。

- **udld reset** インターフェイス コンフィギュレーション コマンド。
- **shutdown** インターフェイス コンフィギュレーション コマンドに続いて **no shutdown** インターフェイスコンフィギュレーションコマンドを入力すると、ディセーブル化されたポートを再起動できます。
- **no udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドの後に **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを実行すると、ディセーブル化されたポートが再びイネーブルになります。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** [**aggressive**] インターフェイス コンフィギュレーション コマンドを実行すると、ディセーブル化された光ファイバ ポートが再びイネーブルになります。
- **errdisable recovery cause udld** グローバル コンフィギュレーション コマンドを入力すると、UDLD の errdisable ステートから自動回復するタイマーをイネーブルにできます。さらに、**errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンドを入力すると、UDLD の errdisable ステートから回復する時間を指定できます。

関連トピック

UDLD のグローバルなイネーブル化（CLI） （1028 ページ）
インターフェイスでの UDLD のイネーブル化（CLI） （1029 ページ）

UDLD のデフォルト設定

表 *64 : UDLD* のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ ポート上でディセーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX ポート上でディセーブル
UDLD アグレッシブ モード	ディセーブル

関連トピック

UDLD のグローバルなイネーブル化（CLI） （1028 ページ）
インターフェイスでの UDLD のイネーブル化（CLI） （1029 ページ）

UDLD の設定方法

UDLD のグローバルなイネーブル化（CLI）

アグレッシブ モードまたは通常モードで UDLD をイネーブルにし、デバイス上のすべての光ファイバ ポートに設定可能なメッセージ タイマーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*} 例： `Device(config)# udld enable message time 10`	UDLD モードの動作を指定します。 • **aggressive**：すべての光ファイバ ポートにおいて、アグレッシブ モードでUDLDをイネーブルにします。 • **enable**：デバイス上のすべての光ファイバ ポート上で、UDLD を通常モードでイネーブルにします。UDLDはデフォルトでディセーブルです。 個々のインターフェイスの設定は、**udld enable** グローバル コンフィギュレーション コマンドの設定を上書きします。 • **message time** *message-timer-interval*：アドバタイズメント フェーズにあり、双方向リンクが検出されたポートでの UDLD プローブ メッセージの時間間隔を設定します。有効な範囲は 1 ～ 90 秒です。デフォルト値は 15 です。

	コマンドまたはアクション	目的
		（注） このコマンドが作用するのは、光ファイバ ポートだけです。他のポート タイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。 UDLD をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

UDLD のモニタおよびメンテナンス
アグレッシブ モード （1025 ページ）
通常モード （1024 ページ）
単一方向の検出方法 （1026 ページ）
イベントドリブン検出およびエコー （1026 ページ）
UDLD リセット オプション （1027 ページ）
UDLD のデフォルト設定 （1027 ページ）

インターフェイスでの UDLD のイネーブル化（CLI）

アグレッシブ モードまたは通常モードをイネーブルにする、またはポート上で UDLD をディセーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	UDLD 用にイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**udld port** [**aggressive**] 例： `Device(config-if)# udld port aggressive`	UDLD はデフォルトでディセーブルです。 • **udld port**：指定されたポート上で、UDLD を通常モードでイネーブルにします。 • **udld port aggressive**：（任意）指定されたインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。 （注） 特定の光ファイバ ポート上で UDLD をディセーブルにする場合は、 **no udld port** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

UDLD のモニタおよびメンテナンス
アグレッシブ モード （1025 ページ）
通常モード （1024 ページ）
単一方向の検出方法 （1026 ページ）
イベントドリブン検出およびエコー （1026 ページ）
UDLD リセット オプション （1027 ページ）
UDLD のデフォルト設定 （1027 ページ）

UDLD のモニタおよびメンテナンス

コマンド	目的
show udld [*interface-id* | **neighbors**]	指定されたポートまたはすべてのポートの UDLD ステータスを表示します。

UDLD の追加リファレンス

関連資料

関連項目	マニュアル タイトル
レイヤ 2 コマンド リファレンス	『*Layer 2/3 Command Reference (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

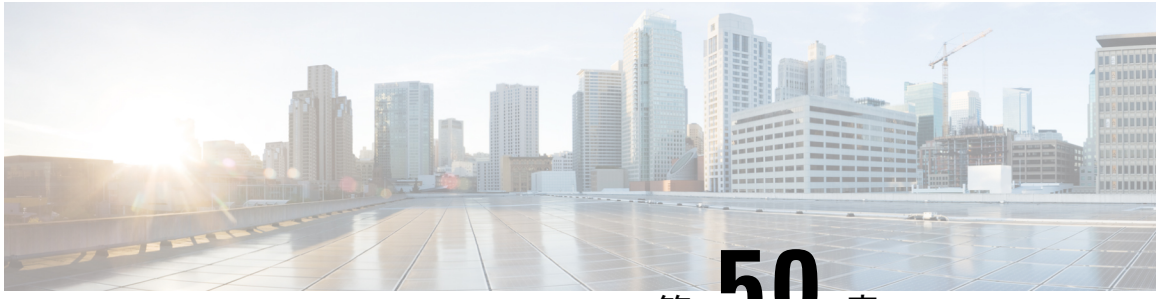
UDLD の機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 IX 部

Lightweight アクセス ポイント

- アクセス ポイント ディスカバリ用のデバイスの設定 （1035 ページ）
- データ暗号化の設定 （1045 ページ）
- 再送信間隔および再試行回数の設定 （1049 ページ）
- 適応型ワイヤレス侵入防御システムの設定 （1053 ページ）
- アクセス ポイントの認証の設定 （1059 ページ）
- 自律アクセス ポイントの Lightweight モードへの変換 （1069 ページ）
- Cisco ワークグループ ブリッジの使用 （1081 ページ）
- プローブ要求フォワーディングの設定 （1085 ページ）
- RFID トラッキングの最適化 （1089 ページ）
- 国番号の設定 （1093 ページ）
- リンク遅延の設定 （1099 ページ）
- Power over Ethernet の設定 （1109 ページ）



第 50 章

アクセス ポイント ディスカバリ用のデバイスの設定

- 機能情報の確認 （1035 ページ）
- アクセス ポイント ディスカバリ用のデバイスの設定の前提条件 （1035 ページ）
- アクセス ポイント ディスカバリ用のデバイスの設定の制約事項 （1036 ページ）
- アクセス ポイント ディスカバリ用のデバイスの設定に関する情報 （1037 ページ）
- アクセス ポイント ディスカバリの設定方法 （1039 ページ）
- アクセス ポイント ディスカバリ用のデバイスの設定例 （1040 ページ）
- AP パススルーの設定 （1042 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

アクセスポイントディスカバリ用のデバイスの設定の前提条件

⚠

注意 ワイヤレス機能を使用するには、Cisco Catalyst 3850 スイッチ ポートに AP を直接接続する必要があります。

- Control and Provisioning of Wireless Access Points（CAPWAP）UDP ポート 5246 および 5247（Lightweight Access Point Protocol（LWAPP）UDP ポート 12222 および 12223 と同等のポー

ト）が有効になっており、アクセス ポイントがデバイスに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。

- アクセス コントロール リスト（ACL）がデバイスとアクセス ポイントの間の制御パスにある場合は、新しいプロトコル ポートを開いてアクセス ポイントが孤立しないようにする必要があります。
- アクセス ポイントが UP 状態であり、IP アドレスが変更される場合は、既存の CAPWAP トンネルを解除してデバイスに再 join します。
- アクセス ポイントをネットワークでアクティブにするには、デバイスがそのアクセス ポイントを検出する必要があります。Lightweightアクセスポイントでは、次のデバイスディスカバリのプロセスがサポートされています。
  - レイヤ 3 CAPWAP ディスカバリ：アクセス ポイントから複数のサブネットでこの機能をイネーブルにできます。この機能は、レイヤ 2 ディスカバリで使用される MAC アドレスではなく IP アドレスと UDP パケットを使用します。
  - ローカルに保存されているデバイスの IP アドレス ディスカバリ：アクセス ポイントがすでにデバイスにアソシエートされている場合、プライマリ、セカンダリ、およびターシャリ デバイスの IP アドレスはアクセス ポイントの不揮発性メモリに保存されます。今後の展開用にアクセスポイントにデバイスの IP アドレスを保存するこのプロセスは、「アクセス ポイントのプライミング」と呼ばれます。
  - DHCP サーバの検出：この機能では、デバイスDHCP オプション 43 を使用してアクセス ポイントにの IP アドレスを割り当てます。Cisco スイッチでは、通常この機能に使用される DHCP サーバ オプションをサポートしています。
  - DNS の検出：アクセス ポイントでは、ドメイン ネーム サーバ（DNS）を介してデバイスを検出できます。CISCO-CAPWAP-CONTROLLER.*localdomain* に応答してデバイス IP アドレスを返すように DNS を設定する必要があります。ここで *localdomain* はアクセス ポイントのドメイン名です。アクセス ポイントは、DHCP サーバから IP アドレスと DNS の情報を受信すると、DNS に接続して CISCO-CAPWAP-CONTROLLER.*localdomain* を解決します。DNS からデバイスの IP アドレスのリストを受信すると、アクセスポイントはデバイスにディスカバリ要求を送信します。

アクセスポイントディスカバリ用のデバイスの設定の制約事項

- デバイスが適切な日時で設定されていることを確認してください。デバイスに設定されている日時がアクセスポイントの証明書の作成日とインストール日に先行すると、アクセスポイントはデバイスに join しません。

- ディスカバリ プロセス中は、1140、1260、3500、1040、1600、2600、または3600などの、シスコ デバイスによってサポートされるアクセス ポイントはシスコ デバイスに対してのみクエリを行います。

アクセスポイントディスカバリ用のデバイスの設定に関する情報

CAPWAP 環境では、Lightweight アクセス ポイントは CAPWAP 検出メカニズムを用いてデバイスを検出し、デバイスに CAPWAP 接続要求を送信します。デバイスはデバイスに接続するためのアクセス ポイントを許可するため、アクセス ポイントに CAPWAP 接続応答を送信します。アクセス ポイントがデバイスに接続されると、デバイスはその構成、ファームウェア、コントロール トランザクション、データ トランザクションを管理します。

アクセス ポイント通信プロトコル

Cisco Lightweight アクセス ポイントは、IETF 標準 CAPWAP を使用してネットワーク上のデバイスおよび他の Lightweight アクセス ポイントと通信します。

CAPWAP は LWAPP に基づく標準の互換プロトコルであり、デバイスによる無線アクセス ポイントの集合の管理を可能にします。CAPWAP は、次の理由によりデバイスに実装されます。

- LWAPP を使用するシスコ製品に、CAPWAP を使用する次世代シスコ製品へのアップグレード パスを提供するため。
- RFID リーダーおよび類似のデバイスを管理するため。
- デバイスにサードパーティのアクセス ポイントとの将来的な互換性を持たせるため。

アクセス ポイントの join 情報の表示

CAPWAP discovery 要求をデバイスに少なくとも 1 回送信するアクセス ポイントの接続に関する統計情報は、アクセス ポイントがリブートまたは切断されても、デバイス上に維持されます。これらの統計情報が削除されるのは、デバイスがリブートされた場合、または統計情報のクリアを選択した場合のみです。

アクセス ポイント接続プロセスのトラブルシューティング

アクセスポイントがデバイスへの接続に失敗するのには、RADIUS認証が保留になっている、デバイスで自己署名証明書が有効になっていない、アクセスポイントとデバイスとで規制ドメインが一致しないなど、多くの原因が考えられます。

アクセス ポイントには、CAPWAP 関連のすべてのエラーを syslog サーバに送信するよう設定できます。すべての CAPWAP エラー メッセージが syslog サーバでそのまま表示できるので、デバイスでデバッグ コマンドを有効にする必要はありません。

デバイスがアクセス ポイントからの CAPWAP join 要求を受信するまで、アクセス ポイントの状態は保持されません。そのため、特定のアクセス ポイントからの CAPWAP discovery 要求が拒否された理由を判断することは難しい場合があります。そのような接続の問題を、デバイスで CAPWAP のデバッグ コマンドを有効にせずトラブルシューティングするため、デバイスはこのデバイスにディスカバリ メッセージを送信するすべてのアクセス ポイントの情報を収集し、このデバイスに正常に接続したアクセス ポイントがあればその情報を保持します。

デバイスは、CAPWAP discovery 要求をデバイスに送信する各アクセス ポイントについて、接続関連のすべての情報を収集します。収集は、最初のディスカバリ メッセージがアクセス ポイントから受信されたときに開始し、最後の設定ペイロードがデバイスからアクセスポイントに送信されたときに終了します。

デバイスが接続関連情報を保持しているアクセスポイントが最大数に達すると、それ以外のアクセス ポイントの情報は収集されなくなります。

DHCP サーバで syslog サーバの IP アドレスをアクセス ポイントに返すよう設定することもできます。サーバ上でオプション 7 を使用します。それにより、アクセスポイントではすべての syslog メッセージがこの IP アドレスへ送信されるようになります。

アクセス ポイントがデバイスに接続していない場合、syslog サーバの IP アドレスは、アクセス ポイントの CLI を介して設定します。**capwap ap log-server***syslog_server_IP_address* コマンドを入力します。

アクセス ポイントが最初にデバイスに接続する際、デバイスはグローバル syslog サーバの IP アドレス（デフォルトは 255.255.255.255）をアクセスポイントにプッシュします。その後、IP アドレスが次のいずれかのシナリオで上書きされるまで、アクセスポイントはすべての syslog メッセージをこの IP アドレスに送信します。

- アクセス ポイントが接続されているデバイスは同じだが、**ap syslog host** *Syslog_Server_IP_Address* コマンドを使用して、デバイスのグローバル syslog サーバの IP アドレス設定を変更した。この場合、デバイスはグローバル syslog サーバの新しい IP アドレスをアクセス ポイントにプッシュします。
- アクセス ポイントが接続されているデバイスは同じだが、デバイスのアクセス ポイントについて、**ap name** *Cisco_AP* **syslog host** *Syslog_Host_IP_Address* コマンドを使用して、特定の syslog サーバの IP アドレスを設定した。この場合、デバイスは特定の syslog サーバの新しい IP アドレスをアクセス ポイントにプッシュします。
- アクセス ポイントがデバイスから切断され、**capwap ap log-server** *syslog_server_IP_address* コマンドを使用して、アクセス ポイントの CLI から syslog サーバの IP アドレスを設定した。このコマンドは、アクセスポイントがどのデバイスにも接続されていない場合に限り機能します。
- アクセスポイントがデバイスから切断され、別のデバイスに接続した。この場合、新しいデバイスはそのグローバル syslog サーバの IP アドレスをアクセス ポイントへプッシュします。

新しい syslog サーバの IP アドレスが既存の syslog サーバの IP アドレスを上書きするたびに、古いアドレスは固定記憶域から消去され、新しいアドレスがそこに保存される。アクセス ポイントも、その syslog サーバの IP アドレスに到達できるのであれば、すべての syslog メッセージを新しい IP アドレスに送信するようになります。

アクセス ポイント ディスカバリの設定方法

アクセス ポイントの Syslog サーバの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**show ap config global** 例： `Device# show ap config global`	デバイスを join するすべてのアクセス ポイントのグローバル Syslog サーバ設定を表示します。
ステップ 2	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name AP03 config general`	特定のアクセス ポイントの Syslog サーバ設定を表示します。

アクセス ポイントの join 情報のモニタリング（CLI）

（注） デバイス GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**show ap join stats summary** 例： `Device# show ap join stats summary`	デバイスに join しているまたは join を試行したすべてのアクセス ポイントの MAC アドレスを表示します。

	コマンドまたはアクション	目的
ステップ 3	**show ap mac-address** *mac_address* **join stats summary** 例： `Device# show ap mac-address 000.2000.0400 join stats summary`	最後の join エラーの詳細を含む AP のすべての統計情報を表示します。
ステップ 4	**show ap mac-address** *mac_address* **join stats detailed** 例： `Device# show ap mac-address 000.2000.0400 join stats detailed`	特定のアクセス ポイントについて収集された join 関連の統計情報を表示します。
ステップ 5	**clear ap join statistics** 例： `Device# clear ap join statistics`	すべてのアクセス ポイントの join 統計情報をクリアします。 （注） 特定のアクセスポイントに対応する join 統計情報をクリアするには、**clear ap mac-address** *mac_address* **join statistics** コマンドを入力します。

関連トピック

すべてのアクセス ポイントの MAC アドレスの表示：例 （1040 ページ）
Lightweight Cisco Aironet アクセス ポイントの DHCP オプション 43 の設定例 （1041 ページ）

アクセス ポイント ディスカバリ用のデバイスの設定例

すべてのアクセス ポイントの MAC アドレスの表示：例

次に、デバイスに join しているすべてのアクセス ポイントの MAC アドレスを表示する例を示します。

```
Device# show ap join stats summary
Number of APs.......................................... 4

Base Mac           EthernetMac        AP Name IP Address    Status
----------------- ----------------- ------- ------------- ----------
00:0b:85:57:bc:c0 00:0b:85:57:bc:c0 AP1130  10.10.163.217 Joined
00:1c:0f:81:db:80 00:1c:63:23:ac:a0 AP1140  10.10.163.216 Not joined
00:1c:0f:81:fc:20 00:1b:d5:9f:7d:b2 AP1     10.10.163.215 Joined
00:21:1b:ea:36:60 00:0c:d4:8a:6b:c1 AP2     10.10.163.214 Not joined
```

次に、特定のアクセス ポイントに関する最後の join エラーの詳細を表示する例を示します。

```
Device# show ap mac-address 000.2000.0400 join stats summary
Is the AP currently connected to controller................ Yes
```

```
Time at which the AP joined this
controller last time................................ Aug 21 12:50:36.061
Type of error
that occurred last................. AP got or has been disconnected
Reason for error
that occurred last........... The AP has been reset by the controller
Time at which the last join error occurred......... Aug 21 12:50:34.374
```

次に、特定のアクセス ポイントに関して収集されたすべての join 関連の統計情報を表示する例を示します。

```
Device# show ap mac-address 000.2000.0400 join stats detailed
Discovery phase statistics
- Discovery requests received........................ 2
- Successful discovery responses sent................ 2
- Unsuccessful discovery request processing.......... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt.......... Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt........ Not applicable

Join phase statistics
- Join requests received............................. 1
- Successful join responses sent..................... 1
- Unsuccessful join request processing............... 1
- Reason for last unsuccessful join attempt.....      RADIUS authorization
                                                      is pending
                                                      for the AP
- Time at last successful join attempt............... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt............. Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received.................... 1
- Successful configuration responses sent............ 1
- Unsuccessful configuration request processing....... 0
- Reason for last unsuccessful configuration attempt.. Not applicable
- Time at last successful configuration attempt....... Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt..... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure.......... Not applicable

Last AP disconnect details
- Reason for last AP connection failure............... The AP has been reset by
                                                       the controller
Last join error summary
- Type of error that occurred last................... AP got or has been
                                                       disconnected
- Reason for error that occurred last................. The AP has been reset
                                                       by the controller
- Time at which the last join error occurred.......... Aug 21 12:50:34.374
```

Lightweight Cisco Aironet アクセス ポイントの DHCP オプション 43 の設定例

AP join プロセスの詳細については、「*DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example*」を参照してください。

AP パススルーの設定

AP パススルーについて

AP パススルーでは、 Cisco Catalyst 3850 シリーズ スイッチおよび Cisco Catalyst 3650 シリーズ スイッチに接続されているすべてのアクセスポイントをネットワーク上の別のコントローラに接続します。

このリリースに先立ち、Cisco Catalyst 3850 シリーズ スイッチおよび Cisco Catalyst 3650 シリーズ スイッチに接続されているすべてのアクセス ポイントは 、ワイヤレス マネジメント VLAN がオンのときにデバイス上で終端します。デバイスに接続したサポート対象外のアクセス ポイントは、異なる VLAN 上のコントローラに接続できません。AP パススルーでは、異なる VLAN を割り当てることで、接続された AP を VLAN ネットワーク上の別のワイヤレス コントローラに接続します。

AP パスの利点は次のとおりです。

- 一部の AP が、Cisco Catalyst 3850 シリーズ スイッチおよび Cisco Catalyst 3650 シリーズ スイッチに接続され、他の AP がネットワーク上の他のコントローラに接続し続けているとき、新世代の Cisco Wireless Controller の部分的な展開を許可します。
- Cisco Catalyst 3850 シリーズ スイッチおよび Cisco Catalyst 3650 シリーズ スイッチでサポート対象外の AP がネットワーク内の他のコントローラに接続するのを許可します。
- ワイヤレス LAN コントローラは、有線およびワイヤレス ゲストへのアクセスを提供するために使用されます。AP パススルーにより、AP は有線ゲスト アクセスがオンになると、Cisco Catalyst 3850 シリーズ スイッチおよび Cisco Catalyst 3650 シリーズ スイッチを他の任意のコントローラに接続します。

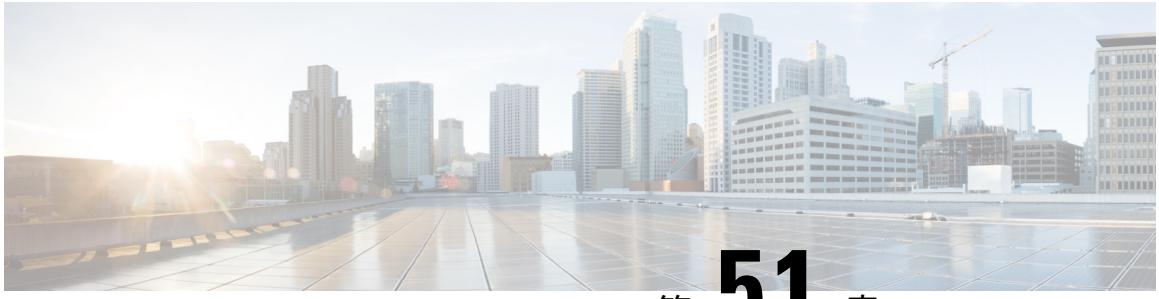
AP パススルーの設定

サポートされるアクセス ポイントのもの以外の VLAN のすべてのアクセス ポイントは、AP のパススルー モードになり、Deviceでは終了しません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless management interface vlan** *vlan_id* 例：	ワイヤレス管理の VLAN でサポートされるアクセス ポイントに接続されているポートを設定します。

	コマンドまたはアクション	目的
	`Device(config)# wireless management interface vlan10`	
ステップ 3	**interface GigabitEthernet1/0/1** 例： `Device(config)# interface TenGigabitEthernet1/0/1`	10 ギガビット イーサネット インターフェイスを設定します。 コマンド プロンプトが (config)# から (config-if)# に変わります。
ステップ 4	**description Supported AP switchport access** *vlan_id* 例： `Device(config-if)# switchport access vlan10`	このアクセス ポートがトラフィックを伝送する VLAN を指定します。
ステップ 5	**description Unsupported AP switchport access** *vlan_id* 例： `Device(config-if)# switchport access vlan20`	ワイヤレス管理の VLAN 以外の VLAN でサポートされていないアクセス ポイントに接続されているポートを設定します。



第 51 章

データ暗号化の設定

- 機能情報の確認 （1045 ページ）
- データ暗号化の設定の前提条件 （1045 ページ）
- データ暗号化の設定に関する制約事項 （1046 ページ）
- データの暗号化について （1046 ページ）
- データ暗号化の設定方法 （1046 ページ）
- データ暗号化の設定例 （1047 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

データ暗号化の設定の前提条件

- Cisco 1260、3500、3600、801、1140、1310、および 1520 シリーズのアクセス ポイントは、Datagram Transport Layer Security（DTLS）のデータ暗号化をサポートします。
- デバイスを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効化または無効化できます。
- シスコ デバイスを使用するロシア人以外のお客様はデータ DTLS ライセンスは必要ありません。

データ暗号化の設定に関する制約事項

- 暗号化はデバイスおよびアクセス ポイントの両方においてスループットを制限するため、多くのエンタープライズ ネットワークにおいて最大スループットが必要です。
- デバイスにデータ DTLS のライセンスがなく、デバイスに関連付けられているアクセス ポイントで DTLS が有効になっている場合、データ パスは暗号化されません。
- DTLS ライセンスがないイメージでは DTLS コマンドは使用できません。

データの暗号化について

デバイスにより、DTLS を使用してアクセス ポイントとデバイスの CAPWAP コントロール パケット（および、オプションとして CAPWAP データ パケット）の暗号化が可能です。DTLS は、標準化過程にある TLS に基づくインターネット技術特別調査委員会（IETF）プロトコルです。CAPWAP コントロール パケットとは、デバイスとコントローラとアクセス ポイントの間で交換される管理パケットであり、CAPWAP データ パケットは転送された無線フレームをカプセル化します。CAPWAP コントロールおよびデータ パケットはそれぞれ異なる UDP ポートである 5246（コントロール）および 5247（データ）で送信されます。アクセス ポイントが DTLS データ暗号化をサポートしない場合、DTLS はコントロール プレーンにのみ有効となり、データ プレーンの DTLS セッションは確立されません。

データ暗号化の設定方法

データ暗号化の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap link-encryption** 例： `Device(config)# ap link-encryption`	このコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントのデータ暗号化をイネーブルにします。デフォルト値は [disabled] です。 データ暗号化モードに変更するには、アクセス ポイントをデバイスに再 join する必要があります。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 4	**show ap link-encryption** 例： `Device# show ap link-encryption`	すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化の状態を表示します。このコマンドはまた、整合性チェックの失敗およびリプレイエラーの数を追跡する認証エラーを表示します。リレー エラーは、アクセス ポイントが同じパケットを受信する回数の追跡に役立ちます。
ステップ 5	**show wireless dtls connections** 例： `Device# show wireless dtls connections`	すべてのアクティブなDTLS接続の概要を表示します。 （注） DTLSデータの暗号化に問題が生じた場合は、**debug dtls ap {all | event | trace}** コマンドを入力して、すべての DTLS メッセージ、イベント、またはトレースをデバッグします。

関連トピック

すべてのアクセス ポイントのデータ暗号化の状態の表示：例 （1047 ページ）

データ暗号化の設定例

すべてのアクセス ポイントのデータ暗号化の状態の表示：例

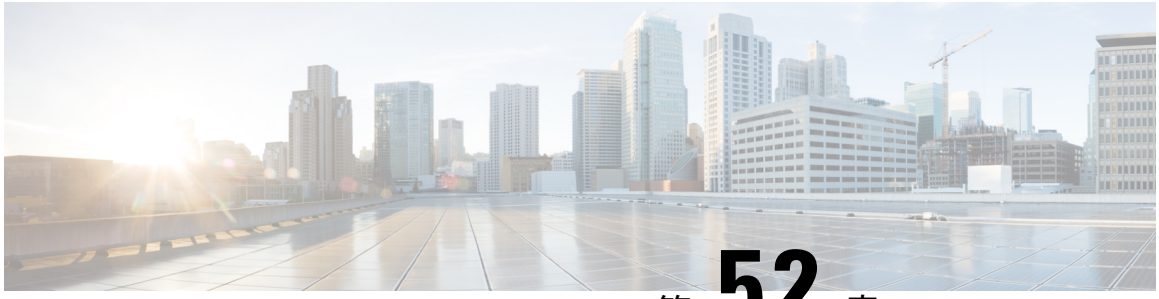
次に、すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化の状態を表示する例を示します。このコマンドはまた、整合性チェックの失敗およびリプレイ エラーの数を追跡する認証エラーを表示します。リレー エラーは、アクセス ポイントが同じパケットを受信する回数の追跡に役立ちます。

```
Device# show ap link-encryption
                    Encryption  Dnstream  Upstream    Last
AP Name                  State     Count     Count  Update
------------------  ----------  --------  --------  ------
3602a                   Enabled         0         0   Never
```

次に、すべてのアクティブな DTLS 接続のサマリーを表示する例を示します。

すべてのアクセス ポイントのデータ暗号化の状態の表示：例

```
Device# show wireless dtls connections
AP Name         Local Port   Peer IP       Peer Port  Ciphersuite
--------------- ------------ ------------- ---------- --------------------
3602a           Capwap_Ctrl  10.10.21.213  46075      TLS_RSA_WITH_AES_128_CBC_SHA
3602a           Capwap_Data  10.10.21.213  46075      TLS_RSA_WITH_AES_128_CBC_SHA
```



第 52 章

再送信間隔および再試行回数の設定

- 機能情報の確認 （1049 ページ）
- アクセス ポイントの再送信間隔と再試行回数の設定の前提条件 （1049 ページ）
- 再送信間隔および再試行回数について （1050 ページ）
- アクセス ポイントの再送信間隔と再試行回数の設定方法 （1050 ページ）
- CAPWAP の最大伝送単位情報の表示（CLI） （1051 ページ）
- アクセス ポイントの再送信間隔と再試行回数の設定例 （1052 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

アクセスポイントの再送信間隔と再試行回数の設定の前提条件

- 再送信間隔と再試行回数の両方とも、グローバルと特定のアクセス ポイント レベルで設定できます。グローバル設定では、これらの設定パラメータがすべてのアクセスポイントに適用されます。また、特定のアクセス ポイント レベルで再送信間隔と再試行回数を設定すると、値はその特定のアクセス ポイントに適用されます。アクセス ポイント固有の設定は、グローバル設定よりも優先されます。

再送信間隔および再試行回数について

デバイスとアクセス ポイントは、Control And Provisioning of Wireless Access Points（CAPWAP）の信頼性の高いトランスポート プロトコルを使用してパケットを交換します。各要求に対して、応答が定義されています。この応答を使用して、要求メッセージの受信を確認します。応答メッセージは明示的に確認されません。したがって、応答メッセージが受信されない場合は、再送信間隔後に元の要求メッセージが再送信されます。最大再送信回数に達しても要求が確認されないと、セッションが終了し、アクセス ポイントは再度別のデバイスに関連付けられます。

アクセスポイントの再送信間隔と再試行回数の設定方法

アクセス ポイントの再送信間隔と再試行回数の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap capwap retransmit interval** *interval_time* 例： `Device(config)# ap capwap retransmit interval 2`	すべてのアクセス ポイントに対してコントロール パケットの再送信間隔をグローバルに設定します。 （注） 間隔パラメータの範囲は 2 ～ 5 です。
ステップ 4	**ap capwap retransmit count** *count_value* 例： `Device(config)# ap capwap retransmit count 3`	すべてのアクセス ポイントに対してコントロール パケットの再試行回数をグローバルに設定します。 （注） 回数の範囲は 3 ～ 8 です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

	コマンドまたはアクション	目的
ステップ 6	**ap name** *Cisco_AP* **capwap retransmit interval** *interval_time* 例： `Device# ap name AP02 capwap retransmit interval 2`	ユーザが指定した個々のアクセス ポイントに対してコントロール パケットの再送信間隔を設定します。 （注） 間隔の範囲は 2 ～ 5 です。 （注） **ap name** コマンドを使用するには、特権 EXEC モードを開始しておく必要があります。
ステップ 7	**ap name** *Cisco_AP* **capwap retransmit count** *count_value* 例： `Device# ap name AP02 capwap retransmit count 3`	ユーザが指定した個々のアクセス ポイントに対してコントロール パケットの再試行回数を設定します。 （注） 再試行回数の範囲は 3 ～ 8 です。
ステップ 8	**show ap capwap retransmit** 例： `Device# show ap capwap retransmit`	CAPWAP の再送信の詳細を表示します。

CAPWAP の最大伝送単位情報の表示（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name Maria-1250 config general | include MTU`	デバイス上の CAPWAP パスの最大伝送単位（MTU）を表示します。MTU は、送信されるパケットの最大サイズ（バイト）を指定します。

関連トピック

CAPWAP 再送信の詳細の表示：例 （1052 ページ）
最大伝送単位情報の表示：例 （1052 ページ）

アクセス ポイントの再送信間隔と再試行回数の設定例

CAPWAP 再送信の詳細の表示：例

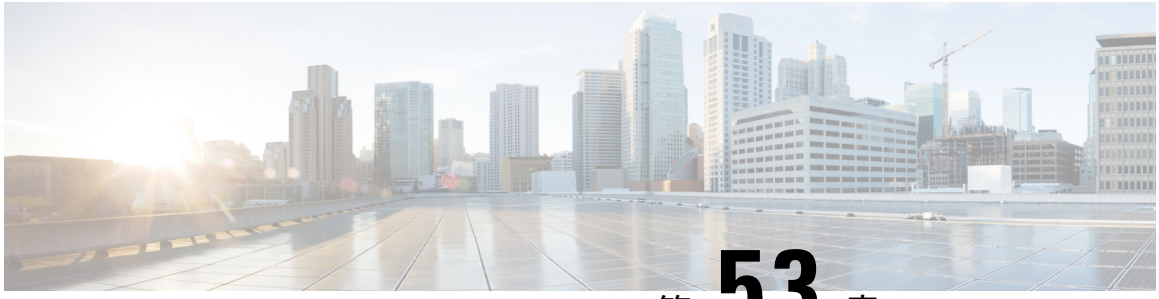
次のコマンドを入力します。

```
Device# show ap capwap retransmit
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval             Retransmit Count

--------------------------------- -------------------------------
---------------------------------
3602a                            5                               3
```

最大伝送単位情報の表示：例

次に、デバイスのCAPWAPパスの最大伝送単位（MTU）を表示する例を示します。MTUは、送信されるパケットの最大サイズ（バイト）を指定します。

```
Device# show ap name cisco-ap-name config general | include MTU
CAPWAP Path MTU................................. 1500
```



第 53 章

適応型ワイヤレス侵入防御システムの設定

- 機能情報の確認 （1053 ページ）
- wIPS 設定の前提条件 （1053 ページ）
- アクセス ポイントでの wIPS の設定方法 （1054 ページ）
- wIPS 情報のモニタリング （1056 ページ）
- アクセス ポイントでの wIPS の設定例 （1056 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

wIPS 設定の前提条件

- 通常のローカル モードのアクセス ポイントは、ワイヤレス侵入防御システム（wIPS）機能のサブセットによって拡張されています。この機能を使用すると、分離されたオーバーレイ ネットワークがなくても、アクセス ポイントを展開して保護機能を提供できます。

アクセス ポイントでの wIPS の設定方法

アクセス ポイントでの wIPS の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *Cisco_AP* **mode local** 例： `Device# ap name AP01 mode local`	モニタ モードのアクセス ポイントを設定します。 AP のモードを変更するとアクセス ポイントがリブートされることを示すメッセージが表示されます。このメッセージは、AP モードの変更を続行するかどうかを指定できるプロンプトも表示します。続行するには、プロンプトで **y** を入力します。
ステップ 2	**ap name** *Cisco_AP* **dot11 5ghz shutdown** 例： `Device# ap name AP01 dot11 5ghz shutdown`	アクセス ポイントの 802.11a 無線を無効にします。
ステップ 3	**ap name** *Cisco_AP* **dot11 24ghz shutdown** 例： `Device# ap name AP02 dot11 24ghz shutdown`	アクセス ポイントの 802.11b 無線を無効にします。
ステップ 4	**ap name** *Cisco_AP* **mode monitor submode wips** 例： `Device# ap name AP01 mode monitor submode wips`	アクセス ポイントで wIPS サブモードを設定します。 （注） アクセス ポイントで wIPS を無効にするには、**ap name** *Cisco_AP* **modemonitor submode none** コマンドを入力します。
ステップ 5	**ap name** *Cisco_AP* **monitor-mode wips-optimized** 例：	アクセス ポイントに対して wIPS が最適化されたチャネル スキャンを有効にします。

	コマンドまたはアクション	目的
	`Device# ap name AP01 monitor-mode wips-optimized`	アクセスポイントは、250 ミリ秒の間、各チャネルをスキャンします。監視設定に基づいてスキャンされるチャネルの一覧が取得されます。次のオプションから選択できます。 • [All]：アクセス ポイントの無線でサポートされているすべてのチャネル。 • [Country]：アクセス ポイントの使用国でサポートされているチャネルのみ。 • [DCA]：動的チャネル割り当て（DCA）アルゴリズムによって使用されるチャネル セットのみ（デフォルトでは、アクセス ポイントの使用国で許可された、オーバーラップしないすべてのチャネルを含む）。
ステップ 6	**show ap dot11 24ghz monitor** 例： `Device# show ap dot11 24ghz monitor`	監視設定チャネルセットを表示します。 （注） コマンド出力の 802.11b 監視チャネル値は監視設定チャネル セットを示します。
ステップ 7	**ap name** *Cisco_AP* **no dot11 5ghz shutdown** 例： `Device# ap name AP01 no dot11 5ghz shutdown`	アクセスポイントの 802.11a 無線を有効にします。
ステップ 8	**ap name** *Cisco_AP* **no dot11 24ghz shutdown** 例： `Device# ap name AP01 no dot11 24ghz shutdown`	アクセスポイントの 802.11b 無線を有効にします。

wIPS 情報のモニタリング

（注） デバイス GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name AP01 config general`	アクセス ポイントの wIPS サブモードで情報を表示します。
ステップ 2	**show ap monitor-mode summary** 例： `Device# show ap monitor-mode summary`	アクセス ポイントで wIPS 最適化チャネル スキャン コンフィギュレーションを表示します。
ステップ 3	**show wireless wps wips summary** 例： `Device# show wireless wps wips summary`	NCS または Prime によって転送した wIPS コンフィギュレーションをデバイスに表示します。
ステップ 4	**show wireless wps wips statistics** 例： `Device# show wireless wps wips statistics`	現在の wIPS オペレーションをデバイスに表示します。
ステップ 5	**clear wireless wips statistics** 例： `Device# clear wireless wips statistics`	デバイスで wIPS 統計をクリアします。

関連トピック

モニタ設定チャネル セットの表示：例 （1056 ページ）
wIPS 情報の表示：例 （1057 ページ）

アクセス ポイントでの wIPS の設定例

モニタ設定チャネル セットの表示：例

次に、モニタ設定チャネル セットを表示する例を示します。

```
Device# show ap dot11 24ghz monitor
Default 802.11b AP monitoring
802.11b Monitor Mode........................... enable
802.11b Monitor Channels....................... Country channels
802.11b AP Coverage Interval................... 180 seconds
802.11b AP Load Interval....................... 60 seconds
802.11b AP Noise Interval...................... 180 seconds
802.11b AP Signal Strength Interval............ 60 seconds
```

wIPS 情報の表示：例

次に、アクセス ポイントの wIPS サブモードの情報を表示する例を示します。

```
Device# show ap name AP01 config general
Cisco AP Identifier............. 3
Cisco AP Name................... AP1131:46f2.98ac
...
AP Mode ........................ Monitor
Public Safety .................. Disabled Disabled
AP SubMode ..................... WIPS
```

次に、アクセス ポイントの wIPS が最適化されたチャネル スキャンの設定を表示する例を示します。

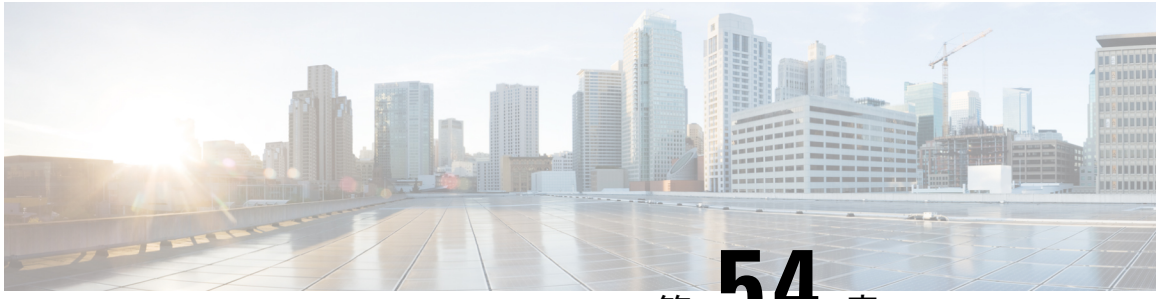
```
Device# show ap monitor-mode summary
AP Name       Ethernet MAC   Status   Scanning
                                      Channel
                                      List
------------- -------------- -------- ---------
AP1131:4f2.9a 00:16:4:f2:9:a WIPS     1,6,NA,NA
```

次に、WCS によってデバイスに転送される wIPS 設定を表示する例を示します。

```
Device# show wireless wps wips summary
Policy Name............. Default
Policy Version.......... 3
```

次に、デバイスでの wIPS 動作の現在の状態を表示する例を示します。

```
Device# show wireless wps wips statistics
Policy Assignment Requests............ 1
Policy Assignment Responses........... 1
Policy Update Requests................ 0
Policy Update Responses............... 0
Policy Delete Requests................ 0
Policy Delete Responses............... 0
Alarm Updates......................... 13572
Device Updates........................ 8376
Device Update Requests................ 0
Device Update Responses............... 0
Forensic Updates...................... 1001
Invalid WIPS Payloads................. 0
Invalid Messages Received............. 0
CAPWAP Enqueue Failed................. 0
NMSP Enqueue Failed................... 0
NMSP Transmitted Packets.............. 22950
NMSP Transmit Packets Dropped......... 0
NMSP Largest Packet................... 1377
```



第 54 章

アクセス ポイントの認証の設定

- 機能情報の確認 （1059 ページ）
- アクセス ポイントの認証を設定するための前提条件 （1059 ページ）
- アクセス ポイントの認証の設定の制約事項 （1060 ページ）
- アクセス ポイントに対する認証の設定について （1060 ページ）
- アクセス ポイントの認証の設定方法 （1061 ページ）
- アクセス ポイントの認証の設定例 （1067 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

アクセス ポイントの認証を設定するための前提条件

- デバイスに現在 join しているすべてのアクセス ポイント、また今後 join するアクセスポイントがデバイスに join するときに継承するグローバル ユーザ名、パスワード、およびイネーブルパスワードを設定することができます。必要に応じて、このグローバル資格情報よりも優先される、独自のユーザ名、パスワード、およびイネーブルパスワードを特定のアクセス ポイントに割り当てることができます。
- アクセス ポイントをデバイスに join すると、そのアクセス ポイントのコンソール ポートセキュリティが有効になり、コンソール ポートへログインするたびにユーザ名とパスワードの入力を要求されます。ログインした時点では非特権モードのため、特権モードを使用するには、イネーブル パスワードを入力する必要があります。

- デバイスで設定したグローバル資格情報はデバイスやアクセス ポイントをリブートした後も保持されます。この情報が上書きされるのは、アクセス ポイントを、グローバル ユーザ名およびパスワードが設定された新しいデバイスにjoinした場合のみです。グローバル資格情報を使って新しいデバイスを設定しなかった場合、このアクセス ポイントは最初のデバイスに設定されているグローバル ユーザ名とパスワードをそのまま保持します。
- アクセス ポイントにより使用される資格情報を追跡する必要があります。そうしないと、アクセス ポイントのコンソール ポートにログインできなくなることがあります。アクセス ポイントをデフォルトの *Cisco/Cisco* ユーザ名およびパスワードに戻す必要がある場合は、デバイスの設定をクリアする必要があります。これにより、アクセス ポイントの設定は工場出荷時のデフォルト設定に戻ります。デフォルトのアクセス ポイント設定をリセットするには、**ap name** *Cisco_AP* **mgmtuser username** *Cisco* **password** *Cisco* コマンドを入力します。コマンドを入力しても、アクセス ポイントの固定 IP アドレスはクリアされません。アクセス ポイントがデバイスに再 join すると、デフォルトの *Cisco/Cisco* のユーザ名およびパスワードを適用します。
- 現在デバイスに join している、また、今後 join するすべてのアクセス ポイントにグローバル認証を設定できます。必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセス ポイントに割り当てることができます。
- この機能は、次のハードウェアによりサポートされます。
  - 認証をサポートするすべての Cisco スイッチ。
  - Cisco Aironet 1140、1260、1310、1520、1600、2600、3500、および 3600 アクセス ポイント

アクセス ポイントの認証の設定の制約事項

- AP設定におけるデバイス名は、大文字と小文字が区別されます。したがって、AP設定には、必ず正確なシステム名を設定してください。正確に設定しないと、AP フォールバックが機能しません。

アクセス ポイントに対する認証の設定について

Cisco IOS アクセス ポイントには、工場出荷時にデフォルトの enable パスワード *Cisco* が設定されています。このパスワードを使用して、非特権モードでログインすると、ネットワークのセキュリティに対する脅威となる **show** および **debug** コマンドの入力が許可されます。不正アクセスを防止し、ユーザがアクセス ポイントのコンソール ポートからコンフィギュレーション コマンドを入力できるようにするには、デフォルトのイネーブル パスワードを変更する必要があります。

Lightweight アクセス ポイントとシスコのスイッチの間で 802.1X 認証を設定できます。アクセス ポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用するスイッチにより認証されます。

アクセス ポイントの認証の設定方法

アクセス ポイントのグローバル資格情報の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap mgmtuser username** *user_name* **password 0** *passsword* **secret 0** *secret_value* 例： `Device(config)# ap mgmtuser apusr1 password appass 0 secret 0 appass1`	デバイスに現在joinしているすべてのアクセス ポイント、および今後デバイスに join するアクセス ポイントに対し、グローバル ユーザ名とパスワードを設定し、パスワードをイネーブルにします。このコマンドでは、パラメータ 0 は暗号化されていないパスワードが続くことを指定し、8 は AES 暗号化パスワードが続くことを指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**ap name** *Cisco_AP* **mgmtuser username** *user_name* **password** *password* **secret** *secret* 例： `Device(config)# ap name TSIM_AP-2 mgmtuser apusr1 password appass secret secret`	特定のアクセス ポイントのグローバル資格情報を上書きし、固有のユーザ名とパスワードを割り当て、このアクセス ポイントに対しパスワードをイネーブルにします。 このコマンドに入力した資格情報は、デバイスやアクセス ポイントをリブートした後や、アクセス ポイントが新しい

	コマンドまたはアクション	目的
		デバイスにjoinされた場合でも保持されます。 （注） このアクセスポイントでデバイスのグローバル資格情報を強制的に使用する必要がある場合は、**ap name** *Cisco_AP* **no mgmtuser** コマンドを入力します。このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。
ステップ 6	**show ap summary** 例： `Device# show ap summary`	接続されたすべてのCisco APのサマリーを表示します。
ステップ 7	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name AP02 config general`	特定のアクセス ポイントのグローバル資格情報の設定を表示します。 （注） このアクセス ポイントがグローバル クレデンシャル用に設定されている場合は、[AP User Mode] テキスト ボックスに [Automatic] と表示されます。このアクセス ポイントのグローバル クレデンシャルが上書きされている場合は、[AP User Mode] テキスト ボックスに [Customized] と表示されます。

アクセス ポイントの認証の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap dot1x username** *user_name_value* **password 0** *password_value* 例： `Device(config)# ap dot1x username AP3 password 0 password`	にデバイス現在 join しているすべてのアクセス ポイント、または今後 join するデバイスアクセスポイントにグローバル認証のユーザ名とパスワードを設定します。このコマンドには、次のキーワードと引数が含まれます。 • **username**：すべてのアクセス ポイントの 802.1X ユーザ名を指定します。 • *user-id*：ユーザ名。 • **password**：すべてのアクセス ポイントの 802.1X パスワードを指定します。 • **0**：暗号化されないパスワードを指定します。 • **8**：AES 暗号化パスワードを指定します。 • *passwd*：パスワード。 （注） password パラメータには強力なパスワードを入力する必要があります。強力なパスワードの長さは少なくとも 8 文字で、大文字と小文字、数字、および記号の組み合わせを含み、いずれの言語の単語でもありません。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**ap name** *Cisco_AP* **dot1x-user username** *username_value* **password** *password_value*	グローバル認証設定を無効にし、独自のユーザ名およびパスワードを特定のアクセス ポイントに割り当てます。こ

	コマンドまたはアクション	目的
	例： `Device# ap name AP03 dot1x-user username apuser1 password appass`	のコマンドには、次のキーワードと引数が含まれます。 • **username**：ユーザ名を追加するように指定します。 • *user-id*：ユーザ名。 • **password**：パスワードを追加するように指定します。 • **0**：暗号化されないパスワードを指定します。 • **8**：AES 暗号化パスワードを指定します。 • *passwd*：パスワード。 （注） password パラメータには強力なパスワードを入力する必要があります。強力なパスワードの特徴については、ステップ 2 の注記を参照してください。 このコマンドに入力した認証設定は、デバイスやアクセスポイントをリブートした後や、アクセスポイントが新しいデバイスに join された場合でも保持されます。
ステップ 6	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 7	**no ap dot1x username** *user_name_value* **password 0** *password_value* 例：	すべてのアクセスポイントまたは特定のアクセス ポイントに対して 802.1X 認証をディセーブルにします。 このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。

	コマンドまたはアクション	目的
	`Device(config)# no ap dot1x username dot1xusr password 0 dot1xpass`	（注） 特定のアクセス ポイントの 802.1X 認証は、グローバル 802.1X認証が有効でない場合にだけ無効にできます。グローバル 802.1X 認証が有効な場合は、すべてのアクセス ポイントに対してだけ 802.1X を無効にできます。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。
ステップ 9	**show ap summary** 例： `Device# show ap summary`	デバイスに join するすべてのアクセス ポイントの認証設定を表示します。 （注） グローバルな認証が設定されていない場合、[Global AP Dot1x User Name] テキスト ボックスには「Not Configured」と表示されます。
ステップ 10	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name AP02 config general`	特定のアクセスポイントの認証設定を表示します。 （注） このアクセス ポイントがグローバル認証用に設定されている場合は、[AP Dot1x User Mode] テキスト ボックスに「Automatic」と表示されます。このアクセスポイントのグローバル認証設定が上書きされている場合は、[AP Dot1x User Mode] テキスト ボックスに「Customized」と表示されます。

関連トピック

アクセス ポイントの認証設定の表示：例 （1067 ページ）

認証のスイッチの設定（CLI）

（注） デバイス GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	システム認証制御をイネーブルにします。
ステップ 4	**aaa new-model** 例： `Device(config)# aaa new-model`	新しいアクセスコントロールコマンドと機能をイネーブルにします
ステップ 5	**aaa authentication dot1x default group radius** 例： `Device(config)# aaa authentication dot1x default group radius`	サーバ グループ内のすべての RADIUS ホストを使用して、IEEE 802.1X のデフォルトの認証リストを設定します。
ステップ 6	**radius-server host** *host_ip_adress* **acct-port** *port_number* **auth-port** *port_number* **key 0** *unencryptied_server_key* 例： `Device(config)# radius-server host 10.1.1.1 acct-port 1813 auth-port 6225 key 0 encryptkey`	RADIUS 認証サーバのクリア テキストの暗号キーを設定します。
ステップ 7	**interface TenGigabitEthernet1/0/1** 例：	10 ギガビット イーサネット インターフェイスを設定します。

	コマンドまたはアクション	目的
	`Device(config)# interface TenGigabitEthernet1/0/1`	コマンド プロンプトが Controller(config)# から Controller(config-if)# に変更します。
ステップ 8	**switch mode access** 例： `Device(config-if)# switch mode access`	インターフェイスへの無条件の truncking モード アクセスを設定します。
ステップ 9	**dot1x pae authenticator** 例： `Device(config-if)# dot1x pae authenticator`	オーセンティケータとして 802.1X インターフェイスの PAE タイプを設定します。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

アクセス ポイントの認証設定の表示：例 （1067 ページ）

アクセス ポイントの認証の設定例

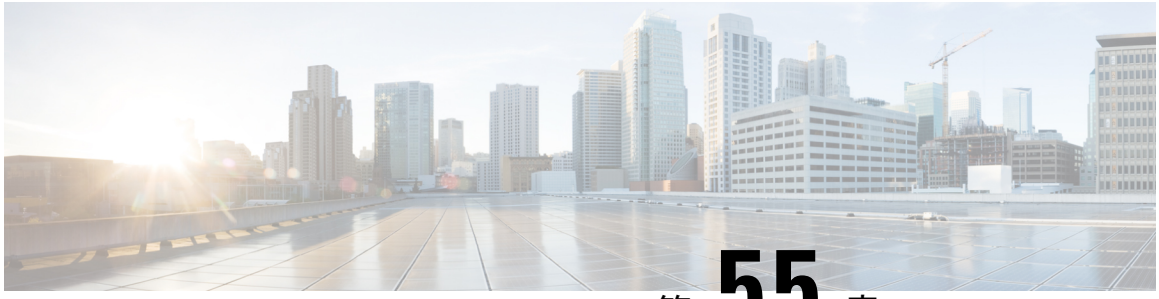
アクセス ポイントの認証設定の表示：例

次に、デバイスに接続するすべてのアクセス ポイントの認証設定を表示する例を示します。

```
Device# show ap summary
Number of APs.................................... 1
Global AP User Name.............................. globalap
Global AP Dot1x User Name........................ globalDot1x
```

次に、特定のアクセス ポイントの認証設定を表示する例を示します。

```
Device# show ap name AP02 config dot11 24ghz general
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... TSIM_AP2
...
AP Dot1x User Mode............................... AUTOMATIC
AP Dot1x User Name............................... globalDot1x
```



第 55 章

自律アクセス ポイントの Lightweight モードへの変換

- 機能情報の確認 （1069 ページ）
- Autonomous アクセス ポイントの Lightweight モードへの変換の前提条件 （1070 ページ）
- Lightweight モードに変換される Autonomous アクセス ポイントについて （1070 ページ）
- Lightweight アクセス ポイントの Autonomous アクセス ポイントへの再変換方法 （1072 ページ）
- アクセス ポイントの認可（CLI） （1073 ページ）
- 変換したアクセス ポイントでの Reset ボタンのディセーブル化（CLI） （1075 ページ）
- AP クラッシュ ログ情報のモニタリング （1076 ページ）
- アクセス ポイントでの固定 IP アドレスの設定方法 （1076 ページ）
- TFTP リカバリ手順を使用したアクセス ポイントのリカバリ （1078 ページ）
- Autonomous アクセス ポイントを Lightweight モードに変換する場合の設定例 （1078 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

Autonomous アクセス ポイントの Lightweight モードへの変換の前提条件

- Lightweight モードに変換したアクセス ポイントは、無線ドメイン サービス（WDS）をサポートしません。変換したアクセス ポイントは、Cisco ワイヤレス LAN デバイスとのみ通信し、WDS デバイスとは通信できません。ただし、アクセス ポイントがコントローラにアソシエートする際、デバイスが WDS に相当する機能を提供します。
- すべての Cisco Lightweight アクセス ポイントでは、無線ごとに 16 の Basic Service Set Identifier（BSSID）およびアクセス ポイントごとに合計 16 のワイヤレス LAN をサポートします。変換されたアクセス ポイントがデバイスにアソシエートすると、アクセス ポイントがアクセス ポイント グループのメンバーでない限り、ID 1～16 のワイヤレス LAN のみがアクセス ポイントにプッシュされます。
- Lightweight モードに変換したアクセス ポイントは、DHCP、DNS、または IP サブネット ブロードキャストを使用して IP アドレスを取得し、デバイスを検出する必要があります。

Lightweight モードに変換される Autonomous アクセス ポイントについて

Autonomous Cisco Aironet アクセス ポイントを Lightweight モードに変換できます。アクセス ポイントを Lightweight モードにアップグレードしようとすると、アクセス ポイントはデバイスと通信し、デバイスから構成およびソフトウェア イメージを受信します。

Lightweight モードから Autonomous モードへの復帰

Autonomous アクセス ポイントを Lightweight モードに変換してから、Autonomous モードをサポートする Cisco IOS リリース（Cisco IOS リリース 12.3(7)JA 以前のリリース）をロードして、そのアクセス ポイントを Lightweight 装置から Autonomous 装置に戻すことができます。アクセス ポイントがデバイスに関連付けられている場合、デバイスを使用して Cisco IOS リリースをロードします。アクセス ポイントがデバイスに関連付けられていない場合、TFTP を使用して Cisco IOS リリースをロードします。いずれの方法でも、ロードする Cisco IOS Release を含む TFTP サーバにアクセス ポイントがアクセスできる必要があります。

DHCP オプション 43 および DHCP オプション 60 の使用

Cisco Aironet アクセス ポイントは、DHCP オプション 43 に Type-Length-Value（TLV）形式を使用します。DHCP サーバは、アクセス ポイントの DHCP ベンダー クラス ID（VCI）文字列に基づいてオプションを返すよう、プログラムする必要があります（DHCP オプション 60）。

DHCP オプション 43 の設定方法については、ご使用の DHCP サーバの製品ドキュメンテーションを参照してください。『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*』には、DHCP サーバのオプション 43 の設定手順の例が記載されています。

アクセス ポイントが、サービス プロバイダー オプション AIR-OPT60-DHCP を選択して注文された場合、そのアクセス ポイントの VCI 文字列は、前の表にある VCI 文字列と異なります。VCI 文字列の末尾には「ServiceProvider」が付きます。たとえば、このオプションが付いた 1260 は、VCI 文字列「Cisco AP c1260-ServiceProvider」を返します。

（注） DHCP サーバから取得するデバイスの IP アドレスは、ユニキャスト IP アドレスになります。DHCP オプション 43 を設定する場合は、デバイスの IP アドレスをマルチキャスト アドレスとして設定しないでください。

変換したアクセスポイントがクラッシュ情報をデバイスに送信する方法

変換したアクセス ポイントが予期せずリブートした場合、アクセス ポイントではクラッシュ発生時にローカル フラッシュ メモリ上にクラッシュ ファイルが保存されます。装置がリブートしたら、アクセスポイントはリブートの理由をデバイスに送信します。クラッシュにより装置がリブートした場合、デバイスは既存の CAPWAP メッセージを使用してクラッシュ ファイルを取得し、デバイスのフラッシュ メモリに保存します。クラッシュ情報のコピーは、デバイスがアクセス ポイントから取得した時点で、アクセス ポイントのフラッシュ メモリから削除されます。

変換したアクセス ポイントからのメモリ コア ダンプのアップロード

デフォルトでは、Lightweight モードに変換したアクセス ポイントは、デバイスにメモリ コア ダンプを送信しません。このセクションでは、デバイス GUI または CLI を使用してアクセス ポイント コア ダンプをアップロードする手順について説明します。

変換されたアクセス ポイントの MAC アドレスの表示

コントローラが変換されたアクセス ポイントの MAC アドレスをコントローラ GUI の情報ページに表示する方法には、いくつか異なる点があります。

- [AP Summary] ページには、コントローラにより変換されたアクセス ポイントのイーサネット MAC アドレスのリストが表示されます。
- [AP Detail] ページには、変換されたアクセス ポイントの BSS MAC アドレスとイーサネット MAC アドレスのリストが、コントローラにより表示されます。
- [Radio Summary] ページには、変換されたアクセス ポイントのリストがデバイスにより無線 MAC アドレス順に表示されます。

Lightweight アクセス ポイントの静的 IP アドレスの設定

DHCP サーバに IP アドレスを自動的に割り当てさせるのではなく、アクセス ポイントに IP アドレスを指定する場合は、コントローラ GUI または CLI を使用してアクセス ポイントに固定 IP アドレスを設定できます。静的 IP アドレスは、通常、AP 数の限られた導入でのみ使用されます。

静的 IP アドレスがアクセス ポイントに設定されている場合は、DNS サーバと、アクセス ポイントが属するドメインとを指定しない限り、アクセス ポイントはドメイン ネーム システム（DNS）解決を使用してデバイスを検出できません。これらのパラメータは、デバイス CLI または GUI のいずれかを使用して設定できます。

（注） アクセス ポイントを設定して、アクセス ポイントの以前の DHCP アドレスが存在したサブネット上にない固定 IP アドレスを使用すると、そのアクセス ポイントはリブート後に DHCP アドレスにフォール バックします。アクセス ポイントが DHCP アドレスにフォール バックした場合は、**show ap config general** *Cisco_AP* CLI コマンドを入力すると、アクセス ポイントがフォールバック IP アドレスを使用していることが表示されます。ただし、GUI は固定 IP アドレスと DHCP アドレスの両方を表示しますが、DHCP アドレスをフォールバック アドレスであるとは識別しません。

Lightweight アクセス ポイントの Autonomous アクセス ポイントへの再変換方法

Lightweight アクセス ポイントを Autonomous モードに戻す方法（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *Cisco_AP* **tftp-downgrade** *tftp_server_ip_address tftp_server_image_filename* 例： `Device# ap name AP02 tftp-downgrade 10.0.0.1 tsrvname`	Lightweight アクセス ポイントを Autonomous モードに戻します。 （注） このコマンドを入力したら、アクセス ポイントが再起動するまで待機し、CLI または GUI を使用してアクセス ポイントを再設定します。

モード ボタンと TFTP サーバを使用して Lightweight アクセス ポイントを Autonomous モードに戻す方法

手順

ステップ 1 TFTP サーバ ソフトウェアを実行している PC に、10.0.0.2 ～ 10.0.0.30 の範囲に含まれる固定 IP アドレスを設定します。

ステップ 2 コンピュータの TFTP サーバ フォルダにアクセス ポイントのイメージ ファイル（たとえば、1140 シリーズ アクセス ポイントの場合は *c1140-k9w7-tar.123-7.JA.tar* ）が存在すること、およびその TFTP サーバがアクティブであることを確認します。

ステップ 3 TFTP サーバ フォルダ内の 1140 シリーズ アクセス ポイントのイメージ ファイルの名前を **c1140-k9w7-tar.default** に変更します。

ステップ 4 Category 5（CAT 5; カテゴリ 5）のイーサネット ケーブルを使用して、PC をアクセス ポイントに接続します。

ステップ 5 アクセス ポイントの電源を切ります。

ステップ 6 MODE ボタンを押しながら、アクセス ポイントに電源を再接続します。

（注） アクセス ポイントの **MODE** ボタンを有効にしておく必要があります。

ステップ 7 MODE ボタンを押し続けて、ステータス LED が赤色に変わったら（約 20 ～ 30 秒かかります）、MODE ボタンを放します。

ステップ 8 アクセス ポイントがリブートしてすべての LED が緑色に変わった後、ステータス LED が緑色に点滅するまで待ちます。

ステップ 9 アクセス ポイントがリブートしたら、GUI または CLI を使用してアクセス ポイントを再設定します。

アクセス ポイントの認可（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ap auth-list ap-policy authorize-ap** 例： `Device(config)# ap auth-list ap-policy authorize-ap`	アクセスポイントの許可ポリシーを設定します。
ステップ 4	**username** *user_name* **mac aaa attribute list** *list_name* 例： `Device(config)# username aaa.bbb.ccc mac aaa attribute list attrlist`	アクセス ポイントの MAC アドレスをローカルで設定します。
ステップ 5	**aaa new-model** 例： `Device(config)# aaa new-model`	新しいアクセスコントロールコマンドと機能をイネーブルにします
ステップ 6	**aaa authorization credential-download** *auth_list* **local** 例： `Device(config)# aaa authorization credential-download auth_download local`	ローカル サーバから EAP 資格情報をダウンロードします。
ステップ 7	**aaa attribute list** リスト 例： `Device(config)# aaa attribute list alist`	AAA 属性リストの定義を設定します。
ステップ 8	**aaa session-id common** 例： `Device(config)# aaa session-id common`	AAA の共通セッション ID を設定します。
ステップ 9	**aaa local authentication default authorization default** 例： `Device(config)# aaa local authentication default authorization default`	ローカル認証方式リストを設定します。
ステップ 10	**show ap name** *Cisco_AP* **config general** 例： `Device(config)# show ap name AP01 config general`	特定のアクセスポイントに対応する設定情報を表示します。

変換したアクセス ポイントでの Reset ボタンのディセーブル化（CLI）

Lightweight モードに変換したアクセス ポイントの Reset ボタンをイネーブルまたはディセーブルにできます。Reset ボタンには、アクセス ポイントの外面に MODE と書かれたラベルが付けられています。

（注） コントローラ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ap reset-button** 例： `Device(config)# no ap reset-button`	デバイスに関連付けられ、変換したすべてのアクセス ポイントの Reset ボタンをディセーブルにします。 （注） デバイスに関連付けられ、変換したすべてのアクセス ポイントの Reset ボタンをイネーブルにするには、**ap reset-button** コマンドを入力します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**ap name** *Cisco_AP* **reset-button** 例： `Device# ap name AP02 reset-button`	指定した変換済みアクセス ポイントの Reset ボタンをイネーブルにします。

AP クラッシュ ログ情報のモニタリング

（注） デバイス GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**show ap crash-file** 例： `Device# show ap crash-file`	クラッシュ ファイルがデバイスにダウンロードされているかどうかを確認します。

アクセス ポイントでの固定 IP アドレスの設定方法

アクセス ポイントでの固定 IP アドレスの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway* 例： `Device# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2`	アクセス ポイントの固定 IP アドレスを設定します。このコマンドには、次のキーワードと引数が含まれます。 • **ip-address**：Cisco アクセス ポイントの固定 IP アドレスを指定します。 • *ip-address*：Cisco アクセス ポイントの固定 IP アドレス。

	コマンドまたはアクション	目的
		• **netmask**：Cisco アクセス ポイントの固定 IP ネットマスクを指定します。 • *netmask*：Cisco アクセス ポイントの固定 IP ネットマスク。 • **gateway**：Cisco アクセス ポイントゲートウェイを指定します。 • *gateway*：Cisco アクセス ポイントゲートウェイの IP アドレス。 アクセス ポイントがリブートしてデバイスに再 join し、指定した固定 IP アドレスがアクセス ポイントにプッシュされます。固定 IP アドレスがアクセス ポイントに送信された後、DNS サーバの IP アドレスおよびドメイン名を設定できます。アクセス ポイントのリブート後にステップ 3 と 4 を実行します。
ステップ 3	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 4	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 5	**ap static-ip name-server** *nameserver_ip_address* 例： `Device(config)# ap static-ip name-server 10.10.10.205`	特定のアクセス ポイントまたはすべてのアクセス ポイントが DNS 解決を使用してデバイスを検出できるよう DNS サーバを設定します。 （注） DNS サーバ設定を元に戻すには、**no ap static-ip name-server** *nameserver_ip_address* コマンドを入力します。
ステップ 6	**ap static-ip domain** *static_ip_domain* 例： `Device(config)# ap static-ip domain domain1`	特定のアクセス ポイントまたはすべてのアクセス ポイントが属するドメインを設定します。

	コマンドまたはアクション	目的
		（注） ドメイン名の設定を元に戻すには、**no ap static-ip domain** *static_ip_domain* コマンドを入力します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name AP03 config general`	アクセス ポイントの IP アドレス設定を表示します。

TFTPリカバリ手順を使用したアクセスポイントのリカバリ

手順

ステップ 1 必要なリカバリ イメージを Cisco.com（ap3g2-k9w8-tar.152-2.JA.tar）からダウンロードし、ご利用の TFTP サーバのルート ディレクトリにインストールします。

ステップ 2 TFTP サーバをターゲットのアクセス ポイントと同じサブネットに接続して、アクセス ポイントをパワーサイクリングします。アクセス ポイントは TFTP イメージから起動し、デバイスに接続してサイズの大きなアクセス ポイントのイメージをダウンロードし、アップグレード手順を完了します。

ステップ 3 アクセス ポイントが回復したら、TFTP サーバを削除できます。

Autonomous アクセス ポイントを Lightweight モードに変換する場合の設定例

アクセス ポイントの IP アドレス設定の表示：例

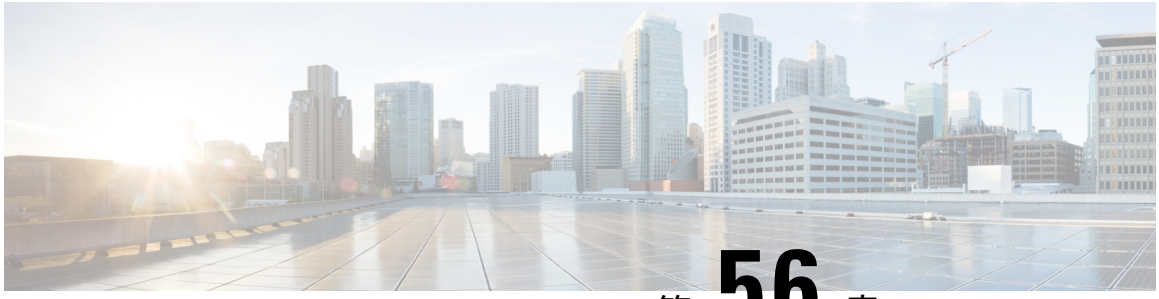
次に、アクセス ポイントの IP アドレス設定を表示する例を示します。

```
Device# show ap name AP03 dot11 24ghz config general
Cisco AP Identifier.............. 4
Cisco AP Name............................. AP6
IP Address Configuration................... Static IP assigned
IP Address................................ 10.10.10.118
IP NetMask................................ 255.255.255.0
Gateway IP Addr........................... 10.10.10.1
Domain.................................... Domain1
Name Server............................... 10.10.10.205
...
```

アクセス ポイントのクラッシュ ファイル情報の表示：例

次の例は、アクセス ポイントのクラッシュ ファイル情報を表示する方法を示しています。このコマンドを使用して、ファイルがデバイスにダウンロードされたかどうかを確認できます。

```
Device# show ap crash-file
Local Core Files:
lrad_AP1130.rdump0 (156)

The number in parentheses indicates the size of the file. The size should
be greater than zero if a core dump file is available.
```



第 56 章

Cisco ワークグループ ブリッジの使用

- 機能情報の確認 （1081 ページ）
- Cisco ワークグループ ブリッジと Cisco 以外のワークグループ ブリッジについて （1081 ページ）
- ワークグループ ブリッジ状態のモニタリング （1082 ページ）
- WGB の問題のデバッグ（CLI） （1082 ページ）
- ワークグループ ブリッジの設定例 （1084 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

Cisco ワークグループ ブリッジと Cisco 以外のワークグループ ブリッジについて

WGB とは、Autonomous IOS アクセス ポイント上で設定でき、イーサネットで WGB アクセス ポイントに接続されたクライアントの代わりに Lightweight アクセス ポイントに無線で接続を提供するモードです。イーサネット インターフェイス上の有線クライアントの MAC アドレスを記憶し、それを Internet Access Point Protocol（IAPP）メッセージングを使用して Lightweight アクセス ポイントに報告することで、WGB は単一の無線セグメントを介して有線ネットワークに接続します。WGB は、単一の無線接続を Lightweight アクセス ポイントに確立して、有線クライアントに無線で接続できるようになります。

Cisco WGB が使用されている場合、WGB は、アソシエートされているすべてのクライアントをアクセス ポイントに通知します。デバイスアクセス ポイントにアソシエートされたクライ

アントを認識します。シスコ以外の WGB が使用されている場合、デバイスには、WGB の後方にある有線セグメントのクライアントの IP アドレスに関する情報は伝わりません。この情報がないと、デバイスは以下の種類のメッセージをドロップします。

- WGB クライアントに対するディストリビューション システムからの ARP REQ
- WGB クライアントからの ARP RPLY
- WGB クライアントからの DHCP REQ
- WGB クライアントに対する DHCP RPLY

ワークグループ ブリッジ状態のモニタリング

（注） デバイス GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**show wireless wgb summary** 例： `Device# show wireless wgb summary`	ネットワーク上のワークグループブリッジ（WGB）を表示します。
ステップ 3	**show wireless wgb mac-address** *wgb_mac_address* **detail** 例： `Device# show wireless wgb mac-address 00:0d:ed:dd:25:82 detail`	特定の WGB に接続されている有線クライアントの詳細を表示します。

WGB の問題のデバッグ（CLI）

（注） デバイス GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**debug iapp all** 例： `Device# debug iapp all`	IAPP メッセージのデバッグをイネーブルにします。
ステップ 3	**debug iapp error** 例： `Device# debug iapp error`	IAPP エラー イベントのデバッグをイネーブルにします。
ステップ 4	**debug iapp packet** 例： `Device# debug iapp packet`	IAPP パケットのデバッグをイネーブルにします。
ステップ 5	**debug mobility handoff** [**switch** *switch_number*] 例： `Device# debug mobility handoff`	ローミング問題のデバッグをイネーブルにします。
ステップ 6	**debug dhcp** 例： `Device# debug dhcp`	DHCP を使用する場合の IP 割り当ての問題をデバッグします。
ステップ 7	**debug dot11 mobile** 例： `Device# debug dot11 mobile`	dot11/モバイルデバッグをイネーブルにします。スタティック IP を使用する場合の IP 割り当ての問題をデバッグします。
ステップ 8	**debug dot11 state** 例： `Device# debug dot11 state`	dot11/ステートデバッグをイネーブルにします。スタティック IP を使用する場合の IP 割り当ての問題をデバッグします。

ワークグループ ブリッジの設定例

WGB の設定：例

次に、40 ビットの WEP キーでスタティック WEP を使用して WGB アクセス ポイントを設定する例を示します。

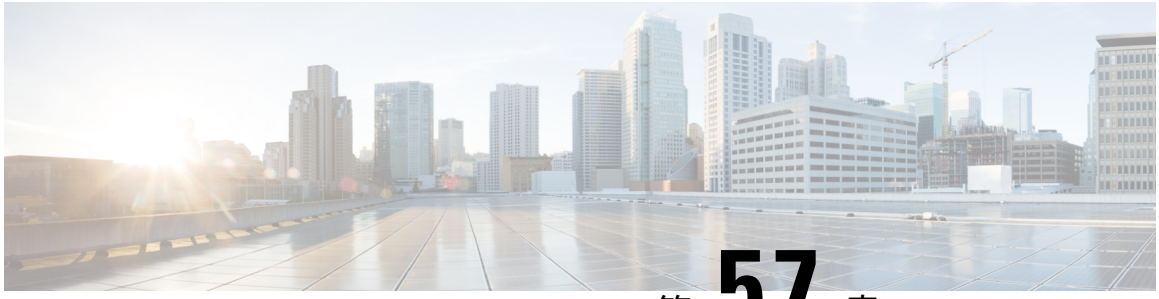
```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# dot11 ssid WGB_with_static_WEP
Device(config-ssid)# authentication open
Device(config-ssid)# guest-mode
Device(config-ssid)# exit
Device(config)# interface  dot11Radio 0
Device(config)# station-role workgroup-bridge
Device(config-if)# encry mode wep 40
Device(config-if)# encry key 1 size 40 0 1234567890
Device(config-if)# ssid WGB_with_static_WEP
Device(config-if)# end
```

この WGB がアクセス ポイントにアソシエートしていることを確認するには、WGB に次のコマンドを入力します。

show dot11 association

以下に類似した情報が表示されます。

```
Device# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address    IP address      Device        Name            Parent         State
000b.8581.6aee 10.11.12.1      WGB-client    map1            -              Assoc
ap#
```



第 57 章

プローブ要求フォワーディングの設定

- 機能情報の確認 （1085 ページ）
- プローブ要求フォワーディングの設定について （1085 ページ）
- プローブ要求フォワーディングの設定方法（CLI） （1085 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

プローブ要求フォワーディングの設定について

プローブ要求とはクライアントが送信する 802.11 管理フレームであり、SSID の機能についての情報を要求します。デフォルトでは、アクセス ポイントは応答済みのプローブ要求をデバイスが処理できるよう送信します。応答済みの（acknowledged）プローブ要求とは、アクセス ポイントがサポートする SSID のプローブ要求です。必要に応じて、応答済みのプローブ要求および未応答のプローブ要求の両方をデバイスにフォワードするようアクセス ポイントを設定できます。デバイスは応答済みのプローブ要求からの情報を使用してロケーションの精度を向上できます。

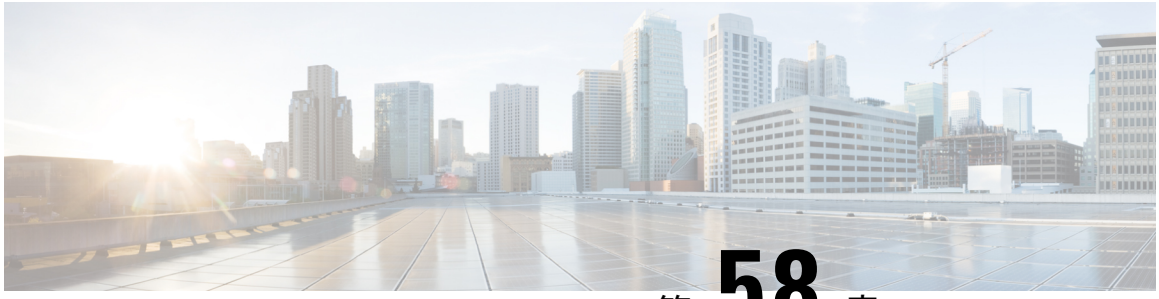
プローブ要求フォワーディングの設定方法（CLI）

（注） デバイス GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless probe filter** 例： `Device(config)# wireless probe filter`	アクセス ポイントからデバイスに転送されたプローブ要求のフィルタリングをイネーブルまたはディセーブルにします。 （注） デフォルトのフィルタ設定であるプローブ フィルタリングを有効にすると、アクセス ポイントは応答済みのプローブ要求のみをデバイスに転送します。プローブ フィルタリングを無効にすると、アクセス ポイントは応答済みのプローブ要求と未応答のプローブ要求の両方をデバイスに転送します。
ステップ 3	**wireless probe filter** *num_probes interval* 例： `Device(config)# wireless probe filter 5 5`	指定された間隔のアクセス ポイント無線ごとにクライアント単位でデバイスに送信されるプローブ要求の数を制限します。このコマンドで次の引数を指定する必要があります。 • *num_probes*：指定された間隔での、1 つのアクセス ポイント無線および 1 つのクライアントあたりのデバイスへ送られたプローブ要求数。範囲は 1 ～ 100 です。 • *interval*：ミリ秒単位でのプローブ制限間隔。範囲は 100 ～ 10000 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

	コマンドまたはアクション	目的
ステップ 5	**show wireless probe** 例： `Device# show wireless probe`	詳細なプローブ要求の設定を表示します。



第 58 章

RFID トラッキングの最適化

- 機能情報の確認 （1089 ページ）
- アクセス ポイントでの RFID トラッキングの最適化 （1089 ページ）
- アクセス ポイントでの RFID トラッキングの最適化方法 （1090 ページ）
- RFID トラッキングの最適化の設定例 （1091 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

アクセス ポイントでの RFID トラッキングの最適化

RFID タグの監視とロケーション計算を最適化するには、802.11b/g アクセス ポイント無線用の 2.4GHz 帯域内で最高 4 つのチャネルでトラッキングの最適化を有効化できます。この機能を使用して、通常、タグが動作するようにプログラムされているチャネル（チャネル 1、6、11 など）のみをスキャンすることができます。

アクセス ポイントでの RFID トラッキングの最適化方法

アクセス ポイントでの RFID トラッキングの最適化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *Cisco_AP* **mode monitor submode none** 例： `Device# ap name 3602a mode monitor submode none`	アクセス ポイントの監視サブモードを none として指定します。 （注） アクセス ポイントのモードを変更するとアクセス ポイントがリブートすることを示す警告メッセージが表示され、**Y** を入力することで続行するかどうかを指定するプロンプトが表示されます。 **Y**を入力すると、アクセスポイントがリブートします。
ステップ 2	**ap name** *Cisco_AP* **dot11 24ghz shutdown** 例： `Device# ap name AP01 dot11 24ghz shutdown`	アクセス ポイント無線をディセーブルにします。
ステップ 3	**ap name** *Cisco_AP* **monitor-mode tracking-opt** 例： `Device# ap name TSIM_AP1 monitor-mode tracking-opt`	使用する国でサポートされる動的チャネル割り当て（DCA）チャネルのみをスキャンするようにアクセス ポイントを設定します。 （注） アクセス ポイントのトラッキングの最適化をディセーブルにするには、**ap name** *Cisco_AP* **monitor-mode tracking-opt no-optimization** コマンドを入力します。

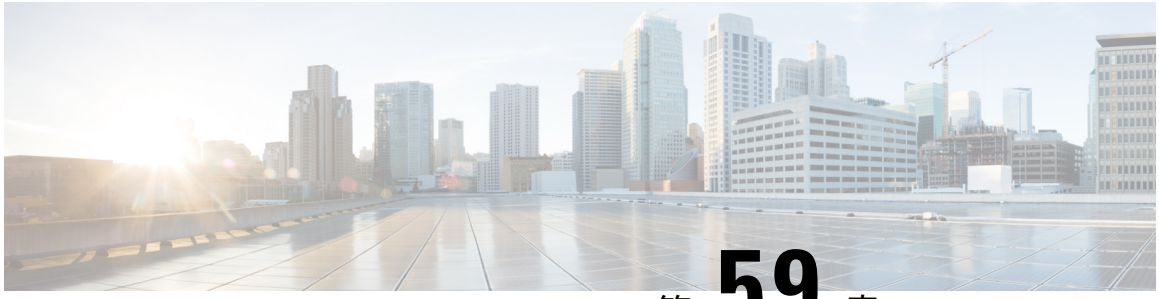
	コマンドまたはアクション	目的
ステップ 4	**ap name** *Cisco_AP* **monitor-mode dot11b** {**fast-channel** [*first_channel second_channel third_channel fourth_channel*]} 例： `Device# ap name AP01 monitor-mode dot11b fast-channel 1 2 3 4`	アクセス ポイントによりスキャンされる特定の 802.11b チャネルを最大 4 つ選択します。 （注） 米国では、チャネル変数に 1 ～ 11 の値（両端の値を含む）を割り当てることができます。その他の国ではさらに多くのチャネルがサポートされています。少なくともチャネルを 1 つ割り当てる必要があります。
ステップ 5	**ap name** *Cisco_AP* **no dot11 24ghz shutdown** 例： `Device# ap name AP01 no dot11 24ghz shutdown`	アクセス ポイント無線をイネーブルにします。
ステップ 6	**show ap monitor-mode summary** 例： `Device# show ap monitor-mode summary`	モニタ モードですべてのアクセス ポイントを表示します。

RFID トラッキングの最適化の設定例

モニタ モードでのすべてのアクセス ポイントの表示：例

次に、モニタ モードですべてのアクセス ポイントを表示する例を示します。

```
Device# show ap monitor-mode summary

AP Name       Ethernet MAC   Status   Scanning
                                      Channel
                                      List
------------- -------------- -------- ---------
AP1131:4f2.9a 00:16:4:f2:9:a Tracking 1,6,NA,NA
```



第 59 章

国番号の設定

- 機能情報の確認 （1093 ページ）
- 国番号の設定の前提条件 （1093 ページ）
- 国番号の設定について （1094 ページ）
- 国番号の設定方法（CLI） （1094 ページ）
- 国番号の設定例 （1097 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

国番号の設定の前提条件

- 通常、デバイスごとに 1 つの国番号を設定します。そのデバイスの物理的な場所とそのアクセス ポイントが一致しているコードを 1 つ設定します。デバイスごとに最大 20 の国番号を設定できます。これによって、複数の国がサポートされ、1 つのデバイスからさまざまな国にあるアクセス ポイントを管理できます。
- multiple-country 機能を使用している場合、同じ RF グループに join する予定のすべてのデバイスは、同じ国のセットを同じ順序で設定する必要があります。
- アクセス ポイントは、使用可能なすべての法定周波数を使用できます。ただし、アクセス ポイントは関連するドメインでサポートされる周波数に割り当てられます。
- RF グループ リーダーに設定されている国リストによって、メンバーが動作するチャネルが決定します。このリストは、RF グループ メンバーに設定されている国とは無関係です。

- 日本の規制ドメインにあるデバイスの場合は、最後にデバイスをブートしたときにデバイスで設定した 1 つ以上の日本の国番号（JP、J2、または J3）を持っている必要があります。
- 日本の規制ドメインにあるデバイスの場合は、デバイスに join された - J 規制ドメインのアクセス ポイントを少なくとも 1 つ持っている必要があります。

国番号の設定について

コントローラおよびアクセスポイントは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。アクセスポイント内の無線は、製造時に特定の規制区域に割り当てられています（ヨーロッパの場合には E など）。しかし、Country Code を使用すると、稼働する特定の国を指定できます（フランスの場合には FR、スペインの場合には ES など）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

日本の国番号について

国番号は、各国で合法的に使用できるチャネルを定義します。日本で使用できる Country Code は、次のとおりです。

- JP：コントローラに join できるのは、-J 無線のみです。
- J2：コントローラに join できるのは、-P 無線のみです。
- J3：WLC に join できるのは、-U、-P、および -Q（1550/1600/2600/3600 以外）無線ですが、-U の周波数を使用します。
- J4：コントローラに join できるのは、2.4G JPQU および 5G PQU です。

（注） 1550、1600、2600、および 3600 AP には J4 が必要です。

日本の規制区域のアクセスポイントでサポートされているチャネルと電力レベルの一覧については、『*Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points*』を参照してください。

国番号の設定方法（CLI）

（注） デバイス GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**show wireless country supported** 例： `Device# show wireless country supported`	すべての使用可能な国番号のリストを表示します。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**ap dot11 24ghz shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	802.11a ネットワークをディセーブルにします。
ステップ 5	**ap dot11 5ghz shutdown** 例： `Device(config)# ap dot11 24ghz shutdown`	802.11b/g ネットワークをディセーブルにします。
ステップ 6	**ap country** *country_code* 例： `Device(config)# ap country IN`	特定の国にアクセスポイントを割り当てます。 （注） 選択した Country Code が、アクセスポイントの無線のうち少なくとも 1 つの無線の規制ドメインに適合していることを確認します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。
ステップ 8	**show wireless country channels** 例： `Device# show wireless country channels`	デバイスに設定された国番号の使用可能なチャネルのリストを表示します。 （注） ステップ 6 で複数の国番号を設定した場合にのみ、ステップ 9 ～ 17 を実行します。

	コマンドまたはアクション	目的
ステップ 9	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 10	**no ap dot11 5ghz shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	802.11a ネットワークをイネーブルにします。
ステップ 11	**no ap dot11 24ghz shutdown** 例： `Device(config)# no ap dot11 24ghz shutdown`	802.11b/g ネットワークをイネーブルにします。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。
ステップ 13	**ap name** *Cisco_AP* **shutdown** 例： `Device# ap name AP02 shutdown`	アクセスポイントをディセーブルにします。 （注） 国番号を設定しているアクセスポイントのみをディセーブルにすることを確認します。
ステップ 14	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 15	**ap country** *country_code* 例： `Device# ap country IN`	アクセスポイントを特定の国に割り当てます。 （注） 選択した国番号が、アクセスポイントの無線のうち少なくとも 1 つの無線の規制ドメインに適合していることを確認します。

	コマンドまたはアクション	目的
		（注） ネットワークをイネーブルにし、いくつかのアクセスポイントをディセーブルにして、**ap country** *country_code* コマンドを入力した場合、指定された国番号は、ディセーブルにされたアクセスポイントでのみ設定されます。他のアクセスポイントは、すべて無視されます。
ステップ 16	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。
ステップ 17	**ap name** *Cisco_AP* **no shutdown** 例： `Device# ap name AP02 no shutdown`	アクセス ポイントを有効にします。

国番号の設定例

国番号のチャネル リストの表示：例

次に、デバイスに設定されている国番号に使用可能なチャネルの一覧を表示する例を示します。

```
Device# show wireless country channels

Configured Country.......................: US - United States
KEY: * = Channel is legal in this country and may be configured manually.
A = Channel is the Auto-RF default in this country.
. = Channel is not legal in this country.
C = Channel has been configured for use by Auto-RF.
x = Channel is available to be configured for use by Auto-RF.
(-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11bg :
Channels : 1 1 1 1 1
: 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US : A * * * * A * * * * A . . .
Auto-RF : . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11a : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
: 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

```
(-A ,-AB ) US : . A . A . A . A A A A A * * * * * . . . * * * A A A A
*
Auto-RF : . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
4.9GHz 802.11a :
Channels : 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
: 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
US (-A ,-AB ): * * * * * * * * * * * * * * * * * * A * * * * * A
Auto-RF : . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

第 60 章

リンク遅延の設定

- 機能情報の確認 （1099 ページ）
- リンク遅延の設定の前提条件 （1099 ページ）
- リンク遅延の設定の制約事項 （1100 ページ）
- リンク遅延の設定について （1100 ページ）
- リンク遅延の設定方法 （1101 ページ）
- TCP MSS の設定方法 （1104 ページ）
- リンク テストの実行（CLI） （1105 ページ）
- リンク遅延の設定例 （1105 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

リンク遅延の設定の前提条件

- デバイスにより、現在のラウンドトリップ時間および継続的な最短および最長ラウンドトリップ時間が表示されます。最短および最長時間はデバイスが動作している限り維持され、クリアして再開することもできます。
- デバイス GUI または CLI を使用して特定のアクセス ポイントのリンク遅延を設定することも、CLI を使用してデバイスに join されたすべてのアクセス ポイントのリンク遅延を設定することもできます。

リンク遅延の設定の制約事項

- リンク遅延は、アクセス ポイントとデバイス間の Control and Provisioning of Wireless Access Points（CAPWAP）の応答所要時間を計算します。ネットワーク遅延や ping 応答は計測しません。

リンク遅延の設定について

デバイスでリンク遅延を設定して、アクセスポイントとデバイスとの間のリンクを計測できます。この機能は、リンクが低速または信頼できない WAN 接続の可能性があるデバイスに接続されたすべてのアクセス ポイントで使用できます。

TCP MSS

トランスミッション コントロール プロトコル（TCP）スリーウェイ ハンドシェイクにおけるクライアントの最大セグメントサイズ（MSS）が、最大伝送単位で処理できるサイズよりも大きい場合、スループットの低下およびパケットのフラグメンテーションが発生する場合があります。この問題を回避するには、デバイスに接続されているすべてのアクセスポイント、または特定のアクセス ポイントに対して、MSS を指定します。

この機能を有効にすると、アクセス ポイントがデータ パスのワイヤレス クライアントと送受信する TCP パケットの MSS を選択します。これらのパケットの MSS が設定した値または CAPWAP トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、設定された新しい値に変更します。

リンク テスト

リンクテストを使用して、2つのデバイス間の無線リンクの質を決定します。リンクテストの際には、要求と応答の 2 種類のリンク テスト パケットを送信します。リンク テストの要求パケットを受信した無線は、適切なテキスト ボックスを記入して、応答タイプ セットを使用して送信者にパケットを返信します。

クライアントからアクセス ポイント方向への無線リンクの質は、アクセス ポイントからクライアント方向へのものと異なることがあり、それは双方の送信電力と受信感度が非対称であることによるものです。2 種類のリンク テスト（ping テストおよび CCX リンク テスト）を実行できます。

ping リンク テストでは、コントローラはクライアントからアクセス ポイント方向でのみリンクの質をテストできます。アクセスポイントで受信された ping パケットの RF パラメータは、クライアントからアクセス ポイント方向のリンクの質を決定するためにコントローラによりポーリングされます。

CCX リンク テストでは、デバイスはアクセス ポイントからクライアントの方向でもリンクの質をテストできます。デバイスはクライアントにリンク テスト要求を発行し、クライアント

は、応答パケットで受信した要求パケットの RF パラメータ（受信信号強度インジケータ [RSSI]、信号対雑音比 [SNR] など）を記録します。リンク テストの要求と応答の両方のロールを、アクセス ポイントとデバイスに実装します。アクセス ポイントまたはデバイスから CCX v4 クライアントまたは v5 クライアントに対してリンク テストを開始できるのと同様に、CCX v4 クライアントまたは v5 クライアントからもアクセス ポイントまたはデバイスに対してリンク テストを開始できます。

デバイスでは、CCX リンク テストでのリンクの質のメトリックが両方向（アウト：アクセス ポイントからクライアント、イン：クライアントからアクセス ポイント）で表示されます。

- RSSI の形式の信号強度（最小、最大、および平均）
- SNR の形式の信号の質（最小、最大、および平均）
- 再試行されたパケットの合計数
- 単一パケットの最大再試行回数
- 消失パケット数
- 正常に送信されたパケットのデータ レート

コントローラにより、方向とは無関係に次のメトリックが表示されます。

- リンク テストの要求/応答の往復時間（最小、最大、および平均）

コントローラ ソフトウェアは、CCX バージョン 1 ～ 5 をサポートします。CCX サポートは、コントローラ上の各 WLAN について自動的に有効となり、無効にできません。コントローラでは、クライアント データベースにクライアントの CCX バージョンが格納されます。このクライアントの機能を制限するには、これを使用します。クライアントが CCX v4 または v5 をサポートしていない場合、コントローラはクライアント上で ping リンク テストを実行します。クライアントが CCX v4 または v5 をサポートしている場合、コントローラはクライアント上で CCX リンク テストを実行します。クライアントが CCX リンク テストの間にタイムアウトになった場合、コントローラは ping リンク テストに自動的に切り替わります。

リンク遅延の設定方法

リンク遅延の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap link-latency** 例： `Device(config)# ap link-latency`	現在デバイスに関連付けられているすべてのアクセス ポイントのリンク遅延をイネーブルにします。 （注） デバイスと関連付けられているすべてのアクセス ポイントのリンク遅延をディセーブルにするには、**no ap link-latency** コマンドを使用します。 （注） これらのコマンドは、現在デバイスにジョインされているアクセス ポイントのリンク遅延のみをイネーブルまたはディセーブルにします。将来ジョインするアクセス ポイントのリンク遅延をイネーブルまたはディセーブルにする必要があります。 （注） このデバイスに関連付けられている特定のアクセス ポイントのリンク遅延をイネーブルまたはディセーブルにするには、特権 EXEC モードで次のコマンドを入力します。 • **ap name** *Cisco_AP* **link-latency**：リンク遅延をイネーブルにします。 • **ap name** *Cisco_AP* **no link-latency**：リンク遅延をディセーブルにします。
ステップ 4	**ap tcp-adjust-mss size** *size* 例： `Device(config)# ap tcp-adjust-mss size 537`	すべてのアクセス ポイントの TCP MSS 調整サイズを設定します。範囲は 536 ～ 1363 です。

	コマンドまたはアクション	目的
ステップ 5	**show ap name** *Cisco_AP* **config general** 例： `Device(config)# show ap name AP02 config general`	アクセス ポイントの一般的な設定の詳細を表示します。これらの設定の詳細には、コマンドで指定したアクセス ポイントに対応するリンク遅延の結果が含まれます。 このコマンドの出力には、次のリンク遅延結果が含まれます。 • [Current Delay]：アクセス ポイントからデバイス、およびその逆の方向の CAPWAP ハートビート パケットの現在のラウンドトリップ時間（ミリ秒）。 • [Maximum Delay]：リンク遅延がイネーブルになったか、またはリセットされてからのアクセス ポイントからデバイス、およびその逆の方向の CAPWAP ハートビート パケットの最長のラウンドトリップ時間（ミリ秒）。 • [Minimum Delay]：リンク遅延がイネーブルになったか、またはリセットされてからのアクセス ポイントからデバイス、およびその逆の方向の CAPWAP ハートビート パケットの最長のラウンドトリップ時間（ミリ秒）。
ステップ 6	**ap name** *Cisco_AP* **link-latency** [**reset**] 例： `Device(config)# ap name AP02 link-latency reset`	特定のアクセス ポイントのデバイスの現在、最短、および最長リンク遅延統計情報をクリアします。
ステップ 7	**show ap name** *Cisco_AP* **config general** 例： `Device(config)# show ap name AP02 config general`	アクセス ポイントの一般的な設定の詳細を表示します。リセット操作の結果を表示するには、このコマンドを使用します。

TCP MSS の設定方法

TCP MSS の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap tcp-adjust-mss size** *size_value* 例： `Device(config)# ap tcp-adjust-mss size 537`	ユーザが指定した特定のアクセス ポイントで TCP MSS をイネーブルにします。 （注） デバイスに関連付けられているすべてのアクセス ポイントで TCP MSS をイネーブルにするには、**ap tcp-adjust-mss size** *size_value* コマンドを入力します。ここで、サイズ パラメータの範囲は 536～1363 バイトです。デフォルト値はクライアントにより異なります。
ステップ 3	**reload** 例： `Device# reload`	変更をイネーブルにするには、デバイスをリブートします。
ステップ 4	**show ap tcp-adjust-mss** 例： `Device# show ap tcp-adjust-mss`	このデバイスに関連付けられているすべてのアクセス ポイントの現在の TCP MSS 設定を表示します。 （注） 特定のアクセス ポイントに対応する TCP MSS 設定を表示するには、**show ap name** *Cisco_AP* **tcp-adjust-mss** コマンドを入力します。

リンク テストの実行（CLI）

（注） デバイス GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**test wireless linktest** *mac_address* 例： `Device# test wireless linktest 00:0d:88:c5:8a:d1`	リンク テストを実行します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**wireless linktest frame-size** *frame_size* 例： `Device(config)# wireless linktest frame-size 41`	各パケットのリンク テスト フレームのサイズを設定します。
ステップ 4	**wireless linktest number-of-frames** *number_of_frames* 例： `Device(config)# wireless linktest number-of-frames 50`	リンク テスト用に送信するフレームの数を設定します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

リンク遅延の設定例

リンク テストの実行：例

次に、リンク テストを実行する例を示します。

```
Device# test wireless linktest 6470.0227.ca55
Device# show wireless linktest statistic
```

```
Link Test to 64700227CA55 with 500 frame-size.
Client MAC Address                           : 6470.0227.ca55
AP Mac Address                               : 44e4.d901.19c0
Link Test Packets Sent                       : 20
Link Test Packets Received                   : 20
Link Test Pkts Lost(Total/AP->Clnt/Clnt->AP) : 0/0/0
Link Test Pkts round trip time (min/max/avg) : 9ms/31ms/14ms
RSSI at AP (min/max/average)                 : -53dBm/-51dBm/-52dBm
RSSI at Client (min/max/average)             : -48dBm/-40dBm/-44dBm
```

リンク遅延情報の表示：例

この例は、アクセスポイントの一般的な設定の詳細を表示する方法を示しています。これらの設定の詳細には、コマンドで指定したアクセスポイントに対応するリンク遅延の結果が含まれます。

```
Device# show ap name AP01 config general

Cisco AP Name                                    : AP01
Cisco AP Identifier                              : 55
Country Code                                     : US  - United States
Regulatory Domain Allowed by Country             : 802.11bg:-A     802.11a:-A
AP Country Code                                  : US  - United States
AP Regulatory Domain                             : Unconfigured
Switch Port Number                               : Te1/0/1
MAC Address                                      : 0000.2000.03f0
IP Address Configuration                         : Static IP assigned
IP Address                                       : 9.9.9.16
IP Netmask                                       : 255.255.0.0
Gateway IP Address                               : 9.9.9.2
Fallback IP Address Being Used                   : 9.9.9.16
Domain                                           : Cisco
Name Server                                      : 0.0.0.0
CAPWAP Path MTU                                  : 1485
Telnet State                                     : Enabled
SSH State                                        : Disabled
Cisco AP Location                                : default-location
Cisco AP Group Name                              : default-group
Primary Cisco Controller Name                    : CAPWAP Controller
Primary Cisco Controller IP Address              : 9.9.9.2
Secondary Cisco Controller Name                  :
Secondary Cisco Controller IP Address            : Not Configured
Tertiary Cisco Controller Name                   :
Tertiary Cisco Controller IP Address             : Not Configured
Administrative State                             : Enabled
Operation State                                  : Registered
AP Mode                                          : Local
AP Submode                                       : Not Configured
Remote AP Debug                                  : Disabled
Logging Trap Severity Level                      : informational
Software Version                                 : 7.4.0.5
Boot Version                                     : 7.4.0.5
Stats Reporting Period                           : 180
LED State                                        : Enabled
PoE Pre-Standard Switch                          : Disabled
PoE Power Injector MAC Address                   : Disabled
Power Type/Mode                                  : Power Injector/Normal Mode
Number of Slots                                  : 2
AP Model                                         : 3502E
AP Image                                         : C3500-K9W8-M
IOS Version                                      :
```

```
Reset Button                                        :
AP Serial Number                                    : SIM1140K002
AP Certificate Type                                 : Manufacture Installed
Management Frame Protection Validation              : Disabled
AP User Mode                                        : Customized
AP User Name                                        : Not Configured
AP 802.1X User Mode                                 : Not Configured
AP 802.1X User Name                                 : Not Configured
Cisco AP System Logging Host                        : 255.255.255.255
AP Up Time                                          : 16 days 3 hours 14 minutes 1 s
econd
AP CAPWAP Up Time                                   : 33 minutes 15 seconds
Join Date and Time                                  : 01/02/2013 22:41:47
Join Taken Time                                     : 16 days 2 hours 40 minutes 45
seconds
Join Priority                                       : 1
Ethernet Port Duplex                                : Auto
Ethernet Port Speed                                 : Auto
AP Link Latency                                     : Enabled
Current Delay                                       : 0
Maximum Delay                                       : 0
Minimum Delay                                       : 0
Last Updated (based on AP up time)                  : 0 seconds
Rogue Detection                                     : Disabled
AP TCP MSS Adjust                                   : Disabled
AP TCP MSS Size                                     : 536
```

TCP MSS 設定の表示：例

次に、デバイスに関連付けられているすべてのアクセス ポイントの現在の TCP MSS 設定を表示する例を示します。

```
Device# show ap tcp-adjust-mss

AP Name                     TCP State        MSS Size
-------------------------------------------------------
AP01                        Disabled         6146
AP02                        Disabled         536
AP03                        Disabled         6146
AP04                        Disabled         6146
AP05                        Disabled         6146
```

第 61 章

Power over Ethernet の設定

- 機能情報の確認 （1109 ページ）
- Power over Ethernet の設定について （1109 ページ）
- Power over Ethernet の設定方法 （1110 ページ）
- Power over Ethernet の設定例 （1111 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

Power over Ethernet の設定について

Lightweight モードに変換されたアクセス ポイント（AP1262 など）アクセス ポイントが Cisco pre-Intelligent Power Management（pre-IPM）スイッチに接続されたパワー インジェクタで電源を供給されている場合、インライン パワーとも呼ばれる Power over Ethernet（PoE）を設定する必要があります。

Power over Ethernet の設定方法

Power over Ethernet の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *Cisco_AP* **power injector installed** 例： `Device# ap name AP02 power injector installed`	PoE パワー インジェクタ状態をイネーブルにします。アクセス ポイントは、パワーインジェクタがこの特定のスイッチ ポートに接続されていることを記憶します。アクセス ポイントを再配置する場合、新しいパワー インジェクタの存在を検証した後で、このコマンドを再度入力する必要があります。 （注） ネットワークに、12 W アクセス ポイントへ直接接続すると過負荷を発生する可能性のある、従来のシスコ 6 W スイッチが装備されている場合には、このコマンドを入力します。このコマンドを入力する前に Cisco Discovery Protocol（CDP）がイネーブルになっていることを確認します。有効になっていない場合、このコマンドは失敗します。
ステップ 2	**ap name** *Cisco_AP* **power injector override** 例： `Device# ap name AP02 power injector override`	セーフティ チェックを解除し、アクセス ポイントが他のスイッチ ポートに接続できるようにします。ネットワークに、12 W アクセス ポイントに直接接続すると過負荷を発生する可能性のある従来のシスコ 6 W スイッチが装備されていない場合は、このコマンドを使用できます。アクセス ポイントは、パワー インジェクタが常に接続されていることを前提としています。アクセス ポイントを再配置した場合も、パワー インジェクタの存在を前提とします。

	コマンドまたはアクション	目的
ステップ 3	**ap name** *Cisco_AP* **power injector switch-mac-address** *switch_mac_address* 例： `Device# ap name AP02 power injector switch-mac-address 10a.2d.5c.3d`	パワーインジェクタが設置されたスイッチ ポートの MAC アドレスを設定します。 （注） 接続スイッチ ポートの MAC アドレスがわかっていて、[Installed] オプションを使用して自動的に検出しない場合は、このコマンドを入力します。
ステップ 4	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name AP02 config general`	特定のアクセス ポイントの PoE 設定を含む共通の情報を表示します。 （注） アクセス ポイントが最大電力で動作していない場合、[Power Type/Mode] テキスト ボックスには、「degraded mode」と表示されます。

Power over Ethernet の設定例

Power over Ethernet 情報の表示：例

次に、特定のアクセス ポイントの PoE 設定を含む共通の情報を表示する例を示します。

```
Device# show ap name AP01 config general

Cisco AP Identifier............... 1
Cisco AP Name..................... AP1
...
PoE Pre-Standard Switch........... Enabled
PoE Power Injector MAC Addr....... Disabled
Power Type/Mode................... PoE/Low Power (degraded mode)
...
```

第 X 部

モビリティ

- モビリティについて （1115 ページ）
- モビリティ ネットワーク要素 （1121 ページ）
- モビリティ制御プロトコル （1125 ページ）
- モビリティの設定 （1133 ページ）

第 62 章

モビリティについて

- 概要 （1115 ページ）
- 有線およびワイヤレス モビリティ （1116 ページ）
- モビリティの機能 （1117 ページ）
- 低遅延ローミングを実現するスティッキ アンカリング （1118 ページ）
- ブリッジ ドメイン ID および L2/L3 ローミング （1119 ページ）
- リンク ダウンの動作 （1119 ページ）
- モビリティ コントローラのプラットフォーム固有のスケール要件 （1120 ページ）

概要

は、単に速度やフィードの増加をもたらすだけではなく、アクセス レイヤでより多くのサービスを提供します。ワイヤレス サービスはスイッチと統合され、アクセス レイヤ スイッチがワイヤレスユーザのデータ プレーンの終端となります。これにより、シスコのユニファイドアーキテクチャを実現できます。統合とは、モビリティ サービスがワイヤレスと有線の両方のステーションに提供されることを意味します。

は、シームレスなローミングを提供します。これには、クライアントに対するネットワーク構成と展開オプションの透過性が必要です。

エンド ユーザの観点からすれば、どのモビリティ イベントも IP アドレス、デフォルト ルータ、またはDHCPサーバを変更することはできません。これは、ステーションがローミングするときに、次のことができるようにする必要があることを意味します。

- デフォルト ルータに ARP を送信します。
- 以前にアドレスを割り当てているサーバに DHCP 要求を送信します。

インフラストラクチャの観点からすれば、モビリティイベントが発生した場合、ステーションのトラフィックは現在の接続ポイントに従う必要があります。これは、モビリティエージェント（MA）またはモビリティ コントローラ（MC）のどちらかです。これは、ステーションが異なるサブネットに設定されたネットワークに移動したかどうかに関係なく当てはまります。ステーションがモビリティイベント後にトラフィックを受信しない期間は、可能な限り短くする必要があります（できれば 40 ms 以下）。これには、必要な認証手順も含まれます。

インフラストラクチャの観点からすれば、モビリティ管理ソリューションには4つの主要なコンポーネントが必要です。これらの機能はすべて、ローミングの制約の範囲内で実行する必要があります。

- 最初のアソシエーション：この機能は、ネットワーク内でユーザの新しい接続ポイントを識別するために使用されます。
- コンテキストの転送：この機能は、ステーションに関連するステート情報を転送するために使用されます。これにより、セキュリティおよびアプリケーション ACL やサービスなど、ステーションの静的なリアルタイム ポリシーがハンドオフ全体にわたって等しく保たれるようにします。
- ハンドオフ：この機能は、ステーションの接続ポイントが変更され、以前のアクセス によってステーションの制御が放棄される必要があることを示すために使用されます。
- データ プレーン：通常、この機能はハンドオフ プロセスに関連しており、パフォーマンスを著しく低下させずにステーションのトラフィックがステーションから引き続き提供および受信されるようにします。

注意 ワイヤレス管理インターフェイス VLAN において Virtual Routing and Forwarding（VRF）を設定した場合は、モビリティ機能は正常に動作しない可能性があります。

（注） ワイヤレス モビリティ マルチキャストを機能させるには、PIM、IP ルーティングおよび IP マルチキャスト ルーティングを有効にする必要があります。

有線およびワイヤレス モビリティ

統合アクセス ソリューションの主な機能の 1 つ（Cisco Catalyst 3850 スイッチと Cisco WLC 5700 シリーズ コントローラの両方に適用）は、イーサネット接続からワイヤレスへ（逆も同様）のモビリティ イベント全体にわたり、デバイスに IP アドレスを設定し、セッションの持続性を維持する機能です。この機能により、ユーザはイーサネット ネットワークに可能な限りとどまり、必要に応じてワイヤレス モビリティを自由に使用できます。

この機能は、クライアントとインフラストラクチャの両方のサポートを活用し、2要素認証（デバイスとユーザ）を使用します。デバイス認証クレデンシャルは、モビリティ コントローラ（MC）でキャッシュされます。デバイスがリンク層間を移行し、デバイス クレデンシャルの検証で一致が見つかった場合、MCは同じIPアドレスが新しいインターフェイスに割り当てられるようにします。

モビリティの機能

- モビリティ コントローラ（MC）：コントローラは、ピア グループ間のローミング イベントに対するモビリティ管理サービスを提供します。MC は、RADIUS などの管理およびポリシーベースの制御プロトコルに単一の窓口を提供します。これにより、ネットワーク全体にわたって移行するユーザの位置をインフラストラクチャ サーバが維持する必要性がなくなります。MC は、サブドメイン内のすべてのモビリティ エージェントに、モビリティ設定、ピア グループ メンバーシップ、およびメンバーのリストを送信します。サブドメインは、それを形成する MC と同義です。各サブ ドメインは、MC、および AP が関連付けられたアクセス スイッチ（0 台以上）で構成されます。

- モビリティ エージェント（MA）：モビリティ エージェントは、ワイヤレス モジュールを実行しているアクセス スイッチ、または内部MAを実行しているMCです。モビリティ エージェントは、MA を実行しているデバイスに AP を介して接続されたモバイル クライアント用のクライアント モビリティ ステート マシンを維持するワイヤレス コンポーネントです。

- モビリティ サブドメイン：モビリティ ドメイン ネットワークの自律部分です。モビリティ サブドメインは、単一のモビリティ コントローラおよび関連するモビリティ エージェント（MA）で構成されます。

  （注） 複数のモビリティ コントローラが存在する場合でも、1 台の MC だけを常にアクティブにできます。

  モビリティ サブドメインは、アクティブなモビリティ コントローラにより管理されるデバイスのセットです。モビリティ サブドメインは、一連のモビリティ エージェントおよび関連するアクセス ポイントで構成されます。

- モビリティ グループ：高速ローミングがサポートされるモビリティ コントローラ（MC）の集まりです。モビリティ グループの概念は、頻繁な移動が必要なキャンパス内の建物の集まりと同じです。

- モビリティ ドメイン：モビリティがサポートされるモビリティ サブドメインの集まりです。モビリティ ドメインという用語は、キャンパス ネットワークと同じ意味合いがあります。

- Mobility Oracle （MO）：Mobility Oracle は、モビリティ サブドメインで発生するモビリティ イベントの窓口として機能します。また、モビリティ ドメイン全体、ホーム、および現在のサブドメインにある各ステーションのローカルデータベースを維持します。モビリティ ドメインには 1 つ以上の Mobility Oracle が含まれますが、常にアクティブなのは 1 つだけです。

- モビリティ トンネル エンドポイント（MTE）：モビリティ トンネル エンドポイント（MTE）は、トンネリングを使用してモバイル デバイスにデータ プレーン サービスを提

供します。これにより、ネットワーク上のユーザの Point of Presence を一定に保ち、ローミング イベントのネットワークへの影響を最小化します。

- 接続ポイント：ステーションの接続ポイントは、ネットワークへの接続時にデータ パスが最初に処理される場所です。これは、現在サービスを提供しているアクセス スイッチ、またはワイヤレス LAN コントローラになります。
- Point of Presence：ステーションの Point of Presence は、ステーションがアドバタイズされているネットワーク内の場所です。たとえば、アクセス スイッチがルーティング プロトコルを介してステーションへ到達可能性をアドバタイズしている場合、ルートがアドバタイズされているインターフェイスはステーションの Point of Presence と見なされます。
- スイッチ ピア グループ（SPG）：ピア グループは、高速モビリティ サービスが提供される隣接アクセス スイッチの静的に作成されたリストです。ピア グループは、ハンドオフ中のスイッチ間のインタラクションの範囲を地理的に近いものだけに限定します。
- ステーション：ネットワークに接続し、ネットワークからサービスを要求するユーザデバイス。デバイスには、有線、ワイヤレス、またはその両方のインターフェイスがあります。
- 同じ SPG 内のスイッチ：ローカル スイッチのピア グループに属するピア スイッチ。
- SPG 外のスイッチ：ローカル スイッチのピア グループに属さないピア アクセス スイッチ。
- 外部モビリティ コントローラ：外部モビリティ サブドメインのステーションにモビリティ管理サービスを提供するモビリティ コントローラ。外部モビリティ コントローラは、外部サブドメインのアクセス スイッチとホーム ドメインのモビリティ コントローラ間の連絡窓口として機能します。
- 外部モビリティ サブドメイン：モビリティ コントローラで制御され、別のモビリティ サブドメインに固定されたステーションをサポートするモビリティ サブドメイン
- 外部スイッチ：現在ステーションにサービスを提供している外部モビリティ サブドメインのアクセス スイッチ。
- アンカー モビリティ コントローラ：ホーム モビリティ サブドメインでステーションの制御およびモビリティ管理サービスを一元化するモビリティ コントローラ。
- アンカー モビリティ サブドメイン：モビリティ コントローラによって制御される、IP アドレスが割り当てられたステーションのモビリティ サブドメイン。
- アンカー スイッチ：ステーションに最後にサービスを提供したホーム モビリティ サブドメインのスイッチ。

低遅延ローミングを実現するスティッキ アンカリング

スティッキアンカリングにより、クライアントが最初にネットワークに参加するスイッチにおいて、クライアントの Point of Presence からのローミングの遅延を低く保つことができます。

クライアントをローミングするためにクライアントのポリシーをスイッチに適用するのはコストがかかります。ダウンロード可能な ACL を AAA サーバに問い合わせる必要があるため、大幅な遅延が生じる可能性があります。これは、時間的制約のあるクライアント トラフィックを復元するのにはふさわしくありません。

この遅延を管理するため、異なるスイッチに接続された AP 間でクライアントがローミングを行うときに、クライアント トラフィックはクライアントが最初にアソシエートするスイッチに常にトンネル経由で送信されます。サブドメイン内のローミングであるか、サブドメイン間のローミングであるかは関係ありません。クライアントは、ネットワークの初期接続ポイントにずっと固定されます。

この動作はデフォルトでイネーブルにされています。サブネット間のローミングにのみクライアント アンカリングを許可するには、この動作をディセーブルにできます。これは、WLAN コンフィギュレーションごとに設定され、WLAN コンフィギュレーション モードで使用できます。お客様は、時間的制約のあるアプリケーションとそうでないアプリーションそれぞれに、異なる SSID を設定できます。

ブリッジ ドメイン ID および L2/L3 ローミング

ブリッジ ドメイン ID は、特定のローミング タイプ（L2 または L3）を選択するための情報をモビリティ ノードに提供します。また、ネットワーク管理者はネットワーク配信全体で VLAN ID を再使用できるようになります。VLAN ID に関連付けられたサブネット設定がない場合、VLAN ID と共に追加パラメータの使用が必要になる可能性があります。ネットワーク管理者は、同じブリッジ ドメイン ID の特定の VLAN が一意のサブネットに関連付けられていることを確認します。まず、モバイル ノードは、そのノードのブリッジ ドメイン ID およびクライアントに関連付けられた VLAN ID を確認して、ローミング タイプを特定します。L2 ローミングとして処理するには、ブリッジ ドメイン ID と VLAN ID が同じである必要があります。

SPG とその後の MC の作成時に、各 SPG にブリッジ ドメイン ID が設定されます。複数の SPG で同じブリッジ ドメイン ID を使用できます。また、SPG 内のすべての MA は同じブリッジ ドメイン ID を共有します。この情報は、設定のダウンロードの一部として MA が最初に起動したときに MA へプッシュされます。システムの起動時にブリッジ ドメイン ID が変更された場合、変更された SPG 内のすべての MA にプッシュされ、次のローミングですぐに有効になります。

リンク ダウンの動作

ここでは、冗長マネージャがなく、MC や MO でダウンタイムが発生した場合の MA-MC および MC-MO 間のデータ同期に関する情報を提供します。MA-MC または MC-MO 間でキープアライブが設定されている場合、クライアントのデータベースは MO とその MC および MC とその MA の間で同期されます。

モビリティ コントローラのプラットフォーム固有のスケール要件

モビリティ コントローラ（MC）の役割は、Cisco WLC 5700 シリーズ、CUWN および Catalyst 3850 スイッチなど、さまざまなプラットフォームでサポートされています。次の表に、これら 3 つのプラットフォームのスケール要件の概要を示します。

拡張性	MC としての Catalyst 3850	MC としての Catalyst 3650	MC としての Cisco WLC 5700	MC としての CUWN 5508	MC としての WiSM2
モビリティ ドメイン内の MC の最大数	8	8	72	72	72
モビリティ グループ内の MC の最大数	8	8	24	24	24
サブドメイン内の MA の最大数（MC ごと）	16	16	350	350	350
サブドメイン内の SPG の最大数（MC ごと）	8	8	24	24	24
SPG 内の MA の最大数	16	16	64	64	64

第 63 章

モビリティ ネットワーク要素

- Mobility Agent （1121 ページ）
- モビリティ コントローラ （1122 ページ）
- Mobility Oracle （1123 ページ）
- ゲスト コントローラ （1124 ページ）

Mobility Agent

モビリティ コントローラはスイッチに配置されます。モビリティ コントローラは、制御パスおよびデータ パスのエンティティであり、次の処理を実行します。

- スイッチ上でのモビリティ イベントの処理
- モビリティ用スイッチのデータ パス要素の設定
- モビリティ コントローラとの通信

デバイスは、ワイヤレス ステーションで 802.11 トラフィックをカプセル化する CAPWAP トンネルを終端することにより、MA としてデータ パス機能を実行します。

これにより、デバイスは有線およびワイヤレス トラフィックに機能を均等に適用できます。デバイスに関する限り、802.11 は単なる別のアクセス メディアです。

MA では次の機能が実行されます。

- モビリティ プロトコルのサポート：MA のタイムリーな対応により、デバイスがローミング バジェットを達成できるようにします。
- Point of Presence：ワイヤレス サブネットが MC で使用できず、ワイヤレス クライアント VLAN が新しい接続ポイントで使用できない場合、MA が Point of Presence を引き継ぎ、クライアント トラフィックをトンネル経由で送信します。
- ARP サーバ：ネットワークがレイヤ 2 モードで設定されている場合、MA が接続されているステーションの到達可能性をアドバタイズします。トンネリングを使用する場合、ステーションのために ARP 要求がトンネル経由で送信されます。ここで、Point of Presence（アンカー スイッチ）がアップリンク インターフェイスへブリッジします。
- プロキシ IGMP：デバイス上の MA が、ローミング イベントの発生後、ステーションのためにマルチキャスト グループへの登録を行います。この情報は、新しいデバイスへコンテ

キストの一部として渡されます。これにより、ローミング時にマルチキャスト フローがユーザを追跡します。

- ルーティング：デバイスがレイヤ3アクセス ネットワークに接続されている場合、MA はトンネリングが提供されていない関連付けられたステーションのルートをインジェクトします。
- 802.1X オーセンティケータ：オーセンティケータ機能は MA に含まれており、有線およびワイヤレスのステーションを処理します。
- セキュアな PMK の共有：ステーションがネットワークに正常に認証されると、MA は PMK を MC に転送します。MC は、サブドメインに属するすべての MA、およびモビリティ グループのピア MC へ PMK をフラッディングします。

MA では次のデータ パス機能も実行されます。

- モビリティ トンネル：トンネリングの使用時に、アクセス スイッチが Point of Presence として機能している場合、MA はモビリティ トンネルから MC へのパケット、さらにピア グループ内の他の MA へのパケットをカプセル化および非カプセル化します。MA は、接続ポイント間のクライアント データ トラフィックのトンネリングをサポートします。他のスイッチに使用するパケット形式は CAPWAP（802.3 ペイロードと併用）です。MA は、モビリティ トンネルの再構成およびフラグメンテーションもサポートします。
- 暗号化：モビリティ ノード間のモビリティ制御トラフィックは暗号化された DTLS です。MA は、接続ポイントで CAPWAP 制御とデータ（任意）も暗号化します。
- CAPWAP：デバイスは、CAPWAP 制御とデータ プレーンをサポートします。デバイス転送ロジックは、CAPWAP トンネルを 802.11 および 802.3 のペイロードと終端させます。大きなフレーム（1500バイト以上）のサポートは一般的に使用できないため、デバイスが CAPWAP フラグメンテーションと再構成をサポートします。

（注） 4500 上の L3 インターフェイス、またはアップリンク ポート上の L3 インターフェイス経由のモビリティ トンネル パスはサポートされていません。L3 ワイヤレス管理インターフェイスを設定することはできません。トンネルが稼働しても、パケット転送はサポートされていないため実行できません。SSID が別の Cisco WLC にアンカーされた場合、4510 はワイヤレス クライアントから DHCP パケットをドロップします。

モビリティ コントローラ

モビリティ コントローラの主な機能は、スイッチ ピア グループの範囲外のクライアント ローミングを調整することです。モビリティ コントローラのその他の機能は次のとおりです。

- ステーション データベース：モビリティ コントローラはローカル モビリティ サブドメイン内で接続されたすべてのクライアントのデータベースを維持します。

- モビリティ プロトコル：MC はモビリティ プロトコルをサポートします。これにより、対象ローミング ポイントが迅速に応答し、150 ms というローミング バジェットを達成できます。
- Mobility Oracle へのインターフェイス：モビリティ コントローラは、とMobility Oracle 間のゲートウェイとして機能します。モビリティ コントローラがローカル データベースで一致を見つけられない場合、ワイヤレスクライアントエントリの一致（データベース内）を提案し、モビリティ ドメインを管理する Mobility Oracle に要求を転送します。

（注） Mobility Oracle の機能は、プラットフォームでサポートされている場合にのみ MC でイネーブルにできます。

- ARP サーバ：ステーションに対してトンネリングを使用する場合、ネットワーク上の Point of Presence はモビリティ トンネル エンドポイント（MTE）です。モビリティ コントローラは、担当するステーションで受信する ARP 要求に応答します。
- ルーティング：モビリティ コントローラがレイヤ 3 ネットワークに接続されている場合、モビリティ コントローラはサポートするステーションのルートをネットワークへインジェクトする必要があります。
- MTE の設定：モビリティ コントローラは、すべてのモビリティ管理関連の要求においてのコントロールポイントです。ステーションの接続ポイントで変更が発生すると、モビリティ コントローラは MTE の転送ポリシーを設定します。
- NTP サーバ：モビリティ コントローラは、に対して NTP サーバとして機能し、クロックを同期化するようにすべてのノードをサポートします。

（注） デフォルトでイネーブルにされたモビリティ コントローラ機能を持つ Cisco 5700 シリーズ WLC および他のコントローラ プラットフォームは、スイッチ ピア グループ（SPG）に追加できません。

Mobility Oracle

Mobility Oracle は必要に応じてサブドメインを越えたクライアントのローミングを調整します。次の機能で構成されます。

- ステーション データベース：Mobility Oracle はモビリティ ドメイン内でサービスが提供されているすべてのステーションのデータベースを維持します。このデータベースは、サポートするモビリティ サブドメインすべてにおいて、Mobility Oracle とすべてのモビリティ コントローラとのインタラクション時に入力されます。

- モビリティ コントローラへのインターフェイス：Mobility Oracle がモビリティ コントローラから要求を受信すると、ステーションの検索を実行し、必要に応じてモビリティ コントローラへ要求を転送します。

- NTP サーバ：Mobility Oracle はモビリティ コントローラに対する NTP サーバとして機能し、モビリティ ドメイン内のすべてのクロックを同期します。

ゲスト コントローラ

ゲストアクセス機能により、ワイヤレスクライアントへのゲストアクセスが可能になります。ゲスト トンネルはモビリティ トンネルと同じ形式を使用します。ゲスト アクセス機能を使用すれば、アクセス スイッチ上でゲスト VLAN を設定する必要はありません。有線およびワイヤレスクライアントからのトラフィックは、ゲストコントローラで終端します。ゲストVLANがアクセススイッチに存在しないため、トラフィックは既存のモビリティトンネルを介して、さらにゲスト コントローラへのゲスト トンネルを介して、MTE に送信されます。

このアプローチの利点は、ゲストコントローラにトンネル経由で送信される前に、すべてのゲストトラフィックがMTEを通過することです。ゲストコントローラは、自身とすべてのMTE間のトンネルだけをサポートする必要があります。

このアプローチの欠点は、ゲストクライアントからのトラフィックが2回トンネル経由で送信されることです。最初は MTE に、さらにゲスト コントローラにトンネル経由で送信されます。

ゲスト コントローラではローミングがサポートされていないため、クライアントはゲスト コントローラへローミングできません。この制限は、IOS-XE のゲスト アンカーのみに適用され、AireOS へは適用されません。

第 64 章

モビリティ制御プロトコル

- モビリティ制御プロトコルについて （1125 ページ）
- 最初のアソシエーションとローミング （1125 ページ）
- 最初のアソシエーション （1126 ページ）
- スイッチ内のハンドオフ （1128 ページ）
- スイッチ ピア グループ内のハンドオフ （1128 ページ）
- スイッチ ピア グループ間のハンドオフ （1129 ページ）
- サブ ドメイン間のハンドオフ （1130 ページ）
- モビリティ グループ間のハンドオフ （1131 ページ）

モビリティ制御プロトコルについて

モビリティ制御プロトコルは、トンネル型とルーティング型のどちらでも使用されます。モビリティ制御プロトコルは、MO、MC、および MA 間のモビリティ イベントに使用されます。

モビリティ アーキテクチャは、次の両方のアプローチを使用します。

- 各 SPG 内のスイッチとの直接通信を使用した分散型アプローチ
- MC と MO を使用した集中型アプローチ

この目的は、スイッチ間のインタラクションを制限してシステム全体を拡張しつつ、集中化された MC 上でオーバーヘッドを削減することです。

最初のアソシエーションとローミング

次のシナリオは、モビリティ管理プロトコルに適用されます。

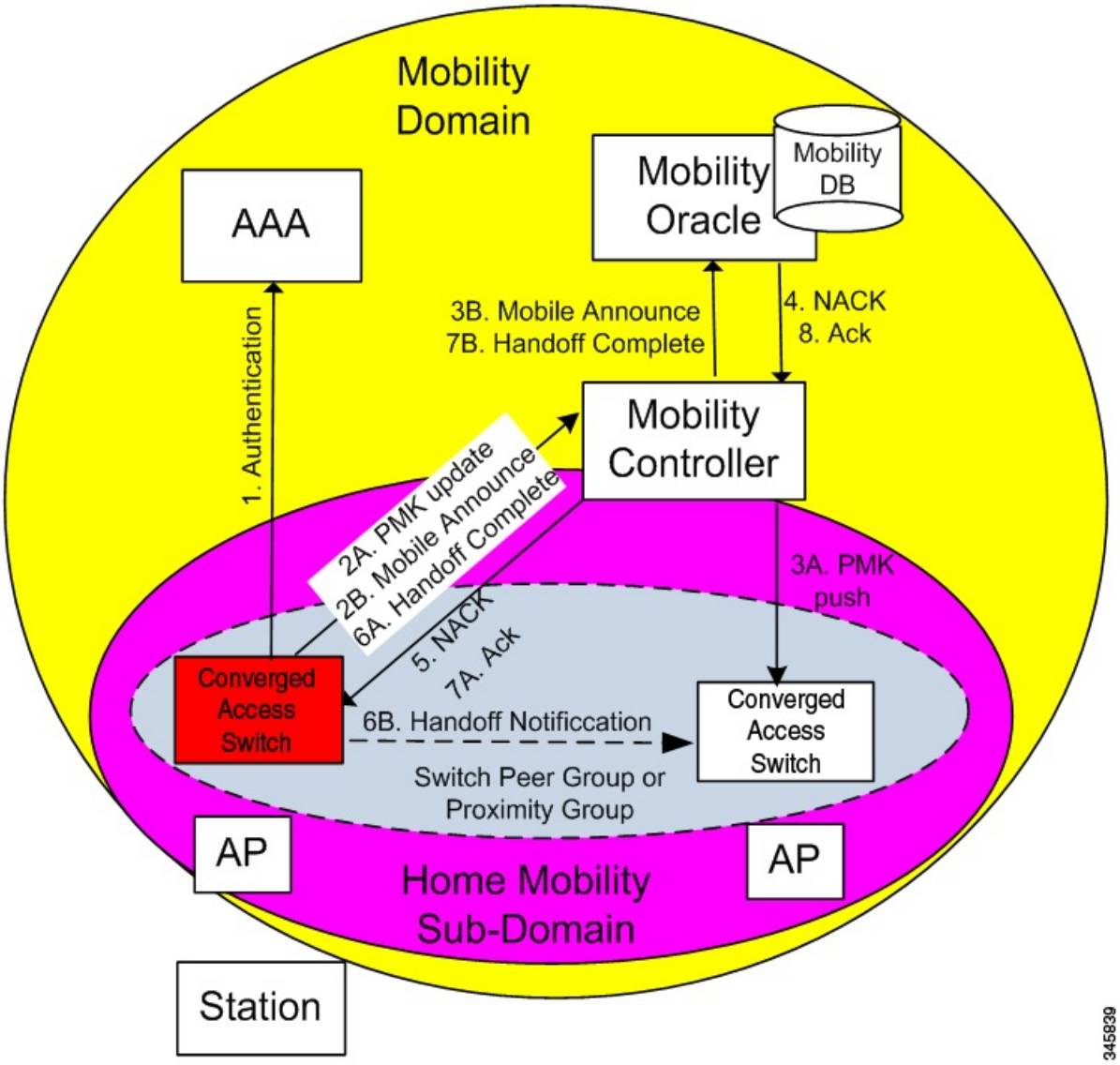
- 最初のアソシエーション
- スイッチ内のローミング
- スイッチ ピア グループ内のローミング
- スイッチ ピア グループ間のローミング
- サブドメイン間のローミング

- グループ間のローミング

最初のアソシエーション

次の図では、最初のアソシエーション プロセスとそれに続くデバイスについて説明します。

図 *70* : 最初のアソシエーション



1. ステーションがモビリティ エージェントに最初に関連付けられると、MA は検索を実行して、キー キャッシングのキーイング情報を MA でローカルに入手できるかどうか判断します。キーイング情報が入手できない場合、つまりステーションがネットワークに最初に表示される場合、デバイスはデバイスに自身を認証して、Pairwise Master Key（PMK）

を生成するように求めます。PMK はクライアントと RADIUS サーバ側で生成され、RADIUS サーバはオーセンティケータである MA に PMK を転送します。

2. MA は MC に PMK を送信します。
3. MA から PMK を受け取ると、MC はサブドメイン内のすべての MA、およびモビリティグループ内の他のすべての MC に PMK を送信します。
4. モビリティ グループは、単一キー ドメインです。これにより、802.11r に対応するステーションはキー ドメインを認識し、802.11r で定義された高速移行手順の使用を試みます。

（注） 802.11r プロトコルは、キーイング情報を共有するアクセス ポイントの集まりであるキー ドメインを定義します。

5. （図のステップ 2B を参照）PMK が MA のローカル キー キャッシュ内に存在しないという事実が示すように、ステーションはモビリティ サブドメインにとって新しいため、MA は MC にモバイル通知メッセージを送信します。
6. MC は、クライアントがデータベース内に存在するかどうかを確認します。クライアントが検出されない場合、MC は MO に転送します（可能な場合）。
7. （図のステップ 5 を参照）ステーションがネットワークにとって新しいため、MO は否定応答（NACK）を返します。これは、MC によりデバイスへ転送されます。Mobility Oracle が使用できない場合、モバイル通知への応答がない原因は MC にあります。

（注） 新しいモビリティで多数のピアがある場合、IOS コントローラは AirOS ピアからの NACK メッセージに反応せず、さらに 2 つのプローブを送信します。NACK は、クライアントが存在しない場合は無視され、単にドロップされます。そのようなシナリオでは、AIREOS は NACK を送信します。したがってモビリティ コントローラからの NACK は処理されません。

8. デバイスの MA は、Handoff Complete メッセージにより、ステーションの新しい接続ポイントについて MC に通知します。
9. MA は、Handoff Notification メッセージによって、ステーションの新しい接続ポイントについてスイッチ ピア グループ（SPG）内の他の MA に通知します。MC とやり取りすることなくローカル ハンドオフを可能にするには、SPG 内の MA にこの通知を送信する必要があります。SPG 内の MA に送信された Handoff Notification メッセージで、MC に送信された Handoff Complete メッセージ内のすべての情報を伝える必要はありません。
10. （図のステップ 7B を参照）MC はデータベースを更新し、Mobility Oracle に Handoff Complete メッセージを転送します。これにより、Mobility Oracle のデータベースが更新され、ステーションの現在のホーム モビリティ サブドメインが記録されます。

デバイス全体にわたり迅速に移動するデバイスにより発生する競合状態を解消するため、モビリティ サブドメイン内に存在するかどうかに関係なく、MA と MC/MO 間のメッセージは時間同期されます。これにより、受信した要求に異常があったとしても、MC と MO はそれらの要求を適切に処理できます。

SPG 内の MA に送信された Handoff Notification は認識されません。

スイッチ内のハンドオフ

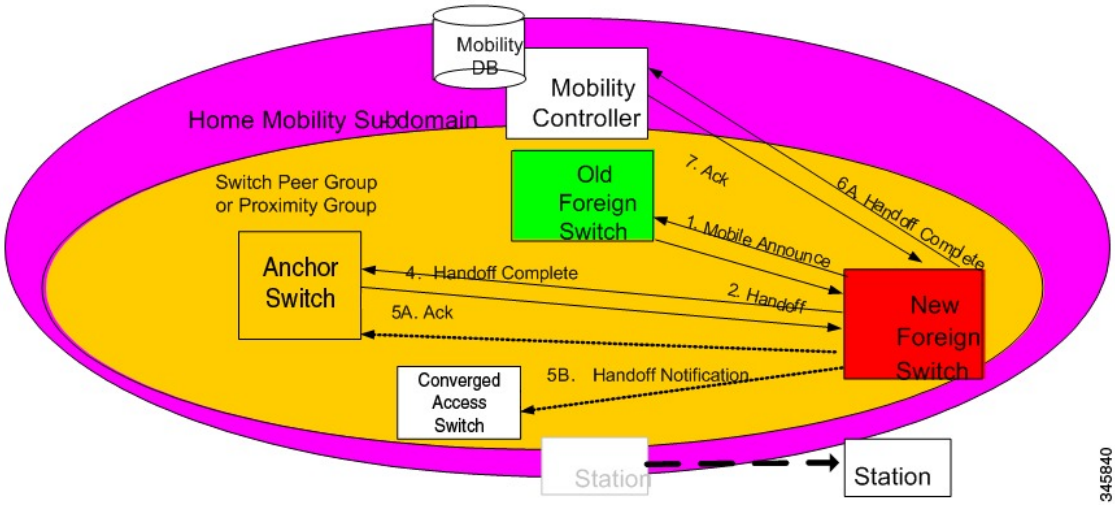
MA 内のモビリティ イベントは SPG と MC に対して完全に透過的です。ステーションが同じ MA の AP 間を移動して、迅速なハンドオフの実行を試みる場合、PMK は MA 上にあります。MA はその他の信号を呼び出すことなく迅速なハンドオフを完了します。

スイッチ ピア グループ内のハンドオフ

スイッチ ピア グループ（SPG）とは、ユーザがローミングを行う MA のグループのことで、高速ローミング サービスを提供します。SPG 内で MA が直接ハンドオフを実行することにより、必要な交換メッセージの数が少なくなり、MC のオーバーヘッドが減少します。

最初のアソシエーションが完了すると、ステーションはその SPG に属する別の MA に移動します。スイッチ ピア グループ内のローミングでは、最初のアソシエーション、ステーション PMK はモビリティ サブドメイン内のすべての MA に転送されています。

図 *71* : スイッチ ピア グループ内のハンドオフ



次のプロセスでは、スイッチ ピア グループ内のハンドオフについて説明します。

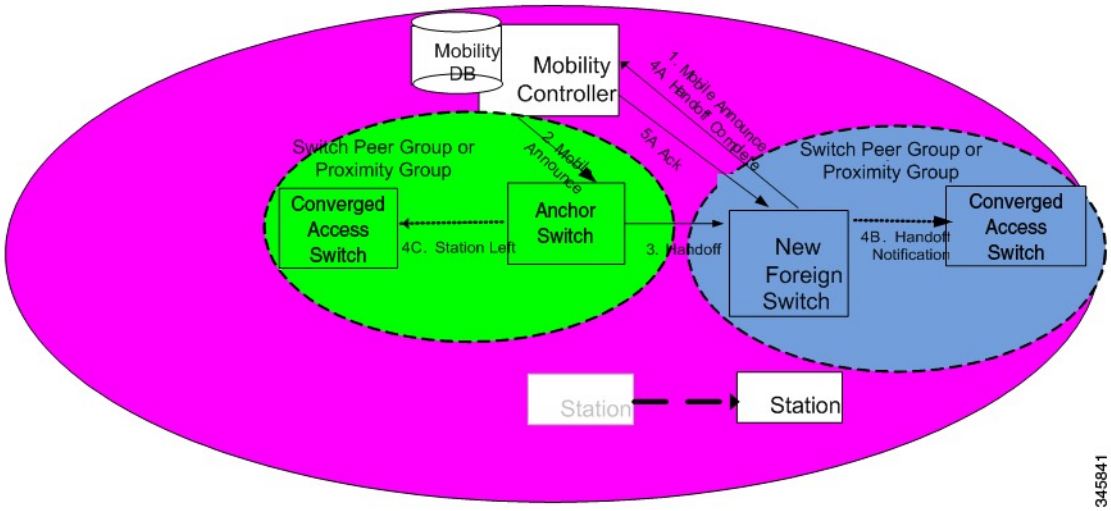
1. 最初のアソシエーションの例では、ステーションの現在の接続ポイントを確認するために、Handoff Notification メッセージがすべての MA に送信されます。
2. 新しい MA は、クライアントが関連付けられた以前の MA にユニキャスト モバイル通知メッセージを送信します。
3. ハンドオフが完了したら、新しい MA は MC へ Handoff Complete メッセージを送信します。
4. 新しいデバイスは、同じ SPG 内のすべての MA に Handoff Notification を送信して、クライアントの新しい Point of Presence について通知します。

スイッチ ピア グループ間のハンドオフ

SPG内ローミングは、考えられるすべてのシナリオをカバーしているわけではありません。同じ SPG に存在しない 2 つの MA 間でモビリティ イベントが発生する可能性があります。

ネットワーク内での Handoff Notification メッセージの紛失や新しい SPG に存在しない MA へのステーションのローミングなどの理由により、MA にステーションの現在の接続ポイントに関する情報がない場合、MA は MC を参照します。MC は、モビリティ サブドメイン内のクライアントの Point of Presence に関する情報を提供します。これにより、モビリティ サブドメイン内の他の MC すべてを参照せずに済みます。

図 *72*：スイッチ ピア グループ間のハンドオフ



上記の図は、同じ SPG ではなく、同じモビリティ サブドメインに存在する MA で発生するモビリティ イベントの例を示します。

（注） MA の色は SPG を表す円と一致します。

1. 新しい MA には、クライアントの初期認証時にモビリティ サブドメインの各 MA に転送されたステーションの PMK があります。
2. MA は内部の隣接する MA にあるステーションの存在を前もって通知されていなかったため、別の SPG がサブドメインの MC へモバイル通知を送信します。
3. （図のステップ 2 を参照）モバイル通知メッセージを受信すると、MC はデータベース内で検索を実行し、以前にステーションにサービスを提供していた MA へ要求を転送します。この情報は、信頼性の高い方法で古い MA から送信された Handoff Complete メッセージにより、MC に通知されます。
4. （図のステップ 3 を参照）上の緑色で示されている古い MA は、新しい MA へハンドオフ メッセージを直接送信します。

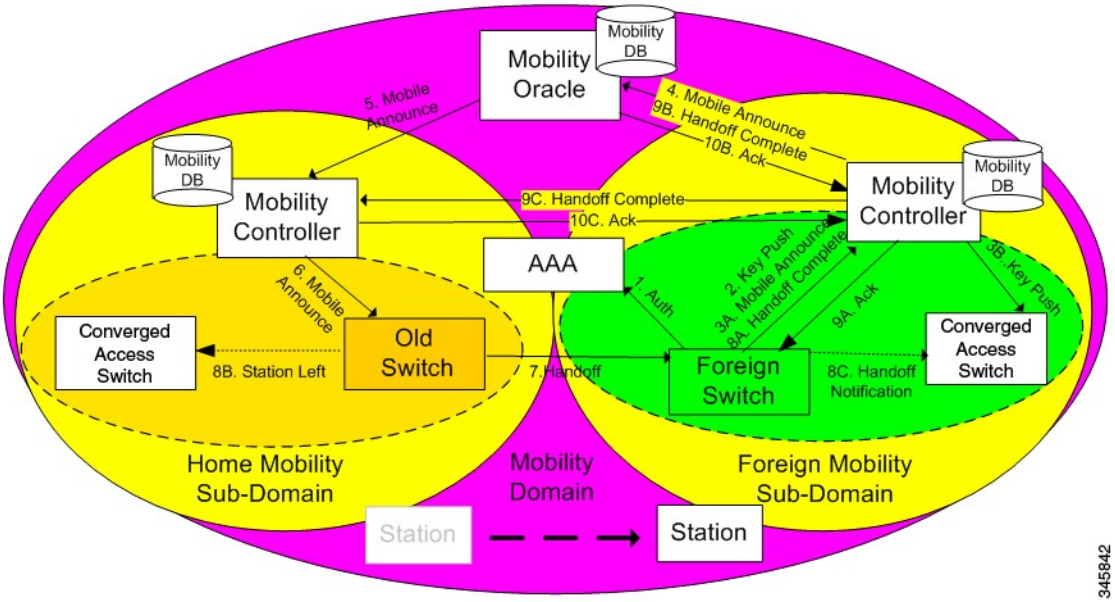
5. 古い MA は、Station Left メッセージを使用して、ステーションがグループを離れたことを SPG 内の他の MA に通知する必要があります。これにより、ステーションが MA の 1 つに戻ったとしても、古い MA はもはやサービスをステーションに提供しないことを MA は認識できます。
6. ハンドオフが完了すると、新しい MA は信頼性の高い方法で MC に Handoff Complete メッセージを送信します。
7. 新しい MA は SPG 内の他の MA に Handoff Notification を送信します。

サブ ドメイン間のハンドオフ

サブドメインは、モビリティ コントローラとそのモビリティ コントローラが直接管理するモビリティ エージェントによって形成される集合体です。サブドメイン間のモビリティ イベントは、2 台のモビリティ コントローラ間の通信を意味しています。これら 2 台のモビリティ コントローラは、同じモビリティ グループ値で設定され、相互に認識できます。これらは互いのモビリティ リストに表示されます。また、異なるモビリティ グループ値で設定しても、相互に認識できます。

同じモビリティ グループの MC 間のサブドメインでローミング イベントが発生した場合、新しい AP によりアドバタイズされる 802.11r キー ドメインは同じです。また、クライアントの初期認証時に、クライアントの PMK もすべての MC へ送信されます。新しい MC はクライアントに再認証を強制する必要がありません。また、新しい MC は、以前の MC のうちどれがワイヤレス クライアント モビリティを管理しているかも認識します。

図 *73*：サブ ドメイン間のハンドオフ



次の手順は、モビリティ コントローラが同じモビリティ グループに属している場合のサブ ドメイン間のハンドオフに関するものです。

1. 最初の MA によりクライアントの PMK がモビリティ グループのすべての MC へ送信されたときに、新しい MA は MC からクライアントの PMK をすでに受信したため、再認証は必要ではありません。
2. 新しい MA は、サブドメインの MC へモバイル通知を送信する別の SPG 内で、隣接する MA にあるステーションの存在を前もって通知されていませんでした。
3. モバイル通知メッセージを受信すると、MC はモバイル通知を MO へ転送します。MO はデータベース内で検索を実行して、以前にステーションにサービスを提供していた MC へ要求を転送します。
4. 以前の MC は、ステーションにサービスを提供していた MA へその要求を転送します。
5. 黄色で示されている古い MA は、新しい MA へハンドオフ メッセージを直接送信します。
6. 古い MA は、Station Left メッセージを使用して、ステーションが SPG を離れたことを SPG 内の他の MA に通知する必要があります。これにより、ステーションが MA の 1 つに戻った場合に、古い MA はもはやサービスをステーションに提供しないことを MA は認識できます。
7. ハンドオフが完了すると、新しいMAは信頼性の高い方法で新しいモビリティ コントローラに Handoff Complete メッセージを送信します。
8. 新しい MA は他のすべての MA に Handoff Notification を送信します。
9. 新しい MC は、古い MC に Handoff Complete を送信します。

モビリティ グループ間のハンドオフ

モビリティ グループは、同じモビリティ グループ名を共有し、相互に認識する MC により形成されます。

ローミング イベントはモビリティ グループ全体で発生するため、新しい AP によってアドバタイズされる 802.11r キー ドメインは異なります。結果として、クライアントは再認証を行う必要があります。MCはモビリティ グループ内でのみ伝搬されます。また、モビリティ グループ間のローミングでステーションがモビリティ グループの境界を越える際に、ステーションの再認証が必要です。認証が完了すると、生成される PMK は同じモビリティ グループ内の MA および MCS にプッシュされます。各 PMK は特定のサブドメイン（802.11y キー ドメイン）に関連付けられているため、ステーションは以前のサブドメインから PMK をキャッシュします。これにより、PMK キャッシュ タイムアウト インターバル内に PMK が以前のサブドメインへローミングで戻る場合、再認証を行う必要がなくなります。残りの手順は、サブドメイン間のハンドオフのステップと同じです（ただし、これらのステップはモビリティ グループ間のローミングに関連しています）。

第 65 章

モビリティの設定

- モビリティ コントローラの設定 （1133 ページ）
- モビリティ エージェントの設定 （1140 ページ）
- モビリティ コントローラによるモビリティ エージェントの管理 （1142 ページ）

モビリティ コントローラの設定

統合アクセス コントローラの設定

ピア グループ、ピア グループ メンバー、ブリッジ ドメイン ID の作成（CLI）

始める前に

- モビリティ エージェントでは、モビリティ コントローラの IP アドレスだけを設定できます。
- モビリティ コントローラでは、各ピア グループ メンバーのピア グループおよび IP アドレスを定義できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility controller** 例： `Device(config)# wireless mobility controller`	デバイスのモビリティ コントローラ機能をイネーブルにします。このコマンドはスイッチだけに適用されます。デフォルトのコントローラはモビリティ コントローラです。
ステップ 2	**wireless mobility controller peer-group** *SPG1* 例：	SPG1 という名前のピア グループが作成されます。

	コマンドまたはアクション	目的
	`Device(config)# wireless mobility controller peer-group SPG1`	
ステップ 3	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* 例： `Device(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip 10.10.20.2`	ピア グループにモビリティ エージェントを追加します。 （注） **10.10.20.2** は、モビリティ エージェントの直接 IP アドレスです。NAT を使用する場合、任意のパブリック IP アドレスを使用して、モビリティ エージェントの NATed アドレスを入力します。NAT を使用しない場合、パブリック IP アドレスは使用されず、デバイスはモビリティ エージェントの直接 IP アドレスを表示します。
ステップ 4	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* 例： `Device(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip 10.10.20.6`	ピア グループ SPG1 に別のメンバーを追加します。
ステップ 5	**wireless mobility controller peer-group** *SPG2* 例： `Device(config)# wireless mobility controller peer-group SPG2`	別のピア グループ SPG2 を作成します。
ステップ 6	**wireless mobility controller peer-group** *SPG2* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* 例： `Device(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip 10.10.10.20`	ピア グループ SPG2 にメンバーを追加します。
ステップ 7	**wireless mobility controller peer-group** *SPG1* **bridge-domain-id** *id* 例：	（任意）他の SPG でサブネット VLAN マッピングを定義するために使用される SPG1 にブリッジ ドメインを追加します。

	コマンドまたはアクション	目的
	`Device(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54`	

例

次に、ピア グループを作成し、メンバーを追加する例を示します。

```
Device(config)# wireless mobility controller
Device(config)# wireless mobility controller peer-group SPG1
Device(config)# wireless mobility controller peer-group SPG1
Device(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip
 10.10.20.2
Device(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip
 10.10.20.6
Device(config)# wireless mobility controller peer-group SPG2
Device(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20
public-ip 10.10.10.20
Device(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54
```

ローカル モビリティ グループの設定（CLI）

モビリティ グループが MC のグループである場合の、ワイヤレス モビリティ グループとモビリティ グループ メンバーの設定。

始める前に

MC は 1 つのグループだけに所属できますが、複数のモビリティ グループ内の MC を認識できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility group name** *group-name* 例： `Device(config)# wireless mobility group name Mygroup`	**Mygroup** という名前のモビリティ グループを作成します。
ステップ 2	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* 例： `Device(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28`	**Mygroup** モビリティ グループにモビリティ コントローラを追加します。 （注） NAT を使用する場合、任意のパブリック IP アドレスを使用して、モビリティ コントローラの NATed IP アドレスを入力します。

	コマンドまたはアクション	目的
ステップ 3	**wireless mobility group keepalive interval** *time-in-seconds* 例： `Device(config)# wireless mobility group keepalive interval 5`	モビリティ メンバーに送信される 2 つのキープアライブの間隔を設定します。
ステップ 4	**wireless mobility group keepalive count** *count* 例： `Device(config)# wireless mobility group keepalive count 3`	メンバー ステータスがダウン状態に移行するまでのキープアライブ再試行回数を入力します。

例

```
Device(config)# wireless mobility group name Mygroup
Device(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28
Device(config)# wireless mobility group keepalive interval 5
Device(config)# wireless mobility group keepalive count 3
```

ピア モビリティ グループの追加（CLI）

始める前に

MC は 1 つのグループだけに所属しますが、複数のグループ内の MC を認識できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **group** *group-name* 例： `Device(config)# wireless mobility group member ip 10.10.10.24 public-ip 10.10.10.25 group Group2`	**Mygroup** 以外のグループにメンバーをピア MC として追加します。

ローミング動作のオプション パラメータの設定

この設定により、スティッキ アンカーをディセーブルにします。必要に応じ、このコマンドは、ターゲット SSID にローミングが必要なすべての MA と MC との間で使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan open21** 例： `Device(config)# wlan open20`	WLAN を設定します。
ステップ 2	**no mobility anchor sticky** 例： `Device(config-wlan)# no mobility anchor sticky`	デフォルトのスティッキ モビリティ アンカーをディセーブルにします。

例

```
Device(config)# wlan open20
Device(config-wlan)# no mobility anchor sticky
```

モビリティ コントローラの Mobility Oracle への指定（CLI）

始める前に

既知のモビリティ コントローラ上で Mobility Oracle を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility group member ip** *member-ip-addr* **group** *group-name* 例： `Device(config)# wireless mobility group member ip 10.10.10.10 group Group3`	MC を作成してモビリティ グループに追加します。
ステップ 2	**wireless mobility oracle ip** *oracle-ip-addr* 例： `Device(config)# wireless mobility oracle ip 10.10.10.10`	Mobility Oracle としてモビリティ コントローラを設定します。

例

```
Device(config)# wireless mobility group member ip 10.10.10.10 group Group3
Device(config)# wireless mobility oracle ip 10.10.10.10
```

ゲスト コントローラの設定

ゲスト コントローラは、クライアント トラフィックを非武装地帯（DMZ）のゲスト アンカー コントローラへトンネル経由で送信する場合に使用されます。ゲスト クライアントは Web 認証プロセスを通過します。Web認証プロセスは任意です。ゲストは認証なしでトラフィックを渡すこともできます。

ゲスト クライアントがゲスト コントローラのモビリティ アンカー アドレスと接続するモビリティ エージェントの WLAN をイネーブルにします。

Cisco 5500 シリーズ WLC、Cisco WiSM2、Cisco 5700 シリーズ WLC などのゲスト コントローラ WAN で、独自の IP アドレスとしてモビリティ アンカーの IP アドレスを設定します。これにより、トラフィックはモビリティ エージェントからゲスト コントローラへトンネル経由で送信されます。

（注） Cisco 5700 シリーズ WLC をゲスト アンカー コントローラとして、また Cisco 5500 シリーズ WLC または Cisco WiSM2 をエクスポートまたは外部コントローラとした場合、Cisco 5700 シリーズ WLC ではユーザごとのゲスト ユーザ ロールはサポートされていません。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *wlan-id* 例： `Device(config)# wlan Mywlan1`	クライアントの WLAN を作成します。
ステップ 2	**mobility anchor** *guest-anchor-ip-addr* 例： `Device(config-wlan)# mobility anchor 10.10.10.2`	MA でゲスト アンカー（GA）の IP アドレスをイネーブルにします。 （注） モビリティ コントローラでゲスト アンカーをイネーブルにする場合、IP アドレスを入力する必要はありません。WLAN コンフィギュレーション モードで **mobility anchor** コマンドを入力して、モビリティ コントローラの GA をイネーブルにします。
ステップ 3	**client vlan** *vlan-name* 例： `Device(config-wlan)# client vlan gc_ga_vlan1`	クライアントの WLAN に VLAN を割り当てます。

	コマンドまたはアクション	目的
ステップ 4	**security open** 例： `Device(config-wlan)# security open`	WLAN にセキュリティ タイプを割り当てます。

例

```
Device(config)# wlan Mywlan1
Device(config-wlan)# mobility anchor 10.10.10.2
Device(config-wlan)# client vlan gc_ga_vlan1
Device(config-wlan)# security open
```

ゲスト アンカーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan Mywlan1** 例： `Device(config)# wlan Mywlan1`	クライアントの WLAN を作成します。
ステップ 2	**mobility anchor <guest-anchors-own-ip-address>** 例： `Device(config-wlan)# mobility anchor 10.10.10.2`	ゲスト アンカー（GA）のゲスト アンカーIPアドレスをイネーブルにします。GA は自身のアドレスを割り当てます。
ステップ 3	**client vlan<vlan-name>** 例： `Device(config-wlan)# client vlan gc_ga_vlan1`	クライアントの WLAN に VLAN を割り当てます。
ステップ 4	**security open** 例： `Device(config-wlan)# security open`	WLAN にセキュリティ タイプを割り当てます。

例

```
Device(config)# wlan Mywlan1
Device(config-wlan)# mobility anchor 10.10.10.2
Device(config-wlan)# client vlan gc_ga_vlan1
Device(config-wlan)# security open
```

モビリティ エージェントの設定

モビリティ コントローラの指定によるモビリティ エージェントの設定（CLI）

始める前に

- デフォルトでは、スイッチはモバイル エージェントとして設定されます。
- ネットワークには少なくとも 1 台のモビリティ コントローラがあり、モビリティ コントローラとのネットワーク接続が動作している必要があります。
- モビリティ エージェントからはモビリティを設定できません。モビリティ エージェントでは、SPG コンフィギュレーションをダウンロードするモビリティ コントローラの IP アドレスだけを設定できます。
- モビリティエージェントでは、外部モビリティエージェントを指定するようにモビリティコントローラ アドレスを設定するか、モビリティ コントローラ機能をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless management interface vlan 21** 例： `Device (config)# wireless management interface vlan 21`	デバイスのワイヤレス機能をイネーブルにし、モビリティ エージェント機能をアクティブ化します。これにより、AP が CAPWAP トンネルを終端する場所を確保できます。

例

次に、モビリティ コントローラを指定して、モビリティ グループにモビリティ エージェントを追加する例を示します。

```
Device(config)# wireless management interface vlan 21
```

モビリティ エージェントのモビリティ コントローラの設定（CLI）

手順

	コマンドまたはアクション	目的

ステップ 1	**wireless mobility controller**
	例：
	`Device (config)# wireless mobility controller`
	`Mobility role changed to Mobility Controller.`
	`Please save config and reboot the whole stack.`
		デバイスでモビリティ機能をイネーブルにします。
		（注） このコマンドの入力後、設定を保存してデバイスをリブートし、モビリティ コントローラ機能を有効にします。

ステップ 2	**wireless mobility controller ip** *ip-addr* 例： `Device (config)# wireless mobility controller ip 10.10.21.3`	モバイル エージェントに関連するモビリティ コントローラを指定します。 （注） モバイル エージェントが設定され、モビリティ コントローラが別のデバイスにある場合、モビリティ コントローラの SPG を設定して、モビリティ エージェントが正しく機能するようにします。

次のタスク

モビリティ エージェントにモビリティ コントローラのロールを追加したら、モビリティ エージェントに任意のパラメータを設定できます。

モビリティ エージェントへのモビリティ コントローラの役割の追加

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility controller ip 10.10.21.3** 例： `Device(config)# wireless mobility controller ip 10.10.21.3`	モビリティ エージェントをモビリティ コントローラに変換します。

例

次に、モビリティエージェントにモビリティコントローラの役割を追加する例を示します。

```
Device(config)# wireless mobility controller ip 10.10.21.3
Mobility role changed to Mobility Controller.
Please save config and reboot the whole stack.
```

モビリティ エージェントのオプション パラメータの設定（CLI）

ここでは、デバイスのロード バランシングを設定する方法を示します。

- デフォルトでは、ロードバランシングはイネーブルにされており、ディセーブルにはできません。
- デバイスは最大 2000 のクライアントをサポートし、デフォルト値はクライアントの最大負荷の 50 % です。
- デバイスがしきい値に達すると、同じ SPG 内のより負荷が低いモビリティ エージェントに新しいクライアントの負荷を再配信します。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility load-balance threshold** *threshold-value* **例：** `Device(config)# wireless mobility load-balance threshold 150`	ロード バランシングをトリガーするしきい値を設定します。

モビリティコントローラによるモビリティエージェントの管理

モビリティ コントローラによるモビリティ エージェントの管理

モビリティコントローラが管理するモビリティエージェント機能では、モビリティコントローラ（MC）からモビリティエージェント（MA）へのワイヤレス設定および共通設定がプッシュされます。このことにより、MC からすべての MA を設定、監視、トラブルシューティングするのに役立ちます。MC は最大 16 の MA をサポートできます。ワイヤレスおよび AAA、ACL などの一般的なコンフィギュレーションは、通常、すべてのスイッチで同じです。

モビリティ コントローラによるモビリティ エージェントの管理に関する制約事項

- 新しい MA が MC に加入し、この MA が一元管理される場合、また、MA が 1 つの MC から別の MC に移動した場合、MC および MA が非同期になる可能性があります。
- MA が一元化モードになると、グローバルな設定が無効になり、残りの設定およびモニタリングは Web GUI で使用可能です。
- この機能は、Cisco Prime Infrastructure ではサポートされていません。
- MC が同期していない MA を検出すると、MA は強制的にリロードされ、リロード後に再度 MC から全体のコンフィギュレーションを再同期します。
- QoS の設定は、MC から MA へプッシュされません。
- MC は、すべての構成を一元管理された MA へすべてプッシュします。設定のサブセットを選択し、すべての MA ではなく特定の MA グループへプッシュすることはできません。
- WLAN 設定は MC からプッシュされるため、L3 ローミングはサポートされません。
- 同じスイッチ ピア グループ（SPG）または別の SPG のサブドメイン内のさまざまなソフトウェア バージョンを使用している MA はサポートされません。
- Catalyst 3850 および 3650 スイッチがモビリティ サブドメインで MC として機能している場合、MC と MA は Polaris リリース 16.2 および Polaris リリース 16.1.1 のみを実行します。
- モビリティ サブドメインで許可されるのは Catalyst 3850 スイッチのみなので、Polaris のバージョンが MA として機能している場合は、5760 を MC に追加することはできません。
- 16.2 Denali のリリースでは、Cisco 3850 コントローラは MA または MC で最大 50 の AP をサポートしています。MC-MA のシナリオでは、MA および MC 両方の AP を含む、最大 100 の AP がサポートされます。

機能の履歴

リリース	**Remarks**
Cisco IOS XE Denali 16.2.1	この機能は、Cisco Catalyst 3850 および Cisco Catalyst 3650 シリーズ スイッチで導入されました。

MC と MA の間で同期されたコマンドの完全なリストについては、次の URL にある *MC Managing MA - List of Commands Synchronized Between MC and MA* を参照してください。

http://www.cisco.com/c/en/us/td/docs/wireless/controller/mc-ma/mc-ma-sync.html.

モビリティ コントローラによるモビリティ エージェントの管理について

モビリティ コントローラ（MC）では、一元管理されるモビリティ エージェント（MA）と一元管理されないモビリティ エージェント（MA）を同時に所有できます。一元管理される MA は、MC で設定した一連の設定を受信します。一元管理されない MA では、MC の設定を受信しません。MA が一元管理されている間は、MC から MA にプッシュされている設定の変更はできません。

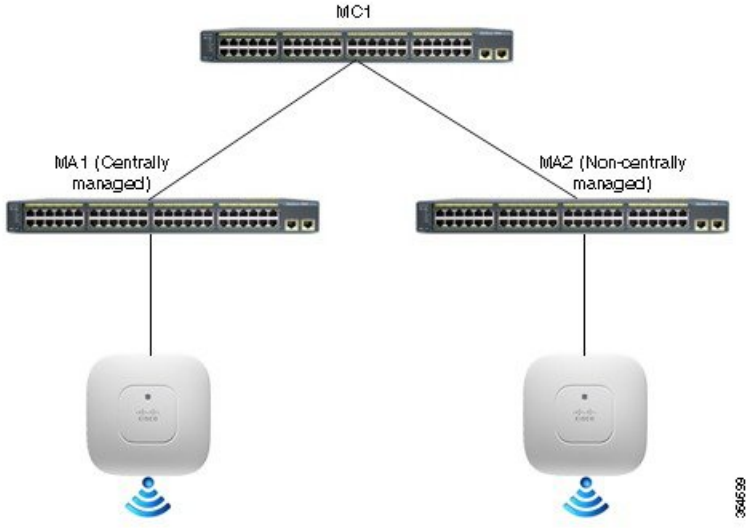
MC は、すべての一元管理される MA に、既存の Control And Provisioning of Wireless Access Point（CAPWAP）トンネルを介して、すべての関連する設定をプッシュします。また、MC は、増分設定を MA にプッシュします（ある場合）。

（注） この機能を使用する前に、MC と MA の間の CAPWAP トンネルを起動するための設定を行う必要があります。

次の設定は MA に送信されます。

- 共通設定：セキュリティ設定、たとえば、認証、許可、およびアカウンティング（AAA）など、有線設定とワイヤレス設定の間で共有される設定。
- ワイヤレス設定：すべてのワイヤレス設定。

図 *74 : MC* が管理する *MA*



分散モードと一元化モード

分散モードは、すべての MA で明示的に実行する必要がある設定を示しています。

一元化モードは、ワイヤレス設定および共通設定がMCからMAに適用される設定を示しています。次の表に、分散モードと一元化モードの違いを示します。

表：分散モードと一元化モードの違い

分散モード	一元化モード
MC での設定	MC での設定
• MA から MC へのモビリティ ピアリング設定 • Wireless LAN（ワイヤレス LAN） • ワイヤレス QoS ポリシー • ワイヤレス セキュリティ ACL • AAA グローバル コンフィギュレーション • ロケーション • Cisco CleanAir、無線リソース管理（RRM）、クライアント リンク • グローバルおよび AP ごとの設定	• MA から MC へのモビリティ ピアリング設定 • Wireless LAN（ワイヤレス LAN） • ワイヤレス セキュリティ ACL • AAA グローバル コンフィギュレーション • ロケーション • Cisco CleanAir、RRM、クライアント リンク • グローバルおよび AP ごとの設定
MA での設定	MA での設定
• MA から MC へのモビリティ ピアリング設定 • Wireless LAN（ワイヤレス LAN） • ワイヤレス QoS ポリシー • ワイヤレス セキュリティ ACL • AAA グローバル コンフィギュレーション • ロケーション • Cisco CleanAir、RRM、クライアント リンク • グローバルおよび AP ごとの設定	• MA から MC へのモビリティ ピアリング設定 • ワイヤレス QoS ポリシー

モビリティ コントローラによるモビリティ エージェントの管理に関する制約事項

- 新しい MA が MC に加入し、この MA が一元管理される場合、また、MA が 1 つの MC から別の MC に移動した場合、MC および MA が非同期になる可能性があります。
- MA が一元化モードになると、グローバルな設定が無効になり、残りの設定およびモニタリングは Web GUI で使用可能です。
- この機能は、Cisco Prime Infrastructure ではサポートされていません。
- MC が同期していない MA を検出すると、MA は強制的にリロードされ、リロード後に再度 MC から全体のコンフィギュレーションを再同期します。
- QoS の設定は、MC から MA へプッシュされません。
- MC は、すべての構成を一元管理された MA へすべてプッシュします。設定のサブセットを選択し、すべての MA ではなく特定の MA グループへプッシュすることはできません。
- WLAN 設定は MC からプッシュされるため、L3 ローミングはサポートされません。
- 同じスイッチ ピア グループ（SPG）または別の SPG のサブドメイン内のさまざまなソフトウェア バージョンを使用している MA はサポートされません。
- Catalyst 3850 および 3650 スイッチがモビリティ サブドメインで MC として機能している場合、MC と MA は Polaris リリース 16.2 および Polaris リリース 16.1.1 のみを実行します。
- モビリティ サブドメインで許可されるのは Catalyst 3850 スイッチのみなので、Polaris のバージョンが MA として機能している場合は、5760 を MC に追加することはできません。
- 16.2 Denali のリリースでは、Cisco 3850 コントローラは MA または MC で最大 50 の AP をサポートしています。MC-MA のシナリオでは、MA および MC 両方の AP を含む、最大 100 の AP がサポートされます。

MA を管理する MC の設定（CLI）

次に、モビリティ コントローラによるモビリティ エージェントの管理を設定する手順を示します。

手順

ステップ 1 MC の設定：

a) 次のコマンドを入力して、ワイヤレス管理インターフェイスを設定します。

```
Device(config)# wireless management interface vlan vlan-id
```

b) 次のコマンドを入力して、スイッチ ピア グループを設定します。

```
Device(config)# wireless mobility controller peer-group spg-name
```

c) 次のコマンドを入力して、MA を SPG に追加し、一元管理されるように設定します（一元化オプションのみ使用）。

```
Device(config)# wireless mobility controller peer-group spg-name member ip ip-addr
mode centralized
```

ステップ 2 MA の設定：

a) 次のコマンドを入力して、MC の IP アドレスを指定します。

```
Device(config)# wireless mobility controller ip mc-ip-addr
```

b) 次のコマンドを入力して、ワイヤレス管理インターフェイスを設定します。

```
Device(config)# wireless management interface vlan vlan-id
```

ステップ 3 一元化モードの設定：

a) MC から、次のコマンドを入力して MA の状態を確認できます。

```
Device(config)# show wireless mobility summary

Mobility Controller Summary:

Mobility Role                                : Mobility Controller
Mobility Protocol Port                       : 16666
Mobility Group Name                          : default
Mobility Oracle IP Address                   : 0.0.0.0
DTLS Mode                                    : Enabled
Mobility Domain ID for 802.11r               : 0xac34
Mobility Keepalive Interval                  : 10
Mobility Keepalive Count                     : 3
Mobility Control Message DSCP Value          : 48
Mobility Domain Member Count                 : 1

IP         Public IP        Link   Status     Centralized(Cfgd : Running)
--------------------------------------------------------------------------------
1.1.1.1     1.1.1.1          UP   : UP         Enabled        Enabled
3.3.3.1     3.3.3.1          DOWN : DOWN       Enabled        Enabled
```

次の表に、上記の例と関連する一元化モード（設定済みと実行中の両方）の詳細を示します。

表 *65*：一元化モード（設定済みで実行中）

番号いいえ。	一元化モード設定	実行中の一元化モード	説明
1.	ディセーブル	ディセーブル	MA は、MC で一元管理されるように設定されていません。

番号いいえ。	一元化モード設定	実行中の一元化モード	説明
2.	イネーブル	無効	MA は、MC で一元管理されるように設定されていますが、MA へのトンネルはまだダウン状態である、または MA はまだ MC からのメッセージ（MC が MA に一元管理されていることを通知するメッセージ）を確認していません。
3.	イネーブル	イネーブル	MA は、MC で一元管理されるように設定されており、MA は一元管理モードで実行中です。
4.	無効	イネーブル	なし。

b) このコマンドを入力すると、SPG に関係なく、および一元管理されているかどうかに関わらず、MC 上で設定されているすべての MA を確認できます。

```
Device(config)# show cmm member-table

CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 16

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.155
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 16
Last rcvd cfg rev on MA = 16
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 16
Last sent cfg timestamp = 1427826323 sec 936009397 nsec
----------------


Members: No. of MAs configured on the MC
System Rev No on MC: What version number the MC is at

Entry
```

c) MC で実行され、CMM エージェントに格納された設定を確認するには、次のコマンドを入力します。

```
Device(config)# show cmm config

Current version number: 17
To sync and save configuration to Mobility Agents execute: "write memory"

Config commands present in the buffer:
access-list 1 permit any
wlan MCMA_Demo 4 MCMA_Demo
client vlan 22
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

（注） MC からの設定は、「**write memory**」コマンドが MC で実行された後にのみ MA と同期されます。

ステップ 4 MC からリモートで MA 上でコマンドを実行するには、次のコマンドを使用します。例えば、次のコマンドをMCで入力して、クライアントが稼働時間に達したかどうかを確認できます。

```
Device(config)# remote command 1.1.1.1 show wcdb da all
Total Number of Wireless Clients = 1
Clients Waiting to Join = 0
Local Clients = 0
Anchor Clients = 1
Foreign Clients = 0
MTE Clients = 0
Mac Address VlanId IP Address Src If Auth Mob
---------- --------- ------------- -------- ----- -------
ec55.f9c6.35c3 22 53.1.1.2 0x00D19B00000001C5 RUN ANCHOR
```

ステップ 5 MC から MA にリモートでログインするには、次のコマンドを使用します。

```
DeviceControllerDevice(config)# remote login 1.1.1.1

Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session


User Access Verification

Password:
MA1>en
Password:
MA1#
```

MC での WLAN の設定

次の手順では、MC で WLAN を作成して、一元管理される MC と WLAN 設定を同期する方法を示しています。

手順

ステップ 1 MC では、次のコマンドを入力して、MCMA_Demo という名前の WLAN を作成します。

```
Device(config)# wlan MCMA_Demo 1 MCMA_Demo
Device(config-wlan)# exit
Device(config)# exit
```

ステップ 2 設定を確認するには、次のコマンドを入力します。

```
Device(config)# show cmm config

Current version number: 3
To sync and save configuration to Mobility Agents execute: "write memory"

Config commands present in the buffer:
wlan MCMA_Demo 1 MCMA_Demo
exit
```

ステップ 3 一元管理されるように設定されている MA の数を調べるには、次のコマンドを入力します。

```
Device(config)# show cmm member-table

CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 2

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 2
Last rcvd cfg rev on MA = 2
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 2
Last sent cfg timestamp = 1432843797 sec 57656031 nsec
----------------
```

ステップ 4 次のコマンドを入力して、WLAN の詳細を確認します。

```
Device(config)# show wlan summary

Number of WLANs: 1

WLAN  Profile Name    SSID          VLAN Status
-----------------------------------------------------
1        MCMA_Demo    MCMA_Demo       1    DOWN
```

ステップ 5 次のコマンドを入力して、設定を保存します。

```
Device(config)# write memory

Building configuration...
```

```
Compressed configuration from 7612 bytes to 3409 bytes[OK]
```

ステップ 6 次のコマンドを入力して、MA の同期ステータスを確認します。

```
Device(config)# show cmm member-table

CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 3

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 2
Last rcvd cfg rev on MA = 2
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_STALE
Last sent cfg rev to MA = 3
Last sent cfg timestamp = 1432847325 sec 107200589 nsec
----------------
```

ステップ 7 MA で、次のコマンドを入力して、MC で作成された WLAN が MA と同期しているかどうかを確認します。

```
Device(config)# show wlan summary

Number of WLANs: 1

WLAN  Profile Name    SSID           VLAN Status
-----------------------------------------------------
1    MCMA_Demo     MCMA_Demo          1    DOWN
```

例：

複数の設定が同期されている様子を示すログの例

次に、**cmm** 設定の出力例を示します。

次に、**cmm** メンバー テーブルを表示する出力例を示します。

次に、**WLAN** の概要を表示する出力例を示します。

次に、メモリ書き込みの出力例を示します。

次に、**WLAN** の概要の出力例を示します。

次に、**cmm** メンバー テーブルの出力例を示します。

次に、**cmm** メンバー テーブルの出力例を示します。

次に、**cmm** メンバー テーブルの出力例を示します。

次に、設定 **MA** の出力例を示します。

次に、**WLAN** の概要の出力例を示します。

次に、**cmm** 設定の出力例を示します。

次に、**WLAN** の表示および実行の出力例を示します。

次に、**WLAN** オープンの表示および実行の出力例を示します。

```
MC#show cmm config
Current version number: 4
To sync and save configuration to Mobility Agents execute: "write memory"

Config commands present in the buffer:
wlan open 2 open
assisted-roaming dual-list
assisted-roaming neighbor-list
broadcast-ssid
ccx aironet-iesupport
channel-scan defer-priority 4
client association limit ap 0
client association limit radio 0
client vlan default
exclusionlist
exclusionlist timeout 60
ip access-group web none
mac-filtering test
mobility anchor sticky
radio all
security wpa
security wpa akm dot1x
security wpa wpa2
```

```
security wpa wpa2 ciphers aes
security dot1x authentication-list test
security dot1x encryption 104
security ft over-the-ds
security ft reassociation-timeout 20
security static-wep-key authentication open
security tkip hold-down 60
security web-auth authentication-list test2
security web-auth parameter-map test3
service-policy client input un
service-policy client output un
service-policy input unk
service-policy output unk
session-timeout 1800
no shutdown
exit
```

```
To view cmm member-table:
MC#show cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 3

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 3
Last rcvd cfg rev on MA = 3
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 3
Last sent cfg timestamp = 1433441315 sec 669464681 nsec
----------------
```

```
To view WLAN summary:
MC#show wlan summary

Number of WLANs: 2

WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test                            test                           1    DOWN
2    open                            open                           1    UP
```

```
To write memory:
MC#write mem
Building configuration...
Compressed configuration from 7972 bytes to 3619 bytes[OK]
```

```
MC#show wlan summary

Number of WLANs: 2
```

```
WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test                            test                           1    DOWN
2    open                            open                           1    UP

To view cmmm config:
MC#show cmm config
Current version number: 4
To sync and save configuration to Mobility Agents execute: "write memory"

Config commands present in the buffer:



MC#show cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 4

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 3
Last rcvd cfg rev on MA = 3
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_STALE
Last sent cfg rev to MA = 4
Last sent cfg timestamp = 1433488804 sec 349065646 nsec
----------------



MC#show cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 4

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 3
Last rcvd cfg rev on MA = 3
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_STALE
Last sent cfg rev to MA = 4
Last sent cfg timestamp = 1433488812 sec 349323943 nsec
----------------



MC#show cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 4
```

```
entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 4
Last rcvd cfg rev on MA = 4
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 4
Last sent cfg timestamp = 1433488820 sec 349544632 nsec
----------------
MC#


To view the cmm configuration
MA21#show cmm config
Current version number: 3
Centrally Managed: True


MA21#show wlan summary

Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test                             test                           1    DOWN

MA21#
Building configuration...

*Jun  5 07:21:18.295: %SYS-5-CONFIG_I: Configured from console by vty1
*Jun  5 07:21:18.314: %CMM-6-CONFIG_SYNC_SAVE_MSG: Saving config rev#4 received
from Mobility Controller.Compressed configuration from 13033 bytes to 4340 bytes[OK]



MA21#show cmm config
Current version number: 4
Centrally Managed: True
MA21#show wlan summary

Number of WLANs: 2

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test                             test                           1    DOWN
2    open                             open                           1    UP


MA21#show run wlan
wlan test 1 test
 shutdown
wlan open 2 open
 assisted-roaming dual-list
 assisted-roaming neighbor-list
 ip access-group web none
 mac-filtering test
 security dot1x authentication-list test
 security web-auth authentication-list test2
```

```
 security web-auth parameter-map test3
 service-policy client input un
 service-policy client output un
 service-policy input unk
 service-policy output unk
 no shutdown
MA21#



To view and run the WLAN open
MA21#show run wlan open
wlan open 2 open
 assisted-roaming dual-list
 assisted-roaming neighbor-list
 ip access-group web none
 mac-filtering test
 security dot1x authentication-list test
 security web-auth authentication-list test2
 security web-auth parameter-map test3
 service-policy client input un
 service-policy client output un
 service-policy input unk
 service-policy output unk
 no shutdown
MA21#
MA21#
```

第 XI 部

マルチプロトコル ラベル スイッチング（MPLS）

- マルチプロトコル ラベル スイッチング（MPLS） （1159 ページ）
- マルチキャスト バーチャル プライベート ネットワークの設定 （1167 ページ）

第 66 章

マルチプロトコル ラベル スイッチング（MPLS）

• シスコ スイッチでのマルチプロトコル ラベル スイッチング（MPLS）（1159 ページ）

シスコ スイッチでのマルチプロトコル ラベル スイッチング（MPLS）

このドキュメントでは、シスコ スイッチ上でマルチプロトコル ラベル スイッチング（MPLS）機能の設定とモニタリングを行うためのコマンドについて説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

MPLS に関する情報

MPLS の概要

マルチプロトコル ラベル スイッチング（MPLS）は、レイヤ 3（ネットワーク層）ルーティングの実績のある拡張性とレイヤ2（データ リンク層）スイッチングのパフォーマンスおよび機能を組み合わせたものです。MPLS により、既存のネットワーク インフラストラクチャを犠牲にすることなく、サービスを差別化する機会を提供しながら、ネットワーク使用率の急激な増

加の課題に対処できるようになります。MPLS アーキテクチャは柔軟性があり、レイヤ 2 テクノロジーを任意に組み合わせて使用することができます。MPLS のサポートは、すべてのレイヤ 3 プロトコルに対して提供され、今日のネットワークで一般的に提供されているものよりもはるかに優れたスケーリングが可能です。

MPLS の機能の説明

ラベル スイッチングは、高性能のパケット転送テクノロジーであり、データリンク層（レイヤ 2）スイッチングのパフォーマンスおよびトラフィック管理機能と、ネットワーク層（レイヤ 3）ルーティングの拡張性、柔軟性、およびパフォーマンスが統合されています。

ラベル スイッチング機能

従来のレイヤ 3 転送メカニズムでは、パケットがネットワークを通過するとき、各スイッチがパケットの転送に関連するすべての情報をレイヤ 3 ヘッダーから抽出します。この情報をルーティング テーブル検索のインデックスとして使用して、パケットのネクスト ホップを決定します。

最も一般的なケースでは、ヘッダーで唯一該当するフィールドは宛先アドレス フィールドですが、場合によっては、他のヘッダー フィールドが該当する場合もあります。その結果、ヘッダーの分析はパケットが通過する各スイッチで個別に実行する必要があります。また、各スイッチで複雑なテーブル検索も行う必要があります。

ラベル スイッチングでは、レイヤ 3 ヘッダーの分析が一度だけ実行されます。その後、レイヤ 3 ヘッダーは、ラベルという固定長の非構造化値にマップされます。

複数の異なるヘッダーで常に同じネクストホップが選択される場合は、これらのヘッダーを同じラベルにマッピングできます。実際、ラベルは転送等価クラス（つまり、パケットがそれぞれ別のものである可能性はあるが、転送機能によって識別不能な一連のパケット）を表します。

最初のラベル選択は、レイヤ 3 パケット ヘッダーの内容だけに基づいている必要はありません。たとえば、後続ホップでの転送判断はルーティング ポリシーに基づくこともあります。

ラベルを割り当てると、短いラベル ヘッダーがレイヤ 3 パケットの前に追加されます。このヘッダーは、パケットの一部としてネットワークを介して伝送されます。ネットワーク内の各 MPLS スイッチを介する後続ホップでは、ラベルはスワップされ、パケット ヘッダーで伝送されるラベルの MPLS 転送テーブル検索を使用して転送が判断されます。そのため、ネットワークを介したパケットの送信中にパケット ヘッダーを再評価する必要はありません。ラベルは構造化されていない固定長の値であるため、MPLS 転送テーブル検索プロセスは簡単かつ高速です。

ラベル バインディングの配布

ネットワーク内の各ラベル スイッチング ルータ（LSR）は、転送同等クラスを表すためにどのラベル値を使用するかについて独立したローカルな決定を行います。このアソシエーションは、ラベル バインディングと呼ばれます。各 LSR は、自身が行ったラベル バインディングをネイバーに通知します。このようにネイバー スイッチにラベル バインディングを認識させる処理は、次のプロトコルによって促進されます。

- ラベル配布プロトコル（LDP）：MPLS ネットワーク内のピア LSR は、MPLS ネットワークでのホップバイホップ転送をサポートするためのラベルバインディング情報を交換できます
- Border Gateway Protocol（BGP）：MPLS バーチャル プライベート ネットワーク（VPN）をサポートするために使用

ラベル付きパケットが LSR A からネイバー LSR B に送信されている場合、単一の IP パケットによって伝送されるラベル値は、パケットの転送等価クラスを表すために LSR B によって割り当てられたラベル値です。このため、IP パケットがネットワークを通過するにつれて、ラベル値は変更されます。

MPLS の設定方法

このセクションでは、MPLS スイッチングと転送用にスイッチを準備するために必要な基本設定を行う方法について説明します。

他の MPLS アプリケーション用の設定タスクは、アプリケーションの機能モジュールのドキュメントで説明されています。

MPLS スイッチング用のスイッチの設定

シスコ スイッチ上の MPLS スイッチングでは、Cisco Express Forwarding がイネーブルである必要があります。

Cisco Express Forwarding コマンドの詳細については、『Cisco IOS Switching Command Reference』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip cef distributed** 例： `Device(config)# ip cef distributed`	スイッチでシスコ エクスプレス フォワーディングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**mpls label range** *minimum-value maximum-value* 例： `Device(config)# mpls label range 16 4096`	パケット インターフェイス上で MPLS アプリケーションで使用可能なローカル ラベルの範囲を設定します。
ステップ 5	**mpls label protocol ldp** 例： `Device(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を指定します。

MPLS スイッチングの構成の確認

Cisco Express Forwarding が正しく設定されていることを確認するには、**show ip cef summary** コマンドを発行します。次に示すような出力が生成されます。

手順

show ip cef summary

例：

```
Switch# show ip cef summary
IPv4 CEF is enabled for distributed and running
VRF Default
 150 prefixes (149/1 fwd/non-fwd)
 Table id 0x0
 Database epoch:        4 (150 entries at this epoch)
Switch#
```

MPLS 転送用のスイッチの設定

シスコ スイッチ上の MPLS 転送では、IPv4 パケットの転送がイネーブルになっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot/subslot /port* 例： `Device(config)# interface gigabitethernet 1/0/0`	ギガビット イーサネット インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。スイッチ仮想インターフェイス（SVI）の場合の例を次に示します。 `Device(config)# interface vlan 1000`
ステップ 4	**mpls ip** 例： `Device(config-if)# mpls ip`	ルーテッド物理インターフェイス（ギガビット イーサネット）、スイッチ仮想インターフェイス（SVI）、またはポート チャネルに沿った IPv4 パケットの MPLS 転送を有効にします。
ステップ 5	**mpls label protocol ldp** 例： `Device(config-if)# mpls label protocol ldp`	インターフェイスの Label Distribution Protocol を指定します。 （注） MPLS LDP は、Virtual Routing and Forwarding（VRF）インターフェイスで有効にすることはできません。
ステップ 6	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MPLS 転送の構成の確認

MPLS 転送が正しく設定されていることを確認するには、**show mpls interfaces detail** コマンドを発行します。次に示すような出力が生成されます。

手順

ステップ 1 **show mpls interfaces detail**

例：

```
For physical (Gigabit Ethernet) interface:
Switch# show mpls interfaces detail interface GigabitEthernet 1/0/0
        Type Unknown
```

```
        IP labeling enabled
        LSP Tunnel labeling not enabled
        IP FRR labeling not enabled
        BGP labeling not enabled
        MPLS not operational
        MTU = 1500

For Switch Virtual Interface (SVI):
Switch# show mpls interfaces detail interface Vlan1000
        Type Unknown
        IP labeling enabled (ldp) :
          Interface config
        LSP Tunnel labeling not enabled
        IP FRR labeling not enabled
        BGP labeling not enabled
        MPLS operational
        MTU = 1500
```

ステップ 2 show running-config interface

例：

```
For physical (Gigabit Ethernet) interface:
Switch# show running-config interface interface GigabitEthernet 1/0/0
Building configuration...


Current configuration : 307 bytes
!
interface TenGigabitEthernet1/0/0
no switchport
ip address xx.xx.x.x xxx.xxx.xxx.x
mpls ip
mpls label protocol ldp
end

For Switch Virtual Interface (SVI):
Switch# show running-config interface interface Vlan1000
Building configuration...


Current configuration : 187 bytes
!
interface Vlan1000
ip address xx.xx.x.x xxx.xxx.xxx.x
mpls ip
mpls label protocol ldp
end
```

MPLS レイヤ 3 VPN

マルチプロトコルラベルスイッチング（MPLS）バーチャルプライベートネットワーク（VPN）は、MPLS プロバイダー コア ネットワークによって相互接続された一連のサイトで構成されます。各カスタマー サイトでは、1 つ以上のカスタマー エッジ（CE）ルータが、1 つ以上のプロバイダー エッジ（PE）ルータに接続されます。

MPLS レイヤ 3 VPN を設定する前に、MPLS、ラベル配布プロトコル（LDP）、およびシスコ エクスプレス フォワーディング（CEF）が、ネットワークにインストールされている必要があります。PE ルータを含む、コア内のすべてのルータは、CEF および MPLS 転送をサポートできる必要があります。

MPLS QoS EXP の分類とマーキング

QoS EXP Matching 機能を使用すれば、IP パケットのマルチプロトコル ラベル スイッチング（MPLS）Experimental ビット（EXP ビット）フィールドを変更して、ネットワーク トラフィックを分類してマーキングすることができます。

QoS EXP Matching 機能を使用すれば、MPLS パケットの MPLS EXP フィールドに値を設定することによってネットワーク トラフィックを整理できます。MPLS EXP フィールドで異なった値を選択することにより、輻輳時にパケットが必要なプライオリティを持つようパケットをマーキングすることができます。MPLS EXP 値の設定によって次のことが可能になります。

- **トラフィックの分類**：分類プロセスでマーキングするトラフィックが選択されます。分類は、トラフィックを複数の優先順位レベル、つまり、サービス クラスに分割することによりこのプロセスを実施します。トラフィック分類は、クラス ベースの QoS プロビジョニングのプライマリ コンポーネントです。
- **トラフィックのポリシングとマーキング**：ポリシングでは、設定されたレートを上回るトラフィックが廃棄されるか、別のドロップ レベルにマーキングされます。トラフィックのマーキングは、パケット フローを特定してそれらを区別する方法です。パケット マーキングを利用すれば、ネットワークを複数の優先プライオリティ レベルまたはサービス クラスに分割することができます。

注意事項

次に注意事項を示します。

- 均一モードとパイプ モードのみがサポートされます。ショートパイプ モードはサポートされません。
- サポートされる QoS グループ値の範囲は 0 ～ 30 です。（合計 31 の QoS グループ）。
- QoS ポリシーを使用した EXP マーキングは外部ラベルでのみサポートされます。内部の EXP マーキングはサポートされません。

用語集

BGP：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。IP ネットワークで主に使用されるドメイン間ルーティング プロトコルです。

BorderGatewayProtocol：BGP を参照。

FIB：Forwarding Information Base（転送情報ベース）。IP ルーティング テーブル内の転送情報のコピーを格納したテーブルです。

ForwardingInformationBase：FIB を参照。

label：データ（パケットまたはセル）の転送方法をスイッチング ノードに指示する短い固定長の識別子。

labelbinding：ラベルと一連のパケット間のアソシエーション。これは、ラベル スイッチド パスを設定できるようにネイバーにアドバタイズできます。

LabelDistributionProtocol：LDP を参照。

LabelForwardingInformationBase：LFIB を参照。

labelimposition：最初のラベルをパケットに追加する動作。

labelswitchingrouter：LSR を参照。

LDP：Label Distribution Protocol（ラベル配布プロトコル）。ラベルとネットワーク プレフィックスの間のバインディングを配布することによって、MPLS ホップバイホップ転送をサポートするプロトコル。

LFIB：Label Forwarding Information Base（ラベル転送情報ベース）。宛先および着信ラベルが発信インターフェイスおよびラベルに関連付けられているデータ構造。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ラベル スイッチングの基礎となる業界標準。

MPLShop-by-hopforwarding：MPLS 転送メカニズムを使用した通常のルーティッド パスによるパケットの転送。

MultiprotocolLabelSwitching：MPLS を参照。

RIB：Routing Information Base（ルーティング情報ベース）。ルータで動作するすべてのルーティング プロトコルを格納した共通データベース。

RoutingInformationBase：RIB を参照。

VirtualPrivateNetwork：VPN を参照。

VPN：Virtual Private Network（仮想プライベート ネットワーク）。トンネリングを使用することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できるネットワーク。

第 67 章

マルチキャスト バーチャル プライベート ネットワークの設定

• マルチキャスト VPN の設定 （1167 ページ）

マルチキャスト VPN の設定

マルチキャスト VPN（MVPN）機能は、レイヤ 3 VPN 上でマルチキャストをサポートできるようにします。企業がマルチキャストアプリケーションの範囲を拡大するにつれて、サービスプロバイダーは、マルチプロトコル ラベル スイッチング（MPLS）コア ネットワークを通じてそれらに対応できます。IP マルチキャストは、ビデオ、音声、およびデータを MPLS VPN ネットワーク コア経由でストリーミングするために使用します。

従来、ポイントツーポイント トンネルはサービス プロバイダー ネットワークに接続する唯一の方法でした。このようなトンネルネットワークは、スケーラビリティの問題が発生する傾向がありますが、IP マルチキャスト トラフィックを VPN に通過させる唯一の方法でした。

レイヤ 3 VPN はユニキャスト トラフィック接続のみをサポートするため、レイヤ 3 VPN を併用して MPLS を導入することによって、サービスプロバイダーは、レイヤ 3 VPN のカスタマーにユニキャスト接続とマルチキャスト接続の両方を提供できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

マルチキャスト VPN の設定に関する前提条件

「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用して、IP マルチキャストを有効にして PIM インターフェイスを設定します。

マルチキャスト VPN の設定の制限

- ボーダー ゲートウェイ プロトコル（BGP）ピアリングのアップデート ソース インターフェイスは、デフォルト マルチキャスト配信ツリー（MDT）を適切に設定するために、デバイス上に設定されたすべての BGP ピアリングで同じにする必要があります。BGP ピアリングにループバック アドレスを使用する場合は、ループバック アドレスで PIM スパース モードをイネーブルにする必要があります。
- MVPN では、複数の BGP ピアリング更新送信元をサポートしていません。
- 複数の BGP 更新送信元はサポートされていません。これらを設定すると、リバース パス フォワーディング（RPF）のチェックが中断される可能性があります。MVPN トンネルの送信元 IP アドレスは、BGP ピアリング更新送信元に使用される最高の IP アドレスによって決まります。この IP アドレスが、リモートのプロバイダー エッジ（PE）デバイスを含む BGP ピアリング アドレスとして使用される IP アドレスでない場合、MVPN は適切に機能しません。

マルチキャスト VPN の設定について

マルチキャスト VPN の操作

MVPN IP を使用すると、サービス プロバイダーは MPLS VPN 環境でマルチキャスト トラフィックを設定およびサポートできます。この機能は、個々の VRF インスタンスでのマルチキャスト パケットのルーティングおよび転送をサポートし、サービス プロバイダーのバックボーンに VPN マルチキャスト パケットを転送するメカニズムも提供します。

VPN は、ISP などの共有インフラストラクチャを介するネットワークの接続性です。その役割は、プライベート ネットワークとして、同じポリシーとパフォーマンスを低い所有コストで提供することによって、業務とインフラストラクチャを通して、多くのコスト削減の機会を作り出すことです。

MVPN により、企業はサービス プロバイダーのネットワーク バックボーンでプライベート ネットワークをトランスペアレントに相互接続することができます。このように MVPN を使用して企業ネットワークを相互接続しても、企業ネットワークの管理方法や、企業の全体的な接続性は変更されません。

マルチキャスト VPN の利点

- 複数の場所に情報を動的に送信するスケーラブルなメソッドを提供します。
- 高速な情報伝送を提供します。

- 共有インフラストラクチャを介して接続性を提供します。

マルチキャスト VPN ルーティングおよび転送とマルチキャスト ドメイン

MVPN は、VPN ルーティングおよび転送テーブルにマルチキャスト ルーティング情報を導入します。プロバイダー エッジ（PE）デバイスがマルチキャスト データまたは制御パケットをカスタマー エッジ（CE）ルータから受信すると、マルチキャスト VPN ルーティングおよび転送インスタンス（MVRF）の情報に従って転送が実行されます。MVPN は、ラベル スイッチングを使用しません。

マルチキャスト トラフィックを相互に送信できる MVRF のセットは、マルチキャスト ドメインの構成要素です。たとえば、特定タイプのマルチキャスト トラフィックをすべてのグローバルな従業員に送信するカスタマーのマルチキャスト ドメインは、そのエンタープライズと関連するすべての CE ルータから構成されます。

マルチキャスト配信ツリー

MVPN は、各マルチキャスト ドメインにスタティック デフォルト マルチキャスト配信ツリー（MDT）を確立します。デフォルト MDT は、PE ルータが使用するパスを定義し、マルチキャスト ドメインにある他のすべての PE ルータに、マルチキャスト データとコントロール メッセージを送信します。

Source Specific Multicast（SSM; 送信元特定マルチキャスト）がコア マルチキャスト ルーティング プロトコルとして使用される場合、デフォルト MDT およびデータ MDT に使用されるマルチキャスト IP アドレスは、すべての PE ルータの SSM 範囲内に設定する必要があります。

また、MVPN は、高帯域幅伝送用の MDT のダイナミックな作成もサポートします。データ MDT は、Cisco IOS ソフトウェアに一意な機能です。データ MDT は、VPN 内のフルモーション ビデオなどの高帯域幅の送信元向けであり、MPLS VPN コアの最適なトラフィック転送を確保することを目的としています。データ MDT が作成されるしきい値は、ルータ単位または VRF 単位で設定できます。マルチキャスト伝送が定義されたしきい値を超えると、送信側の PE ルータがデータ MDT を作成し、データ MDT に関する情報を含む UDP メッセージをデフォルト MDT のすべてのルータに送信します。マルチキャスト ストリームがデータ MDT のしきい値を超えたかどうかを判断する統計情報は、1 秒に 1 回確認されます。PE ルータは UDP メッセージを送信した後、切り替わるまでに 3 秒以上待機します。最も長くかかる場合は 13 秒、最良の場合は 3 秒です。

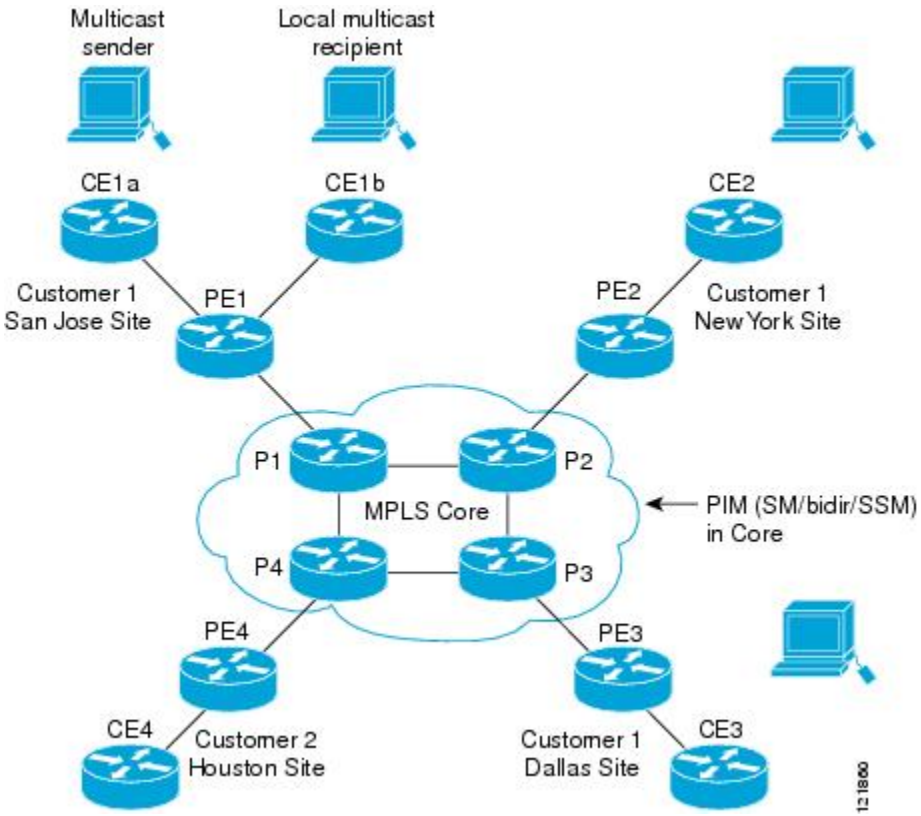
データ MDT は、VRF マルチキャスト ルーティング テーブル内で、（S,G）マルチキャスト ルート エントリ専用に作成されます。個々のソースデータ レートの値に関係なく、(*, G) エントリ用には作成されません。

次の例のサービス プロバイダーには、San Jose、New York、Dallas にオフィスがあるマルチキャスト カスタマーがいます。San Jose では、一方向のマルチキャスト プレゼンテーションが行われています。サービス プロバイダー ネットワークでは、このカスタマーと関連する 3 つすべてのサイト、および別のエンタープライズ カスタマーの Houston サイトがサポートされます。

エンタープライズ カスタマーのデフォルト MDT は、プロバイダーのルータ P1、P2、P3、およびその関連 PE ルータから構成されています。PE4 は別のカスタマーに関連付けられているため、デフォルト MDT の一部ではありません。次の図からは、San Jose 以外はマルチキャス

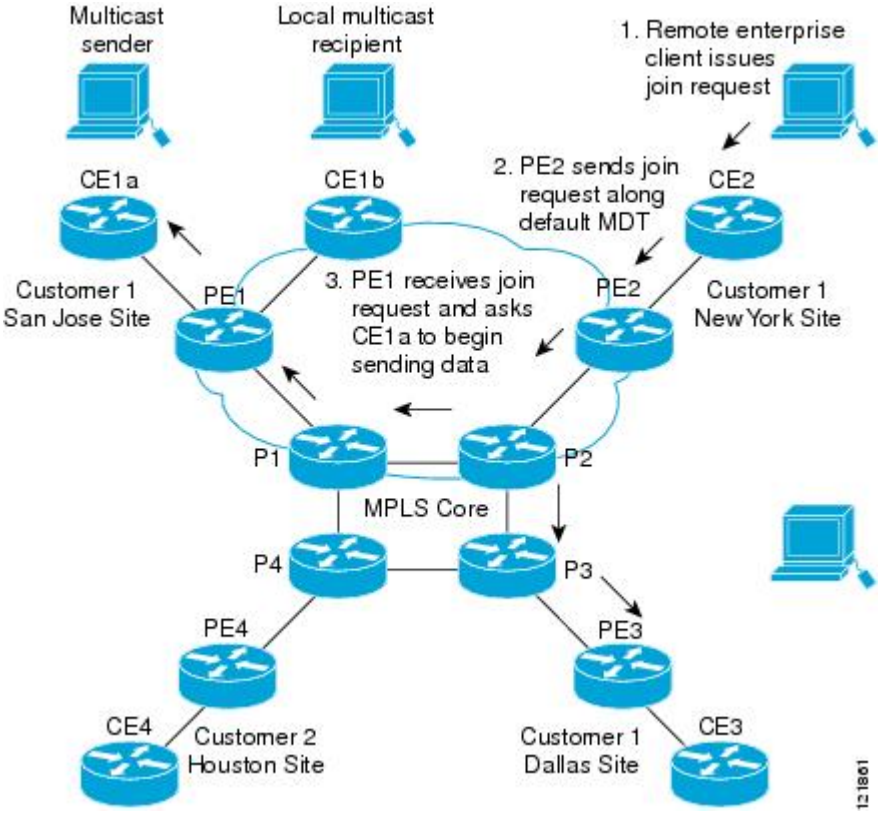
トに加入していないため、データがデフォルト MDT に沿って転送されていないことがわかります。

図 *75*：デフォルト マルチキャスト配信ツリーの概要



New York の従業員がマルチキャスト セッションに加入します。New York のサイトに関連付けられている PE ルータは、カスタマーのマルチキャスト ドメインのデフォルト MDT を介して転送される加入要求を送信します。PE1 は、マルチキャスト セッションの送信元に関連付けられている PE ルータであり、この要求を受信します。次の図は、PE ルータが、マルチキャスト送信元（CE1a）と関連する CE ルータに要求を転送する方法を示しています。

図 *76*：データ *MDT* の初期化



CE ルータ（CE1a）が関連する PE ルータ（PE1）へマルチキャスト データの送信を開始すると、PE ルータ（PE1）は、デフォルト MDT に沿ってマルチキャスト データを送信します。PE1 は、マルチキャスト データを送信すると、マルチキャスト データがデータ MDT を作成する対象の帯域幅のしきい値を超えていることを認識します。したがって、PE1 はデータ MDT を作成し、データ MDT に関する情報を含むデフォルト MDT を使用して、すべてのルータにメッセージを送信し、3 秒後、データ MDT を使用して、その特定のストリームのマルチキャスト データを送信し始めます。このソースに関係する受信先は PE2 だけにあるので、PE2 だけがデータ MDT に加入し、データ MDT でトラフィックを受信します。

PE ルータは、デフォルト MDT を介して他の PE ルータと PIM 関係を維持するとともに、直接接続された PE ルータとの PIM 関係をも維持します。

マルチキャスト トンネル インターフェイス

マルチキャスト ドメインごとに作成される MVRF では、デバイスは、すべての MVRF トラフィックが発信されるトンネルインターフェイスを作成する必要があります。マルチキャスト トンネル インターフェイスは、MVRF がマルチキャスト ドメインにアクセスするために使用するインターフェイスです。これは MVRF とグローバル MVRF をつなぐコンジットと見なすことができます。MVRF ごとに 1 つのトンネル インターフェイスが作成されます。

マルチキャスト VPN での BGP の MDT アドレス ファミリ

MDT アドレス ファミリ セッションを設定するために、**mdt** キーワードが **address-family ipv4** コマンドに追加されました。MDT アドレス ファミリ セッションは、Border Gateway Protocol（BGP）MDT Subaddress Family Identifier（SAFI）のアップデートを使用して PIM に送信元 PE アドレスと MDT グループ アドレスを渡すために使用されます。

マルチキャスト VPN サポートの BGP アドバタイズメント方式

1 つの自律システムで、MVPN のデフォルト MDT がランデブー ポイント（RP）のあるスパース モード（PIM-SM）を使用している場合、ソース PE とレシーバ PE は RP を通して互いを検出するため、PIM は、マルチキャスト トンネル インターフェイス（MTI）に隣接を確立できます。このシナリオでは、ローカル PE（送信元 PE）が RP に登録メッセージを送信し、次に RP が送信元 PE に向けて最短パスツリーを構築します。次にリモート PE（MDT マルチキャスト グループの受信者として機能します）が RP に向けて (*, G) 加入メッセージを送信し、そのグループの配信ツリーに参加します。

しかし、デフォルト MDT グループが PIM-SM 環境ではなく PIM Source Specific Multicast（PIM-SSM）環境で設定されている場合、受信側 PE は送信元 PE とデフォルト MDT グループに関する情報を必要とします。この情報は、送信元 PE に向けて (S, G) 加入メッセージを送信し、送信元PEからの配信ツリーを構築するために使用されます。（RPは必要ありません）。送信元 PE アドレスとデフォルト MDT グループ アドレスは、BGP を使用して送信されます。

BGP 拡張コミュニティ

BGP 拡張コミュニティを使用すると、PE ループバック（発信元アドレス）情報は VPNv4 プレフィックスとしてルート識別子（RD）タイプ 2 を使用して送信されます（ユニキャスト VPNv4 プレフィックスと区別するため）。MDT グループ アドレスは、BGP 拡張コミュニティに伝えられます。VPNv4 アドレスに組み込まれた送信元と拡張コミュニティ内のグループの組み合わせを使用すると、同じ MVRF インスタンス内の PE ルータは相互に SSM ツリーを確立できます。

（注） MDT SAFI サポートが導入される前、BGP 拡張コミュニティの属性は、IETF によって標準化される前のソース PE およびデフォルト MDT グループの IP アドレスをアドバタイズするための暫定的ソリューションとして使用されていました。しかし、MVPN 環境の BGP 拡張コミュニティ属性には一定の制限があります。AS 間シナリオでは使用できず（属性が非推移的であるため）、RD タイプ 2 が使用されます（これはサポートされる標準ではありません）。

マルチキャスト VPN の設定方法

データ マルチキャスト グループの設定

データ MDT グループには、VPN、VRF、PE デバイスごとに最大 256 のマルチキャスト グループを含むことができます。データ MDT グループの作成に使用されるマルチキャスト グループ

は、設定済み IP アドレスのプールからダイナミックに選択されます。デバイス でデータ マルチキャスト グループを設定するには、次の手順を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition vrf1`	VRF コンフィギュレーション モードを開始し、VRF 名を割り当てることにより VPN ルーティング インスタンスを定義します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 1:1`	VRF のルーティング テーブルと転送テーブルを作成します。 • *route-distinguisher* 引数では、8 バイトの値を IPv4 プレフィックスに追加して VPN IPv4 プレフィックスを作成することを指定します。*route-distinguisher* は、次のいずれかの形式で入力できます。 • 16 ビット ASN：32 ビット数値。たとえば、101:3 と指定します。 • 32 ビット IP アドレス：16 ビット数値。たとえば、192.168.122.15:1 と指定します。
ステップ 5	**route-target both** *ASN:nn or IP-address:nn* 例： `Device(config-vrf)# route-target both 1:1`	VRF 用にルート ターゲット拡張コミュニティを作成します。**both** キーワードを使用すると、ルーティング情報のターゲット VPN 拡張コミュニティからのインポート、およびターゲット VPN 拡張コミュニティへのエクスポートの両方が行われます。

	コマンドまたはアクション	目的
ステップ 6	**address family ipv4 unicast** *value* 例： `Device(config-vrf)# address family ipv4 unicast`	VRF アドレス ファミリ コンフィギュレーションモードを開始して、VRF のアドレス ファミリを指定します。 • **ipv4** キーワードは、VRF の IPv4 アドレスファミリを指定します。
ステップ 7	**mdt default** *group-address* 例： `Device(config-vrf-af)# mdt default 226.10.10.10`	VRF に、データ MDT グループのマルチキャスト グループ アドレスの範囲を設定します。 • このコマンドによって、トンネルインターフェイスが作成されます。 • デフォルト MDT グループ アドレス設定は、同じ VRF 内のすべての PE で同一にする必要があります。
ステップ 8	**mdt data** グループ番号 例： `Device(config-vrf-af)# mdt data 232.0.1.0 0.0.0.31`	データ MDT プールで使用されるアドレスの範囲を指定します。
ステップ 9	**mdt datathreshold** *kbps* 例： `Device(config-vrf-af)# mdt data threshold 50`	しきい値を *kbps* 単位で指定します。範囲は 1 ～ 4294967 です。
ステップ 10	**mdt log-reuse** 例： `Device(config-vrf-af)# mdt log-reuse`	（任意）データ MDT 再使用の記録をイネーブルにし、データ MDT が再使用された場合に、syslog メッセージを生成します。
ステップ 11	**end** 例： `Device(config-vrf-af)# end`	特権 EXEC モードに戻ります。

VRF のデフォルト MDT グループの設定

VRF にデフォルト MDT グループを設定するには、次の作業を実行します。

デフォルトMDTグループは、同じVPNに属するすべてのデバイスに設定された同じグループである必要があります。送信元 IP アドレスは、BGP セッションの送信元を特定するために使用するアドレスです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** 例： `Device(config)# ip multicast-routing`	マルチキャストルーティングをイネーブルにします。
ステップ 4	**ip multicast-routing vrf** *vrf-name* 例： `Device(config)# ip multicast-routing vrf vrf1`	MVPN VRF インスタンスをサポートします。
ステップ 5	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition vrf1`	VRF コンフィギュレーション モードを開始し、VRF 名を割り当てることにより VPN ルーティング インスタンスを定義します。
ステップ 6	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 1:1`	VRF のルーティング テーブルと転送テーブルを作成します。 • *route-distinguisher* 引数では、8 バイトの値を IPv4 プレフィックスに追加して VPN IPv4 プレフィックスを作成することを指定します。*route-distinguisher* は、次のいずれかの形式で入力できます。 • 16 ビット ASN：32 ビット数値。たとえば、101:3 と指定します。

	コマンドまたはアクション	目的
		• 32 ビット IP アドレス：16 ビット数値。たとえば、192.168.122.15:1 と指定します。
ステップ 7	**route-target both** *ASN:nn or IP-address:nn* 例： `Device(config-vrf)# route-target both 1:1`	VRF 用にルートターゲット拡張コミュニティを作成します。**both** キーワードを使用すると、ルーティング情報のターゲット VPN 拡張コミュニティからのインポート、およびターゲット VPN 拡張コミュニティへのエクスポートの両方が行われます。
ステップ 8	**address family ipv4 unicast** *value* 例： `Device(config-vrf)# address family ipv4 unicast`	VRF アドレス ファミリ コンフィギュレーションモードを開始して、VRF のアドレス ファミリを指定します。 • **ipv4** キーワードは、VRF の IPv4 アドレスファミリを指定します。
ステップ 9	**mdt default** *group-address* 例： `Device(config-vrf-af)# mdt default 226.10.10.10`	VRF に、データ MDT グループのマルチキャストグループアドレスの範囲を設定します。 • このコマンドによって、トンネルインターフェイスが作成されます。 • デフォルト MDT グループ アドレス設定は、同じ VRF 内のすべての PE で同一にする必要があります。
ステップ 10	**end** 例： `Device(config-vrf-af)# end`	特権 EXEC モードに戻ります。
ステップ 11	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 12	**ip pim vrf** *vrf-name***rp-address** *value* 例： `Device(config-vrf-af)# ip pim vrf vrf1 rp-address 1.1.1.1`	RP コンフィギュレーション モードを開始します。

マルチキャスト VPN での BGP の MDT アドレス ファミリの設定

PE デバイスに MDT アドレス ファミリ セッションを設定し、MVPN の MDT ピアリング セッションを確立するには、次の作業を実行します。

始める前に

MDT アドレス ファミリを通して MVPN ピアリングを確立する前に、CE デバイスに VPN サービスを提供する PE デバイス上の BGP ネットワークおよびマルチプロトコル BGP に、MPLS およびシスコ エクスプレス フォワーディング（CEF）を設定する必要があります。

（注） 次のポリシー設定パラメータは、サポートされていません。

- ルートオリジネータ属性
- ネットワーク層到着可能性情報（NLRI）プレフィックス フィルタリング（プレフィックス リスト、配信リスト）
- 拡張コミュニティ属性（ルート ターゲットおよび発信元サイト）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65535`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family ipv4 mdt** 例： `Device(config-router)# address-family ipv4 mdt`	アドレス ファミリ コンフィギュレーションを開始し、IP MDT アドレス ファミリ セッションを作成します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** *neighbor-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.1 activate`	このネイバーの MDT アドレス ファミリをイネーブルにします。
ステップ 6	**neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**] 例： `Device(config-router-af)# neighbor 192.168.1.1 send-community extended`	指定されたネイバーとのコミュニティおよび（または）拡張コミュニティの交換をイネーブルにします。
ステップ 7	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 8	**address-family vpnv4** 例： `Device(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーションモードを開始し、VPNv4 アドレスファミリ セッションを作成します。
ステップ 9	**neighbor** *neighbor-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.1 activate`	このネイバーの VPNv4 アドレス ファミリをイネーブルにします。
ステップ 10	**neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**] 例： `Device(config-router-af)# neighbor 192.168.1.1 send-community extended`	指定されたネイバーとのコミュニティおよび（または）拡張コミュニティの交換をイネーブルにします。
ステップ 11	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

MDT デフォルト グループの情報の確認

手順

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **showippim**[**vrf** *vrf-name*] **mdtbgp**

例：

```
Device# show ip pim mdt bgp

MDT-default group 232.2.1.4
rid:1.1.1.1 next_hop:1.1.1.1
```

MDT デフォルト グループの RD の BGP アドバタイズメントに関する情報を表示します。

ステップ 3 **showippim**[**vrf** *vrf-name*] **mdtsend**

例：

```
Device# show ip pim mdt send

MDT-data send list for VRF:vpn8
  (source, group)                      MDT-data group      ref_count
  (10.100.8.10, 225.1.8.1)             232.2.8.0           1
  (10.100.8.10, 225.1.8.2)             232.2.8.1           1
  (10.100.8.10, 225.1.8.3)             232.2.8.2           1
  (10.100.8.10, 225.1.8.4)             232.2.8.3           1
  (10.100.8.10, 225.1.8.5)             232.2.8.4           1
  (10.100.8.10, 225.1.8.6)             232.2.8.5           1
  (10.100.8.10, 225.1.8.7)             232.2.8.6           1
  (10.100.8.10, 225.1.8.8)             232.2.8.7           1
  (10.100.8.10, 225.1.8.9)             232.2.8.8           1
  (10.100.8.10, 225.1.8.10)            232.2.8.9           1
```

指定されたデバイスが行った MDT アドバタイズメントを含む MDT データ グループに関する詳細情報を表示します。

ステップ 4 **showippimvrf** *vrf-name* **mdthistoryinterval** *minutes*

例：

```
Device# show ip pim vrf vrf1 mdt history interval 20

   MDT-data send history for VRF - vrf1 for the past 20 minutes
MDT-data group        Number of reuse
     10.9.9.8           3
     10.9.9.9           2
```

過去に設定されたインターバル中に再利用されたデータ MDT を表示します。

マルチキャスト VPN の設定例

例：MVPN および SSM の設定

次の例では、PIM-SSM がバックボーンに設定されています。そのため、デフォルト グループとデータ MDT グループは、IP アドレスの SSM 範囲内に設定されています。VPN の内部では、PIM-SM が設定され、Auto-RP アナウンスのみが受け入れられます。

```
ip vrf vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 232.0.0.1
 mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
```

例：マルチキャスト ルーティングの VPN のイネーブル化

次の例では、マルチキャスト ルーティングは、vrf1 という VPN ルーティング インスタンスを使用してイネーブル化されます。

```
ip multicast-routing vrf1
```

例：データ MDT グループ用のマルチキャスト グループ アドレス範囲の設定

次の例では、VPN ルーティング インスタンスは、blue という VRF が割り当てられます。VPN VRF の MDT デフォルト グループは 239.1.1.1、MDT グループのマルチキャスト グループ アドレスの範囲は 239.1.2.0（ワイルドカード ビットが 0.0.0.3）です。

```
ip vrf blue
 rd 55:1111
 route-target both 55:1111
 mdt default 239.1.1.1
 mdt data 239.1.2.0 0.0.0.3
 end
```

例：マルチキャスト ルートの数の制限

次の例では、マルチキャスト ルーティング テーブルに追加できるマルチキャスト ルートの数が 200,000 に設定され、警告メッセージが発生する原因となる mroute の数のしきい値が 20,000 に設定されています。

```
!
ip multicast-routing
ip multicast-routing vrf cisco
```

```
ip multicast cache-headers
ip multicast route-limit 200000 20000
ip multicast vrf cisco route-limit 200000 20000
no mpls traffic-eng auto-bw timers frequency 0
!
```

マルチキャスト VPN の設定に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
この章で使用するコマンドの完全な構文および使用方法の詳細。	

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 XII 部

Network Management

- Cisco IOS Configuration Engine の設定 （1185 ページ）
- Cisco Discovery Protocol の設定 （1209 ページ）
- 簡易ネットワーク管理プロトコルの設定 （1221 ページ）
- サービス レベル契約の設定 （1255 ページ）
- ローカル ポリシーの設定 （1281 ページ）
- SPAN および RSPAN の設定 （1293 ページ）
- ERSPAN の設定 （1343 ページ）
- パケット キャプチャの設定 （1353 ページ）
- Flexible NetFlow の設定 （1409 ページ）

第 68 章

Cisco IOS Configuration Engine の設定

- 機能情報の確認 （1185 ページ）
- Configuration Engine を設定するための前提条件 （1185 ページ）
- Configuration Engine の設定に関する制約事項 （1186 ページ）
- Configuration Engine の設定について （1186 ページ）
- Configuration Engine の設定方法 （1193 ページ）
- CNS 設定のモニタリング （1206 ページ）
- その他の参考資料 （1207 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Configuration Engine を設定するための前提条件

- ユーザが接続している Configuration Engine インスタンスの名前を取得します。
- CNS は、イベント バスとコンフィギュレーション サーバの両方を使用してデバイスに設定を提供するので、設定済みのデバイスごとに ConfigID と DeviceID の両方を定義する必要があります。
- **cns config partial** グローバル コンフィギュレーション コマンドを使用して設定したすべてのデバイスがイベントバスにアクセスする必要があります。デバイスを起源とする DeviceID

は、Cisco Configuration Engine 内の対応するデバイス定義の DeviceID と一致する必要があります。ユーザが接続しているイベント バスのホスト名を把握する必要があります。

関連トピック

Cisco Networking Service ID およびデバイスのホスト名 （1188 ページ）
DeviceID （1189 ページ）

Configuration Engine の設定に関する制約事項

- コンフィギュレーション サーバの 1 つのインスタンスでは、設定済みの 2 つのデバイスが同じ ConfigID 値を共有できません。
- イベント バスの 1 つのインスタンスでは、設定済みの 2 つのデバイスが同じ DeviceID 値を共有できません。

関連トピック

Cisco Networking Service ID およびデバイスのホスト名 （1188 ページ）

Configuration Engine の設定について

Cisco Configuration Engine ソフトウェア

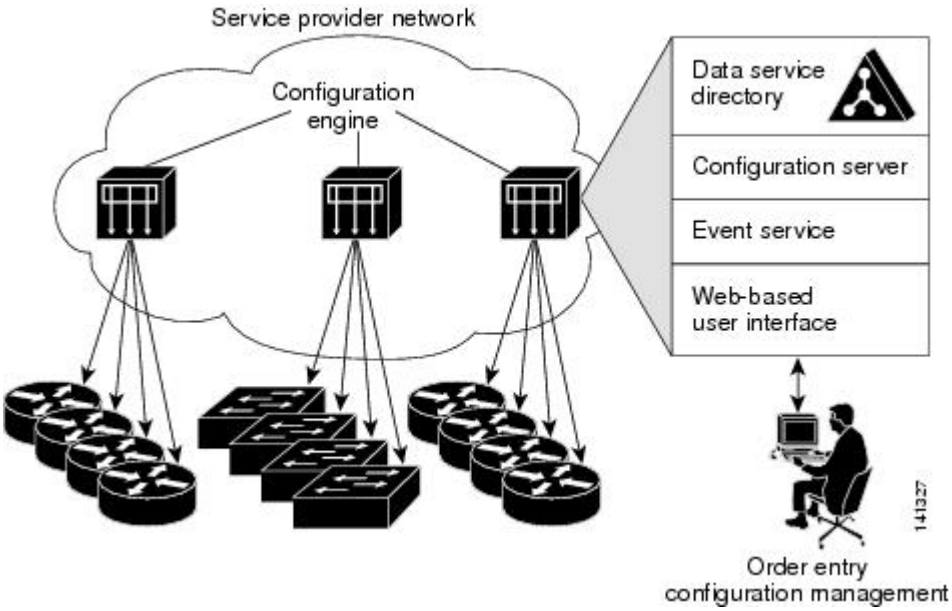
Cisco Configuration Engine は、ネットワーク管理ユーティリティ ソフトウェアで、ネットワーク デバイスおよびサービスの配置と管理を自動化するためのコンフィギュレーション サービスとして機能します。各 Cisco Configuration Engine は、シスコ デバイス（デバイスとルータ）のグループとデバイスが提供するサービスを管理し設定を保存して、必要に応じて配信します。Cisco Configuration Engine は、デバイス固有のコンフィギュレーション変更を生成してデバイスに送信し、コンフィギュレーション変更を実行して結果をログに記録することにより、初期設定とコンフィギュレーションの更新を自動化します。

Cisco Configuration Engine は、スタンドアロン モードとサーバ モードをサポートし、次の Cisco Networking Service（CNS）コンポーネントがあります。

- コンフィギュレーション サービス
  - Web サーバ
  - ファイル マネージャ
  - ネームスペース マッピング サーバ
- イベント サービス（イベント ゲートウェイ）
- データ サービス ディレクトリ（データ モデルおよびスキーマ）

スタンドアロンモードでは、内部に組み込まれたディレクトリ サービスがサポートされます。このモードでは、外部ディレクトリまたはその他のデータ ストアは必要ありません。サーバモードでは、ユーザが定義した外部ディレクトリの使用がサポートされます。

図 *77 : Cisco Configuration Engine* のアーキテクチャの概要



コンフィギュレーション サービス

コンフィギュレーション サービスは、Cisco Configuration Engine の中核コンポーネントです。デバイス上にある Cisco IOS CNS エージェントと連携して動作するコンフィギュレーション サーバで構成されています。コンフィギュレーション サービスは、初期設定と論理グループによる大規模な再設定のために、デバイスとサービスの設定をデバイスに配信します。デバイスはネットワーク上で初めて起動するときに、コンフィギュレーション サービスから初期設定を受信します。

コンフィギュレーション サービスは CNS イベント サービスを使用して設定変更イベントを送受信し、成功および失敗の通知を送信します。

コンフィギュレーション サーバは Web サーバであり、コンフィギュレーション テンプレートと組み込み型ディレクトリ（スタンドアロン モード）またはリモート ディレクトリ（サーバ モード）に保存されているデバイス固有の設定情報を使用します。

コンフィギュレーションテンプレートは、CLI（コマンドライン インターフェイス）コマンド形式で静的な設定情報を含んだテキスト ファイルです。テンプレートでは、変数は、Lightweight Directory Access Protocol（LDAP）URL を使用して指定します。この URL はディレクトリに保存されているデバイス固有の設定情報を参照します。

Cisco IOS エージェントは受信したコンフィギュレーション ファイルの構文をチェックし、イベントを発行して構文チェックが成功または失敗したかを表示します。コンフィギュレーショ

ン エージェントは設定をただちに適用することも、あるいは同期化イベントをコンフィギュレーション サーバから受信するまで適用を遅らせることもできます。

イベント サービス

Cisco Configuration Engine は、設定イベントの受信および生成にイベント サービスを使用します。イベント サービスはイベント エージェント、イベント ゲートウェイから構成されます。イベント エージェントはデバイス上にあり、デバイスと Cisco Configuration Engine のイベント ゲートウェイ間の通信を容易にします。

イベント サービスは、非常に有効なパブリッシュ サブスクライブ通信方式です。イベント サービスは、サブジェクトベースのアドレス指定を使用して、メッセージを宛先に送信します。サブジェクトベースのアドレス表記法では、メッセージおよび宛先には簡単で均一なネームスペースを定義します。

関連トピック

CNS イベント エージェントのイネーブル化 （1193 ページ）

名前空間マッパー

Cisco Configuration Engine はネームスペース マッパー（NSM）を備えています。これは、アプリケーション、デバイスまたはグループ ID、およびイベントに基づいてデバイスの論理グループを管理するための検索サービスを提供します。

Cisco IOS デバイスは、たとえば cisco.cns.config.load といった、Cisco IOS ソフトウェアで設定されたサブジェクト名と一致するイベント サブジェクト名のみを認識します。ネームスペース マッピング サービスを使用すると、希望する命名規則を使用することでイベントを指定できます。サブジェクト名でデータ ストアにデータを入力した場合、NSM はイベント サブジェクト名ストリングを、Cisco IOS が認識するものに変更します。

サブスクライバの場合、一意のデバイス ID とイベントが指定されると、ネームスペース マッピング サービスは、サブスクライブ対象のイベント セットを返します。同様にパブリッシャの場合、一意のグループ ID、デバイス ID、およびイベントが指定されると、マッピング サービスは、パブリッシュ対象のイベント セットを返します。

Cisco Networking Service ID およびデバイスのホスト名

Cisco Configuration Engine は、設定対象の各デバイスに一意の識別子が関連付けられていることを前提としています。一意の識別子は複数の同義語を持つことができますが、各同義語は特定のネームスペース内で一意です。イベント サービスは、ネームスペースの内容を使用してメッセージのサブジェクトベース アドレス指定を行います。

Cisco Configuration Engine は、イベント バス用とコンフィギュレーション サーバ用の 2 つの名前空間を交差します。コンフィギュレーション サーバのネームスペースでは、*ConfigID* という用語がデバイスの一意な識別子です。イベント バスのネームスペースでは、*DeviceID* という用語がデバイスの CNS 一意識別子です。

関連トピック

Configuration Engine を設定するための前提条件 （1185 ページ）
Configuration Engine の設定に関する制約事項 （1186 ページ）

ConfigID

設定対象のデバイスはそれぞれ固有の ConfigID を持ちます。これは Cisco Configuration Engine ディレクトリからデバイス CLI 属性の対応するセットを取得するためのキーとなります。デバイスで定義された ConfigID は、Cisco Configuration Engine 上の対応するデバイス定義の ConfigID と一致する必要があります。

ConfigID は起動時に固定され、デバイス ホスト名を再設定した場合でもデバイスを再起動するまで変更できません。

DeviceID

イベント バスに参加している設定済みのデバイスごとに一意の DeviceID があります。これはデバイスの送信元アドレスに似ているので、デバイスをバス上の特定の宛先として指定できます。

DeviceID の発信元は、デバイスの Cisco IOS ホスト名によって定義されます。ただし、DeviceID 変数およびその使用は、デバイスに隣接するイベント ゲートウェイ内にあります。

イベント バス上の Cisco IOS の論理上の終点は、イベント ゲートウェイに組み込まれ、それがデバイスの代わりにプロキシとして動作します。イベント ゲートウェイはイベント バスに対して、デバイスおよび対応する DeviceID を表示します。

デバイスは、イベント ゲートウェイとの接続が成功するとすぐに、そのホスト名をイベント ゲートウェイに宣言します。接続が確立されるたびに、イベント ゲートウェイは DeviceID 値を Cisco IOS ホスト名に組み合わせます。イベント ゲートウェイは、デバイスと接続している間、この DeviceID 値を保持します。

関連トピック

Configuration Engine を設定するための前提条件 （1185 ページ）

ホスト名および DeviceID

DeviceID は、イベント ゲートウェイと接続したときに固定され、デバイス ホスト名を再設定した場合でも変更されません。

デバイスでデバイス ホスト名を変更するとき、DeviceID を更新する唯一の方法は、デバイスとイベント ゲートウェイ間の接続を切断することです。DeviceID 更新の手順については、以下の「関連項目」を参照してください。

接続が再確立されると、デバイスは変更したホスト名をイベント ゲートウェイに送信します。イベント ゲートウェイは DeviceID を新しい値に再定義します。

⚠

注意 Cisco Configuration Engine ユーザ インターフェイスを使用するときは、最初に DeviceID フィールドを、デバイスが前ではなく後に取得するホスト名値に設定する必要があります。Cisco IOS CNS エージェント用に設定を再初期化する必要があります。そのようにしないと、後続の部分的なコンフィギュレーション コマンド操作で誤動作が発生する可能性があります。

関連トピック

DeviceID の更新 （1202 ページ）

ホスト名、DeviceID、および ConfigID

スタンドアロンモードでは、ホスト名の値をデバイスに設定すると、コンフィギュレーションサーバはイベントをホスト名に送信する場合、そのホスト名を DeviceID として使用します。ホスト名が設定されていない場合、イベントはデバイスの cn=<*value*>で送信されます。

サーバモードでは、ホスト名は使用されません。このモードでは、バス上のイベント送信には常に一意の DeviceID 属性が使用されます。この属性が設定されていない場合はデバイスを更新できません。

Cisco Configuration Engine で **Setup** を実行する場合、これらの属性および関連する属性（タグ値のペア）を設定します。

Cisco IOS CNS エージェント

CNS イベント エージェント機能によって、デバイスはイベント バス上でイベントにパブリッシュおよびサブスクライブを行い、Cisco IOS CNS エージェントと連携できます。デバイス Cisco IOS ソフトウェアに組み込まれているこれらのエージェントでは、デバイスを接続して、自動的に設定できます。

関連トピック

Cisco IOS CNS エージェントのイネーブル化 （1195 ページ）

初期設定

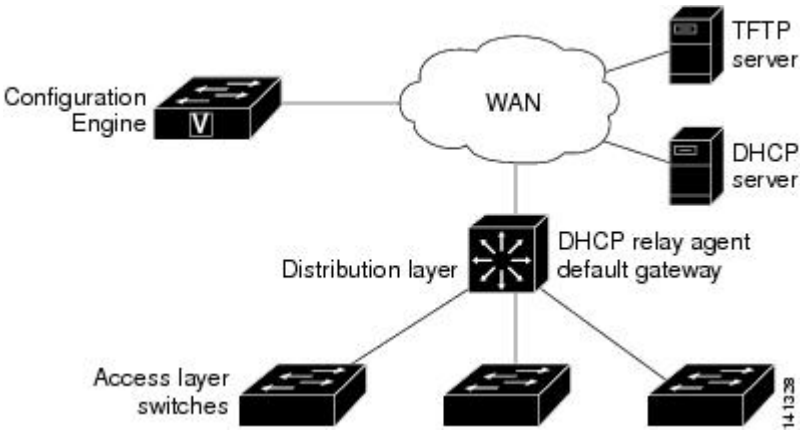
デバイスが最初に起動すると、ネットワークで Dynamic Host Configuration Protocol（DHCP）要求をブロードキャストすることで IP アドレスを取得しようとします。サブネット上には DHCP サーバがないものと想定し、ディストリビューション デバイスは DHCP リレー エージェントとして動作し、要求を DHCP サーバに転送します。DHCP サーバは要求を受信すると、新しいデバイスに IP アドレスを割り当て、Trivial File Transfer Protocol（TFTP）サーバのインターネットプロトコル（IP）アドレス、ブートストラップ コンフィギュレーション ファイルへのパス、デフォルト ゲートウェイの IP アドレスを、DHCP リレー エージェントに対するユニキャスト応答に組み入れます。DHCP リレー エージェントは、この応答をデバイスに転送します。

デバイスは、割り当てられた IP アドレスを自動的にインターフェイス VLAN 1（デフォルト）に設定し、TFTP サーバからブートストラップ コンフィギュレーション ファイルをダウンロードします。ブートストラップ コンフィギュレーション ファイルが正常にダウンロードされると、デバイスはそのファイルを実行コンフィギュレーションにロードします。

Cisco IOS CNS エージェントは、該当する ConfigID および EventID を使用して Configuration Engine との通信を開始します。Configuration Engine はこの ConfigID をテンプレートにマッピングして、デバイスに完全なコンフィギュレーション ファイルをダウンロードします。

次の図に、DHCP ベースの自動設定を使用して初期ブートストラップ コンフィギュレーション ファイルを取得するためのネットワーク構成例を示します。

図 *78* : 初期設定



関連トピック

Cisco IOS CNS エージェントの初期設定のイネーブル化 （1197 ページ）
CNS 設定のモニタリング （1206 ページ）

差分（部分的）設定

ネットワークが稼働すると、Cisco IOS CNS エージェントを使用して新しいサービスを追加できます。差分（部分）設定は、デバイスに送信できます。実際の設定を、イベントペイロードとしてイベントゲートウェイを介して（プッシュ処理）送信するか、デバイスにプルオペレーションを開始させる信号イベントとして送信できます。

デバイスは、適用する前に設定の構文をチェックできます。構文が正しい場合は、デバイスは差分設定を適用し、コンフィギュレーションサーバに成功を信号で伝えるイベントを発行します。デバイスが差分設定を適用しない場合、エラーステータスを示すイベントを発行します。デバイスが差分設定を適用した場合、不揮発性RAM（NVRAM）に書き込むか、または書き込むように指示されるまで待つことができます。

関連トピック

Cisco IOS CNS エージェントの部分的設定のイネーブル化 （1204 ページ）
CNS 設定のモニタリング （1206 ページ）

コンフィギュレーションの同期

デバイスは、設定を受信した場合、書き込み信号イベントの受信時に設定の適用を遅らせることができます。書き込み信号イベントは、更新された設定をNVRAMに保存しないようにデバイスに指示します。デバイスは更新された設定を実行コンフィギュレーションとして使用しま

す。これによりデバイスの設定は、次のリブート時の使用のためにNVRAMに設定を保存する前に、他のネットワーク アクティビティと同期化されます。

自動 CNS 設定

デバイスの自動 CNS 設定をイネーブルにするには、まずこのトピックに示す前提条件を完了する必要があります。条件設定を完了したらデバイスの電源を入れます。**setup** プロンプトでは何も入力しません。デバイスが初期設定を開始します。コンフィギュレーション ファイル全体がデバイスにロードされると作業は完了です。

初期設定中の動作については、「関連項目」を参照してください。

表 *66*：自動設定イネーブル化の条件

デバイス	必要な設定
アクセス デバイス	出荷時の設定（コンフィギュレーション ファイルなし）
ディストリビューション デバイス	• IP ヘルパー アドレス • DHCP リレー エージェントをイネーブルにする[2] • IP ルーティング（デフォルト ゲートウェイとして使用する場合）
DHCP サーバ	• IP アドレスの割り当て • TFTP サーバの IP アドレス • TFTP サーバのブートストラップ コンフィギュレーション ファイルへのパス • デフォルト ゲートウェイの IP アドレス
TFTP サーバ	• デバイスと Configuration Engine との通信を可能にする CNS コンフィギュレーション コマンドを含むブートストラップ コンフィギュレーション ファイル • （デフォルトのホスト名の代わりに）デバイス MAC アドレスまたはシリアル番号のいずれかを使用して ConfigID および EventID を生成するように設定されたデバイス • デバイスにコンフィギュレーション ファイルをプッシュするように設定された CNS イベント エージェント
CNS Configuration Engine	デバイス タイプ別の 1 つまたは複数のテンプレートで、テンプレートにデバイスの ConfigID がマッピングされています。

[2] DHCP リレーは、DHCP サーバがクライアントとは異なるサブネット上にある場合にのみ必要です。

Configuration Engine の設定方法

CNS イベント エージェントのイネーブル化

（注） デバイス上で CNS イベント エージェントをイネーブルにしてから、CNS 設定エージェントをイネーブルにする必要があります。

デバイス上で CNS イベント エージェントをイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cns event** {*hostname* | *ip-address*} [*port-number*] [[**keepalive** *seconds retry-count*] [**failover-time** *seconds*] [**reconnect-time** *time*] | **backup**] 例： `Device(config)# cns event 10.180.1.27 keepalive 120 10`	イベント エージェントをイネーブルにして、ゲートウェイ パラメータを入力します。 • {*hostname* | *ip-address*} に、イベント ゲートウェイのホスト名または IP アドレスを入力します。 • （任意）*port number* に、イベント ゲートウェイのポート番号を入力します。デフォルトのポート番号は 11011 です。 • （任意）**keepalive** *seconds* に、デバイスがキープアライブ メッセージを送信する間隔を入力します。

	コマンドまたはアクション	目的
		retry-count に、キープアライブ メッセージへの応答がない場合に接続を終了するまでのデバイスのメッセージ送信回数を入力します。デフォルト値はいずれも 0 です。 • （任意）**failover-time** *seconds* に、バックアップ ゲートウェイが確立された後にデバイスがプライマリ ゲートウェイ ルートを待つ時間を入力します。 • （任意）**reconnect-time** *time* に、デバイスがイベント ゲートウェイに再接続しようとする前の最大時間間隔を入力します。 • （任意）バックアップ ゲートウェイであることを示す場合は、**backup** を入力します（省略した場合は、プライマリ ゲートウェイになります）。 （注） **encrypt** キーワードおよび **clock-timeout***time* キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

次のタスク

イベント エージェントに関する情報を確認するには、**show cns event connections** コマンドを特権 EXEC モードで使用します。

CNS イベント エージェントをディセーブルにするには、**no cns event** { *ip-address* | *hostname* } グローバル コンフィギュレーション コマンドを使用します。

関連トピック

イベント サービス （1188 ページ）

Cisco IOS CNS エージェントのイネーブル化

デバイス上で Cisco IOS CNS エージェントをイネーブルにするには、次の手順を実行します。

始める前に

このエージェントをイネーブルにする前に、デバイスで CNS イベント エージェントをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cns config initial** {*hostname* | *ip-address*} [*port-number*] 例： `Device(config)# cns config initial 10.180.1.27 10`	Cisco IOS CNS エージェントをイネーブルにし、コンフィギュレーション サーバ パラメータを入力します。 • {*hostname* | *ip-address*} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。

	コマンドまたはアクション	目的
		• （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。 このコマンドが Cisco IOS CNS エージェントをイネーブルにして、デバイスで初期設定を開始します。
ステップ 4	**cns config partial** {*hostname* | *ip-address*} [*port-number*] 例： `Device(config)# cns config partial 10.180.1.27 10`	Cisco IOS CNS エージェントをイネーブルにし、コンフィギュレーション サーバ パラメータを入力します。 • {*hostname* | *ip-address*} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。 Cisco IOS CNS エージェントをイネーブルにして、デバイスで部分的設定を開始します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 8	Cisco IOS CNS エージェントを、デバイスで開始します。	

次のタスク

リモートで差分設定をデバイスに送信するために、Cisco Configuration Engine を使用できるようになりました。

関連トピック

Cisco IOS CNS エージェント （1190 ページ）

Cisco IOS CNS エージェントの初期設定のイネーブル化

デバイス上で、CNS コンフィギュレーション エージェントをイネーブルにして初期設定を開始するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cns template connect** *name* 例： `Device(config)# cns template connect template-dhcp`	CNS テンプレート接続コンフィギュレーション モードを開始して、CNS 接続テンプレートの名前を指定します。
ステップ 4	**cli** *config-text* 例： `Device(config-tmpl-conn)# cli ip address dhcp`	CNS 接続テンプレートにコマンドラインを入力します。テンプレート内の各コマンドラインにこの手順を繰り返します。
ステップ 5	別の CNS 接続テンプレートを設定する場合は、ステップ 3 ～ 4 を繰り返します。	
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**cns connect** *name* [**retries** *number*] [**retry-interval** *seconds*] [**sleep** *seconds*] [**timeout** *seconds*] 例： `Device(config)# cns connect dhcp`	CNS 接続コンフィギュレーションモードを開始し、CNS 接続プロファイルの名前を指定し、プロファイルパラメータを定義します。デバイスはCNS 接続プロファイルを使用して Configuration Engine に接続します。 • CNS 接続プロファイルの *name* を入力します。 • （任意）**retries** *number* に、接続のリトライ回数を入力します。指定できる範囲は 1 ～ 30 です。デフォルト値は 3 です。 • （任意）**retry-interval** *seconds* に、Configuration Engine への連続する接続の試行間隔を入力します。指定できる範囲は 1 ～ 40 秒です。デフォルトは 10 秒です。 • （任意）**sleep** *seconds* に、最初の接続試行を実行するまで待機する時間を入力します。指定できる範囲は 0 ～ 250 秒です。デフォルト値は 0 です。 • （任意）**timeout** *seconds* に、接続が終了しようとした後に待機する時間を入力します。値の範囲は 10 ～ 2000 秒です。デフォルト値は 120 です。
ステップ 8	**discover** {**controller** *controller-type* | **dlci** [**subinterface** *subinterface-number*] | **interface** [*interface-type*] | **line** *line-type*} 例： `Device(config-cns-conn)# discover interface gigabitethernet`	CNS 接続プロファイル内のインターフェイス パラメータを入力します。 • **controller** *controller-type* に、コントローラ タイプを入力します。 • **dlci** に、アクティブなデータリンク接続識別子（DLCI）を入力します。 （任意）**subinterface** *subinterface-number* に、アクティブな DLCI の検索に使用するポイン

	コマンドまたはアクション	目的
		トツーポイントサブインターフェイス番号を指定します。 • **interface** [*interface-type*] に、インターフェイスのタイプを入力します。 • **line** *line-type* に、回線タイプを入力します。
ステップ 9	**template** *name* [... *name*] 例： `Device(config-cns-conn)# template template-dhcp`	デバイスの設定に適用する CNS 接続プロファイル内の CNS 接続テンプレートのリストを指定します。複数のテンプレートを指定できます。
ステップ 10	ステップ 8 ～ 9 を繰り返し、CNS 接続プロファイルにさらに多くのインターフェイス パラメータと CNS 接続テンプレートを指定します。	
ステップ 11	**exit** 例： `Device(config-cns-conn)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**hostname** *name* 例： `Device(config)# hostname device1`	デバイスのホスト名を入力します。
ステップ 13	**ip route** *network-number* 例： `RemoteDevice(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1`	（任意）IP アドレスが *network-number* の Configuration Engine へのスタティック ルートを確立します。
ステップ 14	**cns id** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] 例： `RemoteDevice(config)# cns id GigabitEthernet1/0/1 ipaddress`	（任意）Configuration Engine が使用する一意の EventID または ConfigID を設定します。このコマンドを入力する場合は、**cns id** {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**] コマンドを入力しないでください。 • *interface num* に、インターフェイスのタイプを入力します。たとえ

	コマンドまたはアクション	目的
		ば、ethernet、group-async、loopback、virtual-template を入力します。この設定では、一意の ID を定義するためにどのインターフェイスから IP アドレスまたは MAC アドレスを取得するかを指定します。 • {**dns-reverse** | **ipaddress** | **mac-address**} では、ホスト名を取得してそのホスト名を一意の ID として割り当てるには **dns-reverse** を入力し、IP アドレスを使用するには **ipaddress** を入力し、MAC アドレスを一意の ID として使用するには **mac-address** を入力します。 • （任意）ID をデバイスの識別に使用する event-id 値になるように設定するには、**event** を入力します。 • （任意）ID をデバイスの識別に使用する image-id 値になるように設定するには、**image** を入力します。 （注） **event** と **image** キーワードの両方を省略した場合は、デバイスの識別には image-id 値が使用されます。
ステップ 15	**cns id** {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**] 例： `RemoteDevice(config)# cns id hostname`	（任意）Configuration Engine が使用する一意の EventID または ConfigID を設定します。このコマンドを入力する場合は、**cns id** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] コマンドを入力しないでください。 • For {**hardware-serial** | **hostname** | **string** *string* | **udi**}, enter **hardware-serial** to set the デバイス serial number as the unique ID, enter **hostname** (the default) to select the デバイス hostname as the unique ID, enter an arbitrary text string for **string** *string* as the unique ID, or enter **udi** to

	コマンドまたはアクション	目的
		set the unique device identifier (UDI) as the unique ID.
ステップ 16	**cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page** *page*] [**source** *ip-address*] [**syntax-check**] 例： `RemoteDevice(config)# cns config initial 10.1.1.1 no-persist`	Cisco IOS エージェントをイネーブルにして、初期設定を開始します。 • {*hostname* | *ip-address*} に、コンフィギュレーションサーバのホスト名または IP アドレスを入力します。 • （任意）*port number* に、コンフィギュレーションサーバのポート番号を入力します。デフォルトのポート番号は 80 です。 • （任意）設定が完了したときの設定の成功、失敗、または警告のメッセージ用に **event** をイネーブルにします。 • （任意）**no-persist** グローバル コンフィギュレーション コマンドの入力結果によってプルされた設定の NVRAM への自動書き込みを抑制するには、**cns config initial** を入力します。**no-persist** キーワードを入力しない場合、**cns config initial** コマンドを使用すると、その結果の設定が自動的に NVRAM に書き込まれます。 • （任意）**page** *page* に、初期設定の Web ページを入力します。デフォルトは /Config/config/asp です。 • （任意）送信元 IP アドレスに使用するには、**source** *ip-address* を入力します。 • （任意）このパラメータを使用したときの構文をチェックするには、**syntax-check** をイネーブルにします。

	コマンドまたはアクション	目的
		（注） **encrypt**、**status** *url* および **inventory** は、コマンドラインヘルプの文字列に表示されますが、これらのキーワードはサポートされていません。
ステップ 17	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 18	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 19	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次のタスク

コンフィギュレーションエージェントに関する情報を確認するには、**show cns config connections** コマンドを特権 EXEC モードで使用します。

CNS Cisco IOS エージェントをディセーブルにするには、**no cns config initial** { *ip-address* | *hostname* } グローバル コンフィギュレーション コマンドを使用します。

関連トピック

初期設定 （1190 ページ）
CNS 設定のモニタリング （1206 ページ）

DeviceID の更新

デバイス上でホスト名を変更するときに DeviceID を更新するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show cns config connections** 例： `Device# show cns config connections`	CNS イベント エージェントがゲートウェイに接続しているか、接続されているか、またはアクティブか、およびイベントエージェントに使用されているゲートウェイ、その IP アドレス、およびポート番号を表示します。
ステップ 3	CNS イベントエージェントがイベントゲートウェイに正しく接続されていることを確認します。	次のように **show cns config connections** の出力を確認します。 • 接続がアクティブになっている。 • 接続で現在設定されているデバイス ホスト名を使用している。DeviceID はこれらの手順を使用して、新しいホスト名の設定に対応するように更新されます。
ステップ 4	**show cns event connections** 例： `Device# show cns event connections`	デバイスのイベント接続情報を表示します。
ステップ 5	ステップ 4 の出力に基づいて、次に示す現在接続されている接続に関する情報を記録します。この手順の以降のステップで IP アドレスとポート番号を使用します。	
ステップ 6	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 7	**no cns event** *ip-address port-number* 例： `Device(config)# no cns event 172.28.129.22 2012`	このコマンドで、ステップ 5 で記録した IP アドレスとポート番号を指定します。

	コマンドまたはアクション	目的
		このコマンドで、デバイスとイベントゲートウェイ間の接続が解除されます。最初に接続を解除し、次にこの接続を再確立して、DeviceID を更新する必要があります。
ステップ 8	**cns event** *ip-address port-number* 例： `Device(config)# cns event 172.28.129.22 2012`	このコマンドで、ステップ 5 で記録した IP アドレスとポート番号を指定します。 このコマンドで、デバイスとイベントゲートウェイ間の接続が再確立されます。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show cns event connections** からの出力を調べて、デバイスとイベント接続間の接続が再確立されていることを確認します。	
ステップ 11	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

ホスト名および DeviceID （1189 ページ）

Cisco IOS CNS エージェントの部分的設定のイネーブル化

デバイス上で Cisco IOS CNS エージェントをイネーブルにして部分設定を開始するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source** *ip-address*] 例： `Device(config)# cns config partial 172.28.129.22 2013`	コンフィギュレーション エージェントをイネーブルにし、部分設定を開始します。 • {*ip-address* | *hostname*} に、コンフィギュレーション サーバの IP アドレスまたはホスト名を入力します。 • （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は 80 です。 • （任意）送信元 IP アドレスに使用するには、**source** *ip-address* を入力します。 （注） **encrypt** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

コンフィギュレーション エージェントに関する情報を確認するには、**show cns config stats** または **show cns config outstanding** コマンドのいずれかを特権 EXEC モードで使用します。

Cisco IOS エージェントをディセーブルにするには、**no cns config partial** { *ip-address* | *hostname* } グローバル コンフィギュレーション コマンドを使用します。部分設定を取り消すには、**cns config cancel** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

差分（部分的）設定 （1191 ページ）
CNS 設定のモニタリング （1206 ページ）

CNS 設定のモニタリング

表 *67 : CNS show* コマンド

コマンド	目的
show cns config connections `Device# show cns config connections`	CNS Cisco IOS CNS エージェントの接続のステータスを表示します。
show cns config outstanding `Device# show cns config outstanding`	開始されたがまだ終了していない差分（部分）CNS 設定に関する情報を表示します。
show cns config stats `Device# show cns config stats`	Cisco IOS CNS エージェントに関する統計情報を表示します。
show cns event connections `Device# show cns event connections`	CNS イベント エージェントの接続のステータスを表示します。
show cns event gateway `Device# show cns event gateway`	デバイスのイベント ゲートウェイ情報を表示します。

コマンド	目的
show cns event stats `Device# show cns event stats`	CNS イベント エージェントに関する統計情報を表示します。
show cns event subject `Device# show cns event subject`	アプリケーションによってサブスクライブされたイベント エージェントのサブジェクト一覧を表示します。

関連トピック

Cisco IOS CNS エージェントの部分的設定のイネーブル化 （1204 ページ）
差分（部分的）設定 （1191 ページ）
Cisco IOS CNS エージェントの初期設定のイネーブル化 （1197 ページ）
初期設定 （1190 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Configuration Engine のセットアップ	『*Cisco Configuration Engine Installation and Setup Guide, 1.5 for Linux*』 http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/1.5/installation_linux/guide/setup_1.html

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および **RFC**

標準/RFC	Title
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 69 章

Cisco Discovery Protocol の設定

- 機能情報の確認 （1209 ページ）
- CDP に関する情報 （1209 ページ）
- CDP の設定方法 （1210 ページ）
- CDP のモニタおよびメンテナンス （1217 ページ）
- その他の参考資料 （1219 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

CDP に関する情報

CDP の概要

CDP はすべてのシスコ デバイス（ルータ、ブリッジ、アクセス サーバ、コントローラ、およびスイッチ）のレイヤ 2（データリンク層）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスにネイバー シスコ デバイスを検出できます。また、下位レイヤのトランスペアレント プロトコルが稼働しているネイバーデバイスのデバイスタイプや、簡易ネットワーク管理プロトコル（SNMP）エージェントアドレスを学習することもできます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDP は、サブネットワーク アクセス プロトコル（SNAP）をサポートしているすべてのメディアで動作します。CDP はデータリンク層でのみ動作するため、異なるネットワーク層プロトコルをサポートする 2 つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャスト アドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。このアドバタイズには、受信側デバイスで CDP 情報を廃棄せずに保持する時間を表す存続可能時間、つまりホールドタイム情報も含まれます。各デバイスは他のデバイスから送信されたメッセージも待ち受けて、ネイバー デバイスについて学習します。

CDP はデバイス上で Network Assistant をイネーブルにすることで、ネットワークをグラフィカルに表示できます。デバイスは CDP を使用してクラスタ候補を検出し、クラスタ メンバ、およびコマンドデバイスから最大 3 台（デフォルト）離れたクラスタ対応の他のデバイスについての情報を維持します。

関連トピック

CDP 特性の設定 （1210 ページ）
CDP のモニタおよびメンテナンス （1217 ページ）

CDP のデフォルト設定

この表は、CDP のデフォルト設定を示します。

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP タイマー（パケット更新頻度）	60 秒
CDP ホールドタイム（廃棄までの時間）	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

関連トピック

CDP のイネーブル化 （1213 ページ）
CDP のディセーブル化 （1212 ページ）
インターフェイス上での CDP のイネーブル化 （1216 ページ）
インターフェイス上での CDP のディセーブル化 （1215 ページ）

CDP の設定方法

CDP 特性の設定

次の CDP 特性を設定できます。

- CDP 更新の頻度
- 破棄するまで情報を保持する時間の長さ
- バージョン 2 アドバタイズを送信するかどうか

（注） ステップ 3 ～ 5 はすべて任意であり、どの順番で実行してもかまいません。

CDP 特性を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cdp timer** *seconds* 例： `Device(config)# cdp timer 20`	（任意）CDP 更新の送信頻度を秒単位で設定します。 指定できる範囲は5～254 です。デフォルトは 60 秒です。
ステップ 4	**cdp holdtime** *seconds* 例： `Device(config)# cdp holdtime 60`	（任意）受信デバイスがこのデバイスから送信された情報を破棄せずに保持する時間を指定します。 指定できる範囲は 10 ～ 255 秒です。デフォルトは 180 秒です。
ステップ 5	**cdp advertise-v2** 例： `Device(config)# cdp advertise-v2`	（任意）バージョン2アドバタイズを送信するように CDP を設定します。 これは、デフォルトの状態です。
ステップ 6	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

デフォルト設定に戻すには、CDP コマンドの **no** 形式を使用します。

関連トピック

CDP の概要 （1209 ページ）
CDP のモニタおよびメンテナンス （1217 ページ）

CDP のディセーブル化

CDP はデフォルトで有効になっています。

（注） デバイス クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

CDP デバイス検出機能をディセーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no cdp run** 例： `Device(config)# no cdp run`	CDP をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

CDP を使用するには、再びイネーブルにする必要があります。

関連トピック

CDP のイネーブル化 （1213 ページ）
CDP のデフォルト設定 （1210 ページ）

CDP のイネーブル化

CDP はデフォルトで有効になっています。

（注） デバイス クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

ディセーブルになっている CDP をイネーブルにするには、次の手順を実行します。

始める前に

CDP をディセーブルにする必要があります。そのようにしないとイネーブルにできません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cdp run** 例： `Device(config)# cdp run`	ディセーブルになっている場合は、CDP をイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

CDP が有効になっていることを示すには、**showrunall** コマンドを使用します。**showrun** だけを入力した場合、CDP の有効化が表示されないことがあります。

関連トピック

CDP のデフォルト設定 （1210 ページ）
CDP のディセーブル化 （1212 ページ）

インターフェイス上での CDP のディセーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。

（注） デバイス クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

ポート上で CDP をディセーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	CDP をディセーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no cdp enable** 例： `Device(config-if)# no cdp enable`	ステップ 3 で指定したインターフェイスで CDP をディセーブルにします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

インターフェイス上での CDP のイネーブル化 （1216 ページ）
CDP のデフォルト設定 （1210 ページ）

インターフェイス上での CDP のイネーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。

（注） デバイス クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

ポート上でディセーブルになっている CDP をイネーブルにするには、次の手順を実行します。

始める前に

CDP をイネーブルにしようとしているポートで、CDP がディセーブルになっている必要があります。そうでない場合は、イネーブルにできません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	CDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cdp enable** 例： `Device(config-if)# cdp enable`	ディセーブルにされているインターフェイスで CDP をイネーブルにします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

CDP のデフォルト設定 （1210 ページ）
インターフェイス上での CDP のディセーブル化 （1215 ページ）

CDP のモニタおよびメンテナンス

表 *68 : CDP* 情報を表示するためのコマンド

コマンド	説明
clear cdp counters	トラフィック カウンタを 0 にリセットします。

コマンド	説明
clear cdp table	ネイバー デバイスに関する情報を収めた CDP テーブルを削除します。
show cdp	送信間隔、送信したパケットの保持時間などのグローバル情報を表示します。
show cdp entry *entry-name* ［**version**］［**protocol**］	特定のネイバーに関する情報を表示します。 アスタリスク（*）を入力してすべての CDP ネイバーを表示することも、情報が必要なネイバーの名前を入力することもできます。 また、指定されたネイバー上でイネーブルになっているプロトコルの情報や、デバイス上で稼働しているソフトウェアのバージョン情報が表示されるように、表示内容を制限することもできます。
show cdp interface［*interface-id*］	CDP がイネーブルに設定されているインターフェイスの情報を表示します。 必要なインターフェイスの情報だけを表示できます。
show cdp neighbors［*interface-id*］［*detail*］	装置タイプ、インターフェイス タイプ、インターフェイス番号、保持時間の設定値、機能、プラットフォーム、ポート ID を含めたネイバー情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show cdp traffic	CDP カウンタ（送受信されたパケット数およびチェックサムエラーを含む）を表示します。

関連トピック

CDP 特性の設定 （1210 ページ）
CDP の概要 （1209 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*Network Management Command Reference, Cisco IOS XE Release 3E*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

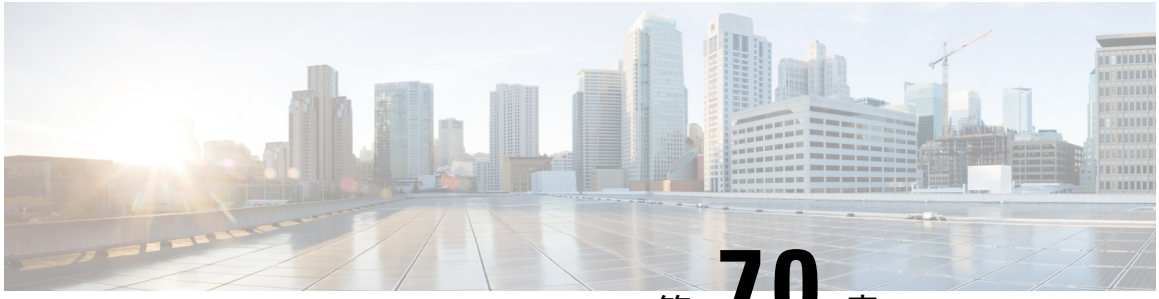
標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support



第 70 章

簡易ネットワーク管理プロトコルの設定

- 機能情報の確認 （1221 ページ）
- SNMP の前提条件 （1221 ページ）
- SNMP の制約事項 （1224 ページ）
- SNMP に関する情報 （1225 ページ）
- SNMP の設定方法 （1229 ページ）
- SNMP ステータスのモニタリング （1250 ページ）
- SNMP の例 （1251 ページ）
- その他の参考資料 （1252 ページ）
- 簡易ネットワーク管理プロトコルの機能の履歴と情報 （1253 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

SNMP の前提条件

サポートされている SNMP バージョン

このソフトウェア リリースは、次の SNMP バージョンをサポートしています。

- SNMPv1：RFC1157 に規定された SNMP（完全インターネット標準）。

- SNMPv2C は、SNMPv2Classic のバルク検索機能を残し、エラー処理を改善したうえで、SNMPv2Classic のパーティ ベースの管理およびセキュリティ フレームワークをコミュニティ ストリング ベースの管理フレームワークに置き換えたものです。次の機能があります。
  - SNMPv2：RFC 1902 ～ 1907 に規定された SNMP バージョン 2（ドラフト版インターネット標準）
  - SNMPv2C：RFC 1901 に規定された SNMPv2 のコミュニティ ストリング ベースの管理フレームワーク（試験版インターネット プロトコル）
- SNMPv3：SNMP のバージョン 3 は、RFC 2273 ～ 2275 に規定されている相互運用可能な標準ベースプロトコルです。SNMPv3 は、ネットワーク上のパケットを認証、暗号化することでデバイスへのアクセスに対するセキュリティを提供します。SNMPv3 は、次のセキュリティ機能を備えています。
  - メッセージの完全性：パケットが伝送中に改ざんされないようにします。
  - 認証：有効な送信元からのメッセージであるかどうかを判別します。
  - 暗号化：パッケージの内容をミキシングし、許可されていない送信元に内容が読まれることを防止します。

（注） 暗号化を選択するには、**priv** キーワードを入力します。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティが、IP アドレス アクセス コントロール リストおよびパスワードによって定義されます。

SNMPv2C にはバルク検索機能が組み込まれ、より詳細なエラー メッセージを管理ステーションに報告します。バルク検索機能は、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラー コードが使用されています。これらのエラーは、SNMPv1 では単一のエラー コードで報告されます。SNMPv2 では、エラー リターン コードでエラー タイプが報告されるようになりました。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ レベルとセキュリティ モデルの組み合わせにより、SNMP パケットを扱うときに使用するセキュリティ方式が決まります。使用可能なセキュリティ モデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

次の表では、この特性を識別し、セキュリティ モデルとセキュリティ レベルの異なる組み合わせを比較します。

表 *69 : SNMP* セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	未対応	コミュニティ ストリングの照合を使用して認証します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	未対応	コミュニティ ストリングの照合を使用して認証します。
SNMPv3	noAuthNoPriv	ユーザ名	未対応	ユーザ名の照合を使用して認証します。
SNMPv3	authNoPriv	Message Digest 5（MD5）または Secure Hash Algorithm（SHA）	未対応	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。

モデル	レベル	認証	暗号化	結果
SNMPv3	authPriv	MD5 または SHA	データ暗号規格（DES）または Advanced Encryption Standard（AES）	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。 次の暗号化アルゴリズムで、User-based Security Model（USM）を指定できます。 • CBC-DES（DES-56）規格に基づく認証に加えた DES 56 ビット暗号化 • 3DES 168 ビット暗号化 • AES 128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化

管理ステーションでサポートされている SNMP バージョンを使用するには、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、および SNMPv3 を使用する通信をサポートするようにソフトウェアを設定できます。

SNMP の制約事項

バージョンの制約事項

- SNMPv1 は informs をサポートしていません。

SNMP に関する情報

SNMP の概要

SNMP は、マネージャとエージェント間の通信のメッセージ フォーマットを提供するアプリケーションレイヤプロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および管理情報ベース（MIB）で構成されます。SNMP マネージャは、Cisco Prime Infrastructure などのネットワーク管理システム（NMS）に統合できます。エージェントおよび MIB は、デバイスに常駐します。デバイス上で SNMP を設定するには、マネージャとエージェント間の関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイスパラメータやネットワーク データの保存場所である MIB から値を収集します。また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、次の表に示す動作を実行します。

表 *70 : SNMP* の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。[3]
get-bulk-request[4]	テーブルの複数の行など、通常はサイズの小さい多数のデータ ブロックに分割して送信する必要がある巨大なデータ ブロックを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

[3] この動作を使用した場合、SNMP マネージャは厳密な変数名を知る必要はありません。テーブル内を順に検索して、必要な変数を検出します。

[4] get-bulk コマンドを使用できるのは、SNMPv2 以上に限られます。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニングツリー トポロジが変更された場合、認証に失敗した場合などがあります。

関連トピック

SNMP エージェントのディセーブル化 （1229 ページ）
SNMP ステータスのモニタリング （1250 ページ）

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。NMS が デバイス にアクセスするには、NMS 上のコミュニティ ストリング定義が デバイス 上の 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致しなければなりません。

コミュニティ ストリングの属性は、次のいずれかです。

- 読み取り専用（RO）：コミュニティ ストリングを除き MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りアクセス権を与えますが、書き込みアクセスは許可しません。
- 読み取り-書き込み（RW）：MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りおよび書き込みアクセス権を与えますが、コミュニティ ストリングへのアクセスは許可しません。
- クラスタを作成すると、コマンド デバイスがメンバ デバイスと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンド デバイス上で最初に設定された RW および RO コミュニティ ストリングにメンバ デバイス番号（@esN、N はデバイス番号）を追加し、これらのストリングをメンバ デバイスに伝播します。

関連トピック

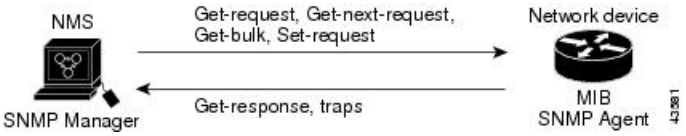
コミュニティ ストリングの設定 （1231 ページ）

SNMP MIB 変数アクセス

NMS の例として、Cisco Prime Infrastructure ネットワーク管理ソフトウェアがあります。Cisco Prime Infrastructure 2.0 ソフトウェアは、デバイス MIB 変数を使用して装置変数を設定し、ネットワーク上の装置をポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

次の図に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対し、トラップ（特定イベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス トラッキングなどの状況を SNMP マネージャに通知します。SNMP エージェントはさらに、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送信される MIB 関連のクエリに応答します。

図 *79 : SNMP* ネットワーク



SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、デバイスから SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、トラップまたは情報を選択するオプションがコマンドにない限り、キーワード traps はトラップ、情報、またはその両方を表します。**snmp-server host** コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

（注） SNMPv1 は informs をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうかが送信側にわからないからです。情報要求の場合、受信した SNMP マネージャは SNMP 応答プロトコル データ ユニット（PDU）でメッセージを確認します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。再送信できるので、情報の方がトラップより意図した宛先に届く可能性が高くなります。

情報の方がトラップより信頼性が高いのは、デバイスおよびネットワークのリソースを多く消費するという特性にも理由があります。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は 1 回限りですが、情報は数回にわたって再送信つまり再試行が可能です。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因に

もなります。したがって、トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。SNMP マネージャですべての通知を受信することが重要な場合は、情報要求を使用してください。ネットワークまたはデバイスのメモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

関連トピック

SNMP 通知の設定 （1237 ページ）
SNMP ステータスのモニタリング （1250 ページ）

SNMP ifIndex MIB オブジェクト値

SNMP エージェントの IF-MIB モジュールがリブート後すぐに起動されます。さまざまな物理インターフェイス ドライバが IF-MIB モジュールの登録を初期化されているように、「インデックス番号をください」と示します。IF-MIB モジュールが先着順で使用可能な次の ifIndex 番号を割り当てます。つまり、1 つのリブートから他のリブートへのドライバの初期化順序のマイナーな違いが、同じ物理インターフェイスにリブートを行う以前のものとは別のインデックス番号を取得する可能性があるということです（インデックス持続が有効化されていない限り）。

SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル[5]
SNMP トラップ レシーバ	未設定
SNMP トラップ	TCP 接続のトラップ（tty）以外は、イネーブルではありません。
SNMP バージョン	バージョン キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで **noauth**（noAuthNoPriv）になります。
SNMP 通知タイプ	タイプが指定されていない場合、すべての通知が送信されます。

[5] これは、デバイスが起動し、スタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが設定されていない場合のデフォルトです。

SNMP 設定時の注意事項

デバイスが起動し、デバイスのスタートアップ コンフィギュレーションに少なくとも 1 つの **snmp-server** グローバル コンフィギュレーション コマンドが設定されている場合、SNMP エージェントはイネーブルになります。

SNMP グループは、SNMP ユーザを SNMP ビューに対応付けるテーブルです。SNMP ユーザは、SNMP グループのメンバです。SNMP ホストは、SNMP トラップ動作の受信側です。SNMP エンジン *ID* は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP グループを設定するときには、次の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しません。**snmp-server host** グローバル コンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザを対応するグループに追加します。グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。
- リモートユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応する IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモート ユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドを **remote** オプションとともに使用して、SNMP エンジン ID を設定してください。リモート エージェントの SNMP エンジン ID およびユーザ パスワードを使用して認証およびプライバシーダイジェストが算出されます。先にリモート エンジン ID を設定しておかないと、コンフィギュレーション コマンドがエラーになります。
- SNMP 情報を設定するときには、プロキシ要求または情報の送信先となるリモート エージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。
- ローカル ユーザがリモート ホストと関連付けられていない場合、デバイスは **auth**（authNoPriv）および **priv**（authPriv）の認証レベルの情報を送信しません。
- SNMP エンジン ID の値を変更すると、重大な影響が生じます。（コマンド ラインで入力された）ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて、MD5 または SHA セキュリティ ダイジェストに変換されます。コマンドラインのパスワードは、RFC 2274 の規定に従って廃棄されます。このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合は SNMPv3 ユーザのセキュリティ ダイジェストが無効となり、**snmp-server user** *username* グローバル コンフィギュレーション コマンドを使用して、SNMP ユーザを再設定する必要があります。エンジン ID を変更した場合は、同様の制限によってコミュニティ ストリングも再設定する必要があります。

関連トピック

SNMP グループおよびユーザの設定 （1234 ページ）
SNMP ステータスのモニタリング （1250 ページ）

SNMP の設定方法

SNMP エージェントのディセーブル化

no snmp-server グローバル コンフィギュレーション コマンドは、デバイス上で実行している SNMP エージェントのすべてのバージョン（バージョン 1、バージョン 2C、バージョン 3）を

ディセーブルにします。入力した最初の **snmp-server** グローバル コンフィギュレーション コマンドによって、SNMPエージェントのすべてのバージョンを再度イネーブルにします。特にSNMP をイネーブルにするために指定された Cisco IOS コマンドはありません。

SNMP エージェントをディセーブルにするには、次の手順を実行します。

始める前に

SNMPエージェントをディセーブルにする前にイネーブルにする必要があります。デバイス上で入力した最初の **snmp-server** グローバル コンフィギュレーション コマンドによって SNMP エージェントがイネーブルになります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no snmp-server** 例： `Device(config)# no snmp-server`	SNMPエージェント動作をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

関連トピック

SNMP エージェント機能 （1226 ページ）
SNMP ステータスのモニタリング （1250 ページ）

コミュニティ ストリングの設定

SNMPマネージャとエージェントの関係を定義するには、SNMPコミュニティストリングを使用します。コミュニティストリングは、デバイス上のエージェントへのアクセスを許可する、パスワードと同様の役割を果たします。ストリングに対応する次の特性を1つまたは複数指定することもできます。

- コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限

デバイス上でコミュニティ ストリングを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*access-list-number*]	コミュニティ ストリングを設定します。

	コマンドまたはアクション	目的
	例： `Device(config)# snmp-server community comaccess ro 4`	（注） コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。 • *string* には、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。任意の長さのコミュニティ ストリングを 1 つまたは複数設定できます。 • （任意）**view** には、コミュニティがアクセスできるビュー レコードを指定します。 • （任意）許可された管理ステーションで MIB オブジェクトを取得する場合は読み取り専用（**ro**）、許可された管理ステーションで MIB オブジェクトを取得および変更する場合は読み書き（**rw**）を指定します。デフォルトでは、コミュニティ ストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 • （任意）*access-list-number* には、1 ～ 99 および 1300 ～ 1999 の標準 IP アクセスリスト番号を入力します。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 4 deny any`	（任意）ステップ 3 で標準 IP アクセスリスト番号を指定してリストを作成した場合は、必要に応じてコマンドを繰り返します。 • *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。

	コマンドまたはアクション	目的
		• *source* には、コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します（コミュニティ ストリングに値を入力しないでください）。

特定のコミュニティ ストリングを削除するには、**no snmp-server** コミュニティ ストリング グローバル コンフィギュレーション コマンドを使用します。

デバイスのローカルまたはリモート SNMP サーバ エンジンを表す識別名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

関連トピック

SNMP コミュニティ ストリング （1226 ページ）

SNMP グループおよびユーザの設定

デバイスのローカルまたはリモート SNMP サーバ エンジンを表す識別名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

デバイス上の SNMP グループとユーザを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server engineID** { **local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string* } 例： `Device(config)# snmp-server engineID local 1234`	SNMP のローカル コピーまたはリモート コピーに名前を設定します。 • *engineid-string* は、SNMP のコピー名を指定する 24 文字の ID ストリングです。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。手順例では、123400000000000000000000 のエンジン ID を設定します。 • **remote**を指定した場合、SNMP のリモート コピーが置かれているデバイスの *ip-address* を指定し、任意でリモート デバイスのユーザ データグラム プロトコル（UDP）ポートを指定します。デフォルトは 162 です。

	コマンドまたはアクション	目的
ステップ 4	**snmp-server group** *group-name readview writeview notifyview access* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read**] [**write**] [**notify**] [**access**] 例： `Device(config)# snmp-server group public v2c access lmnop`	リモート デバイス上で新しい SNMP グループを設定します。 *group-name* には、グループの名前を指定します。 次のいずれかのセキュリティ モデルを指定します。 • **v1** は、最も安全性の低いセキュリティ モデルです。 • **v2c** は、2 番目に安全性の低いセキュリティ モデルです。標準の 2 倍の幅で情報および整数を伝送できます。 • **v3**最も安全な場合には、次の認証レベルの 1 つを選択する必要があります。 **auth**：Message Digest 5（MD5） およびセキュア ハッシュ アルゴリズム（SHA）によるパケット認証を可能にします。 **noauth**：noAuthNoPriv セキュリティ レベルを可能にします。キーワードを指定しなかった場合、これがデフォルトです。 **priv**：データ暗号規格（DES）によるパケット暗号化（プライバシーともいう）を可能にします。 （任意）**read** *readview* とともに、エージェントの内容を表示できるビューの名前を表すストリング（64 文字以下）を入力します。 （任意）**write** *writeview* とともに、データを入力し、エージェントの内容を設定できるビューの名前を表すストリング（64 文字以下）を入力します。 （任意）**notify** *notifyview* とともに、通知、情報、またはトラップを指定するビューの名前を表すストリング（64 文字以下）を入力します。

	コマンドまたはアクション	目的
		（任意）**access** *access-list* とともに、アクセス リスト名のストリング（64 文字以下）を入力します。
ステップ 5	**snmp-server user** *username group-name host port access-list access-list access-list auth-passwordpriv* [illegible] 例： `Device(config)#  snmp-server user Pat public v2c`	SNMP グループに対して新規ユーザを追加します。 *username* は、エージェントに接続するホスト上のユーザ名です。 *group-name* は、ユーザが関連付けられているグループの名前です。 **remote** を入力して、ユーザが所属するリモート SNMP エンティティおよびそのエンティティのホスト名または IP アドレスとともに、任意で UDP ポート番号を指定します。デフォルトは 162 です。 SNMP バージョン番号（**v1**、**v2c**、または **v3**）を入力します。**v3** を入力すると、次のオプションが追加されます。 • **encrypted** パスワードを暗号化形式で表示するように指定します。このキーワードは、**v3** キーワードが指定されている場合のみ使用可能です。 • **auth** では、認証レベルを設定します。HMAC-MD5-96（**md5**）または HMAC-SHA-96（**sha**）認証レベルのいずれかを指定できます。また、*auth-password* でパスワードの文字列を指定する必要があります（最大 64 文字）。 **v3** を入力すると、次のキーワードを使用して（64 文字以下）、プライベート（**priv**）暗号化アルゴリズムおよびパスワード ストリング *priv-password* を設定することもできます。 • **priv** ユーザベース セキュリティ モデル（USM）を指定します。

	コマンドまたはアクション	目的
		• **des** 56 ビット DES アルゴリズムを使用する場合に指定します。 • **3des** 168 ビット DES アルゴリズムを使用する場合に指定します。 • **aes** DES アルゴリズムを使用する場合に指定します。128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化のいずれかを選択する必要があります。 （任意）**access** *access-list* とともに、アクセス リスト名のストリング（64 文字以下）を入力します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

SNMP 設定時の注意事項 （1228 ページ）
SNMP ステータスのモニタリング （1250 ページ）

SNMP 通知の設定

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生したときにデバイスが生成するシステム アラートです。デフォルトでは、トラップ マネージャは定義されず、トラップは送信されません。この Cisco IOS Release が稼働しているデバイスでは、トラップ マネージャを無制限に設定できます。

（注） コマンド構文で **traps** というワードを使用するコマンドは多数あります。トラップまたは情報を選択するオプションがコマンドにない限り、キーワード **traps** はトラップ、情報のいずれか、またはその両方を表します。**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

snmp-server enable traps グローバル コンフィギュレーション コマンドを **snmp-server host** グローバル コンフィギュレーション コマンドと組み合わせて使用すると、次の表に示す通知タイプを特定のホストで受信できます。これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定できます。

（注） **snmp-server enable traps** コマンドは、デバイスのローカル認証のためのトラップをサポートしていません。

表 *71 :* デバイスの通知タイプ

通知タイプのキーワード	説明
bridge	STP ブリッジ MIB トラップを生成します。
cluster	クラスタ設定が変更された場合に、トラップを生成します。
config	SNMP 設定が変更された場合に、トラップを生成します。
copy-config	SNMP コピー設定が変更された場合に、トラップを生成します。
cpu threshold	CPU に関連したトラップをイネーブルにします。
entity	SNMP エンティティが変更された場合に、トラップを生成します。
envmon	環境モニタ トラップを生成します。ファン（fan）、シャットダウン（shutdown）、ステータス（status）、電源（supply）、温度（temperature）の環境トラップのいずれかまたはすべてをイネーブルにできます。
flash	SNMP FLASH 通知を生成します。デバイス スタックでは、オプションとして、フラッシュの追加または削除に関する通知を有効にできます。このようにすると、スタックからデバイスを削除するか、またはスタックにスイッチを追加した場合に（物理的な取り外し、電源の再投入、またはリロードの場合に）、トラップが発行されます。

通知タイプのキーワード	説明
fru-ctrl	エンティティ現場交換可能ユニット（FRU）制御トラップを生成します。デバイス スタックでは、このトラップはスタックにおけるデバイスの挿入/取り外しを意味します。
hsrp	ホットスタンバイ ルータ プロトコル（HSRP）が変更された場合に、トラップを生成します。
ipmulticast	IP マルチキャスト ルーティングが変更された場合に、トラップを生成します。
mac-notification	MAC アドレス通知のトラップを生成します。
ospf	Open Shortest Path First（OSPF）が変更された場合に、トラップを生成します。シスコ固有、エラー、リンクステートアドバタイズ、レート制限、再送信、ステート変更に関するトラップを任意にイネーブルにできます。
pim	Protocol-Independent Multicast（PIM）が変更された場合に、トラップを生成します。無効な PIM メッセージ、ネイバー変更、およびランデブー ポイント（RP）マッピングの変更に関するトラップを任意にイネーブルにできます。
port-security	SNMP ポート セキュリティ トラップを生成します。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。 （注） 通知タイプ **port-security** を使用してトラップを設定する際に、まずポート セキュリティ トラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。 **1. snmp-server enable trapsport-security** **2. snmp-server enable trapsport-securitytrap-rate** *rate*
snmp	認証、コールドスタート、ウォームスタート、リンクアップ、またはリンク ダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 1000 です。デフォルトは 0 に設定されています（制限なしの状態では、発生ごとにトラップが送信されます）。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP の Syslog トラップを生成します。

通知タイプのキーワード	説明
tty	TCP 接続のトラップを生成します。このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバーシップが変更された場合に、トラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN トランキングプロトコル（VTP）が変更された場合に、トラップを生成します。

ホストにトラップまたは情報を送信するようにデバイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server engineID remote** *ip-address engineid-string* 例： `Device(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b`	リモート ホストのエンジン ID を指定します。
ステップ 4	**snmp-server user** *username group-name host port access-list access-list access-list* [udp-port port] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth password]} 例：	SNMP ユーザを設定し、ステップ 3 で作成したリモートホストに関連付けます。

	コマンドまたはアクション	目的
	`Device(config)# snmp-server user Pat public v2c`	（注） アドレスに対応するリモートユーザを設定するには、先にリモート ホストのエンジン ID を設定しておく必要があります。このようにしないと、エラーメッセージが表示され、コマンドが実行されません。
ステップ 5	**snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*] 例： `Device(config)# snmp-server group public v2c access lmnop`	SNMP グループを設定します。
ステップ 6	**snmp-server host** *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [*notification-type*] 例： `Device(config)# snmp-server host 203.0.113.1 comaccess snmp`	SNMP トラップ動作の受信先を指定します。 *host-addr* には、ホスト（対象となる受信側）の名前またはインターネットアドレスを指定します。 （任意）SNMP トラップをホストに送信するには、**traps**（デフォルト）を指定します。 （任意）SNMP 情報をホストに送信するには、**informs** を指定します。 （任意）SNMP **version**（**1**、**2c**、または **3**）を指定します。SNMPv1 は informs をサポートしていません。 （任意）バージョン 3 の場合、認証レベル **auth**、**noauth**、または **priv** を選択します。 （注） **priv** キーワードは、暗号化ソフトウェアイメージがインストールされている場合のみ使用可能です。 *community-string* には、**version 1** または **version 2c** が指定されている場合、通知動作で送信される、パスワードに類似したコミュニティ ストリングを入力し

	コマンドまたはアクション	目的
		ます。**version 3** が指定されている場合、SNMPv3 ユーザ名を入力します。 コンテキスト情報を区切るには@記号を使用します。このコマンドの設定時にSNMPコミュニティストリングの一部として@記号を使用しないでください。 （任意）*notification-type* には、上の表に記載されているキーワードを使用します。タイプが指定されていない場合、すべての通知が送信されます。 （注） SNMP バージョン 3 の場合には、SNMPv3 ユーザを SNMPv3 ホスト設定の前に設定する必要があります。そうしないと、SNMP トラップは送信されません。
ステップ **7**	**snmp-server enable traps** *notification-types* 例： `Device(config)# snmp-server enable traps snmp`	デバイスでのトラップまたはインフォームの送信を有効にし、送信する通知の種類を指定します。通知タイプの一覧については、上の表を参照するか、次のコマンドを入力してください。 **snmp-server enable traps?** 複数のトラップタイプを有効にするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。 （注） 通知タイプ **port-security** を使用してトラップを設定する際に、まずポートセキュリティトラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。 **1. snmp-server enable trapsport-security** **2. snmp-server enable trapsport-securitytrap-rate** *rate*

	コマンドまたはアクション	目的
ステップ 8	**snmp-server trap-source** *interface-id* 例： `Device(config)# snmp-server trap-source GigabitEthernet1/0/1`	（任意）送信元インターフェイスを指定します。このインターフェイスによってトラップ メッセージの IP アドレスが提供されます。情報の送信元 IP アドレスも、このコマンドで設定します。
ステップ 9	**snmp-server queue-length** *length* 例： `Device(config)# snmp-server queue-length 20`	（任意）各トラップホストのメッセージキューの長さを指定します。指定できる範囲は 1 ～ 1000 です。デフォルトは 10 です。
ステップ 10	**snmp-server trap-timeout** *seconds* 例： `Device(config)# snmp-server trap-timeout 60`	（任意）トラップメッセージを再送信する頻度を指定します。指定できる範囲は 1 ～ 1000 です。デフォルトは 30 秒です。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 13	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次のタスク

snmp-server host コマンドでは、通知を受信するホストを指定します。**snmp-server enable traps** コマンドによって、指定された通知方式（トラップおよび情報）がグローバルで有効になります。ホストが情報を受信できるようにするには、そのホストに対応する **snmp-server host informs** コマンドを設定し**snmp-server enable traps** コマンドを使用して情報をグローバルに有効にする必要があります。

指定したホストがトラップを受信しないようにするには、**no snmp-server host** *host* グローバルコンフィギュレーション コマンドを使用します。キーワードを指定しないで **no snmp-server**

host コマンドを使用すると、ホストへのトラップは無効になりますが、情報は無効になりません。情報を無効にするには、**no snmp-server host informs** グローバル コンフィギュレーション コマンドを使用してください。特定のトラップ タイプを無効にするには、**no snmp-server enable traps** *notification-types* グローバル コンフィギュレーション コマンドを使用します。

関連トピック

SNMP 通知 （1227 ページ）
SNMP ステータスのモニタリング （1250 ページ）

エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム接点およびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server contact** *text* 例： `Device(config)# snmp-server contact Dial System Operator at beeper 21555`	システムの連絡先文字列を設定します。
ステップ 4	**snmp-server location** *text* 例： `Device(config)# snmp-server location Building 3/Room 222`	システムの場所を表す文字列を設定します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP を通して使用する TFTP サーバの制限

SNMP を介したコンフィギュレーション ファイルの保存とロードに使用する TFTP サーバを、アクセス リストで指定されたサーバに限定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server tftp-server-list** *access-list-number* 例： `Device(config)# snmp-server tftp-server-list 44`	SNMP を介したコンフィギュレーション ファイルのコピーに使用する TFTP サーバを、アクセス リストのサーバに限定します。 *access-list-number* には、1 ～ 99 および 1300 ～ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 4	**access-list** *access-list-number sourcesource-wildcard* { **deny** | **permit** } [ ] 例：	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。

	コマンドまたはアクション	目的
	`Device(config)# access-list 44 permit 10.1.1.2`	*access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 *source* には、デバイスにアクセスできる TFTP サーバの IP アドレスを入力します。 （任意）*source-wildcard* には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP のトラップフラグの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**trapflags ap** { **interfaceup** | **register**} 例： `Device(config)# trapflags ap interfaceup`	AP 関連トラップの送信をイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの**no** 形式を使用します。 • **interfaceup**：Cisco AP インターフェイス（A または B）が起動したときにトラップをイネーブルにします。 • **register**：Cisco AP が Cisco デバイス に登録するときにトラップをイネーブルにします。
ステップ 3	**trapflags client** {**dot11** | **excluded**} 例： `Device(config)# trapflags client excluded`	クライアント関連 DOT11 トラップの送信をイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの**no** 形式を使用します。 • **dot11**：クライアントの DOT11 トラップをイネーブルにします。 • **excluded**：クライアント用の除外されたトラップをイネーブルにします。
ステップ 4	**trapflags dot11-security** {**ids-sig-attack** | **wep-decrypt-error**} 例： `Device(config)# trapflags dot11-security wep-decrypt-error`	802.11 セキュリティ関連トラップの送信をイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの**no** 形式を使用します。 • **ids-sig-attack**：IDS シグニチャ攻撃トラップをイネーブルにします。 • **wep-decrypt-error**：クライアントの WEP 復号化エラーのトラップをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**trapflags mesh** 例： `Device(config)# trapflags mesh`	メッシュのトラップをイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの**no** 形式を使用します。
ステップ 6	**trapflags rogueap** 例： `Device(config)# trapflags rogueap`	不正 AP 検出のトラップをイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの**no** 形式を使用します。
ステップ 7	**trapflags rrm-params** {**channels** | **tx-power**} 例： `Device(config)# trapflags rrm-params tx-power`	RRM-parameter 更新関連トラップの送信をイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの**no** 形式を使用します。 • **channels**：RF マネージャが自動的に Cisco AP インターフェイスのチャネル番号を変更するときにトラップをイネーブルにします。 • **tx-power**：RF マネージャが自動的に Cisco AP インターフェイスの Tx-Power レベルを変更するときにトラップをイネーブルにします。
ステップ 8	**trapflags rrm-profile** {**coverage** | **interference** | **load** | **noise**} 例： `Device(config)# trapflags rrm-profile interference`	RRM-Profile 関連トラップの送信をイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの**no** 形式を使用します。 • **coverage**：RF マネージャによって保持されるカバレッジ プロファイルでエラーが発生したときにトラップをイネーブルにします。 • **interference**：RF マネージャによって保持される干渉プロファイルでエラーが発生したときにトラップをイネーブルにします。 • **load**：RF マネージャによって保持される負荷プロファイルでエラーが発生したときにトラップをイネーブルにします。 • **noise**：RF マネージャによって保持されるノイズプロファイルでエラー

	コマンドまたはアクション	目的
		が発生したときにトラップをイネーブルにします。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

SNMP ワイヤレス トラップ通知のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server enable traps wireless** ［**AP** | **RRM** | **bsn80211SecurityTrap** | **bsnAPParamUpdate** | **bsnAPProfile** | **bsnAccessPoint** | **bsnMobileStation** | **bsnRogue** | **client** | **mfp** | **rogue**］ 例： `Device(config)# snmp-server enable traps wireless AP`	SNMP ワイヤレス トラップ通知をイネーブルにします。 • **AP**：アクセス ポイント トラップをイネーブルにします。 • **RRM**：RRM トラップをイネーブルにします。 • **bsn80211SecurityTrap**：セキュリティ関連のトラップをイネーブルにします。 • **bsnAPParamUpdate**：更新される AP パラメータのトラップをイネーブルにします。 • **bsnAPProfile**：BSN AP プロファイル トラップをイネーブルにします。 • **bsnAccessPoint**：BSN アクセス ポイント トラップをイネーブルにします。 • **bsnMobileStation**：ワイヤレス クライアント トラップを制御します。

	コマンドまたはアクション	目的
		• **bsnRogue**：BSN 不正関連トラップをイネーブルにします。 • **client**：クライアント トラップをイネーブルにします。 • **mfp**：MFP トラップをイネーブルにします。 • **rogue**：不正関連トラップをイネーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

SNMP ステータスのモニタリング

不正なコミュニティ ストリング エントリ、エラー、要求変数の数など、SNMP の入出力統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。また、次の表にリストされたその他の特権 EXEC コマンドを使用して、SNMP 情報を表示することもできます。

表 *72 : SNMP* 情報を表示するためのコマンド

コマンド	目的
show snmp	SNMP 統計情報を表示します。
show snmp engineID	デバイスに設定されているローカル SNMP エンジンおよびすべてのリモート エンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求の情報を表示します。
show snmp sessions	現在のSNMPセッションの情報を表示します。

コマンド	目的
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。 （注） このコマンドは、**auth** | **noauth** | **priv** モードの SNMPv3 設定情報を表示するときに使用する必要があります。この情報は、**show running-config** の出力には表示されません。

関連トピック

SNMP エージェントのディセーブル化 （1229 ページ）
SNMP エージェント機能 （1226 ページ）
SNMP グループおよびユーザの設定 （1234 ページ）
SNMP 設定時の注意事項 （1228 ページ）
SNMP 通知の設定 （1237 ページ）
SNMP 通知 （1227 ページ）

SNMP の例

次に、SNMP のすべてのバージョンをイネーブルにする例を示します。この設定では、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定では、デバイス はトラップを送信しません。

```
Device(config)# snmp-server community public
```

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。デバイスはさらに、SNMPv1 を使用してホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に VTP トラップを送信します。コミュニティ ストリング *public* は、トラップとともに送信されます。

```
Device(config)# snmp-server community public
Device(config)# snmp-server enable traps vtp
Device(config)# snmp-server host 192.180.1.27 version 2c public
Device(config)# snmp-server host 192.180.1.111 version 1 public
Device(config)# snmp-server host 192.180.1.33 public
```

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証障害トラップは、SNMPv2C がコミュニティ ストリング *public* を使用してホスト *cisco.com* に送信します。

```
Device(config)# snmp-server community comaccess ro 4
Device(config)# snmp-server enable traps snmp authentication
Device(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは制限されます。1 行めで、デバイス はすでにイネーブルになっているトラップ以

外に、エンティティ MIB トラップを送信できるようになります。2行目はこれらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の **snmp-server** ホスト コマンドを無効にします。

```
Device(config)# snmp-server enable traps entity
Device(config)# snmp-server host cisco.com restricted entity
```

次に、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにデバイスをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com public
```

次に、ユーザとリモート ホストを関連付けて、ユーザがグローバル コンフィギュレーション モードのときに **auth**（authNoPriv）認証レベルで情報を送信する例を示します。

```
Device(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Device(config)# snmp-server group authgroup v3 auth
Device(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Device(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Device(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Device(config)# snmp-server enable traps
Device(config)# snmp-server inform retries 0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
SNMP コマンド	『*Network Management Command Reference, Cisco IOS XE Release 3E*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
なし	-

MIB

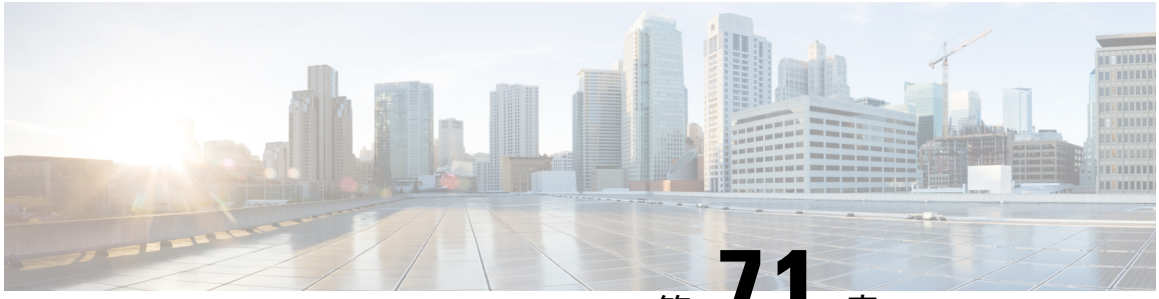
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

簡易ネットワーク管理プロトコルの機能の履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。



第 71 章

サービス レベル契約の設定

この章では、スイッチで Cisco IOS IP サービス レベル契約（SLA）を使用する方法について説明します。

特に明記しないかぎり、スイッチという用語はスタンドアロンスイッチまたはスイッチスタックを意味します。

- 機能情報の確認 （1255 ページ）
- SLA の制約事項 （1255 ページ）
- SLA について （1256 ページ）
- IP SLA 動作の設定方法 （1262 ページ）
- IP SLA 動作のモニタリング （1276 ページ）
- IP SLA 動作のモニタリングの例 （1277 ページ）
- その他の参考資料 （1278 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

SLA の制約事項

ここでは、SLA の制約事項を示します。

次に示すのは、IP SLA ネットワーク パフォーマンス測定の制約事項です。

- デバイスは、ゲートキーパー登録遅延動作測定を使用した Voice over IP（VoIP）サービスレベルはサポートしていません。
- Cisco IOS デバイスだけが宛先 IP SLA Responder の送信元になります。
- 他社製のデバイスに IP SLA Responder を設定することはできません。また、Cisco IOS IP SLA はこれらのデバイス固有のサービスに対してだけ動作パケットを送信できます。

関連トピック

IP SLA ネットワーク パフォーマンス測定の実装 （1264 ページ）
Cisco IOS IP SLA でのネットワーク パフォーマンスの測定 （1257 ページ）
IP SLA レスポンダおよび IP SLA 制御プロトコル （1258 ページ）

SLA について

Cisco IOS IP サービス レベル契約（SLA）

Cisco IOS IP SLA はネットワークにデータを送信し、複数のネットワーク ロケーション間あるいは複数のネットワーク パス内のパフォーマンスを測定します。Cisco IOS IP SLA は、ネットワーク データおよび IP サービスをシミュレーションし、ネットワーク パフォーマンス情報をリアル タイムで収集します。Cisco IOS IP SLA は、Cisco IOS デバイス間のトラフィックまたは Cisco IOS デバイスからネットワーク アプリケーション サーバのようなリモート IP デバイスへのトラフィックを生成し、分析します。さまざまな Cisco IOS IP SLA 動作で評価を実行し、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用します。

Cisco IOS IP SLA 動作に応じてシスコ デバイスのネットワーク パフォーマンス統計情報がモニタリングされ、コマンドラインインターフェイス（CLI）MIB および簡易ネットワーク管理プロトコル（SNMP）MIB に格納されます。IP SLA パケットには設定可能な IP レイヤおよびアプリケーション層のオプションがあります。たとえば、発信元および宛先 IP アドレス、ユーザ データグラム プロトコル（UDP）/TCP ポート番号、タイプ オブ サービス（ToS）バイト（DiffServ コード ポイント（DSCP）および IP プレフィックス ビットを含む）、VPN ルーティング/転送インスタンス（VRF）、URL Web アドレスなどが設定できます。

Cisco IP SLA はレイヤ 2 転送に依存していないので、異なるネットワーク間にエンドツーエンド動作を設定してエンドユーザが経験しそうなメトリックを最大限に反映させることができます。IP SLA は、次のパフォーマンス メトリックを収集して分析します。

- 遅延（往復および一方向）
- ジッタ（方向性あり）
- パケット損失（方向性あり）
- パケット シーケンス（パケット順序）
- パス（ホップ単位）
- 接続（方向性あり）

- サーバまたは Web サイトのダウンロード時間

Cisco IP SLA は SNMP によるアクセスが可能なので、Cisco Prime Internetwork Performance Monitor（IPM）やサードパーティ製パフォーマンス管理製品などのパフォーマンス モニタリング アプリケーションでも使用できます。

IP SLA を使用すると、次の利点が得られます。

- SLA モニタリング、評価、検証。
- ネットワーク パフォーマンス モニタリング。
  - ネットワークのジッター、遅延、パケット損失の測定。
  - 連続的で信頼性のある予測可能な測定。
- IP サービス ネットワーク ヘルス アセスメントにより、既存の QoS が新しい IP サービスに適していることを確認できる。
- 端末間のネットワーク アベイラビリティをモニタリングして、ネットワーク リソースをあらかじめ検証し接続をテストできる（たとえば、ビジネス上の重要なデータを保存する NFS サーバのネットワーク アベイラビリティをリモート サイトから確認できる）。
- 問題をすぐに認識し、トラブルシューティングにかかる時間を短縮できる一貫性のある信頼性の高い測定によるネットワーク動作のトラブルシューティング。
- マルチプロトコル ラベル スイッチング（MPLS）パフォーマンス モニタリングとネットワークの検証を行う（デバイスが MPLS をサポートする場合）。

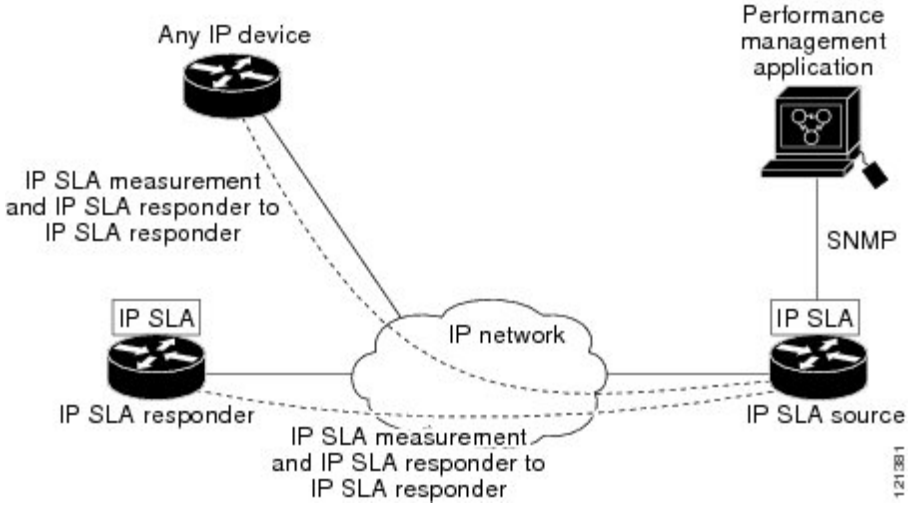
Cisco IOS IP SLA でのネットワーク パフォーマンスの測定

IP SLA を使用して、プローブを物理的に配置せずに、コア、分散、エッジといったネットワーク内の任意のエリア間のパフォーマンスをモニタリングすることができます。2 つのネットワーク デバイス間のネットワーク パフォーマンスは、生成トラフィックで測定します。

図 *80 : Cisco IOS IP SLA* 動作

次の図に、送信元デバイスが宛先デバイスに生成パケットを送信するときに IP SLA が開始される手順を示します。宛先デバイスがパケットを受信すると、IP SLA 動作の種類によって、送信元のタイム スタンプ情報に応じてパフォーマンス メトリックを算出します。IP SLA 動作

は、特定のプロトコル（UDP など）を使用してネットワークの送信元から宛先へのネットワーク測定を行います。



関連トピック

IP SLA ネットワーク パフォーマンス測定の実装 （1264 ページ）
SLA の制約事項 （1255 ページ）

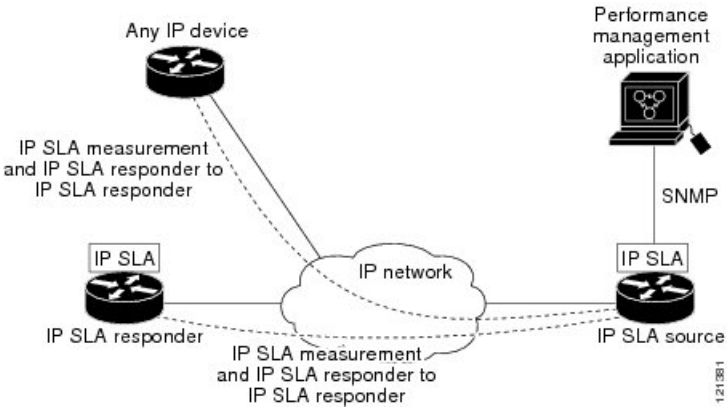
IP SLA レスポンダおよび IP SLA 制御プロトコル

IP SLA レスポンダは宛先 Cisco デバイスに組み込まれたコンポーネントで、システムが IP SLA 要求パケットを予想して応答します。Responderは専用プローブなしで正確な測定を行います。レスポンダは、受信および応答するポートが通知されるメカニズムを Cisco IOS IP SLA コントロール プロトコルを通じて実現します。

（注） IP SLA レスポンダはレスポンダ設定可能なデバイスである Cisco IOS レイヤ 2 にすることもできます。レスポンダは、IP SLA 機能を全面的にサポートする必要はありません。

次の図は、IP ネットワーク内での Cisco IOS IP SLA レスポンダの配置場所を示します。レスポンダは、IP SLA 動作から送信されたコントロール プロトコル メッセージを指定されたポートで受信します。コントロール メッセージを受信したら、指定された UDP または TCP ポートを指定された時間だけイネーブルにします。この間に、レスポンダは要求を受け付け、応答します。レスポンダは、IP SLA パケットに応答した後または指定の時間が経過したら ポートを無効にします。セキュリティの向上のために、コントロール メッセージでは MD5 認証が利用できます。

図 *81 : Cisco IOS IP SLA* 動作



すべての IP SLA 動作に対して宛先デバイスのレスポンダを有効にする必要はありません。たとえば、宛先ルータが提供しているサービス（Telnet や HTTP など）は Responder では必要ありません。

関連トピック

SLA の制約事項 （1255 ページ）

IP SLA の応答時間の計算

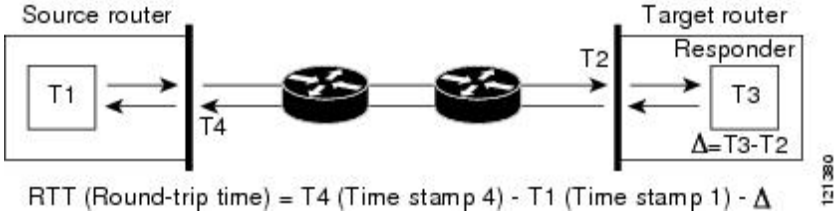
スイッチ、コントローラ、ルータは、他の高優先度プロセスがあるために、着信パケットの処理に数十ミリ秒かかることがあります。この遅延により応答時間が影響を受けます。テストパケットの応答が処理待ちのキューに入っていることもあるからです。この場合、応答時間は正しいネットワーク遅延を反映しません。IP SLA はソース デバイスとターゲット デバイス（レスポンダが使用されている場合）の処理遅延を最小化し、正しいラウンドトリップ時間（RTT）を識別します。IP SLA テスト パケットは、タイム スタンプによって処理遅延を最小化します。

IP SLA レスポンダが有効の場合、パケットが割り込みレベルでインターフェイスに着信したときおよびパケットが出て行くときにターゲット デバイスでタイム スタンプを付け、処理時間は含めません。タイム スタンプはサブミリ秒単位で構成されます。

図 *82 : Cisco IOS IP SLA* レスポンダ タイム スタンプ

次の図は、レスポンダの動作を示します。RTT を算出するためのタイム スタンプが 4 つ付けられます。ターゲットルータでレスポンダ機能がイネーブルの場合、タイム スタンプ 3（TS3）からタイム スタンプ 2（TS2）を引いてテスト パケットの処理にかかった時間を求め、デルタ（Δ）で表します。次に全体の RTT からこのデルタの値を引きます。IP SLA により、この方法はソース ルータにも適用されます。その場合、着信タイム スタンプ 4（TS4）が割り込みレ

ベルで付けられ、より正確な結果を得ることができます。



この他にも、ターゲット デバイスに 2 つのタイム スタンプがあれば一方向遅延、ジッタ、方向性を持つパケット損失がトラッキングできるという利点があります。大半のネットワーク動作は非同期なので、このような統計情報があるのは問題です。ただし一方向遅延測定を取り込むには、ソース ルータとターゲット ルータの両方にネットワーク タイム プロトコル（NTP）を設定し、両方のルータを同じくロック ソースに同期させる必要があります。一方向ジッタ測定にはクロック同期は不要です。

IP SLA 動作のスケジューリング

IP SLA 動作を設定する場合、統計情報の取り込みとエラー情報の収集から開始するように動作をスケジューリングする必要があります。スケジューリングは、すぐに動作を開始する、または特定の月、日、時刻に開始するように設定できます。また、*pending* オプションを使用して、あとで動作を開始するように設定することもできます。pending オプションは動作の内部状態に関するもので、SNMP で表示できます。トリガーを待機する反応（しきい値）動作の場合も pending オプションを使用します。1 度に 1 つの IP SLA 動作をスケジューリングしたり、グループの動作をスケジューリングすることもできます。

Cisco IOS CLI または CISCO RTTMON-MIB で 1 つのコマンドを使用して、複数の IP SLA 動作をスケジューリングできます。等間隔で動作を実行するようにスケジューリングすると、IP SLA モニタリング トラフィックの数を制御できます。IP SLA 動作をこのように分散させると CPU 使用率を最小限に抑え、ネットワーク スケーラビリティを向上させることができます。

IP SLA 複数動作のスケジューリング機能の詳細については、『*Cisco IOS IP SLA Configuration Guide*』の「IP SLAs—Multiple Operation Scheduling」の章を参照してください。

IP SLA 動作のしきい値のモニタリング

サービス レベル契約モニタリングを正しくサポートするには、違反が発生した場合にすぐに通知されるメカニズムにする必要があります。IP SLA は次のような場合にイベントによってトリガーされる SNMP トラップを送信できます。

- 接続の損失
- タイムアウト
- RTT しきい値
- 平均ジッタしきい値
- 一方向パケット損失

- 一方向ジッタ
- 一方向平均オピニオン評点（MOS）
- 一方向遅延

IP SLA しきい値違反が発生した場合も、あとで分析するために別の IP SLA 動作がトリガーされます。たとえば、回数を増やしたり、Internet Control Message Protocol（ICMP）パス エコーや ICMP パス ジッター動作を開始してトラブルシューティングを行うことができます。

ICMP Echo

ICMP エコー動作は、シスコ デバイスと IP を使用するその他のデバイス間のエンドツーエンド応答時間を測定します。応答時間は、ICMP エコー要求メッセージを宛先に送信し、ICMP エコー応答を受信するのにかかる時間を測定して算出されます。多くのお客様は、IP SLA ICMP ベース動作、社内 ping テスト、またはこの応答所要時間を測定するために ping ベース専用プローブを使用します。IP SLA ICMP エコー動作は、ICMP ping テストと同じ仕様に準拠しており、どちらの方法でも同じ応答所要時間になります。

関連トピック

ICMP エコー動作を使用した IP サービス レベルの分析 （1273 ページ）

UDP Jitter

ジッターとは、パケット間遅延の差異を説明する簡単な用語です。複数のパケットが送信元から宛先まで 10 ミリ秒の間隔で継続的に送信される場合、宛先は 10 ミリ秒間隔で受信します（ネットワークが正常に動作している場合）。しかし、ネットワークに遅延がある場合（キューイングや代替ルートを通じた到着など）、パケットの着信の間隔が 10 ミリ秒を超える場合や 10 ミリ秒未満になる場合があります。正のジッター値は、パケットが 10 ミリ秒を超える間隔で到着することを示します。負のジッター値は、パケットが 10 ミリ秒未満の間隔で到着することを示します。パケットの到着が 12 ミリ秒間隔の場合、正のジッター値は 2 ミリ秒です。8 ミリ秒間隔で到着する場合、負のジッター値は 2 ミリ秒です。遅延による影響を受けやすいネットワークの場合、正のジッタ値は望ましくありません。ジッタ値 0 が理想的です。

ジッターのモニタリング以外にも、IP SLA UDP ジッター動作を多目的データ収集動作に使用できます。IP SLA によって生成されるパケットは、データを送受信するパケットを含めて、送信元および動作ターゲットからシーケンス情報とタイムスタンプを伝送します。このデータに基づいて、UDP ジッター動作は次を測定します。

- 方向別ジッター（送信元から宛先へ、宛先から送信元へ）
- 方向別パケット損失
- 方向別遅延（一方向遅延）
- ラウンドトリップ遅延（平均 RTT）

データを送受信するパスが異なる場合もあるので（非同期）、方向別データを使用すればネットワークで発生している輻輳や他の問題の場所を簡単に突き止めることができます。

UDP ジッタ動作では合成（シミュレーション）UDP トラフィックを生成し、送信元ルータからターゲット ルータに多数の UDP パケットを送信します。その際の各パケットのサイズ、パケット同士の間隔、送信間隔は決められています。デフォルトでは、10 バイトのペイロードサイズのパケット フレームを 10 ミリ秒で 10 個生成し、60 秒間隔で送信します。これらのパラメータは、提供する IP サービスを最適にシミュレートするように設定できます。

一方向遅延を正確に測定する場合、（NTP によって提供される）送信元デバイスとターゲットデバイス間のクロック同期が必要です。一方向ジッタおよびパケット損失を測定する場合は、クロック同期は不要です。送信元デバイスとターゲットデバイスの間でクロックが同期していない場合、一方向ジッターとパケット損失のデータは戻されますが、UDP ジッター動作による一方向遅延測定は 0 の値が戻ります。

関連トピック

UDP ジッター動作を使用した IP サービス レベルの分析 （1269 ページ）

IP SLA 動作の設定方法

ここでは、利用可能なすべての動作の設定情報について説明されているわけではありません。設定情報の詳細については『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。ここでは、応答側の設定、UDP ジッター動作の設定（応答側が必要）、ICMP エコー動作の設定（応答側が不要）などの動作例を説明します。他の動作の設定の詳細については、『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。

デフォルト設定

IP SLA 動作は設定されていません。

設定時の注意事項

IP SLA のコマンドについては、『*Cisco IOS IP SLA Command Reference, Release 12.4T*』のコマンド リファレンスを参照してください。

説明と設定手順の詳細については、『*Cisco IOS IP SLAs Configuration Guide, Release 12.4TL*』を参照してください。

ガイドに記載されている IP SLA コマンドまたは動作の中にはデバイスでサポートされないものもあります。デバイスでは、UDP ジッター、UDP エコー、HTTP、TCP 接続、ICMP エコー、ICMP パス エコー、ICMP パス ジッター、FTP、DNS、DHCP を使用する IP サービス レベル分析がサポートされます。また、複数動作スケジューリングおよび事前に設定されたしきい値のモニタリングもサポートされます。ゲートキーパー登録遅延動作測定を使用した Voice over IP（VoIP）サービス レベルはサポートしていません。

IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用してソフトウェア イメージで動作タイプがサポートされていることを確認してください。コマンド出力例は次のとおりです。

```
Device# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

IP SLA レスポンダの設定

IP SLA レスポンダは、Cisco IOS ソフトウェアベース デバイスだけで利用可能です。これには、IP SLA 機能をフルにサポートしていない一部のレイヤ 2 デバイスも含まれます。

ターゲット デバイス（動作ターゲット）上の IP SLA 応答側を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sla responder** {**tcp-connect** | **udp-echo**} **ipaddress** *ip-address* **port** *port-number* 例： `Device(config)# ip sla responder`	デバイスを IP SLA レスポンダとして設定します。 キーワードの意味は次のとおりです。 • **tcp-connect**：レスポンダの TCP 接続動作をイネーブルにします。

	コマンドまたはアクション	目的
	`udp-echo 172.29.139.134 5000`	• **udp-echo**：レスポンダの User Datagram Protocol（UDP）エコー動作またはジッター動作をイネーブルにします。 • **ipaddress** *ip-address*：宛先 IP アドレスを入力します。 • **port** *port-number*：宛先ポート番号を入力します。 （注） IP アドレスとポート番号は、IP SLA 動作のソースデバイスに設定した IP アドレスおよびポート番号と一致している必要があります。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA ネットワーク パフォーマンス測定の実装

デバイス上で IP SLA ネットワーク パフォーマンス測定を実施するには、次の手順を実行します。

始める前に

show ip sla application 特権 EXEC コマンドを使用して、ソフトウェア イメージで目的の動作タイプがサポートされていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] 例： `Device(config-ip-sla)# udp-jitter 172.29.139.134 5000`	IP SLA 動作を目的の動作タイプとして設定して（例ではUDP ジッター動作が使用されています）、そのコンフィギュレーション モードを開始します（例では UDP ジッター コンフィギュレーション モードが使用されています）。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • *destination-port*：宛先ポート番号を 1 ～ 65535 の範囲で指定します。 • （任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。送信元IPアドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近いIPアドレスが選択されます。 • （任意）**source-port** *port-number*：送信元ポート番号を 1 ～ 65535 の範囲で指定します。ポート番号を

	コマンドまたはアクション	目的
		指定しない場合、IP SLA は利用可能なポートを選択します。 • （任意）**control**：IP SLA 制御メッセージの IP SLA レスポンダへの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA 制御メッセージは宛先デバイスに送信され、IP SLA レスポンダとの接続が確立されます。 • （任意）**num-packets** *number-of-packets*：生成するパケット数を入力します。指定できる範囲は 1 ～ 6000 です。デフォルトは 10 です。 • （任意）**interval** *inter-packet-interval*：パケットの送信間隔をミリ秒で入力します。指定できる範囲は 1 ～ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-jitter)# frequency 45`	（任意）SLA 動作のオプションを設定します。次の例では、指定された IP SLA 動作が繰り返されるレートを設定します。指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 6	**threshold** *milliseconds* 例： `Device(config-ip-sla-jitter)# threshold 200`	（任意）しきい値条件を設定します。次の例では、指定された IP SLA 動作のしきい値が 200 に設定されます。有効な範囲は 0 ～ 60000 ミリ秒です。
ステップ 7	**exit** 例： `Device(config-ip-sla-jitter)# exit`	SLA 動作コンフィギュレーションモード（この例では UDP ジッターコンフィギュレーションモード）を終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 8	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** |	個々の IP SLA 動作のスケジューリングパラメータを設定します。

	コマンドまたはアクション	目的
	now | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**] 例： `Device(config)# ip sla schedule 10 start-time now life forever`	• *operation-number*：RTR エントリ番号を入力します。 • （任意）**life**：動作の実行を無制限（**forever**）に指定するか、特定の秒数（*seconds*）を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 • （任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24 時間表記）、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すると、開始時刻を指定するまでは情報を収集しません。 **now** と入力すると、ただちに動作を開始します。 **after** *hh:mm:ss* と入力すれば、指定した時刻の経過後に動作を開始します。 • （任意）**ageout** *seconds*：情報を収集していないとき、メモリの動作を保存する秒数を指定します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	Device# **show running-config**	
ステップ 11	**copy running-config startup-config** 例： Device# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

UDP ジッター コンフィギュレーション

次に、UDP ジッター IP SLA 動作の設定例を示します。

```
Device(config)# ip sla 10
Device(config-ip-sla)# udp-jitter 172.29.139.134 5000
Device(config-ip-sla-jitter)# frequency 30
Device(config-ip-sla-jitter)# exit
Device(config)# ip sla schedule 5 start-time now life forever
Device(config)# end
Device# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

関連トピック

Cisco IOS IP SLA でのネットワーク パフォーマンスの測定 （1257 ページ）
SLA の制約事項 （1255 ページ）

UDP ジッター動作を使用した IP サービス レベルの分析

送信元デバイス上の UDP ジッター作を設定するには、次の手順を実行します。

始める前に

送信元デバイス上で UDP ジッター動作を設定するには、ターゲット デバイス（動作ターゲット）で、IP SLA レスポンダをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] 例： `Device(config-ip-sla)# udp-jitter 172.29.139.134 5000`	IP SLA 動作を UDP ジッター動作として設定し、UDP ジッター コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • *destination-port*：宛先ポート番号を 1 ～ 65535 の範囲で指定します。 • （任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスま

	コマンドまたはアクション	目的
		たはホスト名を指定します。送信元IPアドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近いIPアドレスが選択されます。 • （任意）**source-port** *port-number*：送信元ポート番号を 1 ～ 65535 の範囲で指定します。ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 • （任意）**control**：IP SLA 制御メッセージの IP SLA レスポンダへの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA 制御メッセージは宛先デバイスに送信され、IP SLA レスポンダとの接続が確立されます。 • （任意）**num-packets** *number-of-packets*：生成するパケット数を入力します。指定できる範囲は 1 ～ 6000 です。デフォルトは 10 です。 • （任意）**interval** *inter-packet-interval*：パケットの送信間隔をミリ秒で入力します。指定できる範囲は 1 ～ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-jitter)# frequency 45`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 6	**exit** 例： `Device(config-ip-sla-jitter)# exit`	UDP ジッター コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**] 例： `Device(config)# ip sla schedule 10 start-time now life forever`	個々の IP SLA 動作のスケジューリングパラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 • （任意）**life**：動作の実行を無制限（**forever**）に指定するか、特定の秒数（*seconds*）を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 • （任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24 時間表記）、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すると、開始時刻を指定するまでは情報を収集しません。 **now** と入力すると、ただちに動作を開始します。 **after** *hh:mm:ss* と入力すれば、指定した時刻の経過後に動作を開始します。 • （任意）**ageout** *seconds*：情報を収集していないとき、メモリの動作を保存する秒数を指定します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

UDP ジッター IP SLA 動作の設定

次に、UDP ジッター IP SLA 動作の設定例を示します。

```
Device(config)# ip sla 10
Device(config-ip-sla)# udp-jitter 172.29.139.134 5000
Device(config-ip-sla-jitter)# frequency 30
Device(config-ip-sla-jitter)# exit
Device(config)# ip sla schedule 5 start-time now life forever
Device(config)# end
Device# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

関連トピック

UDP Jitter （1261 ページ）

ICMP エコー動作を使用した IP サービス レベルの分析

送信元デバイス上の ICMP エコー動作を設定するには、次の手順を実行します。

始める前に

この動作では、IP SLA レスポンダ側を有効にしておく必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sla** *operation-number* 例： `Device(config)# ip sla 10`	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-id*] 例： `Device(config-ip-sla)# icmp-echo 172.29.139.134`	IP SLA 動作を ICMP エコー動作として設定し、ICMP エコー コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • （任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA で

	コマンドまたはアクション	目的
		は、宛先に最も近いIPアドレスが選択されます。 • （任意）**source-interface** *interface-id*：動作に対する送信元インターフェイスを指定します。
ステップ 5	**frequency** *seconds* 例： `Device(config-ip-sla-echo)# frequency 30`	（任意）指定したIP SLA動作を繰り返す間隔を設定します。指定できる範囲は1 ～ 604800秒で、デフォルトは60秒です。
ステップ 6	**exit** 例： `Device(config-ip-sla-echo)# exit`	UDP エコー コンフィギュレーション モードを終了します。続いて、グローバルコンフィギュレーションモードに戻ります。
ステップ 7	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**] 例： `Device(config)# ip sla schedule 5 start-time now life forever`	個々のIP SLA動作のスケジューリングパラメータを設定します。 • *operation-number*：RTRエントリ番号を入力します。 • （任意）**life**：動作の実行を無制限（**forever**）に指定するか、特定の秒数（*seconds*）を指定します。指定できる範囲は0 ～ 2147483647です。デフォルトは3600秒（1時間）です。 • （任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24時間表記）、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すると、開始時刻を指定するまでは情報を収集しません。 **now** と入力すると、ただちに動作を開始します。

	コマンドまたはアクション	目的
		after *hh:mm:ss* と入力すれば、指定した時刻の経過後に動作を開始します。 • （任意）**ageout** *seconds*：情報を収集していないとき、メモリの動作を保存する秒数を指定します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ICMP エコー IP SLA 動作の設定

次に、ICMP エコー IP SLA 動作の設定例を示します。

```
Device(config)# ip sla 12
Device(config-ip-sla)# icmp-echo 172.29.139.134
Device(config-ip-sla-echo)# frequency 30
Device(config-ip-sla-echo)# exit
Device(config)# ip sla schedule 5 start-time now life forever
Device(config)# end
Device# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
```

```
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

関連トピック

IP SLA 動作のしきい値のモニタリング （1260 ページ）

IP SLA 動作のモニタリング

次の表で、IP SLA 動作の設定と結果を表示するために使用するコマンドについて説明します。

表 *73 : IP SLA* 動作のモニタリング

show ip sla application	Cisco IOS IP SLA のグローバル情報を表示します。
show ip sla authentication	IP SLA 認証情報を表示します。
show ip sla configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する、デフォルト値をすべて含めた設定値を表示します。
show ip sla enhanced-history {**collection-statistics** | **distribution statistics**} [*entry-number*]	収集した履歴バケットの拡張履歴統計情報、あるいはすべての IP SLA 動作または特定の IP SLA 動作に関する分散統計情報を表示します。
show ip sla ethernet-monitor configuration [*entry-number*]	IP SLA 自動イーサネット設定を表示します。

show ip sla group schedule [*schedule-entry-number*]	IP SLA グループ スケジューリング設定と個別情報を表示します。
show ip sla history [*entry-number* | **full** | **tabular**]	すべての IP SLA 動作について収集した履歴を表示します。
show ip sla mpls-lsp-monitor {**collection-statistics** | **configuration** | **ldp operational-state** | **scan-queue** | **summary** [*entry-number*] | **neighbors**}	MPLS ラベル スイッチド パス（LSP）ヘルスモニタ動作を表示します。
show ip sla reaction-configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する、予防的しきい値のモニタリングの設定を表示します。
show ip sla reaction-trigger [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する反応トリガー情報を表示します。
show ip sla responder	IP SLA レスポンダ側の情報を表示します。
show ip sla statistics [*entry-number* | **aggregated** | **details**]	動作ステータスおよび統計情報の現在値または合計値を表示します。

IP SLA 動作のモニタリングの例

次の例は、アプリケーションごとのすべての IP SLA を示しています。

```
Device# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

次の例は、すべての IP SLA ディストリビューション統計情報を示しています。

```
Device# show ip sla enhanced-history distribution-statistics

Point by point Enhanced History
Entry    = Entry Number
```

```
Int      = Aggregation Interval
BucI     = Bucket Index
StartT   = Aggregation Start Time
Pth      = Path index
Hop      = Hop in path index
Comps    = Operations completed
OvrTh    = Operations completed over thresholds
SumCmp   = Sum of RTT (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry Int BucI StartT     Pth Hop Comps OvrTh SumCmp     SumCmp2L   SumCmp2H   T
Max    TMin
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco Medianet Metadata Guide	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mdata/configuration/15-sy/mdata-15sy-book/metadata-framework.pdf
Cisco Media Services Proxy Configuration Guide	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/msp/configuration/15-mt/msp-15-mt-book.pdf
Cisco Mediatrace and Cisco Performance Monitor Configuration Guide	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/media_monitoring/configuration/15-mt/mm-15-mt-book/mm-mediatrace.html

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

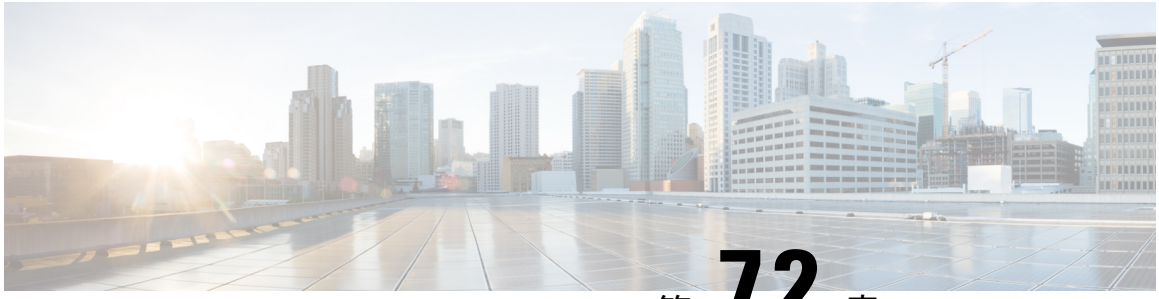
標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support



第 72 章

ローカル ポリシーの設定

- 機能情報の確認 （1281 ページ）
- ローカル ポリシーの設定に関する制限 （1281 ページ）
- ローカル ポリシーの設定に関する情報 （1282 ページ）
- ローカル ポリシーの設定方法 （1284 ページ）
- ローカル ポリシーの監視 （1289 ページ）
- 例：ローカル ポリシーの設定 （1290 ページ）
- ローカル ポリシーの設定に関する追加情報 （1291 ページ）
- ローカル ポリシーの設定の実行に関する機能履歴 （1292 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ローカル ポリシーの設定に関する制限

- デバイス上でサポートされるポリシーマップ属性は、QoS、VLAN、セッションタイムアウト、および ACL です。
- Apple iphone 6s は、HTTP プロファイリング後に「ワークステーション」として分類されます。

関連トピック

パラメータ マップの作成（CLI） （1285 ページ）

クラス マップの作成（CLI）（1286 ページ）
ポリシー マップの作成（CLI）（1287 ページ）
WLAN 上のデバイスのローカル ポリシーの適用（CLI）（1288 ページ）
インターフェイス テンプレートの作成（CLI）（1284 ページ）
ローカル ポリシーの設定に関する情報（1282 ページ）

ローカル ポリシーの設定に関する情報

ローカル ポリシーは、HTTP と DHCP に基づいてデバイスをプロファイルすることで、ネットワーク上のエンドデバイスを識別できるようにします。ユーザは、デバイス ベースのポリシーを設定して、それをネットワーク上でユーザ単位またはデバイス ポリシー単位に適用できます。

ローカル ポリシーを使用すれば、モバイル デバイスのプロファイリングと、プロファイルしたデバイスの特定の VLAN への基本オンボーディングが可能になります。また、ACL と QoS を割り当てたり、セッション タイムアウトを設定したりできます。

ローカル ポリシーは次の 2 種類のコンポーネントとして設定できます。

- ネットワークに参加しているクライアントに固有のサービス テンプレートとしてのポリシー属性の定義とポリシー一致基準の適用。
- ポリシーへの一致基準の適用。

次のポリシー一致属性がローカル ポリシーの設定に使用されます。

- デバイス：デバイスのタイプを定義します。Windows ベースのコンピュータ、スマートフォン、iPad や iPhone などの Apple デバイス。
- ユーザ名：ユーザのユーザ名を定義します。
- ユーザ ロール：学生や従業員などのユーザ タイプまたはユーザが属しているユーザ グループを定義します。
- MAC：エンド ポイントの MAC アドレスを定義します。
- MAC OUI：MAC アドレス OUI を定義します。

デバイスでエンドポイントごとにこれらのパラメータに対応する一致が検出されたら、ポリシーを追加できます。ポリシー強制は、次のセッション属性に基づくモバイルデバイスの基本デバイス オンボーディングを可能にします。

- VLAN
- QoS
- ACL
- Session timeout

これらのポリシーを設定して、エンドポイントに指定したポリシーを強制できます。ワイヤレス クライアントは、MAC OUI と DHCP に基づいてプロファイルされます。デバイスは、これらの属性と事前定義の分類プロファイルを使用してデバイスを識別します。

デフォルト プロファイル テキスト ファイルの置き換え

新しいデバイスが未分類の場合は、デバイスの MAC アドレスをシスコ サポート チームまでご連絡ください。シスコ サポート チームがその MAC アドレスを含む新しい **dc_default_profile.txt** ファイルを提供します。**dc_default_profile.txt** ファイルを以前のファイルと置き換える必要があります。**dc_default_profile.txt** ファイルを変更するには、次の手順に従ってください。

1. 次のコマンドを入力して、デバイス分類子を停止します。

   デバイス**(config)#no device classifier**

2. 次のコマンドを入力して、ファイルをコピーします。

   デバイス**#device classifier profile location** *filepath*

3. 次のコマンドを入力して、デバイス分類子を開始します。

   デバイス**(config)# device classifier**

トランク ポート上のセッション モニタの無効化

アップリンク トランク ポート上では、セッション モニタリングを作成しないでください。デフォルトで、セッション モニタリングは有効になっています。セッション モニタリングを無効にする必要があります。

1. 次のコマンドを入力して、グローバル コンフィギュレーション モードを開始します。

   デバイス**#configure terminal**

2. 次のコマンドを入力して、インターフェイス コンフィギュレーション モードを開始します。

   デバイス**(config)#interface** *interface-id*

3. 次のコマンドを入力して、セッション モニタリングを無効にします。

   デバイス**(config-if)#no access-session monitor**

関連トピック

パラメータ マップの作成（CLI）（1285 ページ）
クラス マップの作成（CLI）（1286 ページ）
ポリシー マップの作成（CLI）（1287 ページ）
WLAN 上のデバイスのローカル ポリシーの適用（CLI）（1288 ページ）
インターフェイス テンプレートの作成（CLI）（1284 ページ）
ローカル ポリシーの設定に関する制限（1281 ページ）
ローカル ポリシーの監視（1289 ページ）
例：ローカル ポリシーの設定（1290 ページ）

ローカル ポリシーの設定方法

ローカル ポリシーの設定（CLI）

ローカル ポリシーを設定するには、次の手順を実行します。

1. サービス テンプレートを作成します。
2. インターフェイス テンプレートを作成します。
3. パラメータ マップを作成します。
4. ポリシー マップを作成します。
5. WLAN 上でローカル ポリシーを適用します。

インターフェイス テンプレートの作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**template** *interface-template-name*
	例：
	`Device(config)# template cisco-phone-template`
	`Device(config-template)#`
		インターフェイス テンプレート コンフィギュレーション モードを開始します。

ステップ 3	**switchport mode access** 例： `Device(config-template)# switchport mode access`	トランキングなし、タグなしの単一 VLAN イーサネット インターフェイスとして、インターフェイスを設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。アクセスポートは、デフォルトで、VLAN 1 のトラフィックを送受信します。
ステップ 4	**switchport voice vlan** *vlan_id* 例： `Device(config-template)# switchport voice vlan 20`	すべての音声トラフィックを指定された VLAN 経由で転送するように指定します。1 ～ 4094 の値を指定できます。
ステップ 5	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config)# end`	ンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報 （1282 ページ）
ローカル ポリシーの設定に関する制限 （1281 ページ）
ローカル ポリシーの監視 （1289 ページ）
例：ローカル ポリシーの設定 （1290 ページ）

パラメータ マップの作成（CLI）

クラス マップよりパラメータ マップの使用をお勧めします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map typesubscriberattribute-to-service** *parameter-map-name* 例： `Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para`	パラメータ マップのタイプと名前を指定します。
ステップ 3	*map-index* *frame*map{device-type|media-type|oui|user-agent|username} {eq|neq|regex} 例： `Device(config-parameter-map-filter)# 10 map device-type eq "WindowsXP-Workstation"`	パラメータ マップ属性フィルタ基準を指定します。

ステップ 4	**interface-template** *interface-template-name*
	例：
	`Device(config-parameter-map-filter-submode)# interface-template cisco-phone-template`
	`Device(config-parameter-map-filter-submode)#`
		サービス テンプレート コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報 （1282 ページ）
ローカル ポリシーの設定に関する制限 （1281 ページ）
ローカル ポリシーの監視 （1289 ページ）
例：ローカル ポリシーの設定 （1290 ページ）

クラス マップの作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map typecontrol subscriber** *class-map-name* {**match-all** | **match-any** | **match-first**} 例： `Device(config)# class-map type control subscriber CLASS_AC_1 match-all`	クラス マップのタイプと名前を指定します。
ステップ 3	**match** {**device-type** | **mac-address** | **oui** | **username** | **userrole**} *filter-type-name* 例： `Device(config-class-map)# match device-type Cisco-IP-Phone-7961`	クラス マップ属性フィルタ基準を指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報 （1282 ページ）
ローカル ポリシーの設定に関する制限 （1281 ページ）
ローカル ポリシーの監視 （1289 ページ）

例：ローカル ポリシーの設定 （1290 ページ）

ポリシー マップの作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map typecontrolsubscriber** *policy-map-name* 例： `Device(config)# policy-map type control subscriber Aironet-Policy`	ポリシー マップ タイプを指定します。
ステップ 3	**eventidentity-update**{**match-all** | **match-first**} 例： `Device(config-policy-map)# event identity-update match-all`	ポリシー マップに対する一致基準を指定します。
ステップ 4	*class_numberclass_map_name***class** { | **always** }{**do-all** | **do-until-failure** | **do-until-success**} 例： `Device(config-class-control-policymap)# 1 class local_policy1_class do-until-success`	ローカル プロファイリング ポリシー クラス マップ番号を設定し、処理の実行方法を指定します。クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • **always**：照合を行わずに実行しますが、成功を返します。 • **do-all**：すべての処理を実行します。 • **do-until-failure**：照合が失敗するまですべての処理を実行します。これはデフォルト値です。 • **do-until-success**：照合が成功するまですべての処理を実行します。
ステップ 5	*action-index***map attribute-to-servicetable** *parameter-map-name* 例： `Device(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-para`	使用するパラメータ マップ テーブルを指定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報 （1282 ページ）
ローカル ポリシーの設定に関する制限 （1281 ページ）
ローカル ポリシーの監視 （1289 ページ）
例：ローカル ポリシーの設定 （1290 ページ）

WLAN 上のデバイスのローカル ポリシーの適用（CLI）

始める前に

パラメータ マップのサービス ポリシーにデバイス タイプ ベースのルールが含まれる場合、デバイス分類子がイネーブルになっていることを確認します。

（注） **device classification** コマンドを使用して、show コマンドの出力で正しく表示されるようにデバイスを分類する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan-name* 例： `Device(config)# wlan wlan1`	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**service-policy type controlsubscriber** *policymapname* 例： `Device(config-wlan)# service-policy type control subscriber Aironet-Policy`	WLAN にローカル ポリシーを適用します。

	コマンドまたはアクション	目的
ステップ 4	**profiling local http (optional)** 例： `Device(config-wlan)# profiling local http`	HTTP プロトコルに基づいて、デバイスのプロファイリングのみをイネーブルにします（任意）。
ステップ 5	**profiling radius http (optional)** 例： `Device(config-wlan)# profiling radius http`	ISE でデバイスのプロファイリングをイネーブルにします（任意）。
ステップ 6	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をシャットダウンしないように指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報 （1282 ページ）
ローカル ポリシーの設定に関する制限 （1281 ページ）
ローカル ポリシーの監視 （1289 ページ）
例：ローカル ポリシーの設定 （1290 ページ）

ローカル ポリシーの監視

次のコマンドを使用して、デバイス上で設定されたローカル ポリシーを監視できます。

表 *74*：ローカル ポリシーの監視コマンド

コマンド	目的
show access-session	表示されたクライアントまたはMACアドレスごとの承認ステータス、メソッド、およびドメインを含むアクセス セッションのサマリーを表示します。
show access-session cache	クライアントの最新の分類を表示します。
show device classifier attached detail	Mac、DHCP、HTTP などのパラメータに基づくクライアントの最新の分類を表示します。

show access-session mac *mac-address***details**	マップされたポリシー、使用されたサービス テンプレート、およびクライアントの属性を表示します。 （注） **show access-session detail** コマンド出力にセッション タイムアウトの詳細が表示されていない場合は、クライアント アクセス セッションでセッション タイムアウトを使用してクライアント プロファイルを有効にしてから、**show access-session mac** *mac-address***details** コマンドを実行してセッション タイムアウトの詳細を表示する必要があります。
show access-session mac *mac-address***policy**	マップされたポリシー、使用されたサービス テンプレート、およびクライアントの属性を表示します。 また、次の情報を表示する [**Resultant Policy**] も確認できます。 • セッションにローカルで属性が設定されているときに、セッションに適用された最終属性。 • サーバから適用された属性。

関連トピック

パラメータ マップの作成（CLI）（1285 ページ）
クラス マップの作成（CLI）（1286 ページ）
ポリシー マップの作成（CLI）（1287 ページ）
WLAN 上のデバイスのローカル ポリシーの適用（CLI）（1288 ページ）
インターフェイス テンプレートの作成（CLI）（1284 ページ）
ローカル ポリシーの設定に関する情報（1282 ページ）

例：ローカル ポリシーの設定

（注） 各コンフィギュレーション コマンド ラインの最後で、CTRL Z を入力して、コマンドを実行し、次の行に移動します。

次の例は、インターフェイス テンプレートの作成方法を示しています。

```
Device# configure terminal
Device(config)#template cisco-phone-template
Device(config-template)#switchport mode access
Device(config-template)#switchport voice vlan 20
Device(config-template)# end
```

次の例は、パラメータ マップの作成方法を示しています。

```
Device# configure terminal
Device(config)#parameter-map type subscriber attribute-to-service param-wired
Device(config-parameter-map-filter)#10 map device-type regex Cisco-IP-Phone
Device(config-parameter-map-filter-submode)#10 interface-template cisco-phone-template
Device(config-parameter-map)# end
```

次の例は、ポリシー マップの作成方法を示しています。

```
Device(config)# policy-map type control subscriber apple-tsim
Device(config-policy-map)# event identity-update match-all
Device(config-policy-map)# 1 class always do-until-failure
Device(config-policy-map)# 1 map attribute-to-service table apple-tsim-param
Device(config-policy-map)# end
```

次の例は、WLAN 上のデバイスにポリシーを適用する方法を示しています。

```
Device(config)# wlan wlan1
Device(config-wlan)# client vlan VLAN0054
Device(config-wlan)# profiling local http
Device(config-wlan)# service-policy type control subscriber apple-tsim
Device(config-wlan)# no shutdown
Device# end
```

関連トピック

パラメータ マップの作成（CLI）（1285 ページ）
クラス マップの作成（CLI）（1286 ページ）
ポリシー マップの作成（CLI）（1287 ページ）
WLAN 上のデバイスのローカル ポリシーの適用（CLI）（1288 ページ）
インターフェイス テンプレートの作成（CLI）（1284 ページ）
ローカル ポリシーの設定に関する情報（1282 ページ）

ローカル ポリシーの設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

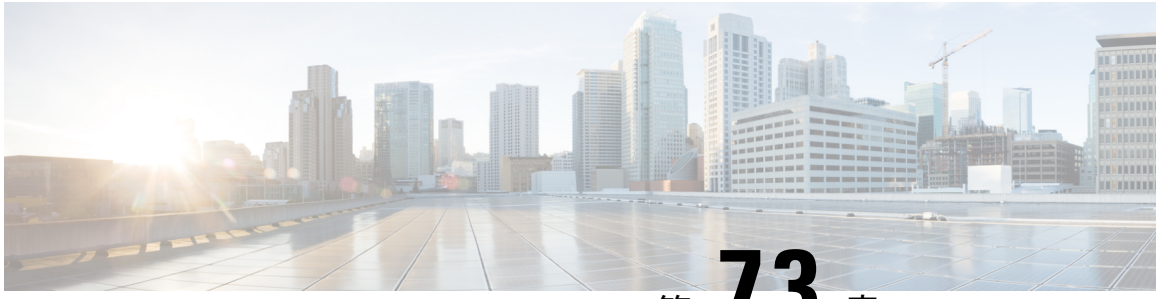
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ローカル ポリシーの設定の実行に関する機能履歴

リリース	機能情報
Cisco IOS XE 3E	この機能が導入されました。



第 73 章

SPAN および RSPAN の設定

- 機能情報の確認 （1293 ページ）
- SPAN および RSPAN の前提条件 （1293 ページ）
- SPAN および RSPAN の制約事項 （1294 ページ）
- SPAN および RSPAN について （1296 ページ）
- SPAN および RSPAN の設定方法 （1310 ページ）
- SPAN および RSPAN 動作のモニタリング （1337 ページ）
- SPAN および RSPAN の設定例 （1337 ページ）
- その他の参考資料 （1340 ページ）
- SPAN および RSPAN の機能の履歴と情報 （1341 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

SPAN および RSPAN の前提条件

SPAN

- SPAN トラフィックを特定の VLAN に制限するには、**filter vlan** キーワードを使用します。トランク ポートをモニタしている場合、このキーワードで指定された VLAN 上のトラフィックのみがモニタされます。デフォルトでは、トランク ポート上のすべての VLAN がモニタされます。

RSPAN

- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。

SPAN および RSPAN の制約事項

SPAN

SPAN の制約事項は次のとおりです。

- 各 デバイス で 66 のセッションを設定できます。最大 8 の送信元セッションを設定できます。残りのセッションは、RSPAN 宛先セッションとして設定できます。送信元セッションは、ローカル SPAN セッションまたは RSPAN 送信元セッションのどちらかになります。
- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックをモニタできます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- デバイス ポートを SPAN 宛先ポートとして設定すると、通常のデバイス ポートではなくなります。SPAN 宛先ポートを通過するのは、監視対象トラフィックのみになります。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、**no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなし、ISL、または IEEE 802.1Q）を伝送します。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。
- ディセーブルのポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN がイネーブルになってからです。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。

SPAN セッションのトラフィック監視には次の制約事項があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。

- Wireshark は、出力スパンがアクティブな場合は出力パケットをキャプチャしません。
- 同じデバイスまたはデバイス スタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。デバイスまたはデバイス スタックは合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つのデバイス スタックあたりに設定できる宛先ポートは最大で 64 個です。
- SPAN セッションがデバイスの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN がイネーブルの場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。多数のポートまたは VLAN を監視すると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- デバイスは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じデバイスまたはデバイス スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

RSPAN

RSPAN の制約事項は次のとおりです。

- RSPAN は、BPDU パケット監視または他のレイヤ 2 デバイス プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのデバイスで VLAN RSPAN 機能がサポートされていることを確認してください。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。ただし、デバイスはスパンされ

たトラフィックを監視しないため、デバイスの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパニングがサポートされません。

- CDP パケットは、ハードウェアの制限により、RSPAN が設定された VLAN では転送されません。
- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがプルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラッディングが防止されます。
- RSPAN を使用するには、スイッチが LAN Base イメージを実行している必要があります。

SPAN および RSPAN について

SPAN および RSPAN

ポートまたは VLAN を通過するネットワーク トラフィックを解析するには、SPAN または RSPAN を使用して、そのデバイス上、またはネットワーク アナライザやその他のモニタ デバイス、あるいはセキュリティ デバイスに接続されている別のデバイス上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。SPAN は送信元ポートまたは VLAN 上のネットワーク トラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に出入りするトラフィックだけです。送信元 VLAN にルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックはモニタできません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは、モニタできます。

ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先ポートを使用できます。たとえば、Cisco 侵入検知システム（IDS）センサー装置を宛先ポートに接続した場合、IDS デバイスは TCP リセット パケットを送信して、疑わしい攻撃者の TCP セッションを停止させることができます。

ローカル SPAN

ローカル SPAN は 1 つのデバイス内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じデバイスまたはデバイス スタック内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。

図 *83* : 単一デバイスでのローカル *SPAN* の設定例

ポート 5（送信元ポート）上のすべてのトラフィックがポート 10（宛先ポート）にミラーリングされます。ポート 10 のネットワーク アナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 からのすべてのネットワーク トラフィックを受信します。

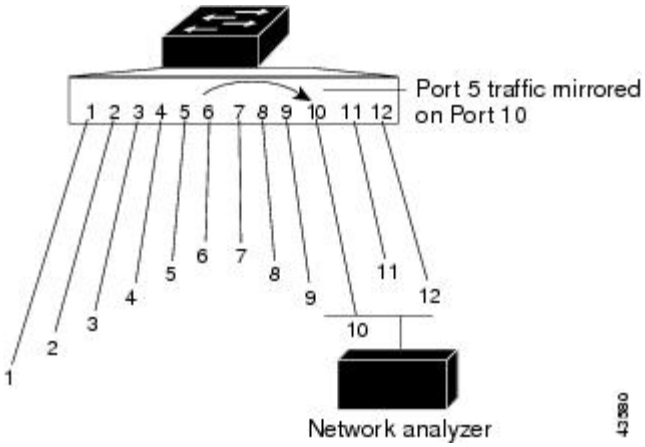
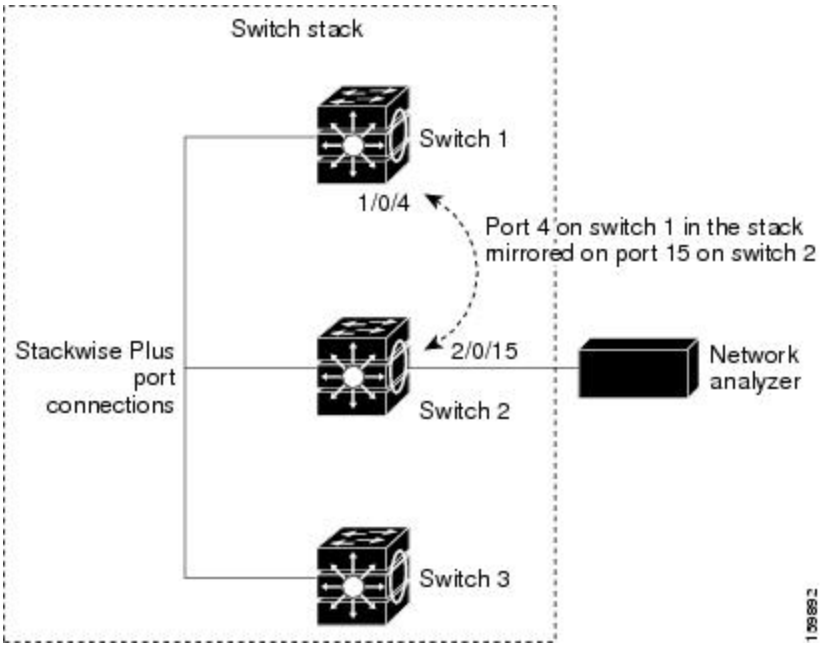


図 *84* : デバイス スタックでのローカル *SPAN* の設定例

これは、デバイス スタック内のローカル SPAN の例です。送信元ポートと宛先ポートは異なるスタック メンバにあります。



関連トピック

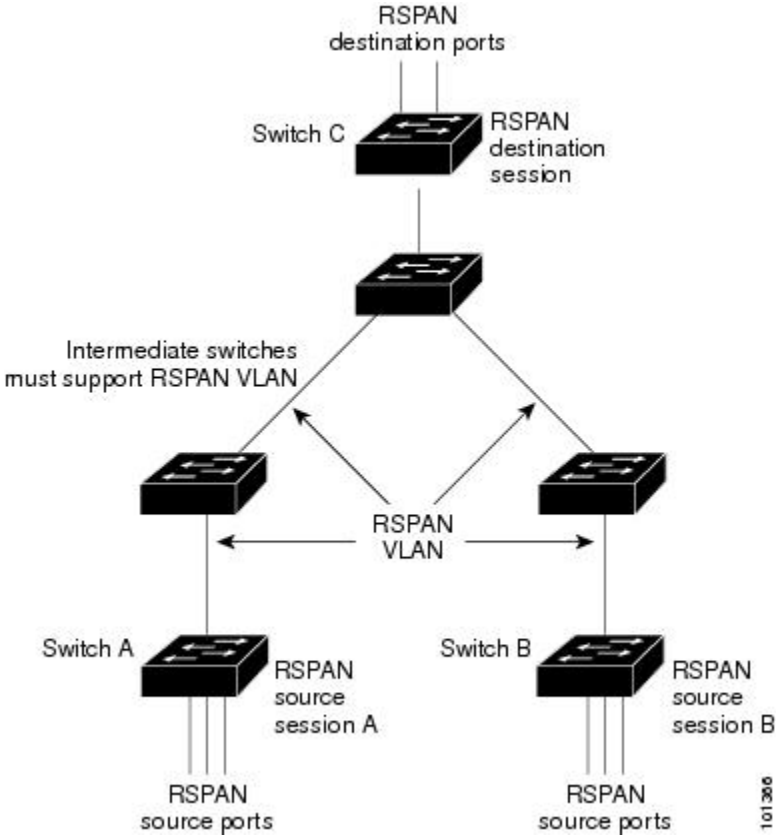
ローカル SPAN セッションの作成 （1310 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定 （1313 ページ）
例：ローカル SPAN の設定 （1337 ページ）

リモート SPAN

RSPAN は、異なるデバイス（または異なるデバイス スタック）上の送信元ポート、送信元 VLAN、および宛先ポートをサポートしているので、ネットワーク上で複数のデバイスをリモート監視できます。

図 *85 : RSPAN* の設定例

下の図にデバイス A とデバイス B の送信元ポートを示します。各 RSPAN セッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのデバイスの RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランクポートを介して、RSPAN VLAN をモニタする宛先セッションに転送されます。各 RSPAN 送信元デバイスには、ポートまたは VLAN のいずれかが RSPAN 送信元として必要です。図中のデバイス C のように、宛先は常に物理ポートになります。



関連トピック

RSPAN 送信元セッションの作成 （1320 ページ）
RSPAN 宛先セッションの作成 （1324 ページ）
RSPAN 宛先セッションの作成および着信トラフィックの設定 （1327 ページ）
例：RSPAN VLAN の作成 （1338 ページ）

SPAN と RSPAN の概念および用語

- SPAN セッション
- モニタ対象トラフィック
- 送信元ポート
- 送信元 VLAN
- VLAN フィルタリング
- 宛先ポート
- RSPAN VLAN

SPAN セッション

SPAN セッション（ローカルまたはリモート）を使用すると、1 つまたは複数のポート上、あるいは 1 つまたは複数の VLAN 上でトラフィックをモニタし、そのモニタしたトラフィックを 1 つまたは複数の宛先ポートに送信できます。

ローカル SPAN セッションは、宛先ポートと送信元ポートまたは送信元 VLAN（すべて単一のネットワーク デバイス上にある）を結び付けたものです。ローカル SPAN には、個別の送信元および宛先のセッションはありません。ローカル SPAN セッションはユーザが指定した入力および出力のパケット セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は少なくとも 1 つの RSPAN 送信元セッション、1 つの RSPAN VLAN、および少なくとも 1 つの RSPAN 宛先セッションで構成されています。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN に関連付けます。宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームが転送される点を除き、ローカル SPAN セッションに非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再設定され、通常のトランク ポートを介して宛先デバイスに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットを取得し、VLAN のタギングを除去し、宛先ポートに送ります。セッションは、（レイヤ 2 制御パケットを除く）すべての RSPAN VLAN パケットのコピーを分析のためにユーザに提供します。

複数のソースおよび宛先ポートを持つ単一 RSPAN セッションを同じセッションに使用できますが、ソースが同じリモート VLAN であるソース セッションの複数使用は許可されていません。

SPAN セッションでのトラフィックのモニタには、次のような制約があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。
- 同じデバイスまたはデバイス スタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。デバイスまたはデバイス スタックは合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つのデバイス スタックあたりに設定できる宛先ポートは最大で 64 個です。
- SPAN セッションがデバイスの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN がイネーブルの場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。したがって、多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- デバイスは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じデバイスまたはデバイス スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

関連トピック

ローカル SPAN セッションの作成 （1310 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定 （1313 ページ）
例：ローカル SPAN の設定 （1337 ページ）

モニタ対象トラフィック

SPAN セッションは、次のトラフィック タイプを監視できます。

- 受信（Rx）SPAN：受信（または入力）SPAN は、デバイスが変更または処理を行う前に、送信元インターフェイスまたは VLAN が受信したすべてのパケットをできるだけ多くモニタリングします。送信元が受信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。

Diffserv コード ポイント（DSCP）の変更など、ルーティングや Quality of Service（QoS）が原因で変更されたパケットは、変更される前にコピーされます。

受信処理中にパケットをドロップする可能性のある機能は、入力 SPAN には影響を与えません。宛先ポートは、実際の着信パケットがドロップされた場合でも、パケットのコピーを受信します。パケットをドロップする可能性のある機能は、標準および拡張 IP 入力アクセス コントロール リスト（ACL）、入力 QoS ポリシング、VLAN ACL、および出力 QoS ポリシングです。

- 送信（Tx）SPAN：送信（または出力）SPAN は、デバイスによる変更または処理がすべて実行されたあとに、送信元インターフェイスから送信されたすべてのパケットをできる限り多くモニタリングします。送信元が送信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。コピーはパケットの変更後に用意されます。

  ルーティングが原因で変更されたパケット（存続可能時間（TTL）、MAC アドレス、QoS 値の変更など）は、宛先ポートで（変更されて）コピーされます。

  送信処理中にパケットをドロップする可能性のある機能は、SPAN 用の複製コピーにも影響します。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングがあります。

- 両方：SPAN セッションで、受信パケットと送信パケットの両方について、ポートまたは VLAN をモニタすることもできます。これはデフォルトです。

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。ただし、宛先ポートを設定するときに **encapsulation replicate** キーワードを入力すると、次の変更が発生します。

- 送信元ポートと同じカプセル化設定（タグなし、または IEEE 802.1Q）を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコル パケットを含むすべてのタイプのパケットがモニタされます。

したがって、カプセル化レプリケーションがイネーブルにされたローカル SPAN セッションでは、タグなし、および IEEE 802.1Q タグ付きパケットが宛先ポートに混在することがあります。

デバイスの輻輳により、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットがドロップされることがあります。一般に、これらの特性は互いに無関係です。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因でモニタされないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- デバイスの輻輳が原因でドロップされた出力パケットは、出力 SPAN からもドロップされます。

SPAN の設定によっては、同一送信元のパケットのコピーが複数、SPAN 宛先ポートに送信されます。たとえば、ポート A での RX モニタ用とポート B での TX モニタ用に双方向（RX と TX）SPAN セッションが設定されているとします。パケットがポート A からデバイスに入ってポートBにスイッチされると、着信パケットも発信パケットも宛先ポートに送信されます。このため、両方のパケットは同じものになります。レイヤ3書き換えが行われた場合には、パケット変更のため異なるパケットになります。

送信元ポート

送信元ポート（別名モニタ側ポート）は、ネットワーク トラフィック分析のために監視するスイッチドポートまたはルーテッドポートです。1つのローカルSPANセッションまたはRSPAN送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向でモニタできます。デバイスは、任意の数の送信元ポート（デバイスで利用可能なポートの最大数まで）と任意の数の送信元 VLAN（サポートされている VLAN の最大数まで）をサポートしています。ただし、デバイスが送信元ポートまたは VLAN でサポートするセッション数には上限（2 つ）（ローカルまたは RSPAN）があります。単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- 複数の SPAN セッションでモニタできます。
- モニタする方向（入力、出力、または両方）を指定して、各送信元ポートを設定できます。
- すべてのポート タイプ（EtherChannel、ギガビット イーサネットなど）が可能です。
- EtherChannel 送信元の場合は、EtherChannel 全体で、または物理ポートがポート チャネルに含まれている場合は物理ポート上で個別に、トラフィックをモニタできます。
- アクセス ポート、トランク ポート、ルーテッド ポート、または音声 VLAN ポートに指定できます。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニタすることが可能です。

送信元 VLAN

VLAN ベースの SPAN（VSPAN）では、1 つまたは複数の VLAN のネットワーク トラフィックをモニタできます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスが VLAN ID となり、トラフィックはその VLAN のすべてのポートでモニタされます。

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブ ポートは送信元ポートとして含まれ、単一方向または双方向でモニタできます。
- 指定されたポートでは、モニタ対象の VLAN 上のトラフィックのみが宛先ポートに送信されます。

- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、モニタされません。
- ポートが送信元 VLAN に追加または削除されると、これらのポートで受信された送信元 VLAN のトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニタできるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブなすべての VLAN がモニタされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニタ対象を特定の VLAN に制限できます。

- VLAN フィルタリングが適用されるのは、トランク ポートまたは音声 VLAN ポートのみです。
- VLAN フィルタリングはポートベース セッションにのみ適用され、VLAN 送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセス ポートではリスト内の該当 VLAN のみがモニタされます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートおよび VLAN からのトラフィックのコピーを受信し、SPAN パケットをユーザ（通常はネットワーク アナライザ）に送信する宛先ポート（別名モニタ側ポート）が必要です。

宛先ポートの特性は、次のとおりです。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じデバイスまたはデバイス スタックに存在している必要があります。RSPAN セッションの場合は、RSPAN 宛先セッションを含むデバイス上にあります。RSPAN 送信元セッションのみを実行するデバイスまたはデバイス スタックには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先設定を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。

（注） SPAN の宛先ポートに QoS が設定されている場合、QoS はただちに有効になります。

- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。削除されたポートがルーテッドポートであった場合、このポートはルーテッド ポートでなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにすることはできません。
- 送信元ポートにすることはできません。
- EtherChannel グループにできます（**オン** モードのみ）。
- VLAN にすることはできません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。ポートは SPAN セッションに必要なトラフィック以外は送信しません。宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- デバイスまたはデバイス スタックの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化で次のように動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、各パケットに元のカプセル化が使用されます（タグなし、ISL、または IEEE 802.1Q）。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、**encapsulation replicate** がイネーブルになっているローカル SPAN セッションの出力に、タグなし、ISL、または IEEE 802.1Q タグ付きパケットが混在することがあります。
- RSPAN の場合は、元の VLAN ID は RSPAN VLAN ID で上書きされるため失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

RSPAN VLAN は、RSPAN の送信元セッションと宛先セッション間で SPAN トラフィックを伝送します。RSPAN VLAN には、次の特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上のみです。
- RSPAN VLAN は、**remote-span** VLAN コンフィギュレーション モード コマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN を、プライベート VLAN のプライマリまたはセカンダリ VLAN にはできません。

VLAN トランキング プロトコル（VTP）に対して可視である VLAN 1 ～ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。拡張 VLAN 範囲（1006 ～ 4094）内の RSPAN VLAN ID を割り当てる場合は、すべての中間デバイスを手動で設定する必要があります。

通常は、ネットワークに複数の RSPAN VLAN を配置し、それぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションで、パケットを RSPAN セッションに送信できます。また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN をモニタしたり、ユーザにトラフィックを送信したりできます。セッションは RSPAN VLAN ID によって区別されます。

関連トピック

RSPAN 送信元セッションの作成 （1320 ページ）
RSPAN 宛先セッションの作成 （1324 ページ）
RSPAN 宛先セッションの作成および着信トラフィックの設定 （1327 ページ）
例：RSPAN VLAN の作成 （1338 ページ）

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッド トラフィックを監視しません。VSPAN が監視するのはデバイスに出入りするトラフィックに限られ、VLAN間でルーティングされるトラフィックは監視しません。たとえば、VLAN が受信モニタされ、デバイスが別の VLAN から監視対象VLANにトラフィックをルーティングする場合、そのトラフィックは監視されず、SPAN 宛先ポートで受信されません。
- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参

加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。

- CDP：SPAN セッションがアクティブな間、SPAN 宛先ポートは CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。

  ASIC の制限のため、CDP パケットは RSPAN が設定された VLAN でドロップされません。

- VTP：VTP を使用すると、デバイス間で RSPAN VLAN のプルーニングが可能です。

- VLAN およびトランキング：送信元ポート、または宛先ポートの VLAN メンバーシップまたはトランクの設定値を、いつでも変更できます。ただし、宛先ポートの VLAN メンバーシップまたはトランクの設定値に対する変更が有効になるのは、SPAN 宛先設定を削除してからです。送信元ポートの VLAN メンバーシップまたはトランクの設定値に対する変更は、ただちに有効になり、対応する SPAN セッションが変更に応じて自動的に調整されます。

- EtherChannel：EtherChannelグループを送信元ポートとして設定することはできますが、SPAN 宛先ポートとして設定することはできません。グループが SPAN 送信元として設定されている場合、グループ全体がモニタされます。

  モニタ対象の EtherChannel グループに物理ポートを追加すると、SPAN 送信元ポート リストに新しいポートが追加されます。モニタ対象の EtherChannel グループからポートを削除すると、送信元ポート リストからそのポートが自動的に削除されます。

  EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータはモニタされます。ただし、EtherChannel グループに含まれる物理ポートを SPAN 宛先として設定した場合、その物理ポートはグループから削除されます。SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。EtherChannel グループから削除されたポートは、グループ メンバのままですが、inactive または suspended ステートになります。

  EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが送信元の場合、ポートは EtherChannel グループおよびモニタ対象ポート リストから削除されます。

- マルチキャスト トラフィックをモニタできます。出力ポートおよび入力ポートのモニタでは、未編集のパケットが 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト パケットの送信回数は反映されません。

- プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。

- セキュア ポートを SPAN 宛先ポートにすることはできません。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。

- IEEE 802.1x ポートは SPAN 送信元ポートにできます。SPAN 宛先ポート上で IEEE 802.1x をイネーブルにできますが、SPAN宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブルに設定されます。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。

SPAN と RSPAN とデバイス スタック

デバイスのスタックは 1 つの論理デバイスを表すため、ローカル SPAN の送信元ポートおよび宛先ポートは、スタック内の異なるデバイスである場合があります。したがって、スタック内でのデバイスの追加または削除は、RSPAN の送信元セッションまたは宛先セッションだけではなく、ローカル SPAN セッションにも影響を及ぼします。デバイスがスタックから削除されると、アクティブセッションが非アクティブになります。また、デバイスがスタックに追加されると、非アクティブ セッションがアクティブになります。

フローベースの SPAN

送信元ポートで監視されるトラフィックにアクセス コントロール リスト（ACL）を適用するフローベース SPAN（FSPAN）またはフローベース RSPAN（FRSPAN）を使用して、SPAN または RSPAN で監視するネットワーク トラフィックのタイプを制御できます。FSPAN ACL は、IPv4、IPv6、および監視される非 IP トラフィックをフィルタリングするように設定できます。

インターフェイスを通して ACL を SPAN セッションに適用します。ACL は SPAN セッション内のすべてのインターフェイスで監視されるすべてのトラフィックに適用されます。この ACL によって許可されるパケットは、SPAN宛先ポートにコピーされます。ほかのパケットは SPAN 宛先ポートにコピーされません。

元のトラフィックは継続して転送され、接続している任意のポート、VLAN、およびルータ ACL が適用されます。FSPAN ACL は転送の決定に影響を与えることはありません。同様に、ポート、VLAN、およびルータ ACL は、トラフィックのモニタリングに影響を与えません。セキュリティ入力 ACL がパケットを拒否したために転送されない場合でも、FSPAN ACL が許可すると、パケットは SPAN 宛先ポートにコピーされます。しかし、セキュリティ出力 ACL がパケットを拒否したために転送されない場合、パケットは SPAN 宛先ポートにコピーされません。ただし、セキュリティ出力 ACL がパケットの送信を許可した場合だけ、パケットは、FSPAN ACL が許可した場合 SPAN 宛先ポートにコピーされます。これは RSPAN セッションについてもあてはまります。

SPAN セッションには、次の 3 つのタイプの FSPAN ACL を接続できます。

- IPv4 FSPAN ACL：IPv4 パケットだけをフィルタリングします。
- IPv6 FSPAN ACL：IPv6 パケットだけをフィルタリングします。
- MAC FSPAN ACL：IP パケットだけをフィルタリングします。

スタックに設定された VLAN ベースの FSPAN セッションが 1 つまたは複数のデバイス上のハードウェア メモリに収まらない場合、セッションはこれらのデバイス上でアンロードされたものとして処理され、デバイスでの FSPAN ACL およびソーシングのためのトラフィックは、SPAN 宛先ポートにコピーされません。FSPAN ACL は継続して正しく適用され、トラフィックは FSPAN ACL がハードウェア メモリに収まるデバイスの SPAN 宛先ポートにコピーされます。

空の FSPAN ACL が接続されると、一部のハードウェア機能により、その ACL の SPAN 宛先ポートにすべてのトラフィックがコピーされます。十分なハードウェア リソースが使用できない場合、空の FSPAN ACL もアンロードされる可能性があります。

IPv4 および MAC FSPAN ACL は、すべてのフィーチャ セットでサポートされています。IPv6 FSPAN ACL は、拡張 IP Services フィーチャ セットでだけサポートされています。

関連トピック

FSPAN セッションの設定 （1329 ページ）
FRSPAN セッションの設定 （1333 ページ）

SPAN および RSPAN のデフォルト設定

表 *75 : SPAN* および *RSPAN* のデフォルト設定

機能	デフォルト設定
SPAN のステート（SPAN および RSPAN）	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィックの両方（**both**）
カプセル化タイプ（宛先ポート）	ネイティブ形式（タグなしパケット）
入力転送（宛先ポート）	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。
RSPAN VLAN	未設定

設定時の注意事項

SPAN 設定時の注意事項

- SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination interface**

interface-id グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの **no** 形式では、**encapsulation** オプションは無視されます。

- トランク ポート上のすべての VLAN をモニタするには、**no monitor session** *session_number* **filter** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

ローカル SPAN セッションの作成 （1310 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定 （1313 ページ）
例：ローカル SPAN の設定 （1337 ページ）

RSPAN 設定時の注意事項

- すべての SPAN 設定時の注意事項が RSPAN に適用されます。
- RSPAN VLAN には特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定のパケットを選択的にフィルタリングまたはモニタできます。RSPAN 送信元デバイス内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数のデバイスに分散させることができます。
- RSPAN VLAN 上のアクセス ポート（音声 VLAN ポートを含む）は、非アクティブ ステートになります。
- 次の条件を満たす限り、任意の VLAN を RSPAN VLAN として設定できます。
  - すべてのデバイスで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
  - 参加しているすべてのデバイスで RSPAN がサポートされている。

関連トピック

RSPAN 送信元セッションの作成 （1320 ページ）
RSPAN 宛先セッションの作成 （1324 ページ）
RSPAN 宛先セッションの作成および着信トラフィックの設定 （1327 ページ）
例：RSPAN VLAN の作成 （1338 ページ）

FSPAN および FRSPAN 設定時の注意事項

- 少なくとも 1 つの FSPAN ACL が接続されている場合、FSPAN はイネーブルになります。
- SPAN セッションに空ではない FSPAN ACL を少なくとも 1 つ接続し、ほかの 1 つまたは複数の FSPAN ACL を接続しなかった場合（たとえば、空ではない IPv4 ACL を接続し、IPv6 と MAC ACL を接続しなかった場合）、FSPAN は、接続されていない ACL によって

フィルタリングされたと思われるトラフィックをブロックします。したがって、このトラフィックは監視されません。

関連トピック

FSPAN セッションの設定 （1329 ページ）
FRSPAN セッションの設定 （1333 ページ）

SPAN および RSPAN の設定方法

ローカル SPAN セッションの作成

SPAN セッションを作成し、送信元（監視対象）ポートまたは VLAN、および宛先（監視側）ポートを指定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session all`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。

	コマンドまたはアクション	目的
ステップ 4	**monitor session** *session_number***source** {**interface** *interface-id* |**vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Device(config)# monitor session 1 source interface gigabitethernet1/0/1`	SPAN セッションおよび送信元ポート（監視対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、監視する送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタリングする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （任意）**[,** | **-]** は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**both** | **rx** | **tx**：監視するトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 • **both**：受信トラフィックと送信トラフィックの両方を監視します。

	コマンドまたはアクション	目的
		• **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックを監視します。 （注） **monitor session** *session_number***source** コマンドを複数回使用して、複数の送信元ポートを設定できます。
ステップ 5	**monitor session** *session_number***destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]} 例： `Device(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate`	SPAN セッションおよび宛先ポート（監視側ポート）を指定します。 （注） ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）**[,** | **-]** は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。

	コマンドまたはアクション	目的
		（注） **monitor session** *session_number* **destination** コマンドを複数回使用して、複数の宛先ポートを設定できます。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ローカル SPAN （1296 ページ）
SPAN セッション （1299 ページ）
SPAN 設定時の注意事項 （1308 ページ）

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成し、さらに送信元ポートまたは VLAN および宛先ポートを指定した後、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置等）用に着信トラフィックをイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session all`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number***source** {**interface** *interface-id* |**vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Device(config)# monitor session 2 source gigabitethernet1/0/1 rx`	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。
ステップ 5	**monitor session** *session_number***destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id*| **vlan** *vlan-id*}]} 例： `Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6`	SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）**[,|-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマまたはハイフンの前後にスペースを 1 つずつ入力します。

	コマンドまたはアクション	目的

		• （任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。
		• **ingress** 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。
		  • **dot1q vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受信します。
		  • **untagged vlan** *vlan-id* または **vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受信します。

ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ローカル SPAN （1296 ページ）

SPAN セッション （1299 ページ）
SPAN 設定時の注意事項 （1308 ページ）
例：ローカル SPAN の設定 （1337 ページ）

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session all`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number* **source interface** *interface-id* 例： `Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx`	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。指定したインターフェイスは、あらかじめ

	コマンドまたはアクション	目的
		トランク ポートとして設定しておく必要があります。
ステップ 5	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**] 例： `Device(config)# monitor session 2 filter vlan 1 - 5 , 9`	SPAN 送信元トラフィックを特定の VLAN に制限します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* に指定できる範囲は 1 ～ 4094 です。 • （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 6	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]} 例： `Device(config)# monitor session 2 destination interface gigabitethernet1/0/1`	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）[**,** | **-**] は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

RSPAN VLAN としての VLAN の設定

新しい VLAN を作成し、RSPAN セッション用の RSPAN VLAN になるように設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan** *vlan-id* 例： `Device(config)# vlan 100`	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。

	コマンドまたはアクション	目的
		RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN 専用）にすることはできません。
ステップ 4	**remote-span** 例： `Device(config-vlan)# remote-span`	VLAN を RSPAN VLAN として設定します。
ステップ 5	**end** 例： `Device(config-vlan)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

RSPAN に参加するすべてのデバイスに RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲（1005 未満）であり、VTP がネットワーク内でイネーブルである場合は、1 つのデバイスに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のデバイスに伝播するように設定できます。拡張範囲 VLAN（1005 を超える ID）の場合、送信元と宛先の両方のデバイス、および中間デバイスに RSPAN VLAN を設定する必要があります。

VTP プルーニングを使用して、RSPAN トラフィックが効率的に流れるようにするか、または RSPAN トラフィックの伝送が不要なすべてのトランクから、RSPAN VLAN を手動で削除します。

VLAN からリモート SPAN 特性を削除して、標準 VLAN に戻すように変換するには、**no remote-span** VLAN コンフィギュレーション コマンドを使用します。

SPAN セッションから送信元ポートまたは VLAN を削除するには、**no monitor session** *session_number***source** {**interface** *interface-id* |**vlan** *vlan-id*} グローバル コンフィギュレーション

コマンドを使用します。セッションから RSPAN VLAN を削除するには、**no monitor session** *session_number***destination remote vlan** *vlan-id* コマンドを使用します。

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを作成および開始し、モニタ対象の送信元および宛先 RSPAN VLAN を指定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session 1`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number***source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Device(config)# monitor session 1 source interface gigabitethernet1/0/1 tx`	RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • RSPAN セッションの送信元ポートまたは送信元VLANを入力します。 • *interface-id* には、モニタリングする送信元ポートを指定しま

	コマンドまたはアクション	目的
		す。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。 • （任意）**[,|-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**both | rx | tx**：監視するトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 • **both**：受信トラフィックと送信トラフィックの両方を監視します。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックをモニタします。

	コマンドまたはアクション	目的
ステップ 5	**monitor session** *session_number* **destination remote vlan** *vlan-id* 例： `Device(config)# monitor session 1 destination remote vlan 100`	RSPAN セッション、宛先 RSPAN VLAN、および宛先ポートグループを指定します。 • *session_number* には、ステップ 4 で指定した番号を入力します。 • *vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

リモート SPAN （1298 ページ）
RSPAN VLAN （1305 ページ）
RSPAN 設定時の注意事項 （1309 ページ）

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するように RSPAN 送信元セッションを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number* **source interface** *interface-id* 例： `Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx`	送信元ポート（モニタ対象ポート）と SPANセッションの特性を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。
ステップ 5	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**] 例： `Device(config)# monitor session 2 filter vlan 1 - 5 , 9`	SPAN 送信元トラフィックを特定の VLAN に制限します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* に指定できる範囲は 1 ～ 4094 です。 •（任意）**,** | **-**：カンマ（**,**）を使用して一連の VLAN を指定するか、ハ

	コマンドまたはアクション	目的
		イフン（-）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 6	**monitor session** *session_number* **destinationremote vlan** *vlan-id* 例： `Device(config)# monitor session 2 destination remote vlan 902`	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは、別のデバイスまたはデバイス スタック（送信元セッションが設定されていないデバイスまたはデバイス スタック）に設定します。

このデバイス上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan** *vlan-id* 例： `Device(config)# vlan 901`	送信元デバイスで作成された RSPAN VLAN の VLAN ID を指定し、VLAN コンフィギュレーション モードを開始します。 両方のデバイスが VTP に参加し、RSPAN VLAN ID が 2 ～ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 3 ～ 5 は不要です。
ステップ 4	**remote-span** 例： `Device(config-vlan)# remote-span`	VLAN を RSPAN VLAN として識別します。
ステップ 5	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session 1`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカルセッションを削除します。

	コマンドまたはアクション	目的
		• **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 7	**monitor session** *session_number* **sourceremote vlan** *vlan-id* 例： `Device(config)# monitor session 1 source remote vlan 901`	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 8	**monitor session** *session_number* **destination interface** *interface-id* 例： `Device(config)# monitor session 1 destination interface gigabitethernet2/0/1`	RSPAN セッションと宛先インターフェイスを指定します。 • *session_number* には、ステップ 7 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 • *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 • **encapsulation replicate** はコマンドラインのヘルプストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

リモート SPAN （1298 ページ）
RSPAN VLAN （1305 ページ）
RSPAN 設定時の注意事項 （1309 ページ）

RSPAN 宛先セッションの作成および着信トラフィックの設定

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定し、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置等）用に着信トラフィックをイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。

	コマンドまたはアクション	目的
		• **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number***sourceremote vlan** *vlan-id* 例： `Device(config)# monitor session 2 source remote vlan 901`	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id*| **vlan** *vlan-id*}]} 例： `Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6`	SPAN セッション、宛先ポート、パケット カプセル化、および着信 VLAN とカプセル化を指定します。 • *session_number* には、ステップ 5 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 • *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 • **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。 • （任意）**[,** | **-]** は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress**

	コマンドまたはアクション	目的
		を追加のキーワードと一緒に入力します。 • **dot1q vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを転送します。 • **untagged vlan** *vlan-id* または **vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを転送します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

リモート SPAN （1298 ページ）
RSPAN VLAN （1305 ページ）
RSPAN 設定時の注意事項 （1309 ページ）
例：RSPAN VLAN の作成 （1338 ページ）

FSPAN セッションの設定

SPAN セッションを作成し、送信元（監視対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定し、セッションに FSPAN を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Device(config)# monitor session 2 source interface gigabitethernet1/0/1`	SPAN セッションおよび送信元ポート（監視対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタリングする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。

	コマンドまたはアクション	目的
		（注） 1つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （任意）**[,|-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。 • （任意）**[both|rx|tx]**：モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。 • **both**：送信トラフィックと受信トラフィックの両方をモニタします。これはデフォルトです。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックを監視します。 （注） **monitor session** *session_number***source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。
ステップ 5	**monitor session** *session_number***destination** {**interface** *interface-id* **[,|-] [encapsulation replicate]**} 例：	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。

	コマンドまたはアクション	目的
	`Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate`	• **destination** には、次のパラメータを指定します。 • *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）**[, | -]** は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 （注） ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 **monitor session** *session_number* **destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 6	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*} 例： `Device(config)# monitor session 2 filter ipv6 access-group 4`	SPAN セッション、フィルタリングするパケットのタイプ、および FSPAN セッションで使用する ACL を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *access-list-number* には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。

	コマンドまたはアクション	目的
		• *name* には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

フローベースの SPAN （1307 ページ）
FSPAN および FRSPAN 設定時の注意事項 （1309 ページ）

FRSPAN セッションの設定

RSPAN 送信元セッションを開始し、監視対象の送信元および宛先 RSPAN VLAN を指定し、セッションに FRSPAN を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカルセッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Device(config)# monitor session 2 source interface gigabitethernet1/0/1`	SPAN セッションおよび送信元ポート（監視対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタリングする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。

	コマンドまたはアクション	目的
		• （任意）**[,** | **-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意） **[both** | **rx** | **tx]**：モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。 • **both**：送信トラフィックと受信トラフィックの両方をモニタします。これはデフォルトです。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックを監視します。 （注） **monitor session** *session_number***source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。
ステップ 5	**monitor session** *session_number***destinationremote vlan** *vlan-id* 例： `Device(config)# monitor session 2 destination remote vlan 5`	RSPAN セッションと宛先 RSPAN VLAN を指定します。 • *session_number* には、ステップ 4 で指定した番号を入力します。 • *vlan-id* には、モニタリングする宛先 RSPAN VLAN を指定します。
ステップ 6	**vlan** *vlan-id* 例： `Device(config)# vlan 10`	VLAN コンフィギュレーション モードを開始します。*vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 7	**remote-span** 例： `Device(config-vlan)# remote-span`	ステップ 5 で指定した VLAN が RSPAN VLAN の一部であることを指定します。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*} 例： `Device(config)# monitor session 2 filter ip access-group 7`	RSPAN セッション、フィルタリングするパケットのタイプ、および FRSPAN セッションで使用する ACL を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *access-list-number* には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • *name* には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

フローベースの SPAN （1307 ページ）
FSPAN および FRSPAN 設定時の注意事項 （1309 ページ）

SPAN および RSPAN 動作のモニタリング

次の表で、SPAN および RSPAN 動作の設定と結果を表示して動作を監視するために使用するコマンドについて説明します。

表 *76 : SPAN* および *RSPAN* 動作のモニタリング

コマンド	目的
show monitor	現在の SPAN、RSPAN、FSPAN、または FRSPAN 設定を表示します。

SPAN および RSPAN の設定例

例：ローカル SPAN の設定

次に、SPAN セッション 1 を設定し、宛先ポートへ向けた送信元ポートのトラフィックをモニタする例を示します。最初に、セッション 1 の既存の SPAN 設定を削除し、カプセル化方式を維持しながら、双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 にミラーリングします。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
Device(config)# end
```

次に、SPAN セッション 1 の SPAN 送信元としてのポート 1 を削除する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1 source interface gigabitethernet1/0/1
Device(config)# end
```

次に、双方向モニタが設定されていたポート 1 で、受信トラフィックのモニタをディセーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx
```

ポート 1 で受信するトラフィックのモニタはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ～ 3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィッ

クを宛先ポート GigabitEthernet 2 に送信する例を示します。さらに、この設定は VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするよう変更されます。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source vlan 1 - 3 rx
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2
Device(config)# monitor session 2 source vlan 10
Device(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、送信元ポート GigabitEthernet 1 上で受信されるトラフィックをモニタするように SPAN セッション 2 を設定し、送信元ポートと同じ出力カプセル化方式を使用してそれを宛先ポート GigabitEthernet 2 に送信し、VLAN 6 をデフォルトの入力 VLAN として IEEE 802.1Q カプセル化を使用する入力転送をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source gigabitethernet1/0/1 rx
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 replicate ingress dot1q vlan 6
Device(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、トランク ポート GigabitEthernet 2 で受信されたトラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先ポート GigabitEthernet 1 に送信する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 2 filter vlan 1 - 5 , 9
Device(config)# monitor session 2 destination interface gigabitethernet1/0/1
Device(config)# end
```

関連トピック

ローカル SPAN セッションの作成および着信トラフィックの設定 （1313 ページ）
ローカル SPAN （1296 ページ）
SPAN セッション （1299 ページ）
SPAN 設定時の注意事項 （1308 ページ）

例：RSPAN VLAN の作成

この例は、RSPAN VLAN 901 の作成方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# vlan 901
Device(config-vlan)# remote span
Device(config-vlan)# end
```

次に、セッション 1 に対応する既存の RSPAN 設定を削除し、複数の送信元インターフェイスをモニタするように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Device(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 1 source interface port-channel 2
Device(config)# monitor session 1 destination remote vlan 901
Device(config)# end
```

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 2 filter vlan 1 - 5 , 9
Device(config)# monitor session 2 destination remote vlan 902
Device(config)# end
```

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 source remote vlan 901
Device(config)# monitor session 1 destination interface gigabitethernet2/0/1
Device(config)# end
```

次に、RSPAN セッション 2 で送信元リモート VLAN として VLAN 901 を設定し、送信元ポート GigabitEthernet 2 を宛先インターフェイスとして設定し、VLAN 6 をデフォルトの受信 VLAN として着信トラフィックの転送をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# monitor session 2 source remote vlan 901
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
vlan 6
Device(config)# end
```

関連トピック

RSPAN 宛先セッションの作成および着信トラフィックの設定 （1327 ページ）
リモート SPAN （1298 ページ）
RSPAN VLAN （1305 ページ）
RSPAN 設定時の注意事項 （1309 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
system コマンド	『*Network Management Command Reference, Cisco IOS XE Release 3E*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

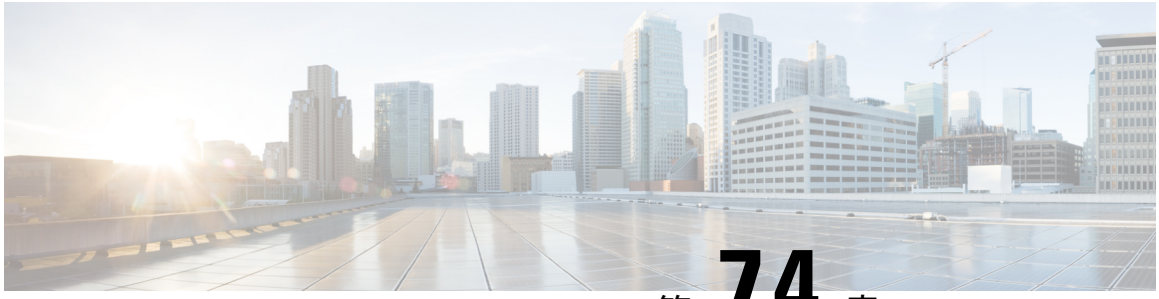
シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

SPAN および RSPAN の機能の履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	スイッチ ポート アナライザ（SPAN）：スニファやアナライザまたは RMON プローブを使用してポートまたは VLAN のデバイスのトラフィックを監視できます。 この機能が導入されました。
Cisco IOS XE 3.2SE、	フローベースのスイッチ ポート アナライザ（SPAN）：指定されたフィルタを使用してエンド ホスト間の必要なデータのみをキャプチャする手段を提供します。フィルタは、IPv4、IPv6 または IPv4 と IPv6、あるいは指定された送信元と宛先アドレス間の IP トラフィック（MAC）以外を制限するアクセス リストの観点から定義されます。 この機能が導入されました。

リリース	変更内容
Cisco IOS XE 3.2SE	EtherChannel での SPAN 宛先ポートのサポート：EtherChannel で SPAN 宛先ポートを設定できるようにします。 この機能が導入されました。
Cisco IOS XE 3.2SE	スイッチ ポート アナライザ（SPAN） - 分散型出力 SPAN：ラインカードにすでに分散された入力 SPAN とともにラインカードに出力 SPAN 機能を分散させます。出力 SPAN 機能をラインカードに分散させることで、システムのパフォーマンスが向上します。 この機能が導入されました。



第 74 章

ERSPAN の設定

このモジュールは、Encapsulated Remote Switched Port Analyzer（ERSPAN）を設定する方法について説明します。Cisco ERSPAN 機能を使用すると、ポートまたは VLAN のトラフィックをモニタし、モニタされたトラフィックを宛先ポートに送信できます。

- ERSPAN の設定の前提条件 （1343 ページ）
- ERSPAN 設定時の制約事項 （1343 ページ）
- ERSPAN の設定に関する情報 （1344 ページ）
- ERSPAN の設定方法 （1346 ページ）
- ERSPAN の設定例 （1348 ページ）
- ERSPAN の確認 （1348 ページ）
- その他の参考資料 （1350 ページ）
- ERSPAN の設定に関する機能情報 （1350 ページ）

ERSPAN の設定の前提条件

- IPv4 配信/転送ヘッダーのみサポートされます。
- アクセス コントロール リスト（ACL）のフィルタは、トンネルにモニタ対象トラフィックを送信する前に適用されます。
- タイプ II ERSPAN ヘッダーのみサポートします。

ERSPAN 設定時の制約事項

この機能には、次の制限があります。

- 宛先セッションはサポートされません。
- デバイスは、最大 66 のセッションをサポートします。最大 8 つの送信元セッションを設定できます。残りのセッションは、RSPAN 宛先セッションとして設定できます。送信元セッションは、ローカル SPAN 送信元セッションまたは RSPAN 送信元セッションあるいは ERSPAN 送信元セッションのいずれかになります。

- 送信元としてポートのリストまたは VLAN のリストを設定できますが、特定のセッションに両方を設定することはできません。
- ERSPAN CLI を介してセッションが設定されると、セッション ID とセッション タイプは変更できません。これらを変更するには、コンフィギュレーション コマンドの no 形式を使用してセッションを削除してから、セッションを再設定する必要があります。
- ERSPAN 送信元セッションは、RSPAN VLAN を伝送する送信元トランク ポートからローカルに送信されたリモート SPAN（RSPAN）VLAN トラフィックをコピーしません。
- ERSPAN 送信元セッションは、ローカルに送信された ERSPAN GRE でカプセル化されたトラフィックを送信元ポートからコピーしません。

ERSPAN の設定に関する情報

ERSPAN の概要

Cisco ERSPAN 機能を使用すると、ポートまたは VLAN のトラフィックをモニタし、モニタされたトラフィックを宛先ポートに送信できます。ERSPAN は、スイッチ プローブ デバイスやリモート モニタリング（RMON）プローブなどのネットワーク アナライザにトラフィックを送信します。ERSPAN は、異なるデバイス上のソース ポート、ソース VLAN、および宛先ポートをサポートして、ネットワーク上での複数のデバイスのリモート モニタリングを支援します。

ERSPAN は、最大 9180 バイトのカプセル化されたパケットをサポートします。ERSPAN は、ERSPAN 送信元セッション、ルーティング可能な ERSPAN GRE カプセル化トラフィック、および ERSPAN 宛先セッションで構成されています。

ERSPAN は、ERSPAN 送信元セッション、ルーティング可能な ERSPAN GRE カプセル化トラフィック、および ERSPAN 宛先セッションで構成されています。ERSPAN 送信元セッション、ERSPAN 宛先セッション、またはその両方をデバイスで設定できます。ERSPAN 送信元セッションだけが設定されたデバイスは、ERSPAN 送信元デバイスと呼ばれ、ERSPAN 宛先セッションだけが設定されたデバイスは ERSPAN 終端デバイスと呼ばれます。デバイスは、ERSPAN 送信元デバイスと終端デバイスの両方として機能できます。

送信元ポートまたは送信元 VLAN については、ERSPAN は、入力トラフィック、出力トラフィック、または入出力トラフィックを監視できます。デフォルトでは、ERSPAN は、マルチキャストおよびブリッジ プロトコル データ ユニット（BPDU）フレームを含む、すべてのトラフィックを監視します。

ERSPAN 送信元セッションは、次のパラメータによって定義されます。

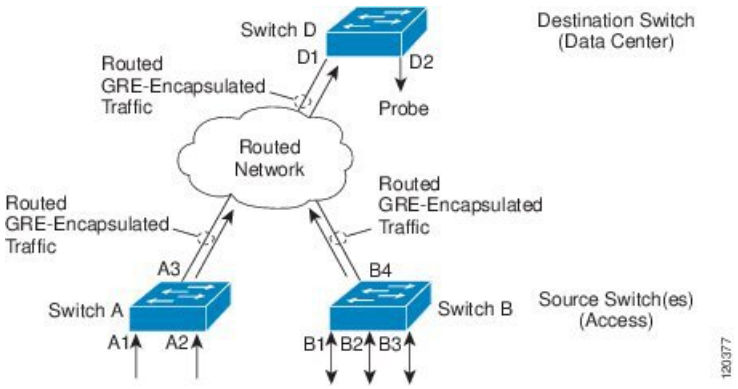
- セッション ID
- セッションでモニタされる送信元ポートまたは送信元 VLAN の一覧

- キャプチャされたトラフィックの Generic Routing Encapsulation（GRE）エンベロープの宛先 IP アドレスおよび送信元 IP アドレスとしてそれぞれ使用される、宛先および元の IP アドレス
- ERSPAN フロー ID
- IP 有効時間（TTL）などの、GRE エンベロープに関連したオプション属性

（注） ERSPAN 送信元セッションは、ERSPAN GRE カプセル化されたトラフィックを送信元ポートからコピーしません。ERSPAN 送信元セッションごとに、送信元としてポートまたは VLAN を使用することはできますが、両方は使用できません。

（注） カプセル化はハードウェアで実行されるため、CPU パフォーマンスは影響を受けません。

図 *86 : ERSPAN* の設定



ERSPAN 送信元

Cisco ERSPAN 機能は次の送信元をサポートします。

- 送信元ポート：トラフィック分析のためにモニタされる送信元ポートです。任意の VLAN の送信元ポートを設定することができ、トランク ポートは、非トランク送信元ポートとともに送信元ポートとして設定できます。
- 送信元 VLAN：トラフィック分析のためにモニタされる VLAN です。

次のインターフェイスが送信元ポートとしてサポートされています。

- GigabitEthernet
- PortChannel
- TenGigabitEthernet

ERSPAN の設定方法

ERSPAN 送信元セッションの設定

ERSPAN送信元セッションは、モニタするセッション設定パラメータおよびポートまたはVLANを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**monitor session** *span-session-number* **type erspan-source** 例： `Switch(config)# monitor session span-session-number type erspan-source`	セッション ID とセッション タイプを使用して ERSPAN 送信元セッションを定義し、ERSPAN のモニタ送信元セッション コンフィギュレーション モードを開始します。 • 送信元セッションまたは宛先セッションのセッション ID は同じグローバルな ID スペース内にあるため、各セッション ID は両方のセッション タイプに対してグローバルに一意です。 • *span-session-number* およびセッション タイプ（**erspan-source** キーワードによって設定）は、設定後は変更できません。セッションを削除するには、このコマンドの no 形式を使用し、新しいセッション ID または新しいセッション タイプでセッションを再作成します。

	コマンドまたはアクション	目的
ステップ 4	**description** 説明 例： `Switch(config-mon-erspan-src)# description source1`	ERSPAN 送信元セッションの説明を入力します。
ステップ 5	**source** {**interface** *type number* | **vlan** *vlan-ID*} [**,** | **-**| **both** | **rx** | **tx**] 例： `Switch(config-mon-erspan-src)# source interface fastethernet 0/1 rx`	送信元インターフェイスまたは VLAN、およびモニタするトラフィックの方向を設定します。
ステップ 6	**filter** {**ip access-group** {*standard-access-list* | *expanded-access-list* | *acl-name* } | **ipv6 access-group** *acl-name* | **mac access-group** *acl-name* | **vlan** *vlan-ID* [**, -**]} 例： `Switch(config-mon-erspan-src)# filter vlan 3`	（任意）ERSPAN 送信元がトランクポートである場合、送信元 VLAN フィルタリングを設定します。 • （注） 送信元 VLAN とフィルタ VLAN を同じセッションに含めることはできません。
ステップ 7	**no shutdown** 例： `Switch(config-mon-erspan-src)# no shutdown`	設定されたセッションのシャットダウンを無効にします。
ステップ 8	**destination** 例： `Switch(config-mon-erspan-src)# destination`	ERSPAN 宛先セッションを定義し、ERSPAN モニタ宛先セッション コンフィギュレーションモードを開始します。
ステップ 9	**ip address** *ip-address* 例： `Switch(config-mon-erspan-src-dst)# ip address 192.0.2.9`	ERSPAN 宛先セッションの IP アドレスを設定します。
ステップ 10	**erspan-id** *erspan-ID* 例： `Switch(config-mon-erspan-src-dst)# erspan-id 2`	ERSPAN トラフィックを識別するため、宛先セッションで使用される ID を設定します。
ステップ 11	**origin** *ip-address* 例： `Switch(config-mon-erspan-src-dst)# origin ip-address 203.0.113.2`	ERSPAN トラフィックの宛先として使用される IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 12	**ip ttl** *ttl-value* 例： `Switch(config-mon-erspan-src-dst)# erspan ttl 32`	ERSPAN トラフィックのパケットの存続可能時間（TTL）値を設定します。
ステップ 13	**end** 例： `Switch(config-mon-erspan-src-dst)# end`	ERSPAN モニタ宛先セッション コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

ERSPAN の設定例

例：ERSPAN 送信元セッションの設定

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor session 1 type erspan-source
Switch(config-mon-erspan-src)# description source1
Switch(config-mon-erspan-src)# source interface fastethernet 0/1 rx
Switch(config-mon-erspan-src)# filter vlan 3
Switch(config-mon-erspan-src)# no shutdown
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# ip address 192.0.2.9
Switch(config-mon-erspan-src-dst)# erspan-id 2
Switch(config-mon-erspan-src-dst)# origin ip-address 203.0.113.2
Switch(config-mon-erspan-src-dst)# ip ttl 32
Switch(config-mon-erspan-src-dst)# end
```

ERSPAN の確認

ERSPAN 設定を確認するには、次のコマンドを使用します。

次に、**showmonitorsessionerspan-source** コマンドの出力例を示します。

```
Switch# show monitor session erspan-source session

Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
RX Only : Gi1/4/33
Destination IP Address : 192.0.2.1
Destination ERSPAN ID : 110
Origin IP Address : 10.10.10.216
IPv6 Flow Label : None
```

次に、**show monitor session erspan-source detail** コマンドの出力例を示します。

```
Switch# show monitor session erspan-source detail

Type : ERSPAN Source Session
Status : Admin Enabled
Description : -
Source Ports :
RX Only : Gi1/4/33
TX Only : None
Both : None
Source VLANs :
RX Only : None
TX Only : None
Both : None
Source RSPAN VLAN : None
Destination Ports : None
Filter VLANs : None
Filter Addr Type :
RX Only : None
TX Only : None
Both : None
Filter Pkt Type :
RX Only : None
Dest RSPAN VLAN : None
IP Access-group : None
IPv6 Access-group : None
Destination IP Address : 192.0.2.1
Destination IPv6 Address : None
Destination IP VRF : None
Destination ERSPAN ID : 110
Origin IP Address : 10.10.10.216
IP QOS PREC : 0
IP TTL : 255
```

次の **showcapabilityfeaturemonitor erspan-source** コマンドの出力は、設定された ERSPAN 送信元セッションに関する情報を表示しています。

```
Switch# show capability feature monitor erspan-source

ERSPAN Source Session Supported: true
No of Rx ERSPAN source session: 8
No of Tx ERSPAN source session: 8
ERSPAN Header Type supported: II
ACL filter Supported: true
Fragmentation Supported: true
Truncation Supported: false
Sequence number Supported: false
QOS Supported: true
```

次の **showcapabilityfeaturemonitorerspan-destination** コマンドの出力は、設定されたすべてのグローバル組み込みテンプレートを表示しています。

```
Switch# show capability feature monitor erspan-destination

ERSPAN Destination Session Supported: false
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Catalyst 3650 スイッチ コマンド	
Catalyst 3850 スイッチ コマンド	

RFC

標準/RFC	Title
RFC 2784	『Generic Routing Encapsulation (GRE)』

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

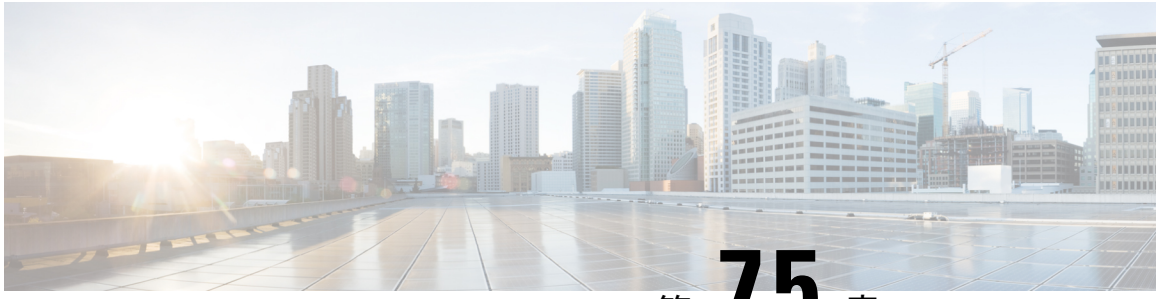
ERSPAN の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *77 : ERSPAN* の設定に関する機能情報

機能名	リリース	機能情報
ERSPAN	Cisco IOS XE Denali 16.3.1	このモジュールは、Encapsulated Remote Switched Port Analyzer（ERSPAN）を設定する方法について説明します。Cisco ERSPAN 機能を使用すると、ポートまたは VLAN のトラフィックをモニタし、モニタされたトラフィックを任意の VRF の Generic Routing Encapsulation（GRE）トンネルを介して宛先ポートに送信できます。 Cisco IOS XE Denali 16.3.1 では、この機能が Cisco Catalyst 3650 シリーズ スイッチと Cisco Catalyst 3850 シリーズ スイッチに導入されました。 次のコマンドが導入または変更されました。destination (ERSPAN)、erspan、filter (ERSPAN)、および show capability feature monitor 次のコマンドが導入または変更されました。**destination (ERSPAN)**、**filter (ERSPAN)**、および **show capability feature monitor**



第 75 章

パケット キャプチャの設定

- パケット キャプチャの前提条件 （1353 ページ）
- パケット キャプチャの制約事項 （1354 ページ）
- パケット キャプチャの概要 （1357 ページ）
- パケット キャプチャの設定 （1370 ページ）
- パケット キャプチャのモニタリング （1389 ページ）
- その他の参考資料 （1407 ページ）

パケット キャプチャの前提条件

パケット キャプチャの前提条件

- パケット キャプチャは Catalyst 3850 および Catalyst 3650 でサポートされています。
- Wireshark は、IP Base イメージおよび IP Services イメージを実行するスイッチのみでサポートされています。
- 組み込みパケット キャプチャは、LAN Base イメージを実行しているスイッチのみでサポートされています。

組み込みパケット キャプチャ（EPC）のソフトウェア サブシステムは、その動作で CPU とメモリ リソースを消費します。さまざまなタイプの操作を行うために十分なシステム リソースを準備する必要があります。システム リソースを使用するためのガイドラインを以下の表に示します。

表 *78 : EPC* サブシステムのシステム要件

システム リソース	要件
ハードウェア	CPU 利用率の要件は、プラットフォームによって異なります。

システム リソース	要件
メモリ	パケット バッファは DRAM に保存されます。パケット バッファのサイズは、ユーザが指定します。
ディスクスペース	パケットは外部のデバイスにエクスポートできます。フラッシュ ディスクでの中間保管は必要ありません。

パケット キャプチャの制約事項

パケット キャプチャの制約事項

- Cisco IOS Release XE 3.3.0(SE) 以降では、Wireshark のグローバル キャプチャはサポートされません。
- 表示フィルタは、Wireshark でサポートされています。
- Wireshark を設定するための CLI では、機能を EXEC モードからのみ実行する必要があります。通常は設定サブモードで発生するアクション（キャプチャ ポイントの定義など）は、代わりに EXEC モードから処理されます。すべての主要コマンドは NVGEN の対象ではなく、NSF と SSO のシナリオではスタンバイ スーパーバイザに同期されません。
- インターフェイスの出力方向にキャプチャされたパケットは、 rewrite（TTL、VLAN タグ、CoS、チェックサム、MAC アドレス、DSCP、precedent、UP などを含む）によって加えられる変更を反映しない場合があります。
- 入力および出力の両方のパケットの書き換え情報はキャプチャされません。
- ファイル サイズによる循環ファイル保存の制限はサポートされません。
- ファイル制限は、IP Base、および IP Services のフラッシュ ファイルのサイズに制限されています。
- Control and Provisioning of Wireless Access Points（CAPWAP）などのプロトコルのデコードは、IP Base と IP Services でサポートされています。
- IP Base および IP Services では、ファイル モードにおいて、パケットはエクスポートされずにファイルに書き込まれます。
- LAN Base イメージは、次の制限付きで、組み込み Wireshark をサポートしています。
  - キャプチャ フィルタと表示フィルタはサポートされません。
  - アクティブなキャプチャの復号化は使用できません。
  - 出力形式は、以前のリリースとは異なります。

- 組み込みパケット キャプチャ（EPC）は、入力のマルチキャスト パケットのみをキャプチャし、出力の複製パケットはキャプチャしません。

ワイヤレス パケット キャプチャ

- ワイヤレス キャプチャの唯一の形式は CAPWAP トンネル キャプチャです。
- CAPWAP トンネルをキャプチャする場合、同じキャプチャ ポイントで他のインターフェイス タイプを接続ポイントとして使用することはできません。
- 複数の CAPWAP トンネルのキャプチャがサポートされています。
- コア フィルタは適用されず、CAPWAP トンネルをキャプチャする場合は省略する必要があります。
- CAPWAP データ トンネルをキャプチャするために、各 CAPWAP トンネルは物理的ポートにマッピングされ、トラフィックをフィルタするための適切な ACL が適用されます。
- CAPWAP 非データ トンネルをキャプチャするため、スイッチはすべてのポート上のトラフィックをキャプチャし、トラフィックをフィルタするための適切な ACL を適用するように設定されます。

設定の制限

- 最大 8 つのキャプチャ ポイントを定義できますが、一度にアクティブにできるのは 1 つだけです。1 つ開始するには 1 つ停止する必要があります。
- VRF、管理ポート、プライベート VLAN はいずれも接続ポイントとして使用することはできません。
- Wireshark クラス マップでは、1 つの ACL（IPv4、IPv6、MAC）のみが許可されます。
- Wireshark は宛先 SPAN ポートでパケットをキャプチャできません。
- Wireshark は、キャプチャ ポイントにアタッチされる接続ポイント（インターフェイス）のいずれかが動作を停止するとキャプチャを停止します。たとえば、接続ポイントに関連付けられているデバイスがから切断された場合です。キャプチャを再開するには、手動で再起動する必要があります。
- CPU 注入されたパケットは、コントロール プレーン パケットと見なされます。したがって、これらのタイプのパケットはインターフェイスの出力キャプチャではキャプチャされません。
- MAC ACL は、ARP などの非 IP パケットだけに使用されます。レイヤ 3 ポートまたは SVI ではサポートされません。
- MAC フィルタは、MAC アドレスに一致しても IP パケットをキャプチャしません。これは、すべてのインターフェイス（L2 スイッチ ポート、L3 ルーテッド ポート）に適用されます。

- MAC フィルタは、L3 インターフェイスと L2 パケット（ARP）をキャプチャすることはできません。
- IPv6 ベースの ACL は VACL ではサポートされません。
- レイヤ 2 EtherChannels はサポートされません。
- Cisco IOS リリース 16.1 以降では、レイヤ 3 PortChannel サポートが使用できます。
- キャプチャがすでにアクティブである、または開始されている場合、キャプチャ ポイント パラメータを変更することはできません。
- ACL ロギングおよび Wireshark には互換性がありません。Wireshark はアクティブになると優先されます。任意のポートにロギング中の ACL にキャプチャされているものも含めたすべてのトラフィックが Wireshark にリダイレクトされます。Wireshark を開始する前に、ACL ロギングを非アクティブにすることをお勧めします。これを実行しないと、Wireshark のトラフィックは ACL ロギング トラフィックに汚染されます。
- Wireshark は floodblock によってドロップされるパケットをキャプチャしません。
- 同じポートの PACL および RACL の両方をキャプチャすると、1 つのコピーだけが CPU に送信されます。DTLS 暗号化 CAPWAP インターフェイスをキャプチャすると、暗号化されたものと復号化されたものの 2 つのコピーが Wireshark に送信されます。DTLS 暗号化 CAPWAP トラフィックを運ぶレイヤ 2 インターフェイスをキャプチャすると同じ動作が発生します。コア フィルタは外部 CAPWAP ヘッダーに基づいています。
- Cisco IOS リリース 16.1 以降：
  - L3 ポート チャネルのサポートが追加されます。
  - 表示形式がマイナーチェンジされました。
  - cap ファイルのパケット数を表示する機能
  - キャプチャされたバッファをクリアすると、その内容とともにバッファも削除されます。パケット キャプチャがアクティブなときに実行することはできません。
  - 追加の警告メッセージが、コントロール プレーンのキャプチャで表示されます。
  - バッファ モードでは、パケットの表示は停止後のみに許可されます。
  - IP Base および IP Services にて停止のときに表示されるパケットの統計情報。
  - pcap ファイルでキャプチャされたパケット数を問い合わせる機能。
  - 表示が cap ファイルからの場合、packet-number を使用して指定されたパケットの詳細を表示できます。
  - 表示フィルタは、ファイル モードで使用可能です。
  - パケット キャプチャの統計情報（受信またはドロップされたパケットおよびバイト）は、キャプチャ中またはキャプチャ停止後のいずれかに表示できます。

- システムは、Wireshark でサポートされるように、pcap/cap ファイルの内容に関する統計情報について問い合わせることができます。
- パケット キャプチャ セッションは、バッファのサイズに関係なく常にストリーミング モードです。ロックステップ モードは使用できません。
- アクティブなキャプチャ ポイントのバッファのクリアは、内容をクリアするだけのため、LAN Base でのみサポートされています。他のすべてのライセンスでは、バッファ自体が削除されるため、キャプチャがアクティブなときに実行することはできません。

警告 コントロール プレーン パケットは、レート制限とパフォーマンスへの影響はありません。コントロールプレーンパケットのキャプチャを制限するフィルタを使用してください。

- ユーザがスイッチ ポートからルーテッド ポート（L2 > L3）へ、またはその逆へインターフェイスを変更した場合、インターフェイスが再び起動したときに、そのキャプチャ ポイントを削除し、新しいファイルを作成する必要があります。キャプチャ ポイントの停止/開始が機能しません。
- ユーザがアクティブなキャプチャ セッションで使用されたファイルを削除した場合、そのキャプチャ セッションは新しいファイルを作成できないため、キャプチャされたすべてのパケットが失われます。ユーザは、キャプチャ ポイントを再起動する必要があります。

パケット キャプチャの概要

パケット キャプチャ ツールの概要

パケットキャプチャ機能は、オンボードのパケットキャプチャ ファシリティです。ネットワーク管理者がデバイスを出入りするかデバイスを通るパケットをキャプチャすることで、パケットをローカルで分析したり、Wireshark や Embedded Packet Capture（EPC）のようなツールを使用するオフライン分析に向けてパケットを保存してエクスポートしたりできるようにするものです。この機能は、デバイスがネットワークの管理と操作にアクティブに参加できるようにすることによって、ネットワーク操作を簡略化します。この機能は、パケットの形式に関する情報を収集することによって、トラブルシューティングを容易にします。また、アプリケーションの分析とセキュリティも容易にします。

Embedded Packet Capture は LAN Base でサポートされています。Wireshark を使用する Embedded Packet Capture は、IP Base および IP Services でサポートされています。

Wireshark について

Wireshark の概要

Wireshark は、複数のプロトコルをサポートし、テキストベース ユーザ インターフェイスで情報を提供する、以前は Ethereal と呼ばれていたパケット アナライザ プログラムです。

トラフィックをキャプチャおよび分析する機能により、ネットワーク アクティビティにデータを提供します。Cisco IOS Release XE 3.3.0(SE) 以前のリリースでは、このニーズに対応したのは SPAN およびデバッグ プラットフォーム パケットの 2 つの機能だけでした。これらにはいずれも制限があります。SPAN は、パケットのキャプチャにおいては理想的ですが、指定したローカルまたはリモートの宛先にパケットを転送することによりこれを実現しているだけで、ローカル表示や分析をサポートしていません。

そのため、ハードウェアおよびソフトウェア送信トラフィックの両方に適用可能で、可能なら既知のインターフェイスを使用した高度なパケットキャプチャ、表示、および分析サポートを提供する、トラフィック キャプチャおよび分析機構のニーズが存在します。

Wireshark は、.pcap と呼ばれる既知の形式を使用してファイルへパケットをダンプし、個々のインターフェイスに対して適用されイネーブルになります。EXEC モードでインターフェイスを指定し、フィルタおよび他のパラメータも指定します。Wireshark アプリケーションは、**start** コマンドを入力した場合にだけ適用され、Wireshark が自動または手動でキャプチャを停止した場合にだけ削除されます。

（注） スイッチにインストールされている Wireshark の現在のバージョンは 1.10.8 です。

キャプチャ ポイント

キャプチャ ポイントとは、Wireshark 機能の一元的なポリシー定義です。キャプチャ ポイントは、どのパケットをキャプチャするか、どこからキャプチャするか、キャプチャ パケットに何を実行するか、およびいつ停止するかなど、Wireshark の特定のインスタンスに関連付けられたすべての特徴を説明します。キャプチャ ポイントは作成後に変更される場合があり、**start** コマンドを使用して明示的にアクティブ化しない限り、アクティブになりません。このプロセスは、キャプチャ ポイントのアクティブ化またはキャプチャ ポイントの開始といいます。キャプチャ ポイントは名前で識別され、手動または自動で非アクティブ化または停止する場合もあります。

複数のキャプチャ ポイントを定義してできますが、一度にアクティブにできるのは1つだけです。1 つ開始するには 1 つ停止する必要があります。

スタック構成のシステムの場合、キャプチャ ポイントはアクティブなメンバーによりアクティブ化されます。スイッチオーバーが発生すると、アクティブなすべてのパケット キャプチャ セッションが終了し、再起動する必要があります。

接続ポイント

接続ポイントは、キャプチャ ポイントに関連付けられた論理パケットのプロセス パスのポイントです。接続ポイントはキャプチャ ポイントの属性です。接続ポイントに影響するパケットはキャプチャ ポイント フィルタに対してテストされます。一致するパケットはキャプチャ ポイントの関連する Wireshark インスタンスにコピーされ、送信されます。特定のキャプチャ ポイントを複数の接続ポイントに関連付けることができます。異なるタイプ接続ポイントの混合に制限はありません。一部の制限は、異なるタイプの添付ポイントを指定すると適用されます。接続ポイントは、常に双方向であるレイヤ 2 VLAN の接続ポイントを除き、方向性あり（入力/出力/両方）です。

スタック型システムの場合では、すべてのスタック メンバの接続ポイントに有効です。EPC は定義されたすべての接続ポイントからパケットをキャプチャします。ただし、これらのパケットはアクティブ メンバーでのみに処理されます。

Filters

フィルタは、Wireshark にコピーされ、渡されるキャプチャ ポイントの接続ポイントを通過するトラフィックのサブセットを識別し制限するキャプチャ ポイントの属性です。Wireshark で表示されるためには、パケットは接続ポイントと、キャプチャ ポイントに関連付けられたすべてのフィルタも通過する必要があります。

キャプチャ ポイントには以下のタイプのフィルタがあります。

- コア システム フィルタ：コア システム フィルタはハードウェアによって適用され、一致基準はハードウェアによって制限されます。このフィルタは、ハードウェア転送トラフィックが Wireshark の目的でソフトウェアにコピーするかどうかを決定します。
- 表示フィルタ：表示フィルタは、Wireshark によって適用されます。表示フィルタに失敗したパケットは表示されません。

コア システム フィルタ

クラス マップまたは ACL を使用して、または CLI を使用して明示的にコア システム フィルタの一致基準を指定できます。

（注） CAPWAP を接続ポイントとして指定すると、コア システム フィルタは使用されません。

一部のインストール済み環境では、承認プロセスが長い場合さらに遅延を引き起こす可能性がある の設定を変更する権限を取得する必要があります。これにより、ネットワーク管理者の機能がトラフィックの監視および分析に制限される場合があります。この状況に対処するため、Wireshark は、EXEC モード CLI から、コア システム フィルタ一致基準の明示的な仕様をサポートします。この対処方法の欠点は、指定できる一致基準が、クラスマップがサポートする対象の限定的なサブセットである（MAC、IP 送信元アドレスおよび宛先アドレス、イーサネット タイプ、IP プロトコル、および TCP/UDP の発信元および宛先ポートなど）ことです。

コンフィギュレーション モードを使用する場合は ACL を定義するか、クラス マップでそこへキャプチャ ポイントを参照させることができます。明示的かつ ACL ベースの一致基準がクラス マップとポリシー マップの作成に内部的に使用されます。

注：ACL およびクラス マップの設定はシステムの一部であり、Wireshark 機能の側面ではありません。

Display Filter

表示フィルタを使用すると、.pcap ファイルからデコードして表示するときに表示するパケットの集合をさらに絞り込むように Wireshark に指示できます。

Actions

Wireshark はライブ トラフィックまたは前の既存 .pcap ファイルで呼び出すことができます。ライブ トラフィックに対して起動されたとき、その表示フィルタを通過するパケットに対して次の 4 種類の処理を実行できます。

- デコード、分析、保存のためにメモリ内バッファへキャプチャ
- .pcap ファイルへ保存
- デコードおよび表示
- 保存および表示

.pcap ファイルのみに対して起動された場合は、デコードと表示の処理だけが適用できます。

キャプチャ パケットのメモリ内のバッファへのストレージ

パケットは、メモリ内のキャプチャ バッファに格納して、後でデコード、分析、または .pcap ファイルへ保存できます。

キャプチャ バッファは線形モードまたは循環モードを選択できます。線形モードでは、バッファが上限に達すると、新しいパケットが廃棄されます。循環モードでは、バッファが上限に達すると、新しいパケットを格納するために最も古いパケットが廃棄されます。必要に応じてバッファをクリアすることもできますが、このモードは、ネットワーク トラフィックのデバッグに主に使用されます。ただし、これを削除せずに、バッファの内容をクリアだけすることはできません。これを有効にするためには、現行のキャプチャを停止し、キャプチャをもう一度再起動します。

（注） パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。

.pcap ファイルにキャプチャされたパケットのストレージ

（注） WireShark がスタック内のスイッチで使用される場合は、パケット キャプチャをアクティブ スイッチに接続されたフラッシュまたは USB フラッシュ デバイスにのみ保存できます。

たとえば、flash1 がアクティブなスイッチに接続されており、flash2 がセカンダリ スイッチに接続されている場合、flash1 にのみパケット キャプチャを保存できます。

アクティブ スイッチに接続されたフラッシュまたは USB フラッシュ デバイス以外のデバイスにパケット キャプチャを保存しようとすると、エラーが発生する場合があります。

Wireshark は .pcap ファイルにキャプチャされたパケットを保存できます。キャプチャ ファイルは次のストレージ デバイスに配置可能です。

- オンボード フラッシュ ストレージ（flash:）
- USB ドライブ(usbflash0:)

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

Wireshark のキャプチャ ポイントを設定する場合は、ファイル名を関連付けることができます。キャプチャ ポイントをアクティブにすると、Wireshark は指定された名前でファイルを作成し、パケットを書き込みます。キャプチャ ポイントの作成時にファイルがすでに存在する場合、Wireshark はファイルを上書きできるかどうかについて問い合わせます。キャプチャポイントの有効化時にファイルがすでに存在する場合、Wireshark は既存のファイルを上書きします。特定のファイル名には 1 つのキャプチャ ポイントのみ関連付けることができます。

Wireshark が書き込んでいるファイル システムが一杯になると、Wireshark はファイルの一部のデータで失敗します。そのため、キャプチャ セッションを開始する前に、ファイル システムに十分な領域があることを確認する必要があります。Cisco IOS Release IOS XE 3.3.0(SE) では、ファイル システムの完全なステータスは一部のストレージ デバイスに対しては検出されません。

パケット全体ではなくセグメントのみを保持して、必要な記憶域を減らすことができます。通常、最初の 64 または 128 バイトを超える詳細は不要です。デフォルトの動作は、パケット全体の保存です。

ファイルシステムを処理し、ファイルシステムへの書き込みを行う際、パケットのドロップの発生を避けるため、Wireshark ではオプションでメモリ バッファを使用してパケットの到着時に一時的に保持できます。メモリ バッファのサイズは、キャプチャ ポイントが .pcap ファイルに関連付けられる際に指定できます。

パケットのデコードおよび表示

Wireshark はコンソールにパケットをデコードして表示できます。この機能は、ライブ トラフィックに適用されるキャプチャ ポイントと前の既存 .pcap ファイルに適用されるキャプチャ ポイントで使用可能です。

（注） パケットをデコードして表示すると、CPU への負荷が高くなる場合があります。

Wireshark は、幅広い種類のパケット形式に対してパケット詳細をデコードおよび表示できます。詳細は、**monitor capture name start** コマンドを以下のキーワード オプション付きですることにより表示されます。これにより、表示およびデコード モードが開始します。

- brief：パケットごとに 1 行表示します（デフォルト）。
- detailed：プロトコルがサポートされているすべてのパケットのすべてのフィールドをデコードして表示します。詳細モードでは、他の 2 種類のモードよりも多くの CPU が必要です。
- (hexadecimal) dump：パケット データの 16 進ダンプおよび各パケットの印刷可能文字としてパケットごとに 1 行表示します。

capture コマンドをデコードおよび表示オプション付きで入力すると、Wireshark 出力が Cisco IOS に返され、変更なしでコンソールに表示されます。

ライブ トラフィックの表示

Wireshark はコア システムからパケットのコピーを受信します。Wireshark は、表示フィルタを適用して、不要なパケットを破棄し、残りのパケットをデコードおよび表示します。

.pcap ファイルの表示

Wireshark は、以前に保存された .pcap ファイルからのパケットをデコードして表示し、選択的にパケットを表示するように表示フィルタに指示できます。

パケットのストレージおよび表示

機能的には、このモードは以前の 2 種類のモードの組み合わせです。Wireshark は指定された .pcap ファイルにパケットを保存し、これらをコンソールにデコードおよび表示します。ここではコア フィルタ フィルタだけが該当します。

Wireshark キャプチャ ポイントのアクティブ化および非アクティブ化

Wireshark のキャプチャ ポイントが、接続ポイント、フィルタ、アクション、およびその他のオプションで定義された場合、Wireshark をアクティブにする必要があります。キャプチャ ポイントがアクティブになるまで、実際にパケットをキャプチャしません。

キャプチャ ポイントがアクティブになる前に、一部の機能性チェックが実行されます。キャプチャ ポイントは、コア システム フィルタと接続ポイントのどちらも定義されていない場合は

アクティブにできません。これらの要件を満たしていないキャプチャ ポイントをアクティブ化しようとすると、エラーが生成されます。*

（注） *ワイヤレス キャプチャを CAPWAP トンネリング インターフェイスで実行する場合、コア システムのフィルタは必要なく、使用することができません。

表示フィルタを、必要に応じて指定します。

Wireshark のキャプチャ ポイントはアクティブになると、複数の方法で非アクティブにできます。.pcap ファイルにパケットを格納するだけのキャプチャ ポイントは手動で停止することも、また時間制限またはパケット制限付きで設定することもでき、その後でキャプチャ ポイントは自動的に停止します。

Wireshark のキャプチャ ポイントがアクティブになると、固定レート ポリサーがハードウェアに自動的に適用され、CPU が Wireshark によって指示されたパケットでフラッディングしないようになります。レート ポリサーの短所は、リソースが使用可能な場合でも、確立されたレートを超えて連続するパケットをキャプチャできないことです。

パケット キャプチャ設定レートは、1 秒あたり 1000 パケット（pps）です。1000 pps の制限は、すべての接続ポイントの合計に適用されます。たとえば、3 つの接続ポイントにキャプチャ セッションがあれば、3 つの接続ポイントすべてのレートの合計が 1000 pps にポリシングされます。

（注） ポリサーは、コントロール プレーン パケット キャプチャではサポートされていません。コントロール プレーン キャプチャ ポイントを有効化するときは、CPU があふれないよう慎重に行う必要があります。

Wireshark 機能

ここでは、Wireshark 機能が 環境でどのように動作するかについて説明します。

- ポート セキュリティおよび Wireshark が入力キャプチャに適用された場合でも、ポート セキュリティによってドロップされたパケットは Wireshark でキャプチャされます。ポート セキュリティが入力キャプチャに適用され、Wireshark が出力キャプチャに適用された場合、ポート セキュリティによってドロップされたパケットは Wireshark ではキャプチャされません。
- ダイナミック ARP インスペクション（DAI）によってドロップされたパケットは Wireshark ではキャプチャされません。
- STP ブロック ステートのポートが接続ポイントとして使用され、コア フィルタが一致する場合、Wireshark は、パケットがスイッチにドロップされる場合でもポートに入ってくるパケットをキャプチャします。
- 分類ベースのセキュリティ機能：入力分類ベースのセキュリティ機能によってドロップされたパケット（ACL および IPSG など）は同じ層の接続ポイントに接続する Wireshark キャ

プチャポイントでは検出されません。一方、出力分類ベースのセキュリティ機能によってドロップされたパケットは、同じ層の接続ポイントに接続されている Wireshark のキャプチャ ポイントでキャッチされます。論理モデルは、Wireshark の接続ポイントが、入力側のセキュリティ機能のルックアップ後、および出力側のセキュリティ機能のルックアップ前に発生することです。

入力では、パケットはレイヤ 2 ポート、VLAN、およびレイヤ 3 ポート/SVI を介して送信されます。出力では、パケットはレイヤ 3 ポート/SVI、VLAN、およびレイヤ 2 ポートを介して送信されます。接続ポイントがパケットがドロップされるポイントの前にある場合、Wireshark はパケットをキャプチャします。これ以外の場合は、Wireshark はパケットをキャプチャしません。たとえば、入力方向のレイヤ2接続ポイントに接続される Wireshark のキャプチャ ポリシーはレイヤ3分類ベースのセキュリティ機能によってドロップされたパケットをキャプチャします。対照的に、出力方向のレイヤ 3 接続ポイントに接続する Wireshark のキャプチャ ポリシーは、レイヤ2分類ベースのセキュリティ機能によりドロップされたパケットをキャプチャします。

- ルーテッドポートおよびスイッチ仮想インターフェイス（SVIs）：SVI の出力から送信されるパケットは CPU で生成されるため、Wireshark は SVI の出力をキャプチャできません。これらのパケットをキャプチャするには、コントロールプレーンを接続ポイントとして含めます。
- VLAN：Cisco IOS リリース 16.1 以降、VLAN が Wireshark の接続ポイントとして使用されている場合、パケット キャプチャは、入力方向と出力方向の両方の L2 と L3 でサポートされます。
- リダイレクション機能：入力方向では、レイヤ3（PBR および WCCP など）でリダイレクトされる機能トラフィックは、レイヤ 3 の Wireshark の接続ポイントよりも論理的に後です。Wireshark は、後で別のレイヤ 3 インターフェイスにリダイレクトされる可能性がある場合でも、これらのパケットをキャプチャします。対照的に、レイヤ3によってリダイレクトされる出力機能（出力 WCCP など）は論理的にレイヤ3接続ポイントの前にあり、Wireshark ではキャプチャされません。
- SPAN：Wireshark は、SPAN 宛先として設定されたインターフェイスでパケットをキャプチャできません。
- SPAN：Wireshark は、入力方向の SPAN 送信元として設定されたインターフェイスでパケットをキャプチャできます。出力方向でも使用できる可能性があります。
- ACL が適用されていない場合、最大 1000 の VLAN からパケットを一度にキャプチャできます。ACL が適用されている場合、Wireshark の使用できるハードウェア領域はより少なくなります。結果として、パケット キャプチャに一度に使用できる VLAN の最大数は低くなります。1000 以上の VLAN トンネルを一度に使用したり、ACL を多数使用すると予測されない結果が生じる可能性があります。たとえば、モビリティがダウンする可能性があります。

（注） 過剰なCPU使用につながり、予測されないハードウェア動作の原因となる可能性があるため、過剰な数の接続ポイントを一度にキャプチャしないことを強くお勧めします。

Wireshark でのワイヤレス パケット キャプチャ

- ワイヤレス トラフィックはCAPWAPパケット内にカプセル化されます。ただし、CAPWAP トンネル内の特定のワイヤレス クライアントのトラフィックだけの検出は、CAPWAP トンネルを接続ポイントとして使用する場合はサポートされません。特定のワイヤレス クライアントのトラフィックだけをキャプチャするには、クライアント VLAN を接続ポイントとして使用し、それに応じてコア フィルタを設定します。
- 内部ワイヤレス トラフィックのデコードは制限付きでサポートされます。暗号化された CAPWAP トンネル内の内部ワイヤレス パケットのデコードはサポートされません。
- 同じキャプチャ ポイント上で他のインターフェイス タイプを CAPWAP トンネリング インターフェイスと併用することはできません。CAPWAP トンネリング インターフェイスおよびレベル 2 ポートは、同じキャプチャ ポイントの接続ポイントにはできません。
- CAPWAP トンネルを介して Wireshark にパケットをキャプチャする場合、コア フィルタの指定はできません。ただし、Wireshark 表示フィルタを使用して、特定のワイヤレス クライアントに対してワイヤレス クライアントをフィルタすることができます。
- ACL が適用されていない場合、最大 135 の CAPWAP トンネルからパケットを一度にキャプチャできます。ACL が適用されている場合、Wireshark の使用できるハードウェア メモリ領域はより少なくなります。結果として、パケット キャプチャに一度に使用できる CAPWAP トンネルの最大数は低くなります。一度に 135 以上の CAPWAP トンネル、または多くの ACL を使用すると予測できない結果が生じる場合があります。たとえば、モビリティがダウンする可能性があります。

（注） 過剰なCPU使用につながり、予測されないハードウェア動作の原因となる可能性があるため、過剰な数の接続ポイントを一度にキャプチャしないことを強くお勧めします。

Wireshark のガイドライン

- Wireshark でのパケット キャプチャ中に、ハードウェア転送が同時に発生します。
- Wireshark のキャプチャ プロセスを開始する前に、CPU 使用率が妥当であり、十分なメモリ（少なくとも 200 MB）が使用可能であることを確認します。
- ストレージ ファイルにパケットを保存する予定の場合、Wireshark キャプチャ プロセスを開始する前に十分なスペースが利用可能であることを確認してください。

- Wireshark のキャプチャ中の CPU 使用率は、設定された基準に一致するパケットの数と、一致したパケット用のアクション（ストア、デコードして表示、あるいはこの両方）によって異なります。
- 高 CPU 使用率および他の不要な条件を避けるため、可能な限りキャプチャを最小限に抑えてください（パケット、期間による制限）。
- パケット転送はハードウェアで通常実行されるため、パケットは、ソフトウェア処理のために CPU にコピーされません。Wireshark のパケット キャプチャの場合、パケットは CPU にコピーされ、配信されて、これが CPU 使用率の増加につながります。

  CPU 使用率を高くしないようにするには、次の手順を実行します。

  - 関連ポートだけに接続します。
  - 一致条件を表すにはクラス マップを使用し、二次的にアクセス リストを使用してください。いずれも実行可能でない場合は、明示的な、インライン フィルタを使用します。
  - フィルタ規則に正しく準拠させます。緩和されたのではなく制限的な ACL で、トラフィック タイプを（IPv4 のみなどに）制限して、不要なトラフィックを引き出します。
- パケット キャプチャを短い期間または小さなパケット番号に常に制限します。capture コマンドのパラメータにより、次を指定することができます。
  - キャプチャ期間
  - キャプチャされたパケットの数
  - ファイル サイズ
  - パケットのセグメント サイズ
- コア フィルタと一致するトラフィックが非常に少ないことが判明している場合は、制限なしでキャプチャ セッションを実行します。
- 次の場合に高い CPU（またはメモリ）使用率になる可能性があります。
  - キャプチャ セッションをイネーブルにし長期間不在のままにして、予期しないトラフィックのバーストが起きた場合。
  - リング ファイルまたはキャプチャ バッファを使用してキャプチャ セッションを起動して、長期間不在のままにすると、パフォーマンスまたはシステム ヘルスの問題が引き起こされます。
- キャプチャ セッション中に、 のパフォーマンスやヘルスに影響する可能性のある Wireshark による高い CPU 使用率およびメモリ消費がないか監視します。こうした状況が発生した場合、Wireshark セッションをすぐに停止します。
- 大きなファイルの .pcap ファイルからのパケットをデコードして表示することは避けてください。代わりに、PC に .pcap ファイルを転送し PC 上で Wireshark を実行します。

- Wireshark インスタンスは最大 8 個まで定義できます。 .pcap ファイルまたはキャプチャ バッファからパケットをデコードして表示するアクティブな **show** コマンドは、1 個のインスタンスとしてカウントされます。ただし、アクティブにできるインスタンスは1つだけです。
- 実行中のキャプチャに関連付けられた ACL が変更された場合は常に、ACL 変更を有効にするにはキャプチャを再起動する必要があります。キャプチャを再起動しないと、変更前の元の ACL が継続して使用されます。
- パケット損失を防ぐには、次の点を考慮します。
  - ライブ パケットをキャプチャしている間は、CPU に負荷のかかる操作であるデコードと表示ではなく（特に detailed モードの場合）、保存のみを使用します（display オプションを指定しない場合）。
  - パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。
  - デフォルト バッファ サイズを使用し、パケットが失われている場合、バッファ サイズを増加してパケットの喪失を防ぐことができます。
  - フラッシュ ディスクへの書き込みは、CPU に負荷のかかる操作であるため、キャプチャ レートが不十分な場合、バッファ キャプチャの使用をお勧めします。
  - Wireshark キャプチャ セッションは 1000 pps のレートで常にストリーミング モードで動作します。
- ストリーミング キャプチャ モードのレートは 1000 pps です。
- コンソール ウィンドウのライブ パケットをデコードして表示する場合は、Wireshark セッションが短いキャプチャ期間によって抑制されていることを確認します。

警告 期間制限がより長いまたはキャプチャ期間がない（**term len 0** コマンドを使用して auto-more サポートのない端末を使用した）Wireshark セッションでは、コンソールまたは端末が使用できなくなる場合があります。

- 高 CPU 使用率につながるライブ トラフィックのキャプチャに Wireshark を使用している場合、QoS ポリシーを一時的に適用して、キャプチャ プロセスが終了するまで実際のトラフィックを制限することを考慮してください。
- すべての Wireshark 関連のコマンドは EXEC モードで、コンフィギュレーション コマンドは、Wireshark にありません。

  Wireshark CLI でアクセス リストまたはクラス マップを使用する必要がある場合は、コンフィギュレーション コマンドでアクセス リストおよびクラス マップを定義する必要があります。
- 特定の順序はキャプチャ ポイントを定義する場合には適用されません。CLI で許可されている任意の順序でキャプチャ ポイント パラメータを定義できます。Wireshark CLI では、

単一行のパラメータ数に制限はありません。これはキャプチャ ポイントを定義するために必要なコマンドの数を制限します。

- 接続ポイントを除くすべてのパラメータは、単一の値を取ります。通常、コマンドを再入力することにより、値を新しいものに置き換えることができます。ユーザの確認後にシステムが新しい値を受け入れ、古い値を上書きします。コマンドの **no** 形式は、新しい値の入力には必要はありませんが、パラメータの削除には必要です。
- Wireshark では 1 つ以上の接続ポイントを指定することができます。複数の接続ポイントを追加するには、新しい接続ポイントでコマンドを再入力します。接続ポイントを削除するには、コマンドの **no** 使用します。接続ポイントとしてインターフェイス範囲を指定できます。たとえば、**monitor capture mycap interface GigabitEthernet1/0/1 in** を入力します。ここではインターフェイス GigabitEthernet1/0/1 が接続ポイントです。

  またインターフェイス GigabitEthernet1/0/2 にも接続する必要がある場合、次のように、別の行で指定します。

  monitor capture mycap interface GigabitEthernet1/0/2 in

- キャプチャがアクティブなときは、キャプチャに対する変更を行うことはできません。
- 実行する処理は、いずれのパラメータが必須であるかを決定します。Wireshark CLI では、**start** コマンドを入力する前に任意のパラメータを指定または変更することができます。**start** コマンドを入力すると、すべての必須パラメータが入力されたと判断した後にのみ Wireshark が開始します。
- キャプチャ ポイントの作成時にファイルがすでに存在する場合、Wireshark はファイルを上書きできるかどうかについて問い合わせます。キャプチャポイントの有効化時にファイルがすでに存在する場合、Wireshark は既存のファイルを上書きします。
- コア フィルタは明示的なフィルタ、アクセス リスト、またはクラス マップにできます。これらのタイプの新しいフィルタを指定すると、既存のものを置き換えます。

  （注） コア フィルタは、CAPWAP トンネル インターフェイスをキャプチャ ポイントの接続ポイントとして使用している場合を除き、必須です。

- 明示的な **stop** コマンドを使用するか、automore モードに **q** を入力して、Wireshark のセッションを終了します。セッションは、期間やパケット キャプチャの制限などの停止の条件が満たされたときに、自動的に終了します。
- ドロップされたパケットはキャプチャの最後に表示されません。ただし、ドロップされたサイズ超過のパケット数のみが表示されます。

デフォルトの Wireshark の設定

次の表は、デフォルトの Wireshark の設定を示しています。

機能	デフォルト設定
持続時間	No limit
Packets	No limit
パケット長	制限なし（フル パケット）
ファイル サイズ	No limit
リング ファイル ストレージ	なし
バッファのストレージ モード	線形

組み込みパケット キャプチャについて

組み込みパケット キャプチャの概要

組み込みパケット キャプチャ（EPC）は、パケットのトレースとトラブルシューティングに役立つ組み込みシステム管理機能を提供します。この機能を使用すると、ネットワーク管理者は、シスコ デバイスを出入りするか通過するデータ パケットをキャプチャできます。ネットワーク管理者は、キャプチャ バッファ サイズとタイプ（循環またはリニア）およびキャプチャする各パケットの最大バイト数を定義する場合があります。パケット キャプチャ レートは、詳細な管理制御を使用してスロットリングできます。たとえば、アクセス コントロール リストを使用してキャプチャ対象パケットをフィルタリングするオプションや、最大パケット キャプチャ レートまたはサンプリング間隔の指定などの詳細な定義を行うオプションが利用できます。

組み込みパケット キャプチャの利点

- デバイスで IPv4 および IPv6 パケットをキャプチャでき、MAC フィルタを使用したり、MAC アドレスをマッチさせたりして、非 IP パケットもキャプチャ可能。
- パケット キャプチャ ポイントをイネーブルにする拡張可能なインフラストラクチャキャプチャ ポイントは、パケットがキャプチャされ、バッファと関連付けられるトラフィック トランジット ポイントです。
- 外部ツールを使用した分析に適したパケット キャプチャ ファイル（PCAP）形式でパケット キャプチャをエクスポートする機能。
- さまざまな詳細レベルでキャプチャされたデータ パケットをデコードする方法。

パケット データ キャプチャ

パケット データ キャプチャは、バッファに格納されるデータ パケットのキャプチャです。パケット データ キャプチャは、一意の名前とパラメータを入力することによって定義します。

こうしたキャプチャでは、次のアクションを実行できます。

- インターフェイスでのキャプチャのアクティブ化。

- キャプチャ ポイントへのアクセス コントロール リスト（ACL）やクラス マップの適用。

（注） Network Based Application Recognition（NBAR）と MAC スタイルのクラス マップは、サポートされていません。

- キャプチャの破棄。
- サイズやタイプなどのバッファ ストレージ パラメータの指定。サイズの範囲は 1 ～ 100 MB です。デフォルトのバッファは線形です。もう 1 つのバッファ オプションは循環です。
- プロトコル、IP アドレス、ポート アドレスに関する情報を含む一致基準の指定。

パケット キャプチャの設定

Wireshark の設定方法

Wireshark を設定するには、次の基本的な手順を実行します。

1. キャプチャ ポイントを定義します。
2. （任意）キャプチャ ポイントのパラメータを追加または変更します。
3. キャプチャ ポイントをアクティブ化または非アクティブ化します。
4. キャプチャ ポイントを今後使用しない場合は削除します。

キャプチャ ポイントの定義

この手順の例では、非常にシンプルなキャプチャ ポイントを定義します。必要に応じて、**monitor capture** コマンドの 1 つのインスタンスを使用してキャプチャ ポイントとそのすべてのパラメータを定義できます。

（注） 接続ポイント、キャプチャの方向、およびコア フィルタが機能するキャプチャ ポイントを持つよう定義する必要があります。

コア フィルタを定義する必要がないのは、CAPWAP トンネリング インターフェイスを使用してワイヤレス キャプチャ ポイントを定義する場合です。この場合、コア フィルタは定義しません。これは使用できません。

キャプチャ ポイントを定義するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show capwap summary** 例： `Device# show capwap summary`	ワイヤレス キャプチャの接続ポイントとして使用できる CAPWAP トンネルを表示します。 （注） このコマンドは、ワイヤレス キャプチャを実行するために CAPWAP トンネルを接続ポイントとして使用している場合にのみ使用します。例の項の CAPWAP の例を参照してください。
ステップ 3	**monitor capture** {*capture-name*interface-*type*interface-*id*} {**interface** | **control-plane**} {**in** | **out** | **both**} 例： `Device# monitor capture mycap interface GigabitEthernet1/0/1 in`	キャプチャ ポイントを定義し、キャプチャ ポイントが関連付けられている接続ポイントを指定し、キャプチャの方向を指定します。 キーワードの意味は次のとおりです。 • *capture-name*：定義するキャプチャ ポイントの名前を指定します（例では mycap が使用されています）。キャプチャ名の長さは8文字以下にしてください。英数字、アンダースコア（_）のみが許可されます • （任意）**interface** *interface-type interface-id*：キャプチャ ポイントが関連付けられる接続ポイントを指定します（例では GigabitEthernet1/0/1 が使用されています）。

	コマンドまたはアクション	目的
		（注） オプションで、このコマンド インスタンス 1 つでこのキャプチャ ポイントの複数の接続ポイントおよびパラメータすべてを定義できます。これらのパラメータについては、キャプチャ ポイント パラメータの変更に関する手順で説明されています。範囲のサポートは、接続ポイントを追加および削除するためにも使用できます。 *interface-type* には次のいずれかを使用します。 • **GigabitEthernet**：接続ポイントを GigabitEthernet として指定します。 • **vlan**：接続ポイントを VLAN として指定します。 （注） このインターフェイスを接続ポイントとして使用する場合は、入力キャプチャのみが可能です。 • **capwap**：接続ポイントを CAPWAP トンネルとして指定します。 （注） このインターフェイスを接続ポイントとして使用すると、コア フィルタは使用できません。 • （任意）**control-plane**：接続ポイントとしてコントロール プレーンを指定します。

	コマンドまたはアクション	目的
		• **in** | **out** | **both**：キャプチャの方向を指定します。
ステップ 4	**monitor capture** {*capture-name*}[**match** {**any** | **ipv4 any any** | **ipv6**} **any any**}] 例： `Device# monitor capture mycap interface GigabitEthernet1/0/1 in match any`	コア システムのフィルタを定義します。 （注） コア フィルタが使用できなくなるため、CAPWAP のトンネリング インターフェイスを接続ポイントとして使用する場合はこの手順を実行しないでください。 キーワードの意味は次のとおりです。 • *capture-name*：定義するキャプチャ ポイントの名前を指定します（例では mycap が使用されています）。 • **match**：フィルタを指定します。定義されている最初のフィルタはコア フィルタです。 （注） キャプチャ ポイントは、コア システム フィルタと接続ポイントのどちらも定義されていない場合はアクティブにできません。これらの要件を満たしていないキャプチャ ポイントをアクティブ化しようとすると、エラーが生成されます。 • **ipv4**：IP バージョン 4 のフィルタを指定します。 • **ipv6**：IP バージョン 6 のフィルタを指定します。

ステップ 5	**show monitor capture** {*capture-name*}[**parameter**]
	例：
	`Device# show monitor capture mycap parameter`
	`monitor capture mycap interface GigabitEthernet1/0/1 in`
	`monitor capture mycap match any`
		ステップ 2 で定義したキャプチャ ポイント パラメータを表示し、キャプチャ ポイントを定義したことを確認します。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

例

CAPWAP 接続ポイントでキャプチャ ポイントを定義するには次を実行します。

```
Device# show capwap summary

CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 1
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0


Name   APName                           Type PhyPortIf Mode      McastIf
------ ------------------------------- ---- --------- --------- -------
Ca0    AP442b.03a9.6715                 data Gi3/0/6   unicast   -


Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU   Xact
------ --------------- ------- --------------- ------- ------ ----- ----
Ca0    10.10.14.32     5247    10.10.14.2      38514   No     1449  0

Device# monitor capture mycap interface capwap 0 both
Device# monitor capture mycap file location flash:mycap.pcap
Device# monitor capture mycap file buffer-size 1
Device# monitor capture mycap start

*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on

Device# show monitor capture mycap parameter
   monitor capture mycap interface capwap  0 in
   monitor capture mycap interface capwap  0 out
   monitor capture mycap file location flash:mycap.pcap buffer-size 1
Device#
Device# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
```

```
  Filter Details:
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
Device#
Device# show monitor capture file flash:mycap.pcap
  1   0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  2   0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  3   2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  4   2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  5   3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  6   4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  7   4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  8   5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  9   5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 10   6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 11   8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 12   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 13   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 14   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 15   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 16   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 17   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 18   9.236987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 19  10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 20  10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 21  12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 22  12.239993   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 23  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 24  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 25  12.250994   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 26  12.256990   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 27  12.262987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 28  12.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 29  12.802012   10.10.14.3 -> 10.10.14.255 NBNS Name query NB WPAD.<00>
 30  13.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
```

次のタスク

さらなる接続ポイントを追加して、キャプチャ ポイントのパラメータを変更し、アクティブ化できます。または、キャプチャ ポイントをそのまま使用したい場合はすぐにアクティブ化することもできます。

（注） このトピックで説明されているメソッドを使用してキャプチャ ポイントのパラメータを変更することはできません。

ユーザが誤ったキャプチャ名、または無効/存在しない接続ポイントを入力すると、スイッチは、「Capture Name should be less than or equal to 8 characters.Only alphanumeric characters and underscore (_) is permitted」および「% Invalid input detected at '^' marker」のようなエラーを表示します。

キャプチャ ポイント パラメータの追加または変更

パラメータの値を指定する手順は、順番にリストされますが、任意の順序で実行できます。1行、2行、または複数行で指定できます。複数指定が可能な接続ポイントを除き、同じオプションを再定義することで、任意の値をより最近の値に置き換えることができます。すでに指定された特定のパラメータが変更されている場合は、インタラクティブに確認する必要があります。

キャプチャ ポイントのパラメータを変更するには、次の手順を実行します。

始める前に

以下の手順を実行する前にキャプチャ ポイントを定義する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture** {*capture-namemac-match-string*} **match** {**any** | **mac** | **ipv4** {**any** | **host** | **protocol**}{**any** | **host**} | **ipv6** {**any** | **host** | **protocol**}{**any** | **host**}}	明示的に、または ACL を介して、またはクラス マップを介して定義されたコア システム フィルタ（**ipv4 any any**）を定義します。

	コマンドまたはアクション	目的
	例： `Device# monitor capture mycap match ipv4 any any`	（注） CAPWAP トンネリング インターフェイスを使用してワイヤレス キャプチャを定義している場合、このコマンドには効果がないので使用しないでください。
ステップ 3	**monitor capture** {*capture-namesecondssizenum*} **limit** {[**duration**][**packet-length**][**packets**]} 例： `Device# monitor capture mycap limit duration 60 packet-len 400`	秒単位のセッション制限（60）、キャプチャされたパケット、または Wireshark によって保持されるパケット セグメント長（400）を指定します。
ステップ 4	**monitor capture** {*capture-name*} **file** {**location** *filename*} 例： `Device# monitor capture mycap file location flash:mycap.pcap`	キャプチャ ポイントがパケットを表示するだけでなくキャプチャできるようにする場合は、ファイルのアソシエーションを指定します。 （注） すでにファイルが存在する場合、それが上書きが可能かどうかを確認する必要があります。 （注） ファイル オプションは、LAN Base ライセンスには存在しません。
ステップ 5	**monitor capture** {*capture-namesize*} **file** {**buffer-size** } 例： `Device# monitor capture mycap file buffer-size 100`	トラフィック バーストの処理に Wireshark で使用されるメモリ バッファのサイズを指定します。

ステップ 6	**show monitor capture** {*capture-name*}[**parameter**]
	例：
	`Device# show monitor capture mycap parameter`
	`monitor capture mycap interface GigabitEthernet1/0/1 in`
	`monitor capture mycap match ipv4 any any`
	`monitor capture mycap limit duration 60 packet-len 400`
	`monitor capture point mycap file`
		以前に定義したキャプチャ ポイント パラメータを表示します。

	コマンドまたはアクション	目的
	`location bootdisk:mycap.pcap monitor capture mycap file buffer-size 100`	
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

例

パラメータの変更

キャプチャ ファイルの関連付けまたは関連付け解除

```
Device# monitor capture point mycap file location flash:mycap.pcap
Device# no monitor capture mycap file
```

パケット バーストの処理にメモリ バッファ サイズを指定する

```
Device# monitor capture mycap buffer size 100
```

IPv4 と IPv6 の両方に一致するように、明示的なコア システム フィルタを定義する

```
Device# monitor capture mycap match any
```

次のタスク

キャプチャ ポイントに必要なパラメータがすべて含まれている場合はアクティブ化します。

キャプチャ ポイント パラメータの削除

順番に表示されていますが、パラメータを削除する手順は任意の順序で実行できます。1 行、2 行、または複数行で削除できます。複数が可能な接続ポイントを除いて、任意のパラメータを削除できます。

キャプチャ ポイントのパラメータを削除するには、次の手順を実行します。

始める前に

キャプチャ ポイント パラメータは、以下の手順を使用して削除する前に定義する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**no monitor capture** {*capture-name*} **match** 例： `Device# no monitor capture mycap match`	キャプチャ ポイント（mycap）で定義されているすべてのフィルタを削除します。

ステップ 3	**no monitor capture** {*capture-name*} **limit** [**duration**] [**packet-length**] [**packets**]
	例：
	`Device# no monitor capture mycap limit duration packet-len`
	`Device# no monitor capture mycap limit`
		Wireshark によって保持されるセッション タイム制限およびパケット セグメント長を削除します。その他の指定された制限はそのままになります。
		Wireshark のすべての制限をクリアします。

ステップ 4	**no monitor capture** {*capture-name*} **file** [**location**] [**buffer-size**]
	例：
	`Device# no monitor capture mycap file`
	`Device# no monitor capture mycap file location`
		ファイルの関連付けを削除します。キャプチャ ポイントはパケットをキャプチャしなくなります。表示だけが実行されます。
		ファイル位置の関連付けを削除します。ファイル位置はキャプチャ ポイントとは関連付けられなくなります。ただし、他の定義されたファイル関連付けはこのアクションによっては影響を受けません。

ステップ 5	**show monitor capture** {*capture-name*} [**parameter**]
	例：
	`Device# show monitor capture mycap parameter`
	`monitor capture mycap interface GigabitEthernet1/0/1 in`
		パラメータの削除操作後にまだ定義されているキャプチャ ポイント パラメータを表示します。このコマンドは、キャプチャ ポイントと関連付けられるパラメータを確認するために手順の任意の地点で実行できます。

ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

次のタスク

キャプチャ ポイントに必要なパラメータがすべて含まれている場合はアクティブ化します。

（注） キャプチャ ポイントがアクティブなときにパラメータが削除されると、スイッチは「キャプチャがアクティブです（Capture is active）」というエラーを表示します。

キャプチャ ポイントの削除

キャプチャ ポイントを削除するには、次の手順を実行します。

始める前に

キャプチャ ポイントは、以下の手順を使用して削除する前に定義する必要があります。削除する前に、キャプチャ ポイントを停止する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**no monitor capture** {*capture-name*} 例： `Device# no monitor capture mycap`	指定されたキャプチャ ポイント（mycap）を削除します。

ステップ 3	**show monitor capture** {*capture-name*} [**parameter**]
	例：
	`Device# show monitor capture mycap parameter`
	`Capture mycap does not exist`
		指定されたキャプチャ ポイントは削除されたため存在しないことを示すメッセージを表示します。

ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

削除したものと同じ名前の新規キャプチャ ポイントを定義できます。これらの手順は通常、キャプチャ ポイントの定義をやり直したい場合に実行します。

キャプチャ ポイントをアクティブまたは非アクティブにする

キャプチャ ポイントをアクティブまたは非アクティブにするには、次の手順を実行します。

始める前に

接続ポイントおよびコア システム フィルタが定義され、関連付けられたファイル名がすでに存在する場合でも、キャプチャ ポイントはアクティブ化することができます。このようなケースでは、既存のファイルは上書きされます。

関連するファイル名のないキャプチャ ポイントは、表示するためだけにアクティブにできます。ファイル名が指定されていないと、パケットはバッファに保管されます。ライブ表示（キャプチャ時の表示）は、ファイルおよびバッファ モードの両方で使用できます。

表示フィルタを指定しない場合、パケットはライブ表示されず、コア システム フィルタによってキャプチャされたすべてのパケットが表示されます。デフォルトの表示モードはbriefです。

（注） CAPWAP のトンネリング インターフェイスを接続ポイントとして使用すると、コア フィルタは使用されないため、この場合は定義する必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**monitor capture** {*capture-name*} **start** [**display** [**display-filter** *filter-string*]] [**brief** | **detailed** | **dump**] 例： `Device# monitor capture mycap start display display-filter "stp"`	キャプチャポイントをアクティブ化し、「stp」を含むパケットだけが表示されるように表示をフィルタします。
ステップ 3	**monitor capture** {*capture-name*} **stop** 例： `Device# monitor capture name stop`	キャプチャ ポイントを非アクティブにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

キャプチャポイントをアクティブおよび非アクティブにする際に、いくつかのエラーが発生する可能性があります。次に、発生する可能性のあるエラーのいくつかの例を示します。

アクティブ化する際に接続ポイントが不明

```
Switch#monitor capture mycap match any
Switch#monitor capture mycap start
No Target is attached to capture failed to disable provision featurefailed to remove
policyfailed to disable provision featurefailed to remove policyfailed to disable provision
 featurefailed to remove policy
Capture statistics collected at software (Buffer):
 Capture duration - 0 seconds
 Packets received - 0
 Packets dropped - 0
 Packets oversized - 0

Unable to activate Capture.
```

```
Switch# unable to get action unable to get action unable to get action
Switch#monitor capture mycap interface g1/0/1 both
Switch#monitor capture mycap start
Switch#
*Nov 5 12:33:43.906: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

アクティブ化する際にフィルタが不明

```
Switch#monitor capture mycap int g1/0/1 both
Switch#monitor capture mycap start
Filter not attached to capture
Capture statistics collected at software (Buffer):
 Capture duration - 0 seconds
 Packets received - 0
 Packets dropped - 0
 Packets oversized - 0

Unable to activate Capture.
Switch#monitor capture mycap match any
Switch#monitor capture mycap start
Switch#
*Nov 5 12:35:37.200: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

キャプチャ ポイントがすでにアクティブ化されているのに、別のキャプチャ ポイントをアクティブ化しようとする

```
Switch#monitor capture mycap start
PD start invoked while previous run is active Failed to start capture : Wireshark operation
 failure
Unable to activate Capture.
Switch#show monitor capture

Status Information for Capture test
 Target Type:
 Interface: GigabitEthernet1/0/13, Direction: both
 Interface: GigabitEthernet1/0/14, Direction: both
 Status : Active
 Filter Details:
 Capture all packets
 Buffer Details:
 Buffer Type: LINEAR (default)
 Buffer Size (in MB): 10
 File Details:
 Associated file name: flash:cchh.pcap
 Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Maximum number of packets to capture per second: 1000
 Packet sampling rate: 0 (no sampling)

Status Information for Capture mycap
 Target Type:
 Interface: GigabitEthernet1/0/1, Direction: both
 Status : Inactive
 Filter Details:
 Capture all packets
 Buffer Details:
 Buffer Type: LINEAR (default)
 Buffer Size (in MB): 10
 File Details:
 File not associated
 Limit Details:
 Number of Packets to capture: 0 (no limit)
```

```
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Maximum number of packets to capture per second: 1000
 Packet sampling rate: 0 (no sampling)
Switch#monitor capture test stop
Capture statistics collected at software (Buffer & Wireshark):
 Capture duration - 157 seconds
 Packets received - 0
 Packets dropped - 0
 Packets oversized - 0

Switch#
*Nov 5 13:18:17.406: %BUFCAP-6-DISABLE: Capture Point test disabled.
Switch#monitor capture mycap start
Switch#
*Nov 5 13:18:22.664: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
Switch#
```

キャプチャ ポイント バッファのクリア

次の手順に従ってバッファ コンテンツをクリアするか、外部ファイルにストレージとして保存します。

（注） パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。アクティブなキャプチャ ポイントのバッファをクリアしないでください。

（注） アクティブなキャプチャ ポイントのバッファのクリアは、内容をクリアするだけのため、LAN Base でのみサポートされています。他のすべてのライセンスでは、バッファ自体が削除されるため、キャプチャがアクティブなときに実行することはできません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**monitor capture** {*capture-name*} [**clear** | **export** *filename*] 例： `Device# monitor capture mycap clear`	clear：完全にバッファを削除します。 （注） clear コマンドを実行すると、 • LAN Base では、このコマンドはバッファを削除せずにバッファの内容をクリアします。 • 他のすべてのライセンスでは、このコマンドはバッファ自体を削除します。 export：バッファでキャプチャされたパケットを保存し、バッファを削除します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

例：キャプチャ ポイント バッファの処理

キャプチャのファイルへのエクスポート

```
Device# monitor capture mycap export flash:mycap.pcap
Storage configured as File for this capture
```

キャプチャ ポイント バッファのクリア

```
Device# monitor capture mycap clear

 Capture configured with file options
```

次のタスク

（注） LAN Base 以外のライセンスでキャプチャ ポイントのバッファをクリアしようとすると、スイッチは「*Failed to clear capture buffer : Capture Buffer BUSY*」エラーを表示します。

組み込みパケット キャプチャの実装方法

パケット データ キャプチャの管理

（注） アクティブなキャプチャ ポイントのエクスポートは、LAN Base ライセンスのみでサポートされています。他のすべてのライセンスでは、まずキャプチャを停止してからエクスポートをする必要があります。

バッファ モードでパケット データ キャプチャを管理するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture** *capture-name* **access-list** *access-list-name* 例： `Device# monitor capture mycap access-list v4acl`	アクセス リストをパケット キャプチャのコア フィルタとして指定し、モニタ キャプチャを設定します。
ステップ 3	**monitor capture** *capture-name* **limit duration** *seconds* 例： `Device# monitor capture mycap limit duration 1000`	モニタ キャプチャの制限を設定します。

	コマンドまたはアクション	目的
ステップ 4	**monitor capture** *capture-name* **interface** *interface-name* **both** 例： `Device# monitor capture mycap interface GigabitEthernet 0/0/1 both`	接続ポイントおよびパケット フロー方向を指定して、モニタ キャプチャを設定します。
ステップ 5	**monitor capture** *capture-name* **buffer circular size** *bytes* 例： `Device# monitor capture mycap buffer circular size 10`	パケット データをキャプチャするようにバッファを設定します。
ステップ 6	**monitor capture** *capture-name* **start** 例： `Device# monitor capture mycap start`	トラフィック トレース ポイントでパケットデータのバッファへのキャプチャを開始します。
ステップ 7	**monitor capture** *capture-name* **stop** 例： `Device# monitor capture mycap stop`	トラフィック トレース ポイントでパケット データのキャプチャを停止します。
ステップ 8	**monitor capture** *capture-name* **export** *file-location/file-name* 例： `Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap`	分析のためにキャプチャされたデータをエクスポートします。
ステップ 9	**end** 例： `Device# end`	特権 EXEC モードに戻ります。

次のタスク

（注） LAN Base 以外のライセンスでアクティブなキャプチャ ポイントをエクスポートしようとすると、スイッチは、「Failed to Export : Capture Buffer BUSY」というエラーを表示します。

キャプチャされたデータのモニタリングとメンテナンス

キャプチャされたパケットデータのモニタリングとメンテナンスを行うには、次の作業を実行します。キャプチャ バッファの詳細とキャプチャ ポイントの詳細を表示します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show monitor capture** *capture-buffer-name* **buffer dump** 例： `Device# show monitor capture mycap buffer dump`	（任意）キャプチャ パケットの 16 進数ダンプおよびそのメタデータを表示します。
ステップ 3	**show monitor capture** *capture-buffer-name* **parameter** 例： `Device# show monitor capture mycap parameter`	（任意）キャプチャを指定するために使用されたコマンドのリストを表示します。
ステップ 4	**debug epc capture-point** 例： `Device# debug epc capture-point`	（任意）パケット キャプチャ ポイントのデバッグをイネーブルにします。
ステップ 5	**debug epc provision** 例： `Device# debug epc provision`	（任意）パケット キャプチャ プロビジョニングのデバッグをイネーブルにします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

パケット キャプチャのモニタリング

Wireshark の設定例

例：.pcap ファイルからの概要出力の表示

次のように入力して、.pcap ファイルからの出力を表示できます。

```
Device# show monitor capture file flash:mycap.pcap brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=0/0, ttl=254
  2 0.000051000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=0/0, ttl=255 (request in 1)
  3 0.000908000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=1/256, ttl=254
  4 0.001782000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=1/256, ttl=255 (request in 3)
  5 0.002961000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=2/512, ttl=254
  6 0.003676000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=2/512, ttl=255 (request in 5)
  7 0.004835000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=3/768, ttl=254
  8 0.005579000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=3/768, ttl=255 (request in 7)
  9 0.006850000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=4/1024, ttl=254
 10 0.007586000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=4/1024, ttl=255 (request in 9)
 11 0.008768000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=5/1280, ttl=254
 12 0.009497000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=5/1280, ttl=255 (request in 11)
 13 0.010695000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=6/1536, ttl=254
 14 0.011427000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=6/1536, ttl=255 (request in 13)
 15 0.012728000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=7/1792, ttl=254
 16 0.013458000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=7/1792, ttl=255 (request in 15)
 17 0.014652000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=8/2048, ttl=254
 18 0.015394000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=8/2048, ttl=255 (request in 17)
 19 0.016682000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=9/2304, ttl=254
 20 0.017439000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=9/2304, ttl=255 (request in 19)
 21 0.018655000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=10/2560, ttl=254
 22 0.019385000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=10/2560, ttl=255 (request in 21)
 23 0.020575000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
```

```
seq=11/2816, ttl=254
 --More‹
```

例：.pcap ファイルからの詳細出力の表示

次のように入力して、.pcap ファイルの出力詳細を表示できます。

```
Device# show monitor capture file flash:mycap.pcap detailed
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  6, 2015 11:44:48.322497000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1446810288.322497000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 114 bytes (912 bits)
    Capture Length: 114 bytes (912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:icmp:data]
Ethernet II, Src: Cisco_f3:63:46 (00:e1:6d:f3:63:46), Dst: Cisco_31:f1:c6
(00:e1:6d:31:f1:c6)
    Destination: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        Address: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        Address: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not
ECN-Capable Transport))
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport)
 (0x00)
    Total Length: 100
    Identification: 0x04ba (1210)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
    Header checksum: 0x8fc8 [validation disabled]
        [Good: False]
        [Bad: False]
    Source: 10.10.10.2 (10.10.10.2)
    Destination: 10.10.10.1 (10.10.10.1)
Internet Control Message Protocol
```

```
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe4db [correct]
    Identifier (BE): 46 (0x002e)
    Identifier (LE): 11776 (0x2e00)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    Data (72 bytes)

0000  00 00 00 00 09 c9 8f 77 ab cd ab cd ab cd ab cd   .......w........
0010  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0020  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0030  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0040  ab cd ab cd ab cd ab cd                           ........
        Data: 0000000009c98f77abcdabcdabcdabcdabcdabcdabcdabcd...
        [Length: 72]

Frame 2: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
    Interface id: 0
```

例：.pcap ファイルからパケット ダンプ出力の表示

次のように入力して、パケット ダンプの出力を表示できます。

```
Device# show monitor capture file flash:mycap.pcap dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0000  00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00   ..m1....m.cF..E.
0010  00 64 04 ba 00 00 fe 01 8f c8 0a 0a 0a 02 0a 0a   .d..............
0020  0a 01 08 00 e4 db 00 2e 00 00 00 00 00 00 09 c9   ................
0030  8f 77 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   .w..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd                                             ..

0000  00 e1 6d 31 f1 80 00 e1 6d 31 f1 80 08 00 45 00   ..m1....m1....E.
0010  00 64 04 ba 00 00 ff 01 8e c8 0a 0a 0a 01 0a 0a   .d..............
0020  0a 02 00 00 ec db 00 2e 00 00 00 00 00 00 09 c9   ................
0030  8f 77 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   .w..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd                                             ..

0000  00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00   ..m1....m.cF..E.
0010  00 64 04 bb 00 00 fe 01 8f c7 0a 0a 0a 02 0a 0a   .d..............
0020  0a 01 08 00 e4 d7 00 2e 00 01 00 00 00 00 09 c9   ................
0030  8f 7a ab cd ab cd ab cd ab cd ab cd ab cd ab cd   .z..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
```

例：表示フィルタを使用した .pcap ファイルからのパケットの表示

次のように入力して、出力された .pcap ファイルのパケットを表示できます。

```
Device# show monitor capture file flash:mycap.pcap display-filter "ip.src == 10.10.10.2"
 brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
```

```
  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=0/0, ttl=254
  3 0.000908000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=1/256, ttl=254
  5 0.002961000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=2/512, ttl=254
  7 0.004835000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=3/768, ttl=254
  9 0.006850000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=4/1024, ttl=254
 11 0.008768000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=5/1280, ttl=254
 13 0.010695000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=6/1536, ttl=254
 15 0.012728000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=7/1792, ttl=254
 17 0.014652000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=8/2048, ttl=254
 19 0.016682000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=9/2304, ttl=254
 21 0.018655000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=10/2560, ttl=254
 23 0.020575000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=11/2816, ttl=254
```

例：.pcap ファイルにキャプチャされたパケットの数を表示

次のように入力して、.pcap ファイルにキャプチャされたパケットの数を表示できます。

```
Device# show monitor capture file flash:mycap.pcap packet-count
File name:           /flash/mycap.pcap
Number of packets:   50
```

例：.pcap ファイルから単一パケット ダンプの表示

次のように入力して、.pcap ファイルから単一のパケット ダンプを表示できます。

```
Device#  show monitor capture file flash:mycap.pcap packet-number 10 dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0000  00 e1 6d 31 f1 80 00 e1 6d 31 f1 80 08 00 45 00   ..m1....m1....E.
0010  00 64 04 be 00 00 ff 01 8e c4 0a 0a 0a 01 0a 0a   .d..............
0020  0a 02 00 00 ec ce 00 2e 00 04 00 00 00 00 09 c9   ................
0030  8f 80 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd
```

例：.pcap ファイルにキャプチャされたパケットの統計情報を表示

次のように入力して、.pcapファイルにキャプチャされたパケットの統計情報を表示できます。

```
Device# show monitor capture file flash:mycap.pcap statistics "h225,counter"
================== H225 Message and Reason Counter ==================
RAS-Messages:
Call Signalling:
=====================================================================
```

例：単純なキャプチャおよび表示

次の例は、レイヤ 3 インターフェイス ギガビット イーサネット 1/0/1 でトラフィックをモニタする方法を示しています。

ステップ 1：次のように入力して関連トラフィックで一致するキャプチャ ポイントを定義します。

```
Device# monitor capture mycap interface GigabitEthernet1/0/3 in
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap limit duration 60 packets 50
Device# monitor capture mycap buffer size 100
```

CPU 使用率の上昇を避けるため、制限として最も低いパケット数および時間が設定されています。

ステップ 2：次のように入力してキャプチャ ポイントが正確に定義されていることを確認します。

```
Device# show monitor capture mycap parameter
      monitor capture mycap interface GigabitEthernet1/0/3 in
   monitor capture mycap match ipv4  any any
   monitor capture mycap buffer size 100
   monitor capture mycap limit packets 50 duration 60

Device# show monitor capture mycap
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 100
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 50
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：キャプチャ プロセスを開始し、結果を表示します。

```
Device# monitor capture mycap start display
 Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1   0.000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=0/0, ttl=254
  2   0.003682   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=1/256, ttl=254
  3   0.006586   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=2/512, ttl=254
  4   0.008941   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=3/768, ttl=254
  5   0.011138   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
```

```
seq=4/1024, ttl=254
  6   0.014099   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=5/1280, ttl=254
  7   0.016868   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=6/1536, ttl=254
  8   0.019210   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=7/1792, ttl=254
  9   0.024785   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=8/2048, ttl=254
 --More--
```

ステップ 4：次のように入力して、キャプチャ ポイントを削除します。

```
Device# no monitor capture mycap
```

（注） 制限が設定してあり、その制限に達するとキャプチャは自動的に停止するため、この特定のケースでは、**stop** コマンドは必要ありません。

pcap の統計情報に使用する構文の詳細については、「その他の参考資料」セクションを参照してください。

例：単純なキャプチャおよび保存

次の例は、フィルタにパケットをキャプチャする方法を示しています。

ステップ 1：次のように入力して、関連トラフィックで一致するキャプチャ ポイントを定義し、それをファイルに関連付けます。

```
Device# monitor capture mycap interface GigabitEthernet1/0/3 in
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap limit duration 60 packets 50
Device# monitor capture mycap file location flash:mycap.pcap
```

ステップ 2：次のように入力してキャプチャ ポイントが正確に定義されていることを確認します。

```
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/3 in
   monitor capture mycap match ipv4  any any
   monitor capture mycap file location flash:mycap.pcap
   monitor capture mycap limit packets 50 duration 60

Device# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
```

```
  File Details:
   Associated file name: flash:mycap.pcap
  Limit Details:
   Number of Packets to capture: 50
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：次のように入力してパケットを開始します。

```
Device# monitor capture mycap start
```

ステップ 4: 次のように入力して実行中のエクステンドキャプチャ統計情報を表示します。

```
Device#  show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 15 seconds
        Packets received - 40
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 40
        Bytes received - 7280
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
        Bytes sent ¬ 4560
```

ステップ 5：十分な時間の経過後に、次のように入力してキャプチャを停止します。

```
Device# monitor capture mycap stop
Capture statistics collected at software (Buffer & Wireshark):
        Capture duration - 20 seconds
        Packets received - 50
        Packets dropped - 0
        Packets oversized - 0
```

（注） あるいは、時間の経過またはパケットカウントが一致した後に、キャプチャ操作を自動的に停止させることもできます。

mycap.pcap ファイルには、キャプチャしたパケットが含まれます。

ステップ 6: 次のように入力して停止後のエクステンドキャプチャの統計情報を表示します。

```
Device#  show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 20 seconds
        Packets received - 50
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 50
        Bytes received - 8190
        Bytes dropped - 0
        Bytes oversized - 0
```

```
        Bytes errored - 0
        Bytes sent ¬ 5130
```

ステップ 7：次のように入力してパケットを表示します。

```
Device# show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=0/0, ttl=254
  2 0.002555000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=1/256, ttl=254
  3 0.006199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=2/512, ttl=254
  4 0.009199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=3/768, ttl=254
  5 0.011647000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=4/1024, ttl=254
  6 0.014168000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=5/1280, ttl=254
  7 0.016737000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=6/1536, ttl=254
  8 0.019403000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=7/1792, ttl=254
  9 0.022151000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=8/2048, ttl=254
 10 0.024722000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=9/2304, ttl=254
 11 0.026890000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=10/2560, ttl=254
 12 0.028862000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=11/2816, ttl=254
 --More--
```

pcap の統計情報に使用する構文の詳細については、「その他の参考資料」セクションを参照してください。

ステップ 8：次のように入力して、キャプチャ ポイントを削除します。

```
Device# no monitor capture mycap
```

例：バッファのキャプチャの使用

次に、バッファのキャプチャを使用する例を示します。

ステップ 1：次のように入力してバッファ キャプチャ オプションでキャプチャ セッションを起動します。

```
Device# monitor capture mycap interface GigabitEthernet1/0/3 in
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap buffer circular size 1
Device# monitor capture mycap start
```

ステップ 2：次のように入力してキャプチャがアクティブであるかどうかを決定します。

```
Device# show monitor capture mycap
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Active
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：次のように入力してランタイム時に拡張キャプチャの統計情報を表示します。

```
Device# show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 88 seconds
        Packets received - 1000
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 1000
        Bytes received - 182000
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
        Bytes sent - 114000
```

ステップ 4：次のように入力してキャプチャを停止します。

```
Device# monitor capture mycap stop
Capture statistics collected at software (Buffer):
        Capture duration - 2185 seconds
        Packets received - 51500
        Packets dropped - 0
        Packets oversized - 0
```

ステップ 5：次のように入力して停止後の拡張キャプチャの統計情報を表示します。

```
Device# show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 156 seconds
        Packets received - 2000
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 2000
        Bytes received - 364000
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
```

```
        Bytes sent - 228000
```

ステップ 6：次のように入力してキャプチャがアクティブであるかどうかを決定します。

```
Device# show monitor capture mycap
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
```

ステップ 7：次のように入力してバッファのパケットを表示します。

```
Device# show monitor capture mycap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1   0.000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40057/31132, ttl=254
  2   0.000030   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40058/31388, ttl=254
  3   0.000052   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40059/31644, ttl=254
  4   0.000073   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40060/31900, ttl=254
  5   0.000094   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40061/32156, ttl=254
  6   0.000115   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40062/32412, ttl=254
  7   0.000137   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40063/32668, ttl=254
  8   0.000158   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40064/32924, ttl=254
  9   0.000179   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40065/33180, ttl=254
 10   0.000200   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40066/33436, ttl=254
 11   0.000221   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40067/33692, ttl=254
 12   0.000243   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40068/33948, ttl=254
 --More--
```

パケットがバッファに入ったことに注意してください。

ステップ 8：他の表示モードでパケットを表示します。

```
Device# show monitor capture mycap buffer detailed
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  6, 2015 18:10:06.297972000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1446833406.297972000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 114 bytes (912 bits)
    Capture Length: 114 bytes (912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:icmp:data]
Ethernet II, Src: Cisco_f3:63:46 (00:e1:6d:f3:63:46), Dst: Cisco_31:f1:c6
(00:e1:6d:31:f1:c6)
    Destination: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        Address: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        Address: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not
ECN-Capable Transport))
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport)
 (0x00)
    Total Length: 100
    Identification: 0xabdd (43997)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
    Header checksum: 0xe8a4 [validation disabled]
        [Good: False]
        [Bad: False]
    Source: 10.10.10.2 (10.10.10.2)
    Destination: 10.10.10.1 (10.10.10.1)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xa620 [correct]
    Identifier (BE): 56 (0x0038)
    Identifier (LE): 14336 (0x3800)
    Sequence number (BE): 40057 (0x9c79)
    Sequence number (LE): 31132 (0x799c)
    Data (72 bytes)

0000  00 00 00 00 0b 15 30 63 ab cd ab cd ab cd ab cd   ......0c........
```

```
0010  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0020  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0030  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0040  ab cd ab cd ab cd ab cd                           ........
        Data: 000000000b153063abcdabcdabcdabcdabcdabcdabcdabcd...
        [Length: 72]

Frame 2: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0


Device# show monitor capture mycap buffer dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0000  00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00   ..m1....m.cF..E.
0010  00 64 ab dd 00 00 fe 01 e8 a4 0a 0a 0a 02 0a 0a   .d..............
0020  0a 01 08 00 a6 20 00 38 9c 79 00 00 00 00 0b 15   ..... .8.y......
0030  30 63 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   0c..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd                                             ..

0000  00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00   ..m1....m.cF..E.
0010  00 64 ab de 00 00 fe 01 e8 a3 0a 0a 0a 02 0a 0a   .d..............
0020  0a 01 08 00 a6 1d 00 38 9c 7a 00 00 00 00 0b 15   .......8.z......
0030  30 65 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   0e..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd
```

ステップ 9：次のように入力してバッファをクリアします。

```
Device# monitor capture mycap clear
```

（注） 注：バッファをクリアすると、その内容とともにバッファが削除されます。

（注） バッファの内容を表示する必要がある場合は、show コマンドの後に clear コマンドを実行します。

ステップ 10：トラフィックを再開し、10 秒待ってから次のように入力してバッファコンテンツを表示します。

（注） キャプチャがアクティブなときに、バッファから show の実行をすることはできません。バッファから show を実行する前に、キャプチャを停止する必要があります。しかし、ファイルおよびバッファ モードの両方においてキャプチャがアクティブなときに pcap ファイルで show の実行ができます。ファイル モードでは、キャプチャがアクティブなときに、現在のキャプチャ セッションの pcap ファイルでパケットを表示することもできます。

```
Device# monitor capture mycap start
Switch#  show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Active
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
```

ステップ 11：次のように入力して、パケットキャプチャを停止し、バッファの内容を表示します。

```
Device# monitor capture mycap stop
Capture statistics collected at software (Buffer):
 Capture duration - 111 seconds
 Packets received - 5000
 Packets dropped - 0
 Packets oversized - 0
```

ステップ 12：次のように入力してキャプチャがアクティブであるかどうかを決定します。

```
Device# show monitor capture mycap
Status Information for Capture mycap
 Target Type:
  Interface: GigabitEthernet1/0/3, Direction: in
 Status : Inactive
Filter Details:
 IPv4
  Source IP: any
  Destination IP: any
 Protocol: any
Buffer Details:
 Buffer Type: CIRCULAR
 Buffer Size (in MB): 1
File Details:
 File not associated
Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Maximum number of packets to capture per second: 1000
 Packet sampling rate: 0 (no sampling)
```

ステップ 13：次のように入力してバッファのパケットを表示します。

```
Device# show monitor capture mycap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=0/0, ttl=254
  2 0.000030000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=1/256, ttl=254
  3 0.000051000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=2/512, ttl=254
  4 0.000072000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=3/768, ttl=254
  5 0.000093000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=4/1024, ttl=254
  6 0.000114000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=5/1280, ttl=254
  7 0.000136000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=6/1536, ttl=254
  8 0.000157000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=7/1792, ttl=254
  9 0.000178000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=8/2048, ttl=254
 10 0.000199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=9/2304, ttl=254
 11 0.000220000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=10/2560, ttl=254
 12 0.000241000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=11/2816, ttl=254
 --More‹
```

ステップ 14：次のように入力して、内部 flash: storage デバイス内の mycap1.pcap ファイルにバッファ コンテンツを保存します。

```
Device# monitor capture mycap export flash:mycap.pcap
Exported Successfully
```

（注） 現在のエクスポート実装では、コマンドを実行すると、エクスポートは「開始」されますが、ユーザにプロンプトを返す場合には完了しません。そこで、ファイルでパケットの表示を実行する前に、Wireshark からコンソールにメッセージが表示されるのを待機する必要があります。

ステップ 15：次のように入力してファイルからキャプチャ パケットを表示します。

```
Device#  show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=0/0, ttl=254
  2 0.000030000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=1/256, ttl=254
  3 0.000051000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=2/512, ttl=254
  4 0.000072000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=3/768, ttl=254
  5 0.000093000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=4/1024, ttl=254
  6 0.000114000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=5/1280, ttl=254
```

```
  7 0.000136000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=6/1536, ttl=254
  8 0.000157000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=7/1792, ttl=254
  9 0.000178000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=8/2048, ttl=254
 10 0.000199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=9/2304, ttl=254
 11 0.000220000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=10/2560, ttl=254
 12 0.000241000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=11/2816, ttl=254
 --More--
```

ステップ 16：次のように入力して、キャプチャ ポイントを削除します。

```
Device# no monitor capture mycap
```

例：出力方向のパケットの簡単なキャプチャおよび保存

次の例は、フィルタにパケットをキャプチャする方法を示しています。

ステップ 1：次のように入力して、関連トラフィックで一致するキャプチャ ポイントを定義し、それをファイルに関連付けます。

```
Device# monitor capture mycap interface Gigabit 1/0/1 out match ipv4 any any
Device# monitor capture mycap limit duration 60 packets 100
Device# monitor capture mycap file location flash:mycap.pcap buffer-size 90
```

ステップ 2：次のように入力してキャプチャ ポイントが正確に定義されていることを確認します。

```
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 out
   monitor capture mycap match ipv4  any any
   monitor capture mycap file location flash:mycap.pcap buffer-size 90
   monitor capture mycap limit packets 100 duration 60

Device# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/1, Direction: out
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 90
  Limit Details:
   Number of Packets to capture: 100
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：次のように入力してパケットを開始します。

```
Device# monitor capture mycap start
A file by the same capture file name already exists, overwrite?[confirm]
Turning on lock-step mode

Device#
*Oct 14 09:35:32.661: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

（注） 時間の経過またはパケットカウントが一致した後に、キャプチャ操作を自動的に停止させてください。出力に次のメッセージが表示された場合は、キャプチャ処理が停止していることを意味します。

```
*Oct 14 09:36:34.632: %BUFCAP-6-DISABLE_ASYNC: Capture Point mycap disabled. Rea
son : Wireshark Session Ended
```

mycap.pcap ファイルには、キャプチャしたパケットが含まれます。

ステップ 4：次のように入力してパケットを表示します。

```
Device# show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  0.000000    10.1.1.30 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000    10.1.1.31 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000    10.1.1.32 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000    10.1.1.33 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000    10.1.1.34 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000    10.1.1.35 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000    10.1.1.36 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000    10.1.1.37 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.38 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.39 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 5：次のように入力してキャプチャ ポイントを削除します。

```
Device# no monitor capture mycap
```

組み込みパケット キャプチャの設定例

例：パケット データ キャプチャの管理

次の例では、パケット データ キャプチャを管理する方法を示します。

```
Device> enable
Device# monitor capture mycap start
Device# monitor capture mycap access-list v4acl
Device# monitor capture mycap limit duration 1000
Device# monitor capture mycap interface GigabitEthernet 0/0/1 both
Device# monitor capture mycap buffer circular size 10
Device# monitor capture mycap start
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# monitor capture mycap stop
Device# end
```

例：キャプチャされたデータのモニタリングとメンテナンス

次の例は、ASCII 形式でパケットをダンプする方法を示しています。

```
Device# show monitor capture mycap buffer dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0
0000: 01005E00 00020000 0C07AC1D 080045C0 ..^...........E.
0010: 00300000 00000111 CFDC091D 0002E000 .0..............
0020: 000207C1 07C1001C 802A0000 10030AFA .........*......
0030: 1D006369 73636F00 0000091D 0001 ..example.......
1
0000: 01005E00 0002001B 2BF69280 080046C0 ..^.....+.....F.
0010: 00200000 00000102 44170000 0000E000 . ......D.......
0020: 00019404 00001700 E8FF0000 0000 .............
2
0000: 01005E00 0002001B 2BF68680 080045C0 ..^.....+.....E.
0010: 00300000 00000111 CFDB091D 0003E000 .0..............
0020: 000207C1 07C1001C 88B50000 08030A6E ...............n
0030: 1D006369 73636F00 0000091D 0001 ..example.......
3
0000: 01005E00 000A001C 0F2EDC00 080045C0 ..^...........E.
0010: 003C0000 00000258 CE7F091D 0004E000 .<.....X........
0020: 000A0205 F3000000 00000000 00000000 ................
0030: 00000000 00D10001 000C0100 01000000 ................
0040: 000F0004 00080501 0300
```

次の例は、mycap という名前のキャプチャの設定に使用するコマンドのリストを表示する方法を示しています。

```
Device# show monitor capture mycap parameter
monitor capture mycap interface GigabitEthernet 1/0/1 both
monitor capture mycap match any
monitor capture mycap buffer size 10
monitor capture mycap limit pps 1000
```

次の例は、キャプチャ ポイントをデバッグする方法を示しています。

```
Device# debug epc capture-point
EPC capture point operations debugging is on

Device# monitor capture mycap start
*Jun 4 14:17:15.463: EPC CP: Starting the capture cap1
*Jun 4 14:17:15.463: EPC CP: (brief=3, detailed=4, dump=5) = 0
*Jun 4 14:17:15.463: EPC CP: final check before activation
*Jun 4 14:17:15.463: EPC CP: setting up c3pl infra
*Jun 4 14:17:15.463: EPC CP: Setup c3pl acl-class-policy
*Jun 4 14:17:15.463: EPC CP: Creating a class
*Jun 4 14:17:15.464: EPC CP: Creating a class : Successful
*Jun 4 14:17:15.464: EPC CP: class-map Created
*Jun 4 14:17:15.464: EPC CP: creating policy-name epc_policy_cap1
*Jun 4 14:17:15.464: EPC CP: Creating Policy epc_policy_cap1 of type 49 and client type
 21
*Jun 4 14:17:15.464: EPC CP: Storing a Policy
*Jun 4 14:17:15.464: EPC CP: calling ppm_store_policy with epc_policy
*Jun 4 14:17:15.464: EPC CP: Creating Policy : Successful
*Jun 4 14:17:15.464: EPC CP: policy-map created
*Jun 4 14:17:15.464: EPC CP: creating filter for ANY
*Jun 4 14:17:15.464: EPC CP: Adding acl to class : Successful
*Jun 4 14:17:15.464: EPC CP: Setup c3pl class to policy
*Jun 4 14:17:15.464: EPC CP: Attaching Class to Policy
*Jun 4 14:17:15.464: EPC CP: Attaching epc_class_cap1 to epc_policy_cap1
*Jun 4 14:17:15.464: EPC CP: Attaching Class to Policy : Successful
```

```
*Jun 4 14:17:15.464: EPC CP: setting up c3pl qos
*Jun 4 14:17:15.464: EPC CP: DBG> Set packet rate limit to 1000
*Jun 4 14:17:15.464: EPC CP: creating action for policy_map epc_policy_cap1 class_map
epc_class_cap1
*Jun 4 14:17:15.464: EPC CP: DBG> Set packet rate limit to 1000
*Jun 4 14:17:15.464: EPC CP: Activating Interface GigabitEthernet1/0/1 direction both
*Jun 4 14:17:15.464: EPC CP: Id attached 0
*Jun 4 14:17:15.464: EPC CP: inserting into active lists
*Jun 4 14:17:15.464: EPC CP: Id attached 0
*Jun 4 14:17:15.465: EPC CP: inserting into active lists
*Jun 4 14:17:15.465: EPC CP: Activating Vlan
*Jun 4 14:17:15.465: EPC CP: Deleting all temp interfaces
*Jun 4 14:17:15.465: %BUFCAP-6-ENABLE: Capture Point cap1 enabled.
*Jun 4 14:17:15.465: EPC CP: Active Capture 1

Device# monitor capture mycap1 stop
*Jun 4 14:17:31.963: EPC CP: Stopping the capture cap1
*Jun 4 14:17:31.963: EPC CP: Warning: unable to unbind capture cap1
*Jun 4 14:17:31.963: EPC CP: Deactivating policy-map
*Jun 4 14:17:31.963: EPC CP: Policy epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Deactivating policy-map Successful
*Jun 4 14:17:31.964: EPC CP: removing povision feature
*Jun 4 14:17:31.964: EPC CP: Found action for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:17:31.964: EPC CP: cleanning up c3pl infra
*Jun 4 14:17:31.964: EPC CP: Removing Class epc_class_cap1 from Policy
*Jun 4 14:17:31.964: EPC CP: Removing Class from epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Successfully removed
*Jun 4 14:17:31.964: EPC CP: Removing acl mac from class
*Jun 4 14:17:31.964: EPC CP: Removing acl from class : Successful
*Jun 4 14:17:31.964: EPC CP: Removing all policies
*Jun 4 14:17:31.964: EPC CP: Removing Policy epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Removing Policy : Successful
*Jun 4 14:17:31.964: EPC CP: Removing class epc_class_cap1
*Jun 4 14:17:31.965: EPC CP: Removing class : Successful
*Jun 4 14:17:31.965: %BUFCAP-6-DISABLE: Capture Point cap1 disabled.
*Jun 4 14:17:31.965: EPC CP: Active Capture 0
```

次の例は、組み込みパケット キャプチャ（EPC）のプロビジョニングをデバッグする方法を示しています。

```
Device# debug epc provision
EPC provisionioning debugging is on

Device# monitor capture mycap start
*Jun 4 14:17:54.991: EPC PROV: No action found for policy-map epc_policy_cap1 class-map
 epc_class_cap1
*Jun 4 14:17:54.991: EPC PROV:
*Jun 4 14:17:54.991: Attempting to install service policy epc_policy_cap1
*Jun 4 14:17:54.992: EPC PROV: Attached service policy to epc idb subblock
*Jun 4 14:17:54.992: EPC PROV: Successful. Create feature object
*Jun 4 14:17:54.992: EPC PROV:
*Jun 4 14:17:54.992: Attempting to install service policy epc_policy_cap1
*Jun 4 14:17:54.992: EPC PROV: Successful. Create feature object
*Jun 4 14:17:54.992: %BUFCAP-6-ENABLE: Capture Point cap1 enabled.

Device# monitor capture mycap stop
*Jun 4 14:18:02.503: EPC PROV: Successful. Remove feature object
*Jun 4 14:18:02.504: EPC PROV: Successful. Remove feature object
*Jun 4 14:18:02.504: EPC PROV: Destroyed epc idb subblock
*Jun 4 14:18:02.504: EPC PROV: Found action for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:18:02.504: EPC PROV: Deleting EPC action
*Jun 4 14:18:02.504: EPC PROV: Successful. CLASS_REMOVE, policy-map epc_policy_cap1,
```

```
class epc_class_cap1
*Jun 4 14:18:02.504: %BUFCAP-6-DISABLE: Capture Point cap1 disabled.
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
表示フィルタ	表示フィルタの構文については、以下を参照して下さい。 『Display Filter Reference』
pcap ファイル統計情報	pcap ファイル統計情報の表示に使用する構文については、以下で「-z」オプションの詳細を参照してください。 『Tshark Command Reference』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

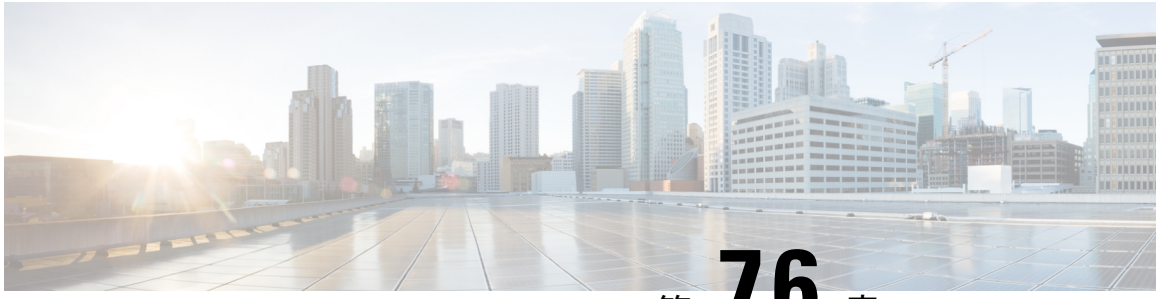
標準/RFC	Title
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support



第 76 章

Flexible NetFlow の設定

- Flexible NetFlow の前提条件 （1409 ページ）
- Flexible Netflow に関する制約事項 （1410 ページ）
- Flexible NetFlow に関する情報 （1413 ページ）
- Flexible NetFlow の設定方法 （1432 ページ）
- Flexible NetFlow の監視 （1449 ページ）
- Flexible NetFlow の設定例 （1449 ページ）
- その他の参考資料 （1455 ページ）
- Flexible NetFlow の機能情報 （1456 ページ）

Flexible NetFlow の前提条件

次に、Flexible NetFlow コンフィギュレーションの前提条件を示します。

- 送信元インターフェイスを設定する必要があります。送信元インターフェイスを設定しなかった場合、エクスポータはディセーブル ステートのままです。
- フロー モニタごとに、有効なレコード名を設定する必要があります。
- IPv6 宛先サーバにフロー レコードをエクスポートするには、IPv6 ルーティングをイネーブルにする必要があります。
- IPFIX 形式の NetFlow レコードをエクスポートするには、フロー エクスポータに IPFIX エクスポート プロトコルを設定する必要があります。
- Flexible NetFlow の key フィールドについて、『Cisco IOS Flexible NetFlow Command Reference』の次のコマンドに定義されている内容をよく理解する必要があります。
  - **match datalink**：データリンク（レイヤ 2）フィールド
  - **match flow**：フィールド識別フロー
  - **match interface**：インターフェイス フィールド
  - **match ipv4**：IPv4 フィールド
  - **match ipv6**：IPv6 フィールド

- **match transport**：トランスポート層フィールド
- **match wireless**：ワイヤレス フィールド
- **match flow cts**：CTS フィールド

- Flexible NetFlow の nonkey フィールドについて、『Cisco IOS Flexible NetFlow Command Reference』で次のコマンドに定義されている内容をよく理解する必要があります。
  - **collect counter**：カウンタ フィールド
  - **collect flow**：フィールド識別フロー
  - **collect interface**：インターフェイス フィールド
  - **collect timestamp**：タイムスタンプ フィールド
  - **collect transport**：トランスポート層フィールド
  - **collect wireless**：ワイヤレス フィールド

IPv4 トラフィック

- ネットワーキング デバイスが IPv4 ルーティング用に設定されていること。
- Cisco Express Forwarding またはdistributed Cisco Express Forwarding のいずれかが、デバイスおよびFlexible NetFlowを有効化するすべてのインターフェイスで有効化されていること。

IPv6 トラフィック

- ネットワーキング デバイスが、IPv6 ルーティング用に設定されていること。
- Cisco Express Forwarding IPv6 または分散型 Cisco Express Forwarding のいずれかが、デバイスおよび Flexible NetFlow を有効化するすべてのインターフェイスで有効化されていること。

Flexible Netflow に関する制約事項

次に、Flexible NetFlow に関する制約事項を示します。

- Flexible NetFlow は、L2 ポートチャネル インターフェイスではサポートされませんが、L2 ポートチャネル メンバー ポートではサポートされます。
- Flexible NetFlow は、L3 ポートチャネル インターフェイスではサポートされませんが、L3 ポートチャネル メンバー ポートではサポートされます。
- Traditional NetFlow（TNF）のアカウンティングはサポートされていません。

- Flexible NetFlow バージョン 9 およびバージョン 10 のエクスポート フォーマットがサポートされています。ただし、エクスポート プロトコルが設定されていない場合は、バージョン 9 のエクスポート フォーマットがデフォルトで適用されます。
- マイクロフロー ポリシング機能は FNF と NetFlow ハードウェア リソースを共有します。
- インターフェイスおよび方向ごとに、1 つのフロー モニタのみサポートされます。
- レイヤ 2、IPv4、および IPv6 のトラフィック タイプがサポートされています。異なるトラフィック タイプの複数のフロー モニタを、指定したインターフェイスと方向に適用できます。同じトラフィック タイプの複数のフロー モニタを指定したインターフェイスと方向には適用できません。
- レイヤ 2、VLAN、WLAN、およびレイヤ 3 インターフェイスがサポートされています。ただし、デバイスは SVI およびトンネルをサポートしていません。
- 次のサイズの NetFlow テーブルがサポートされています。

トリム レベル	入力 NetFlow テーブル	出力 NetFlow テーブル
LAN ベース	サポート対象外	サポート対象外
IP Base	8 K	16 K
IP サービス	8 K	16 K

- スイッチのタイプに応じて、スイッチには 1 個または 2 個の転送 ASIC があります。上記の表に示されているのは、ASIC ごとの容量です。
- スイッチは、1 個または 2 個の ASIC をサポートできます。各 TCAM が最大 6K 入力エントリおよび 12K 出力エントリを処理できる一方、各 ASIC は 8K 入力および 16 K 出力エントリを処理できます。
- NetFlow テーブルは個別のコンパートメントにあり、組み合わせることはできません。パケットを処理した ASIC のテーブルに応じて、対応した ASIC のテーブルにフローが作成されます。
- NetFlow ハードウェアの実装では、4 台のハードウェア サンプラーがサポートされています。1/2 ～ 1/1024 のサンプラー レートを選択できます。ランダム サンプリング モードのみがサポートされています。
- マイクロフロー ポリシング機能（ワイヤレス実装の場合にのみ有効）では、フル フロー モードでのみ NetFlow を使用できます。NetFlow ポリシングは使用できません。マイクロフロー QoS の妨げになるため、ワイヤレス トラフィックにはサンプラーを適用できません。
- ワイヤレス トラフィックでは、フル フロー アカウンティングだけがサポートされています。
- NetFlow ハードウェアの内部では、ハッシュ テーブルが使用されています。ハードウェア内でハッシュ衝突が発生する場合があります。したがって、内部の連想メモリ（CAM）

でオーバーフローが発生しても、実際の NetFlow テーブルの使用率は約 80 % しかない場合があります。

- フローに使用されるフィールドによって異なりますが、単一のフローは2個の連続したエントリを取得できます。IPv6 フローも 2 個のエントリを取得します。この場合、NetFlow エントリを効果的に使用すれば、テーブルサイズの半分で済みます。これは、上記のハッシュ衝突の制限とは別です。
- デバイスは、最大 15 個のフロー モニタをサポートしています。
- SSID ベースの NetFlow アカウンティングがサポートされています。SSID はインターフェイスと同様の方法で扱われます。ただし、ユーザ ID などの一部のフィールドはサポートされていません。
- NetFlow ソフトウェアの実装では、分散 NetFlow エクスポートがサポートされるため、フローが作成された同じデバイスからフローがエクスポートされます。
- 入力フローは最初にフローのパケットを受信した ASIC にあります。出力フローは、パケットが実際に デバイス セットアップを残した ASIC にあります。
- バイトカウントフィールドのレポート値（「bytes long」と呼ばれる）は、レイヤ2パケットサイズの18バイトです。従来のイーサネットトラフィック（802.3）の場合、これは正確です。他のすべてのイーサネット タイプの場合、このフィールドは正確ではありません。「bytes layer2」フィールドを使用すると、常に正確なレイヤ2パケット サイズが報告されます。サポートされる Flexible NetFlow フィールドについては、サポートされている Flexible NetFlow フィールド （1426 ページ） を参照してください。
- AVC フロー モニタの IPFIX エクスポータの設定はサポートされていません。
- Flexible NetFlow エクスポートは、イーサネット管理ポート（Gi0/0）ではサポートされていません。
- フロー レコードに送信元グループ タグ（SGT）と宛先グループ タグ（DGT）のフィールド（またはこの2つのいずれかのフィールド）だけが含まれる場合、両方の値を適用できないとしても、SGT と DGT に値ゼロを設定したフローが作成されます。フロー レコードには、SGT および DGT フィールドと一緒に、送信元および宛先 IP アドレスが含まれる必要があります。
- WLAN（SSID）では接続できないCTSフィールドを含むフロー レコードを使用したフローモニタ。
- QoS のマークが付けられたパケットが出力方向に NetFlow が設定されているインターフェイスで受信されると、パケットの QoS 値がコレクタによってキャプチャされます。しかし、パケットが入力方向に NetFlow が設定されているインターフェイスで受信されると、パケットの QoS 値はコレクタによってキャプチャされません。

Flexible NetFlow に関する情報

Flexible NetFlow の概要

Flexible NetFlow ではフローを使用して、アカウンティング、ネットワーク モニタリング、およびネットワーク プランニングに関連する統計情報を提供します。

フローは送信元インターフェイスに届く単方向のパケット ストリームで、キーの値は同じです。キーは、パケット内のフィールドを識別する値です。フローを作成するには、フロー レコードを使用して、フロー固有のキーを定義します。

デバイス は、ネットワーク異常とセキュリティ問題の高度な検出をイネーブルにする Flexible NetFlow 機能をサポートします。Flexible NetFlow により、大量の定義済みフィールドの集合からキーを選択して、特定のアプリケーションに最適なフロー レコードを定義できます。

1 つのフローと見なされるパケットでは、すべてのキー値が一致している必要があります。フローは、設定したエクスポート レコード バージョンに基づいて、関係のある他のフィールドを集めることもあります。フローはFlexible NetFlow キャッシュに格納されます。

エクスポータを使用してFlexible NetFlowがフローのために収集するデータをエクスポートし、Flexible NetFlow コレクタなどのリモート システムにこのデータをエクスポートできます。Flexible NetFlow コレクタは、IPv4 または IPv6 アドレスを使用できます。

モニタを使用してフローのために収集するデータのサイズを定義します。モニタで、フロー レコードおよびエクスポータを Flexible NetFlow キャッシュ情報と結合します。

ワイヤレス Flexible NetFlow の概要

ワイヤレス Flexible NetFlow インフラストラクチャは次をサポートします。

- Flexible NetFlow バージョン 9.0 および 10
- ユーザ ベースのレート制限
- microflow ポリシング
- 音声およびビデオ フロー モニタリング
- 再帰アクセス コントロール リスト（ACL）

マイクロフロー ポリシングとユーザ ベースのレート制限

マイクロフロー ポリシングは、NetFlow テーブル内の各フローに 2 カラー、1 レートのポリサーと関連ドロップ統計情報を関連付けます。フロー マスクがすべてのパケット フィールドで構成される場合、この機能は「マイクロフロー ポリシング」と呼ばれます。フロー マスクが送信元または宛先のみで構成される場合、この機能は「ユーザ ベースのレート制限」と呼ばれます。

音声およびビデオ フロー モニタリング

音声およびビデオ フローはフル フロー マスク ベースのエントリです。ASIC は、ポリサー パラメータのプログラム、複数のフローでのポリサー共有、フローの IP アドレスとレイヤー 4 ポート番号の書き換えにおいて柔軟性を提供します。

（注） ダイナミック エントリの場合、NetFlow エンジンは、ポリシー（ACL/QoS ベース ポリシー）に基づいてフローに対して取得されたポリサー パラメータを使用します。ダイナミック エントリは複数のフロー間でポリサーを共有できません。

再帰 ACL

再帰 ACL により、上位層セッション情報に基づいて IP パケットをフィルタリングできます。ACL は発信トラフィックを許可し、信頼ネットワーク内で開始されたセッションに応じて、着信トラフィックを制限します。再帰 ACL は、再帰的なエントリと一致するデータ パケットによりアクティブにされるまで、フィルタリング メカニズムに対して透過的です。この時点では、一時 ACL エントリが作成され、IP 名付きアクセス リストに追加されています。再帰 ACL エントリを生成するデータ パケットから取得した情報は、許可/拒否ビット、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、ポート、およびプロトコル タイプです。再帰 ACL エントリの評価において、プロトコル タイプが TCP または UDP の場合、ポート情報は正確に一致する必要があります。他のプロトコルの場合、一致するポート情報はありません。この ACL をインストールすると、通過する応答パケットに対してファイアウォールが開かれます。この時点では、ハッカーがファイアウォールの背後にあるネットワークにアクセスする危険性があります。この危険性を最小限に抑えるには、アイドルタイムアウト期間を定義できます。ただし、TCP の場合、2 つの FIN ビットまたは RST が検出された場合、ACL エントリが削除される可能性があります。

以前の NetFlow と Flexible NetFlow の利点

以前の NetFlow では、フローの判定に固定の 7 タプルの IP 情報を使用していました。

Flexible NetFlow ではフローをユーザが定義できます。次に、Flexible NetFlow の利点を示します。

- スケーラビリティ、フロー情報の集約などの、大容量フロー認識。
- セキュリティの監視と dDoS の検出および識別のための拡張されたフロー インフラストラクチャ。
- フロー情報をネットワーク内の特定のサービスまたはオペレーションに適応させるパケットからの新しい情報。利用できるフロー情報は、Flexible NetFlow ユーザがカスタマイズ可能。
- Cisco の柔軟で拡張可能な NetFlow Version 9 および Version 10 エクスポート フォーマットの活用。Version 10 エクスポート フォーマットでは、ワイヤレス クライアントの SSID の可変長フィールドをサポート。

- IP アカウンティング、ボーダー ゲートウェイ プロトコル（BGP）ポリシー アカウンティング、永続的キャッシュなどの多数のアカウンティング機能を置換するために使用できる包括的な IP アカウンティング機能。
- NetFlow の入出力アカウンティングのサポート。
- フロー アカウンティングのフル サポートおよびサンプリングした NetFlow アカウンティングのサポート。

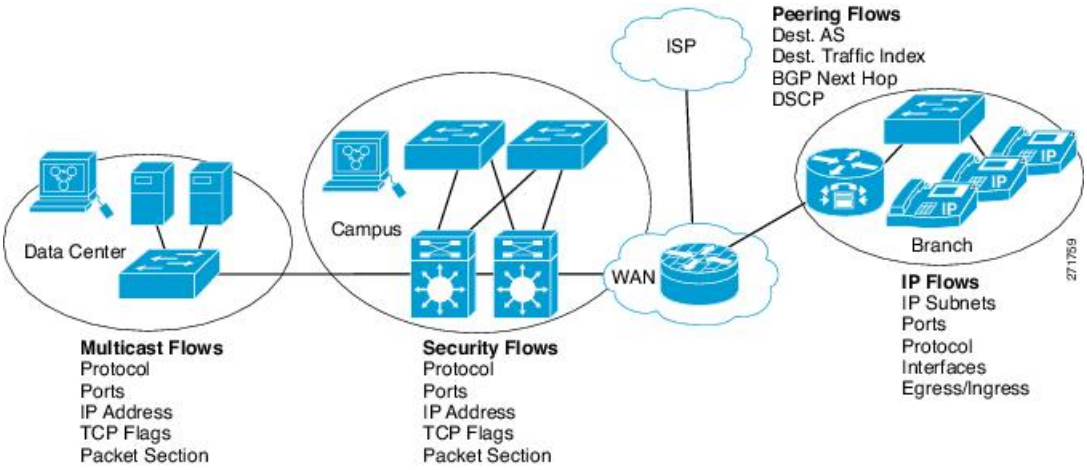
以前の NetFlow では、ネットワーク内のアクティビティを理解して、ネットワーク設計を最適化し、稼働コストを削減できます。

Flexible NetFlow では、ネットワークの動作を、ネットワーク内で使用されるさまざまなサービスに合わせた特定のフロー情報とともに、より効率的に理解できます。次に、Flexible NetFlow 機能用の適用例を示します。

- Flexible NetFlow は Cisco NetFlow をセキュリティ監視ツールとして拡張します。たとえば、ユーザがネットワーク内で特定のタイプの攻撃を検索できるように、パケット長や MAC アドレスのために新しいフロー キーを定義することができます。
- Flexible NetFlow を使用すると、TCP アプリケーションまたは UDP アプリケーションをパケット内のサービス クラス（CoS）ごとに明確に追跡することによって、ホスト間で送信されるアプリケーション トラフィックの量を迅速に識別できます。
- サービス クラスごとに各ネクストホップのマルチプロトコルラベルスイッチング（MPLS）か IP コア ネットワーク、およびその宛先を入力するトラフィックのアカウンティング。この機能では、エッジ間のトラフィック マトリクスを構築できます。

次の表に、Flexible NetFlow をネットワークに導入する方法の例を示します。

図 *87 : Flexible NetFlow* の通常の導入



Flexible NetFlow のコンポーネント

Flexible NetFlow は、いくつかのバリエーションで一緒に使用して、トラフィック分析およびデータ エクスポートに使用できるコンポーネントで構成されます。Flexible NetFlow のユーザ定義のフロー レコードおよびコンポーネントの構造では、最小限の数のコンフィギュレーション コマンドで、ネットワーキング デバイスでのトラフィック分析およびデータ エクスポートのためのさまざまなコンフィギュレーションの作成が容易になります。各フローモニタに、フロー レコード、フロー エクスポータ、およびキャッシュ タイプの固有の組み合わせを設定できます。フロー エクスポータの宛先 IP アドレスなどのパラメータを変更する場合、フロー エクスポータを使用するすべてのフロー モニタに対して自動的に変更されます。同じフロー モニタを複数のフローサンプラと組み合わると、さまざまなインターフェイス上でさまざな速度の同じタイプのネットワーク トラフィックをサンプリングできます。ここでは、Flexible NetFlow コンポーネントのその他の情報を提供します。

フロー レコード

Flexible NetFlow では、キー フィールドと非キー フィールドの組み合わせをレコードと呼びます。Flexible NetFlow のレコードは Flexible NetFlow フロー モニタに割り当てられ、フロー データの格納に使用されるキャッシュが定義されます。Flexible NetFlow には、Flexible NetFlow の使用を開始する際に役立ついくつかの事前定義済みのレコードが含まれています。

フロー レコードでは、フロー内のパケットを識別するために Flexible NetFlow で使用するキーとともに、Flexible NetFlow がフローについて収集する他の関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フロー レコードを定義できます。デバイスは、幅広いキー セットをサポートします。フロー レコードでは、フロー単位で収集するカウンタのタイプも定義します。64 ビットのパケットまたはバイト カウンタを設定できます。デバイスは、フロー レコードの作成時に、デフォルトとして次の match フィールドをイネーブルにします。

- match datalink：レイヤ 2 属性
- match flow direction：フローの方向を識別するフィールドとの一致を指定します。
- match interface：インターフェイス属性
- match ipv4：IPv4 属性
- match ipv6：IPv6 属性
- match transport：トランスポート層フィールド
- match wireless：ワイヤレス フィールド
- match flow cts：CTS フィールド

NetFlow の事前定義済みのレコード

Flexible NetFlow には事前定義済みのレコードがいくつか含まれ、それを使用してネットワーク トラフィックの監視を開始できます。事前定義済みのレコードは、Flexible NetFlow を迅速に導入するために役立ち、ユーザ定義のフロー レコードよりも簡単に使用できます。ネット

ワーク モニタリングのニーズを満たす定義済みのレコードのリストから選択できます。Flexible NetFlow が改良されると、一般的なユーザ定義のフロー レコードを事前定義済みレコードとして使用でき、簡単に導入できるようになります。

事前定義済みレコードにより、エクスポートされるデータのために既存の NetFlow コレクタ コンフィギュレーションとの下位互換性が確保されます。事前定義済みレコードは、それぞれ固有の key および nonkey フィールドの組み合わせを持ち、ルータで Flexible NetFlow をカスタマイズしなくても、ネットワーク内のさまざまなタイプのトラフィックを監視する、内蔵機能を提供します。

2 つの事前定義済みレコード（NetFlow original と NetFlow IPv4/IPv6 original output）は機能的に同等で、以前の（入力）NetFlow、および以前の NetFlow の 出力 NetFlow アカウンティング機能をそれぞれエミュレートします。その他の Flexible NetFlow の事前定義済みレコードのいくつかは、以前の NetFlow で利用できる集約キャッシュ方式に基づきます。以前の NetFlow で利用できる集約キャッシュ方式に基づく Flexible NetFlow の事前定義済みレコードでは、集約を実行しません。代わりに、事前定義済みレコードによって各フローが個別に追跡されます。

ユーザ定義レコード

Flexible NetFlow では、key および nonkey フィールドを指定し、実際の要件に合わせてデータ収集をカスタマイズすることで、Flexible NetFlow フロー モニタ キャッシュ用の独自のレコードを定義できます。Flexible NetFlow フロー モニタ キャッシュに対して独自のレコードを定義する場合、ユーザ定義レコードと呼ばれます。nonkey フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。nonkey フィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、nonkey フィールドの値はフロー内の最初のパケットからのみ取得されます。Flexible NetFlow を使用すると、nonkey フィールドとして、フロー内のバイト数やパケット数などのカウンター値をキャプチャできます。

ユーザ定義レコードは、QoS および帯域幅監視、アプリケーションとユーザのトラフィック プロファイリング、dDoS 攻撃に対するセキュリティ監視などのアプリケーション用に作成できます。また、Flexible NetFlow には以前の NetFlow をエミュレートするいくつかの事前定義済みレコードも含まれています。Flexible NetFlow のユーザ定義レコードでは、ユーザが設定可能なサイズのパケットの連続するセクションを監視する機能を利用でき、key フィールドまたは nonkey フィールドとしてパケットのその他のフィールドや属性とともにフロー レコード内で使用します。セクションにはパケットのレイヤ 3 データが含まれる場合があります。パケットのセクション フィールドでは、ユーザが Flexible NetFlow の事前定義済みレコードの対象外のパケット フィールドを監視できます。事前定義済みキーで収集されないパケット フィールドの分析機能によって、さらに詳細なトラフィック モニタリングが可能になるため、dDoS 攻撃の調査に役立ち、URL モニタリングなど他のセキュリティ アプリケーションの実装が可能になります。

Flexible NetFlow では、事前定義済みタイプのユーザが設定可能なサイズのパケット セクションが提供されます。次の Flexible NetFlow コマンド（Flexible NetFlow フロー レコード コンフィギュレーション モードで使用される）をパケット セクションの事前定義済みタイプの設定に使用できます。

- **collectipv4sectionheadersize** *bytes*：各パケットの IPv4 ヘッダーの先頭から *bytes* 引数で指定されたバイト数のキャプチャを開始します。

- **collectipv4sectionpayloadsize** *bytes*：各パケットの IPv4 ヘッダーの直後からバイトのキャプチャを開始します。キャプチャされるバイト数は *bytes* 引数で指定されます。
- **collectipv6sectionheadersize** *bytes*：各パケットの IPv6 ヘッダーの先頭から *bytes* 引数で指定されたバイト数のキャプチャを開始します。
- **collectipv6sectionpayloadsize** *bytes*：各パケットの IPv6 ヘッダーの直後からバイトのキャプチャを開始します。キャプチャされるバイト数は *bytes* 引数で指定されます。

bytes 値は、フロー レコードのこれらのフィールドのサイズ（バイト単位）です。パケットの対応フラグメントが要求されたセクションサイズよりも小さい場合、Flexible NetFlow はフローレコード内の残りのセクション フィールドを 0 で埋めます。パケット タイプが要求されたセクション タイプと一致しなかった場合、Flexible NetFlow はフロー レコード内のセクション フィールド全体を 0 で埋めます。

Flexible NetFlow では、ヘッダーおよびパケット セクションのタイプに新しいバージョン 9 エクスポート フォーマット フィールド タイプが追加されます。Flexible NetFlow は NetFlow コレクタに、対応するバージョン 9 エクスポート テンプレート フィールドで設定されたセクション サイズを通知します。ペイロード セクションには、対応する長さフィールドがあり、収集されるセクションの実際のサイズを収集するために使用できます。

Flexible NetFlow の match パラメータ

次の表で、Flexible NetFlow の match パラメータについて説明します。フロー レコードごとに、次の match パラメータを 1 つ以上設定する必要があります。

表 *79 : match* パラメータ

コマンド	目的
match datalink {**dot1q** | **ethertype** | **mac** | **vlan** }	データ リンクまたはレイヤ 2 フィールドとの一致を指定します。次のコマンド オプションが使用可能です。 • **dot1q**：dot1q フィールドと一致します。 • **ethertype**：パケットの ethertype と一致します。 • **mac**：送信元または宛先の MAC フィールドと一致します。 • **vlan**：パケットが配置される VLAN と一致します（入力または出力）。
match flow direction	フローを識別するフィールドとの一致を指定します。

コマンド	目的
match interface {**input** | **output**}	インターフェイス フィールドとの一致を指定します。次のコマンド オプションが使用可能です。 • **input**：入力インターフェイスと一致します。 • **output**：出力インターフェイスと一致します。
match ipv4 {**destination** | **protocol** | **source** | **tos** | **ttl** | **version**}	IPv4 フィールドとの一致を指定します。次のコマンド オプションが使用可能です。 • **destination**：IPv4 宛先アドレス ベースのフィールドと一致します。 • **protocol**：IPv4 プロトコルと一致します。 • **source**：IPv4 送信元アドレス ベースのフィールドと一致します。 • **tos**：IPv4 タイプ オブ サービス フィールドと一致します。 • **ttl**：IPv4 存続時間フィールドと一致します。 • **version**：IPv4 ヘッダーの IP バージョンと一致します。

コマンド	目的
match ipv6 {**destination** | **hop-limit** | **protocol** | **source** | **traffic-class** | **version** }	IPv6 フィールドとの一致を指定します。次のコマンド オプションが使用可能です。 • **destination**：IPv6 宛先アドレス ベースのフィールドと一致します。 • **hop-limit**：IPv6 ホップ リミット フィールドと一致します。 • **protocol**：IPv6 ペイロード プロトコル フィールドと一致します。 • **source**：IPv6 送信元アドレス ベースのフィールドと一致します。 • **traffic-class**：IPv6 トラフィック クラスと一致します。 • **version**：IPv6 ヘッダーの IP バージョンと一致します。
match transport {**destination-port** | **igmp** | **icmp** | **source-port**}	トランスポート層フィールドとの一致を指定します。次のコマンド オプションが使用可能です。 • **destination-port**：転送先ポートと一致します。 • **icmp**：ICMP IPv4 および IPv6 フィールドを含む ICMP フィールドと一致します。 • **igmp**：IGMP フィールドと一致します。 • **source-port**：転送元ポートと一致します。
match flow cts {**source** | **destination**} **group-tag**	FNF レコードの CTS フィールドのサポートとの一致を指定します。次のコマンド オプションが使用可能です。 • **source**：ドメインを入力する CTS の送信元と一致します。 • **destination**：ドメインを脱退する CTS の宛先と一致します。

Flexible NetFlow の collect パラメータ

次の表で、Flexible NetFlow の collect パラメータについて説明します。

表 *80 : collect* パラメータ

コマンド	目的
collect counter { **bytes** { **layer2** { **long** } | **long** } | **packets** { **long** } }	カウンタ フィールドの合計バイト数と合計パケット数を収集します。
collect interface {**input** | **output**}	入力または出力インターフェイスからフィールドを収集します。
collect timestamp absolute {**first** | **last**}	最初のパケットが確認された絶対時間、または最新のパケットが最後に確認された絶対時間のフィールドを収集します（ミリ秒）。
collect transport tcp flags	次の転送 TCP フラグを収集します。 • **ack**：TCP 確認応答フラグ • **cwr**：TCP 輻輳ウィンドウ縮小フラグ • **ece**：TCP ECN エコー フラグ • **fin**：TCP 終了フラグ • **psh**：TCP プッシュ フラグ • **rst**：TCP リセット フラグ • **syn**：TCP 同期フラグ • **urg**：TCP 緊急フラグ （注） デバイスでは、収集する TCP フラグを指定できません。転送 TCP フラグの収集のみ指定できます。すべての TCP フラグはこのコマンドで収集されます。

フロー エクスポータ

フロー エクスポータでは、フロー モニタ キャッシュ内のデータをリモート システム（たとえば、分析および保管のために NetFlow コレクタを実行するサーバ）にエクスポートします。フロー エクスポータは、コンフィギュレーションで別のエンティティとして作成されます。フロー エクスポータは、フロー モニタにデータ エクスポート機能を提供するためにフロー モニタに割り当てられます。複数のフローエクスポータを作成して、1 つまたは複数のフローモニタに適用すると、いくつかのエクスポート先を指定することができます。1 つのフローエクスポータを作成し、いくつかのフロー モニタに適用することができます。

NetFlow データ エクスポート フォーマット バージョン 10（IPFIX）

Internet Protocol Flow Information Export（IPFIX）、つまりバージョン 10 は、事前に定義されたか、またはユーザ定義のフロー レコードを収集し、エクスポートするエクスポート プロトコルです。IPFIX は NetFlow バージョン 9に基づいた IETF 標準です。IPFIX 形式は NetFlow バージョン 9 として、個別のテンプレートとレコードについて同じ原則を保ちます。これにより、ワイヤレス クライアントの SSID の可変長フィールドをサポートします。IPFIX エクスポート プロトコルでは、デフォルトの宛先ポートは 4739、DSCP 値は 0、TTL は 255 です。

NetFlow データ エクスポート フォーマットのバージョン 9

NetFlow の基本出力はフロー レコードです。NetFlow が改良され、フロー レコードのいくつかのフォーマットが向上しました。NetFlow エクスポート フォーマットの最新の進化は、バージョン 9 と呼ばれます。NetFlow Version 9 エクスポート フォーマットの識別機能は、テンプレートがベースとなります。テンプレートは、レコードフォーマットの設計を拡張可能なものにします。NetFlow サービスが将来拡張されても、基本フロー レコードフォーマットを変更し続ける必要がありません。テンプレートを使用すると、次のいくつかの利点があります。

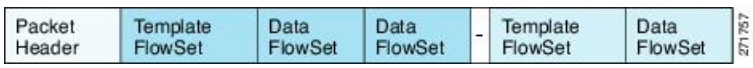
- NetFlow のコレクタを提供したり、サービスを表示したりするアプリケーションを作成するサードパーティ ビジネス パートナーは、新規の NetFlow 機能が追加されるたびにアプリケーションを再コンパイルする必要はありません。代わりに、既知のテンプレートフォーマットを記述する外部のデータ ファイルを使用することができます。
- 新規機能は、現在の導入環境を損ねることなく、NetFlow に迅速に追加できます。
- バージョン 9 フォーマットは新しいプロトコルや開発中のプロトコルに適応できるため、NetFlow はこれらのプロトコルに対して「将来的に対応」します。

NetFlow バージョン 9 エクスポート フォーマットは、次の特徴と機能を提供します。

- 可変フィールド仕様フォーマット
- IPv4 または IPv6 の宛先アドレスのエクスポートのサポート
- ネットワークをより効率的に利用可能

バージョン 9 のエクスポート フォーマットは、パケット ヘッダーとそれに続く 1 つ以上のテンプレート フロー セットまたはデータ フロー セットで構成されています。テンプレート フローセットでは、将来のデータ フローセットに表示されるフィールドの説明が提供されます。このようなデータ フロー セットは、後で同じエクスポート パケットまたは後続のエクスポート パケットで発生する可能性があります。テンプレート フロー セットおよびデータ フローセットは、次の図に示すように、単一のエクスポートパケットに混在させることができます。

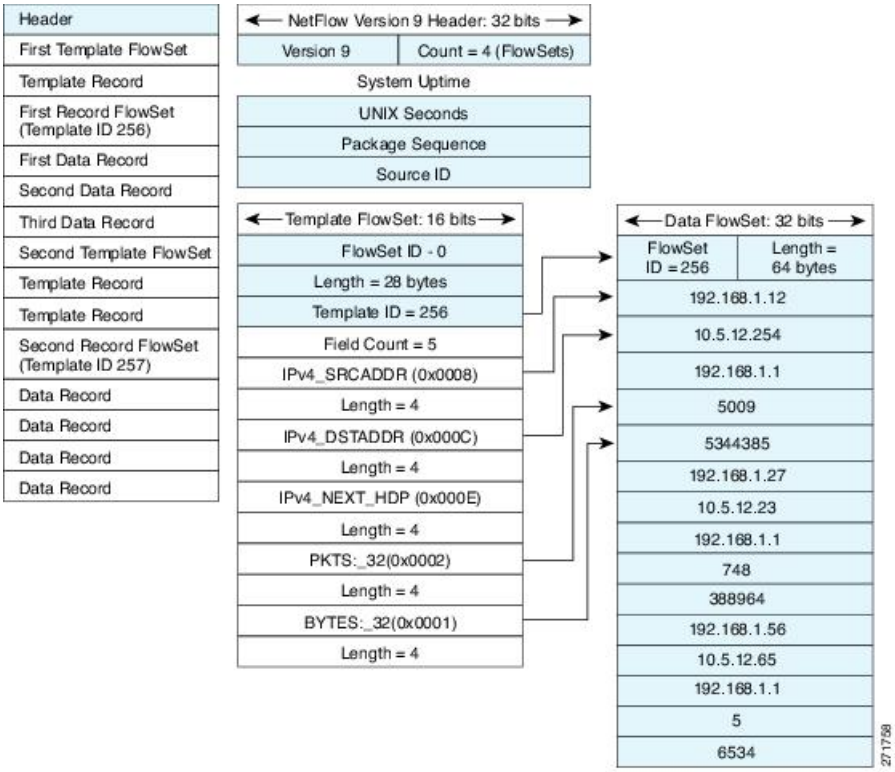
図 *88 :* バージョン *9* エクスポート パケット



NetFlow Version 9 では、送信されるデータを NetFlow コレクタが理解できるように、テンプレート データを定期的にエクスポートします。また、テンプレートのデータ フロー セットもエクスポートします。Flexible NetFlow の主な利点は、ユーザがフロー レコードを設定すると、

バージョン9テンプレートに効率的に変換され、コレクタに転送されることです。下の図に、ヘッダー、テンプレート フロー セットおよびデータ フロー セットを含めて、NetFlow Version 9 エクスポート フォーマットの詳細な例を示します。

図 *89 : NetFlow* バージョン *9* エクスポート フォーマットの詳細例



バージョン 9 エクスポート フォーマットの詳細については、ホワイト ペーパー『Cisco IOS NetFlow Version 9 Flow-Record Format』を参照してください。次の URL から入手できます。
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml

フロー モニタ

フロー モニタは Flexible NetFlow のネットワーク トラフィックの監視を実行するコンポーネントで、インターフェイスに適用されます。

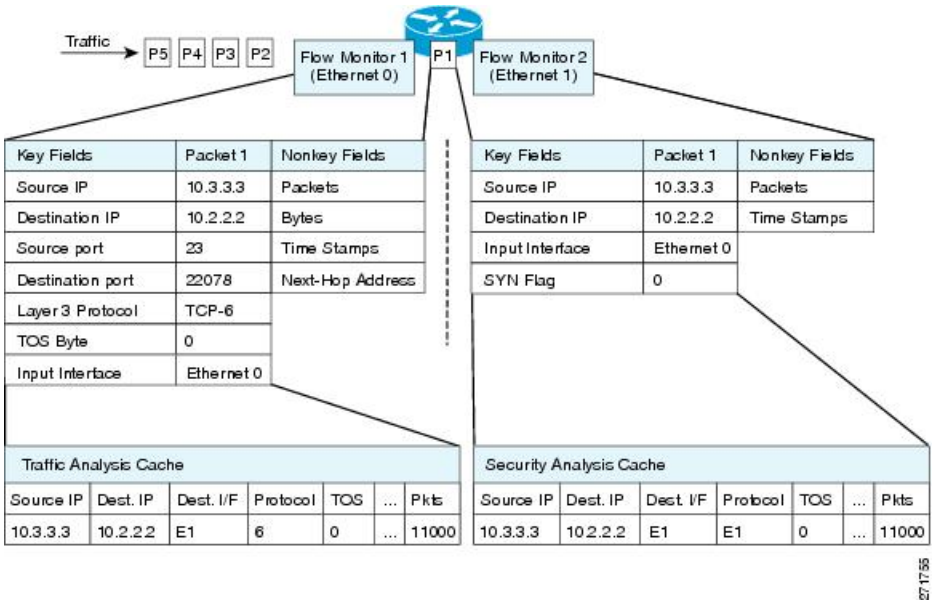
フロー モニタは、ユーザ定義のレコード、オプションのフロー エクスポータ、およびフロー モニタが最初のインターフェイスに適用されるときに自動的に作成されるキャッシュで構成されます。

フロー データはネットワーク トラフィックから収集され、フロー レコードの key フィールドおよび nonkey フィールドに基づいて監視プロセス中にフロー モニタ キャッシュに追加されます。

Flexible NetFlow は、同じトラフィックのさまざまなタイプの分析を実行するために使用できます。下の図では、入力インターフェイス上の標準トラフィック分析のために設計されたレ

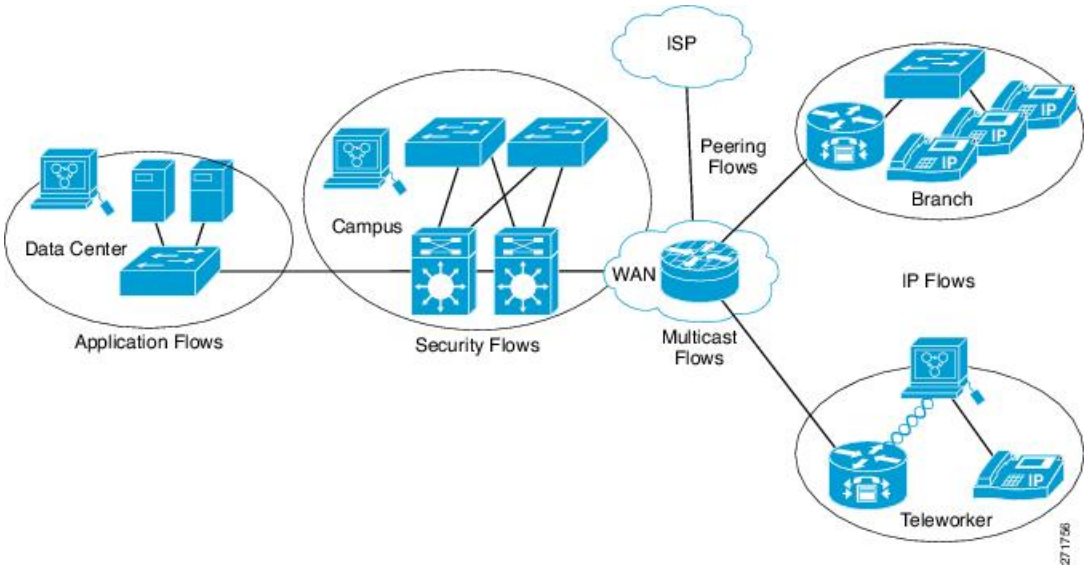
コードと、出力インターフェイス上のセキュリティ分析のために設計されたレコードを使用してパケット 1 が分析されます。

図 *90 : 2* つのフロー モニタを使用した同じトラフィックの分析例



下の図に、カスタム レコードを使用して複数のタイプのフロー モニタを適用するより複雑な方法の例を示します。

図 *91 :* カスタム レコードでの複数のタイプのフロー モニタの複雑な使用例



3 つのタイプのフロー モニタ キャッシュがあります。フロー モニタの作成後に、そのフロー モニタで使用するキャッシュ タイプを変更します。3 タイプのフロー モニタ キャッシュについては、次の各項に説明があります。

標準

デフォルトのキャッシュ タイプは「normal」です。このモードでは、キャッシュ内のエントリが timeout active 設定と timeout inactive 設定に従って期限切れになります。キャッシュ エントリは、期限切れになるとキャッシュから削除され、設定されている何らかのエクスポータによってエクスポートされます。

即時

「immediate」タイプのキャッシュは、作成されるとすぐにレコードを期限切れにします。その結果、どのフローにも 1 パケットしか含まれません。キャッシュ内容を表示するコマンドでは、パケットの履歴が表示されます。

予想されるフローが非常に少なく、パケットが検出されてからレポートがエクスポートされるまでの遅延を最小限にする場合は、このモードが適しています。

注意 このモードでは大量のエクスポートデータが生じて、低速のリンクが過負荷状態になり、エクスポート先のシステムに著しく影響する可能性があります。処理するパケット数を削減するようにサンプリングを設定することをお勧めします。

（注） キャッシュ タイムアウト設定は、このモードでは何の効果もありません。

Permanent

タイプが「permanent」のキャッシュでは、フローが期限切れになることはありません。permanent キャッシュは、検出が予想されるフローの数が少なく、ルータに長期間の統計情報を保存する必要がある場合に便利です。たとえば、フロー レコード内の key フィールドが 8 ビット IP ToS フィールドだけで、256 フローだけを監視する場合があります。ネットワーク トラフィックの IP ToS フィールドの使用状況を長期間に渡って監視するには、permanent キャッシュを使用します。permanent キャッシュは、課金アプリケーション、および追跡対象が固定セットのフローに対する、全域におよぶトラフィック マトリクスに役立ちます。アップデート メッセージは、「timeout update」設定に従って設定されたすべてのフローエクスポータに、定期的に送信されます。

（注） permanent モードでキャッシュがいっぱいになった場合は、新しいフローが監視されなくなります。そうなった場合は、キャッシュの統計情報に「Flows not added」というメッセージが示されます。

（注） permanent キャッシュでは、デルタ カウンタではなくアップデート カウンタが使用されます。そのため、フローがエクスポートされると、カウンタにはフローのライフタイム全体の総検出数が示され、最後のエクスポート送信後に検出された追加パケットは示されません。

フロー サンプラー

フローサンプラーは、ルータのコンフィギュレーションで別のコンポーネントとして作成されます。フロー サンプラーは、分析用に選択されるパケットの数を制限することで、 Flexible NetFlow を実行しているデバイス上の負荷を減らすために使用されます。

サンプラーはランダムサンプリング技術（モード）を使用します。つまり、サンプルを取得するときに、ランダムに選択したサンプリング位置が毎回使用されます。

フロー サンプリングでは、ルータのパフォーマンスに対するモニタリング精度が交換されます。サンプラーをフロー モニタに適用すると、フロー モニタが分析する必要のあるパケット数が減少するため、ルータでフロー モニタを実行するためのオーバーヘッド負荷が低下します。フロー モニタで分析されるパケット数が減少すると、フロー モニタのキャッシュに格納される情報の精度が、それに応じて低下します。

ip flow monitor コマンドを使用してインターフェイスに適用する場合、サンプラーとフロー モニタを組み合わせます。

サポートされている Flexible NetFlow フィールド

次の表では、さまざまなトラフィック タイプおよびトラフィック方向について、Flexible NetFlow（FNF）でサポートされるフィールドの統合リストを提供しています。

（注） パケットに VLAN フィールドがある場合、その長さは考慮されません。

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
Key または **Collect** フィールド							

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
インターフェイス入力	Yes	—	Yes	—	Yes	—	フロー モニタを入力方向に適用する場合： • **match** キーワードを使用し、入力インターフェイスを key フィールドとして使用します。 • **collect** キーワードを使用し、出力インターフェイスを collect フィールドとして使用します。このフィールドはエクスポートされるレコードに含まれますが、値は 0 になります。
インターフェイス出力	—	Yes	—	Yes	—	Yes	フロー モニタを出力方向に適用する場合： • **match** キーワードを使用し、出力インターフェイスを key フィールドとして使用します。 • **collect** キーワードを使用し、入力インターフェイスを collect フィールドとして使用します。このフィールドはエクスポートされるレコードに含まれますが、値は 0 になります。

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
Key フィールド							

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
フロー方向	Yes	Yes	Yes	Yes	Yes	Yes	
Ethertype	Yes	Yes	—	—	—	—	
VLAN 入力	Yes	—	Yes	—	Yes	—	スイッチポートでのみサポートされています。
VLAN 出力	—	Yes	—	Yes	—	Yes	スイッチポートでのみサポートされています。
dot1q VLAN 入力	Yes	—	Yes	—	Yes	—	スイッチポートでのみサポートされています。
dot1q VLAN 出力	—	Yes	—	Yes	—	Yes	スイッチポートでのみサポートされています。
dot1q 優先度	Yes	Yes	Yes	Yes	Yes	Yes	スイッチポートでのみサポートされています。
MAC 送信元アドレス入力	Yes	Yes	Yes	Yes	Yes	Yes	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
MAC 送信元アドレス出力	—	—	—	—	—	—	
MAC 宛先アドレス入力	Yes	—	Yes	—	Yes	—	
MAC 送信先アドレス出力	—	Yes	—	Yes	—	Yes	
IPv4 バージョン	—	—	Yes	Yes	Yes	Yes	
IPv4 TOS	—	—	Yes	Yes	Yes	Yes	
IPv4 プロトコル	—	—	Yes	Yes	Yes	Yes	送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
IPv4 TTL	—	—	Yes	Yes	Yes	Yes	
IPv4 発信元アドレス	—	—	Yes	Yes	—	—	
IPv4 宛先アドレス	—	—	Yes	Yes	—	—	
ICMP IPv4 タイプ	—	—	Yes	Yes	—	—	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
ICMP IPv4 コード	—	—	Yes	Yes	—	—	
IGMP タイプ	—	—	Yes	Yes	—	—	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
Key フィールド（続き）							
IPv6 バージョン	—	—	Yes	Yes	Yes	Yes	IP バージョンと同じです。
IPv6 プロトコル	—	—	Yes	Yes	Yes	Yes	IP プロトコルと同じです。送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
IPv6 送信元アドレス	—	—	—	—	Yes	Yes	
IPv6 宛先アドレス	—	—	—	—	Yes	Yes	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
IPv6 トラフィッククラス	—	—	Yes	Yes	Yes	Yes	IP TOS と同じです。
IPv6 ホップ リミット	—	—	Yes	Yes	Yes	Yes	IP TTL と同じです。
ICMP IPv6 タイプ	—	—	—	—	Yes	Yes	
ICMP IPv6 コード	—	—	—	—	Yes	Yes	
source-port	—	—	Yes	Yes	Yes	Yes	
dest-port	—	—	Yes	Yes	Yes	Yes	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
Collect フィールド							
Bytes long	Yes	Yes	Yes	Yes	Yes	Yes	パケットサイズ =（FCS を含むイーサネットフレームサイズ - 18 バイト） **推奨**： このフィールドを回避し、Bytes layer2 long を使用します。
Packets long	Yes	Yes	Yes	Yes	Yes	Yes	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
Timestamp absolute first	Yes	Yes	Yes	Yes	Yes	Yes	
Timestamp absolute last	Yes	Yes	Yes	Yes	Yes	Yes	
TCP フラグ	Yes	Yes	Yes	Yes	Yes	Yes	すべてのフラグを収集します。
Bytes layer2 long	Yes	Yes	Yes	Yes	Yes	Yes	

デフォルト設定

次の表は、デバイスに対する Flexible NetFlow のデフォルト設定を示します。

表 *81 :* デフォルトの *Flexible NetFlow* 設定

設定	デフォルト
フロー アクティブ タイムアウト	1800 秒
フロー タイムアウトの非アクティブ化	15 秒

Flexible NetFlow の設定方法

Flexible NetFlow を設定するには、次の一般的な手順に従います。

1. フローにキー フィールドおよび非キー フィールドを指定して、フロー レコードを作成します。
2. プロトコルを指定して任意のフローエクスポータを作成し、宛先ポート、宛先、およびその他のパラメータを転送します。
3. フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを作成します。
4. 任意のサンプラーを作成します。
5. レイヤ 2 ポート、レイヤ 3 ポート、または VLAN にフロー モニタを適用します。
6. 必要に応じ、WLAN を設定してフロー モニタを適用します。

カスタマイズしたフロー レコードの設定

カスタマイズしたフロー レコードを設定するには、次のタスクを実行します。

カスタマイズしたフロー レコードは、特定の目的でトラフィック データを分析するために使用します。カスタマイズしたフロー レコードには、key フィールドとして使用する **match** 基準が 1 つ以上必要です。通常は nonkey フィールドとして使用する **collect** 基準が 1 つ以上あります。

カスタマイズしたフロー レコードの順列は、数百もの可能性があります。このタスクでは、可能性のある順列の 1 つを作成するための手順について説明します。必要に応じて当該タスクの手順を変更し、要件に合わせてカスタマイズしたフロー レコードを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flowrecord** *record-name* 例： `Device(config)# flow record FLOW-RECORD-1`	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。 • このコマンドでは、既存のフロー レコードを変更することもできます。
ステップ 4	**description** 説明 例： `Device(config-flow-record)# description Used for basic traffic analysis`	**ipv4**（任意）フロー レコードの説明を作成します。
ステップ 5	**match** { | **ipv6**} {**destination** | **source**} **address** 例：	フロー レコードの key フィールドを設定します。

	コマンドまたはアクション	目的
	`Device(config-flow-record)# match ipv4 destination address`	（注） この例では、IPv4宛先アドレスをレコードのkeyフィールドとして設定します。**matchipv4** コマンドで使用可能な他のkeyフィールド、およびkeyフィールドの設定に使用可能な他の **match** コマンドについては、『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。
ステップ 6	必要に応じてステップ 5 を繰り返し、レコードの追加 key フィールドを設定します。	—

ステップ 7	**match flow cts {source | destination} group-tag**
	例：
	`Device(config-flow-record)# match flow cts source group-tag`
	`Device(config-flow-record)# match flow cts destination group-tag`
		（注） この例では、CTSの送信元グループ タグと宛先グループ タグをレコードのキーフィールドとして設定します。**matchipv4** コマンドで使用可能な他のkeyフィールド、およびkeyフィールドの設定に使用可能な他の **match** コマンドについては、『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。

	コマンドまたはアクション	目的
		（注） • Ingress: • 着信パケットでは、ヘッダーがある場合、SGT にはヘッダーと同じ値が反映されます。値がない場合は、0 が示されます。 • DGT 値は入力ポートの SGACL 設定に依存しません。 • Egress: • SGT または CTS のいずれかの伝播が出力インターフェイス上で無効化されていると、SGT は 0 になります。 • 発信パケットで、（SGT、DGT）に対応する SGACL 設定が存在すれば、DGT はゼロ以外になります。 • SGACL が出力ポート/VLANで無効化されているか、またはグローバル SGACL の強制を無効化されている場合、DGT は 0 になります。
ステップ 8	例：	入力インターフェイスをレコードの nonkey フィールドとして設定します。

	コマンドまたはアクション	目的
		（注） この例では、入力インターフェイスをレコードのnonkeyフィールドとして設定します。nonkeyフィールドの設定に使用可能な他の**collect**コマンドについては、『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。
ステップ 9	必要に応じて上記のステップを繰り返し、レコードの追加nonkeyフィールドを設定します。	—
ステップ 10	**end** 例： `Device(config-flow-record)# end`	Flexible NetFlow フロー レコード コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 11	**showflowrecord** *record-name* 例： `Device# show flow record FLOW_RECORD-1`	（任意）指定したフローレコードの現在のステータスが表示されます。
ステップ 12	**showrunning-configflowrecord** *record-name* 例： `Device# show running-config flow record FLOW_RECORD-1`	（任意）指定したフローレコードの設定が表示されます。

フロー エクスポータの作成

フロー エクスポートを作成して、フローのエクスポート パラメータを定義できます。

（注） フローエクスポータごとに、1つ宛先のみがサポートされます。複数の宛先にデータをエクスポートする場合は、複数のフロー エクスポータを設定してフロー モニタに割り当てる必要があります。

IPv4 または IPv6 アドレスを使用して宛先にエクスポートできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flow exporter** *name* 例： `Device(config)# flow exporter ExportTest`	フローエクスポータを作成し、フローエクスポータ コンフィギュレーション モードを開始します。このコマンドを使用して既存のフローエクスポータを変更することもできます。
ステップ 3	**description** *string* 例： `Device(config-flow-exporter)# description ExportV9`	（任意）最大 63 文字で、このフローの説明を指定します。

ステップ 4	**destination** {*ipv4-address*|*ipv6-address*}
	例：
	`Device(config-flow-exporter)# destination 192.0.2.1 (IPv4 destination)`
	`Device(config-flow-exporter)# destination 2001:0:0:24::10 (IPv6 destination)`
		このエクスポータに IPv4/IPv6 宛先アドレスまたはホスト名を設定します。

ステップ 5	**dscp** *value* 例： `Device(config-flow-exporter)# dscp 0`	（任意）DSCP（DiffServ コードポイント）値を指定します。範囲は 0 ～ 63 です。デフォルトは 0 です。
ステップ 6	**source** { *source type* } 例： `Device(config-flow-exporter)# source gigabitEthernet1/0/1`	（任意）設定された宛先で NetFlow コネクタに到達するために使用するインターフェイスを指定します。送信元として次のインターフェイスを設定できます。 • **Auto Template**：自動テンプレートインターフェイス

	コマンドまたはアクション	目的
		• **Capwap**：Capwap トンネル インターフェイス • **GigabitEthernet**：Gigabit Ethernet IEEE 802 • **GroupVI**：グループ仮想インターフェイス • **Internal Interface**：内部インターフェイス • **Loopback**：ループバック インターフェイス • **Null**：ヌル インターフェイス • **Port-channel**：インターフェイスのイーサネット チャネル • **TenGigabitEthernet**：10 ギガビット イーサネット • **Tunnel**：トンネル インターフェイス • **Vlan**：Catalyst VLAN
ステップ **7**	**transportudp** *number* 例： `Device(config-flow-exporter)# transport udp 200`	（任意）NetFlow コレクタに到達するために使用する UDP ポートを指定します。範囲は 0 ～ 65535 です。 プロトコルをエクスポートする IPFIX の場合、デフォルトの宛先ポートは4739 です。
ステップ **8**	**ttl** *seconds* 例： `Device(config-flow-exporter)# ttl 210`	（任意）エクスポータによって送信されるデータグラムの存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 秒です。デフォルトは 255 です。
ステップ **9**	**export-protocol** {**netflow-v5** |**netflow-v9** | **ipfix**} 例： `Device(config-flow-exporter)# export-protocol netflow-v9`	エクスポータで使用される NetFlow エクスポートプロトコルのバージョンを指定します。 • デフォルト値：**netflow-v9**.
ステップ **10**	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-flow-record)#` **end**	
ステップ 11	**show flow exporter** [**name** *record-name*] 例： `Device` **show flow exporter ExportTest**	（任意）NetFlow のフロー エクスポータ情報を表示します。
ステップ 12	**copy running-config startup-config** 例： `Device#` **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

次のタスク

フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを定義します。

カスタマイズしたフロー モニタの作成

カスタマイズしたフロー モニタを作成するには、この必須のタスクを実行します。

各フロー モニタには、専用のキャッシュが割り当てられています。フロー モニタごとに、キャッシュエントリの内容およびレイアウトを定義するレコードが必要です。これらのレコード フォーマットは、事前定義済みのレコード フォーマットのいずれか、またはユーザ定義にすることができます。上級のユーザであれば **flowrecord** コマンドを使用して、カスタマイズしたフォーマットを作成することもできます。

始める前に

Flexible NetFlow の事前定義済みレコードの代わりにカスタマイズしたレコードを使用する場合は、このタスクを実行する前に、カスタマイズしたレコードを作成する必要があります。データをエクスポートするためにフロー エクスポータをフロー モニタに追加する場合は、このタスクを完了する前にエクスポータを作成する必要があります。

（注） フロー モニタで **record** コマンドのパラメータを変更する前に、**no ip flow monitor** コマンドを使用して、フロー モニタを適用したすべてのインターフェイスから、フロー モニタを削除しておく必要があります。**ip flowmonitor** コマンドの詳細については、『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow monitor** *monitor-name* 例： `Device(config)# flow monitor FLOW-MONITOR-1`	フロー モニタを作成し、Flexible NetFlow フロー モニタ コンフィギュレーション モードを開始します。 • このコマンドでは、既存のフローモニタを変更することもできます。
ステップ 4	**description** 説明 例： `Device(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	（任意）フローモニタの説明を作成します。
ステップ 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} 例： `Device(config-flow-monitor)# record FLOW-RECORD-1`	フロー モニタのレコードを指定します。
ステップ 6	**cache** {**entries** *number* |**timeout** {**active** | **inactive** | **update**} *seconds* | {**immediate** | **normal** | **permanent**}} 例：	**timeout** キーワードに関連するキーワードの値は、キャッシュ タイプが **immediate** に設定されている場合には反映されません。 指定したフローモニタとフローキャッシュを関連付けます。
ステップ 7	必要に応じてステップ 6 を繰り返して、このフローモニタのキャッシュ パラメータの変更を完了します。	—

	コマンドまたはアクション	目的
ステップ 8	**statisticspacket protocol** 例： `Device(config-flow-monitor)# statistics packet protocol`	（任意）Flexible NetFlow モニタのプロトコル分散統計情報の収集をイネーブルにします。
ステップ 9	**statisticspacket size** 例： `Device(config-flow-monitor)# statistics packet size`	（任意）Flexible NetFlow モニタのサイズ分散統計情報の収集をイネーブルにします。
ステップ 10	**exporter** *exporter-name* 例： `Device(config-flow-monitor)# exporter EXPORTER-1`	（任意）事前に作成されたエクスポータの名前を指定します。
ステップ 11	**end** 例： `Device(config-flow-monitor)# end`	Flexible NetFlow フロー モニタ コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 12	**showflowmonitor**[[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] 例： `Device# show flow monitor FLOW-MONITOR-2 cache`	（任意）Flexible NetFlow フロー モニタのステータスおよび統計情報を表示します。
ステップ 13	**showrunning-configflowmonitor** *monitor-name* 例： `Device# show running-config flow monitor FLOW_MONITOR-1`	（任意）指定したフローモニタの設定が表示されます。
ステップ 14	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

フロー サンプリングの設定および有効化フロー サンプラーの作成

フロー サンプラーを設定して有効化するには、この必須のタスクを実行します。

（注） 「NetFlow original」/「NetFlow IPv4 original input」/「NetFlow IPv6 original input」事前定義済みレコードをフロー モニタに指定して、以前の NetFlow をエミュレートする場合は、フロー モニタを入力（受信）トラフィックの分析だけに使用できます。

「NetFlow IPv4 original output」/「NetFlow IPv6 original output」事前定義済みレコードをフローモニタに指定して、出力NetFlowアカウンティング機能をエミュレートする場合は、フローモニタを出力（発信）トラフィックの分析だけに使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**sampler** *sampler-name* 例： `Device(config)# sampler SAMPLER-1`	サンプラーを作成し、サンプラー コンフィギュレーションモードを開始します。 • このコマンドでは、既存のサンプラーを変更することもできます。
ステップ 4	**description** 説明 例： `Device(config-sampler)# description Sample at 50%`	（任意）フローサンプラーの説明を作成します。
ステップ 5	**mode** {**random**} **1 out-of** *window-size* 例： `Device(config-sampler)# mode random 1 out-of 2`	サンプラー モードおよびフローサンプラーのウィンドウ サイズを指定します。 • *window-size* 引数の範囲は、0 ～ 10242 ～ 32768 です。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-sampler)# exit`	サンプラー コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	{**ip** | **ipv6**} **flowmonitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** | **output**} 例： `Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input`	作成したフローモニタおよびフローサンプラーをインターフェイスに割り当てて、サンプリングをイネーブルにします。
ステップ 9	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**showsamplersampler-name** 例： `Device# show sampler SAMPLER-1`	設定し有効化したフローサンプラーのステータスおよび統計情報を表示します。

インターフェイスへのフローの適用

フロー モニタおよびオプションのサンプラーをインターフェイスに適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type* 例： `Device(config)# interface`	インターフェイスコンフィギュレーション モードを開始し、インターフェイスを設定します。

	コマンドまたはアクション	目的
	GigabitEthernet1/0/1	Flexible NetFlow は、L2 ポートチャネル インターフェイスではサポートされませんが、L2 ポートチャネル メンバー ポートではサポートされます。 Flexible NetFlow は、L3 ポートチャネル メンバー ポートではサポートされませんが、L3 ポートチャネル インターフェイスではサポートされます。 インターフェイスコンフィギュレーションのコマンド パラメータは次のとおりです。 • **GigabitEthernet**：GigabitEthernet IEEE 802 • **Loopback**：ループバック インターフェイス • **TenGigabitEthernet**：10 ギガビット イーサネット • **Vlan**：Catalyst VLAN • **Range**：インターフェイス範囲 • **WLAN**：WLAN インターフェイス
ステップ 3	{**ip flow monitor** | **ipv6 flow monitor**}*name* [|**sampler** *name*] { **input**} 例： `Device(config-if)# ip flow monitor MonitorTest input`	入力または出力パケットに対応するインターフェイスに、IPv4 または IPv6 フロー モニタ、およびオプションのサンプラーを関連付けます。
ステップ 4	**end** 例： `Device(config-flow-monitor)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show flow interface** [*interface-type number*] 例： `Device# show flow interface`	（任意）インターフェイスの NetFlow 情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN 上でのブリッジ型 NetFlow の設定

フロー モニタおよびオプションのサンプラーを VLAN に適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vlan** [**configuration**] *vlan-id*
	例：
	`Device(config)# vlan configuration 30`
	`Device(config-vlan-config)#`
		VLAN または VLAN コンフィギュレーション モードを開始します。

ステップ 3	**ip flow monitor** *monitor name* [**sampler** *sampler name*] {**input** |**output**} 例： `Device(config-vlan-config)# ip flow monitor MonitorTest input`	入力または出力パケットに対応する VLANに、フローモニタおよびオプションのサンプラーを関連付けます。
ステップ 4	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

レイヤ 2 NetFlow の設定

Flexible NetFlow レコード内でレイヤ 2 キーを定義できます。このレコードを使用して、レイヤ 2 インターフェイスのフローをキャプチャできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**flow record** *name*
	例：
	`Device(config)# flow record L2_record`
	`Device(config-flow-record)#`
		フロー レコード コンフィギュレーション モードを開始します。

ステップ 3	**match datalink** {**dot1q** |**ethertype** | **mac** | **vlan**} 例： `Device(config-flow-record)# match datalink ethertype`	レイヤ2属性をキーとして指定します。
ステップ 4	**end** 例： `Device(config-flow-record)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show flow record** [*name*] 例： `Device# show flow record`	（任意）インターフェイスの NetFlow 情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

データ リンクの入出力方向にフロー モニタを適用する WLAN 設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan [wlan-name { wlan-id SSID_NetworkName | wlan_id} | wlan-name | shutdown}** 例： `Device (config) # wlan wlan1`	WLAN コンフィギュレーション サブモードを開始します。 *wlan-id* はワイヤレス LAN の ID です。指定できる範囲は 1 ～ 64 です。 SSID_NetworkName は、最大 32 文字の英数字からなる SSID です。 （注） すでにこのコマンドを設定している場合は、**wlan** *wlan-name* コマンドを入力します。
ステップ 3	**datalink flow monitor monitor-name {input | output}** 例： `Device (config-wlan) # datalink flow monitor flow-monitor-1 {input | output}`	目的の方向のレイヤ2 トラフィックにフロー モニタを適用します。
ステップ 4	**end** 例： `Device (config) # end`	特権 EXEC モードに戻ります。
ステップ 5	**show run wlan** *wlan-name* 例： `Device # show wlan mywlan`	（任意）設定を確認します。

例

IPV4 および IPv6 の入出力方向にフロー モニタを適用する WLAN 設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan {wlan-name { wlan-id SSID_NetworkName | wlan_id} | wlan-name | shutdown}** 例： `Device (config) # wlan wlan1`	WLAN コンフィギュレーション サブモードを開始します。 *wlan-id* はワイヤレス LAN の ID です。指定できる範囲は 1 ～ 64 です。 SSID_NetworkName は、最大 32 文字の英数字からなる SSID です。 （注） すでにこのコマンドを設定している場合は、**wlan** *wlan-name* コマンドを入力します。
ステップ 3	**{ip | ipv6} flow monitor monitor-name {input | output}** 例： `Device (config-wlan) # ip flow monitor flow-monitor-1 input`	入力または出力パケットに対応する WLAN にフロー モニタを関連付けます。
ステップ 4	**end** 例： `Device (config) # end`	特権 EXEC モードに戻ります。
ステップ 5	**show run wlan** *wlan-name* 例： `Device # show wlan mywlan`	（任意）設定を確認します。

例

Flexible NetFlow の監視

次の表にあるコマンドを使用して、Flexible NetFlow をモニタリングできます。

表 *82 : Flexible NetFlow* のモニタリング コマンド

コマンド	目的
show flow exporter [**broker** | **export-ids** | **name** | *name* | **statistics** | **templates**]	NetFlow のフロー エクスポータ情報と統計情報を表示します。
show flow exporter [**name** *exporter-name*]	NetFlow のフロー エクスポータ情報と統計情報を表示します。
show flow interface	NetFlowインターフェイスに関する情報を表示します。
show flow monitor [**name** *exporter-name*]	NetFlow のフロー モニタ情報と統計情報を表示します。
show flow monitor statistics	フロー モニタの統計情報を表示します。
show flow monitor cache format {**table** | **record** | **csv**}	指定された形式でフロー モニタのキャッシュの内容を表示します。
show flow record [**name** *record-name*]	NetFlowのフロー レコード情報を表示します。
show flow ssid	WLAN の NetFlow モニタのインストール ステータスを表示します。
show sampler [**broker** | **name** | *name*]	NetFlowサンプラに関する情報を表示します。
show wlan *wlan-name*	デバイスで設定された WLAN を表示します。

Flexible NetFlow の設定例

例：フローの設定

フローを作成し、そのフローをインターフェイスに適用する例を示します。

```
Device# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# flow export export1
Device(config-flow-exporter)# destination 10.0.101.254
Device(config-flow-exporter)# transport udp 2055
Device(config-flow-exporter)# exit
Device(config)# flow record record1
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match flow cts source group-tag
Device(config-flow-record)# match flow cts destination group-tag
Device(config-flow-record)# collect counter byte long
Device(config-flow-record)# collect counter packet long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# exit
Device(config)# flow monitor monitor1
Device(config-flow-monitor)# record record1
Device(config-flow-monitor)# exporter export1
Device(config-flow-monitor)# exit
Device(config)# interface tenGigabitEthernet 1/0/1
Device(config-if)# ip flow monitor monitor1 input
Device(config-if)# end
```

例：IPv4 入力トラフィックのモニタリング

次の例は、IPv4 入力トラフィックをモニタする方法を示しています（int g1/0/11 は、int g1/0/36 および int g3/0/11 にトラフィックを送信します）。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow record  fr-1
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match interface input
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect counter bytes layer2 long
Device(config-flow-record)# exit

Device(config)# flow exporter fe-ipfix6
Device(config-flow-exporter)# destination 2001:0:0:24::10
Device(config-flow-exporter)# source Vlan106
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix
Device(config-flow-exporter)# description IPFIX format collector 100.0.0.80
Device(config-flow-exporter)# destination 100.0.0.80
Device(config-flow-exporter)# dscp 30
```

```
Device(config-flow-exporter)# ttl 210
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-1
Device(config-flow-exporter)# destination 10.5.120.16
Device(config-flow-exporter)# source Vlan105
Device(config-flow-exporter)# dscp 32
Device(config-flow-exporter)# ttl 200
Device(config-flow-exporter)# transport udp 2055

Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow monitor fm-1
Device(config-flow-monitor)# exporter fe-ipfix6
Device(config-flow-monitor)# exporter fe-ipfix
Device(config-flow-monitor)# exporter fe-1
Device(config-flow-monitor)# cache timeout inactive 60
Device(config-flow-monitor)#  cache timeout active 180
Device(config-flow-monitor)# record fr-1
Device(config-flow-monitor)# end

Device# show running-config interface g1/0/11
Device# show running-config interface g1/0/36
Device# show running-config interface g3/0/11
Device# show flow monitor fm-1 cache format table
```

例：IPv4 出力トラフィックのモニタリング

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow record  fr-1 out
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match interface output
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# exit

Device(config)# flow exporter fe-1
Device(config-flow-exporter)# destination 10.5.120.16
Device(config-flow-exporter)# source Vlan105
Device(config-flow-exporter)# dscp 32
Device(config-flow-exporter)# ttl 200
Device(config-flow-exporter)# transport udp 2055
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix6
Device(config-flow-exporter)# destination 2001:0:0:24::10
Device(config-flow-exporter)# source Vlan106
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
```

```
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix
Device(config-flow-exporter)# description IPFIX format collector 100.0.0.80
Device(config-flow-exporter)# destination 100.0.0.80
Device(config-flow-exporter)# dscp 30
Device(config-flow-exporter)# ttl 210
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow monitor fm-1-output
Device(config-flow-monitor)# exporter fe-1
Device(config-flow-monitor)# exporter fe-ipfix6
Device(config-flow-monitor)# exporter fe-ipfix
Device(config-flow-monitor)# cache timeout inactive 50
Device(config-flow-monitor)#  cache timeout active 120
Device(config-flow-monitor)# record fr-1-out
Device(config-flow-monitor)# end

Device# show flow monitor fm-1-output cache format table
```

例：WLAN（入力方向）の IPv4 Flexible NetFlow の設定

次に、WLAN 入力方向で IPv4 Flexible NetFlow を設定する例を示します。

```
flow record WLAN-FLOW07
 description Working AP mac
 match datalink mac source address input
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match wireless ssid
 collect counter bytes long
 collect counter packets long
 collect wireless ap mac address
flow monitor WLAN-FLOW07
 exporter wlan-export
 cache timeout inactive 30
 cache timeout active 10
 record WLAN-FLOW07
wlan CC0506-CC0404
 ip flow monitor WLAN-FLOW07 input

Device#show flow monitor WLAN-FLOW07 cache
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 6

Flows added: 276
Flows aged: 270

    Active timeout ( 10 secs) 257
    Inactive timeout ( 30 secs) 13

DATALINK MAC SOURCE ADDRESS INPUT: 3CA9.F421.4E34
IPV4 SOURCE ADDRESS: 192.168.11.1
```

```
IPV4 DESTINATION ADDRESS: 10.29.5.6
WIRELESS SSID: CC0506-CC0404
IP TOS: 0x00
IP PROTOCOL: 6
counter bytes long: 66
counter packets long: 1
wireless ap mac address: B0AA.778E.EB60
```

例：WLAN（出力方向）の IPv6 および転送フラグ Flexible NetFlow の設定

次に、WLAN 出力方向で IPv6 および転送フラグ Flexible NetFlow を設定する例を示します。

```
Device# configure terminal
Device(config)# flow record fr_v6
Device(config-flow-record)# match ipv6 destination address
Device(config-flow-record)# match ipv6 source address
Device(config-flow-record)# match ipv6 hop-limit
Device(config-flow-record)# match ipv6 protocol
Device(config-flow-record)# match ipv6 traffic
Device(config-flow-record)# match ipv6 version
Device(config-flow-record)# match wireless ssid
Device(config-flow-record)# collect wireless ap mac address
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect transport tcp flags
Device(config-flow-record)# exit

Device(config)# flow monitor fm_v6
Device(config-flow-monitor)# record fr_v6
Device(config-flow-monitor)# exit

Device(config)# wlan wlan_1
Device(config-wlan)# ipv6 flow monitor fm_v6 out
Device(config-wlan)# end

Device# show flow monitor fm_v6 cache
```

（注） デバイスでは、収集する TCP フラグを指定できません。転送 TCP フラグの収集のみ指定できます。

例：WLAN（入力および出力の両方向）の IPv6 Flexible NetFlow の設定

次に、双方向の WLAN 上で IPv6 Flexible NetFlow を設定する例を示します。

```
Device# configure terminal
Device (config)# flow record fr_v6
Device (config-flow-record)# match ipv6 destination address
Device (config-flow-record)# match ipv6 source address
Device (config-flow-record)# match ipv6 hop-limit
```

```
Device (config-flow-record)# match ipv6 protocol
Device (config-flow-record)# match ipv6 traffic
Device (config-flow-record)# match ipv6 version
Device (config-flow-record)# match wireless ssid
Device (config-flow-record)# collect wireless ap mac address
Device (config-flow-record)# collect counter packets long
Device (config-flow-record)# exit

Device (config)# flow monitor fm_v6
Device (config-flow-monitor)# record fr_v6
Device (config-flow-monitor)# exit

Device (config)# wlan wlan_1
Device (config-wlan)# ipv6 flow monitor fm_v6 in
Device (config-wlan)# ipv6 flow monitor fm_v6 out
Device (config-wlan)# end

Device# show flow monitor fm_v6 cache
```

例：ワイヤレス入力トラフィックのモニタリング

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow record fr-wlan-input
Device(config-flow-record)# match datalink mac source address input
Device(config-flow-record)# match datalink mac destination address input
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match wireless ssid
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# exit

Device(config)# flow exporter fe-ipfix
Device(config-flow-exporter)# description IPFIX format collector 100.0.0.80
Device(config-flow-exporter)# destination 100.0.0.80
Device(config-flow-exporter)# dscp 30
Device(config-flow-exporter)# ttl 210
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix6
Device(config-flow-exporter)# destination 2001:0:0:24::10
Device(config-flow-exporter)# source Vlan106
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow monitor fm-wlan-input
Device(config-flow-monitor)# exporter fe-ipfix
Device(config-flow-monitor)# exporter fe-ipfix6
Device(config-flow-monitor)# cache timeout inactive 30
Device(config-flow-monitor)#  cache timeout active 180
Device(config-flow-monitor)# record fr-wlan-input
```

```
Device(config-flow-monitor)# end

Device# show running-config wlan nfl_1
Device# show flow monitor fm-wlan-input cache format table
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Flexible NetFlow の CLI コマンド	『*Cisco Flexible NetFlow Command Reference (Catalyst 3850 Switches)*』 『*Flexible NetFlow Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
RFC 3954	『Cisco Systems NetFlow Services Export Version 9』

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

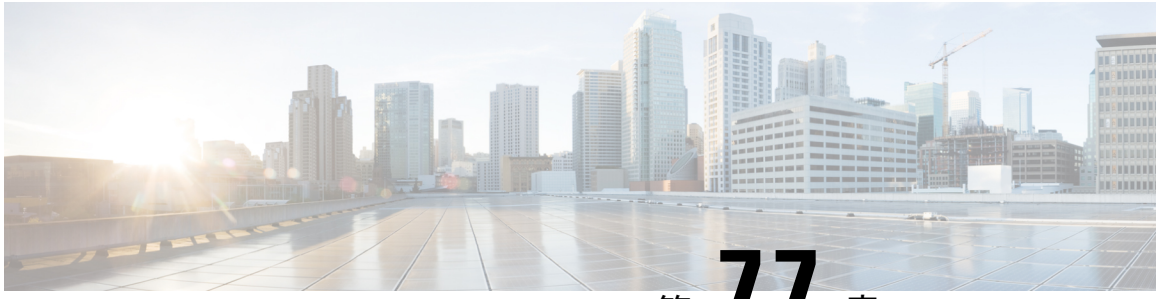
Flexible NetFlow の機能情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。
Cisco IOS XE 3.3SE	次の新しいコマンドが追加されました。 • **match wireless ssid** • **collect wireless ap mac address**

第 XIII 部

Network Powered Lighting

- COAP プロキシ サーバの設定 （1459 ページ）
- Autosmart ポートの設定 （1475 ページ）
- 2 イベント分類の設定 （1479 ページ）
- 無停止型 POE の設定 （1483 ページ）
- FAQ （1489 ページ）



第 77 章

COAP プロキシ サーバの設定

- 機能情報の確認 （1459 ページ）
- COAP プロキシ サーバについて （1459 ページ）
- COAP の制約事項 （1460 ページ）
- COAP プロキシ サーバでサポートされるハードウェア （1460 ページ）
- COAP プロキシ サーバの設定 （1463 ページ）
- COAP プロキシ サーバのモニタリング （1468 ページ）
- 例：COAP プロキシ サーバ （1469 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

COAP プロキシ サーバについて

COAP プロトコルは、制限されたデバイスで使用できるように設計されています。HTTP が情報にアクセスする際にサーバ上で動作するのと同じ方法で、COAP は制限されたデバイス上で動作します。

COAP と HTTP の比較を次に示します。

- Web サーバの場合：**HTTP** がプロトコルで、**TCP** がトランスポートです。**HTML** は転送される最も一般的な情報の形式です。

- 制限されたデバイスの場合：**COAP** がプロトコルで、**UDP** がトランスポートです。そして **JSON/link-format/CBOR** が一般的な情報形式です。

COAP によって、HTTP と同様の **GET/POST** メタファーおよび restful API を使用して、デバイスにアクセスして制御する手段が提供されます。

関連トピック

COAP プロキシの設定 （1464 ページ）
例：COAP プロキシ サーバ （1469 ページ）

COAP の制約事項

次の制約事項は、COAP プロキシ サーバに適用されます。

- スイッチは、ipv6 ブロードキャスト（CSCuw26467）を使用する CoAP クライアントとして自身をアドバタイズできません。
- 監視のサポートは実装されていません。
- Blockwise 要求はサポートされていません。シスコは、block-wise 応答を処理し、block-wise 応答を生成できます。
- DTLS サポートは、RawPublicKey および証明書ベースのモードに対してのみ有効です。
- IPv6 DTLS は、3850 プラットフォームではサポートされません。
- スイッチは、DTLS クライアントとして動作しません。DTLS はエンドポイントに対してのみ。
- エンドポイントは、CBOR ペイロードを処理し、応答すると想定されています。
- クライアント側要求は、JSON であると想定されています。
- IPv6 ブロードキャストの問題により、スイッチは IPv6 として他のリソース ディレクトリに自身をアドバタイズすることはできません。
- 高速 PoE、無停止型 PoE、または 2 イベント分類の設定は、エンドポイントを物理的に接続する前に行う必要があります。または、電力を供給しているポートの手動 shut/no-shut を行います。
- ポートへの電源供給は MCU ファームウェアのアップグレード時には中断され、ポートはアップグレード直後にバックアップされます。

COAP プロキシ サーバでサポートされるハードウェア

COAP プロキシ サーバは、次の Catalyst 3850 スイッチ モデルでサポートされます。

スイッチ モデル	Cisco IOS イメージ	説明
WS-C3850-24T-S	IP Base	Cisco Catalyst 3850 スタッカブル 24 X 10/100/1000 イーサネット ポート、350 WAC 電源 1 RU、IP Base フィーチャ セット搭載
WS-C3850-48T-S	IP Base	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット ポート、350 WAC 電源 1 RU、IP Base フィーチャ セット搭載
WS-C3850-24P-S	IP Base	Cisco Catalyst 3850 スタッカブル 24 X 10/100/1000 イーサネット PoE+ ポート、715 WAC 電源 1 RU、IP Base フィーチャ セット搭載
WS-C3850-48P-S	IP Base	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット PoE+ ポート、715 WAC 電源 1 RU、IP Base フィーチャ セット搭載
WS-C3850-48F-S	IP Base	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット PoE+ ポート、1100 WAC 電源 1 RU、IP Base フィーチャ セット搭載
WS-C3850-24U-S	IP Base	24 X 10/100/1000 Cisco UPOE ポート（スタック可能）、1 X ネットワーク モジュール スロット、1100 W 電源
WS-C3850-48U-S	IP Base	48 X 10/100/1000 Cisco UPOE ポート（スタック可能）、1 X ネットワーク モジュール スロット、1100 W 電源
WS-C3850-12S-S	IP Base	12 × SFP モジュール スロット（スタック可能）、1 × ネットワーク モジュール スロット、350 W 電源
WS-C3850-24S-S	IP Base	24 × SFP モジュール スロット（スタック可能）、1 × ネットワーク モジュール スロット、350 W 電源
WS-C3850-12XS-S	IP Base	Catalyst 3850 12 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、350 W 電源
WS-C3850-16XS-S	IP Base	Catalyst 3850 16 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、350 W 電源 C3850-NM-4-10G ネットワーク モジュールが WS-C3850-12XS-S スイッチに接続されている場合は、16ポートを使用できます。
WS-C3850-24XS-S	IP Base	Catalyst 3850 24 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、715 W 電源

スイッチ モデル	Cisco IOS イメージ	説明
WS-C3850-32XS-S	IP Base	Catalyst 3850 32 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、715 W 電源 C3850-NM-8-10G ネットワーク モジュールが WS-C3850-24XS-S スイッチに接続されている場合は、32 ポートを使用できます。
WS-C3850-48XS-S	IP Base	スタック可能、SFP+ トランシーバ、48 X ポート（最大 10 G をサポート）、4 X ポート（最大 40 G をサポート）、750 W 電源を搭載
WS-C3850-48XS-F-S	IP Base	スタック可能、SFP+ トランシーバ、48 X ポート（最大 10 G をサポート）、4 X ポート（最大 40 G をサポート）、750 W 電源を搭載
WS-C3850-24XU-S	IP Base	24 X 100M/1G/2.5G/5G/10G UPOE ポート（スタック可能）、1 X ネットワーク モジュール スロット、1100 W 電源
WS-C3850-24T-E	IP サービス	Cisco Catalyst 3850 スタッカブル 24 X 10/100/1000 イーサネット ポート、350 WAC 電源 1 RU、IP Services フィーチャ セット搭載
WS-C3850-48T-E	IP サービス	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット ポート、350 WAC 電源 1 RU、IP Services フィーチャ セット搭載
WS-C3850-24P-E	IP サービス	Cisco Catalyst 3850 スタッカブル 24 X 10/100/1000 イーサネット PoE+ ポート、715 WAC 電源 1 RU、IP Services フィーチャ セット搭載
WS-C3850-48P-E	IP サービス	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット PoE+ ポート、715 WAC 電源 1 RU、IP Services フィーチャ セット搭載
WS-C3850-48F-E	IP サービス	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット PoE+ ポート、1100 WAC 電源 1 RU、IP Services フィーチャ セット搭載
WS-3850-24U-E	IP サービス	Cisco Catalyst 3850 スタッカブル 24 × 10/100/1000 Cisco UPOE ポート、1 × ネットワーク モジュール スロット、1100 W 電源
WS-3850-48U-E	IP サービス	Cisco Catalyst 3850 スタッカブル 48 × 10/100/1000 Cisco UPOE ポート、1 × ネットワーク モジュール スロット、1100 W 電源
WS-C3850-12S-E	IP サービス	2 × SFP モジュール スロット（スタック可能）、1 × ネットワーク モジュール スロット、350 W 電源

スイッチ モデル	Cisco IOS イメージ	説明
WS-C3850-24S-E	IP サービス	24 × SFP モジュール スロット（スタック可能）、1 × ネットワーク モジュール スロット、350 W 電源
WS-C3850-12XS-E	IP サービス	Catalyst 3850 12 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、350 W 電源
WS-C3850-16XS-E	IP サービス	Catalyst 3850 16 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、350 W 電源 C3850-NM-4-10G ネットワーク モジュールが WS-C3850-12XS-E スイッチに接続されている場合は、16ポートを使用できます。
WS-C3850-24XS-E	IP サービス	Catalyst 3850 24 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、715 W 電源
WS-C3850-32XS-E	IP サービス	Catalyst 3850 32 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、715 W 電源 C3850-NM-8-10G ネットワーク モジュールが WS-C3850-24XS-E スイッチに接続されている場合は、32ポートを使用できます。
WS-C3850-48XS-E	IP サービス	スタック可能、SFP+ トランシーバ、48 X ポート（最大 10 G をサポート）、4 X ポート（最大 40 G をサポート）、750 W 電源を搭載
WS-C3850-48XS-F-E	IP サービス	スタック可能、SFP+ トランシーバ、48 X ポート（最大 10 G をサポート）、4 X ポート（最大 40 G をサポート）、750 W 電源を搭載
WS-C3850-24XU-E	IP サービス	24 X 100M/1G/2.5G/5G/10G UPOE ポート（スタック可能）、1 X ネットワーク モジュール スロット、1100 W 電源

COAP プロキシ サーバの設定

COAP プロキシ サーバを設定するには、コンフィギュレーション モードで COAP プロキシと COAP エンドポイントを設定できます。

コマンドは **coap [proxy | endpoints]** です。

COAP プロキシの設定

スイッチで COAP プロキシを開始または停止するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**coap proxy** 例： `Device(config)# coap proxy`	COAP プロキシ サブモードを開始します。 （注） coap プロキシを停止して、coap プロキシの下にあるすべての設定を削除するには、**no coap proxy** コマンドを使用します。
ステップ 4	**security** [**none** [[**ipv4** | **ipv6**] {*ip-address ip-mask/prefix*} | **list** {*ipv4-list name* | *ipv6-list-name*}] | **dtls** [**id-trustpoint** {*identity-trustpoint label*}] [**verification-trustpoint** {*verification-trustpoint*} | [**ipv4** | **ipv6** {*ip-address ip-mask/prefix*}] | **list** {*ipv4-list name* | *ipv6-list-name*}]] 例： `Device(config-coap-proxy)# security none ipv4 1.1.0.0 255.255.0.0`	暗号化タイプを引数と見なします。サポートされる 2 つのセキュリティ モードは **none** および **dtls** • none：そのポートにセキュリティがないことを示します。 **security none** を使用して、最大 5 つの ipv4 アドレスと 5 つの ipv6 アドレスを関連付けることができます。 • dtls：DTLS セキュリティは、オプションである RSA トラストポイントと検証トラストポイントを要します。検証トラストポイントがないと、通常の公開キー交換が行われます。

	コマンドまたはアクション	目的
		security dtls を使用して、最大 5 つの ipv4 アドレスと 5 つの ipv6 アドレスを関連付けることができます。 （注） coap プロキシの下にあるすべてのセキュリティ設定を削除するには、**no security** コマンドを使用します。
ステップ 5	**max-endpoints** {*number*} 例： `Device(config-coap-proxy)#max-endpoints 10`	（任意）スイッチで学習できるエンドポイントの最大数を指定します。デフォルト値は 10 です。指定できる範囲は 1 ～ 500 です。 （注） coap プロキシの下に設定されているすべての最大エンドポイントを削除するには、**no max-endpoints** コマンドを使用します。
ステップ 6	**port-unsecure** {*port-num*} 例： `Device(config-coap-proxy)#port-unsecure 5683`	（任意）デフォルト 5683 以外のポートを設定します。指定できる範囲は 1 ～ 65000 です。 （注） coap プロキシの下にあるすべてのポート設定を削除するには、**no port-unsecure** コマンドを使用します。
ステップ 7	**port-dtls** {*port-num*} 例： `Device(config-coap-proxy)#port-dtls 5864`	（任意）デフォルト 5684 以外のポートを設定します。 （注） coap プロキシの下にあるすべての dtls ポート設定を削除するには、**no port-dtls** コマンドを使用します。
ステップ 8	**resource-directory** [ipv4 | ipv6] {*ip-address*}] 例： `Device(config-coap-proxy)#resource-directory`	スイッチが COAP クライアントとして動作できるユニキャスト アップストリーム リソースのディレクトリ サーバを設定します。

	コマンドまたはアクション	目的
	`ipv4 192.168.1.1`	**resource-directory** を使用して、最大 5 つの ipv4 IP アドレスと 5 つの ipv6 IP アドレスを設定できます。 （注） coap プロキシの下にあるすべてのリソースディレクトリ設定を削除するには、**no resource-directory** コマンドを使用します。
ステップ 9	**list** [**ipv4** | **ipv6**] {*list-name*} 例： `Device(config-coap-proxy)#list ipv4 trial_list`	（任意）ライトとリソースを学習できる IP アドレス範囲を制限します。上記の **security** [**none** | **dtls**] コマンド オプションで使用する、IP アドレス/マスクの名前付きリストを作成します。 **list** を使用して、ipv4 または ipv6 に関係なく、最大 5 つの IP リストを設定できます。IP リストにつき最大 5 つの IP アドレスを設定できます。 （注） COAP プロキシ サーバで IP リストを削除するには、**no list** [**ipv4** | **ipv6**] {*list-name*} コマンドを使用します。
ステップ 10	**start** 例： `Device(config-coap-proxy)#start`	このスイッチで COAP プロキシを開始します。
ステップ 11	**stop** 例： `Device(config-coap-proxy)#stop`	このスイッチで COAP プロキシを停止します。
ステップ 12	**exit** 例： `Device(config-coap-proxy)# exit`	COAP プロキシ サブモードを終了します。
ステップ 13	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	

関連トピック

COAP プロキシ サーバについて （1459 ページ）
例：COAP プロキシ サーバ （1469 ページ）

COAP エンドポイントの設定

複数の IPv4/IPv6 スタティック エンドポイントをサポートするように COAP プロキシを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**coap endpoint** [**ipv4** | **ipv6**] {*ip-address*}
	例：
	`Device(config)#coap endpoint ipv4 1.1.1.1`
	`Device(config)#coap endpoint ipv6 2001::1`
		スイッチ上でスタティック エンドポイントを設定します。
		• **ipv4** ：IPv4 スタティック エンドポイントを設定します。
		• **ipv6** ：IPv6 スタティック エンドポイントを設定します。
		（注） エンドポイントで coap プロキシを停止するには、**no coap endpoint** [**ipv4** |**ipv6**] {*ip-address*} コマンドを使用します。

ステップ 4	**exit** 例：	COAP エンドポイント サブモードを終了します。

	コマンドまたはアクション	目的
	`Device(config-coap-endpoint)# exit`	
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

COAP プロキシ サーバのモニタリング

COAP プロトコルの詳細を表示するには、次の表のコマンドを使用します。

表 *83 : COAP* 固有のデータを表示するコマンド

show coap version	IOS COAP バージョンと RFC 情報を表示します。
show coap resources	スイッチのリソースと、スイッチが学習したリソースを表示します。
show coap endpoints	検出され、学習されたエンドポイントを表示します。
show coap globals	タイマー値とエンドポイント値を表示します。
show coap stats	エンドポイント、要求、および外部クエリのメッセージ数を表示します。
show coap dtls-endpoints	dtls エンドポイントのステータスを表示します。

表 *84 : COAP* コマンドをクリアするコマンド

clear coap database	スイッチで学習された COAP、およびエンドポイント情報の内部データベースをクリアします。

COAP プロトコルをデバッグするには、次の表のコマンドを使用します。

表 *85 : COAP* プロトコルをデバッグするコマンド

debug coap database	COAP データベース出力をデバッグします。
debug coap errors	COAP エラー出力をデバッグします。
debug coap events	COAP イベント出力をデバッグします。

debug coap packets	COAP パケット出力をデバッグします。
debug coap trace	COAP トレース出力をデバッグします。
debug coap warnings	COAP 警告出力をデバッグします。
debug coap all	すべての COAP 出力をデバッグします。

（注） デバッグを無効にする場合は、コマンドの前に「**no**」キーワードを追加します。

例：COAP プロキシ サーバ

次の例に、最大 10 のエンドポイントをサポートするようにポート番号 5683 を設定する方法を示します。

```
Device#coap proxy security none ipv4 2.2.2.2 255.255.255.0 port 5683 max-endpoints 10
```

次の例に、セキュリティ設定がされて**いない** *ipv4 1.1.0.0 255.255.0.0* に COAP プロキシを設定する方法を示します。

```
Device(config-coap-proxy)# security ?
  dtls  dtls
  none  no security

Device(config-coap-proxy)#security none ?
  ipv4    IP address range on which to learn lights
  ipv6    IPv6 address range on which to learn lights
  list    IP address range on which to learn lights

Device(config-coap-proxy)#security none ipv4 ?
  A.B.C.D  {/nn || A.B.C.D}  IP address range on which to learn lights

Device(config-coap-proxy)#security none ipv4 1.1.0.0 255.255.0.0
```

次の例に、**dtls id trustpoint** セキュリティ設定がされている *ipv4 1.1.0.0 255.255.0.0* に COAP プロキシを設定する方法を示します。

```
Device(config-coap-proxy)#security dtls ?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
   ipv4 IP address range on which to learn lights
   ipv6 IPv6 address range on which to learn lights
   list IP address range on which to learn lights

Device(config-coap-proxy)#security dtls id-trustpoint ?
  WORD  Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT ?
  verification-trustpoint  Certificate Verification Label
   <cr>
```

```
Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT

Device(config-coap-proxy)#security dtls ?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4 IP address range on which to learn lights
  ipv6 IPv6 address range on which to learn lights
  list IP address range on which to learn lights

Device(config-coap-proxy)# security dtls ipv4 1.1.0.0 255.255.0.0
```

（注） **ipv4 / ipv6 / list** を設定する場合は、**id-trustpoint** および（任意で）**verification-trustpoint** を事前設定する必要があります。そうしないと、システムにエラーが表示されます。

次の例に、トラストポイントを設定する方法を示します。これは、**id trustpoint** による COAP **security dtls** 設定の前提条件です。

```
ip domain-name myDomain
crypto key generate rsa general-keys exportable label MyLabel modulus 2048

Device(config)#crypto pki trustpoint MY_TRUSTPOINT
Device(ca-trustpoint)#rsakeypair MyLabel 2048
Device(ca-trustpoint)#enrollment selfsigned
Device(ca-trustpoint)#exit

Device(config)#crypto pki enroll MY_TRUSTPOINT
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
```

次の例に、**dtls verification trustpoint** によって *ipv4 1.1.0.0 255.255.0.0* に COAP プロキシを設定する方法を示します（証明書または検証トラストポイントによる DTLS）。

```
Device(config-coap-proxy)#security dtls ?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4 IP address range on which to learn lights
  ipv6 IPv6 address range on which to learn lights
  list IP address range on which to learn lights

Device(config-coap-proxy)#security dtls id-trustpoint ?
  WORD  Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT ?
  verification-trustpoint  Certificate Verification Label
  <cr>

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT
verification-trustpoint ?
  WORD  Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT
```

```
verification-trustpoint CA-TRUSTPOINT ?
  <cr>
```

次の例に、検証トラストポイントを設定する方法を示します。これは、**verification trustpoint** による COAP **security dtls** 設定の前提条件です。

```
Device(config)#crypto pki import CA-TRUSTPOINT pkcs12 flash:hostA.p12 password cisco123
% Importing pkcs12...
Source filename [hostA.p12]?
Reading file from flash:hostA.p12
CRYPTO_PKI: Imported PKCS12 file successfully.
```

次の例に、セキュリティ [none | dtls] コマンド オプションで使用する、trial-list という名前のリストを作成する方法を示します。

```
Device(config-coap-proxy)#list ipv4 trial_list
Device (config-coap-proxy-iplist)#1.1.0.0 255.255.255.0
Device (config-coap-proxy-iplist)#2.2.0.0 255.255.255.0
Device (config-coap-proxy-iplist)#3.3.0.0 255.255.255.0
Device (config-coap-proxy-iplist)#exit
Device (config-coap-proxy)#security none list trial_list
```

次の例に、coap プロキシ サブ モードで使用できるすべての拒否コマンドを示します。

```
Device(config-coap-proxy)#no ?
  ip-list             Configure IP-List
  max-endpoints       maximum number of endpoints supported
  port-unsecure       Specify a port number to use
  port-dtls           Specify a dtls-port number to use
  resource-discovery  Resource Discovery Server
  security            CoAP Security features
```

次の例に、coap プロキシで複数の IPv4/IPv6 スタティック エンドポイントを設定する方法を示します。

```
Device (config)# coap endpoint ipv4 1.1.1.1
Device (config)# coap endpoint ipv4 2.1.1.1
Device (config)# coap endpoint ipv6 2001::1
```

次の例に、COAP プロトコルの詳細を表示する方法を示します。

```
Device#show coap version
CoAP version 1.0.0
RFC 7252
```

```
Device#show coap resources
Link format data =
</>
</1.1.1.6/cisco/context>
```

```
</1.1.1.6/cisco/actuator>
</1.1.1.6/cisco/sensor>
</1.1.1.6/cisco/lldp>
</1.1.1.5/cisco/context>
</1.1.1.5/cisco/actuator>
</1.1.1.5/cisco/sensor>
</1.1.1.5/cisco/lldp>
</cisco/flood>
</cisco/context>
</cisco/showtech>
</cisco/lldp>

-----------------------------------------------------------------------------------------

Device#show coap globals
Coap System Timer Values :
   Discovery  : 120 sec
   Cache Exp  : 5 sec
   Keep Alive : 120 sec
   Client DB  : 60 sec
   Query Queue: 500 ms
   Ack delay  : 500 ms
   Timeout    : 5 sec

Max Endpoints      : 10
Resource Disc Mode : POST

-----------------------------------------------------------------------------------------

Device#show coap stats
Coap Stats :
Endpoints : 2
Requests : 20
Ext Queries : 0

-----------------------------------------------------------------------------------------

Device#show coap endpoints
List of all endpoints :

Code : D - Discovered , N - New
#    Status   Age(s)  LastWKC(s)  IP
-------------------------------------------------------------------------------
1    D        10      94          1.1.1.6
2    D        6       34          1.1.1.5

Endpoints - Total : 2 Discovered : 2 New : 0

-----------------------------------------------------------------------------------------

Device#show coap dtls-endpoints
#     Index State  String State     Value   Port IP
-------------------------------------------------------------
1     3     SSLOK       3           48969   20.1.1.30
2     2     SSLOK       3           53430   20.1.1.31
3     4     SSLOK       3           54133   20.1.1.32
4     7     SSLOK       3           48236   20.1.1.33


-----------------------------------------------------------------------------------------
```

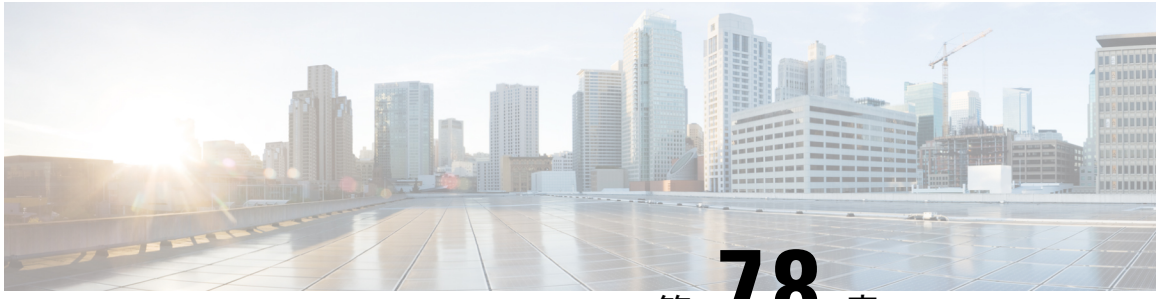
次の例に、COAP プロトコルのデバッグに使用できるすべてのオプションを示します。

```
Device#debug coap ?
all       Debug CoAP all
database  Debug CoAP Database
errors    Debug CoAP errors
```

```
events    Debug CoAP events
packet    Debug CoAP packet
trace     Debug CoAP Trace
warnings  Debug CoAP warnings
```

関連トピック

COAP プロキシの設定 （1464 ページ）
COAP プロキシ サーバについて （1459 ページ）



第 78 章

Autosmart ポートの設定

- 機能情報の確認 （1475 ページ）
- Autosmart ポートに関する情報 （1475 ページ）
- Autosmart ポート マクロ （1476 ページ）
- CISCO_LIGHT_AUTO_SMARTPORT によって実行されるコマンド （1476 ページ）
- Autosmart ポートのイネーブル化 （1477 ページ）
- 例：AutoSmart ポートのイネーブル化 （1478 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Autosmart ポートに関する情報

Auto SmartPort マクロは、ポートで検出されたデバイス タイプに基づいてポートを動的に設定します。スイッチがポートで新しいデバイスを検出すると、適切な Auto SmartPorts マクロを適用します。ポート上でリンク ダウン イベントが発生した場合、スイッチはそのマクロを削除します。たとえば、ポートに Cisco IP Phone を接続した場合は、Auto SmartPorts により自動的に Cisco IP Phone マクロが適用されます。Cisco IP Phone マクロが適用されると、遅延に影響されやすい音声トラフィックを正しく処理できるように QoS（Quality Of Service）、セキュリティ機能、および専用の音声 VLAN がイネーブルになります。

Auto SmartPorts は、イベント トリガーを使用して、マクロにデバイスをマッピングします。最も一般的なイベント トリガーは、接続されているデバイスから受信した Cisco Discovery Protocol

（CDP）メッセージに基づいています。デバイス（Cisco IP Phone、Cisco ワイヤレス アクセス ポイント、Cisco スイッチ、またはCisco ルータ）の検出は、そのデバイスのイベント トリガーを呼び出します。

Link Layer Discovery Protocol（LLDP）は、CDP をサポートしないデバイスを検出するために使用されます。イベント トリガーとして使用される他のメカニズムには、802.1X 認証結果と学習した MAC アドレスなどがあります。

主に CDP および LLDP メッセージと MAC アドレスに基づいて、さまざまなデバイス用にシステムの組み込みイベント トリガーがあります。これらのトリガーは、Auto SmartPort が有効になっている限り有効になっています。

プロファイルとデバイス用のユーザ定義のトリガー グループを設定できます。トリガー グループ名を使用してユーザ定義マクロを関連付けます。

Autosmart ポート マクロ

Auto SmartPort マクロは CLI コマンドのグループです。ポートのデバイスが検出されると、デバイスにマクロが適用されます。システムの組み込みマクロはさまざまなデバイスに存在し、デフォルトでは、システムの組み込みのトリガーは、対応する組み込みマクロにマッピングされます。必要に応じて、組み込みのトリガーまたはマクロのマッピングを変更できます。

マクロは、基本的に、リンク ステータスに基づいて、インターフェイスの CLI のセットを適用または削除します。マクロでは、リンク ステータスがチェックされます。リンクがアップ ステータスの場合は、CLI のセットが適用されます。リンクがダウンしている場合、セットが削除されます（CLI の no 形式が適用されます）。CLI のセットを適用するマクロの部分は、マクロと呼びます。CLI を削除する部分（CLI の no 形式）は、アンチマクロと呼びます。

デバイスが Autosmart ポートに接続されている場合に、点灯しているエンド ポイントとして分類されると、イベント トリガー **CISCO_LIGHT_EVENT** が呼び出され、マクロ **CISCO_LIGHT_AUTO_SMARTPORT** が実行されます。

関連トピック

Autosmart ポートのイネーブル化 （1477 ページ）
例：AutoSmart ポートのイネーブル化 （1478 ページ）

CISCO_LIGHT_AUTO_SMARTPORTによって実行されるコマンド

マクロが実行されると、スイッチで一連のコマンドが実行されます。

マクロ **CISCO_LIGHT_AUTO_SMARTPORT** を実行することで実行されるコマンドは、次のとおりです。

- switchport mode access
- switchport port-security violation restrict

- switchport port-security mac-address sticky
- switchport port-security
- power inline port poe-ha
- storm-control broadcast level 50.00
- storm-control multicast level 50.00
- storm-control unicast level 50.00
- spanning-tree portfast
- spanning-tree bpduguard enable

Autosmart ポートのイネーブル化

（注） デフォルトでは、Auto SmartPort はグローバルにディセーブルです。特定のポートの Auto SmartPorts マクロをディセーブルにするには、Auto SmartPort をグローバルにイネーブルにする前に、**no macro auto global processing** インターフェイス コマンドを使用します。

Auto SmartPort をグローバルにイネーブルにするには、**macro auto global processing** グローバル コンフィギュレーション コマンドを使用します。

Auto SmartPorts をイネーブルにするには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**device classifier** 例： `Device(config)# device classifier`	デバイスの分類子を有効にします。 デバイスの分類子を無効にするには、**no device classifier** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	**macro auto global processing** 例： `Device(config)# macro auto global processing`	スイッチの Auto SmartPorts をグローバルにイネーブルにします。 Auto SmartPort をグローバルにディセーブルにするには、**no macro auto global processing** コマンドを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

Autosmart ポート マクロ （1476 ページ）
例：AutoSmart ポートのイネーブル化 （1478 ページ）

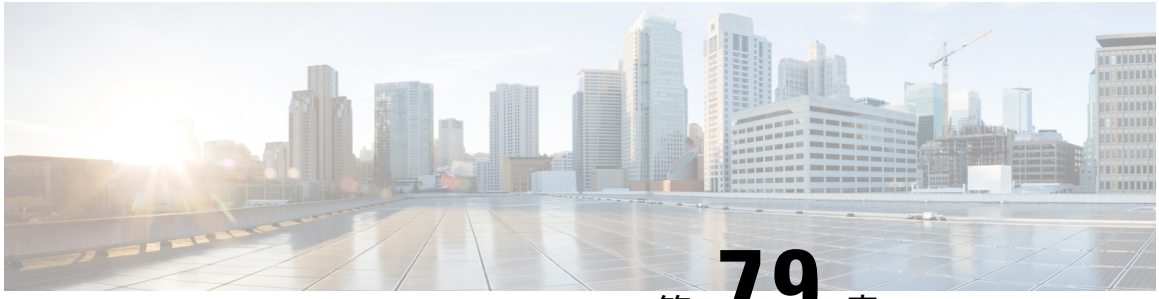
例：AutoSmart ポートのイネーブル化

次に、AutoSmart ポートを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# device classifier
Device(config)# macro auto global processing
Device(config)# end
```

関連トピック

Autosmart ポートのイネーブル化 （1477 ページ）
Autosmart ポート マクロ （1476 ページ）



第 79 章

2 イベント分類の設定

- 機能情報の確認 （1479 ページ）
- 2 イベント分類について （1479 ページ）
- 2 イベント分類の設定 （1480 ページ）
- 例：2 イベント分類の設定 （1480 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

2 イベント分類について

クラス 4 デバイスが検出されると、IOS は、CDP または LLDP のネゴシエーションを行うことなく 30W を割り当てます。これは、リンクがアップする前であっても、クラス 4 の電源デバイスは 30W を得ることを意味します。

また、ハードウェア レベルで、PSE は 2 イベント分類を行い、これにより、クラス 4 PD はハードウェアから 30W を供給する PSE の能力を検出し、それ自体を登録することができます。また、CDP/LLDP パケット交換を待つことなく最大 PoE+ レベルまで移動できます。

2 イベントがポートで有効になったら、ポートの遮断または開放を手動で行うか、または PD を再度接続して IEEE 検出を再度開始する必要があります。2 イベント分類がポートで有効になっている場合、クラス 4 デバイスの電力バジェット割り当ては 30W です。その他の場合は 15.4W です。

2 イベント分類の設定

2 イベント分類についてスイッチを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**power inline port 2-event** 例： `Device(config-if)# power inline port 2-event`	スイッチで 2 イベント分類を設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

例：2 イベント分類の設定 （1480 ページ）

例：2 イベント分類の設定

次に、2 イベント分類を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)#  interface gigabitethernet2/0/1
Device(config-if)# power inline port 2-event
Device(config-if)# end
```

関連トピック

2 イベント分類の設定 （1480 ページ）

第 80 章

無停止型 POE の設定

- 機能情報の確認 （1483 ページ）
- 無停止型 POE （1483 ページ）
- 高速 POE （1484 ページ）
- 無停止型 POE および高速 POE 向けにサポートされるハードウェア （1484 ページ）
- POE の設定 （1487 ページ）
- 例：無停止型 POE の設定 （1488 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

無停止型 POE

無停止型 POE は、PSE スイッチが起動している場合でも、接続された PD デバイスへの連続電源を提供します。

（注） ポートへの電源供給は MCU ファームウェアのアップグレード時には中断され、ポートはアップグレード直後にバックアップされます。

高速 POE

この機能は、IOS が起動するのを待機することなく、AC 電源が接続された瞬間（電源投入の 15 ～ 20 秒以内）に特定の PSE ポートから引き出された最後の電力を記憶し、電源をオンにします。**poe-ha** が特定のポートで有効な場合、電源障害後のリカバリのスイッチによって、IOS の転送さえも開始される前に、短期間内に接続されたエンドポイントデバイスに電力が提供されます。

この機能は、すでに実装済みの **poe-ha** と同じコマンドで設定できます。スイッチの電源がオフになったときにポートに接続されている電源デバイスをユーザが交換した場合、この新しいデバイスは、以前のデバイスが利用していた電力を取得します。

（注） 高速 POE は、Catalyst 3850 でのみサポートされています。

（注） UPOE の場合、高速 POE はスイッチ側で使用可能ですが、UPOE 電力の可用性の信号伝達を LLDP に依存するため、PD エンドポイントは同様の機能を利用できない可能性があります。LLDP に依存する場合、IOS が起動して LLDP パケット交換が可能になり、UPOE 電力の可用性を信号で伝達できるようになるまで、PD エンドポイントはそのまま待機する必要があります。

無停止型 POE および高速 POE 向けにサポートされるハードウェア

無停止型 POE は、次の Catalyst 3850 スイッチ モデルでサポートされます。

スイッチ モデル	Cisco IOS イメージ	説明
WS-C3850-24T-S	IP Base	Cisco Catalyst 3850 スタッカブル 24 X 10/100/1000 イーサネット ポート、350 WAC 電源 1 RU、IP Base フィーチャ セット搭載
WS-C3850-48T-S	IP Base	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット ポート、350 WAC 電源 1 RU、IP Base フィーチャ セット搭載
WS-C3850-24P-S	IP Base	Cisco Catalyst 3850 スタッカブル 24 X 10/100/1000 イーサネット PoE+ ポート、715 WAC 電源 1 RU、IP Base フィーチャ セット搭載

スイッチ モデル	Cisco IOS イメージ	説明
WS-C3850-48P-S	IP Base	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット PoE+ ポート、715 WAC 電源 1 RU、IP Base フィーチャ セット搭載
WS-C3850-48F-S	IP Base	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット PoE+ ポート、1100 WAC 電源 1 RU、IP Base フィーチャ セット搭載
WS-C3850-24U-S	IP Base	24 X 10/100/1000 Cisco UPOE ポート（スタック可能）、1 X ネットワーク モジュール スロット、1100 W 電源
WS-C3850-48U-S	IP Base	48 X 10/100/1000 Cisco UPOE ポート（スタック可能）、1 X ネットワーク モジュール スロット、1100 W 電源
WS-C3850-12S-S	IP Base	12 × SFP モジュール スロット（スタック可能）、1 × ネットワーク モジュール スロット、350 W 電源
WS-C3850-24S-S	IP Base	24 × SFP モジュール スロット（スタック可能）、1 × ネットワーク モジュール スロット、350 W 電源
WS-C3850-12XS-S	IP Base	Catalyst 3850 12 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、350 W 電源
WS-C3850-16XS-S	IP Base	Catalyst 3850 16 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、350 W 電源 C3850-NM-4-10G ネットワーク モジュールが WS-C3850-12XS-S スイッチに接続されている場合は、16 ポートを使用できます。
WS-C3850-24XS-S	IP Base	Catalyst 3850 24 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、715 W 電源
WS-C3850-32XS-S	IP Base	Catalyst 3850 32 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、715 W 電源 C3850-NM-8-10G ネットワーク モジュールが WS-C3850-24XS-S スイッチに接続されている場合は、32 ポートを使用できます。
WS-C3850-48XS-S	IP Base	スタック可能、SFP+ トランシーバ、48 X ポート（最大 10 G をサポート）、4 X ポート（最大 40 G をサポート）、750 W 電源を搭載

スイッチ モデル	Cisco IOS イメージ	説明
WS-C3850-48XS-F-S	IP Base	スタック可能、SFP+ トランシーバ、48 X ポート（最大 10 G をサポート）、4 X ポート（最大 40 G をサポート）、750 W 電源を搭載
WS-C3850-24XU-S	IP Base	24 X 100M/1G/2.5G/5G/10G UPOE ポート（スタック可能）、1 X ネットワーク モジュール スロット、1100 W 電源
WS-C3850-24T-E	IP サービス	Cisco Catalyst 3850 スタッカブル 24 X 10/100/1000 イーサネット ポート、350 WAC 電源 1 RU、IP Services フィーチャ セット搭載
WS-C3850-48T-E	IP サービス	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット ポート、350 WAC 電源 1 RU、IP Services フィーチャ セット搭載
WS-C3850-24P-E	IP サービス	Cisco Catalyst 3850 スタッカブル 24 X 10/100/1000 イーサネット PoE+ ポート、715 WAC 電源 1 RU、IP Services フィーチャ セット搭載
WS-C3850-48P-E	IP サービス	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット PoE+ ポート、715 WAC 電源 1 RU、IP Services フィーチャ セット搭載
WS-C3850-48F-E	IP サービス	Cisco Catalyst 3850 スタッカブル 48 X 10/100/1000 イーサネット PoE+ ポート、1100 WAC 電源 1 RU、IP Services フィーチャ セット搭載
WS-3850-24U-E	IP サービス	Cisco Catalyst 3850 スタッカブル 24 × 10/100/1000 Cisco UPOE ポート、1 × ネットワーク モジュール スロット、1100 W 電源
WS-3850-48U-E	IP サービス	Cisco Catalyst 3850 スタッカブル 48 × 10/100/1000 Cisco UPOE ポート、1 × ネットワーク モジュール スロット、1100 W 電源
WS-C3850-12S-E	IP サービス	2 × SFP モジュール スロット（スタック可能）、1 × ネットワーク モジュール スロット、350 W 電源
WS-C3850-24S-E	IP サービス	24 × SFP モジュール スロット（スタック可能）、1 × ネットワーク モジュール スロット、350 W 電源
WS-C3850-12XS-E	IP サービス	Catalyst 3850 12 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、350 W 電源

スイッチ モデル	Cisco IOS イメージ	説明
WS-C3850-16XS-E	IP サービス	Catalyst 3850 16 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、350 W 電源 C3850-NM-4-10G ネットワーク モジュールが WS-C3850-12XS-E スイッチに接続されている場合は、16ポートを使用できます。
WS-C3850-24XS-E	IP サービス	Catalyst 3850 24 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、715 W 電源
WS-C3850-32XS-E	IP サービス	Catalyst 3850 32 ポート SFP+ トランシーバ、1 X ネットワーク モジュール スロット、最大 10 G SFP+ をサポート、715 W 電源 C3850-NM-8-10G ネットワーク モジュールが WS-C3850-24XS-E スイッチに接続されている場合は、32ポートを使用できます。
WS-C3850-48XS-E	IP サービス	スタック可能、SFP+ トランシーバ、48 X ポート（最大 10 G をサポート）、4 X ポート（最大 40 G をサポート）、750 W 電源を搭載
WS-C3850-48XS-F-E	IP サービス	スタック可能、SFP+ トランシーバ、48 X ポート（最大 10 G をサポート）、4 X ポート（最大 40 G をサポート）、750 W 電源を搭載
WS-C3850-24XU-E	IP サービス	24 X 100M/1G/2.5G/5G/10G UPOE ポート（スタック可能）、1 X ネットワーク モジュール スロット、1100 W 電源

POE の設定

POE を設定するには、次の手順を実行します。

（注） PD を接続する前に **poe-ha** コマンドを設定する、または、**poe-ha** を設定した後にポートを手動で閉じる/開く必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**power inline port poe-ha** 例： `Device(config-if)# power inline port poe-ha`	PoE の高可用性を設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

例：無停止型 POE の設定 （1488 ページ）

例：無停止型 POE の設定

次の例では、スイッチ上で無停止型 POE を設定にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# power inline port poe-ha
Device(config-if)# end
```

関連トピック

POE の設定 （1487 ページ）

第 81 章

FAQ

- 機能情報の確認 （1489 ページ）
- FAQ （1489 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

FAQ

ここでは、Network Powered Lighting に関してよく寄せられる質問（FAQ）をまとめています。

- **質問:**

  「show coap stats」出力の「New Endpoint」は何を意味していますか。「New Endpoint」はいつ「Endpoint」に移行しますか。

  回答：

  新しいエンドポイントとは、エンドポイントが発見された（ディスカバリ パケットが受信された）が、CoAP プロキシによってまだ登録されていないことを意味します。CoAP プロキシは、定期的に新しいエンドポイントを調べ、「./well-known/core」上で GET を送信して詳細を取得します。そして RSP は受信された時点で、「Endpoint」に移動されます。

- **質問:**

  セキュリティ設定がないと「CoAP の開始」を実行できないのはなぜですか。

回答：

CoAP に関連するすべての設定が完了し、その後にそれが明示的に有効になるようにする必要があります。これによって、設定全体にわたる断続的に不安定な状態を回避できます。

- **質問:**

「coap プロキシ」コンフィギュレーション モード「coap プロキシ <cr>」にドロップを強制する必要があるのはなぜですか。設定の完了後、スイッチプロンプトに戻るのに2度終了しなければなりません。これは非常に使いにくいと思います。

回答：

別の方法として、私たちが行っている各設定のプレフィックスとして「coap proxy」と入力する必要があります。coapプロキシに関するサブモード下のすべての設定を実行できるので、これはサブモードに入るのに最適なオプションです。

- **質問:**

最初に coap プロセスを停止しないと、セキュリティやその他のパラメータを設定解除できないのはなぜですか。

回答：

CoAP に関連するすべての設定が完了し、その後にそれが明示的に有効になるようにする必要があります。これによって、CoAP が有効な場合に、ユーザがオンザフライで設定を行う可能性がある複雑性を回避して制御することもできます。

- **質問:**

coap を停止したとき、CoAP プロセスに関連付けられたすべての設定が自動的に削除されません（またはデフォルトに戻ります）。CoAP はなぜ以前の設定を記憶しているのですか。これでは、ユーザはやり直すのが非常に難しいように思います。

回答：

システムは意図的にこのように設計されていて、これは予期された動作です。時々、最大エンドポイントの変更やプロキシの再起動など、軽微な変更だけを行いたい場合があります。これは、他のすべての設定はそのまま保持できるオプションです。これがないと、ユーザはすべてを一から設定し直す必要があります。

- **質問:**

セキュリティ設定がどのように設定されているかはどのように確認できますか。

回答：

コマンド「show run」を使用してすべての設定を表示できます。

- **質問:**

タイマー値はどのように調整できますか。

```
Example:
wtsao-3850#sho coap glo
```

```
Coap System Timer Values:
Discovery : 120 sec
Cache Exp : 5 sec
Keep Alive : 120 sec
Client DB : 5 sec
Query Queue : 500 ms
Ack delay : 500 ms
Timeout : 5 sec
Max Endpoints : 500
Resource Disc Mode : POST
```

回答：

タイマー値は固定で、現在のところ調整不可です。その理由は、システム間での不一致を避けるためです。

- **質問:**

  コマンド「list」および「endpoint」は何に使用するものですか。

  回答：

  「list」コマンドは、複数の IP アドレスを設定し、それに名前を付ける作業をより簡単にするためのものです。その結果、複数の ip を表すために、単一の ip の代わりに名前を割り当てることができます。「endpoint」コマンドは、エンドポイントが自身をアドバタイズしない場合に、スタティック エンド ポイントを設定するために使用されます。

- **質問:**

  「show」コマンドを使用してエンドポイントからポートへのマッピングを見つけるにはどうすればよいですか。

  回答：

  それについては現時点でサポートされていません。しかし、他のコマンドを実行してそのデータを取得することができます。現在でも、「lldp neighbours」、「ip dhcp」、「power inlines」などの個々のコマンドを使用して、言及したすべての詳細を取得できます。

第 XIV 部

QoS

- QoS の設定 （1495 ページ）

第 82 章

QoS の設定

- 機能情報の確認 （1496 ページ）
- 自動 QoS の前提条件 （1496 ページ）
- 自動 QoS の制約事項 （1496 ページ）
- 自動 QoS の設定に関する情報 （1497 ページ）
- 自動 QoS の設定方法 （1500 ページ）
- 自動 QoS の監視 （1507 ページ）
- 自動 QoS に関するトラブルシューティング （1507 ページ）
- 自動 QoS の設定例 （1508 ページ）
- 自動 QoS の関連情報 （1537 ページ）
- 自動 QoS に関する追加情報 （1538 ページ）
- 自動 QoS の機能履歴と情報 （1539 ページ）
- 機能情報の確認 （1539 ページ）
- QoS の前提条件 （1539 ページ）
- QoS コンポーネント （1540 ページ）
- QoS の用語 （1541 ページ）
- QoS の概要 （1541 ページ）
- QoS ポリシーのガイドライン （1583 ページ）
- 有線ターゲットの QoS に関する制約事項 （1583 ページ）
- ワイヤレス ターゲットの QoS に関する制約事項 （1587 ページ）
- QoS の設定方法 （1590 ページ）
- QoS のモニタリング （1646 ページ）
- QoS の設定例 （1650 ページ）
- 次の作業 （1667 ページ）
- QoS に関する追加情報 （1667 ページ）
- QoS の機能履歴と情報 （1669 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

自動 QoS の前提条件

自動 QoS の前提条件は標準 QoS の前提条件と同じです。

自動 QoS の制約事項

次に、自動 QoS の制約事項を示します。

- 自動 QoS は、SVI インターフェイスではサポートされません。
- 自動 QoS は、Etherchannel インターフェイスではサポートされません。メンバー ポートに適用すると、すべてのポートチャネル インターフェイスが同じ自動 QoS ポリシーを共有する必要があります。
- インターフェイス コンフィギュレーション モードで使用可能な **trust device** *device_type* コマンドは、スイッチでのスタンドアロン コマンドです。このコマンドを使用するときに、接続されているピア デバイスが対応デバイス（信頼ポリシーに一致するデバイスとして定義されているデバイス）ではない場合、CoS 値と DSCP 値の両方が「0」に設定され、いずれの入力ポリシーも有効になりません。接続されているピア デバイスが対応するデバイスである場合は、入力ポリシーが有効になります。
- 3.2.2 より古いソフトウェア バージョンのソフトウェア リリースを 3.2.2 またはこれ以降のソフトウェア バージョンにアップグレードする場合は、この章で説明する自動 QoS のアップグレード手順に従ってください。
- ビデオをサポートしている IP フォンには、 **auto qos voip cisco-phone** オプションを設定しないでください。ビデオ パケットには Expedited Forwarding（EF; 完全優先転送）プライオリティが設定されていないため、このオプションを使用すると、ビデオ パケットの DSCP マーキングが上書きされ、これらのパケットが class-default クラスに分類されます。
- 自動 QoS が **auto qos voip cisco-phone** コマンドを使用するスタートアップ コンフィギュレーションから実行コンフィギュレーションにプッシュされた場合、自動 QoS によって設定は生成されません。これは予期された動作であり、これにより、 **auto qos voip**

cisco-phone コマンドがスタートアップ コンフィギュレーションからプッシュされるたびに、ユーザが作成したカスタマイズ済みの QoS ポリシーがデフォルト設定（ある場合）で上書きされないようにします。

この制限に対し、次のいずれかの回避策を使用できます。

- スイッチのインターフェイスで **auto qos voip cisco-phone** コマンドを手動で設定します。
- 新しいスイッチでは、スタートアップ コンフィギュレーションから自動 QoS コマンドをプッシュする場合は、コマンドに標準テンプレートの一部として次の項目をそれぞれ含める必要があります。
  1. インターフェイス レベル：
     - **trust device cisco-phone**
     - **auto qos voip cisco-phone**
     - **service-policy input** AutoQos-4.0-CiscoPhone-Input-Policy
     - **service-policy output** AutoQos-4.0-Output-Policy
  2. グローバル レベル：
     - クラスマップ
     - ポリシーマップ
     - ACL（ACE）
- **auto qos voip cisco-phone** コマンドがインターフェイスですでに設定されているが、ポリシーが生成されていない場合は、すべてのインターフェイスからコマンドを無効にして、各インターフェイスでコマンドを手動で再設定します。

関連トピック

自動 QoS のアップグレード（CLI）（1503 ページ）

自動 QoS の設定に関する情報

自動 QoS の概要

自動 QoS 機能を使用して、QoS 機能の配置を容易にできます。自動 QoS は、ネットワーク設計を確認し、スイッチがさまざまなトラフィック フローに優先度を指定できるように QoS 設定をイネーブルにします。

スイッチは MQC モデルを採用しています。これは、特定のグローバル コンフィギュレーションを使用する代わりに、スイッチ上のインターフェイスに適用された自動 QoS が複数のグローバル クラス マップとポリシー マップを設定することを意味します。

自動 QoS はトラフィックを照合し、各一致パケットを qos-group に割り当てます。これにより、出力ポリシー マップは、プライオリティ キューを含む特定のキューに、特定の qos-group を配置できます。

QoS は、着信と発信の両方向で必要です。着信時に、スイッチ ポートは、パケットの DSCP を信頼する必要があります（デフォルトで実行されます）。発信時に、スイッチ ポートは、音声パケットに「front of line」プライオリティを付与する必要があります。音声が発信キューの他のパケットの後ろで待機して、遅延が長くなりすぎる場合、パケットの受信時間の範囲外となるため、エンド ホストは、そのパケットをドロップします。

自動 QoS 短縮機能の概要

自動QoSコマンドを入力すると、CLIからコマンドを入力する場合と同様に、生成されたすべてのコマンドがスイッチにより表示されます。自動 QoS 短縮機能を使用して、実行コンフィギュレーションから自動 QoS が生成したコマンドを非表示にできます。これにより、実行コンフィギュレーションを容易に把握でき、またメモリをより効率的に使用できるようになります。

自動 QoS グローバル設定テンプレート

一般に、自動 QoS コマンドは、ACL または DSCP で一致する、またはアプリケーション クラスに送信されるトラフィックを識別するCoS値で一致する一連のクラスマップを生成します。また、生成されたクラスに一致する入力ポリシーや、設定されている帯域幅にクラスをポリシングする入力ポリシーも生成されます。8つの出力キュークラスマップが生成されます。実際の出力の出力ポリシーは、この 8 つの出力キュー クラス マップのそれぞれにキューを割り当てます。

自動 QoS コマンドは、必要なテンプレートだけを生成します。たとえば、新しい自動 QoS コマンドを初めて使用するときに、8つのキュー出力サービスポリシーを定義するグローバル設定が生成されます。この時点から、他のインターフェイスに適用された自動QoSコマンドは、出力キューのテンプレートを生成しません。これは、新しい自動 QoS コマンドが最初に使用されてから生成された同じ 8 つのキュー モデルに、すべての自動 QoS コマンドが依存しているためです。

自動 QoS ポリシーとクラス マップ

適切な自動 QoS コマンドを入力すると、次のアクションが実行されます。

- 特定のクラス マップが作成されます。
- 特定のポリシー マップ（入力および出力）が作成されます。
- 指定したインターフェイスにポリシー マップが適用されます。
- インターフェイスの信頼レベルが設定されます。

関連トピック

自動 QoS の設定（CLI）（1500 ページ）
例：auto qos trust cos
例：auto qos trust dscp
例：auto qos video cts
例：auto qos video ip-camera
例：auto qos video media-player
例：auto qos voip trust
例：auto qos voip cisco-phone
例：auto qos voip cisco-softphone
auto qos classify police

実行コンフィギュレーションでの自動 QoS の影響

自動 QoS がイネーブルになると、**auto qos** インターフェイス コンフィギュレーション コマンドおよび生成されたグローバル コンフィギュレーションが実行コンフィギュレーションに追加されます。

スイッチは、自動 QoS が生成したコマンドを、CLI から入力したように適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションが警告なしで発生する可能性があります。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成コマンドが適用されなかった場合、以前の実行コンフィギュレーションが復元されます。

実行コンフィギュレーションでの自動 QoS 短縮機能の影響

自動 QoS 短縮機能をイネーブルにした場合：

- CLI から入力された自動 QoS コマンドだけが実行コンフィギュレーションに表示されます。
- 生成されるグローバル コンフィギュレーションおよびインターフェイス コンフィギュレーションは表示されません。
- コンフィギュレーションを保存するときに、入力した自動 QoS コマンドだけが保存されます（非表示のコンフィギュレーションは保存されません）。
- スイッチをリロードすると、保存された自動 QoS コマンドがシステムにより検出、再実行され、AutoQoS SRND4.0 に準拠したコンフィギュレーション セットが生成されます。

（注） 自動 QoS 短縮機能がイネーブルである場合は、自動 QoS 生成コマンドを変更しないでください。これは、スイッチのリロード時にユーザ変更がオーバーライドされるためです。

自動 QoS グローバル短縮機能をイネーブルにした場合：

- **show derived-config** 非表示の AQC 派生コマンドを表示するには、コマンドを使用します。
- AQC コマンドはメモリに保存されません。これらは、スイッチがリロードされるたびに再生成されます。
- 短縮機能がイネーブルである場合、自動 QoS により生成されたコマンドは変更しないでください。
- 自動 QoS でインターフェイスが設定されており、AQC をディセーブルにする必要がある場合は、最初に自動 QoS をインターフェイス レベルでディセーブルにする必要があります。

自動 QoS の設定方法

自動 QoS の設定（CLI）

QoS パフォーマンスを最適化するには、ネットワーク内のすべてのデバイスで自動 QoS を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 3/0/1`	VoIP ポートやビデオ デバイスに接続されているポート、またはネットワーク内部の他の信頼できるスイッチまたはルータに接続されているアップリンク ポートを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	自動 QoS 設定によって、次のコマンドの 1 つを使用します。 • **auto qos voip** {**cisco-phone** | **cisco-softphone** | **trust**} • **auto qos video** {**cts** | **ip-camera** | **media-player**} • **auto qos classify** [**police**]	次のコマンドによって、VoIP 用の自動 QoS が有効になります。 • **auto qos voip cisco-phone**：ポートが Cisco IP Phone に接続されている場合、着信パケットの QoS ラベルは電話機が検出された場合だけ信頼されます（CDP を介して条件付き信頼）。

	コマンドまたはアクション	目的
	• **auto qos trust** {**cos** | **dscp**} 例： `Device(config-if)# auto qos trust dscp`	（注） ビデオをサポートしている IP フォンには、 **auto qos voip cisco-phone** オプションを設定しないでください。ビデオ パケットには Expedited Forwarding（EF;完全優先転送）プライオリティが設定されていないため、このオプションを使用すると、ビデオ パケットの DSCP マーキングが上書きされ、これらのパケットが class-default クラスに分類されます。 • **auto qos voip cisco-softphone**：ポートが Cisco SoftPhone 機能を実行するデバイスに接続されています。このコマンドによって Cisco IP SoftPhone アプリケーションおよびマーキングを実行する PC に接続しているインターフェイスの QoS 設定が生成され、そのようなインターフェイスからのトラフィックをマーキングおよびポリシングします。このコマンドで設定されたポートは、信頼できないと見なされます。 • **auto qos voip trust**：アップリンクポートが信頼性のあるスイッチまたはルータに接続されていて、入力パケットの VoIP トラフィック分類が信頼されています。 次のコマンドは、指定されたビデオ デバイス（システム、カメラ、メディアプレーヤー）用の自動 QoS を有効にします。 • **auto qos video cts**：Cisco Telepresence System に接続されているポート。着信パケットの QoS ラベルは Cisco TelePresence が検出された場合だけ

	コマンドまたはアクション	目的
		信頼されます（CDP を介した条件付き信頼） • **auto qos video ip-camera**：Cisco ビデオ監視カメラに接続されているポート。着信パケットの QoS ラベルはCiscoカメラが検出された場合だけ信頼されます（CDP を介した条件付き信頼） • **auto qos video media-player**：CDP 対応 Cisco Digital Media Player に接続されているポート。着信パケットの QoS ラベルはデジタル メディア プレイヤーが検出された場合だけ信頼されます（CDP を介した条件付き信頼）。 次のコマンドは、分類の自動 QoS を有効にします。 • **auto qos classify police**：このコマンドは、信頼できないインターフェイスの QoS 設定を生成します。この設定では、信頼できないデスクトップ/デバイスから着信するトラフィックを分類してマークするため、サービス ポリシーがインターフェイスに適用されます。生成されたサービス ポリシーは、ポリシングを実行します。 次のコマンドによって、信頼できるインターフェイス用の自動 QoS が有効になります。 • **auto qos trust cos**：サービス クラス • **auto qos trust dscp**：DiffServ コードポイント
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show auto qos interface** *interface-id* 例： `Device# show auto qos interface gigabitethernet 3/0/1`	（任意）自動 QoS がイネーブルであるインターフェイス上の自動 QoS コマンドを表示します。自動 QoS 設定およびユーザ変更を表示する場合は、**show running-config** コマンドを使用します。

関連トピック

自動 QoS ポリシーとクラス マップ （1498 ページ）
例：auto qos trust cos
例：auto qos trust dscp
例：auto qos video cts
例：auto qos video ip-camera
例：auto qos video media-player
例：auto qos voip trust
例：auto qos voip cisco-phone
例：auto qos voip cisco-softphone
auto qos classify police

自動 QoS のアップグレード（CLI）

この手順は、3.2.2 より古いソフトウェア バージョンのソフトウェア リリースを 3.2.2 以降のソフトウェア バージョンにアップグレードする場合にのみ、実行してください。

始める前に

アップグレードを行う前に、スイッチ上のすべての自動QoS設定を削除する必要があります。この例では、その手順について説明します。

この例の手順を実行した後で、新しいソフトウェア イメージまたはアップグレード後のソフトウェア イメージのスイッチをリブートし、自動 QoS を再設定する必要があります。

手順

ステップ 1 **show auto qos**

例：

```
Device# show auto qos

GigabitEthernet2/0/3
auto qos voip cisco-phone

GigabitEthernet2/0/27
```

```
auto qos voip cisco-softphone
```

特権 EXEC モードでこのコマンドを入力して、現在の自動 QoS 設定をすべて記録します。

ステップ 2 no auto qos

例：

```
Device(config-if)#no auto qos
```

インターフェイス コンフィギュレーション モードで、自動 QoS 設定が行われている各インターフェイスで適切な **no auto qos** コマンドを実行します。

ステップ 3 show running-config | i autoQos

例：

```
Device# show running-config | i autoQos
```

特権EXECモードに戻り、このコマンドを入力して、残りの自動QoSマップ、クラスマップ、ポリシー マップ、アクセス リスト、テーブル マップ、またはその他の設定を記録します。

ステップ 4 no policy-map *policy-map_name*

例：

```
Device)config# no policy-map pmap_101
Device)config# no class-map cmap_101
Device)config# no ip access-list extended AutoQos-101
Device)config# no table-map 101
Device)config# no table-map policed-dscp
```

グローバル コンフィギュレーション モードでこのコマンドを入力して、QoS クラス マップ、ポリシー マップ、アクセス リスト、テーブル マップ、およびその他の自動 QoS 設定を削除します。

- **no policy-map** *policy-map-name*
- **no class-map** *class-map-name*
- **no ip access-list extended** *Auto-QoS-x*
- **no table-map** *table-map-name*
- **no table-map policed-dscp**

ステップ 5 show running-config | i AutoQoS

例：

```
Device# show running-config | i AutoQos
```

特権 EXEC モードに戻り、このコマンドを実行して、自動 QoS 設定がないこと、または自動 QoS 設定の残りの部分がないことを確認します。

ステップ 6 **show auto qos**

例：

```
Device# show auto qos
```

このコマンドを実行して、自動 QoS 設定がないこと、または設定の残りの部分がないことを確認します。

ステップ 7 **write memory**

例：

```
Device# write memory
```

write memory コマンドを入力して、自動 QoS 設定に対する変更を NV メモリに書き込みます。

次のタスク

新しいソフトウェア イメージまたはアップグレード後のソフトウェア イメージでスイッチをリブートします。

新しいソフトウェア イメージまたはアップグレード後のソフトウェア イメージでリブートしたら、ステップ 1 で説明した **show auto qos** コマンドを実行した結果に基づいて、適切なスイッチ インターフェイスの自動 QoS を再設定します。

（注） スイッチまたはスタックごとに、マークダウンの超過用に 1 つのテーブルマップ、マークダウンの違反用に 1 つのテーブルマップが存在します。超過アクションのテーブルマップがスイッチにすでに存在している場合は、自動 QoS ポリシーを適用できません。

関連トピック

自動 QoS の制約事項 （1496 ページ）

自動 QoS 短縮機能のイネーブル化

自動 QoS 短縮機能をイネーブルにするには、次のコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**auto qos global compact** 例： `Device(config)# auto qos global compact`	自動QoS短縮機能がイネーブルになり、自動 QoS のグローバル コンフィギュレーション（非表示）が生成されます。 その後、インターフェイスコンフィギュレーション モードで設定する自動 QoS コマンドを入力できます。システムにより生成されるインターフェイス コマンドも非表示になります。 適用された自動 QoS 設定を表示するには、次の特権 EXEC コマンドを使用します。 • **show derived-config** • **show policy-map** • **show access-list** • **show class-map** • **show table-map** • **show auto-qos** • **show policy-map interface** • **show ip access-lists** これらのコマンドにはキーワード「**AutoQos-**」が付きます。

次のタスク

自動 QoS 短縮機能をディセーブルにするには、対応する自動 QoS コマンドの **no** 形式を入力して自動 QoS インスタンスをすべてのインターフェイスから削除し、次に **no auto qos global compact** グローバル コンフィギュレーション コマンドを実行します。

自動 QoS の監視

表 *86 :* 自動 *QoS* の監視用コマンド

コマンド	説明
show auto qos [**interface** [*interface-id*]]	最初の自動 QoS 設定を表示します。 **show auto qos** コマンド出力と **show running-config** コマンド出力を比較してユーザ定義の QoS 設定を比較できます。
show running-config	自動 QoS によって影響されるかもしれない QoS 設定に関する情報を表示します。 **show auto qos** コマンド出力と **show running-config** コマンド出力を比較してユーザ定義の QoS 設定を比較できます。
show derived-config	自動qosテンプレートにより実行コンフィギュレーションとともに設定される非表示の **mls qos** コマンドを表示します。

自動 QoS に関するトラブルシューティング

自動 QoS のトラブルシューティングを行うには、**debug auto qos** 特権 EXEC コマンドを使用します。詳細については、このリリースのコマンド リファレンスに記載された **debug auto qos** コマンドの説明を参照してください。

ポートで自動QoSをディセーブルにするには、**auto qos** コマンドのインターフェイス コンフィギュレーション コマンドの **no** 形式（**no auto qos voip** など）を使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

自動 QoS の設定例

例：auto qos trust cos

次の例は、**auto qos trust cos** コマンドと、適用されるポリシーとクラス マップを示しています。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

```
Device(config)# interface GigabitEthernet1/0/17
Device(config-if)# auto qos trust cos
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/17

GigabitEthernet1/0/17

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
```

```
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match:  dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10
```

```
Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

例：auto qos trust dscp

次の例は、**auto qos trust dscp** コマンドと、適用されるポリシーとクラス マップを示しています。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Dscp-Input-Policy

- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

```
Device(config)# interface GigabitEthernet1/0/18
Device(config-if)# auto qos trust dscp
Device(config-if)# end
Device#show policy-map interface GigabitEthernet1/0/18


GigabitEthernet1/0/18

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
```

```
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
```

```
    0 packets
    Match:  dscp cs1 (8)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

例：auto qos video cts

次の例は、**auto qos video cts** コマンドと、適用されるポリシーとクラス マップを示しています。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）

- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

```
Device(config)# interface GigabitEthernet1/0/12
Device(config-if)# auto qos video cts
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/12

GigabitEthernet1/0/12

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue-limit dscp 16 percent 80
      queue-limit dscp 24 percent 90
      queue-limit dscp 48 percent 100
      queue-limit dscp 56 percent 100

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 10%
```

```
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
```

```
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

例：auto qos video ip-camera

次の例は、**auto qos video ip-camera** コマンドと、適用されるポリシーとクラス マップを示しています。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

```
Device(config)# interface GigabitEthernet1/0/9
Device(config-if)# auto qos video ip-camera
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/9


GigabitEthernet1/0/9
```

```
Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp dscp table AutoQos-4.0-Trust-Dscp-Table

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
```

```
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
```

```
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

例：auto qos video media-player

次の例は、**auto qos video media-player** コマンドと、適用されるポリシーとクラス マップを示しています。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

```
Device(config)# interface GigabitEthernet1/0/7
Device(config-if)# auto qos video media-player
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/7


 GigabitEthernet1/0/7

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
```

```
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match:  dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
```

```
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

例：auto qos voip trust

次の例は、**auto qos voip trust** コマンドと、適用されるポリシーとクラス マップを示しています。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

```
Device(config)# interface GigabitEthernet1/0/31
Device(config-if)# auto qos voip trust
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/31

GigabitEthernet1/0/31

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1
```

```
Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10
```

```
Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

例：auto qos voip cisco-phone

次の例は、**auto qos voip cisco-phone** コマンドと、適用されるポリシーとクラス マップを示しています。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-CiscoPhone-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- AutoQos-4.0-Voip-Data-CiscoPhone-Class（match-any）
- AutoQos-4.0-Voip-Signal-CiscoPhone-Class（match-any）
- AutoQos-4.0-Default-Class（match-any）
- class-default（match-any）

- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

```
Device(config)# interface GigabitEthernet1/0/5
Device(config-if)# auto qos voip cisco-phone
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/5

GigabitEthernet1/0/5

  Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp cs3
      police:
          cir 32000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Default-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-Default
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp default
```

```
  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
    0 packets
```

```
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

例：auto qos voip cisco-softphone

次の例は、**auto qos voip cisco-softphone** コマンドと、適用されるポリシーとクラス マップを示しています。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-CiscoSoftPhone-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- AutoQos-4.0-Voip-Data-Class（match-any）
- AutoQos-4.0-Voip-Signal-Class（match-any）
- AutoQos-4.0-Multimedia-Conf-Class（match-any）
- AutoQos-4.0-Bulk-Data-Class（match-any）
- AutoQos-4.0-Transaction-Class（match-any）
- AutoQos-4.0-Scavanger-Class（match-any）
- AutoQos-4.0-Signaling-Class（match-any）
- AutoQos-4.0-Default-Class（match-any）
- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

```
Device(config)# interface GigabitEthernet1/0/20
Device(config-if)# auto qos voip cisco-softphone
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/20


GigabitEthernet1/0/20

  Service-policy input: AutoQos-4.0-CiscoSoftPhone-Input-Policy
```

```
Class-map: AutoQos-4.0-Voip-Data-Class (match-any)
  0 packets
  Match:  dscp ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp ef
  police:
      cir 128000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-Class (match-any)
  0 packets
  Match:  dscp cs3 (24)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
      cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af41
  police:
      cir 5000000 bps, bc 156250 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Bulk-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af11
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
```

```
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavanger-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Scavanger
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs1
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Signaling
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
      cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: class-default (match-any)
```

```
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
    0 packets
    Match:  dscp af21 (18) af22 (20) af23 (22)
```

```
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

auto qos classify police

次の例は、**auto qos classify police** コマンドと、適用されるポリシーとクラス マップを示しています。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Classify-Police-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- AutoQos-4.0-Multimedia-Conf-Class（match-any）
- AutoQos-4.0-Bulk-Data-Class（match-any）
- AutoQos-4.0-Transaction-Class（match-any）
- AutoQos-4.0-Scavanger-Class（match-any）
- AutoQos-4.0-Signaling-Class（match-any）
- AutoQos-4.0-Default-Class（match-any）
- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

```
Device(config)# interface GigabitEthernet1/0/6
Device(config-if)# auto qos classify police
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/6


GigabitEthernet1/0/6

  Service-policy input: AutoQos-4.0-Classify-Police-Input-Policy

    Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
```

```
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af41
  police:
      cir 5000000 bps, bc 156250 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Bulk-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af11
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavanger-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Scavanger
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs1
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Signaling
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
```

```
    police:
        cir 32000 bps, bc 8000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Default-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Default
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp default
    police:
        cir 10000000 bps, bc 312500 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100
```

```
  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
```

```
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

auto qos global compact

次に、**auto qos global compact** コマンドの例を示します。

```
Device# configure terminal
Device(config)# auto qos global compact
Device(config)# interface GigabitEthernet1/2
Device(config-if)# auto qos voip cisco-phone

Device# show auto-qos

GigabitEthernet1/2
auto qos voip cisco-phone

Device# show running-config interface GigabitEthernet 1/0/2

interface GigabitEthernet1/0/2
auto qos voip cisco-phone
end
```

自動 QoS の関連情報

自動 QoS 設定で特定の QoS の変更をする必要がある場合は、QoS のマニュアルを確認してください。

自動 QoS に関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	『*QoS Command Reference (Catalyst 3850 Switches)*』 『*Cisco IOS Quality of Service Solutions Command Reference*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
—	

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

自動 QoS の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

QoS の前提条件

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 標準 QoS の概念。
- ワイヤレスの概念とネットワーク トポロジ。
- 従来の Cisco IOS QoS。

- モジュラ QoS CLI（MQC）
- QoS 実装について。
- 使用するアプリケーションのタイプおよびネットワークのトラフィック パターン
- トラフィックの特性およびネットワークのニーズ。たとえば、ネットワークのトラフィックがバーストであるかどうか。音声およびビデオ ストリーム用の帯域幅確保の必要性
- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

関連トピック

有線ターゲットの QoS に関する制約事項 （1583 ページ）
ワイヤレス ターゲットの QoS に関する制約事項 （1587 ページ）

QoS コンポーネント

Quality of Service（QoS）は、次の主要コンポーネントで構成されています。

- 分類：分類は、アクセス コントロール リスト（ACL）、DiffServ コード ポイント（DSCP）、サービス クラス（CoS）、およびその他の要因に基づいて、トラフィックの 1 つのタイプを区別するプロセスです。
- マーキングと変換：マーキングは、特定の情報をネットワークのダウンストリームデバイスに伝送するか、内の 1 つのインターフェイスから別のインターフェイスに情報を伝送するためにトラフィック上で使用されます。トラフィックをマークすると、そのトラフィックの QoS 動作が適用されます。これは、**set** コマンドを直接使用するか、テーブル マップ経由で入力値を受け取って出力の値に直接変換することで実行します。
- シェーピングとポリシング：シェーピングはダウンストリームデバイスで輻輳が発生しないようにトラフィック レートを調整しながら、トラフィックの最大レートを強制するプロセスのことです。最も一般的な形式のシェーピングは、物理または論理インターフェイスから送信されるトラフィックを制限するために使用されます。ポリシングは、トラフィック クラスに最大レートを強制するために使用されます。レートを超過した場合は、イベント発生直後に特定のアクションが実行されます。
- キューイング：キューイングは、トラフィックの輻輳を防止するために使用されます。トラフィックは、帯域割り当てに基づいて処理およびスケジューリングするために、特定のキューに送信されます。次に、トラフィックはポートを介してスケジュールまたは送信されます。
- 帯域幅：帯域幅の割り当てにより、QoS ポリシーが適用されるトラフィックで使用可能な容量が決まります。
- 信頼：信頼により、トラフィックがを通過できるようになります。明示なポリシー設定がない場合、エンド ポイントから、またはエンド ポイントへの DiffServ コード ポイント（DSCP）値、precedence 値、または CoS 値は保持されます。

QoS の用語

この QoS コンフィギュレーション ガイドでは、次の用語が同じ意味で使用されます。

- アップストリーム（に対する方向）は、入力と同じ意味です。
- ダウンストリーム（に対する方向）は、出力と同じ意味です。

（注） アップストリームは、ワイヤレスから有線への方向を指します。ダウンストリームは、有線からワイヤレスへの方向を指します。ワイヤレスからワイヤレスへの方向を指す用語はありません。

QoS の概要

QoS の概要

Quality of Service（QoS）を設定することで、他のトラフィック タイプの代わりに特定のトラフィック タイプを優先的に処理できます。QoS を設定しなかった場合、デバイス はパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。デバイスは、信頼性、遅延限界、またはスループットが保証されていないパケットを送信します。

次に、QoS が提供する具体的な機能を示します。

- 低遅延
- 帯域幅保証
- バッファリング能力とドロップ分野
- トラフィック ポリシング
- フレームまたはパケット ヘッダーの属性変更のイネーブル化
- 関連サービス

関連トピック

有線ターゲットの QoS に関する制約事項 （1583 ページ）
ワイヤレス ターゲットの QoS に関する制約事項 （1587 ページ）

モジュラ QoS コマンドライン インターフェイス

デバイスでは、QoS 機能はモジュラ QoS コマンドライン インターフェイス（MQC）を使用してイネーブルにできます。MQC はコマンドライン インターフェイス（CLI）構造を採用しています。これを使用すると、トラフィック ポリシーを作成し、作成したポリシーをインター

フェイスにアタッチできます。1 つのトラフィック ポリシーには、1 つのトラフィック クラスと 1 つ以上の QoS 機能が含まれます。トラフィック クラスがトラフィックを分類するために使用されるのに対して、トラフィック ポリシーの QoS 機能は分類されたトラフィックの処理方法を決定します。MQC の主な目的の 1 つは、プラットフォームに依存しないインターフェイスを提供することにより、シスコ プラットフォーム全体の QoS を設定することです。

ワイヤレス QoS の概要

ワイヤレス QoS は次のワイヤレス ターゲットで設定できます。

- アクセス ポイントを関連付けることができるすべての物理ポートを含むワイヤレス ポート。
- Radio
- SSID（無線単位、AP 単位、SSID 単位で適用可能）
- クライアント

IOS XE Release 3E 以降、入力 SSID のマーキングおよびポリシング アクションとクライアントのポリシーは、アクセス ポイントで適用されます。で設定する SSID とクライアント入力ポリシーは、アクセス ポイントに移動されます。アクセス ポイントは各パケットのポリシングおよびマーキング アクションを実行します。ただし、は QoS ポリシーを選択します。出力 SSID とクライアント ポリシーのマーキングおよびポリシングは、で適用されます。

次の表に、ワイヤレス ターゲットでポリシーがどのようにサポートされるかを示します。

表 *87*：ワイヤレス ターゲットのポリシーのサポート

ワイヤレスターゲット	サポートされるワイヤレスターゲットのポリシー	出力方向をサポートするポリシー	入力方向をサポートするポリシー
ワイヤレス ポート	Yes	はい：ユーザ設定可能	いいえ
Radio	Yes	はい：ただし、ユーザ設定不可	いいえ
SSID	Yes	はい：ユーザ設定可能	はい：ユーザ設定可能
クライアント	Yes	はい：ユーザ設定可能	はい：ユーザ設定可能

（注） ユーザが設定可能なその他のポリシーには、複数宛先のポリサーおよびVLANが含まれます。

ワイヤレス QoS は次の機能をサポートします。

- 出力方向のキューイング。
- ワイヤレス トラフィックのポリシング

- ワイヤレス トラフィックのマーキング。
- 出力方向のワイヤレス トラフィックのシェーピング。
- 出力方向の Approximate Fair Drop（AFD）。
- QoS のモビリティ サポート。
- Cisco Unified Wireless Controller で使用可能な貴金属の QoS ポリシーとの互換性。
- CLI/Traffic クラス（TCLAS）および CLI/スヌーピングの組み合わせ。
- AVC QoS クライアント ポリシーの設定によるアプリケーション制御（データ トラフィックのドロップやマーキングが可能）。
- 入力ポリシーのドロップ処理。
- クライアントの QoS 統計情報および入力方向の SSID ターゲット。
- ローカル プロファイリング ポリシーの QoS 属性。
- 階層型ポリシー

ワイヤレス用の QoS および IPv6

は IPv4 および IPv6 トラフィックの QoS をサポートし、クライアント ポリシーに IPv4 および IPv6 のフィルタを設定できます。

有線およびワイヤレス アクセスでサポートされる機能

次の表で、有線およびワイヤレス アクセスでサポートされる機能について説明します。

表 *88 :* 有線およびワイヤレス アクセスでサポートされる *QoS* 機能

機能	有線	ワイヤレス
ターゲット	• ギガビットイーサネット • 10 ギガビット イーサネット • VLAN	• ワイヤレス ポート（CAPWAP トンネル） • SSID • クライアント • Radio • CAPWAP マルチキャスト トンネル

機能	有線	ワイヤレス
設定手順	**service-policy** コマンドを使用してインストールされた QoS ポリシー。	• アクセス ポイントがスイッチに接続すると、スイッチはポートにポリシーをインストールします。ポート ポリシーには、port_child_policy という子ポリシーがあります。 • ポリシーは、無線のレートに設定されたシェーパーを持つ無線にインストールされます。デフォルトの無線ポリシー（変更不可）が無線に付加されます。 • WMM クライアントがアソシエートし、アドミッション コントロールが無線でイネーブルにされた場合、デフォルトのクライアント ポリシーが有効になります。 • ユーザは port_child_policy を変更して、さらにクラスを追加できます。 • ユーザは SSID レベルでユーザ定義のポリシーを付加できます。 • ユーザはクライアント レベルでユーザ定義のポリシーを付加できます。
ポート レベルで許可されたキューの数	ポートでは最大 8 つのキューがサポートされます。	サポートされているキューは4つだけです。

機能	有線	ワイヤレス

分類メカニズム	• DSCP
	• IP precedence
	• CoS
	• QoS-group
	• 次を含む ACL のメンバーシップ：
	  • IPv4 ACL
	  • IPv6 ACL
	  • MAC ACL
		• ポート レベル
		  • 入力：ワイヤレス ポートの入力で QoS ポリシーがサポートされていません。
		  • 出力：DSCP ベースの分類だけです。
		• SSID レベル
		  • 入力： DSCP、UP
		  • 出力：DSCP、CoS、QoS グループ
		• クライアント レベル
		  • 入力：ACL、DSCP、 Up
		  • 出力：DSCP および COS

関連トピック

ポート ポリシーの形式 （1547 ページ）

ワイヤレス ターゲットでサポートされる QoS 機能

次の表に、ワイヤレス ターゲットで使用可能なさまざまな機能について説明します。

表 *89*：ワイヤレス ターゲットで使用可能な *QoS* 機能

Target	機能	Traffic	ポリシーが適用される方向	注
ポート	• ポート シェーパー • プライオリティ キューイング • マルチキャストのポリシング	非リアルタイム（NRT）、リアルタイム（RT）	Egress	
Radio	• シェーピング	非リアルタイム	Egress	無線ポリシーはユーザ設定可能ではありません。

Target	機能	Traffic	ポリシーが適用される方向	注
SSID	• ポリシング • テーブル マップ	非リアルタイム、リアルタイム	入力および出力	
	シェーピング		Egress	
	BRR		Egress	
	セット アクション • テーブル マップ • set dscp • set cos		入力	SSID の入力ポリシーのクラス デフォルト クラスおよびユーザ定義クラスの両方でセットを使用できます。 SSID ポリシーのクラス デフォルト クラスのみでテーブル マップを定義できます。
	セット アクション • テーブル マップ • set dscp • set wlan user-priority		Egress	
	ドロップ		入力	
クライアント	ポリシング	非リアルタイム、リアルタイム	入力および出力	クライアント ポリシーでは、次のフィルタがサポートされます。 • ACL • DSCP • Cos（出力の場合のみ） • WLAN UP • プロトコル
	ドロップ		入力	
	セット アクション • set dscp • set cos		入力	
	セット アクション • set dscp • set wlan user-priority		Egress	

関連トピック

ポート ポリシー （1547 ページ）
ポート ポリシーの形式 （1547 ページ）
無線ポリシー （1549 ページ）
WLAN での SSID またはクライアント ポリシーの適用（CLI） （1608 ページ）
SSID ポリシー （1550 ページ）
クライアント ポリシーの設定（CLI）

クライアント ポリシー （1550 ページ）

ポート ポリシー

デバイスはポートベースのポリシーをサポートしています。ポート ポリシーには、ポート シェーパーと子ポリシー（port_child_policy）が含まれます。

（注） ポートの子ポリシーは、スイッチの有線ポートには適用されず、ワイヤレス ポートにだけ適用されます。ワイヤレス ポートは、AP が join するポートとして定義されます。デフォルト ポートの子ポリシーは、起動時にスイッチのワイヤレス ポートに適用されます。ポートのシェーパー レートは 1G に制限されています

ポート シェーパーは、デバイスと AP との間に適用可能なトラフィック ポリシーを指定します。これは、アクセス ポイントでサポートされる無線レートの合計です。

子ポリシーは、ポート子ポリシーで定義されたパケットとキューとの間のマッピングを指定します。子ポリシーは、音声、ビデオ、class-default、および non-client-nrt クラスを含めるように設定できます。この音声とビデオは、DSCP 値（外部 CAPWAP ヘッダーの DSCP 値）に基づいています。class-default の定義は、音声およびビデオ DSCP 以外の値としてシステムに認識されます。

DSCP 値は、パケットがポートに到達するときに割り当てられます。パケットがポートに到着する前に、SSID ポリシーがパケットに適用されます。ポートの子ポリシーには、特定のポート トラフィックでのマルチキャストの割合が含まれます。デフォルトでは、ポートの子ポリシーは使用できるレートの最大 10 % を割り当てます。

関連トピック

ワイヤレス ターゲットの QoS に関する制約事項 （1587 ページ）
ワイヤレス ターゲットでサポートされる QoS 機能 （1545 ページ）
例：音声、ビデオ、およびマルチキャスト トラフィックで分類されたワイヤレス QoS ポリシー （1654 ページ）

ポート ポリシーの形式

ここでは、スイッチのポート ポリシーの動作について説明します。スイッチ ポートでは、有線またはワイヤレスの物理ポートは区別されません。ポリシーは、スイッチに関連付けられたデバイスの種類に応じて適用されます。たとえば、アクセス ポイントがスイッチ ポートに接続されている場合、スイッチはアクセス ポイントをワイヤレス デバイスとして検出し、親子ポリシー形式のデフォルトの階層型ポリシーを適用します。このポリシーは、階層型ポリシーです。親ポリシーは変更できませんが、子ポリシー（port-child ポリシー）は、QoS 設定に合わせて変更できます。スイッチは、デフォルトのクラス マップとポリシー マップで事前に設定されます。

デフォルトのクラス マップ：

```
Class Map match-any non-client-nrt-class
   Match non-client-nrt
```

上記のポート ポリシーは、すべてのネットワーク トラフィックをQ3キューに向けて処理します。クラス マップは、**show class-map** コマンドを実行して表示します。

デフォルトのポリシー マップ：

```
Policy Map port_child_policy
    Class non-client-nrt-class
      bandwidth remaining ratio 10
```

（注） リストされているクラス マップとポリシー マップはシステム定義のポリシーであり、変更できません。

次に、ワイヤレスデバイスが関連付けられているポートで使用可能なシステム定義のポリシー マップを示します。親ポリシーと子ポリシー サービス（**port_child_policy**）で構成される形式です。ネットワークのニーズに応じてポリシーをカスタマイズするには、ポートの子ポリシーを設定する必要があります。

```
Policy-map policy_map_name
    Class class-default
         Shape average average_rate
         Service-policy port_child_policy
```

（注） 親ポリシーは自動生成され、変更できません。ネットワークの QoS 要件に合わせて *port_child_policy* ポリシーを設定する必要があります。

ネットワーク トラフィックのタイプによっては、ポートの子ポリシーを設定できます。たとえば、一般的なワイヤレス ネットワーク構成において、音声およびビデオ トラフィックに特定のプライオリティを割り当てることができます。次に例を示します。

```
Policy-map port_child_policy
     Class  voice-policy-name (match dscp ef)
          Priority level 1
         Police (multicast-policer-name-voice) Multicast Policer
    Class video-policy-name (match dscp af41)
        Priority level 2
        Police (multicast-policer-name-video) Multicast Policer
Class non-client-nrt-class traffic(match non-client-nrt)
        Bandwidth remaining ratio (brr-value-nrt-q2)
    Class class-default  (NRT Data)
        Bandwidth remaining ratio (brr-value-q3)
```

上記のポートの子ポリシー：

- *voice-policy-name*：音声パケット トラフィック用のルールを指定するクラス名を参照します。ここで DSCP 値は、値 46（キーワード **ef** で表される）にマッピングされます。音声トラフィックにはプライオリティ 1 が割り当てられます。

- *video-policy-name*：ビデオ パケット トラフィック用のルールを指定するクラス名を参照します。DSCP 値は、値 34（キーワード **af41** で表される）にマッピングされます。
- *multicast-policer-name-voice*：マルチキャスト音声トラフィックを設定する必要がある場合、音声クラス マップのポリシングを設定できます。
- *multicast-policer-name-video*：マルチキャスト ビデオ トラフィックを設定する必要がある場合、ビデオ クラス マップのポリシングを設定できます。

上記の設定例では、すべての音声およびビデオ トラフィックは Q0 および Q1 キューにそれぞれ送信されます。これらのキューは完全プライオリティを維持します。Q0 および Q1 のパケットはこの順序で処理されます。帯域幅余剰比率 *brr-value-nrt-q2* および *brr-value-q3* はそれぞれ、クラス マップ、*class-default* および *non-client-nrt* で指定された Q2 と Q3 に送信されます。Q2 および Q3 のパケット処理は重み付けラウンドロビン アプローチに基づいています。たとえば *brr-value-nrtq2* の値が 90 で *brr-value-nrtq3* が 10 である場合、キュー 2 とキュー 3 のパケットは 9:1 の比率で処理されます。

関連トピック

ワイヤレス ターゲットの QoS に関する制約事項 （1587 ページ）
ワイヤレス ターゲットでサポートされる QoS 機能 （1545 ページ）
例：音声、ビデオ、およびマルチキャスト トラフィックで分類されたワイヤレス QoS ポリシー （1654 ページ）
有線およびワイヤレス アクセスでサポートされる機能 （1543 ページ）
ポリシー マップ （1561 ページ）

無線ポリシー

無線ポリシーはシステム定義であり、ユーザは設定できません。無線ワイヤレス ターゲットは、出力方向にだけ適用されます。

無線ポリシーは無線単位、アクセス ポイント単位で適用されます。無線のレート制限は、AP 無線レートの実際の制限です。この値は、アクセス ポイントでサポートされている無線の合計と同じです。

次の無線がサポートされます。

- 802.11 a/n
- 802.11 b/n
- 802.11 ac

関連トピック

ワイヤレス ターゲットの QoS に関する制約事項 （1587 ページ）
ワイヤレス ターゲットでサポートされる QoS 機能 （1545 ページ）

SSID ポリシー

入力および出力方向で SSID BSSID（基本サービス セット ID）の QoS ポリシーを作成できます。デフォルトでは、SSID ポリシーはありません。ワイヤレス トラフィックが信頼できないため、すべてのトラフィックはベスト エフォートとして送信されます。SSID の名前に基づいて SSID ポリシーを設定できます。ポリシーは、BSSID 単位で適用できます。

SSID で作成できるポリシーのタイプには、テーブル マップ（table-map）、シェープ レート、RT1（Real Time 1）および RT2（Real Time 2）ポリサーを使用したマーキングが含まれます。トラフィックが入力の場合、通常は、SSID でマーキングおよびポリシング ポリシーを設定します。トラフィックがダウンストリームの場合は、マーキングおよびキューイングを設定できます。

ポートと SSID で設定されているポリシー間では、1 対 1 のマッピングが必要です。たとえば、ポートでクラス音声とクラス ビデオを設定すると、SSID に同様のポリシーを設定できます。

SSID のプライオリティは、帯域幅余剰比率を設定して指定できます。SSID ポリシーのキューイングは、ダウンストリーム方向で適用されます。

関連トピック

WLAN での SSID またはクライアント ポリシーの適用（CLI）（1608 ページ）
ワイヤレス ターゲットでサポートされる QoS 機能（1545 ページ）
例：SSID ポリシー
例：ダウンストリーム SSID ポリシーの設定（1655 ページ）

クライアント ポリシー

クライアント ポリシーは、入力方向と出力方向に適用できます。デバイスのワイヤレス制御モジュールは、WMM クライアントでアドミッション制御がイネーブルの場合に、デフォルト クライアント ポリシーを適用します。アドミッション制御がディセーブルの場合、デフォルト クライアント ポリシーはありません。クライアントではポリシング ポリシーおよびマーキング ポリシーを設定できます。

（注） クライアント ポリシーには、IPv4 フィルタと IPv6 フィルタの両方を設定できます。

クライアント ポリシーは次のように設定できます。

- AAA の使用
- Cisco IOS MQC CLI の使用
  - **service policy client** コマンドは WLAN 設定で使用できます。
- デフォルト設定の使用
- ローカル ポリシーの使用（ネイティブ プロファイリング）

show wireless client mac address *mac_address***service-policy** コマンドを使用して、クライアント ポリシーのソース（ローカル プロファイリング ポリシー、AAA、CLI など）を表示します。クライアント ポリシーの優先順位は、AAA > ローカル ポリシー > WLAN サービス クライアント ポリシー CLI > デフォルト設定です。

（注） ユニファイド ワイヤレス コントローラ手順を設定し、MQC QoS コマンドを使用して AAA を設定した場合は、MQC QoS コマンドによって設定されたポリシーが優先されます。

（注） WLAN にクライアント ポリシーを適用する場合は、クライアント ポリシーを変更する前に WLAN をディセーブルにします。SSID ポリシーは、WLAN がイネーブルでも変更できます。

デフォルトのクライアント ポリシーは、アドミッション制御（ACM）対応の Wi-Fi マルチメディア（WMM）クライアント上でのみイネーブルにされます。

ポリシーの連結

すべてのパケットに最大2つのポリシーを適用できます。最初にクライアントターゲット、次に SSID ターゲットです。クライアントのポリシングアクションは、クライアント ポリシーで指定されたマーキングアクションの前にパケットに適用されます。クライアントのポリシングおよびマーキング アクションがパケットに適用されると、SSID ポリシー アクションが更新されたパケットに適用されます。カスタム ポリシーが指定されていない場合は、システムの信頼設定がパケットに適用されます。出力の信頼は DSCP に基づいており、入力の信頼は WLAN ユーザ プライオリティに基づいています。

関連トピック

クライアント ポリシーの設定（CLI）
ワイヤレス ターゲットでサポートされる QoS 機能 （1545 ページ）
例：クライアント ポリシー （1657 ページ）

階層型 QoS

は階層型 QoS（HQoS）をサポートします。HQoS を使用すると、次の作業を実行できます。

- 階層型分類：トラフィック分類は、他のクラスに基づいています。
- 階層型ポリシング：階層型ポリシーの複数のレベルでポリシングを設定するプロセス。
- 階層型シェーピング：シェーピングは、階層の複数のレベルで設定できます。

（注） 階層型シェーピングは、ポート シェーパーでのみサポートされます。ポート シェーパーでは、親に対してクラス デフォルトの設定だけが可能で、クラスデフォルトのアクションはシェーピングだけです。

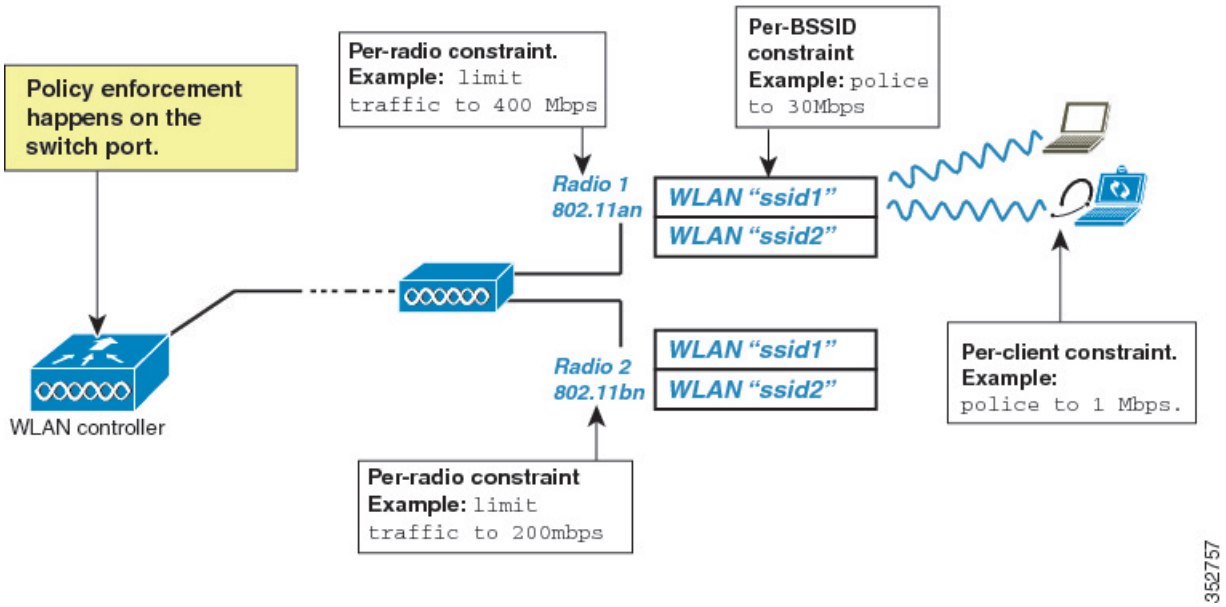
関連トピック

例：階層型分類 （1652 ページ）
例：階層型ポリシーの設定 （1652 ページ）

階層型ワイヤレス QoS

デバイスは、ワイヤレス ターゲットの階層型 QoS をサポートしています。階層型 QoS ポリシーは、ポート、無線、SSID、およびクライアントに適用されます。デバイスに設定された QoS ポリシー（マーキング、シェーピング、ポリシングを含む）は、複数のターゲットに適用できます。ネットワークに非リアルタイム トラフィックが含まれている場合、非リアルタイム トラフィックは Approximate Fair Drop に従います。階層は、デバイスに送信されるパケット上のさまざまな QoS ポリシーの適用プロセスに関係します。親と子ポリシーの両方に対してポリシングを設定できます。

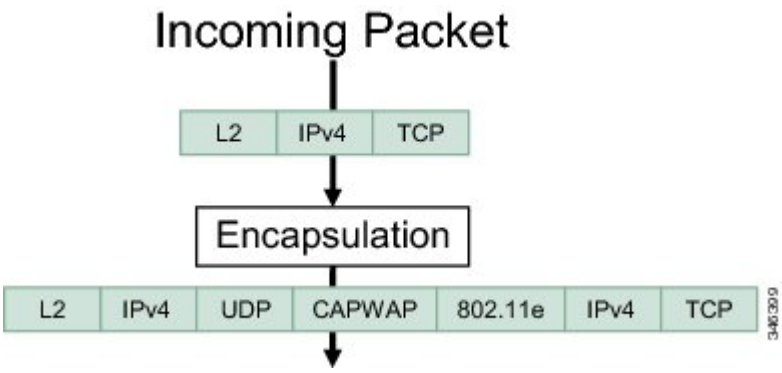
（注） 階層型クライアントおよび SSID ポリシーでは、親または子ポリシーのいずれかに対してのみポリシングを設定できます。



ワイヤレス パケット形式

図 *92*：最初のパスでの出力方向のワイヤレス パケット パス

この図は、階層型ワイヤレス QoS で使用されるワイヤレス パケット フローおよびカプセル化を示します。着信パケットは、デバイスに入ります。デバイスはこの着信パケットをカプセル化し、802.11e および CAPWAP ヘッダーを追加します。



階層型 AFD

Approximate Fair Dropping（AFD）は、Cisco IOS の QoS インフラストラクチャが提供する機能です。ワイヤレス ターゲットの場合、AFD は SSID（シェーピングによる）とクライアント（ポリシングによる）で設定できます。AFD のシェーピング レートはダウンストリーム方向のみに適用されます。ユニキャストのリアルタイム トラフィックは AFD ドロップの対象ではありません。

QoS の実装

ネットワークは通常、ベストエフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、正しいタイミングで配信される可能性も同じです。輻輳が発生すると、すべてのトラフィックが等しくドロップされます。

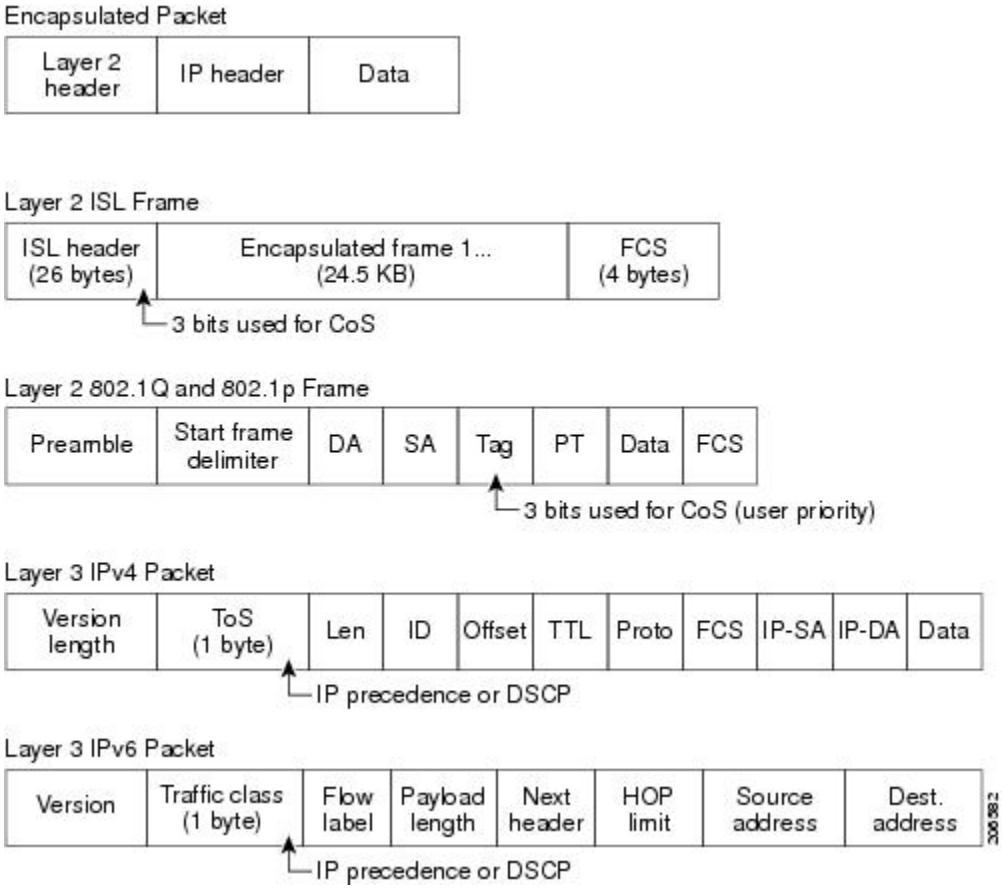
QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、相対的な重要性に応じてそのトラフィックに優先度を指定し、輻輳管理および輻輳回避技術を使用して、優先処理を実行できます。ネットワークに QoS を実装すると、ネットワーク パフォーマンスがさらに予測しやすくなり、帯域幅をより効率的に利用できるようになります。

QoS は、インターネット技術特別調査委員会（IETF）の規格である Differentiated Services（Diff-Serv）アーキテクチャに基づいて実装されます。このアーキテクチャでは、ネットワークに入るときに各パケットを分類することが規定されています。

この分類は IP パケット ヘッダーに格納され、推奨されない IP タイプ オブ サービス（ToS）フィールドの 6 ビットを使用して、分類（クラス）情報として伝達されます。分類情報をレイヤ 2 フレームでも伝達できます。

図 *93*：フレームおよびパケットにおける *QoS* 分類レイヤ

次の図にレイヤ 2 フレームまたはレイヤ 3 パケットの特殊ビットを示します。



関連トピック

有線ターゲットの QoS に関する制約事項 （1583 ページ）
ワイヤレス ターゲットの QoS に関する制約事項 （1587 ページ）

レイヤ 2 フレームのプライオリティ ビット

レイヤ 2 の ISL（スイッチ間リンク）フレーム ヘッダーには、下位 3 ビットで IEEE 802.1p サービス クラス（CoS）値を伝達する 1 バイトのユーザ フィールドがあります。レイヤ 2 ISL トランクとして設定されたポートでは、すべてのトラフィックが ISL フレームに収められます。

レイヤ 2 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット（ユーザ プライオリティ ビット）で CoS 値が伝達されます。レイヤ 2 802.1Q トランクとして設定されたポートでは、ネイティブ Virtual LAN（VLAN）のトラフィックを除くすべてのトラフィックが 802.1Q フレームに収められます。

他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。

レイヤ 2 CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

レイヤ 3 パケットのプライオリティ ビット

レイヤ 3 IP パケットは、IP precedence 値または Diffserv コード ポイント（DSCP）値のいずれかを伝送できます。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値も使用できます。

IP precedence 値の範囲は 0 ～ 7 です。DSCP 値の範囲は 0 ～ 63 です。

分類を使用したエンドツーエンドの QoS ソリューション

インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンドホストが割り当てるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳細な検証は、コア スイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィック クラスに割り当てるリソースの量を制限できます。Diff-Serv アーキテクチャでトラフィックを処理するときの、各デバイスの動作をホップ単位動作といいます。パス上のすべてのデバイスに一貫性のあるホップ単位動作をさせることによって、エンドツーエンドの QoS ソリューションを構築できます。

ネットワーク上で QoS を実装する作業は、インターネットワーキング デバイスが提供する QoS 機能、ネットワークのトラフィック タイプおよびパターン、さらには着信および発信トラフィックに求める制御のきめ細かさによって、簡単にも複雑にもなります。

パケット分類

パケット分類は、特定の基準に基づいて定義したポリシーの複数のクラスの 1 つに属するものとしてパケットを識別するプロセスです。モジュラ QoS CLI（MQC）は、ポリシー クラス ベースの言語です。ポリシー クラスの言語は、次の定義に使用されています。

- 1 つまたは複数の一致基準があるクラス マップ テンプレート
- 1 つまたは複数のクラスがポリシー マップに関連付けられているポリシーマップ テンプレート

ポリシーマップ テンプレートは、の 1 つまたは複数のインターフェイスに関連付けられます。

パケット分類は、ポリシーマップで定義されたクラスの 1 つに属するものとしてパケットを識別するプロセスです。分類プロセスは、処理されるパケットがクラス内の特定のフィルタに一致した場合に終了します。これは、最初の一致による終了と呼ばれます。つまり、ポリシーマップ内のクラスの順序に関係なく、パケットがポリシー内の複数のクラスに一致する場合、最初のクラスの一致後に分類プロセスが終了します。

パケットがポリシーのクラスと一致しない場合は、ポリシーのデフォルト クラスに分類されます。すべてのポリシー マップには、システム定義のクラスのデフォルト クラスがあり、どのユーザ定義クラスにも一致しないパケットに一致します。

パケット分類は次のタイプに分類できます。

- パケットと合わせて伝搬される情報に基づく分類
- 固有の情報に基づく分類
- 階層型分類

パケットと合わせて伝搬される情報に基づく分類

パケットの一部としてエンドツーエンドまたはホップ間で伝搬される情報に基づく分類には、一般的に次のものがあります。

- レイヤ 3 またはレイヤ 4 ヘッダーに基づく分類
- レイヤ 2 情報に基づく分類

レイヤ *3* またはレイヤ *4* ヘッダーに基づく分類

これは最も一般的な導入シナリオです。レイヤ 3 およびレイヤ 4 ヘッダーの多くのフィールドは、パケット分類に使用できます。

最もきめ細かいレベルでは、この分類方法はフロー全体を照合するために使用できます。この導入タイプで、アクセス コントロール リスト（ACL）を使用できます。ACL は、フローのさまざまなサブセット（送信元 IP アドレスのみ、宛先 IP アドレスのみ、または両方の組み合わせなど）に基づく照合に使用することもできます。

分類は、IP ヘッダーの precedence 値または DSCP 値に基づいて実行することもできます。IP precedence フィールドは、特定のパケットを処理する必要がある相対プライオリティを示すために使用されます。これは、IP ヘッダー内のタイプ オブ サービス（ToS）バイトの 3 ビットで構成されます。

次の表に、さまざまな IP precedence ビット値と名前を示します。

（注） IP precedence はワイヤレス QoS ではサポートされません。

表 *90 : IP precedence* 値と名前

IP precedence 値	IP precedence ビット	IP precedence の名前
0	000	ルーチン
1	001	プライオリティ
2	010	即時
3	011	Flash
4	100	フラッシュ オーバーライド
5	101	重大
6	110	インターネットワーク制御

IP precedence 値	IP precedence ビット	IP precedence の名前
7	111	ネットワーク制御

（注） ネットワークのルーティング制御トラフィックすべては、IP precedence 値 6 をデフォルトで使用します。また、IP precedence 値 7 は、ネットワーク制御トラフィック用に予約されています。したがって、IP precedence 値 6 および 7 はユーザ トラフィック用に推奨されません。

DSCP フィールドは、IP ヘッダーの 6 ビットで構成され、インターネット技術特別調査委員会（IETF）の DiffServ ワーキング グループにより標準化されています。DSCP ビットが含まれた元の ToS バイトは、DSCP バイトの名前を変更しました。DSCP フィールドは、IP precedence と同様に IP ヘッダーの一部です。DSCP フィールドは、IP precedence フィールドのスーパー セットです。したがって、DSCP フィールドは、IP precedence に関連して説明した内容と同様の方法で使用され、設定されます。

（注） DSCP フィールド定義は IP precedence 値と下位互換性があります。

レイヤ *2* ヘッダーに基づく分類

レイヤ 2 ヘッダー情報に基づく分類は、さまざまな方法で実行できます。最も一般的な方法は次のとおりです。

- MAC アドレスベースの分類（アクセス グループの場合のみ）：分類は送信元 MAC アドレス（入力方向のポリシー用）および宛先 MAC アドレス（出力方向のポリシー用）に基づいています。
- サービス クラス：分類は、IEEE 802.1p 標準に基づくレイヤ 2 ヘッダーの 3 ビットに基づいて行われます。これは通常、IP ヘッダーの ToS バイトにマッピングします。
- VLAN ID：分類は、パケットの VLAN ID に基づいて行われます。

（注） レイヤ 2 ヘッダー内のこれらフィールドの一部は、ポリシーを使用して設定することもできます。

デバイス固有の情報に基づく分類（QoS グループ）

は分類がパケット ヘッダーまたはペイロードの情報に基づいていない場合に使用できる分類メカニズムを提供します。

複数の入力インターフェイスから出力インターフェイスの特定のクラスに送信されるトラフィックを集約する必要が生じる場合があります。たとえば、複数のカスタマー エッジ ルータが、異なるインターフェイスの同じアクセス に接続される可能性があります。サービス プロバイ

ダーは、特定のレートでコアに送信されるすべての集約音声トラフィックをポリシングする場合があります。ただし、異なるカスタマーからの音声トラフィックには、異なるToS設定がなされている可能性があります。QoS グループベースの分類は、次のシナリオで役立つ機能です。

入力インターフェイスで設定されたポリシーは、QoS グループを特定の値に設定します。この値は出力インターフェイスでイネーブルになっているポリシーのパケットの分類に使用できます。

QoS グループは、内部のパケット データ構造内のフィールドです。QoS グループは、の内部ラベルであり、パケット ヘッダーの一部ではないことに注意してください。

階層型分類

では、他のクラスに基づく分類を実行できます。通常このアクションは、1つのクラスマップに複数クラスの分類メカニズム（フィルタ）を組み合わせる場合に必要になります。

QoS 有線モデル

QoS を実装するには、で次のタスクを実行する必要があります。

- トラフィック分類：パケットまたはフローを相互に区別します。
- トラフィック マーキングおよびポリシング：パケットがを移動するときに、特定の QoS を示すラベルを割り当て、パケットが設定されたリソース使用率制限に準拠するようにします。
- キューイングおよびスケジューリング：リソース競合があるすべての状況で、異なる処理を行います。
- シェーピング：から送信されるトラフィックが、特定のトラフィック プロファイルに適合するようにします。

入力ポートのアクティビティ

次のアクティビティはの入力ポートで発生します。

- 分類：パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。たとえば、は、ある種類のトラフィックを別の種類のトラフィックと区別するためにパケット内の CoS または DSCP を QoS ラベルにマッピングします。生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを識別します。
- ポリシング：ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィック フローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。
- マーキング：マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットのQoSラベルをマークダウンするか、またはパケットをドロップするか）を決定します。

（注） ワイヤレス入力ポートでのポリシー適用は、ではサポートされていません。

出力ポートのアクティビティ

次のアクティビティは、の出力ポートで発生します。

- ポリシング：ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィック フローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。
- マーキング：マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットのQoSラベルをマークダウンするか、またはパケットをドロップするか）を決定します。
- キューイング：キューイングでは、使用する出力キューを選択する前に、QoS パケット ラベルおよび対応するDSCP値またはCoS値を評価します。複数の入力ポートが1つの出力ポートに同時にデータを送信すると輻輳が発生することがあるため、重み付けテール ドロップ（WTD）によってトラフィック クラスを区別し、QoS ラベルに基づいてパケットに別々のしきい値を適用します。しきい値を超過している場合、パケットはドロップされます。

分類

分類とは、パケットのフィールドを検証して、トラフィックの種類を区別するプロセスです。分類は、で QoS がイネーブルの場合のみイネーブルになります。デフォルトでは、QoS はでイネーブルにされています。

分類中に、は検索処理を実行し、パケットに QoS ラベルを割り当てます。QoS ラベルは、パケットに対して実行するすべての QoS アクション、およびパケットの送信元キューを識別します。

アクセス コントロール リスト

IP標準ACL、IP拡張ACL、またはレイヤ2MAC ACLを使用すると、同じ特性を備えたパケット グループ（クラス）を定義できます。また IPv6 ACL に基づいて IP トラフィックを分類することもできます。

QoSのコンテキストでは、アクセス コントロール エントリ（ACE）の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なります。

- 許可アクションとの一致が検出されると（最初の一致の原則）、指定のQoS関連アクションが実行されます。
- 拒否アクションと一致した場合は、処理中の ACL がスキップされ、次の ACL が処理されます。

- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットでは QoS 処理は実行されず、によってベストエフォート型サービスが実行されます。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの一致が見つかると、それ以降の検索処理は中止され、QoS 処理が開始されます。

（注） アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

ACL でトラフィック クラスを定義した後で、そのトラフィック クラスにポリシーを結合できます。ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。ポリシーには、特定の集約としてクラスを分類する（DSCP を割り当てるなど）コマンドまたはクラスのレート制限を実施するコマンドを含めることができます。このポリシーを特定のポートに結合すると、そのポートでポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類する場合は、**access-list** グローバル コンフィギュレーション コマンドを使用します。レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

クラス マップ

クラス マップは、特定のトラフィック フロー（またはクラス）に名前を付けて、他のすべてのトラフィックと区別するためのメカニズムです。クラスマップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。この条件には、ACL で定義されたアクセス グループとの照合、または DSCP 値や IP precedence 値の特定のリストとの照合を含めることができます。複数のトラフィック タイプを分類する場合は、別のクラスマップを作成し、異なる名前を使用できます。パケットをクラスマップ条件と照合した後で、ポリシー マップを使用してさらに分類します。

クラスマップを作成するには、**class-map** グローバル コンフィギュレーション コマンドまたは **class** ポリシー マップ コンフィギュレーション コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用する必要があります。**class-map** コマンドを入力すると、によってクラスマップ コンフィギュレーション モードが開始されます。このモードで、**match** クラス マップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

class class-default ポリシー マップ コンフィギュレーション コマンドを使用して、デフォルト クラスを作成できます。デフォルト クラスはシステム定義であり、設定することはできません。分類されていないトラフィック（トラフィック クラスで指定された一致基準を満たさないトラフィック）は、デフォルト トラフィックとして処理されます。

関連トピック

トラフィック クラスの作成（CLI） （1590 ページ）

例：アクセス コントロール リストによる分類 （1650 ページ）

ポリシー マップ

ポリシー マップでは、作用対象のトラフィック クラスを指定します。アクションには次が含まれます。

- トラフィック クラスに特定の DSCP 値または IP precedence 値を設定する
- トラフィック クラスに CoS 値を設定する
- QoS グループを設定する
- トラフィック クラスのワイヤレス LAN（WLAN）値を設定する
- トラフィックがアウト オブ プロファイルになった場合の、トラフィックの帯域幅制限やアクションを指定する

ポリシー マップを効率的に機能させるには、ポートにポリシー マップを結合する必要があります。

ポリシー マップを作成して名前を付けるには、**policy-map** グローバル コンフィギュレーション コマンドを使用します。このコマンドを入力すると、によってポリシーマップ コンフィギュレーション モードが開始されます。このモードでは、**class**、または **set** ポリシー マップ コンフィギュレーション コマンドおよびポリシー マップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行するアクションを指定します。

ポリシー マップは、ポリシーマップ クラス コンフィギュレーション コマンド **police** と **bandwidth** を使用して設定することもできます。これらのコマンドは、ポリサー、トラフィックの帯域幅制限、および制限を超過した場合のアクションを定義します。加えて、ポリシー マップは、**priority** ポリシーマップ クラス コンフィギュレーション コマンド（クラスの優先順位をスケジューリングする）、またはキューイング ポリシーマップ クラス コンフィギュレーションコマンド（**queue-buffers** および **queue-limit**）を使用すると、より詳細に設定できます。

ポリシー マップを有効化するには、**service-policy**インターフェイス コンフィギュレーション コマンドを使用してポートに接続します。

（注） ポリシー マップに **priority** と **set** を両方設定することはできません。これらのコマンド両方をポリシー マップに設定すると、ポリシー マップをインターフェイスに適用した際に、エラーメッセージが表示されます。次に、この制限の例を示します。

```
Switch# configure terminal
Switch(config)# class-map cmap
Switch(config-cmap)# exit
Switch(config)# class-map classmap1
Switch(config-cmap)# exit
Switch(config)# policy-map pmap
Switch(config-pmap)# class cmap
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classmap1
Switch(config-pmap-c)# set
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1/1
Switch(config-if)# service-policy output pmap

Non-queuing action only is unsupported in a queuing policy!!!
%QOS-6-POLICY_INST_FAILED:
Service policy installation failed
```

関連トピック

トラフィック ポリシーの作成（CLI） （1593 ページ）
ポート ポリシーの形式 （1547 ページ）

物理ポートのポリシー マップ

実行対象となるトラフィック クラスを指定する非階層型ポリシー マップを、物理ポート上に設定できます。アクションには、トラフィック クラスでの特定の DSCP または IP precedence 値の設定、一致する各トラフィック クラス（ポリサー）に対するトラフィックの帯域幅限度の指定、トラフィックがアウト オブ プロファイル（マーキング）の場合の処理などが含まれます。

ポリシー マップには、次の特性もあります。

- 1 つのポリシー マップに、それぞれ異なる一致条件とポリサーを指定した複数のクラス ステートメントを指定できます。
- ポリシー マップには、事前に定義されたデフォルトのトラフィック クラスを含めることができます。デフォルトのトラフィック クラスはマップの末尾に明示的に配置されます。

  class class-default ポリシーマップ コンフィギュレーション コマンドを使用してデフォルトのトラフィック クラスを設定すると、未分類トラフィック（トラフィック クラスで指定された一致基準に一致しないトラフィック）はデフォルトのトラフィック クラス（**class-default**）として処理されます。
- 1 つのポートから受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。

関連トピック

トラフィック ポリシーのインターフェイスへの付加（CLI）（1606 ページ）

VLAN のポリシー マップ

は、VLAN の QoS 機能をサポートします。これにより、ユーザは、着信フレームの VLAN 情報を使用して VLAN レベルで QoS 処理（分類と QoS アクション）を実行できます。VLAN ベースの QoS では、サービス ポリシーが SVI インターフェイスに適用されます。VLAN ポリシー マップに属するすべての物理インターフェイスは、ポートベースのポリシー マップの代わりに VLAN ベースのポリシー マップが表示されるようにプログラムする必要があります。

ポリシーマップはVLAN SVIに適用されますが、ポリシング（レート制限）アクションはポート単位でしか実行できません。複数の物理ポートからのトラフィックの合計が認識されるようにポリサーを設定できません。各ポートは、そのポートに着信するトラフィックを制御する別のポリサーを必要とします。

関連トピック

ポリシーマップによるSVIのトラフィックの分類、ポリシング、およびマーキング（CLI）（1613 ページ）
例：ポリサーの VLAN 設定 （1663 ページ）

ワイヤレス QoS マルチキャスト

ポート レベルでマルチキャストのポリシング レートを設定できます。

関連トピック

例：音声、ビデオ、およびマルチキャスト トラフィックで分類されたワイヤレス QoS ポリシー （1654 ページ）

ポリシング

パケットが分類され、DSCP ベース、CoS ベース、または QoS グループのラベルが割り当てられると、ポリシングおよびマーキング プロセスを開始できます。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。制限を超えるパケットは、「アウト オブ プロファイル」または「不適合」になります。各ポリサーはパケットごとに、パケットが適合か不適合かを判別し、パケットに対するアクションを指定します。これらのアクションはマーカーによって実行されます。パケットを変更しないで通過させるアクション、パケットをドロップするアクション、またはパケットに割り当てられたDSCPまたはCoS値を変更（マークダウン）してパケットの通過を許可するアクションなどがあります。

パケットの混乱を避けるため、通常、適合トラフィックも不適合トラフィックも同じキューを通過します。

（注） すべてのトラフィックは、ブリッジングされるかルーティングされるかに関係なく、ポリサーの影響を受けます（ポリサーが設定されている場合）。その結果、ブリッジングされたパケットは、ポリシングまたはマーキングが行われたときにドロップされたり、DSCP または CoS フィールドが変更されたりすることがあります。

物理ポートでのみポリシングを設定できます。

ポリシー マップおよびポリシング アクションを設定したら、**service-policy**インターフェイス コンフィギュレーション コマンドを使用して、入力ポートまたは SVI にポリシーを付加します。

関連トピック

ポリシングの設定（CLI） （1631 ページ）
例：ポリシング アクションの設定 （1662 ページ）

トークンバケット アルゴリズム

ポリシングはトークンバケット アルゴリズムを使用します。各フレームがに着信すると、バケットにトークンが追加されます。バケットにはホールがあり、平均トラフィック レートとして指定されたレート（ビット/秒）で送信されます。バケットにトークンが追加されるたびに、はバケット内に十分なスペースがあるかを確認します。十分なスペースがなければ、パケットは不適合とマーキングされ、指定されたポリサーアクション（ドロップまたはマークダウン）が実行されます。

バケットが満たされる速度は、バケット深度（burst-byte）、トークンが削除されるレート（rate-bps）、および平均レートを上回るバースト期間によって決まります。バケットのサイズによってバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バースト期間が短い場合、バケットはオーバーフローせず、トラフィック フローに何のアクションも実行されません。ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシングアクションが実行されます。

バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの burst-byte オプションを使用します。トークンがバケットから削除される速度（平均速度）を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの rate オプションを使用します。

関連トピック

ポリシングの設定（CLI） （1631 ページ）
例：ポリシングの単位 （1663 ページ）

マーキング

マーキングは、特定の情報をネットワークのダウンストリームデバイスに伝送するか、内の 1 つのインターフェイスから別のインターフェイスに情報を伝送するために使用します。

マーキングは、パケット ヘッダーの特定のフィールド/ビットを設定するか、内部のパケット構造内の特定のフィールドを設定するために使用できます。さらに、マーキング機能はフィールド間のマッピングの定義に使用できます。QoS では次のマーキング方法を使用できます。

- パケット ヘッダー
- デバイス（）固有の情報
- テーブル マップ

パケット ヘッダーのマーキング

パケット ヘッダー フィールドのマーキングは 2 種類の一般的なカテゴリに分類できます。

- IPv4/v6 ヘッダー ビット マーキング
- レイヤ 2 ヘッダー ビット マーキング

IP レベルのマーキング機能は、precedence を設定したり、IP ヘッダー内の DSCP を特定の値に設定したりして、ダウンストリームデバイス（スイッチまたはルータ）で特定のホップごとの動作を実行するために使用されます。また、異なる入力インターフェイスからのトラフィックを、出力インターフェイス内の単一のクラスに集約するためにも使用できます。この機能は現在、IPv4 および IPv6 ヘッダーでサポートされています。

レイヤ 2 ヘッダーのマーキングは、通常、ダウンストリーム デバイス（スイッチまたはルータ）のドロップ動作に影響を与えるために使用されます。これは、レイヤ2ヘッダーの一致と並行して動作します。ポリシーマップを使用して設定されるレイヤ2ヘッダーのビットはサービス クラスです。

スイッチ固有の情報のマーキング

この形式のマーキングには、パケットヘッダーの一部ではないパケットデータ構造内のフィールドのマーキングが含まれます。これにより、後でデータパスでマーキングを使用できるようになります。これはスイッチ間で伝搬されません。QoS グループのマーキングはこのカテゴリに分類されます。この形式のマーキングは、入力インターフェイスで有効になっているポリシーだけでサポートされます。対応する照合機能を同じスイッチの出力インターフェイスでイネーブルにし、適切な QoS アクションを適用することができます。

テーブル マップのマーキング

テーブル マップ マーキングは変換表を使用したフィールド間のマッピングおよび変換を可能にします。この変換表はテーブル マップと呼ばれます。

インターフェイスに接続されているテーブル マップに応じて、パケット内の CoS、DSCP、および UP 値（ワイヤレス パケットに固有の UP）が書き換えられます。により、入力のテーブル マップ ポリシーと出力のテーブル マップ ポリシーを設定できます。

（注） のスタックは、合計 14 のテーブル マップをサポートします。各方向の有線ポート単位で 1 つのテーブル マップだけがサポートされます。

たとえば、テーブル マップは、レイヤ 2 CoS 設定をレイヤ 3 の precedence 値にマッピングするのに使用できます。この機能により、マッピングを実行する方法を示す 1 つのテーブルに複数の **set** コマンドを組み合わせて使用することができます。このテーブルは複数のポリシーで参照するか、または同じポリシー内で複数回参照することができます。

次の表に、現在サポートされているマッピング形式を示します。

表 *91 : To-From* 関係を確立するために使用されるパケット マーキング タイプ

パケット マーキング タイプ「To」	パケット マーキング タイプ「From」
Precedence	CoS
Precedence	QoS グループ
DSCP	CoS
DSCP	QoS グループ
CoS	Precedence
CoS	DSCP
QoS グループ	Precedence
QoS グループ	DSCP

テーブル マップ ベースのポリシーでは、次の機能がサポートされています。

- 変換：1 つの DSCP 値セットから別の DSCP 値セットにマッピングするテーブル マップを利用できます。また、このテーブル マップは出力ポートに付加できます。
- 書き換え：入力パケットは設定されたテーブル マップに基づいて書き換えられます。
- マッピング：テーブル マップ ベースのポリシーは、set ポリシーの代わりに使用できます。

テーブル マップ マーキングには、次の手順が必要です。

1. テーブルマップの定義：**table-map** グローバル コンフィギュレーション コマンドを使用して値をマッピングします。テーブルが使用されるクラスまたはポリシーは認識されません。テーブルマップのデフォルトのコマンドは、「from」フィールドで一致がない場合に値が「to」フィールドにコピーされることを示すために使用されます。
2. ポリシー マップの定義：テーブル マップを使用するポリシー マップを定義します。
3. ポリシーをインターフェイスに関連付けます。

（注） 入力ポートのテーブル マップ ポリシーによって、そのポートの信頼設定が qos-marking の「from」タイプに変更されます。

関連トピック

テーブル マップの設定（CLI） （1617 ページ）
例：テーブル マップのマーキング設定 （1665 ページ）

トラフィックの調整

ネットワークで QoS をサポートするには、サービス プロバイダー ネットワークに入るトラフィックをネットワーク境界ルータでポリシングし、トラフィック レートがサービス範囲内に収まるようにする必要があります。ネットワーク コアのプロビジョニングで処理できるように設定されているトラフィックよりも多くのトラフィックがネットワーク境界のいくつかのルータから送信開始されると、トラフィック負荷の増加によってネットワーク輻輳が発生します。ネットワークのパフォーマンスが低下すると、すべてのネットワーク トラフィックで QoS を提供することが困難になります。

トラフィック ポリシング機能（ポリシング機能を使用）およびシェーピング機能（トラフィック シェーピング機能を使用）はトラフィック レートを管理しますが、トークンが不足した場合のトラフィックの処理方法が異なります。トークンの概念は、トークン バケット方式、トラフィック測定機能に基づいています。

（注） ネットワーク トラフィックで QoS テストを実行すると、シェーパー データとポリシング データで異なる結果が生じることがあります。シェーピングからのネットワーク トラフィック データの方が、より正確な結果が得られます。

この表は、ポリシングとシェーピングの機能を比較します。

表 *92*：ポリシングとシェーピングの機能の比較

ポリシング機能	シェーピング機能
適合するトラフィックをライン レートで送信し、バーストを許可します。	トラフィックが固定レートでスムーズに送信されます。
トークンが不足すると、アクションがただちに実行されます。	トークンが不足すると、パケットをバッファし、後でトークンが使用可能になった時点で送信します。シェーピングを使用するクラスにはキューが関連付けられており、このキューを使用してパケットがバッファされます。
ポリシングは、ビット/秒、パケット/秒、およびセル/秒など複数の単位で設定できます。	シェーピングの設定単位はビット/秒だけです。

ポリシング機能	シェーピング機能
ポリシングには、イベントに複数の可能なアクションが関連付けられています。このようなアクションの例としては、イベント、マーキング、ドロッピングなどがあります。	シェーピングはプロファイルを満たさないパケットをマークできません。
入出力両方のトラフィックで機能します。	出力トラフィックに対してのみ実装されます。
ウィンドウ サイズを小さくしたためにパケット ドロップが発生すると、伝送制御プロトコル（TCP）は、回線速度でラインを検出しますが、設定されたレートに適合します。	TCP は低速回線があることを検出し、再送信タイマーを適切に調整できます。これにより、再送信の範囲が狭くなり、TCP に負担をかけません。

ポリシング

QoS ポリシング機能は、トラフィック クラスに最大レートを強制するために使用されます。QoS ポリシング機能は、プライオリティ機能と合わせて、プライオリティ トラフィックを制限するためにも使用できます。レートを超過した場合は、イベント発生直後に特定のアクションが実行されます。レート（認定情報レート [CIR] および最大情報レート [PIR]）とバーストパラメータ（適合バースト サイズ [B_c] および拡張バースト サイズ [B_e]）は、すべてバイト/秒で設定されます。

QoS では次のポリシング形式またはポリサーがサポートされます。

- シングルレート 2 カラー ポリシング
- デュアルレート 3 カラー ポリシング

（注） シングルレート 3 カラー ポリシングはサポートされません。

シングルレート 2 カラー ポリシング

シングルレート 2 カラー ポリサーは、CIR と B_c だけを設定するモードです。

B_c は任意のパラメータであり、これが指定されていない場合、デフォルトで計算されます。このモードでは、着信パケットに十分なトークンがある場合、パケットは適合すると見なされます。パケットの到着時に、十分なトークンが B_c の範囲内で使用できない場合、パケットは設定レートを超えたと見なされます。

（注） トークンバケットアルゴリズムの詳細については、トークンバケットアルゴリズム（1564 ページ）を参照してください。

関連トピック

ポリシングの設定（CLI） （1631 ページ）

例：シングルレート 2 カラー ポリシング設定 （1664 ページ）

デュアルレート 3 カラー ポリシング

デュアル レート ポリサーでのは、カラー ブラインド モードのみをサポートします。このモードでは、認定情報レート（CIR）および最大情報レート（PIR）を設定します。名前からわかるように、この場合、最大レート用に 1 つ、認定レート用に 1 つの、合わせて 2 つのトークン バケットがあります。

（注） トークンバケットアルゴリズムの詳細については、トークンバケットアルゴリズム （1564 ページ）を参照してください。

カラー ブラインド モードでは、最大レートのバケットの着信パケットが最初にチェックされます。十分な数のトークンがない場合、パケットはレートに違反していると見なされます。十分な数のトークンがある場合、次に適合レートのバケットのトークンをチェックして、十分な数のトークンがあるかどうかを判別します。最大レートのバケットにあるトークンは、パケットのサイズによって減少します。十分な数のトークンがない場合、パケットが設定されているレートを超過していると見なされます。十分な数のトークンがある場合、パケットは適合すると見なされ、両方のバケットのトークンは、パケットのサイズによって減少します。

トークン補充レートは着信パケットによって異なります。あるパケットが時間 T1 に着信し、次のパケットが時間 T2 に着信したとします。T1 と T2 間の時間間隔は、トークン バケットに追加される必要があるトークンの数を決定します。これは次のように計算されます。

パケットの時間間隔（T2-T1） * CIR）/8 バイト

関連トピック

ポリシングの設定（CLI） （1631 ページ）
例：デュアルレート 3 カラー ポリシング設定 （1665 ページ）

シェーピング

シェーピングは、ダウンストリームスイッチおよびルータで輻輳が発生しないようにトラフィック レートを調整しながら、トラフィックの最大レートを強制するプロセスのことです。最も一般的な形式のシェーピングは、物理または論理インターフェイスから送信されるトラフィックを制限するために使用されます。

シェーピングにはバッファが関連付けられており、十分なトークンがないパケットがすぐにドロップされずにバッファされます。シェーピングされるトラフィックのサブセットで使用可能なバッファ数は制限され、さまざまな要因に基づいて計算されます。使用可能なバッファの数は、特定の QoS コマンドを使用して調整できます。パケットはドロップされずに、バッファが使用可能になった時点でバッファされます。

クラスベース トラフィック シェーピング

は、クラスベースのトラフィック シェーピングを使用します。このシェーピング機能は、インターフェイスに関連付けられたポリシーのクラスでイネーブルになります。シェーピングが設

定されたクラスには、トークンがないパケットを保持する複数のバッファが割り当てられます。バッファされたパケットは FIFO を使用してクラスから送信されます。最も一般的な形式の使用では、クラスベースのシェーピングを使用して、全体として物理インターフェイスまたは論理インターフェイスの最大レートを強制します。クラスでは次のシェーピング形式がサポートされます。

- 平均レート シェーピング
- 階層型シェーピング

シェーピングは、トークンバケットを使用して実行されます。CIR、B_c、B_e の値は、パケットが送信されるレートと、トークンが補充されるレートを決定します。

（注） トークンバケットアルゴリズムの詳細については、トークンバケットアルゴリズム（1564 ページ）を参照してください。

平均レート シェーピング

平均レート シェーピングを設定するには、**shape average** ポリシーマップ クラス コマンドを使用します。

このコマンドは、特定のクラスの最大帯域幅を設定します。キューの帯域幅は、ポートでさらに使用できる帯域幅があってもこの値に制限されます。では、割合またはターゲット ビット レート値でシェーピング平均を設定できます。

関連トピック

シェーピングの設定（CLI） （1643 ページ）
例：平均レート シェーピングの設定 （1660 ページ）

階層型シェーピング

シェーピングは、階層内の複数のレベルで設定することもできます。これは、シェーピングを設定した親ポリシーを作成して、追加のシェーピングを設定した子ポリシーを親ポリシーに付加することで実現できます。

次の 2 つの階層型シェーピングがサポートされています。

- ポート シェーパー
- ユーザ設定のシェーピング

ポート シェーパーでは、クラス デフォルトが使用され、親で実行できるアクションはシェーピングだけです。キュー アクションはポート シェーパーがある子で実行されます。ユーザ設定のシェーピングを使用すると、子のキューイングアクションを設定することはできません。

関連トピック

シェーピングの設定（CLI） （1643 ページ）

キューイングおよびスケジューリング

は、トラフィックの輻輳を防止するためにキューイングおよびスケジューリングを使用します。は、次のキューイングおよびスケジューリング機能をサポートします。

- 帯域幅
- 重み付けテール ドロップ
- プライオリティ キュー
- キュー バッファ

ポートにキューイング ポリシーを定義すると、制御パケットは、しきい値が最も高いベスト プライオリティ キューにマッピングされます。制御パケットのキュー マッピングは、以下の状況では異なって機能します。

- Quality of Service（QoS）ポリシーなし：QoS ポリシーが設定されていない場合、DSCP 値が 16、24、48、および 56 の制御パケットは、最も高いしきい値 threshold2 を持つキュー 0 にマッピングされます。
- ユーザ定義のポリシーあり：出力ポートに設定されているユーザ定義のキューイング ポリシーは、制御パケットのデフォルトのプライオリティ キューの設定に影響する可能性があります。

  制御トラフィックは、次のルールに基づいて最適なキューにリダイレクトされます。

  1. ユーザ ポリシーで定義されている場合、最高レベルのプライオリティ キューがベスト キューとして常に選択されます。
  2. プライオリティ キューがない場合、Cisco IOS ソフトウェアは、ベスト キューとしてキュー 0 を選択します。ソフトウェアがベスト キューとしてキュー 0 を選択した場合は、コントロール プレーン トラフィックに最適な QoS 処理を提供するために、このキューに最大帯域幅を定義する必要があります。
  3. しきい値がベスト キューで設定されていない場合、Cisco IOS ソフトウェアは、DiffServ コード ポイント（DSCP）値が 16、24、48、および 56 の制御パケットを threshold2 にマッピングされるように割り当て、ベスト キュー内の残りの制御トラフィックを threshold1 に再割り当てします。

  ポリシーが制御トラフィックに対して明示的に設定されていない場合、Cisco IOS ソフトウェアはすべての一致しない制御トラフィックを threshold2 を持つベスト キューにマッピングし、一致する制御トラフィックはポリシーで設定されたキューにマッピングされます。

（注） レイヤ 3 パケットに適切な QoS を提供するために、パケットが適切なキューに明示的に分類されていることを確認する必要があります。ソフトウェアはデフォルト キューで DSCP 値を検出すると、自動的にこのキューをベスト キューとして再割り当てします。

帯域幅

は次の帯域幅設定をサポートしています。

- 帯域幅の割合
- 帯域幅余剰比率

関連トピック

帯域幅の設定（CLI） （1628 ページ）

帯域幅の割合

特定のクラスに最小帯域幅を割り当てるには、**bandwidth percent** ポリシーマップ クラス コマンドを使用します。合計が 100 % を超えることはできず、合計が 100 % 未満である場合は、残りの帯域幅がすべての帯域幅キューで均等に分割されます。

（注） キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。

ポリシー マップで帯域幅タイプを混在させることはできません。たとえば、1 つのポリシーマップで帯域幅の割合と kbps の両方を使用して、帯域幅を設定することはできません。

帯域幅余剰比率

指定されたキューでの未使用帯域幅の共有率を作成するには、**bandwidth remaining ratio** ポリシーマップ クラス コマンドを使用します。未使用帯域幅は、これら指定されたキューにより、設定で指定されている比率で使用されます。このコマンドは、**priority** コマンドがポリシー内の特定のキューでも使用される場合に使用します。

比率を割り当てる場合には、これらの比率に従って、キューに特定の重みが割り当てられます。

比率は 0 ～ 100 の範囲で指定できます。たとえば、1 つのクラスの帯域幅余剰比率を 2 に設定し、別のクラスで帯域幅余剰比率 4 のキューを設定できます。帯域幅余剰比率 4 は、帯域幅余剰比率 2 の 2 倍の回数スケジュールされます。

ポリシーの全帯域幅の比率の割り当ては100を超えることができます。たとえば、1つのキューの帯域幅余剰比率を 50 に設定し、別のキューに帯域幅余剰比率 100 を設定できます。

重み付けテール ドロップ

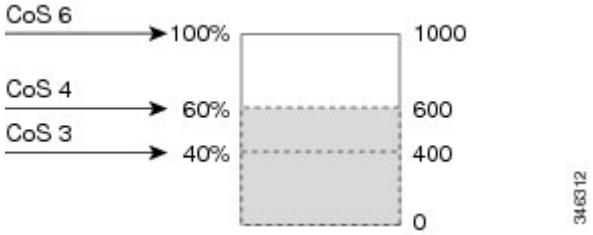
の出力キューは、重み付けテール ドロップ（WTD）と呼ばれるテール ドロップ輻輳回避メカニズムの拡張バージョンを使用します。WTD はキュー長を管理したり、トラフィック分類ごとにドロップ優先順位を設定したりするために実装されています。

フレームが特定のキューにキューイングされると、WTD はフレームに割り当てられた QoS ラベルを使用して、それぞれ異なるしきい値を適用します。この QoS ラベルのしきい値を超えると（宛先キューの空きスペースがフレーム サイズより小さくなると）、がフレームをドロップします。

各キューには 3 種類の設定可能なしきい値があります。QoS ラベルは、3 つのしきい値のうちのどれがフレームの影響を受けるかを決定します。

図 *94 : WTD* およびキューの動作

次の図は、サイズが 1000 フレームであるキューでの WTD の動作の例を示しています。ドロップ割合は次のように設定されています。40%（400 フレーム）、60%（600 フレーム）、および 100%（1000 フレーム）です。これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレーム



をキューイングできるという意味です。

例では、CoS 値 6 は他の CoS 値よりも重要度が高く、100 %のドロップしきい値（キューフルステート）に割り当てられます。CoS 値 4 は 60 % しきい値に、CoS 値 3 は 40 % しきい値に割り当てられます。これらのしきい値の割り当てはすべて、 **queue-limit cos** コマンドを使用します。

600 のフレームが格納されているキューに、新しいフレームが着信したとします。これは CoS 値 4 を使用し、60 % のしきい値が適用されます。このフレームがキューに追加されると、しきい値を超過するため、がフレームをドロップします。

関連トピック

キュー制限の設定（CLI） （1640 ページ）
例：キュー制限の設定 （1661 ページ）

重み付けテール ドロップのデフォルト値

次に、重み付けテール ドロップ（WTD）のデフォルト値と、WTD しきい値を設定するためのルールを示します。

- WTD に対して 2 つ以下のキュー制限割合を設定する場合、WTD のデフォルト値はこれらのしきい値に割り当てられます。

次に、WTD しきい値のデフォルト値を示します。

表 *93 : WTD* しきい値のデフォルト値

しきい値	デフォルト値の割合
0	80
1	90
2	400

- 異なる 3 つの WTD しきい値が設定されている場合、キューは設定どおりにプログラムされます。
- 2 つの WTD しきい値が設定されている場合、最大値の割合は 400 です。
- 1 つの WTD しきい値が x として設定されている場合、最大値の割合は 400 です。
  - x の値が 90 未満の場合、threshold1 = 90 および threshold 0= x です。
  - x の値が 90 の場合、threshold1 = 90、threshold 0 = 80 です。
  - x の値が 90 より大きい場合、threshold1 = x、threshold 0 = 80 です。

プライオリティ キュー

各ポートは 8 つの出力キューをサポートし、そのうち 2 つにプライオリティを設定できます。

2 つのクラスのプライオリティを設定するには、**priority level** ポリシー クラスマップ コマンドを使用します。1 つのクラスにプライオリティ キュー レベル 1 を設定し、別のクラスにプライオリティ キュー レベル 2 を設定する必要があります。これら 2 つのキューのパケットは、他のキューと比較して、低遅延になります。

（注） プライオリティは 1 つのレベルのみ設定できます。

1 つのポリシーマップで使用できる完全プライオリティまたはレベル付きプライオリティは 1 つだけです。kbps または割合のない同じプライオリティ レベルが設定された複数のプライオリティは、ポリシングですべてが設定された場合にのみ使用できます。

関連トピック

プライオリティの設定（CLI） （1634 ページ）

キュー バッファ

の各 1 ギガビット ポートには、ワイヤレス ポート用の 168 バッファと有線ポート用の 300 バッファが割り当てられます。各 10 ギガビット ポートには、1800 バッファが割り当てられます。ブート時に有線ポートでイネーブルになっているポリシーマップがない場合、デフォルトで作成される 2 つのキューがあります。有線ポートには、MQC ベースのポリシーを使用して最大

8 つのキューを設定できます。次の表に、どのパケットがどのキューに入っているかを示します。

表 *94 : DSCP*、*Precedence*、*CoS* : キューのしきい値のマッピング テーブル

DSCP、Precedence、CoS	キュー	しきい値
制御パケット	0	2
他のパケット	1	2

（注） バッファのアベイラビリティを保証し、ドロップしきい値を設定し、キューの最大メモリ割り当てを設定できます。キュー バッファを設定するには、**queue-buffers** ポリシーマップ クラス コマンドを使用します。最大しきい値を設定するには、**queue-limit** ポリシーマップ クラス コマンドを使用します。

バッファ割り当ては2種類あります。キューに明示的に予約される厳格なバッファと、特定のポートで未使用時に他のポートで利用可能な柔軟なバッファです。

ワイヤレス ポートのデフォルトでは、キュー0には、厳格なバッファとしてインターフェイスで利用可能なバッファの40％が割り当てられます。つまり、1ギガビット ポートにおいては、キュー 0 に対して 67 バッファが割り当てられます。このキューの柔軟な最大値は 1 ギガビット ポートに 268 （67 * 400/100 で計算）と設定されます。ここで、400 はキューに設定されたデフォルトの最大しきい値です。

有線ポートのデフォルトでは、キュー0には、厳格なバッファとしてインターフェイスで利用可能なバッファの40％が割り当てられます。つまり、1ギガビット ポートにおいては、キュー 0 に対して 120 バッファが割り当てられ、10 ギガビット ポートにおいては、720 バッファが割り当てられます。このキューの柔軟な最大値は 1 ギガビット ポートで 480（120 * 400/100 で計算）と設定され、10 ギガビット ポートで 2880 と設定されます。ここで、400 はキューに設定された最大しきい値です。

キュー1に割り当てられた厳格なバッファはありません。デフォルトの柔軟なバッファ制限は 400（最大しきい値）に設定されます。しきい値によって、共通プールから借用できる柔軟なバッファの最大数が決まります。

キュー バッファの割り当て

キューに対するバッファ割り当ては、**queue-buffers ratio** ポリシーマップ クラス コンフィギュレーション コマンドを使用して調整できます。

関連トピック

キュー バッファの設定（CLI） （1637 ページ）
例：キュー バッファの設定 （1662 ページ）

ダイナミックなしきい値および拡張

従来、予約バッファは各キューに静的に割り当てられていました。キューがアクティブかどうかにかかわらず、バッファはキューに保持されます。さらに、キューの数が増えるに従って、各キューに割り当てられた予約バッファの部分が徐々に短くなることがあります。最終的に、すべてのキューのジャンボフレームをサポートするのに十分な予約バッファがなくなる可能性があります。

は、バッファリソースを公平かつ効率的に割り当てる機能として、ダイナミックなしきい値および拡張（DTS）をサポートしています。輻輳が発生すると、このDTS機能はグローバル/ポートリソースの占有に基づいて、着信データにバッファを柔軟に割り当てます。概念上、DTSは、リソースを他のキューが使用できるように、キューバッファの割り当てを徐々に縮小します。逆も同様です。この柔軟な方法によって、バッファをより効率的かつ公平に利用できるようになります。

前の項で説明したように、キューには厳格な制限と柔軟な制限の2つの制限が設定されています。

厳格な制限はDTSの一部ではありません。これらのバッファはそのキューにだけ使用できます。厳格な制限の合計は、グローバルに設定された厳格な最大制限未満である必要があります。出力キューイング用に設定されたグローバルな厳格な制限は、現在5705に設定されています。MQCポリシーが設定されていないデフォルトのシナリオでは、24の1ギガビットポートが24 * 67 = 1608を使用し、4つの10ギガビットポートが4 * 720 = 2880を使用し、合計4488のバッファを使用して、設定に基づいてより厳格なバッファを割り当てることができます。

柔軟なバッファ制限はDTSプロセスに参加します。さらに、柔軟なバッファ割り当ての一部は、グローバルな柔軟な制限の割り当てを超えることができます。出力キューイング用のグローバルな柔軟な制限は、現在7607に設定されています。厳格な制限と柔軟な制限の合計は13312になり、3.4 MBに変換されます。柔軟なバッファ割り当ての合計がグローバルな制限を超える場合があるため、システムの負荷が軽ければ、特定のキューで多数のバッファを使用できるようになります。DTSプロセスはシステムの負荷が増大するにしたがって、キュー単位の割り当てを動的に調整します。

ワイヤレスでのキューイング

ワイヤレス コンポーネントでのキューイングはポート ポリシーに基づいて実行され、ダウンストリーム方向にだけ適用されます。ワイヤレスモジュールは次の4種類のキューをサポートします。

- 音声：これは完全プライオリティ キューです。Q0に代表されるこのキューは、制御トラフィックとマルチキャストまたはユニキャスト音声トラフィックを処理します。すべての制御トラフィック（CAPWAPパケットなど）は、音声キューを介して処理されます。QoSモジュールは、制御パケットおよび音声パケットを処理して、制御パケットが他の非制御パケットよりもプライオリティが高くなるように、音声キュー内の別のしきい値を使用します。
- ビデオ：これは完全プライオリティ キューです。Q1に代表されるこのキューは、マルチキャストまたはユニキャスト ビデオ トラフィックを処理します。

- データ NRT：Q2 に代表されるこのキューは、すべての非リアルタイム ユニキャスト トラフィックを処理します。
- マルチキャスト NRT：Q3 に代表されるこのキューは、マルチキャスト NRT トラフィックを処理します。Q0、Q1、または Q2 のトラフィックに一致しないトラフィックは、Q3 を通じて処理されます。

（注） デフォルトでは、キュー Q0 および Q1 はイネーブルになっていません。

（注） キュー Q2 および Q3 のトラフィックには、重み付けラウンド ロビン ポリシーが適用されます。

アップストリーム方向では、キューは1つだけ使用できます。ポートおよび無線ポリシーは、ダウンストリーム方向にだけ適用できます。

（注） 有線ポートでは 8 つのキューがサポートされます。

信頼動作

有線およびワイヤレス ポートの信頼動作

この信頼動作は、アップストリーム QoS とダウンストリーム QoS の両方に適用できます。

パケットはデフォルトの初期設定ごとに適切なキューに入れられます。デフォルトでは、での優先キューイングは実行されません。これは、ユニキャストおよびマルチキャストパケットに当てはまります。

次の表に、着信パケット タイプが発信パケット タイプと異なる場合の信頼動作およびキューイング動作を示します。ポートのデフォルトの信頼モードがDSCPベースであることに注意してください。信頼モードは、着信パケットが純粋なレイヤ2パケットの場合、CoS に「フォールバック」します。また、信頼設定を DSCP から CoS に変更できます。この設定変更は、「set cos cos table default default-cos」アクションのクラス デフォルトがある MQC ポリシーによって実現されます。ここで、default-cos は作成されるテーブル マップ名です（デフォルト コピーだけを実行）。

表 *95 :* 信頼およびキューイング動作

着信パケット	発信パケット	信頼動作	キューイング動作
レイヤ 3	レイヤ 3	DSCP/Precedence の保持	DSCP に基づく

着信パケット	発信パケット	信頼動作	キューイング動作
レイヤ 2	レイヤ 2	N/A	CoS に基づく
タグ付き	タグ付き	DSCP および CoS の保持	DSCP に基づく（信頼 DSCP が優先）
レイヤ 3	タグ付き	DSCP の保持、すなわち CoS が 0 に設定される	DSCP に基づく

Cisco IOS XE 3.2 リリースは、有線およびワイヤレス ポートに対して信頼できるさまざまなデフォルト設定をサポートしました。有線ポートの信頼できるデフォルト設定に関して、このソフトウェア リリースでの変更はありません。ワイヤレス ポートの場合、デフォルトのシステム動作は非信頼でした。つまり、の起動時に、ワイヤレスポートのマーキングすべてがデフォルトでゼロに設定され、トラフィックはプライオリティ処理されませんでした。既存の有線との互換性のために、すべてのトラフィックはデフォルトでベストエフォートのキューへ送信されていました。アクセス ポイントは、プライオリティ キューイングをデフォルトで実行していました。ダウンストリーム方向では、アクセス ポイントは、キューイング用に音声、ビデオ、ベスト エフォート、およびバックグラウンドのキューを保持していました。アクセスは 11e タグ情報に基づいてキューイング戦略を選択していました。デフォルトでは、アクセス ポイントはすべてのワイヤレス パケットをベスト エフォートとして処理していました。

関連トピック

ワイヤレス トラフィックの信頼動作の設定（CLI）（1620 ページ）
例：CoS マーキングを保持するテーブル マップの設定（1666 ページ）

Cisco IP Phone の信頼境界機能のポート セキュリティ

一般的なネットワークでは、ポートに Cisco IP Phone を接続し、電話の背後からデータ パケットを生成するデバイスをカスケードします。Cisco IP Phone では、音声パケット CoS レベルをハイ プライオリティ（CoS＝5）にマーキングし、データ パケットをロープライオリティ（CoS＝0）にマーキングすることで、共有データ リンクを通して音声品質を保証しています。電話からに送信されたトラフィックは通常 802.1Q ヘッダーを使用するタグでマーキングされています。ヘッダーには VLAN 情報およびパケットのプライオリティになる CoS の 3 ビット フィールドが含まれています。

ほとんどの Cisco IP Phone 設定では、電話からに送信されるトラフィックは、音声トラフィックがネットワーク内の他のタイプのトラフィックに対して適切にプライオリティ付けがされていることを保証するように信頼されています。 **trust device** インターフェイス コンフィギュレーション コマンドを使用して、電話が接続されている ポートを設定し、ポートで受信されたトラフィックを信頼するようにします。

（注） インターフェイス コンフィギュレーション モードで使用可能な **trust device** *device_type* コマンドは、デバイスでのスタンドアロン コマンドです。このコマンドを AutoQoS 設定で使用するときに、接続されているピアデバイスが対応デバイス（信頼ポリシーに一致するデバイスとして定義されているデバイス）ではない場合、CoS 値と DSCP 値の両方が「0」に設定され、いずれの入力ポリシーも有効になりません。接続されているピアデバイスが対応するデバイスである場合は、入力ポリシーが有効になります。

信頼設定により、ユーザが電話をバイパスして PC を直接に接続する場合に、ハイプライオリティ キューの誤使用を避けるのにも信頼境界機能を使用できます。信頼境界機能を使用しないと、（信頼済みの CoS 設定により）PC が生成した CoS ラベルがで信頼されてしまいます。それに対して、信頼境界機能は CDP を使用して ポートにある Cisco IP Phone（Cisco IP Phone 7910、7935、7940、7960 など）の存在を検出します。電話が検出されない場合、信頼境界機能がハイプライオリティ キューの誤使用を避けるために ポートの信頼設定をディセーブルにします。信頼境界機能は、PC および Cisco IP Phone がに接続されているハブに接続されている場合は機能しないことに注意してください。

関連トピック

デバイス タイプの信頼動作の設定

ワイヤレス QoS モビリティ

ワイヤレス QoS モビリティによって、ネットワーク内のどの場所でも同じサービスが提供されるように QoS ポリシーを設定することができます。ワイヤレス クライアントは 1 つの場所から別の場所にローミングできるため、ワイヤレスクライアントは異なるデバイスに関連付けられた異なるアクセス ポイントにクライアントを関連付けることができます。ワイヤレス クライアントのローミングは、次の 2 つのタイプに分類できます。

- デバイス内ローミング
- デバイス間ローミング

（注） クライアントのポリシーは、モビリティ グループ内のすべてのデバイスで使用できる必要があります。クライアントに一貫した操作ができるように、同じ SSID およびポート ポリシーをモビリティ グループのすべてのデバイスに適用する必要があります。

デバイス間ローミング

クライアントが 1 つの場所から別の場所にローミングすると、同じデバイス（固定デバイス）または他のデバイス（外部デバイス）に関連付けられたアクセス ポイントに関連付けることができます。デバイス間ローミングは、クライアントのローミング前に同じデバイスに関連付けられていなかったアクセス ポイントに、クライアントが関連付けられるシナリオを示しています。ホスト デバイスは、クライアントが最初に固定されていたデバイスの外部になります。

デバイス間ローミングの場合、クライアントの QoS ポリシーは、常に外部コントローラで実行されます。クライアントが固定デバイスから外部デバイスにローミングされると、QoS ポリシーは固定デバイスでアンインストールされ、外部デバイスにインストールされます。モビリティのハンドオフ メッセージでは、固定デバイスが 外部デバイスにポリシーの名前を渡します。外部デバイスには、QoS ポリシーが正しく適用できるように同じ名前のポリシーが必要です。

デバイス間ローミングの場合、QoS ポリシーはすべて、固定デバイスから外部デバイスに移動します。固定デバイスから外部デバイスへの QoS ポリシーの移行中は、外部デバイスのトラフィックがデフォルトで提供されます。これは、クライアントのターゲットの新しいポリシーインストールに似ています。

（注） 外部デバイスがユーザ定義の物理ポート ポリシーを使用して設定されていない場合、デフォルト ポート ポリシーは RT1 キューを通過する制御トラフィックを除き、NRT キューを介してルーティングされるすべてのトラフィックに適用されます。ネットワーク管理者は、固定および未知のデバイスで同じ物理ポートのポリシーを対称的に設定する必要があります。

デバイス間ローミングでは、クライアントが外部のデバイスに関連付けられている一定の期間だけ、クライアントおよび SSID ポリシー統計情報が収集されます。ローミング全体（固定デバイスおよび外部デバイス）の累積統計情報は収集されません。

デバイス内ローミング

デバイス内ローミングでは、クライアントのローミング前に同じデバイスに関連付けられていたアクセスポイントに、クライアントが関連付けられます。ただしこのデバイスとの関連付けは、別のアクセス ポイントを通じて行われます。

（注） デバイス内ローミングの場合、QoS ポリシーはそのまま残ります。

ワイヤレス QoS の貴金属ポリシー

ワイヤレス QoS はユニファイド ワイヤレス コントローラ プラットフォームによって提供される貴金属ポリシーと下位互換性があります。貴金属ポリシーは、コントローラで使用可能なシステム定義のポリシーです。

次のポリシーを使用できます。

- プラチナ：VoIP クライアントに使用されます。
- ゴールド：ビデオ クライアントに使用されます。
- シルバー：ベスト エフォートであると考えられるトラフィックに使用されます。
- ブロンズ：NRT トラフィックに使用されます。

これらのポリシー（別名プロファイル）は、トラフィックに基づいてWLANに適用できます。Cisco IOS MQC 設定を使用した設定を推奨します。ポリシーは、必要な貴金属ポリシーに基づくシステムで利用可能です。SSID の入力および出力ポリシーに対してのみ貴金属ポリシーを設定できます。

適用されたポリシーに基づいて、パケット内の802.1p、802.11e（WMM）、およびDSCPフィールドが影響を受けます。これらの値は事前設定されており、デバイスの起動時にインストールされます。

（注） Cisco Unified Wireless Controller に適用できる貴金属ポリシーと異なり、属性 rt-average-rate、nrt-average-rate、および最大レートは、このデバイス プラットフォームに設定された貴金属ポリシーには適用できません。

関連トピック

貴金属ポリシーの設定（CLI） （1644 ページ）

標準 QoS のデフォルト設定

デフォルトの有線 QoS 設定

の各有線インターフェイスでは、デフォルトで2つのキューが設定されます。すべての制御トラフィックはキュー0を通過し、処理されます。その他すべてのトラフィックはキュー1を通過し、処理されます。

DSCP マップ

デフォルトの *CoS/DSCP* マップ

CoS/DSCP マップを使用して、着信パケットの CoS 値を、QoS がトラフィックのプライオリティを表すために内部使用するDSCP値にマッピングします。次の表に、デフォルトのCoS/DSCPマップを示します。これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 *96*：デフォルトの *CoS/DSCP* マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40

CoS 値	DSCP 値
6	48
7	56

デフォルトの *IP Precedence/DSCP* マップ

着信パケットの IP precedence 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングするには、IP precedence/DSCP マップを使用します。次の表は、デフォルトの IP Precedence/DSCP マップを示しています。これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 *97* : デフォルトの *IP Precedence/DSCP* マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

デフォルトの *DSCP/CoS* マップ

4 つの出力キューのうち 1 つを選択するために使用される CoS 値を生成するには、DSCP/CoS マップを使用します。次の表に、デフォルトの DSCP/CoS マップを示します。これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 *98* : デフォルトの *DSCP/CoS* マップ

DSCP 値	CoS 値
0 ～ 7	0
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4

DSCP 値	CoS 値
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

デフォルトのワイヤレス QoS 設定

スイッチ ポートでは、有線またはワイヤレスの物理ポートは区別されません。ポリシーは、スイッチに関連付けられたデバイスの種類に応じて適用されます。たとえば、アクセスポイントがスイッチ ポートに接続されている場合、スイッチはアクセス ポイントをワイヤレス デバイスとして検出し、親子ポリシー形式のデフォルトの階層型ポリシーを適用します。このポリシーは、階層型ポリシーです。親ポリシーは変更できませんが、子ポリシー（port-child ポリシー）は、QoS 設定に合わせて変更できます。スイッチは、デフォルトのクラス マップとポリシー マップで事前に設定されます。

QoS ポリシーのガイドライン

不正な形式の QoS ポリシーによりクライアントが除外されるのを防ぐには、次のガイドラインに従います。

- 新しい QoS ポリシーをデバイスに追加する場合、同じ名前の QoS ポリシーは、同じローミングまたはモビリティ ドメイン内の他のデバイスに追加する必要があります。
- デバイスに新しいリリースのソフトウェアイメージがロードされると、新しいポリシー形式がサポートされます。以前のリリースから新しいリリースにソフトウェア イメージをアップグレードした場合は、設定を別々に保存する必要があります。以前のリリースのイメージがロードされると、一部の QoS ポリシーがサポートされていないと表示される場合があり、それらの QoS ポリシーをサポートされるポリシー形式に復元する必要があります。

有線ターゲットの QoS に関する制約事項

ターゲットとは、ポリシーが適用されるエンティティです。有線またはワイヤレスターゲットにポリシーを適用できます。有線ターゲットには、ポートまたは VLAN を指定できます。ワイヤレス ターゲットには、ポート、無線、SSID、またはクライアントを設定できます。ユーザは、ポート、SSID、およびクライアント ポリシーだけを設定できます。ユーザは、無線ポリシングを設定できません。ポート、無線、SSID、クライアントの QoS ポリシーはダウンストリーム方向に適用されます。アップストリーム方向では、SSIDおよびクライアントターゲットだけがサポートされます。ダウンストリームは、トラフィックがデバイスからワイヤレスクライアントに流れていることを示します。アップストリームは、トラフィックがワイヤレスクライアントからデバイスに流れていることを示します。

次に、QoS 機能を有線ターゲットのデバイスに適用する場合の制限事項を示します。

- 有線ターゲットのデバイス ポートでは、最大 8 つのキューイング クラスがサポートされます。
- 有線ターゲットの有線ポートでは、ポリシーごとに最大 63 のポリサーがサポートされます。
- Cisco IOS XE Release 3.7.5E 以降のリリースでは、ダウンリンク ポートのサイズは 10 GB ですが、デフォルトでは、すべてのダウンリンク ポートに 1 GB のポート バッファが割り当てられます。この変更の前は、すべての 1 GB ダウンリンク ポートには 1 GB バッファが、10 GB ダウンリンク ポートには 10 GB バッファが割り当てられていました。
- QoS 階層でサポートされるのは最大 2 レベルです。
- 階層型ポリシーでは、子ポリシーの親およびキュー機能のポリシーにポート シェーパーがある場合を除き、親子間のオーバーラップは許可されていません。
- QoS ポリシーは、EtherChannel インターフェイスに付加できません。
- 親と子の両方のポリシングは、QoS 階層ではサポートされていません。
- 親と子の両方のマーキングは、QoS 階層ではサポートされていません。
- 同じポリシーでのキュー制限とキュー バッファの混在はサポートされません。

（注） キュー制限の割合は、**queue-buffer** コマンドがこの機能を処理するため、デバイスではサポートされていません。キュー制限は、DSCP および CoS 拡張でのみサポートされます。

- シェーピングでは、ハードウェア内部に占める 20 バイトの IPG オーバーヘッドがすべてのパケットにあります。シェーピングの精度はこれにより向上し、とくに小さいサイズのパケットに対して効果があります。
- すべての有線キューイングベース ポリシーの分類シーケンスはすべての有線アップストリーム ポート（10 ギガビット イーサネット）で同じであり、すべてのダウンストリーム有線ポート（1 ギガビット イーサネット）で同じです。
- 空のクラスはサポートされません。
- 空のアクションによるクラス マップはサポートされません。クラス マップの順序が同じポリシーが 2 つあり、どちらかのポリシーにアクションが含まれていないクラスマップがある場合、トラフィックのドロップが起こる可能性があります。回避策として、PRIORITY_QUEUE 内のすべてのクラスに最小帯域幅を割り当てます。
- 有線ターゲットの有線ポートでは、ポリシーごとに最大 256 のクラスがサポートされます。
- ポリシー マップ内のポリサーのアクションには、次の制限事項があります。
  - 適合アクションは送信する必要があります。

  - マークダウン タイプの超過/違反アクションは、cos2cos、prec2prec、dscp2dscp だけです。
  - マークダウン タイプはポリシー内で同じである必要があります。

- ポート レベルの入力マーキング ポリシーは SVI ポリシーより優先されますが、ポート ポリシーが設定されていない場合は、SVI ポリシーが優先されます。優先するポート ポリシーに対し、ポート レベルのポリシーを定義します。SVI ポリシーが上書きされるようにするためです。
- 分類カウンタには、次の制限事項があります。
  - 分類カウンタは、バイトの代わりにパケットをカウントします。
  - フィルタ ベースの分類カウンタはサポートされません。
  - マーキングまたはポリシングによる QoS 設定だけが、分類カウンタをトリガーします。
  - 分類カウンタはポートベースではありません。これは、分類カウンタが、異なるインターフェイスに接続し、同じポリシーの同じクラスに属するすべてのパケットを集約することを意味します。
  - ポリシー内にポリシングまたはマーキング アクションがある限り、クラス デフォルトは分類カウンタを保持します。
  - クラスに複数の match ステートメントがある場合、分類カウンタは match ステートメントの 1 つにだけトラフィック カウンタを表示します。
- テーブル マップには次の制限事項があります。
  - マークダウンを超過するポリシングのテーブルマップとマークダウンに違反するポリシングのテーブルマップがサポートされるのは、方向およびターゲットごとに1つのみです。
  - テーブル マップは class-default で設定する必要があります。テーブル マップはユーザ定義クラスに対してサポートされません。
- 階層型ポリシーは次の機能で必要になります。
  - ポート シェーパー
  - 集約ポリシング機能
  - PV ポリシー
  - 親シェーピングおよび子マーキング/ポリシング
- 有線ターゲットを含むポートでは、次の階層型ポリシーだけがサポートされています。
  - ワイヤレス クライアントの場合を除き、同じポリシー内でのポリシングの連結はサポートされていません。

- 同じポリシー内で階層型キューはサポートされていません（ポート シェーパーは例外）。
- 親クラスでは、すべてのフィルタが同じタイプでなければなりません。子フィルタ タイプは次の例外を除き、親フィルタのタイプと一致している必要があります。
  - IP に一致するように親クラスが設定されている場合、ACL に一致するように子クラスを設定できます。
  - CoS に一致するように親クラスが設定されている場合、ACL に一致するように子クラスを設定できます。

- インターフェイス コンフィギュレーション モードで使用可能な **trust device** *device_type* コマンドは、デバイスでのスタンドアロン コマンドです。このコマンドを AutoQoS 設定で使用するときに、接続されているピア デバイスが対応デバイス（信頼ポリシーに一致するデバイスとして定義されているデバイス）ではない場合、CoS 値と DSCP 値の両方が「0」に設定され、いずれの入力ポリシーも有効になりません。接続されているピア デバイスが対応するデバイスである場合は、入力ポリシーが有効になります。

次に、VLAN の QoS 機能を有線ターゲットに適用する場合の制限事項を示します。

- フラットつまり非階層型ポリシーでは、マーキングまたはテーブルマップのみサポートされます。

次に、EtherChannel とチャネル メンバー インターフェイスで QoS 機能を適用するための制限事項と考慮事項を示します。

- QoS は、EtherChannel インターフェイスではサポートされません。
- QoS は、入力および出力方向の EtherChannel メンバーインターフェイスでサポートされます。すべての EtherChannel メンバーが同じ QoS ポリシーを適用する必要があります。QoS ポリシーが同じでない場合、異なるリンクの個々のポリシーは独立して機能します。
- チャネル メンバーへサービス ポリシーを付加すると、EtherChannel 内のすべてのポートに同じポリシーが接続されていることを確認するようユーザに知らせる、次の警告メッセージが表示されます。「Warning: add service policy will cause inconsistency with port xxx in ether channel xxx.」
- 自動 QoS は EtherChannel メンバーではサポートされません。

（注） EtherChannel へサービス ポリシーを付加すると、次のメッセージがコンソールに表示されます。「Warning: add service policy will cause inconsistency with port xxx in ether channel xxx.」。この警告メッセージは予期されるメッセージです。この警告メッセージは、同じ EtherChannel 内の他のポートに同じポリシーを付加するように促すものです。同じメッセージがブートアップ中にも表示されます。このメッセージは、EtherChannel メンバー ポート間に不一致があることを意味するものではありません。

関連トピック

ワイヤレス ターゲットの QoS に関する制約事項 （1587 ページ）
QoS の前提条件 （1539 ページ）
QoS の概要 （1541 ページ）
QoS の実装 （1553 ページ）

ワイヤレス ターゲットの QoS に関する制約事項

一般的な制約事項

ターゲットとは、ポリシーが適用されるエンティティです。有線またはワイヤレスターゲットにポリシーを適用できます。有線ターゲットには、ポートまたは VLAN を指定できます。ワイヤレス ターゲットには、ポート、無線、SSID、またはクライアントを設定できます。ユーザは、ポート、SSID、およびクライアント ポリシーだけを設定できます。ユーザは、無線ポリシングを設定できません。ポート、無線、SSID、クライアントの QoS ポリシーはダウンストリーム方向に適用されます。アップストリーム方向では、SSIDおよびクライアントターゲットだけがサポートされます。ダウンストリームは、トラフィックがデバイスからワイヤレスクライアントに流れていることを示します。アップストリームは、トラフィックがワイヤレスクライアントからデバイスに流れていることを示します。

- ポート、SSID、および（AAA および Cisco IOS コマンドライン インターフェイスを使用する）クライアント ポリシーのみがユーザ設定可能です。無線ポリシーはワイヤレス制御モジュールで設定されるため、ユーザ設定できません。
- ポートおよび無線ポリシーは、出力方向にのみ適用できます。
- SSID およびクライアント ターゲットには、マーキングおよびポリシング ポリシーのみを設定できます。
- 方向単位ターゲットあたり 1 つのポリシーがサポートされています。
- 出力 class-default SSID ポリシーの場合、平均シェーピング レートを設定した後にキューバッファの割合を 0 に設定する必要があります。
- ポリシー マップのクラス マップには、さまざまなタイプのフィルタを指定できます。ただし、出力方向のマップでサポートされるマーキング アクション（table map、set dscp、または set cos）は 1 つのみです。
- 階層的なクライアントと SSID の入力ポリシーの場合は、親と子ポリシーの両方ともマーキングを設定できません。親ポリシーまたは子ポリシーのいずれかでマーキングを設定できます。
- 同じクラスでの複数の set アクションの設定はできません。
- SSID およびクライアントの入力ポリシーの場合、set アクションは DSCP 値と CoS 値に対してのみサポートされています。
- WLAN グループや QoS ポリシーは削除できません。

ポートのワイヤレス QoS の制約事項

ワイヤレス ポート ターゲットに QoS 機能を適用する場合には、次の制約事項があります。

- すべてのワイヤレス ポートには、1 つのクラス デフォルトとその下に 1 つのアクション シェーピングを持つ同様の親ポリシーが設定されています。シェーピング レートは 802.11a/b/g/ac バンドに依存します。
- `port_chlid_policy` を変更することにより、子ポリシーで最大 4 個のクラスを作成できます。
- ポート レベルの `port_child_policy` に 4 つのクラスがある場合、1 つは non-client-nrt クラス、もう 1 つは class-default である必要があります。
- 2 つのクラスに同じプライオリティ レベルを設定することはできません。プライオリティ レベル 1（音声トラフィックと制御トラフィック用）および 2（ビデオ用）のみがサポートされます。
- マルチキャスト NRT クラス（non-client-nrt クラス）と `class-default` では、プライオリティはサポートされません。
- 4 つのクラスが設定されている場合、いずれか 2 つがプライオリティ クラスでなければなりません。3 つのクラスのみが設定されている場合、少なくとも 1 つがプライオリティ クラスでなければなりません。3 つのクラスが設定されていて、non-client-nrt クラスがない場合、両方のプライオリティ レベルが必要です。
- 一致する DSCP のみサポートされます。
- ワイヤレス制御モジュールによって適用されるポート ポリシーは、CLI を使用して削除することはできません。
- 同じクラスのプライオリティ レートとポリシング CIR（MQC を使用）はサポートされていません。
- キュー制限（重み付けテール ドロップを設定するために使用）はサポートされていません。

SSID に対するワイヤレス QoS の制約事項

次に、SSID で QoS 機能を適用するときの制約事項を示します。

- 入力ポリシーでは 1 つのテーブル マップがサポートされます。
- テーブル マップは、親 class-default でのみサポートされます。最大 2 つのテーブル マップが出力方向でサポートされ、QoS グループが関係する場合、3 つのテーブル マップを設定できます。

（注） テーブル マップは、クライアント ターゲットではサポートされません。

- ワイヤレス ポートのデフォルト ポリシーにキューが 2 つ（マルチキャスト NRT 用に 1 つ、class-default 用に 1 つ）しかない場合、SSID レベルのポリシーは出力方向の音声およびビデオ クラスを設定できません。
- プライオリティのないポリシングは出力方向でサポートされません。
- SSID レベルのプライオリティ設定は、RT1 および RT2 ポリサー（ポリサー用 AFD）を設定する目的でのみ使用されます。プライオリティの設定にシェーピング レートは含まれません。そのため、プライオリティはポリシングのない SSID ポリシーに対して制限されます。
- **set** が class-default で有効にされていない場合、音声やビデオの SSID 分類は、ポート レベルで音声またはビデオ クラスの分類の一部である必要があります。
- DSCP2DSCP および COS2COS テーブルでのマッピングは、ポート レベル ポリシーの音声およびビデオ クラスの分類機能に基づいている必要があります。
- 子ポリシーの class-default ではアクションは許可されません。
- SSID の入力ポリシーでは、UP および DSCP フィルタ（一致基準）のみがサポートされます。ACL およびプロトコルの一致基準はサポートされません。
- 入力方向のフラット ポリシー（非階層型）では、ポリシー設定はセット（テーブル マップ）、ポリシング、またはその両方である必要があります。

クライアントのワイヤレス QoS の制約事項

次は、クライアント ターゲットでの QoS ポリシーの適用に関する制約事項です。

- デフォルトのクライアント ポリシーは、ACM イネーブルの WMM クライアント上でのみイネーブルにされます。
- キューイングはサポートされていません。
- イネーブル状態の WLAN では、クライアント ポリシーの付加、削除また変更はサポートされません。ポリシーを適用、削除、または変更するには、WLAN をシャットダウンする必要があります。
- テーブル マップ設定は、ターゲット クライアントでサポートされていません。
- class-default で一緒に設定されたポリシングとセットは、出力方向でブロックされます。

```
policy-map foo
class class-default
police X
set dscp Y
```

- 親ポリシーが他のユーザ定義クラス マップを含む場合、子ポリシーは class-default でサポートされません。
- フラットな出力クライアント ポリシーでは、class-default 内のポリシングおよび他のクラス内のマーキング アクションはサポートされません。

- クライアント ポリシーでは、セット マーキング アクションのみがサポートされます。
- クライアント入力ポリシーでは、ACL、Up、DSCP、およびプロトコル フィルタ（一致基準）のみがサポートされます。
- クライアント ポリシーのポリシー マップ クラスのフィルタすべてに、同じ属性が必要です。IPv4 または IPv6 アドレスなどのプロトコル固有の属性で一致するフィルタは、異なる属性セットと見なされます。
- ACL で一致するフィルタでは、アクセス リストのすべての ACE（アクセス コントロール エントリ）に同じ種類と同じ数の属性が必要です。
- クライアント出力ポリシーでは、マーキング属性で一致するフィルタにおいて、policy-map 内のすべてのフィルタが同じマーキング属性で一致する必要があります。たとえば、フィルタが DSCP で一致する場合、ポリシー内のすべてのフィルタが DSCP で一致する必要があります。
- ポート範囲で一致する ACL とサブネットは、入力方向でのみサポートされます。

関連トピック

ポート ポリシー （1547 ページ）
ポート ポリシーの形式 （1547 ページ）
無線ポリシー （1549 ページ）
有線ターゲットの QoS に関する制約事項 （1583 ページ）
QoS の前提条件 （1539 ページ）
QoS の概要 （1541 ページ）
QoS の実装 （1553 ページ）

QoS の設定方法

クラス、ポリシー、およびテーブル マップの設定

トラフィック クラスの作成（CLI）

一致基準が含まれるトラフィック クラスを作成するには、**class-map** コマンドを使用してトラフィック クラス名を指定し、必要に応じて、**match** コマンドをクラスマップ コンフィギュレーション モードで使用します。

始める前に

この設定作業で指定するすべての match コマンドの使用は任意ですが、1 つのクラスに少なくとも 1 つの一致基準を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**class-map** {*class-map name* | **match-any**}
	例：
	`Device(config)# class-map test_1000`
	`Device(config-cmap)#`
		クラスマップ コンフィギュレーション モードを開始します。
		• 名前を指定したクラスとパケットとの照合に使用されるクラスマップを作成します。
		• **match-any** を指定すると、トラフィック クラスで受信したトラフィックがトラフィック クラスの一部と分類されるには、一致基準の 1 つを満たす必要があります。これはデフォルトです。

ステップ 3	**matchaccess-group** {*index numbername*} |
	例：
	`Device(config-cmap)# match access-group 100`
	`Device(config-cmap)#`
		このコマンドでは次のパラメータを使用できます。
		• access-group
		• class-map
		• cos
		• dscp
		• ip
		• non-client-nrt
		• precedence
		• qos-group
		• vlan
		• wlan user priority
		（任意）この例では、アクセス グループ ID を入力します。
		• アクセス リスト インデックス（1 ～ 2799 の値）
		• 名前付きアクセス リスト

	コマンドまたはアクション	目的

ステップ 4	**matchclass-map** *class-map name*
	例：
	`Device(config-cmap)# match class-map test_2000`
	`Device(config-cmap)#`
		（任意）別のクラスマップ名に一致します。

ステップ 5	**match cos** *cos value*
	例：
	`Device(config-cmap)# match cos 2 3 4 5`
	`Device(config-cmap)#`
		（任意）IEEE 802.1Q または ISL サービスクラス（ユーザ）プライオリティ値に一致します。
		• 最大 4 つの CoS 値（0 ～ 7）をスペースで区切って入力します。

ステップ 6	**match dscp** *dscp value*
	例：
	`Device(config-cmap)# match dscp af11 af12`
	`Device(config-cmap)#`
		（任意）IPv4 および IPv6 パケットの DSCP 値に一致します。

ステップ 7	**matchip** {**dscp** *dscp value* | **precedence** *precedence value*}
	例：
	`Device(config-cmap)# match ip dscp af11 af12`
	`Device(config-cmap)#`
		（任意）次を含む IP 値に一致します。
		• **dscp**：IP DSCP（DiffServ コードポイント）に一致します。
		• **precedence**：IP precedence（0 ～ 7）に一致します。

ステップ 8	**matchnon-client-nrt**
	例：
	`Device(config-cmap)# match non-client-nrt`
	`Device(config-cmap)#`
		（任意）非クライアントの NRT（非リアルタイム）に一致します。
		（注） この一致は、ワイヤレスポートのポリシーにのみ適用できます。これは、すべての複数の宛先および AP（非クライアント）宛のトラフィックを伝送します。

ステップ 9	**matchqos-group** *qos group value* 例： `Device(config-cmap)# match qos-group 10`	（任意）QoS グループ値（0 ～ 31）に一致します。

	コマンドまたはアクション	目的
	`Device(config-cmap)#`	

ステップ 10	**matchvlan** *vlan value*
	例：
	`Device(config-cmap)# match vlan 210`
	`Device(config-cmap)#`
		（任意）VLAN ID（1 ～ 4095）に一致します。

ステップ 11	**matchwlan user-priority** *wlan value*
	例：
	`Device(config-cmap)# match wlan user priority 7`
	`Device(config-cmap)#`
		（任意）802.11eに固有の値に一致します。ユーザプライオリティ802.11eユーザ プライオリティ（0 ～ 7）を入力します。

ステップ 12	**end** 例： `Device(config-cmap)# end`	設定の変更内容を保存します。

次のタスク

ポリシー マップを設定します。

関連トピック

クラス マップ （1560 ページ）
例：アクセス コントロール リストによる分類 （1650 ページ）

トラフィック ポリシーの作成（CLI）

トラフィック ポリシーを作成するには、**policy-map** グローバル コンフィギュレーション コマンドを使用して、トラフィック ポリシーの名前を指定します。

トラフィック クラスは、**class** コマンドを使用したときにサービス ポリシーと関連付けられます。**class** コマンドは、ポリシー マップ コンフィギュレーション モードを開始した後に実行する必要があります。**class** コマンドを入力すると、が自動的にポリシー マップ クラス コンフィギュレーション モードを開始します。ここでトラフィック ポリシーの QoS ポリシーを定義します。

次のポリシー マップ クラスのアクションがサポートされます。

- admit：コール アドミッション制御（CAC）の要求を許可します。
- bandwidth：帯域幅設定オプション。

- exit：QoS クラス アクション コンフィギュレーション モードを終了します。
- no：コマンドのデフォルト値を無効にするか、設定します。
- police：ポリシング機能の設定オプション。
- priority：このクラスの完全スケジューリング プライオリティの設定オプション。
- queue-buffers：キューのバッファ設定オプション。
- queue-limit：重み付けテール ドロップ（WTD）設定オプションのキューの最大しきい値。
- service-policy：QoS サービス ポリシーを設定します。
- set：次のオプションを使用して QoS 値を設定します。
  - CoS 値
  - DSCP 値
  - precedence 値
  - QoS グループ値
  - WLAN 値
- shape：トラフィック シェーピング設定オプション。

始める前に

最初にクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**policy-map** *policy-map name*
	例：
	`Device(config)# policy-map test_2000`
	`Device(config-pmap)#`
		ポリシーマップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。

ステップ 3	**class** {*class-name* | **class-default**} 例：	ポリシーを作成または変更するクラスの名前を指定します。

	コマンドまたはアクション	目的
	`Device(config-pmap)# class test_1000` `Device(config-pmap-c)#`	未分類のパケットのシステムデフォルト クラスも作成できます。

ステップ 4	**admit**
	例：
	`Device(config-pmap-c)# admit cac wmm-tspec`
	`Device(config-pmap-c)#`
		（任意）コール アドミッション制御（CAC）の要求を許可します。このコマンドおよび使用の詳細な例については、コールアドミッション制御の設定（CLI）（1621 ページ）を参照してください。
		（注） このコマンドは、ワイヤレス QoS の CAC だけを設定します。

ステップ 5	**bandwidth** {**kb/s** *kb/s value* | **percent** *percentage* | **remaining** {*percent* | *ratio*}}
	例：
	`Device(config-pmap-c)# bandwidth 50`
	`Device(config-pmap-c)#`
		（任意）次のいずれかを使用して帯域幅を設定します。
		• **kb/s**：kpbs に 20000 ～ 10000000 の値を入力します。
		• **percent**：このポリシーマップに使用される総帯域幅の割合を入力します。
		• **remaining**：残りの帯域幅の割合を入力します。
		このコマンドおよび使用の詳細な例については、帯域幅の設定（CLI）（1628 ページ）を参照してください。

ステップ 6	**exit**
	例：
	`Device(config-pmap-c)# exit`
	`Device(config-pmap-c)#`
		（任意）QoS クラス アクション コンフィギュレーション モードを終了します。

ステップ 7	**no**
	例：
	`Device(config-pmap-c)# no`
	`Device(config-pmap-c)#`
		（任意）コマンドを無効にします。

ステップ 8	**police** {*target_bit_rate* | **cir** | **rate**} 例：	（任意）ポリサーを設定します。

	コマンドまたはアクション	目的
	`Device(config-pmap-c)# police 100000` `Device(config-pmap-c)#`	• *target_bit_rate*：ビット レート/秒を入力します。8000 ～ 10000000000 の値を入力します。 • **cir**：認定情報レート。 • **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングル レベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。 このコマンドおよび使用の詳細な例については、ポリシングの設定（CLI）（1631 ページ）を参照してください。

ステップ 9	**priority** {*kb/s level value percentage value* | **level** | **percent**}
	例：
	`Device(config-pmap-c)# priority percent 50`
	`Device(config-pmap-c)#`
		（任意）このクラスに完全スケジューリングプライオリティを設定します。コマンド オプションは次のとおりです。
		• *kb/s*：kbps に 1 ～ 2000000 の値を入力します。
		• **level**：マルチレベル プライオリティ キューを確立します。値を入力します（1 または 2）。
		• **percent**：このプライオリティの全帯域幅の割合を入力します。
		
		このコマンドおよび使用の詳細な例については、プライオリティの設定（CLI）（1634 ページ）を参照してください。

ステップ 10	**queue-buffers ratio** *ratio limit*
	例：
	`Device(config-pmap-c)# queue-buffers ratio 10`
	`Device(config-pmap-c)#`
		（任意）クラスのキューバッファを設定します。キューバッファの割合制限（0 ～ 100）を入力します。
		このコマンドおよび使用の詳細な例については、キュー バッファの設定（CLI）（1637 ページ）を参照してください。

ステップ 11	**queue-limit** {パケット | **cos** | **dscp** | **percent**} 例：	（任意）テール ドロップに対してキューの最大しきい値を指定します。

	コマンドまたはアクション	目的
	`Device(config-pmap-c)# queue-limit cos 7 percent 50` `Device(config-pmap-c)#`	• *packets*：デフォルトのパケット数。1 ～ 2000000 の間の値を入力します。 • **cos**：各 CoS 値のパラメータを入力します。 • **dscp**：各 DSCP 値のパラメータを入力します。 • **percent**：しきい値の割合を入力します。 このコマンドおよび使用の詳細な例については、キュー制限の設定（CLI）（1640 ページ）を参照してください。

ステップ 12	**service-policy** *policy-map name*
	例：
	`Device(config-pmap-c)# service-policy test_2000`
	`Device(config-pmap-c)#`
		（任意）QoS サービス ポリシーを設定します。

ステップ 13	**set** {**cos** | **dscp** | **ip** | **precedence** | **qos-group** | **wlan**}
	例：
	`Device(config-pmap-c)# set cos 7`
	`Device(config-pmap-c)#`
		（任意）QoS 値を設定します。使用可能な QoS 設定値は次のとおりです。
		• **cos**：IEEE 802.1Q/ISL サービス クラスまたはユーザ プライオリティを設定します。
		• **dscp**：IP（v4）および IPv6 パケットの DSCP を設定します。
		• **ip**：IP 固有の値を設定します。
		• **precedence**：IP（v4）および IPv6 パケットの precedence を設定します。
		• **qos-group**：QoS グループを設定します。
		• **wlan**：WLAN ユーザ プライオリティを設定します。

	コマンドまたはアクション	目的

ステップ 14	**shape average** {*target_bit_rate* | **percent**}
	例：
	`Device(config-pmap-c) #shape average percent 50`
	`Device(config-pmap-c) #`
		（任意）トラフィック シェーピングを設定します。コマンドパラメータは次のとおりです。
		• *target_bit_rate*：ターゲット ビット レート。
		• **percent**：認定情報レートのインターフェイス帯域幅の割合。
		このコマンドおよび使用の詳細な例については、シェーピングの設定（CLI）（1643 ページ）を参照してください。

ステップ 15	**end**
	例：
	`Device(config-pmap-c) #end`
	`Device(config-pmap-c) #`
		設定の変更内容を保存します。

次のタスク

インターフェイスを設定します。

関連トピック

ポリシー マップ （1561 ページ）

クライアント ポリシーの設定

次のいずれかの方法を使用して、クライアント ポリシーを設定できます。

方式	トピック/詳細
デフォルト クライアント ポリシー	アドミッション制御（ACM）が WMM クライアントに対してイネーブルの場合、のワイヤレス制御モジュールは、デフォルト クライアント ポリシーを適用します。ACM がディセーブルの場合、デフォルト クライアント ポリシーはありません。 デフォルト ポリシーは次のとおりです。 • 入力：cldeffromWMM • 出力：cldeftoWMM **show ap dot11** {**5ghz** | **24ghz**} コマンドを使用して、ACM がイネーブルにされているかどうかの確認が出来ます。ACM をイネーブルにするには、**ap dot11** {**5ghz** | **24ghz**} **cac voice acm** コマンドを使用します。
CLI を使用して WLAN にクライアント ポリシーを適用します。	WLAN での SSID またはクライアント ポリシーの適用（CLI）（1608 ページ）
CLI によるローカル プロファイリング ポリシーを使用して Qos 属性ポリシーを適用します。	WLAN 上のデバイスのローカル ポリシーの適用（CLI）（1288 ページ）
AAA サーバ（ACS/ISE）によりポリシー マップを適用します	『*Cisco Identity Services Engine User Guide*』 『*Cisco Secure Access Control System User Guide*』

クラスベースのパケット マーキングの設定（CLI）

この手順は、次のクラスベースパケット マーキング機能をで設定する方法を示します。

- CoS 値
- DSCP の値
- IP 値
- precedence 値
- QoS グループ値
- WLAN 値

始める前に

この手順を開始する前にクラス マップとポリシー マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**policy-map** *policy name*
	例：
	`Device(config)# policy-map policy1`
	`Device(config-pmap)#`
		ポリシーマップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。

ステップ 3	**class** *class name*
	例：
	`Device(config-pmap)# class class1`
	`Device(config-pmap-c)#`
		ポリシー クラス マップ コンフィギュレーションモードを開始します。ポリシーを作成または変更するクラスの名前を指定します。
		ポリシー クラス マップ コンフィギュレーションモードには、次のコマンドオプションが含まれます。
		• **admit**：コール アドミッション制御（CAC）の要求を許可します。
		• **bandwidth**：帯域幅設定オプション。
		• **exit**：QoS クラス アクション コンフィギュレーションモードを終了します。
		• **no**：コマンドのデフォルト値を無効にするか、設定します。
		• **police**：ポリシング機能の設定オプション。
		• **priority**：このクラスの完全スケジューリングプライオリティの設定オプション。

	コマンドまたはアクション	目的

		• **queue-buffers**：キューのバッファ設定オプション。
		• **queue-limit**：重み付けテール ドロップ（WTD）設定オプションのキューの最大しきい値。
		• **service-policy**：QoS サービス ポリシーを設定します。
		• **set**：次のオプションを使用して QoS 値を設定します。
		  • CoS 値
		  • DSCP 値
		  • precedence 値
		  • QoS グループ値
		  • WLAN 値
		• **shape**：トラフィック シェーピング設定オプション。
		（注） この手順では、**set** コマンド オプションを使用して、使用可能な設定について説明します。その他のコマンド オプション（**admit**、**bandwidth** など）についてはこのマニュアルの他の項で説明します。このタスクでは、使用可能なすべての **set** コマンドが表示されますが、クラス単位でサポートされるのは 1 つの **set** コマンドだけです。

ステップ 4	**set cos** {*cos value* | **cos table** *table-map name* | **dscp table** *table-map name* | **precedence table** *table-map name* | **qos-group table** *table-map name* | **wlan user-priority table** *table-map name*} 例： `Device(config-pmap)# set cos 5`	（任意）発信パケットの固有の IEEE 802.1Q レイヤ 2 CoS 値を設定します。値は 0 ～ 7 です。 **set cos** コマンドを使用して次の値を設定することもできます。 • **cos table**：CoS 値をテーブル マップに基づいて設定します。

	コマンドまたはアクション	目的
	`Device(config-pmap)#`	• **dscp table**：コード ポイント値をテーブルマップに基づいて設定します。 • **precedence table**：コードポイント値をテーブルマップに基づいて設定します。 • **qos-group table**：テーブル マップに基づいて QoS グループから CoS 値を設定します。 • **wlan user-priority table**：テーブルマップに基づいて WLAN ユーザ プライオリティから CoS 値を設定します。

ステップ 5	**set dscp** {*dscp value* | **default** | **dscp table** *table-map name* | **ef** | **precedence table** *table-map name* | **qos-group table** *table-map name* | **wlan user-priority table** *table-map name*}
	例：
	`Device(config-pmap)# set dscp af11`
	`Device(config-pmap)#`
		（任意）DSCP 値を設定します。
		特定の DSCP 値の設定に加えて、**set dscp** コマンドを使用して次を設定できます。
		• **default**：パケットをデフォルト DSCP 値（000000）と一致させます。
		• **dscp table**：テーブルマップに基づいて DSCP からパケットの DSCP 値を設定します。
		• **ef**：パケットを EF DSCP 値（101110）と一致させます。
		• **precedence table**：テーブル マップに基づいて優先順位からパケットの DSCP 値を設定します。
		• **qos-group table**：テーブル マップに基づいて QoS グループからパケットの DSCP 値を設定します。
		• **wlan user-priority table**：パケットの DSCP 値を、テーブル マップに基づいた WLAN ユーザ プライオリティに基づいて設定します。

	コマンドまたはアクション	目的

ステップ 6	**set ip** {**dscp** | **precedence**}
	例：
	`Device(config-pmap)# set ip dscp c3`
	`Device(config-pmap)#`
		（任意）IP 固有の値を設定します。これらの値は、IP DSCP 値または IP precedence 値です。
		set ip dscp コマンドを使用して、次の値を設定することができます。
		• *dscp value*：特定の DSCP の値を設定します。
		• **default**：パケットをデフォルト DSCP 値（000000）と一致させます。
		• **dscp table**：テーブル マップに基づいて DSCP からパケットの DSCP 値を設定します。
		• **ef**：パケットを EF DSCP 値（101110）と一致させます。
		• **precedence table**：テーブル マップに基づいて優先順位からパケットの DSCP 値を設定します。
		• **qos-group table**：テーブル マップに基づいて QoS グループからパケットの DSCP 値を設定します。
		• **wlan user-priority table**：パケットの DSCP 値を、テーブル マップに基づいた WLAN ユーザ プライオリティに基づいて設定します。
		set ip precedence コマンドを使用して、次の値を設定することができます。
		• *precedence value*：precedence 値を設定します（0 ～ 7）。
		• **cos table**：テーブル マップに基づいてレイヤ 2 CoS からパケットの precedence 値を設定します。
		• **dscp table**：テーブル マップに基づいて DSCP 値からパケットの precedence 値を設定します。

	コマンドまたはアクション	目的
		• **precedence table**：テーブル マップに基づいて優先順位から precedence 値を設定します。 • **qos-group table**：テーブル マップに基づいて QoS グループから precedence 値を設定します。

ステップ 7	**set precedence** {*precedence value* | **cos table** *table-map name* | **dscp table** *table-map name* | **precedence table** *table-map name* | **qos-group table** *table-map name*}
	例：
	`Device(config-pmap)# set precedence 5`
	`Device(config-pmap)#`
		（任意）IPv4 と IPv6 パケットの precedence 値を設定します。
		set precedence コマンドを使用して、次の値を設定することができます。
		• *precedence value*：precedence 値を設定します（0 ～ 7）。
		• **cos table**：レイヤ 2 CoS からのパケットの precedence 値をテーブル マップに基づいて設定します。
		• **dscp table**：テーブル マップに基づいて DSCP 値からパケットの precedence 値を設定します。
		• **precedence table**：テーブル マップに基づいて優先順位から precedence 値を設定します。
		• **qos-group table**：テーブル マップに基づいて QoS グループから precedence 値を設定します。

ステップ 8	**set qos-group** {*qos-group value* | **dscp table** *table-map name* | **precedence table** *table-map name*}
	例：
	`Device(config-pmap)# set qos-group 10`
	`Device(config-pmap)#`
		（任意）QoS グループ値を設定します。このコマンドを使用して次の値を設定できます。
		• *qos-group value*：1 から 31 までの数。
		• **dscp table**：テーブル マップに基づいて DSCP からコード ポイント値を設定します。
		• **precedence table**：テーブル マップに基づいて優先順位からコード ポイント値を設定します。

	コマンドまたはアクション	目的

ステップ 9	**set wlan user-priority** {*wlan user-priority value* | **cos table** *table-map name* | **dscp table** *table-map name* | **qos-group table** *table-map name* | **wlan table** *table-map name*}
	例：
	`Device(config-pmap)# set wlan user-priority 1`
	`Device(config-pmap)#`
		（任意）WLANユーザプライオリティ値を設定します。このコマンドを使用して次の値を設定できます。
		• *wlan user-priority value*：0 ～ 7 の範囲の値。
		• **cos table**：テーブル マップに基づいて Cos から WLAN ユーザ プライオリティ値を設定します。
		• **dscp table**：テーブルマップに基づいて DSCP から WLAN ユーザ プライオリティ値を設定します。
		• **qos-group table**：テーブル マップに基づいて QoS グループから WLANユーザプライオリティ値を設定します。
		• **wlan table**：テーブル マップに基づいて WLAN ユーザ プライオリティから WLAN ユーザ プライオリティ値を設定します。

ステップ 10	**end**
	例：
	`Device(config-pmap)# end`
	`Device#`
		設定変更を保存します。

ステップ 11	**show policy-map** 例： `Device# show policy-map`	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

service-policy コマンドを使用して、インターフェイスにトラフィック ポリシーを付加します。

音声およびビデオに対するクラス マップの設定（CLI）

音声およびビデオ トラフィックに対するクラスマップを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** *class-map-name* 例： `Device(config)# class-map voice`	クラス マップを作成します。
ステップ 3	**match dscp** *dscp-value-for-voice* 例： `Device(config-cmap)# match dscp 46`	IPv4 および IPv6 パケットの DSCP 値を照合します。この値を 46 に設定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 6	**class-map** *class-map-name* 例： `Device(config)# class-map video`	クラス マップを設定します。
ステップ 7	**match dscp** *dscp-value-for-video* 例： `Device(config-cmap)# match dscp 34`	IPv4 および IPv6 パケットの DSCP 値を照合します。この値を 34 に設定します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

トラフィック ポリシーのインターフェイスへの付加（CLI）

トラフィック クラスとトラフィック ポリシーの作成後、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、トラフィック ポリシーをインターフェイスに付加し、ポリシーを適用する方向を指定します（インターフェイスに着信するパケットまたはインターフェイスから送信されるパケット）。

始める前に

インターフェイスにトラフィック ポリシーを付加する前に、トラフィック クラスとトラフィック ポリシーを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type*
	例：
	`Device(config)# interface GigabitEthernet1/0/1`
	`Device(config-if)#`
		インターフェイス コンフィギュレーション モードを開始し、インターフェイスを設定します。
		インターフェイス コンフィギュレーションのコマンド パラメータは次のとおりです。
		• **Auto Template**：自動テンプレート インターフェイス
		• **Capwap**：Capwap トンネル インターフェイス
		• **GigabitEthernet**：Gigabit Ethernet IEEE 802
		• **GroupVI**：グループ仮想インターフェイス
		• **Internal Interface**：内部インターフェイス
		• **Loopback**：ループバック インターフェイス
		• **Null**：ヌル インターフェイス
		• **Port-channel**：インターフェイスのイーサネット チャネル
		• **TenGigabitEthernet**：10 ギガビット イーサネット
		• **Tunnel**：トンネル インターフェイス
		• **Vlan**：Catalyst VLAN

	コマンドまたはアクション	目的
		• **Range**：インターフェイス範囲

ステップ 3	**service-policy** {**input** *policy-map* | **output** *policy-map* }
	例：
	`Device(config-if)# service-policy output policy_map_01`
	`Device(config-if)#`
		ポリシー マップを入力または出力インターフェイスに適用します。このポリシー マップは、そのインターフェイスのサービス ポリシーとして使用されます。
		この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 4	**end**
	例：
	`Device(config-if)# end`
	`Device#`
		設定変更を保存します。

ステップ 5	**show policy map** 例： `Device# show policy map`	（任意）指定されたインターフェイスのポリシーの統計情報を表示します。

次のタスク

他のトラフィック ポリシーをインターフェイスに付加し、ポリシーを適用する方向を指定します。

関連トピック

物理ポートのポリシー マップ （1562 ページ）

WLAN での SSID またはクライアント ポリシーの適用（CLI）

始める前に

SSID に適用する前にサービス ポリシー マップを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**service-policy** [**input** | **output**] *policy-name* 例： `Device(config-wlan)# service-policy input policy-map-ssid`	ポリシーを適用します。次のオプションを使用できます。 • **input**：ポリシーマップを WLAN 入力トラフィックに割り当てます。 • **output**：ポリシーマップを WLAN 出力トラフィックに割り当てます。
ステップ 4	**service-policy client** [**input** | **output**] *policy-name* 例： `Device(config-wlan)# service-policy client input policy-map-client`	ポリシーを適用します。次のオプションを使用できます。 • **input**：クライアント ポリシーを WLANの入力方向に割り当てます。 • **output**：クライアント ポリシーを WLANの出力方向に割り当てます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

SSID ポリシー （1550 ページ）
ワイヤレス ターゲットでサポートされる QoS 機能 （1545 ページ）
例：SSID ポリシー
例：ダウンストリーム SSID ポリシーの設定 （1655 ページ）

ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング（CLI）

実行対象となるトラフィック クラスを指定する非階層型ポリシー マップを、物理ポート上に設定できます。サポートされるアクションは再マーキングとポリシングです。

始める前に

この手順を開始する前に、ネットワーク トラフィックの分類、ポリシング、およびマーキングについて、あらかじめポリシー マップによって決定しておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**class-map** {*class-map name* | **match-any**}
	例：
	`Device(config)# class-map ipclass1`
	`Device(config-cmap)# exit`
	`Device(config)#`
		クラスマップ コンフィギュレーション モードを開始します。
		• 名前を指定したクラスとパケットとの照合に使用されるクラスマップを作成します。
		• **match-any** を指定すると、トラフィック クラスで受信したトラフィックの場合、一致基準の 1 つに必ず一致し、そのトラフィック クラスの一部と分類されます。これはデフォルトです。

ステップ 3	**match access-group** { *access list index* | *access list name* }
	例：
	`Device(config-cmap)# match access-group 1000`
	`Device(config-cmap)# exit`
	`Device(config)#`
		分類基準をクラスマップに一致するように指定します。次の基準について照合できます。
		• **access-group**：アクセス グループに一致します。
		• **class-map**：別のクラスマップに一致します。
		• **cos**：CoS 値に一致します。
		• **dscp**：DSCP 値に一致します。
		• **ip**：特定の IP 値に一致します。
		• **non-client-nrt**：非クライアント NRT に一致します。
		• **precedence**：IPv4 および IPv6 パケットの precedence 値に一致します。
		• **qos-group**：QoS グループに一致します。
		• **vlan**：VLAN に一致します。

	コマンドまたはアクション	目的
		• **wlan**：ワイヤレスLANに一致します。

ステップ 4	**policy-map** *policy-map-name*
	例：
	`Device(config)# policy-map flowit`
	`Device(config-pmap)#`
		ポリシー マップ名を入力することによってポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
		デフォルトでは、ポリシーマップは定義されていません。

ステップ 5	**class** {*class-map-name* | **class-default**}
	例：
	`Device(config-pmap)# class ipclass1`
	`Device(config-pmap-c)#`
		トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
		デフォルトでは、ポリシーマップ クラス マップは定義されていません。
		すでに **class-map** グローバル コンフィギュレーションコマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。
		class-default トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシーマップの最後に配置されます。暗黙の **match any** が **class-default** クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは **class-default** と一致します。

ステップ 6	**set** {**cos** | **dscp** | **ip** | **precedence** | **qos-group** | **wlan user-priority**}
	例：
	`Device(config-pmap-c)# set dscp 45`
	`Device(config-pmap-c)#`
		（任意）QoS 値を設定します。使用可能な QoS 設定値は次のとおりです。
		• **cos**：IEEE 802.1Q/ISL サービス クラスまたはユーザプライオリティを設定します。
		• **dscp**：IP（v4）および IPv6 パケットの DSCP を設定します。
		• **ip**：IP 固有の値を設定します。

	コマンドまたはアクション	目的
		• **precedence**：IP（v4）および IPv6 パケットの precedence を設定します。 • **qos-group**：QoS グループを設定します。 • **wlan user-priority**：WLAN ユーザ プライオリティを設定します。 この例では、 **set dscp** コマンドが、パケットでの新しい DSCP 値を設定して IP トラフィックを分類します。

ステップ 7	**police** {*target_bit_rate*| **cir** | **rate**}
	例：
	`Device(config-pmap-c)# police 100000 conform-action transmit exceed-action drop`
	`Device(config-pmap-c)#`
		（任意）ポリサーを設定します。
		• *target_bit_rate*：ビット レート/秒を指定し、8000 ～ 10000000000 の値を入力します。
		• **cir**：認定情報レート。
		• **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングル レベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。
		
		この例では、**police** コマンドが 100000 セットのターゲット ビット レートを超えるトラフィックがドロップされるクラスにポリサーを追加します。

ステップ 8	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 9	**exit** 例： `Device(config-pmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *interface-id* 例： `Device(config)# interface`	ポリシーマップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	gigabitethernet 2/0/1	有効なインターフェイスには、物理ポートが含まれます。
ステップ 11	**service-policy input** *policy-map-name* 例： `Device(config-if)# service-policy input flowit`	ポリシーマップ名を指定し、入力ポートに適用します。サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 12	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show policy-map** [*policy-map-name* [**class** *class-map-name*]] 例： `Device# show policy-map`	（任意）入力を確認します。
ステップ 14	**copy running-config startup-config** 例： `Device# copy-running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次のタスク

必要に応じて QoS 設定は、ポリシー マップを使用して、SVI のトラフィックの分類、ポリシング、およびマーキングを設定します。

ポリシーマップによるSVIのトラフィックの分類、ポリシング、およびマーキング（CLI）

始める前に

この手順を開始する前に、ポリシー マップを使用して、ネットワーク トラフィックの分類、ポリシング、およびマーキングについて決定しておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** {*class-map name* | **match-any**} 例： `Device(config)# class-map class_vlan100`	クラスマップ コンフィギュレーション モードを開始します。 • 名前を指定したクラスとパケットとの照合に使用されるクラスマップを作成します。 • **match-any** を指定すると、トラフィック クラスで受信したトラフィックの場合、一致基準の 1 つに必ず一致し、そのトラフィッククラスの一部と分類されます。これはデフォルトです。

ステップ 3	**match vlan** *vlan number*
	例：
	`Device(config-cmap)# match vlan 100`
	`Device(config-cmap)# exit`
	`Device(config)#`
		VLAN をクラス マップに一致するように指定します。

ステップ 4	**policy-map** *policy-map-name*
	例：
	`Device(config)# policy-map policy_vlan100`
	`Device(config-pmap)#`
		ポリシー マップ名を入力することによってポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
		デフォルトでは、ポリシーマップは定義されていません。

ステップ 5	**description** 説明 例： `Device(config-pmap)# description vlan 100`	（任意）ポリシーマップの説明を入力します。

	コマンドまたはアクション	目的

ステップ 6	**class** {*class-map-name* | **class-default**}
	例：
	`Device(config-pmap)# class class_vlan100`
	`Device(config-pmap-c)#`
		トラフィック分類を定義し、ポリシーマップ クラス コンフィギュレーションモードを開始します。
		デフォルトでは、ポリシーマップ クラス マップは定義されていません。
		すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。
		class-default トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシーマップの最後に配置されます。暗黙の **match any** が **class-default** クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは **class-default** と一致します。

ステップ 7	**set** {**cos** | **dscp** | **ip** | **precedence** | **qos-group** | **wlan user-priority**}
	例：
	`Device(config-pmap-c)# set dscp af23`
	`Device(config-pmap-c)#`
		（任意）QoS 値を設定します。使用可能な QoS 設定値は次のとおりです。
		• **cos**：IEEE 802.1Q/ISL サービス クラスまたはユーザ プライオリティを設定します。
		• **dscp**：IP（v4）および IPv6 パケットの DSCP を設定します。
		• **ip**：IP 固有の値を設定します。
		• **precedence**：IP（v4）および IPv6 パケットの precedence を設定します。
		• **qos-group**：QoS グループを設定します。
		• **wlan user-priority**：WLAN ユーザ プライオリティを設定します。
		この例では、 **set dscp** コマンドが AF23（010010）の DSCP 値にパケットを照

	コマンドまたはアクション	目的
		合することによって、IP トラフィックを分類します。

ステップ 8	**police** {*target_bit_rate*| **cir** | **rate**}
	例：
	`Device(config-pmap-c)# police 200000 conform-action transmit exceed-action drop`
	`Device(config-pmap-c)#`
		（任意）ポリサーを設定します。
		• *target_bit_rate*：ビット レート/秒を指定します。8000 ～ 10000000000 の範囲で値を入力します。
		• **cir**：認定情報レート。
		• **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングル レベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。
		この例では、**police** コマンドが 200000 セットのターゲット ビット レートを超えるトラフィックがドロップされるクラスにポリサーを追加します。

ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 10	**exit** 例： `Device(config-pmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/3`	ポリシーマップを適用するポートを指定し、インターフェイスコンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 12	**service-policy input** *policy-map-name* 例： `Device(config-if)# service-policy input policy_vlan100`	ポリシーマップ名を指定し、入力ポートに適用します。サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 13	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# end`	
ステップ 14	**show policy-map** [*policy-map-name* [**class** *class-map-name*]] 例： `Device# show policy-map`	（任意）入力を確認します。
ステップ 15	**copy running-config startup-config** 例： `Device# copy-running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

VLAN のポリシー マップ （1563 ページ）
例：ポリサーの VLAN 設定 （1663 ページ）

テーブル マップの設定（CLI）

テーブルマップはマーキングの形式であり、テーブルを使用してフィールド間のマッピングと変換を可能にすることもできます。たとえば、テーブル マップはレイヤ 2 の CoS 設定をレイヤ 3 の precedence 値にマッピングして変換するために使用できます。

（注） テーブル マップは、複数のポリシーで、または同じポリシー内で複数回参照できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**table-map** *name* {**default** {*default value* | **copy** | **ignore**} | **exit** | **map** {**from** *from value***to** *to value* } | **no**} 例：	テーブル マップを作成し、テーブル マップ コンフィギュレーション モードを開始します。テーブル マップ コンフィギュレーション モードでは、次のタスクを実行できます。

	コマンドまたはアクション	目的
	`Device(config)# table-map table01` `Device(config-tablemap)#`	• **default**：テーブルマップのデフォルト値を設定するか、テーブルマップ内にない値についてのデフォルトの動作（コピーまたは無視）を設定します。 • **exit**：テーブル マップ コンフィギュレーションモードを終了します。 • **map**：テーブルマップで *from* 値を *to* 値にマッピングします。 • **no**：コマンドのデフォルト値を無効にするか、設定します。

ステップ 3	**mapfrom** *value* **to** *value*
	例：
	`Device(config-tablemap)# map from 0 to 2`
	`Device(config-tablemap)# map from 1 to 4`
	`Device(config-tablemap)# map from 24 to 3`
	`Device(config-tablemap)# map from 40 to 6`
	`Device(config-tablemap)# default 0`
	`Device(config-tablemap)#`
		この手順では、DSCP 値が 0 のパケットを CoS 値 2 に、DSCP 値が 1 のパケットを CoS 値 4 に、DSCP 値が 24 のパケットを CoS 値 3 に、DSCP 値が 40 のパケットを CoS 値 6 に、およびそれ以外のすべてのパケットを CoS 値 0 にマークします。
		（注） この例の CoS 値から DSCP 値へのマッピングは、後で説明するように、**set** ポリシーマップ クラス コンフィギュレーションコマンドを使用して設定します。

ステップ 4	**exit**
	例：
	`Device(config-tablemap)# exit`
	`Device(config)#`
		グローバル コンフィギュレーションモードに戻ります。

ステップ 5	**exit**
	例：
	`Device(config) exit`
	`Device#`
		特権 EXEC モードに戻ります。

ステップ 6	**show table-map** 例：	テーブル マップ設定を表示します。

	コマンドまたはアクション	目的

	`Device# show table-map`
	`Table Map table01`
	`  from 0 to 2`
	`  from 1 to 4`
	`  from 24 to 3`
	`  from 40 to 6`
	`  default 0`	

ステップ 7	**configureterminal**
	例：
	`Device# configure terminal`
	`Device(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 8	**policy-map**
	例：
	`Device(config)# policy-map table-policy`
	`Device(config-pmap)#`
		テーブルマップのポリシーマップを設定します。

ステップ 9	**class class-default**
	例：
	`Device(config-pmap)# class class-default`
	`Device(config-pmap-c)#`
		クラスをシステムデフォルトに一致させます。

ステップ 10	**set cos dscp table** *table map name*
	例：
	`Device(config-pmap-c)# set cos dscp table table01`
	`Device(config-pmap-c)#`
		このポリシーが入力ポートに適用された場合、そのポートでは trust dscp がイネーブルになり、テーブルマップに応じてマーキングが行われます。

ステップ 11	**end**
	例：
	`Device(config-pmap-c)# end`
	`Device#`
		特権 EXEC モードに戻ります。

次のタスク

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

関連トピック

テーブル マップのマーキング （1565 ページ）
例：テーブル マップのマーキング設定 （1665 ページ）

信頼の設定

ワイヤレス トラフィックの信頼動作の設定（CLI）

Cisco IOS XE 3.2 リリースは、有線およびワイヤレス ポートに対して信頼できるさまざまなデフォルト設定をサポートしました。有線ポートの信頼できるデフォルト設定に関して、このソフトウェア リリースでの変更はありません。ワイヤレス ポートの場合、デフォルトのシステム動作は非信頼でした。つまり、の起動時に、ワイヤレスポートのマーキングすべてがデフォルトでゼロに設定され、トラフィックはプライオリティ処理されませんでした。既存の有線との互換性のために、すべてのトラフィックはデフォルトでベストエフォートのキューへ送信されていました。アクセス ポイントは、プライオリティ キューイングをデフォルトで実行していました。ダウンストリーム方向では、アクセス ポイントは、キューイング用に音声、ビデオ、ベスト エフォート、およびバックグラウンドのキューを保持していました。アクセスは 11e タグ情報に基づいてキューイング戦略を選択していました。デフォルトでは、アクセス ポイントはすべてのワイヤレス パケットをベスト エフォートとして処理していました。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**qoswireless-default-untrust** 例： `Device (config)# qos wireless-default-untrust`	デバイスの動作を設定して、ワイヤレス トラフィックを非信頼にします。ワイヤレス トラフィックをデフォルトで信頼するようにデバイスを設定するには、このコマンドの **no** 形式を使用します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

有線およびワイヤレス ポートの信頼動作 （1577 ページ）

QoS の特性と機能の設定

コール アドミッション制御の設定（CLI）

このタスクでは、デバイスでコール アドミッション制御（CAC）用にクラスベースの無条件パケット マーキング機能を設定する方法を説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**class-map** *class name*
	例：
	`Device(config)# class-map voice`
	`Device(config-cmap)#`
		ポリシー クラス マップ コンフィギュレーションモードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシークラスマップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。
		• *word*：クラス マップ名。
		• **class-default**：未分類のパケットを照合するシステムデフォルトクラス。

ステップ 3	**match dscp** *dscp value* 例： `Device(config-cmap)# match dscp 46`	（任意）IPv4 および IPv6 パケットの DSCP 値に一致します。

ステップ 4	**exit**
	例：
	`Device(config-cmap)# exit`
	`Device(config)#`
		グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的

ステップ 5	**class-map** *class name*
	例：
	`Device(config)# class-map video`
	`Device(config-cmap)#`
		ポリシー クラス マップ コンフィギュレーションモードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラスマップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。
		• *word*：クラス マップ名。
		• **class-default**：未分類のパケットを照合するシステムデフォルトクラス。

ステップ 6	**match dscp** *dscp value* 例： `Device(config-cmap)# match dscp 34`	（任意）IPv4 および IPv6 パケットの DSCP 値に一致します。

ステップ 7	**exit**
	例：
	`Device(config-cmap)# exit`
	`Device(config)#`
		グローバル コンフィギュレーション モードに戻ります。

ステップ 8	**table-map** *name*
	例：
	`Device(config)# table-map dscp2dscp`
	`Device(config-tablemap)#`
		テーブル マップを作成し、テーブル マップ コンフィギュレーション モードを開始します。

ステップ 9	**default copy** 例： `Device(config-tablemap)# default copy`	コピーするテーブルマップで検出されない値のデフォルト動作を設定します。 （注） これがデフォルトのオプションです。DSCP から DSCP へ値をマッピングすることもできます。
ステップ 10	**exit** 例： `Device(config-tablemap)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)#`	

ステップ 11	**table-map** *name*
	例：
	`Device(config)# table-map dscp2up`
	`Device(config-tablemap)#`
		新しいテーブルマップを作成し、テーブル マップ コンフィギュレーション モードを開始します。

ステップ 12	**default copy** 例： `Device(config-tablemap)# default copy`	コピーするテーブルマップで検出されない値のデフォルト動作を設定します。 （注） これがデフォルトのオプションです。DSCP から UP へ値をマッピングすることもできます。

ステップ 13	**exit**
	例：
	`Device(config-tablemap)# exit`
	`Device(config)#`
		グローバル コンフィギュレーション モードに戻ります。

ステップ 14	**policy-map** *policy name*
	例：
	`Device(config)# policy-map ssid_child_cac`
	`Device(config-pmap)#`
		ポリシーマップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。

ステップ 15	**class** *class-map-name* 例： `Device(config-pmap)# class voice`	インターフェイス レベルのトラフィック分類を定義し、ポリシーマップ コンフィギュレーションモードを開始します。
ステップ 16	**prioritylevel** *level_value* 例： `Device(config-pmap-c)# priority level`	**priority** コマンドは、クラスに完全スケジューリングプライオリティを割り当てます。

	コマンドまたはアクション	目的
	1	（注） プライオリティ レベル1はプライオリティ レベル2より重要です。プライオリティ レベル1は、QoSに最初に処理される帯域幅を予約するため、遅延は非常に低くなります。プライオリティ レベル1と2はどちらも帯域幅を予約します。
ステップ 17	**police** ［*target_bit_rate*｜ **cir**｜**rate**］ 例： `Device(config-pmap-c)# police cir 10m`	（任意）ポリサーを設定します。 • *target_bit_rate*：ビット レート/秒を指定します。8000 ～ 10000000000の範囲で値を入力します。 • **cir**：認定情報レート。 • **rate**：ポリシング レート、階層型ポリシーのPCR、またはシングルレベルのATM 4.0ポリサー ポリシーのSCRを指定します。

ステップ 18	**admit cac wmm-tspec**
	例：
	`Device(config-pmap-c)# admit cac wmm-tspec`
	`Device(config-pmap-cac-wmm)#`
		ポリシー マップに対するコール アドミッション制御を設定します。
		（注） このコマンドは、ワイヤレスQoSのCACだけを設定します。

ステップ 19	**rate** *value* 例： `Device(config-pmap-admit-cac-wmm)# rate 5000`	ターゲット ビット レート（kbps）を設定します。8 ～ 10000000の範囲の数を入力してください。
ステップ 20	**wlan-up** *value* 例： `Device(config-pmap-admit-cac-wmm)# wlan-up 6 7`	WLAN UP値を設定します。0 ～ 7の範囲の数を入力してください。
ステップ 21	**exit** 例：	ポリシー マップ クラス コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-pmap-admit-cac-wmm)#` **`exit`** `Device(config-pmap-c)#`	
ステップ 22	**exit** 例： `Device(config-pmap-c)#` **`exit`** `Device(config-pmap)#`	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 23	**class** *class name* 例： `Device(config-pmap)#` **`class video`** `Device(config-pmap-c)#`	ポリシー クラス マップ コンフィギュレーションモードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラスマップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。 • *word*：クラス マップ名。 • **class-default**：未分類のパケットを照合するシステムデフォルトクラス。
ステップ 24	**prioritylevel** *level_value* 例： `Device(config-pmap-c)#` **`priority level 2`**	**priority** コマンドは、クラスに完全スケジューリングプライオリティを割り当てます。 （注） プライオリティ レベル1はプライオリティ レベル2より重要です。プライオリティ レベル1は、QoSに最初に処理される帯域幅を予約するため、遅延は非常に低くなります。プライオリティ レベル1と2はどちらも帯域幅を予約します。
ステップ 25	**police** ［*target_bit_rate*｜ **cir**｜ **rate**］ 例： `Device(config-pmap-c)#` **`police cir 20m`**	（任意）ポリサーを設定します。 • *target_bit_rate*：ビット レート/秒を指定します。8000 ～ 10000000000の範囲で値を入力します。 • **cir**：認定情報レート。

	コマンドまたはアクション	目的
		• **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングル レベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。

ステップ 26	**admit cac wmm-tspec**
	例：
	`Device(config-pmap-c)# admit cac wmm-tspec`
	`Device(config-pmap-admit-cac-wmm)#`
		ポリシー マップに対するコール アドミッション制御を設定します。
		（注） このコマンドは、ワイヤレス QoS の CAC だけを設定します。

ステップ 27	**rate** *value* 例： `Device(config-pmap-admit-cac-wmm)# rate 5000`	ターゲット ビット レート（kbps）を設定します。8 ～ 10000000 の範囲の数を入力してください。
ステップ 28	**wlan-up** *value* 例： `Device(config-pmap-admit-cac-wmm)# wlan-up 4 5`	WLAN UP 値を設定します。0 ～ 7 の範囲の数を入力してください。

ステップ 29	**exit**
	例：
	`Device(config-pmap-cac-wmm)# exit`
	`Device(config-pmap)#`
		ポリシーマップ コンフィギュレーション モードに戻ります。

ステップ 30	**exit**
	例：
	`Device(config-pmap)# exit`
	`Device(config)#`
		グローバル コンフィギュレーション モードに戻ります。

ステップ 31	**policy-map** *policy name*
	例：
	`Device(config)# policy-map ssid_cac`
	`Device(config-pmap)#`
		ポリシーマップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。

	コマンドまたはアクション	目的
ステップ 32	**class** *class-map-name* 例： `Device(config-pmap)# class default`	インターフェイス レベルのトラフィック分類を定義し、ポリシーマップ コンフィギュレーション モードを開始します。 この例では、クラスマップはデフォルトに設定されます。
ステップ 33	**set dscp dscp table** *table_map_name* 例： `Device(config-pmap-c)# set dscp dscp table dscp2dscp`	（任意）QoS 値を設定します。この例では、 **set dscp dscp table** コマンドはテーブルマップを作成し、値を設定します。
ステップ 34	**set wlan user-priority dscp table** *table_map_name* 例： `Device(config-pmap-c)# set wlan user-priority dscp table dscp2up`	（任意）QoS 値を設定します。この例では、 **set wlan user-priority dscp table** コマンドは WLAN ユーザ プライオリティを設定します。
ステップ 35	**shapeaverage** {*target bit rate* | **percent** *percentage*} 例： `Device(config-pmap-c)# shape average 100000000`	平均シェーピング レートを設定します。平均シェーピング レートを、ターゲット ビット レート（bps）または認定情報レート（CIR）のインターフェイス帯域幅の割合で設定できます。
ステップ 36	**queue-buffers** {**ratio** *ratio value*} 例： `Device(config-pmap-c)# queue-buffers ratio 0`	キューの相対的なバッファ サイズを設定します。 （注） ポリシーに設定されているすべてのバッファの合計が 100 % 以下である必要があります。未割り当てバッファは、残りのキューに均等に分散されます。プライオリティ キューを含むすべてのキューに十分なバッファが割り当てられるようにします。

	コマンドまたはアクション	目的
		（注） スパニングツリーやLACPなどのネットワーク制御プロトコルのプロトコル データ ユニット（PDU）は、プライオリティ キューまたはキュー0（プライオリティ キューが設定されていない場合）を使用します。プロトコルが機能するには、これらのキューに十分なバッファが割り当てられるようにします。
ステップ 37	**service-policy** *policy_map_name* 例： `Device(config-pmap-c)# service-policy ssid_child_cac`	サービスポリシーのポリシーマップを指定します。

ステップ 38	**end**
	例：
	`Device(config-pmap)# end`
	`Device#`
		設定変更を保存します。

ステップ 39	**show policy-map** 例： `Device# show policy-map`	（任意）すべてのサービスポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

CAC の詳細については、『*System Management Configuration Guide, Cisco IOS XE Release 3SE（Catalyst 3850 Switches）*』を参照してください。

帯域幅の設定（CLI）

この手順は、で帯域幅を設定する方法を示します。

始める前に

この手順を開始する前に、帯域幅のクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**policy-map** *policy name*
	例：
	`Device(config)# policy-map policy_bandwidth01`
	`Device(config-pmap)#`
		ポリシー マップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

ステップ 3	**class** *class name*
	例：
	`Device(config-pmap)# class class_bandwidth01`
	`Device(config-pmap-c)#`
		ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。
		• *word*：クラス マップ名。
		• **class-default**：未分類のパケットを照合するシステム デフォルト クラス。

ステップ 4	**bandwidth** {*Kb/s* | **percent** *percentage* | **remaining** { **ratio** *ratio* }}
	例：
	`Device(config-pmap-c)# bandwidth 200000`
	`Device(config-pmap-c)#`
		ポリシーマップの帯域幅を設定します。パラメータは次のとおりです。
		• *Kb/s*：特定の値を kbps で設定します（20000 ～ 10000000）。
		• **percent-**：割合に基づいて、特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。100 % 未満の場合、帯域幅の残りは、すべ

	コマンドまたはアクション	目的
		ての帯域幅キュー上に均等に分割されます。 • **remaining**：特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。このコマンドは、ポリシー内の特定のキューに対して **priority** コマンドが使用されている場合に使用します。各キューには、割合ではなく比率を割り当てることもできます。キューにはそれらの比率に従って、特定の重みが割り当てられます。比率は 0 ～ 100 の範囲で指定できます。この場合のポリシーの全帯域幅での比率の割り当ては、100 を超えることができます。 （注） ポリシー マップで帯域幅タイプを混在させることはできません。たとえば、1 つのポリシー マップで帯域幅の割合と kbps の両方を使用して、帯域幅を設定することはできません。

ステップ 5	**end**
	例：
	`Device(config-pmap-c)# end`
	`Device#`
		設定変更を保存します。

ステップ 6	**show policy-map** 例： `Device# show policy-map`	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用して、インターフェイスにトラフィック ポリシーを付加します。

関連トピック

帯域幅 （1572 ページ）

ポリシングの設定（CLI）

この手順は、でポリシングを設定する方法を説明しています。

始める前に

この手順を開始する前に、ポリシングのクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**policy-map** *policy name*
	例：
	`Device(config)# policy-map policy_police01`
	`Device(config-pmap)#`
		ポリシー マップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

ステップ 3	**class** *class name*
	例：
	`Device(config-pmap)# class class_police01`
	`Device(config-pmap-c)#`
		ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。
		• *word*：クラス マップ名。
		• **class-default**：未分類のパケットを照合するシステム デフォルト クラス。

	コマンドまたはアクション	目的

ステップ 4	**police** {*target_bit_rate* [*burst bytes* | **bc** | **conform-action** | **pir**] | **cir** {*target_bit_rate* | **percent** *percentage*} | **rate** {*target_bit_rate* | **percent** *percentage*} **conform-actiontransmitexceed-action** {**drop** [**violate action**] | **set-cos-transmit** | **set-dscp-transmit** | **set-prec-transmit** | **transmit** [**violate action**] }}
	
	例：
	
	`Device(config-pmap-c)# police 8000 conform-action transmit exceed-action drop`
	`Device(config-pmap-c)#`
		次の **police** サブコマンド オプションを使用できます。
		
		• *target_bit_rate*：ビット/秒（8000 ～ 10000000000）。
		　• *burst bytes*：1000 ～ 512000000 の値を入力します。
		　• **bc**：適合バースト。
		　• **conform-action**：レートが適合バーストより小さくなる場合に実行されるアクション。
		　• **pir**：最大情報レート。
		
		• **cir**：認定情報レート。
		　• *target_bit_rate*：ターゲット ビット レート（8000 ～ 10000000000）。
		　• **percent**：CIR のインターフェイス帯域幅の割合。
		
		• **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングルレベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。
		　• *target_bit_rate*：ターゲット ビット レート（8000 ～ 10000000000）。
		　• **percent**：レートのインターフェイス帯域幅の割合。
		
		次の **police conform-action transmit exceed-action** サブコマンド オプションを使用できます。
		
		• **drop**：パケットをドロップします。
		• **set-cos-transmit**：CoS 値を設定して送信します。
		• **set-dscp-transmit**：DSCP 値を設定して送信します。

	コマンドまたはアクション	目的
		• **set-prec-transmit**：パケットの precedence を書き換えて送信します。 • **transmit**：パケットを送信します。 （注） ポリサー ベースのマークダウン アクションは、テーブルマップを使用する場合のみサポートされます。内の各マーキング フィールドでは、1 つのマークダウンテーブルマップだけが許可されます。

ステップ 5	**end**
	例：
	`Device(config-pmap-c)# end`
	`Device#`
		設定変更を保存します。

ステップ 6	**show policy-map** 例： `Device# show policy-map`	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。 （注） **show policy-map** コマンドの出力では、適合バイトおよび超過バイトのカウンタを表示しません。

次のタスク

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

関連トピック

シングルレート 2 カラー ポリシング （1568 ページ）
例：シングルレート 2 カラー ポリシング設定 （1664 ページ）
デュアルレート 3 カラー ポリシング （1569 ページ）
例：デュアルレート 3 カラー ポリシング設定 （1665 ページ）
ポリシング （1563 ページ）
例：ポリシング アクションの設定 （1662 ページ）
トークンバケット アルゴリズム （1564 ページ）

例：ポリシングの単位 （1663 ページ）

プライオリティの設定（CLI）

この手順は、でプライオリティを設定する方法を示します。

では、指定されたキューにプライオリティを与えることができます。使用可能な2つのプライオリティ レベルがあります（1 および 2）。

（注） 音声とビデオに対応するキューには、プライオリティ レベル 1 を割り当てます。

始める前に

この手順を開始する前に、プライオリティのクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**policy-map** *policy name*
	例：
	`Device(config)# policy-map policy_priority01`
	`Device(config-pmap)#`
		ポリシー マップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

ステップ 3	**class** *class name*
	例：
	`Device(config-pmap)# class class_priority01`
	`Device(config-pmap-c)#`
		ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。
		• *word*：クラス マップ名。
		• **class-default**：未分類のパケットを照合するシステム デフォルト クラス。

	コマンドまたはアクション	目的

ステップ 4	**priority** [*Kb/s* [*burst_in_bytes*] | **level** *level_value* [*Kb/s* [*burst_in_bytes*] | **percent** *percentage* [*burst_in_bytes*]] | **percent** *percentage* [*burst_in_bytes*]]
	例：
	`Device(config-pmap-c)# priority level 1`
	`Device(config-pmap-c)#`
		（任意）**priority** コマンドは、クラスに完全スケジューリング プライオリティを割り当てます。
		コマンドオプションは次のとおりです。
		• *Kb/s*：kbps を指定します（1 ～ 2000000）。
		• *burst_in_bytes*：バイトでバーストを指定します（32 ～ 2000000）。
		• **level** *level_value*：マルチレベル（1 ～2）のプライオリティ キューを指定します。
		• *Kb/s*：kbps を指定します（1 ～ 2000000）。
		• *burst_in_bytes*：バイトでバーストを指定します（32 ～ 2000000）。
		• **percent**：総帯域幅の割合。
		• *burst_in_bytes*：バイトでバーストを指定します（32 ～ 2000000）。
		• **percent**：総帯域幅の割合。
		• *burst_in_bytes*：バイトでバーストを指定します（32 ～ 2000000）。
		（注） プライオリティ レベル 1 はプライオリティ レベル 2 より重要です。プライオリティ レベル 1 は、 QoS に最初に処理される帯域幅を予約するため、遅延は非常に低くなります。プライオリティ レベル 1 と 2 はどちらも帯域幅を予約します。

	コマンドまたはアクション	目的

ステップ 5	**end**
	例：
	`Device(config-pmap-c)# end`
	`Device#`
		設定変更を保存します。

ステップ 6	**show policy-map** 例： `Device# show policy-map`	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

関連トピック

プライオリティ キュー （1574 ページ）

キューとシェーピングの設定

出力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さによっては、この項の手順をすべて実行する必要があります。次の特性を決定する必要があります。

- DSCP、CoS、または QoS グループ値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューに適用されるドロップ割合のしきい値と、トラフィック タイプで必要な予約メモリと最大メモリ
- キューに割り当てる固定バッファ スペース
- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術（シェーピング、共有、または両方）

（注） 出力キューはでのみ設定できます。

キュー バッファの設定（CLI）

を使用すると、キューにバッファを割り当てることができます。バッファが割り当てられていない場合は、すべてのキューに対して均等に分割されます。queue-buffer ratio を使用して、特定の比率で分割できます。デフォルトでDTS（Dynamic Threshold and Scaling）はすべてのキューでアクティブになるため、これらはソフト バッファになります。

（注） queue-buffer ratio は有線ポートと無線ポートの両方でサポートされますが、queue-buffer ratio は queue-limit とともに設定することはできません。

始める前に

この手順の前提条件を次に示します。

- この手順を開始する前に、キュー バッファのクラス マップを作成する必要があります。
- キュー バッファを設定する前に、ポリシー マップの帯域幅、シェーピング、またはプライオリティを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**policy-map** *policy name*
	例：
	`Device(config)# policy-map policy_queuebuffer01`
	`Device(config-pmap)#`
		ポリシー マップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

ステップ 3	**class** *class name*
	例：
	`Device(config-pmap)# class class_queuebuffer01`
	`Device(config-pmap-c)#`
		ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。
		• *word*：クラス マップ名。

	コマンドまたはアクション	目的
		• **class-default**：未分類のパケットを照合するシステム デフォルト クラス。

ステップ 4	**bandwidth** {*Kb/s* | **percent** *percentage* | **remaining** { **ratio** *ratio value* }}
	例：
	`Device(config-pmap-c)# bandwidth percent 80`
	`Device(config-pmap-c)#`
		ポリシーマップの帯域幅を設定します。コマンドパラメータは次のとおりです。
		• *Kb/s*：特定の値を設定するには、このコマンドを使用します。指定できる範囲は 20000 ～ 10000000 です。
		• **percent**：割合を使用して特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。100％未満の場合、帯域幅の残りは、すべての帯域幅キュー上に均等に分割されます。
		• **remaining**：特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。このコマンドは、ポリシー内の特定のキューに対して **priority** コマンドが使用されている場合に使用します。各キューには、割合ではなく比率を割り当てることもできます。キューにはそれらの比率に従って、特定の重みが割り当てられます。比率は 0 ～ 100 の範囲で指定できます。この場合のポリシーの全帯域幅での比率の割り当ては、100 を超えることができます。
		（注） ポリシー マップで帯域幅タイプを混在させることはできません。

	コマンドまたはアクション	目的

ステップ 5	**queue-buffers** {**ratio** *ratio value*}
	例：
	`Device(config-pmap-c)# queue-buffers ratio 10`
	`Device(config-pmap-c)#`
		キューの相対的なバッファ サイズを設定します。
		（注） ポリシーに設定されているすべてのバッファの合計が 100 % 以下である必要があります。未割り当てバッファは、残りのキューに均等に分散されます。プライオリティ キューを含むすべてのキューに十分なバッファが割り当てられるようにします。
		（注） スパニングツリーや LACP などのネットワーク制御プロトコルのプロトコル データ ユニット（PDU）は、プライオリティ キューまたはキュー 0（プライオリティ キューが設定されていない場合）を使用します。プロトコルが機能するには、これらのキューに十分なバッファが割り当てられるようにします。

ステップ 6	**end**
	例：
	`Device(config-pmap-c)# end`
	`Device#`
		設定変更を保存します。

ステップ 7	**show policy-map** 例： `Device# show policy-map`	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

関連トピック

キュー バッファの割り当て （1575 ページ）

例：キュー バッファの設定 （1662 ページ）

キュー制限の設定（CLI）

重み付けテール ドロップ（WTD）を設定するためにキュー制限を使用します。WTD を使用すると、キューごとに複数のしきい値を設定できます。各サービス クラスが異なるしきい値でドロップされて QoS 差別化が実現されます。によって、3 つの明示的にプログラム可能なしきい値クラスとして各キューに 0、1、2 を指定できます。したがって、キューごとに各パケットのキューイング/ドロップの決定は、フレーム ヘッダーの DSCP、CoS、または QoS グループ フィールドに指定されたパケットのしきい値クラスの割り当てによって決定されます。

WTD では柔軟な制限が使用されるため、最大 400 %（共通プールで予約されるバッファの最大 4 倍）のキュー制限を設定できます。この柔軟な制限は、他の機能に影響することなく、共通プールのオーバーランを防止します。

（注） キュー制限は、有線ポートの出力キューでのみ設定できます。

始める前に

この手順の前提条件を次に示します。

- この手順を開始する前に、キュー制限を使用するクラス マップを作成する必要があります。
- キュー制限を設定する前に、ポリシー マップの帯域幅、シェーピング、またはプライオリティを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**policy-map** *policy name*
	例：
	`Device(config)# policy-map policy_queuelimit01`
	`Device(config-pmap)#`
		ポリシー マップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

ステップ 3	**class** *class name* 例：	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリ

	コマンドまたはアクション	目的
	`Device(config-pmap)# class class_queuelimit01` `Device(config-pmap-c)#`	シーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。 • *word*：クラス マップ名。 • **class-default**：未分類のパケットを照合するシステム デフォルト クラス。

ステップ 4	**bandwidth** {*Kb/s* | **percent** *percentage* | **remaining** { **ratio** *ratio value* }}
	例：
	`Device(config-pmap-c)# bandwidth 500000`
	`Device(config-pmap-c)#`
		ポリシーマップの帯域幅を設定します。パラメータは次のとおりです。
		• *Kb/s*：特定の値を設定するには、このコマンドを使用します。指定できる範囲は 20000 ～ 10000000 です。
		• **percent**：特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。100 % 未満の場合、帯域幅の残りは、すべての帯域幅キュー上に均等に分割されます。
		• **remaining**：特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。このコマンドは、ポリシー内の特定のキューに対して **priority** コマンドが使用されている場合に使用します。各キューには、割合ではなく比率を割り当てることもできます。キューにはそれらの比率に従って、特定の重みが割り当てられます。比率は 0 ～ 100 の範囲で指定できます。この場合のポリシーの全帯域幅での比率の割り当ては、100 を超えることができます。

	コマンドまたはアクション	目的
		（注） ポリシー マップで帯域幅タイプを混在させることはできません。

ステップ 5	**queue-limit** {*packets* | {*cos value* { *maximum threshold value* | *percentage* } | {*cos value* | *percentage* } } | {*dscp value* {*maximum threshold value* | *percentage*} | *match packet* {*maximum threshold value* | *percentage*} | {*maximum threshold value* | *percentage*} | {*maximum threshold value* | *percentage*} | *dscp value*} | *percentage* }}**packetscospercent valuespercentdscppercentpercentdefaultpercentpercentdscp valuespercent**
	例：
	`Device(config-pmap-c)# queue-limit dscp 3 percent 20`
	`Device(config-pmap-c)# queue-limit dscp 4 percent 30`
	`Device(config-pmap-c)# queue-limit dscp 5 percent 40`
		キュー制限のしきい値の割合を設定します。
		すべてのキューで、3つのしきい値（0、1、2）があり、それぞれのしきい値についてデフォルト値があります。デフォルトまたはその他のキュー制限しきい値設定を変更するには、このコマンドを使用します。たとえば、DSCP 3、4、および5のパケットが設定した特定のキューに送信される場合、このコマンドは、この3つのDSCP値のしきい値パーセンテージを設定できます。キュー制限しきい値に関する詳細については、重み付けテール ドロップ（1573ページ）を参照してください。
		（注） は絶対キュー制限の割合をサポートしません。は、dscp または cos キュー制限の割合だけをサポートします。

ステップ 6	**end**
	例：
	`Device(config-pmap-c)# end`
	`Device#`
		設定変更を保存します。

ステップ 7	**show policy-map** 例： `Device# show policy-map`	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークの QoS 用の追加ポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用して、トラフィック ポリシーまたはポリシーをインターフェイスに付加します。

関連トピック

重み付けテール ドロップ （1573 ページ）
例：キュー制限の設定 （1661 ページ）

シェーピングの設定（CLI）

特定のクラスのシェーピング（最大帯域幅）を設定するには、**shape** コマンドを使用します。ポートに残っている追加帯域幅があっても、キューの帯域幅はこの値に制限されます。シェーピングは平均の割合で、または bps のシェーピングの平均値で設定できます。

始める前に

この手順を開始する前に、シェーピングのクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**policy-map** *policy name*
	例：
	`Device(config)# policy-map policy_shaping01`
	`Device(config-pmap)#`
		ポリシー マップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

ステップ 3	**class** *class name*
	例：
	`Device(config-pmap)# class class_shaping01`
	`Device(config-pmap-c)#`
		ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。
		• *word*：クラス マップ名。
		• **class-default**：未分類のパケットを照合するシステム デフォルト クラス。

ステップ 4	**shapeaverage** {*target bit rate* | **percent** *percentage*} 例：	平均シェーピング レートを設定します。平均シェーピング レートを、ターゲット ビット レート（bps）または認定情報

	コマンドまたはアクション	目的
	`Device(config-pmap-c)# shape average percent 50` `Device(config-pmap-c)#`	レート（CIR）のインターフェイス帯域幅の割合で設定できます。 （注） 出力 class-default SSID ポリシーの場合、平均シェーピング レートを設定した後にキュー バッファの割合を 0 に設定する必要があります。

ステップ 5	**end**
	例：
	`Device(config-pmap-c)# end`
	`Device#`
		設定変更を保存します。

ステップ 6	**show policy-map** 例： `Device# show policy-map`	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーをインターフェイスに付加します。

関連トピック

平均レート シェーピング （1570 ページ）
例：平均レート シェーピングの設定 （1660 ページ）
階層型シェーピング （1570 ページ）

貴金属ポリシーの設定（CLI）

WLAN 単位で貴金属 QoS ポリシーを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wlan** *wlan-name* 例： `Device`**`wlan test4`**	WLAN コンフィギュレーション サブモードを開始します。
ステップ 3	**service-policy** {**input** | **output**} *policy-name* 例： `Device(config-wlan)#` **`service-policy output platinum`** 例： `Device(config-wlan)#` **`service-policy input platinum-up`**	QoS ポリシーで WLAN を設定します。貴金属ポリシーで WLAN を設定するには、キーワード **platinum**、**gold**、**silver**、または **bronze** のいずれか 1 つを入力する必要があります。この例に示されるように、**platinum-up** キーワードでアップストリーム ポリシーが指定されます。 （注） アップストリーム ポリシーは、ダウンストリーム ポリシーと異なります。アップストリーム ポリシーには -up サフィックスがあります。
ステップ 4	**end** 例： `Device(config)#` **`end`**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ステップ 5	**show wlan** {*wlan-id* | *wlan-name*}
	例：
	`Device#` **`show wlan name qos-wlan`**
		WLAN の設定済みの QoS ポリシーを検証します。
		`Device#` **`show wlan name qos-wlan`**
		`. . .`
		`. . .`
		`. . .`
		`QoS Service Policy - Input`
		`  Policy Name`
		`  : platinum-up`
		`  Policy State`
		`  : Validated`
		`QoS Service Policy - Output`
		`  Policy Name`
		`  : platinum`
		`  Policy State`
		`  : Validated`
		`. . .`
		`. . .`

関連トピック

ワイヤレス QoS の貴金属ポリシー （1580 ページ）

QoS のモニタリング

での QoS のモニタリングには、次のコマンドを使用できます。

表 *99 : QoS* のモニタリング

コマンド	説明
show class-map [*class_map_name*]	設定されているすべてのクラスマップのリストを表示します。
show class-map type control subscriber {**all** | *name* } **show class-map type control subscriber detail**	制御クラスマップと統計情報を表示します。 • all：すべてのクラスマップに関する情報を表示します。 • name：設定済みのクラスマップを表示します。
show policy-map [*policy_map_name*]	設定されているすべてのポリシーマップのリストを表示します。コマンドパラメータは次のとおりです。 • **policy map name** • **interface** • **session**

コマンド	説明
show policy-map interface { **Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Lspvif** | | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output** | **wireless** }	

コマンド	説明
	で設定されているすべてのポリシーのランタイムと統計情報を表示します。コマンドパラメータは次のとおりです。 • **Auto-template**：Auto-Templateインターフェイス • **Capwap**：Capwap トンネルインターフェイス • **GigabitEthernet**：ギガビット イーサネット IEEE.802.3z • **GroupVI**：グループ仮想インターフェイス • **InternalInterface**：内部インターフェイス • **Loopback**：ループバックインターフェイス • **Lspvif**：LSP 仮想インターフェイス • **Null**：ヌルインターフェイス • **port-channel**：インターフェイスのイーサネットチャネル • **TenGigabitEthernet**：10 ギガビット イーサネット • **Tunnel**：トンネルインターフェイス • **Vlan**：Catalyst VLAN • **brief**：ポリシーマップの簡単な説明 • **class**：各クラスの統計情報 • **input**：入力ポリシー • **output**：出力ポリシー

コマンド	説明
	• **Wireless**：ワイヤレス
show policy-map interface wireless ap [*access point*]	のすべてのワイヤレス AP のランタイムと統計情報を表示します。
show policy-map interface wireless ssid [*ssid*]	のすべての SSID ターゲットのランタイムと統計情報を表示します。
show policy-map interface wireless client mac [*mac_address*]	のすべてのクライアント ターゲットのランタイムと統計情報を表示します。
show policy-map session [**input** | **output** | **uid** *UUID*]	セッションのQoSポリシーを表示します。コマンドパラメータは次のとおりです。 • **input**：入力ポリシー • **output**：出力ポリシー • **uid**：SSS 固有の ID に基づくポリシー
show policy-map type control subscriber { **all** | **name** }	タイプ QoS ポリシー マップを表示します。
show table-map	すべてのテーブルマップと設定を表示します。
show platform qos wireless {**afd** { **client** | **ssid** } | **stats** { **bssid** *bssid-value* | **client** *name* | **ssid** {*ssid-value* | **all**} **client all**}}	ワイヤレスのターゲットが表示されます。次のコマンド パラメータがサポートされています。 • afd：AFD 情報 • stats：統計情報
showpolicy-mapinterface wireless ssid name *ssid-name* [**radio type** {**24ghz** | **5ghz**} **ap name** *ap-name* | **ap name** *ap-name*]	アクセス ポイントの SSID ポリシー設定を表示します。
show wireless client mac-address *mac_address***service-policy** {**input** | **output**}	クライアントポリシーの詳細を表示します。

コマンド	説明
show wlan qos service-policies	すべての WLAN に設定された SSID ポリシーを表示します。
show ap name *ap_name***service-policy**	AP 上に設定されているポリシーをすべて表示します。

QoS の設定例

例：アクセス コントロール リストによる分類

この例は、アクセス コントロール リスト（ACL）を使用して QoS のパケットを分類する方法を示しています。

```
Device# configure terminal
Device(config)# access-list 101 permit ip host 12.4.1.1 host 15.2.1.1
Device(config)# class-map acl-101
Device(config-cmap)# description match on access-list 101
Device(config-cmap)# match access-group 101
Device(config-cmap)#
```

ACL を使用してクラスマップを作成した後で、クラスのポリシー マップを作成し、ポリシー マップを QoS のインターフェイスに適用します。

関連トピック

トラフィック クラスの作成（CLI）（1590 ページ）
クラス マップ（1560 ページ）

例：サービス クラス レイヤ 2 の分類

この例は、サービス クラス レイヤ 2 の分類を使用して QoS に対してパケットを分類する方法を示しています。

```
Device# configure terminal
Device(config)# class-map cos
Device(config-cmap)# match cos ?
  <0-7>  Enter up to 4 class-of-service values separated by white-spaces
Device(config-cmap)# match cos 3 4 5
Device(config-cmap)#
```

CoS レイヤ 2 の分類を使用してクラス マップを作成したら、そのクラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：サービス クラス DSCP の分類

この例は、サービス クラス DSCP の分類を使用して、QoS に対してパケットを分類する方法を示しています。

```
Device# configure terminal
Device(config)# class-map dscp
Device(config-cmap)# match dscp af21 af22 af23
Device(config-cmap)#
```

DSCP 分類を使用してクラス マップを作成したら、クラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：VLAN ID レイヤ 2 の分類

この例は、VLAN ID レイヤ 2 の分類を使用して QoS に分類する方法を示しています。

```
Device# configure terminal
Device(config)# class-map vlan-120
Device(config-cmap)# match vlan ?
  <1-4095>  VLAN id
Device(config-cmap)# match vlan 120
Device(config-cmap)#
```

VLAN レイヤ 2 の分類を使用してクラス マップを作成したら、クラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：DSCP 値または precedence 値による分類

この例は、DSCP 値または precedence 値を使用してパケットを分類する方法を示しています。

```
Device# configure terminal
Device(config)# class-map prec2
Device(config-cmap)# description matching precedence 2 packets
Device(config-cmap)# match ip precedence 2
Device(config-cmap)# exit
Device(config)# class-map ef
Device(config-cmap)# description EF traffic
Device(config-cmap)# match ip dscp ef
Device(config-cmap)#
```

DSCP 値または precedence 値を使用してクラス マップを作成したら、クラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：階層型分類

次の例は、childという名前の別のクラスに一致するparentという名前のクラスが作成される、階層型分類を示しています。childという名前のクラスは、2に設定されたIP precedenceに基づいて照合されます。

```
Device# configure terminal
Device(config)# class-map child
Device(config-cmap)# match ip precedence 2
Device(config-cmap)# exit
Device(config)# class-map parent
Device(config-cmap)# match class child
Device(config-cmap)#
```

親クラス マップを作成したら、クラスのポリシー マップを作成し、QoSのインターフェイスにポリシー マップを適用します。

関連トピック

階層型 QoS （1551 ページ）

例：階層型ポリシーの設定

次の例は、階層型ポリシーを使用した設定を示しています。

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# match dscp 30
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# match precedence 4
Device(config-cmap)# exit

Device(config)# class-map c3
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop

Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
```

```
Device(config-pmap-c)# service-policy child
Device(config-pmap-c)# end
```

次の例は、テーブル マップを使用した階層型ポリシーを示しています。

```
Device(config)# table-map dscp2dscp
 Device(config-tablemap)# default copy
Device(config)# table-map dscp2up
Device(config-tablemap)# map from 46 to 6
Device(config-tablemap)# map from 34 to 5
Device(config-tablemap)# default copy
Device(config)# policy-map ssid_child_policy
Device(config-pmap)# class voice
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 15000000
Device(config-pmap)# class video
Device(config-pmap-c)# priority level 2
Device(config-pmap-c)# police 10000000
Device(config)# policy-map ssid_policy
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 30000000
Device(config-pmap-c)# queue-buffer ratio 0
Device(config-pmap-c)# set dscp dscp table dscp2dscp
Device(config-pmap-c)# service-policy ssid_child_policy
```

関連トピック

階層型 QoS （1551 ページ）

例：音声およびビデオの分類

この例は、デバイス固有の情報を使用して、音声とビデオのパケット ストリームを分類する方法を示しています。

この例では、音声とビデオがエンドポイント A からデバイスの GigabitEthernet1/0/1 に送信され、それぞれ precedence 値 5 と 6 を持ちます。また、音声とビデオは、エンドポイント B からデバイスの GigabitEthernet1/0/2 にそれぞれ DSCP 値 EF と AF11 で送信されます。

両方のインターフェイスからのすべてのパケットがアップリンク インターフェイスに送信されます。その場合、音声は 100 Mbps にポリシングし、ビデオは 150 Mbps にポリシングする必要があります。

上記の要件ごとに分類するために、GigabitEthernet1/0/1 で送信される音声パケットに一致するクラスが作成されます。これには、precedence 5 に一致する voice-interface-1 という名前が付けらます。同様に、GigabitEthernet1/0/2 の音声パケットに一致する、voice-interface-2 という名前の音声用の別のクラスが作成されます。これらのクラスは、GigabitEthernet1/0/1 に接続される input-interface-1 と、GigabitEthernet1/0/2 に接続される input-interface-2 という 2 つの別個のポリシーに関連付けられます。このクラスのアクションは、qos-group に 10 とマーキングすることです。出力インターフェイスで QoS-group 10 のパケットを照合するために、QoS-group 10 で一致する voice という名前のクラスが作成されます。これは、output-interface という名前の別のポリシーに関連付けられ、アップリンク インターフェイスに関連付けられます。ビデオも同じ方法で処理されますが、QoS-group 20 で一致します。

次の例は、上記のデバイス固有の情報を使用して分類する方法を示しています。

```
Device(config)#
Device(config)# class-map voice-interface-1
Device(config-cmap)# match ip precedence 5
Device(config-cmap)# exit

Device(config)# class-map video-interface-1
Device(config-cmap)# match ip precedence 6
Device(config-cmap)# exit

Device(config)# class-map voice-interface-2
Device(config-cmap)# match ip dscp ef
Device(config-cmap)# exit

Device(config)# class-map video-interface-2
Device(config-cmap)# match ip dscp af11
Device(config-cmap)# exit

Device(config)# policy-map input-interface-1
Device(config-pmap)# class voice-interface-1
Device(config-pmap-c)# set qos-group 10
Device(config-pmap-c)# exit

Device(config-pmap)# class video-interface-1
Device(config-pmap-c)# set qos-group 20

Device(config-pmap-c)# policy-map input-interface-2
Device(config-pmap)# class voice-interface-2
Device(config-pmap-c)# set qos-group 10
Device(config-pmap-c)# class video-interface-2
Device(config-pmap-c)# set qos-group 20
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# class-map voice
Device(config-cmap)# match qos-group 10
Device(config-cmap)# exit

Device(config)# class-map video
Device(config-cmap)# match qos-group 20

Device(config)# policy-map output-interface
Device(config-pmap)# class voice
Device(config-pmap-c)# police 256000 conform-action transmit exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class video
Device(config-pmap-c)# police 1024000 conform-action transmit exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit
```

例：音声、ビデオ、およびマルチキャストトラフィックで分類されたワイヤレス QoS ポリシー

次の例では、音声とビデオのトラフィックの Quality of Service を管理するポートの子ポリシーを作成するテンプレートを示します。

```
Policy-map port_child_policy
    Class voice (match dscp ef)
            Priority level 1
            Police  Multicast Policer
    Class video (match dscp af41)
            Priority level 2
            Police  Multicast Policer
    Class mcast-data  (match non-client-nrt)
            Bandwidth remaining ratio <>
    Class class-default  (NRT Data)
            Bandwidth remaining ratio <>
```

（注） 上記の例のマルチキャスト ポリサーはキーワードではありません。これは設定されたポリシング ポリシーを示しています。

名前の音声とビデオを使用する 2 つのクラス マップは、46 および 34 の DSCP の割り当てで設定されます。音声トラフィックにはプライオリティ 1 が割り当てられ、ビデオ トラフィックにはプライオリティ レベル 2 が割り当てられ、Q0 および Q1 を使用して処理されます。ネットワークがマルチキャスト音声およびビデオ トラフィックを受信すると、マルチキャストのポリサーを設定できます。非クライアント NRT データおよび NRT データは Q2 および Q3 キューで処理されます。

関連トピック

ポート ポリシー （1547 ページ）
ポート ポリシーの形式 （1547 ページ）
ワイヤレス QoS マルチキャスト （1563 ページ）

例：ダウンストリーム SSID ポリシーの設定

ダウンストリーム BSSID ポリシーを設定するには、最初にプライオリティ レベルのキューイングでポートの子ポリシーを設定する必要があります。

ポリシーのタイプ。	例

ユーザ定義のポートの子ポリシー	`policy-map port_child_policy`
	`class voice`
	`priority level 1 20000`
	
	`class video`
	`priority level 2 10000`
	
	`class non-client-nrt-class`
	`bandwidth remaining ratio 10`
	
	`class class-default`
	`bandwidth remaining ratio 15`

ポリシーのタイプ。	例

出力 BSSID ポリシー	`policy-map bssid-policer`
	`  queue-buffer ratio 0`
	`  class class-default`
	`  shape average 30000000`
	`set dscp dscp table dscp2dscp`
	`set wlan user-priority dscp table dscp2up`
	`service-policy ssid_child_qos`

SSID の子 QoS ポリシー	`Policy Map ssid-child_qos`
	`  Class voice`
	`  priority level 1`
	`  police cir 5m`
	`  admit cac wmm-tspec`
	`  UP 6,7  / tells WCM allow 'voice'`
	` TSPEC\SIP snoop for this ssid`
	`  rate 4000 / must be police rate`
	` value is in kbps)`
	`  Class video`
	`  priority level 2`
	`  police cir 60000`

関連トピック

WLAN での SSID またはクライアント ポリシーの適用（CLI）（1608 ページ）
SSID ポリシー（1550 ページ）

例：入力 SSID ポリシー

次に、入力 SSID の階層型ポリシーの例を示します。

入力 SSID ポリシーの種類	例

入力 SSID の階層型ポリシー	`policy-map ssid-child-policy`
	`class voice  //match dscp 46`
	`police 3m`
	`class video //match dscp 34`
	`police 4m`
	`policy-map ssid-in-policy`
	`class class-default`
	`set dscp wlan user-priority table up2dscp`
	`service-policy ssid-child-policy`

	`policy-map ssid_in_policy`
	`class dscp-40`
	`set cos 1`
	`police 10m`
	`class up-1`
	`set dscp 34`
	`police 12m`
	`class dscp-10`
	`set dscp 20`
	`police 15m`
	`class class-default`
	`set dscp wlan user-priority table up2dscp`
	
	`police 50m`

例：クライアント ポリシー

クライアント ポリシーの種類	例/詳細

デフォルトの出力クライアント ポリシー	すべての着信トラフィックのユーザプライオリティは 0 です。
	（注） デフォルトのクライアント ポリシーは、ACM イネーブルの WMM クライアント上でのみイネーブルにされます。
	show ap dot11 5ghz network コマンドを使用して、ACM がイネーブルにされているかどうかの確認が出来ます。ACM をイネーブルにするには、**ap dot11 5ghz cac voice acm** コマンドを使用します。
	
	`Policy-map client-def-down`
	`  class class-default`
	`  set wlan user-priority 0`

クライアント ポリシーの種類	例/詳細

デフォルトの入力クライアント ポリシー	ワイヤレス ネットワークから有線ネットワークに送信されるトラフィックは、DSCP 値が 0 に設定されます。
	（注） デフォルトのクライアント ポリシーは、ACM イネーブルの WMM クライアント上でのみイネーブルにされます。
	`Policy-map client-def-up`
	`  class class-default`
	`  set dscp 0`

設定された QoS レベル属性を使用してクライアントが AAA のプロファイルに認証する際に、自動的に生成され、WMM クライアントに適用されるクライアント ポリシー。	`Policy Map platinum-WMM`
	`Class voice-plat`
	`  set wlan user-priority 6`
	`Class video-plat`
	`set wlan user-priority 4`
	`Class class-default`
	`  set wlan user-priority 0`
	
	`Policy Map gold-WMM`
	`Class voice-gold`
	`  set wlan user-priority 4`
	`Class video-gold`
	`set wlan user-priority 4`
	`Class class-default`
	`  set wlan user-priority 0`

非 WMM クライアントの貴金属ポリシー	`Policy Map platinum` `  set wlan user-priority 6`

トラフィックがクラス voice1 と一致し、ユーザプライオリティが事前定義の値に設定された出力クライアント ポリシー。	クラスは DSCP または ACL を割り当てるように設定できます。
	`Policy Map client1-down`
	`Class voice1  //match dscp, cos`
	`  set wlan user-priority <>`
	`Class voice2  //match acl`
	`  set wlan user-priority <>`
	`Class voice3`
	`  set wlan user-priority <>`
	`Class class-default`
	`  set wlan user-priority 0`

クライアント ポリシーの種類	例/詳細

AAA および TCLAS に基づくクライアント ポリシー	`Policy Map client2-down[ AAA+ TCLAS pol example]`
	`Class voice\\match dscp`
	`police <>`
	`set <>`
	`Class class-default`
	`set <>`
	`Class voice1|| voice2 [match acls]`
	`police <>`
	`class voice1`
	`set <>`
	`class voice2`
	`set <>`

出力方向のトラフィック用の音声とビデオのクライアント ポリシー	`Policy Map client3-down`
	`class voice \\match dscp, cos`
	`police X`
	`class video`
	`police Y`
	`class class-default`
	`police Z`

ポリシングを使用する入力方向のトラフィック用の音声とビデオのクライアント ポリシー	`Policy Map client1-up`
	`class voice \\match dscp, up, cos`
	`police X`
	`class video`
	`police Y`
	`class class-default`
	`police Z`

DSCP に基づく音声とビデオのクライアント ポリシー	`Policy Map client2-up`
	`class voice \\match dscp, up, cos`
	`set dscp <>`
	`class video`
	`set dscp <>`
	`class class-default`
	`set dscp <>`

マーキングおよびポリシングを使用したクライアント入力ポリシー	`policy-map client_in_policy`
	`class dscp-48 //match dscp 48`
	`set cos 3`
	`police 2m`
	`class up-4 //match wlan user-priority 4`
	`set dscp 10`
	`police 3m`
	`class acl //match acl`
	`set cos 2`
	`police 5m`
	`class class-default`
	`set dscp 20`
	`police 15m`

クライアント ポリシーの種類	例/詳細

階層型クライアント入力ポリシー	`policy-map client-child-policy`
	`class voice  //match dscp 46`
	`set dscp 40`
	`police 5m`
	`class video //match dscp 34`
	`set dscp 30`
	`police 7m`
	`policy-map client-in-policy`
	`class class-default`
	`police 15m`
	`service-policy client-child-policy`

関連トピック

クライアント ポリシーの設定（CLI）
クライアント ポリシー （1550 ページ）

例：平均レート シェーピングの設定

次の例は、平均レート シェーピングを設定する方法を示しています。

```
Device# configure terminal
Device(config)# class-map prec1
Device(config-cmap)# description matching precedence 1 packets
Device(config-cmap)# match ip precedence 1
Device(config-cmap)# end

Device# configure terminal
Device(config)# class-map prec2
Device(config-cmap)# description matching precedence 2 packets
Device(config-cmap)# match ip precedence 2
Device(config-cmap)# exit

Device(config)# policy-map shaper
Device(config-pmap)# class prec1
Device(config-pmap-c)# shape average 512000
Device(config-pmap-c)# exit

Device(config-pmap)# policy-map shaper
Device(config-pmap)# class prec2
Device(config-pmap-c)# shape average 512000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1024000
```

クラス マップ、ポリシー マップ、シェーピング平均を設定したら、QoS のインターフェイスにポリシー マップを適用します。

関連トピック

シェーピングの設定（CLI） （1643 ページ）

平均レート シェーピング （1570 ページ）

例：キュー制限の設定

次の例は、DSCP 値および割合に基づいて、キュー制限ポリシーを設定する方法を示しています。

```
Device# configure terminal
Device#(config)# policy-map port-queue
Device#(config-pmap)# class dscp-1-2-3
Device#(config-pmap-c)# bandwidth percent 20
Device#(config-pmap-c)# queue-limit dscp 1 percent 80
Device#(config-pmap-c)# queue-limit dscp 2 percent 90
Device#(config-pmap-c)# queue-limit dscp 3 percent 100
Device#(config-pmap-c)# exit

Device#(config-pmap)# class dscp-4-5-6
Device#(config-pmap-c)# bandwidth percent 20
Device#(config-pmap-c)# queue-limit dscp 4 percent 20
Device#(config-pmap-c)# queue-limit dscp 5 percent 30
Device#(config-pmap-c)# queue-limit dscp 6 percent 20
Device#(config-pmap-c)# exit

Device#(config-pmap)# class dscp-7-8-9
Device#(config-pmap-c)# bandwidth percent 20
Device#(config-pmap-c)# queue-limit dscp 7 percent 20
Device#(config-pmap-c)# queue-limit dscp 8 percent 30
Device#(config-pmap-c)# queue-limit dscp 9 percent 20
Device#(config-pmap-c)# exit

Device#(config-pmap)# class dscp-10-11-12
Device#(config-pmap-c)# bandwidth percent 20
Device#(config-pmap-c)# queue-limit dscp 10 percent 20
Device#(config-pmap-c)# queue-limit dscp 11 percent 30
Device#(config-pmap-c)# queue-limit dscp 12 percent 20
Device#(config-pmap-c)# exit

Device#(config-pmap)# class dscp-13-14-15
Device#(config-pmap-c)# bandwidth percent 10
Device#(config-pmap-c)# queue-limit dscp 13 percent 20
Device#(config-pmap-c)# queue-limit dscp 14 percent 30
Device#(config-pmap-c)# queue-limit dscp 15 percent 20
Device#(config-pmap-c)# end
Device#
```

上記のポリシーマップのキュー制限の設定が終了すると、QoS のインターフェイスにポリシーマップを適用することができます。

関連トピック

キュー制限の設定（CLI） （1640 ページ）
重み付けテール ドロップ （1573 ページ）

例：キュー バッファの設定

次の例は、キュー バッファ ポリシーを設定して QoS のインターフェイスに適用する方法を示しています。

```
Device# configure terminal
Device(config)# policy-map policy1001
Device(config-pmap)# class class1001
Device(config-pmap-c)# bandwidth remaining ratio 10
Device(config-pmap-c)# queue-buffer ratio ?
  <0-100>  Queue-buffers ratio limit
Device(config-pmap-c)# queue-buffer ratio 20
Device(config-pmap-c)# end

Device# configure terminal
Device(config)# interface gigabitEthernet2/0/3
Device(config-if)# service-policy output policy1001
Device(config-if)# end
```

関連トピック

キュー バッファの設定（CLI）（1637 ページ）
キュー バッファの割り当て（1575 ページ）

例：ポリシング アクションの設定

次の例は、ポリサーに関連付けることができるさまざまなポリシングアクションを示しています。これらのアクションは、パケット設定の適合、超過、または違反によって実現されます。トラフィック プロファイルを超過または違反したパケットをドロップ、マーク付け、または送信することができます。

たとえば、1 つの一般的な導入シナリオでは、エンタープライズ顧客ポリシー トラフィックがネットワークからサービス プロバイダーに送信され、DSCP 値が異なる、適合、超過、および違反パケットをマーキングします。サービス プロバイダーは、輻輳があると DSCP 値の超過および違反としてマーキングされたパケットをドロップすることができますが、使用可能な帯域幅がある場合は送信することも可能です。

（注） Layer 2 フィールドには CoS フィールドが含まれるようにマーキングでき、Layer 3 フィールドには precedence および DSCP フィールドが含まれるようにマーキングできます。

1 つの便利な機能として、複数のアクションとイベントを関連付ける機能があります。たとえば、すべての適合パケットについて、precedence ビットと CoS を設定できます。アクションを設定するサブモードは、ポリシング機能によって配信できます。

これは、ポリシング アクションの設定例を示しています。

```
Device# configure terminal
Device(config)# policy-map police
```

```
Device(config-pmap)# class class-default
Device(config-pmap-c)# police cir 1000000 pir 2000000
Device(config-pmap-c-police)# conform-action transmit
Device(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table
exceed-markdown-table
Device(config-pmap-c-police)# violate-action set-dscp-transmit dscp table
violate-markdown-table
Device(config-pmap-c-police)# end
```

この例では、exceed-markdown-table と violate-mark-down-table がテーブル マップです。

（注） ポリサー ベースのマークダウン アクションは、テーブル マップを使用する場合のみサポートされます。デバイスの各マーキング フィールドで許可されているマークダウン テーブル マップは 1 つだけです。

関連トピック

ポリシングの設定（CLI） （1631 ページ）
ポリシング （1563 ページ）

例：ポリサーの VLAN 設定

次の例では、VLANのポリサー設定を表示します。この設定の最後に、QoSのインターフェイスに VLAN ポリシー マップを適用します。

```
Device# configure terminal
Device(config)# class-map vlan100
Device(config-cmap)# match vlan 100
Device(config-cmap)# exit
Device(config)# policy-map vlan100
Device(config-pmap)# policy-map class vlan100
Device(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Device(config-pmap-c-police)# end
Device# configure terminal
Device(config)# interface gigabitEthernet1/0/5
Device(config-if)#  service-policy input vlan100
```

関連トピック

ポリシーマップによるSVIのトラフィックの分類、ポリシング、およびマーキング（CLI）（1613 ページ）
VLAN のポリシー マップ （1563 ページ）

例：ポリシングの単位

次の例は、QoS でサポートされるポリシングのさまざまな単位を示しています。ポリシングの単位はトークン バケットが動作する基盤です。

次の単位のポリシングがサポートされています。

- CIR および PIR はビット/秒で指定します。バースト パラメータはバイト単位で指定します。これはデフォルトのモードであり、単位が指定されていない場合に使用される単位です。CIR および PIR は、パーセントでも設定できます。その場合バースト パラメータをミリ秒単位で設定する必要があります。
- CIR および PIR はパケット/秒で指定します。この場合、バースト パラメータもパケットで設定されます。

次の例は、ビット/秒のポリサー設定を示しています。

```
Device(config)# policy-map bps-policer
Device(config-pmap)# class class-default
Device(config-pmap-c) # police rate 256000 bps burst 1000 bytes
conform-action transmit exceed-action drop
```

次の例は、パケット/秒のポリサー設定を示しています。この設定では、測定単位がパケットであるデュアル レートの 3 カラー ポリサーが設定されます。バーストおよびピーク バーストはすべてパケットに指定されます。

```
Device(config)# policy-map pps-policer
Device(config-pmap)# class class-default
Device(config-pmap-c)# police rate 5000 pps burst 100 packets
peak-rate 10000 pps peak-burst 200 packets conform-action transmit
exceed-action drop violate-action drop
```

関連トピック

ポリシングの設定（CLI）（1631 ページ）
トークンバケット アルゴリズム（1564 ページ）

例：シングルレート 2 カラー ポリシング設定

次の例は、シングルレート 2 カラー ポリサーを設定する方法を示しています。

```
Device(config)# class-map match-any prec1
Device(config-cmap)# match ip precedence 1
Device(config-cmap)# exit
Device(config)# policy-map policer
Device(config-pmap)# class prec1
Device(config-pmap-c)# police cir 256000 conform-action transmit exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)#
```

関連トピック

ポリシングの設定（CLI）（1631 ページ）
シングルレート 2 カラー ポリシング（1568 ページ）

例：デュアルレート 3 カラー ポリシング設定

次の例は、デュアルレート 3 カラー ポリサーを設定する方法を示しています。

```
Device# configure terminal
Device(config)# policy-Map dual-rate-3color-policer
Device(config-pmap)# class class-default
Device(config-pmap-c)# police cir 64000 bc 2000 pir 128000 be 2000
Device(config-pmap-c-police)# conform-action transmit
Device(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table
exceed-markdown-table
Device(config-pmap-c-police)# violate-action set-dscp-transmit dscp table
violate-markdown-table
Device(config-pmap-c-police)# exit
Device(config-pmap-c)#
```

この例では、exceed-markdown-table と violate-mark-down-table がテーブル マップです。

（注） ポリサー ベースのマークダウン アクションは、テーブル マップを使用する場合のみサポートされます。デバイスの各マーキング フィールドで許可されているマークダウン テーブル マップは 1 つだけです。

関連トピック

ポリシングの設定（CLI） （1631 ページ）
デュアルレート 3 カラー ポリシング （1569 ページ）

例：テーブル マップのマーキング設定

次のステップと例は、QoS設定でテーブルマップ マーキングを使用する方法を示しています。

1. テーブル マップを定義します。

   table-map コマンドを使用してテーブル マップを定義し、値のマッピングを示します。このテーブルでは、テーブルが使用されるポリシーまたはクラスを認識しません。テーブル マップのデフォルトのコマンドは、一致する「from」フィールドがない場合に、「to」フィールドにコピーされる値を示します。この例では、table-map1 というテーブル マップが作成されます。定義されたマッピングでは、値 0 が 1 に、2 が 3 に変換され、デフォルト値は 4 に設定されます。

```
Device(config)# table-map table-map1
Device(config-tablemap)# map from 0 to 1
Device(config-tablemap)# map from 2 to 3
Device(config-tablemap)# default 4
Device(config-tablemap)# exit
```

2. テーブル マップが使用されるポリシー マップを定義します。

この例では、着信 CoS が table-map1 テーブルで指定されたマッピングに基づいて、DSCP にマッピングされます。この例では、着信パケットの DSCP が 0 である場合、パケット内の CoS は 1 に設定されます。テーブル マップ名が指定されていない場合、このコマンドではデフォルトの動作が実行され、値が「from」フィールド（この場合は DSCP）から「to」フィールド（この場合は CoS）にコピーされます。ただし、CoS が 3 ビット フィールドであっても DSCP は 6 ビット フィールドです。これは、DSCP 内の最初の 3 ビットに CoS がコピーされることを意味します。

```
Device(config)# policy map policy1
Device(config-pmap)# class class-default
Device(config-pmap-c)# set cos dscp table table-map1
Device(config-pmap-c)# exit
```

3. ポリシーをインターフェイスに関連付けます。

```
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# service-policy output policy1
Device(config-if)# exit
```

関連トピック

テーブル マップの設定（CLI）（1617 ページ）
テーブル マップのマーキング（1565 ページ）

例：CoS マーキングを保持するテーブル マップの設定

次の例は、テーブル マップを使用して、QoS 設定のインターフェイスで CoS マーキングを保持する方法を示しています。

（例で設定されている）cos-trust-policy ポリシーは入力方向でイネーブルになり、インターフェイスに着信する CoS マーキングが保持されます。ポリシーがイネーブルになっていない場合は、デフォルトで DSCP だけが信頼されます。純粋なレイヤ 2 パケットがインターフェイスに着信すると、CoS の入力ポートに一致するポリシーがない場合は、CoS 値が 0 に書き換えられます。

```
Device# configure terminal
Device(config)# table-map cos2cos
Device(config-tablemap)# default copy
Device(config-tablemap)# exit


Device(config)# policy map cos-trust-policy
Device(config-pmap)# class class-default
Device(config-pmap-c)# set cos cos table cos2cos
Device(config-pmap-c)# exit

Device(config)# interface GigabitEthernet1/0/2
Device(config-if)# service-policy input cos-trust-policy
Device(config-if)# exit
```

関連トピック

有線およびワイヤレス ポートの信頼動作 （1577 ページ）

次の作業

QoS 設定でこれらの自動機能を使用できるかどうかについては、自動 QoS のマニュアルを参照してください。

QoS に関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	『*QoS Command Reference (Catalyst 3850 Switches)*』 『*Cisco IOS Quality of Service Solutions Command Reference*』
コール アドミッション制御（CAC）	『*System Management Configuration Guide (Catalyst 3850 Switches)*』 『*System Management Command Reference (Catalyst 3850 Switches)*』
マルチキャスト シェーピングおよびポリシング レート	『*IP Multicast Routing Configuration Guide (Catalyst 3850 Switches)*』
Application Visibility and Control（アプリケーションの可視性およびコントロール）	『*System Management Configuration Guide (Catalyst 3850 Switches)*』 *System Management Command Reference (Catalyst 3850 Switches)*
Application Visibility and Control（アプリケーションの可視性およびコントロール）	『*System Management Configuration Guide (Catalyst 3850 Switches)*』 *System Management Command Reference (Catalyst 3850 Switches)*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
—	

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

QoS の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。
Cisco IOS XE 3.3SE	有線ポートとワイヤレス ポートの両方における一貫して信頼できるシステム デフォルトの信頼動作。 Cisco IOS XE 3.2 リリースは、有線およびワイヤレス ポートに対して信頼できるさまざまなデフォルト設定をサポートしました。有線ポートの信頼できるデフォルト設定に関して、このソフトウェア リリースでの変更はありません。ワイヤレス ポートの場合、デフォルトのシステム動作は非信頼でした。つまり、の起動時に、ワイヤレス ポートのマーキングすべてがデフォルトでゼロに設定され、トラフィックはプライオリティ処理されませんでした。既存の有線との互換性のために、すべてのトラフィックはデフォルトでベスト エフォートのキューへ送信されていました。アクセス ポイントは、プライオリティ キューイングをデフォルトで実行していました。 ワイヤレス ポートでのデフォルトの信頼動作は、**noqoswirelessdefaultuntrust** コマンドを使用して変更できます。

リリース	変更内容
Cisco IOS XE 3.3SE	IPv6 ワイヤレス クライアントのサポート。 Cisco IOS XE 3.2 ソフトウェア リリースは、ワイヤレス クライアントに対して IPv6 をサポートしていませんでした。新しいリリースでは、これをサポートしています。クライアント ポリシーは、IPv4 および IPv6 フィルタを設定できるようになりました。
Cisco IOS XE 3.3SE	3 つの無線と 11ac のサポート。
Cisco IOS XE 3.3SE	**show policy-map** コマンドで使用可能な新しい分類カウンタ。 （注） この機能は、有線ターゲットでのみ使用できます。
Cisco IOS XE 3.6E	入力 SSID ポリシーのマーキングおよびポリシング アクション。クライアント ポリシーはアクセス ポイントで適用されます。
Cisco IOS XE 3.6E	ワイヤレス ターゲット用に **show policy-map** コマンドで使用可能な新しい分類カウンタ。
Cisco IOS XE 3.6E	統計情報は、入力ポリシーでだけサポートされます。

第 XV 部

無線リソース管理

- 無線リソース管理の設定 （1673 ページ）
- Cisco 2800/3800 シリーズ アクセス ポイントの XOR スロットの設定 （1711 ページ）
- Cisco 2800/3800 シリーズ アクセス ポイントの Flexible Radio Assignment の設定 （1715 ページ）
- 設定の最適化されたローミング （1725 ページ）
- 設定の Rx SOP （1729 ページ）
- AirTime Fairness の設定 （1731 ページ）
- CA での RF プロファイルの設定 （1737 ページ）

第 83 章

無線リソース管理の設定

- 機能情報の確認 （1673 ページ）
- 無線リソース管理の設定の前提条件 （1673 ページ）
- 無線リソース管理の制約事項 （1674 ページ）
- 無線リソース管理について （1674 ページ）
- RRM の設定方法 （1683 ページ）
- RRM パラメータと RF グループ ステータスの監視 （1705 ページ）
- 例：RF グループの設定 （1707 ページ）
- ED-RRM について （1708 ページ）
- 無線リソース管理に関するその他の参考ドキュメント （1709 ページ）
- 無線リソース管理の設定を行うための機能履歴と情報 （1710 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

無線リソース管理の設定の前提条件

無線リソース管理を設定するには、デバイスをモビリティ アンカーではなくモビリティ コントローラとして設定する必要があります。また、ホーム AP で動的なチャネル割り当て機能のサポートが必要な場合があります。

RRM を機能させるには、モビリティ コントローラとモビリティ エージェントを含む新しいモビリティ アーキテクチャをスイッチまたはコントローラで設定する必要があります。

（注） モビリティコントローラとモビリティエージェントの設定については、『Mobility Configuration Guide』を参照してください。

無線リソース管理の制約事項

RF グループの AP の数は 500 に限定されています。

AP の最大数をすでに保持している RF グループに AP が join しようとすると、デバイスはアプリケーションを拒否し、エラーをスローします。

Ap の通信時間公平性モードを有効にするには、ポリシー識別モードを無効にしてから再度適用する必要があります。これは、すべての AP に対し通信時間の公平性の設定を変更します。また **ap name <ap-name> dot11 24ghz airtime-fairness mode enforce-policy** コマンドを使用して、個々の AP の通信時間の公平性のモードを変更できます。

無線リソース管理について

無線リソース管理（RRM）ソフトウェアはデバイスに組み込まれており、ワイヤレス ネットワークのリアルタイムでの RF 管理を常時提供する組み込みの RF エンジニアとして機能します。RRM を使用すると、デバイスは次の情報について、アソシエートされている Lightweight アクセス ポイントを継続的に監視できます。

- トラフィックの負荷：トラフィックの送受信に使用される帯域幅の合計量。これにより、無線 LAN 管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越して計画を立てることができます。
- 干渉：他の 802.11 発信元から送られてくるトラフィック量。
- ノイズ：現在割り当てられているチャネルに干渉している 802.11 以外のトラフィック量。
- カバレッジ：接続されているすべてのクライアントの受信信号強度インジケータ（RSSI）と信号対雑音比（SNR）。
- その他：近くにあるアクセス ポイントの数。

RRM は次の機能を実行します。

- 無線リソースの監視
- 送信電力の制御
- チャネルの動的割り当て
- カバレッジ ホールの検出と修正
- RF グループ化

（注） RRM のグループ化は、AP が DCA チャネルのリストにないスタティック チャネルで動作するため、実行されません。NDP は、DCA チャネルでのみ送信され、無線が非 DCA チャネルで動作する場合、NDA はオンチャネルで受信しません。

無線リソースの監視

RRM は、ネットワークに追加された新しいデバイスや Lightweight アクセス ポイントを自動的に検出して設定します。その後、アソシエートされている近くの Lightweight アクセス ポイントを自動的に調整して、カバレッジとキャパシティを最適化します。

Lightweight アクセス ポイントでは、使用国で有効なすべての チャネルをスキャンできます。また、他の地域で使用可能なチャネルも同様です。ローカル モードのアクセス ポイントは、これらのチャネルのノイズと干渉を監視するために、最大で 60 ミリ秒の間「オフチャネル」になります。不正アクセス ポイント、不正クライアント、アドホック クライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。

（注） 音声トラフィックやその他の重要なトラフィックがある場合（過去 100 ミリ秒内）、アクセス ポイントはオフチャネル測定を延期できます。また、WLAN スキャンの延期プライオリティ設定に基づいて、延期されます。

各アクセス ポイントがオフチャネルになるのはすべての時間のわずか 0.2% です。この動作はすべてのアクセス ポイントに分散されるので、隣接するアクセス ポイントが同時にスキャンを実行して、無線 LAN のパフォーマンスに悪影響を及ぼすことはありません。

RRM では、モビリティ コントローラ（MC）およびモビリティ エージェント（MA）を含む RF グループ化の新しいモビリティ アーキテクチャがサポートされます。

- モビリティ コントローラ（MC）：Cisco WLC 5700 シリーズ コントローラ、Cisco Catalyst 3850 スイッチ、Cisco Unified Wireless Network ソリューションのコントローラは MC として機能できます。MC には、その中で内部的に実行されている MC 機能および MA 機能があります。
- モビリティ エージェント（MA）：モビリティ エージェントは、モバイル クライアント用のクライアント モビリティ ステート マシンを維持するコンポーネントです。

RF グループについて

RF グループは、無線単位でネットワークの計算を実行するために、グローバルに最適化された方法で RRM の実行を調整する Cisco WLC の論理的な集合です。802.11 ネットワーク タイプごとに RF グループが存在します。単一の RF グループに Cisco WLC をクラスタリングすることによって、RRM アルゴリズムは単一の Cisco WLC の機能を拡張できます。

RF グループは、次のパラメータに基づいて作成されます。

- ユーザ設定の RF ネットワーク名。
- 無線レベルで実行されるネイバー探索。
- MC に設定されている国のリスト。

MC 間で実行する RF グループ化。

Lightweight アクセス ポイントは、定期的にネイバー メッセージを無線で送信します。同じ RF グループ名を使用しているアクセス ポイントは、相互に送信されたメッセージを検証します。

検証されたネイバー メッセージを、異なるコントローラ上のアクセス ポイントが -80 dBm 以上の信号強度で受信すると、Cisco WLC によって自動モードの RF 領域が動的に形成されます。静的モードで、リーダーは手動で選択され、メンバが RF グループに追加されます。RF グループ モードに関する詳細については、「RF グループ リーダー」の項を参照してください。

（注） RF グループとモビリティ グループは、どちらも Cisco WLC のクラスタを定義するという点では同じですが、用途に関しては異なります。RF グループはスケーラブルでシステム全体にわたる動的な RF 管理を実現するのに対して、モビリティ グループはスケーラブルでシステム全体にわたるモビリティと Cisco WLC の冗長性を実現します。

RF グループ リーダー

7.0.116.0 のリリースから、RF グループ リーダーを次の 2 つの方法で設定することができます。

- 自動モード：このモードでは、RF グループのメンバによって、グループの「マスター」電力およびチャネル スキームを管理する RF グループ リーダーが選ばれます。RF グループ アルゴリズムは、RF グループ リーダーを動的に選択し、RF グループ リーダーが常に存在していることを確認します。グループ リーダーの割り当ては変更されることがあります（たとえば、現在の RF グループ リーダーが動作しなくなった場合、または RF グループ メンバが大幅に変更された場合）。
- 静的モード：このモードでは、ユーザは RF グループ リーダーとして Cisco WLC を手動で選択します。このモードでは、リーダーおよびメンバは手動で設定され、固定されます。メンバが RF グループに join できない場合は、理由が表示されます。リーダーは、メンバが前の試行で join しなかった場合、1 分ごとにメンバとの接続を確立しようとします。

RF グループ リーダーは、システムによって収集されたリアルタイムの無線データを分析して、パワーおよびチャネルの割り当てを算出し、RF グループの各 Cisco WLC に送信します。RRM アルゴリズムによって、システム全体の安定性が保証され、チャネルおよびパワー スキームの変更を適切なローカル RF 領域に制限します。

6.0 より前の Cisco WLC ソフトウェア リリースでは、動的チャネル割り当て（DCA）の検索アルゴリズムによって、RF グループの Cisco WLC にアソシエートされた無線について適切なチャネル計画を判別しますが、現在の計画よりも大幅に優れていない限り、新しいチャネル計画は適用されません。両方の計画で最も不適切な無線のチャネル メトリックにより、適用する計画

が決定されます。新しいチャネル計画を適用するための唯一の基準として最もパフォーマンスの低い無線を使用すると、ピンニングまたはカスケードの問題が発生する可能性があります。

ピンニングは、アルゴリズムによって RF グループの一部の無線に適したチャネル計画が検出されても、ネットワーク内の最も条件の悪い無線には適したチャネル オプションがないため、チャネル計画の変更は実施されないことを指します。RF グループ内の最も条件の悪い無線によって、グループ内の他の無線がより適切なチャネル計画を探すことができなくなる場合があります。ネットワークの規模が大きければ大きいほど、よりピンニングになりやすいです。

1 つの無線のチャネルが変更された場合に、RF 領域の残りの無線を最適化するため、連続してチャネル変更が行われると、カスケードが発生します。このような無線を最適化すると、ネイバーおよびネイバーのチャネル計画が次善のものになり、チャネル最適化が起動されます。この影響は、すべてのアクセス ポイント無線が同じ RF グループに属している場合、複数のフロアまたは複数の建物に広がることがあります。この変更は、大きなクライアントの混乱を引き起こし、ネットワークを不安定にします。

ピンニングとカスケードの主な原因は、新しいチャネル計画を検索する方法と、起こる可能性のあるチャネル計画の変更が単一の無線の RF 状態によって制御されていることです。Cisco WLC ソフトウェア リリース 6.0 の DCA アルゴリズムは、ピンニングとカスケードを回避するよう再設計されました。次の変更が実装されました。

- 複数のローカル検索：DCA 検索アルゴリズムでは、単一の無線による単一のグローバル検索ではなく、同じ DCA の処理内で異なる無線によって開始される複数のローカル検索が実行されます。この変更によって、ピンニングとカスケードの両方に対応できるだけでなく、安定性を損なうことなく、DCA に必要な柔軟性と適合性が維持されます。

- 複数のチャネル計画変更イニシエータ（CPCI）：以前は、最も条件の悪い単一の無線が、チャネル計画変更の唯一のイニシエータでした。しかし、RF グループ内の各無線が評価されて、イニシエータ候補として優先順位付けされるようになりました。生成されたリストはインテリジェントにランダム化されるので、最終的にすべての無線が評価され、ピンニングが発生する可能性はなくなります。

- チャネル計画変更の適用制限（ローカリゼーション）：各 CPCI 無線の場合、DCA アルゴリズムは適切なチャネル計画を求めてローカル検索を実行しますが、実際には CPCI 無線自身および 1 ホップ近隣のアクセス ポイントのみが現在の送信チャネルを変更できます。アクセス ポイントによるチャネル計画変更のトリガーの影響は、そのアクセス ポイントの 2 RF ホップ内だけで認識され、実際のチャネル計画変更は 1 ホップ RF 領域内に制限されます。この制限はすべての CPCI 無線にわたって適用されるため、カスケードが発生する可能性はありません。

- 非 RSSI ベースの累積コスト メトリック：累積コスト メトリックによって、全範囲、領域、またはネットワークが指定のチャネル計画でどの程度のパフォーマンスを示すのかを測定します。チャネル計画の品質全体を把握する目的で、その領域内にあるすべてのアクセス ポイントに関する個々のコスト メトリックが考慮されます。これらのメトリックの使用で、すべてのチャネル計画変更に単一の各無線の品質の向上または低下が含まれるようになります。その目的は、単一の無線の品質は向上するが、他の複数の無線のパフォーマンスが大幅に低下するような、チャネル計画変更を避けることです。

RRM アルゴリズムは、指定された更新間隔（デフォルトでは 600 秒）で実行されます。更新間隔の合間に、RF グループ リーダーは各 RF グループ メンバにキープアライブ メッセージを送信し、リアルタイムの RF データを収集します。

（注） 複数の監視間隔を使用することもできます。詳細については、「RRM の設定」の項を参照してください。

RF グループ名

Cisco WLC には RF グループ名が設定されます。この RF グループ名は、その Cisco WLC に join しているすべてのアクセス ポイントに送信され、アクセス ポイントでは、この名前がハッシュ MIC をネイバー メッセージで生成するための共有秘密として使用されます。RF グループを作成するには、グループに含めるすべての Cisco WLC に同じ RF グループ名を設定します。

Cisco WLC に join しているアクセス ポイントが別の Cisco WLC 上のアクセス ポイントから RF 伝送を受け取る可能性がある場合は、それらの Cisco WLC に同じ RF グループ名を設定する必要があります。アクセス ポイント間の RF 伝送を受信する可能性がある場合、802.11 干渉およびコンテンションをできるだけ回避するには、システム全体にわたる RRM が推奨されます。

モビリティ コントローラ

MC には、グループ リーダーまたはグループ メンバを指定できます。RF グループ化と他の MC とのグループ選出に基づいて、MC の 1 つは RF グループ リーダーとして動作することができます。RF リーダーを選出する優先順位は、コントローラまたはスイッチがサポートできる AP の最大数に基づきます。優先順位が最も高いのは 1 で、最も低いのは 5 です。

1. WiSM 2 コントローラ
2. Cisco WLC 5700 シリーズ コントローラ
3. WiSM 1 コントローラ
4. Catalyst 3850 シリーズ スイッチ
5. Catalyst 3650 シリーズ スイッチ

MC の 1 つが RRM グループ リーダーになる場合、残りの MC は RRM グループ メンバになります。RRM グループ メンバは、グループ リーダーに RF 情報を送信します。グループ リーダーはネットワークのチャネルおよび送信電力の計画を決定し、RF グループ メンバへ情報を戻します。MC は、MA に属する無線の電力計画を MA へ配信します。これらのチャネルおよび電力の計画は、最終的に個々の無線にまで配信されます。

（注） MC 内には MA の機能があります。

Mobility Agent

MA は、MC と通信します。MA と通信している場合は、MC にはスイッチ/コントローラの MAC または IP アドレスが含まれます。

MA は、MC によってポーリングされると、次の情報を提供します。

- 干渉またはノイズのデータ
- ネイバー データ
- 無線機能（サポートされているチャネル、電力レベル）
- 無線設定（電源、チャネル、チャネル幅）
- レーダー データ

MC は、スイッチ/コントローラ（MA）と次の情報を交換します。メッセージには次の内容が含まれます。

- 個々の無線の設定（チャネル、電源、チャネル幅）
- 個々の無線の現在の設定と RF 測定のポーリング要求
- グループ リーダーの更新

一方、MA は次のメッセージを MC に伝達します。

- 無線からの RF 測定（ロード、ノイズ、ネイバー情報など）
- 個々の無線の RF 機能と設定

MC から指示された場合、MA は無線のチャンネル、電源、チャネル幅を設定します。DFS、カバレッジ ホールの検出/緩和、静的なチャネル/電源の設定は、MA によって実行されます。

RF グループ内の不正アクセス ポイント検出について

Cisco WLC の RF グループを作成したら、不正アクセス ポイントを検出するように、Cisco WLC に接続されたアクセス ポイントを設定する必要があります。アクセス ポイントによって、近隣のアクセス ポイントのメッセージ内のビーコン/プローブ応答フレームが選択され、RF グループの認証情報要素（IE）と一致するものが含まれているかどうかが確認されます。選択が正常に終了すると、フレームは認証されます。正常に終了しなかった場合は、認証されているアクセス ポイントによって、近隣のアクセス ポイントが不正アクセス ポイントとして報告され、その BSSID が不正テーブルに記録されます。さらに、このテーブルは Cisco WLC に送信されます。

送信電力の制御

デバイスは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。

送信電力制御（TPC）アルゴリズムによって、RF 環境での変化に応じて、アクセス ポイントの電力が増減します。多くの場合、TPC は干渉を低減させるため、アクセス ポイントの電力を下げようとします。しかし、アクセス ポイントで障害が発生したり、アクセス ポイントが無効になったりして、RF カバレッジに急激な変化があると、TPC は周囲のアクセス ポイントで電力を上げることもあります。この機能は、主にクライアントと関係があるカバレッジホールの検出とは異なります。TPC はアクセス ポイント間におけるチャネルの干渉を最小限に抑えながら、必要なカバレッジ レベルを達成するため、十分な RF 電力を提供します。

最小/最大送信電力の設定による TPC アルゴリズムの無効化

TPC アルゴリズムは、数多くのさまざまな RF 環境で RF 電力を分散させます。ただし、自動パワー制御では、アーキテクチャの制約事項またはサイトの制約事項のため、適切な RF 設計を実装できなかった一部のケースは解消できない可能性があります。たとえば、すべてのアクセスポイントを互いに近づけて中央の廊下に設置する必要があるが、建物の端までカバレッジが必要とされる場合などです。

このようなケースでは、最大および最小の送信電力制限を設定し、TPC の推奨を無効化することができます。最大および最小の TPC 電力設定は、RF ネットワークの RF プロファイルを通じてすべてのアクセス ポイントに適用されます。

[Maximum Power Level Assignment] および [Minimum Power Level Assignment] を設定するには、[Tx Power Control] ページのテキスト ボックスに RRM が使用する最大および最小の送信電力を入力します。これらのパラメータの範囲は -10 ～ 30 dBm です。最小値を最大値よりも大きくしたり、最大値を最小値よりも小さくしたりすることはできません。

最大送信電力を設定すると、RRM では、デバイスに接続されているすべてのアクセス ポイントはこの送信電力レベルを上回ることはできません（電力が RRM TPC またはカバレッジ ホールの検出のどちらで設定されるかは関係ありません）。たとえば、最大送信電力を 11 dBm に設定すると、アクセス ポイントを手動で設定しない限りは、11 dBm を上回って伝送を行うアクセス ポイントはありません。

チャネルの動的割り当て

同じチャネル上の 2 つの隣接するアクセス ポイントによって、信号のコンテンションや信号の衝突が発生することがあります。衝突の場合、アクセス ポイントではデータが受信されません。この動作は問題になることがあります。たとえば、誰かがカフェで電子メールを読むことで、近隣の会社のアクセスポイントのパフォーマンスに影響が及ぶような場合です。これらがまったく別のネットワークであっても、チャネル 1 を使用してカフェにトラフィックが送信されることによって、同じチャネルを使用している会社の通信が妨害される可能性があります。デバイスはアクセス ポイント チャネル割り当てを動的に割り当てて、衝突を回避し、キャパシティとパフォーマンスを改善することができます。チャネルは「再利用」され、希少な RF リソースが浪費されるのを防ぐことができます。つまり、チャネル 1 はカフェから離れた別のアクセス ポイントに割り当てられます。これは、チャネル 1 をまったく使用しない場合に比べてより効率的です。

デバイスの動的チャネル割り当て（DCA）機能は、アクセス ポイント間における隣接するチャネルの干渉を最小限に抑える上でも役立ちます。たとえば、チャネル 1 とチャネル 2 など、

802.11b/g 帯域でオーバーラップする 2 つのチャネルは、同時に 11/54 Mbps を使用できません。デバイスは、チャネルを効果的に再割り当てすることによって、隣接するチャネルを分離します。

（注） 重複しないチャネル（1、6、11、など）だけの使用を推奨します。

デバイスは、さまざまなリアルタイムの RF 特性を検証して、次のようにチャネルの割り当てを効率的に処理します。

- アクセス ポイントの受信エネルギー：各アクセス ポイントとその近隣のアクセス ポイント間で測定された受信信号強度。チャネルを最適化して、ネットワーク キャパシティを最大にします。
- ノイズ：ノイズによって、クライアントおよびアクセスポイントの信号の品質が制限されます。ノイズが増加すると、有効なセル サイズが小さくなり、ユーザ エクスペリエンスが低下します。デバイスでは、ノイズ源を避けるようにチャネルを最適化することで、システム キャパシティを維持しながらカバレッジを最適化できます。過剰なノイズのためにチャネルが使用できない場合は、そのチャネルを回避できます。
- 802.11 干渉：干渉とは、不正アクセス ポイントや近隣の無線ネットワークなど、無線 LAN に含まれない 802.11 トラフィックのことです。Lightweight アクセス ポイントは、常にすべてのチャネルをスキャンして干渉の原因を調べます。802.11 干渉の量が定義済みの設定可能なしきい値（デフォルトは 10 %）を超えると、アクセス ポイントからデバイスにアラートが送信されます。その場合、デバイスでは、RRM アルゴリズムを使用してチャネルの割り当てを動的に調整することで、干渉がある状況でシステム パフォーマンスを向上させることができます。このような調整によって、隣接する Lightweight アクセス ポイントが同じチャネルに割り当てられることがありますが、この設定は、干渉している外部アクセス ポイントが原因で使用できないチャネルにアクセス ポイントを割り当てたままにしておくよりも効果的です。

  また、他のワイヤレス ネットワークがある場合、デバイスは、他のネットワークを補足するようにチャネルの使用を変更します。たとえば、チャネル 6 に 1 つのネットワークがある場合、隣接する無線 LAN はチャネル 1 または 11 に割り当てられます。この調整によって、周波数の共有が制限され、ネットワークのキャパシティが増加します。チャネルにキャパシティがほとんど残っていない場合、デバイスはそのチャネルを回避できます。すべての非オーバーラップ チャネルが使用される非常に高密度の展開では、デバイスでも最適な処理が行われますが、期待値を設定する際に RF 密度を考慮する必要があります。
- 負荷および利用率：利用率の監視が有効な場合、（たとえば、ロビーとエンジニアリング エリアを比較して）一部のアクセス ポイントが他のアクセス ポイントよりも多量のトラフィックを伝送するように展開されていることを、キャパシティの計算で考慮できます。これにより、デバイスは、最も低いパフォーマンスが報告されているアクセスポイントを改善するようにチャネルを割り当てることができます。チャネル構造を変更する際には、負荷を考慮して、現在ワイヤレス LAN に存在するクライアントへの影響を最小限に抑えるようにします。このメトリックによって、すべてのアクセスポイントの送信パケットおよび受信パケットの数が追跡されて、アクセスポイントのビジー状態が測定されます。新

しいクライアントは過負荷のアクセス ポイントを回避し、別のアクセス ポイントにアソシエートします。このパラメータはデフォルトではディセーブルになっています。

デバイスは、この RF 特性情報を RRM アルゴリズムとともに使用して、システム全体にわたる判断を行います。相反する要求の解決にあたっては、軟判定メトリックを使用して、ネットワーク干渉を最小限に抑えるための最善の方法が選択されます。最終的には、3 次元空間における最適なチャネル設定が実現します。この場合、上下のフロアにあるアクセスポイントが全体的な無線 LAN 設定において主要な役割を果たします。

（注） 2.4GHz 帯域の 40 MHz チャネル、または 80 MHz チャネルを使用する無線は、DCA ではサポートされていません。

RRM スタートアップ モードは、次のような状況で起動されます

- シングルデバイス 環境では、デバイス をアップグレードしてリブートすると、RRM スタートアップ モードが起動します。
- マルチデバイス環境では、RRM スタートアップ モードは、RF グループ リーダーが選定されてから起動されます。

CLI から RRM スタートアップ モードを開始できます。

RRM スタートアップ モードは、100 分間（10 分間隔で 10 回繰り返し）実行されます。RRM スタートアップ モードの持続時間は、DCA 間隔、感度、およびネットワーク サイズとは関係ありません。スタートアップ モードには、定常ステート チャネル計画に収束するために 10 回の高感度な（チャネルを容易に環境に対して敏感に変更する）DCA 実行が含まれます。スタートアップ モードが終了した後、DCA は指定した間隔と感度で実行を継続します。

（注） DCA アルゴリズム間隔の設定値は 1 時間ですが、DCA アルゴリズムは、常に 10 分間隔（デフォルト）で実行し、最初の 10 サイクルは、10 分ごとにチャネル割り当てが行われ、チャネルは、DCA アルゴリズムに従って 10 分ごとに変更されます。その後、設定した時間間隔に戻ります。DCA アルゴリズム間隔は定常状態に従うため、DCA 間隔とアンカー時間の両方に共通です。

（注） RF グループ メンバーで DCA/TPC をオフにし、RF グループ リーダーに auto を設定すると、メンバーのチャネル/TX の電源は、RF グループ リーダーで実行されるアルゴリズムによって変化します。

カバレッジ ホールの検出と修正

RRM カバレッジ ホール検出アルゴリズムは、堅牢な無線パフォーマンスに必要なレベルに達しない無線 LAN の無線カバレッジの領域を検出することができます。この機能によって、Lightweight アクセス ポイントを追加（または再配置）する必要があるというアラートが生成されます。

RRM 設定で指定されたレベルを下回るしきい値レベル（RSSI、失敗したクライアントの数、失敗したパケットの割合、および失敗したパケットの数）で Lightweight アクセス ポイント上のクライアントが検出されると、アクセス ポイントからデバイスに「カバレッジ ホール」アラートが送信されます。このアラートは、ローミング先の有効なアクセス ポイントがないまま、クライアントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。デバイスでは、修正可能なカバレッジ ホールと不可能なカバレッジ ホールが識別されます。修正可能なカバレッジ ホールの場合、デバイスでは、その特定のアクセス ポイントの送信電力レベルを上げることによってカバレッジホールが解消されます。送信電力を増加させることが不可能なクライアントや、電力レベルが静的に設定されているクライアントによって生じたカバレッジホールがデバイスによって解消されることはありません。ダウンストリームの送信電力を増加させても、ネットワーク内の干渉を増加させる可能性があるからです。

RRM の設定方法

高度な RRM CCX パラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm ccx location-measurement** 間隔 例： `Device(config)# ap dot11 24ghz rrm ccx location-measurement 15`	802.11 CXX クライアントのロケーション測定の間隔を設定します。範囲は 10 ～ 32400 秒です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ネイバー探索タイプの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ap dot11 24ghz | 5ghz rrm ndp-type {protected | transparent}**
	例：
	`Device(config)#ap dot11 24ghz rrm ndp-type protected`
	`Device(config)#ap dot11 24ghz rrm ndp-type transparent`
		ネイバー探索タイプを設定します。デフォルトでは、モードは「transparent」に設定されます。
		• [protected]：セキュアな通信にネイバー探索タイプを「protected」に設定します。 パケットが暗号化されます。
		• [transparent]：ネイバー探索タイプを「transparent」に設定します。 パケットはそのまま送信されます。

ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RRM プロファイルしきい値、監視チャネル、および監視間隔の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[RRM]** > **[General]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[RRM]** > **[General]** を選択して、RRM の [General] ページを開きます。

ステップ 2 次のように、アラームに使用されるプロファイルしきい値を設定します。

（注） プロファイルしきい値は、RRM アルゴリズムの機能には関係ありません。これらのしきい値パラメータに設定された各 AP の値を超えると、デバイスは、Cisco Prime Infrastructure または他のトラップ レシーバに SNMP トラップ（またはアラート）を送信します。

a) [Interference] テキスト ボックスに、1 つのアクセス ポイントにおける干渉（ワイヤレス ネットワーク外の発信元からの 802.11 トラフィック）の割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 10% です。

b) [Clients] テキスト ボックスに、1 つのアクセス ポイントにおけるクライアントの数を入力します。有効な範囲は 1 ～ 75 で、デフォルト値は 12 です。

c) [Noise] テキスト ボックスに、1 つのアクセス ポイントにおけるノイズ（802.11 以外のトラフィック）のレベルを入力します。有効な値の範囲は –127 ～ 0 dBm で、デフォルト値は –70 dBm です。

d) [Utilization] テキスト ボックスに、1 つのアクセス ポイントで使用されている RF 帯域幅の割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 80% です。

e) **[Throughput]** テキスト ボックスに、1 つのアクセス ポイントで使用されるスループット レベルを入力します。有効な範囲は 1000 ～ 10000000 で、デフォルト値は 1000000 です。

ステップ 3 **[Channel List]** ドロップダウン リストから次のオプションのいずれかを選択して、アクセス ポイントで RRM によるスキャンに使用されるチャネルのセットを指定します。

- [All Channels]：選択した無線でサポートされているすべてのチャネルで、RRM によるチャネル スキャンが実行されます。使用国で有効でないチャネルも対象となります。
- [Country Channels]：使用国内の D チャネルのみで、RRM によるチャネル スキャンが実行されます。これはデフォルト値です。
- [DCA Channels]：DCA アルゴリズムによって使用されるチャネル セットのみで、RRM によるチャネルスキャンが実行されます。デフォルトでは、使用国で有効な、オーバーラップしないすべてのチャネルが対象となります。ただし、必要に応じて、DCA で使用するチャネルセットを指定できます。これを行うには、「チャネルの動的割り当て」の手順に従ってください。

ステップ 4 次のように、監視間隔を設定します。

1. [Channel Scan Interval] テキスト ボックスに、無線帯域内の各チャネルでスキャンを実行する時間間隔の合計（秒）を入力します。スキャンプロセス全体の所要時間はチャネル、無線ごとに 50 ミリ秒であり、ここで設定された間隔で実行されます。各チャネルをリッスンするための所要時間は、50 ミリ秒のスキャン時間（設定不可）とスキャン対象チャネル数によって決まります。たとえば、米国の場合、すべての 11 802.11b/g チャネルは、デフォルトの 180 秒の間隔で 50 ミリ秒間スキャンされます。したがって、各スキャン チャネルで 16 秒ごとに 50 ミリ秒がリッスンに費やされます（180/11 = 約 16 秒）。Channel Scan Interval パラメータで、スキャンを実行する間隔を指定します。有効な範囲は 60 ～ 3600 秒で、 802.11a/n/ac および 802.11b/g/n 無線のデフォルト値は 180 秒です。

2. [Neighbor Packet Frequency] テキスト ボックスに、ネイバー パケット（メッセージ）が送信される間隔を秒単位で入力します。ネイバー パケットによって最終的にネイバー リストが構築されます。有効な範囲は 60 ～ 3,600 秒です。デフォルト値は 60 秒です。

   （注） アクセス ポイント無線が 60 分以内に既存のネイバーからネイバー パケットを受信しない場合、Cisco WLC によってネイバー リストからそのネイバーが削除されます。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

（注） Cisco WLC の RRM パラメータをすべて工場出荷時のデフォルト値に戻す場合は、[Set to Factory Default] をクリックします。

RF グループの設定

この項では、GUI または CLI によって RF グループを設定する方法について説明します。

（注） 通常、RF グループ名は展開時にスタートアップ ウィザードを使用して設定されます。ただし、必要に応じて変更できます。

（注） 複数の国番号機能を使用している場合、同じ RF グループに join する予定のすべての Cisco WLC は、同じ国を同じ順序で設定する必要があります。

（注） Cisco Prime インフラストラクチャを使用して RF グループを設定することもできます。

（注） Auto モードでは、RF グループ リーダーは RF グループ安定化のためにグループ設定サイクルの最初の 3 回のランでは、TP と DCA をスキップします。

RF グループ モードの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[RRM]** > **[RF Grouping]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[RRM]** > **[RF Grouping]** を選択して、[RF Grouping] ページを開きます。

ステップ 2 [Group Mode] ドロップダウン リストで、この Cisco WLC に設定するモードを選択します。

次のモードで RF グループ化を設定できます。

- auto：RF グループ選択を自動更新モードに設定します。

（注） 設定したスタティック リーダーは、モードが [auto] に設定されるまで、他の Cisco RF のメンバになることはできません。

- [leader]：RF グループ選択を静的モードに設定し、この Cisco WLC をグループ リーダーとして設定します。
- off：RF グループ選択をオフに設定します。すべての Cisco WLC が自身のアクセス ポイント パラメータを最適化します。

（注） 優先順位が高い Cisco WLC が使用可能な場合、優先順位がより低い Cisco WLC はグループ リーダーの役割を担うことはできません。ここでの優先順位は、Cisco WLC の処理能力に関連しています。

（注） Cisco WLC が自動 RF グループ化に加わるように設定することをお勧めします。RRM の設定を無効にする際には、自動 RF グループ化への参加を無効にする必要はありません。

ステップ 3 [Apply] をクリックして設定を保存し、[Restart] をクリックして RRM RF グループ化アルゴリズムを再起動します。

ステップ 4 この Cisco WLC に対して、スタティック リーダーとして RF グループ化モードを設定した場合、次のように [Group Members] セクションからグループ メンバを追加することができます。

1. デバイスの [Name] テキスト ボックスに、このグループにメンバとして追加する Cisco WLC を入力します。
2. [IP Address] テキスト ボックスに、Cisco WLC の IP アドレスを入力します。
3. [Add] をクリックして、このグループにメンバを追加します。

（注） メンバがスタティック リーダーに join されない場合は、失敗の理由がカッコ内に表示されます。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

RF グループ選択モードの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ap dot11 24ghz | 5ghz rrm group-mode{auto | leader | off}** 例： `Device(config)#ap dot11 24ghz rrm group-mode leader`	802.11 帯域の RF グループ選択モードを設定します。 • [auto]：802.11 RF グループ選択を自動更新モードに設定します。 • [leader]：リーダー モードで 802.11 RF グループ選択をリーダー モードに設定します。 • [off]：802.11 RF グループ選択をディセーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RF グループ名の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless rf-network** *name* 例： `Device (config)# wireless rf-network test1`	RF グループを作成します。グループ名は、最大 19 文字の ASCII 文字列で、大文字と小文字が区別されます。 （注） RF グループに含める各コントローラについて、この手順を繰り返します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 4	**show network profile** *profile_number*	RF グループを表示します。 （注） 1 ～ 4294967295 のネットワーク プロファイル番号を表示できます。

RF グループ名の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Controller]** > **[General]** を選択して、[General] ページを開きます。

ステップ 2 [RF Network Name] テキスト ボックスに RF グループの名前を入力します。名前は最大 19 の ASCII 文字を含むことができ、大文字と小文字が区別されます。

ステップ 3 [Apply] をクリックして、変更を確定します。

ステップ 4 [Save Configuration] をクリックして、変更を保存します。

ステップ 5 RF グループに含める各コントローラについて、この手順を繰り返します。

802.11 静的 RF グループのメンバの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr* 例： `Device(config)#ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1`	802.11 静的 RF グループにメンバを設定します。グループ メンバをアクティブにするには、グループモードをリーダーに設定する必要があります。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

送信電力制御の設定

送信電力制御のしきい値の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm tpc-threshold** *threshold_value* 例： `Device(config)#ap dot11 24ghz rrm tpc-threshold -60`	自動電力割り当てのためにRRMが使用する送信電力制御のしきい値を設定します。範囲は -80 ～ -50 です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

送信電力レベルの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm txpower**{*trans_power_level* **| auto | max | min | once**} 例： `Device(config)#ap dot11 24ghz rrm txpower auto`	802.11 の送信電力レベルを設定します。 • [trans_power_level]：送信電力レベルを設定します。 • [auto]：自動 RF をイネーブルにします。 • [max]：最大自動 RF 送信電力を設定します。 • [min]：最小自動RF送信電力を設定します。 • [once]：自動 RF を一度だけイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

送信電力制御の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[RRM]** > **[TPC]** または **[Configuration]** > **[Wireless]** > **[802.11b]** > **[RRM]** > **[TPC]** を選択して、RRM の [Tx Power Control (TPC)] ページを開きます。

ステップ 2 [Transmit Power Control] を選択します。

[Coverage Optimal Mode (TPCv1)]：強力な信号カバレッジと安定性を提供します。このモードでは、送信電力を低く維持することでキャパシティを増やし、干渉を減らします。

ステップ 3 [Power Level Assignment Method] ドロップダウン リストから次のオプションのいずれかを選択して、Cisco WLC の動的電力割り当てモードを指定します。

- [Automatic]：Cisco WLC よって、join しているすべてのアクセス ポイントの送信電力が定期的に評価され、必要に応じて更新されます。これはデフォルト値です。
- [On Demand]：Cisco WLC によって、join しているすべてのアクセス ポイントの送信電力が定期的に評価されます。ただし、必要に応じて、**[On Demand]** を選択してから **[Apply]** をクリックした場合のみ、Cisco WLC は電力を更新します。

  （注） **[On Demand]** を選択してから **[Apply]** をクリックしても、Cisco WLC は送信電力をすぐに評価したり、更新したりしません。次の間隔（600秒）まで待機します。この値は設定可能です。

- [Fixed]：Cisco WLC によって、join しているアクセス ポイントの送信電力が評価されたり、必要に応じて更新されたりすることはありません。電力レベルは、ドロップダウン リストから選択した固定値に設定されます。CLIから設定する場合、[Fixed]に対応するオプションは **once** です。

  （注） 送信電力 レベルには、mW 単位または dBm 単位の値の代わりに整数値が割り当てられます。この整数は、アクセスポイントが展開されている規制区域、チャネル、およびアンテナによって異なる電力レベルに対応します。

  （注） 最適なパフォーマンスを確保するには、[Automatic] 設定を使用することを、お勧めします。

ステップ 4 [Maximum Power Level Assignment] および [Minimum Power Level Assignment] テキスト ボックスに最大および最小の電力レベル割り当て値を入力します。

[Maximum Power Level Assignment] の範囲は、-10 ～ 30 dBm です。

[Minimum Power Level Assignment] の範囲は、-10 ～ 30 dBm です。

ステップ 5 [Power Threshold] テキスト ボックスに、アクセス ポイントの電力を減らすかどうか判断する際にRRMで使用する切断信号レベルを入力します。このパラメータのデフォルト値は–70 dBm（TPCv1）ですが、アクセス ポイントの伝送パワー レベルが必要以上に高い（または低い）場合は変更できます。

このパラメータの範囲は –80 ～ –50 dBm です。この値を –65 ～ –50 dBm の範囲で増やすと、アクセスポイントは高い送信電力で動作するようになります。値を減らすと、逆の効果が得られます。

多数のアクセス ポイントを使用しているアプリケーションでは、ワイヤレス クライアントが認識する BSSID（アクセス ポイント）やビーコンの数を少なくするために、しきい値を –80 dBm または –75 dBm に下げるのが有用です。一部のワイヤレス クライアントは多数の BSSID や高速ビーコンを処理できない場合があり、デフォルトのしきい値では、問題のある動作を起こす可能性があります。

このページには、次のような送信電力レベルのパラメータの設定も表示されますが、これらは設定できません。

- [Power Neighbor Count]：送信電力制御アルゴリズムを実行するためにアクセス ポイントに必要なネイバーの最小数です。
- [Power Assignment Leader]：パワー レベルの割り当てを担当する RF グループ リーダーの MAC アドレスです。
- [Last Power Level Assignment]：RRM が現在の送信電力 レベルの割り当てを最後に評価した時間です。

ステップ 6 [Apply] をクリックします。

ステップ 7 [Save Configuration] をクリックします。

802.11 RRM パラメータの設定

高度な 802.11 チャネル割り当てパラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**high** | **low** | **medium**} 例： `Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	CleanAir のイベント駆動型 RRM パラメータを設定します。 • [High]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最高に指定します。 • [Low]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最低に指定します。 • [Medium]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を中間に指定します。

ステップ 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** {*channel number* | **anchor-time** | **global** {**auto**| **once**} | **interval** | **min-metric** | **sensitivity** {**high** | **low** | **medium**}}
	例：
	`Device(config)#ap dot11 24ghz rrm channel dca interval 2`
		802.11 帯域の動的チャネル割り当て（DCA）アルゴリズム パラメータを設定します。
		• ***<1-14>***：DCA リストに追加するチャネル番号を入力します。
		• [anchor-time]：DCA のアンカー時間を設定します。範囲は 0 ～ 23 時間です。
		• [global]：すべての 802.11 Cisco AP の DCA モードを設定します。
		  • [auto]：自動 RF をイネーブルにします。
		  • [once]：自動 RF を一度だけイネーブルにします。
		• [interval]：DCA のインターバル値を設定します。値は 1、2、3、4、6、8、12、24 時間です。デフォルト値 0 は 10 分を意味します。
		• [min-metric]：DCA の最小 RSSI エネルギーメトリックを設定します。範囲は -100 ～ -60 です。
		• [sensitivity]：環境の変化に対する DCA 感度レベルを設定します。

	コマンドまたはアクション	目的
		• [high]：最高の感度を指定します。 • [low]：最低の感度を指定します。 • [medium]：中間の感度を指定します。
ステップ 4	**ap dot11 5ghz rrm channel dca chan-width {20 | 40 | 80 | best {20 | 40 | 80 | MAX}}**	5 GHz 帯域のすべての 802.11 無線に対して DCA チャネル幅を設定します。チャネル幅を 20 MHz、40 MHz、 80 MHz、または最良に設定します。チャネル幅のデフォルト値は 20 MHz です。最良のデフォルト値は 80 MHz です。
ステップ 5	**ap dot11 {24ghz | 5ghz} rrm channel device** 例： `Device(config)#ap dot11 24ghz rrm channel device`	802.11 チャネル割り当てで、非 Wi-Fi デバイスの継続的な回避を設定します。
ステップ 6	**ap dot11 {24ghz | 5ghz} rrm channel foreign** 例： `Device(config)#ap dot11 24ghz rrm channel foreign`	チャネル割り当てで、外部 AP の 802.11 干渉の回避を設定します。
ステップ 7	**ap dot11 {24ghz | 5ghz} rrm channel load** 例： `Device(config)#ap dot11 24ghz rrm channel load`	チャネル割り当てで、Cisco AP の 802.11 負荷の回避を設定します。
ステップ 8	**ap dot11 {24ghz | 5ghz} rrm channel noise** 例： `Device(config)#ap dot11 24ghz rrm channel noise`	チャネル割り当てで、802.11 ノイズの回避を設定します。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

動的チャネル割り当ての設定（GUI）

RRM によるスキャンに使用するチャネルの選択時に、Cisco WLC の GUI を使用して動的チャネル割り当て（DCA）アルゴリズムで考慮されるチャネルを指定できます。

（注） この機能は、クライアントが古いデバイスであるため、またはクライアントに特定の制約事項があるために、クライアントで特定のチャネルがサポートされないことがわかっている場合に役立ちます。

手順

ステップ 1 次のように、802.11a/n/ac または 802.11b/g/n ネットワークをディセーブルにします。

a) **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[Network]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[Network]** を選択して、[Global Parameters] ページを開きます。

b) [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオフにします。

c) [Apply] をクリックします。

ステップ 2 **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[RRM]** > **[DCA]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[RRM]** > **[DCA]** を選択して、[Dynamic Channel Assignment (DCA)] ページを開きます。

ステップ 3 [Channel Assignment Method] ドロップダウン リストから次のオプションのいずれかを選択して、Cisco WLC の DCA モードを指定します。

- [Automatic]：Cisco WLC によって、join しているすべてのアクセス ポイントのチャネル割り当てが定期的に評価され、必要に応じて更新されます。これはデフォルト値です。
- [Freeze]：必要に応じて、**[Freeze]** オプションを選択した後、**[Apply]** をクリックした場合にだけ、join しているすべてのアクセス ポイントのチャネル割り当てが Cisco WLC によって評価および更新されます。

  （注） **[Freeze]** オプションを選択した後に **[Apply]** をクリックすると、Cisco WLC はチャネル割り当てをすぐに評価したり、更新したりしません。次の間隔が経過するまで待機します。

- OFF：DCA をオフにして、帯域の最初のチャネルにすべてのアクセス ポイント無線を設定します。このオプションを選択する場合は、すべての無線のチャネルを手動で割り当てる必要があります。

  （注） 最適なパフォーマンスを確保するには、[Automatic] 設定を使用することを、お勧めします。

ステップ 4 [Interval] ドロップダウン リストで、[10 minutes]、[1 hour]、[2 hours]、[3 hours]、[4 hours]、[6 hours]、[8 hours]、[12 hours]、または [24 hours] のいずれかのオプションを選択し、DCA アルゴリズムを実行する間隔を指定します。デフォルト値は 10 分です。

ステップ 5 [AnchorTime] ドロップダウン リストで、DCA アルゴリズムの開始時刻を指定する数値を選択します。オプションは、0 ～ 23 の数値（両端の値を含む）で、午前 12 時～午後 11 時の時刻を表します。

ステップ 6 [DCA Channel Sensitivity] ドロップダウン リストから、次のオプションのいずれかを選択して、チャネルを変更するかどうかを判断する際の、信号、負荷、ノイズ、干渉などの環境の変化に対する DCA アルゴリズムの感度を指定します。

- [Low]：環境の変化に対する DCA アルゴリズムの感度は特に高くありません。
- [Medium]：環境の変化に対する DCA アルゴリズムの感度は中程度です。
- [High]：環境の変化に対する DCA アルゴリズムの感度が高くなります。

デフォルトでは [Medium] です。DCA の感度のしきい値は、次の表で示すように、無線帯域によって異なります。

表 *100 : DCA* の感度のしきい値

オプション	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
大きい	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

ステップ 7 このページには、次のような変更できないチャネル パラメータの設定も表示されます。

- [Channel Assignment Leader]：チャネルの割り当てを担当する RF グループ リーダーの MAC アドレスです。

ステップ 8 [DCA Channel List] 領域の [DCA Channels] テキスト ボックスには、現在選択されているチャネルが表示されます。チャネルを選択するには、[Select] カラムでそのチャネルのチェックボックスをオンにします。チャネルの選択を解除するには、チャネルのチェックボックスをオフにします。

範囲は次のとおりです。

- 802.11a：36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、165（国によって異なる）。
- 802.11b/g：1、2、3、4、5、6、7、8、9、10、11、12、13、14（国によって異なる）。

デフォルトの設定は次のとおりです。

- 802.11a：36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161
- 802.11b/g：1、6、11

ステップ 9 [Apply] をクリックします。

ステップ 10 次の手順で、802.11 ネットワークを再度イネーブルにします。

1. **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[Network]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[Network]** を選択して、[Global Parameters] ページを開きます。
2. [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオンにします。
3. [Apply] をクリックします。

ステップ 11 [Save Configuration] をクリックします。

802.11 カバレッジ ホール検出の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**} 例： `Device(config)#ap dot11 24ghz rrm coverage data fail-percentage 60`	データ パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンク データ パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100 % の範囲で設定します。 • [packet-count]：アップリンク データ パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。 • [rssi-threshold]：データ パケットの 802.11 最小受信カバレッジ レベルを、– 90 ～ 60 dBm の範囲で設定します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm coverage exception global** 例外レベル 例： `Device(config)#ap dot11 24ghz rrm coverage exception global 50`	802.11 Cisco AP のカバレッジ例外レベルを、0 ～ 100 % の範囲で設定します。

	コマンドまたはアクション	目的
ステップ 4	**ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min* 例外レベル 例： `Device(config)#ap dot11 24ghz rrm coverage level global 10`	802.11 Cisco AP クライアントの最小例外を、1 ～ 75 の範囲で指定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**} 例： `Device(config)#ap dot11 24ghz rrm coverage voice packet-count 10`	音声パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンク音声パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100 % の範囲で設定します。 • [packet-count]：アップリンク音声パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。 • [rssi-threshold]：音声パケットの 802.11 最小受信カバレッジ レベルを、–90 ～ -60 dBm の範囲で設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

カバレッジ ホールの検出の設定（GUI）

手順

ステップ 1 次の手順で 802.11 ネットワークを無効にします。

a) **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** を選択して、802.11a/n/ac（または 802.11b/g/n）の [Global Parameters] ページを開きます。

b) [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオフにします。

c) [Apply] をクリックします。

ステップ 2 **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[RRM]** > **[Coverage Thresholds]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[RRM]** > **[Coverage Thresholds]** を選択して、[coverage] ページを開きます。

ステップ 3 カバレッジ ホールの検出を有効にする場合は [Enable Coverage Hole Detection] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。カバレッジホールの検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセス ポイントがあるかどうかを、アクセス ポイントから受信したデータに基づいて Cisco WLC が自動的に判断します。デフォルト値はオンです。

ステップ 4 **[Data RSSI]** テキスト ボックスに、アクセス ポイントで受信されたデータ パケットの最小の受信信号強度インジケータ（RSSI）値を入力します。入力する値は、ネットワーク内のカバレッジ ホール（またはカバレッジが不完全な領域）を特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットがデータ キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は –90 ～ –60 dBm で、デフォルト値は –80 dBm です。アクセス ポイントでは、データ RSSI が 5 秒おきに測定され、それらが 90 秒間隔で Cisco WLC にレポートされます。

ステップ 5 **[Voice RSSI]** テキスト ボックスに、アクセス ポイントで受信された音声パケットの最小の受信信号強度インジケータ（RSSI）値を入力します。入力する値は、ネットワーク内のカバレッジ ホールを特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットが音声キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は –90 ～ –60 dBm で、デフォルト値は –80 dBm です。アクセス ポイントでは、音声 RSSI が 5 秒おきに測定され、それらが 90 秒間隔で Cisco WLC にレポートされます。

ステップ 6 [Min Failed Client Count per AP] テキスト ボックスに、RSSI 値がデータ RSSI または音声 RSSI のしきい値以下である、アクセス ポイント上のクライアントの最小数を入力します。有効な範囲は 1 ～ 75 で、デフォルト値は 3 です。

ステップ 7 [Coverage Exception Level per AP] テキスト ボックスに、信号レベルが低くなっているにもかかわらず別のアクセス ポイントにローミングできない、アクセス ポイント上のクライアントの割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 25% です。

（注） 5 秒間で失敗したパケットの数と割合の両方が、[Failed Packet Count] および [Failed Packet Percentage]（Cisco WLC の CLI を使用して設定可能）に設定された値を超える場合、クライアントは事前アラーム状態と判断されます。Cisco WLC は、この情報を使用して、真のカバレッジ ホールと偽のカバレッジ ホールを区別します。false positive は通常、大部分のクライアントに実装されているローミング ロジックが不適切であることが原因です。180 秒間（90 秒間の 2 倍）で失敗したクライアントの数と割合の両方が、[Min Failed Client Count per AP] および [Coverage Exception Level per AP] テキスト ボックスに入力された値を満たすか超えている場合、カバレッジ ホールが検出されます。Cisco WLC は、カバレッジ ホールが修正可能かどうかを判断し、適切な場合は、その特定のアクセス ポイントの送信電力レベルを上げることによってカバレッジ ホールを解消します。

ステップ 8 [Apply] をクリックします。

ステップ 9 次の手順で 802.11 ネットワークを再度イネーブルにします。

a) **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[Network]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[Network]** を選択して、802.11a（または 802.11b/g）の [Global Parameters] ページを開きます。

b) [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオンにします。

c) [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

802.11 イベント ロギングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ap dot11 24ghz | 5ghz rrm logging {channel | coverage | foreign | load | noise | performance | txpower}**
	例：
	`Device(config)#ap dot11 24ghz rrm logging channel`
	`Device(config)#ap dot11 24ghz rrm logging coverage`
	`Device(config)#ap dot11 24ghz rrm logging foreign`
	`Device(config)#ap dot11 24ghz rrm logging load`
	`Device(config)#ap dot11 24ghz rrm logging noise`
	`Device(config)#ap dot11 24ghz rrm logging performance`
	`Device(config)#ap dot11 24ghz rrm logging txpower`
		各種パラメータに対するイベント ロギングを設定します。
		• [channel]：802.11 チャネル変更ロギング モードを設定します。
		• [coverage]：802.11 のカバレッジ プロファイル ロギング モードを設定します。
		• [foreign]：802.11 外部干渉プロファイル ロギング モードを設定します。
		• [load]：802.11 負荷プロファイル ロギング モードを設定します。
		• [noise]：802.11 ノイズプロファイル ロギング モードを設定します。
		• [performance]：802.11 パフォーマンス プロファイル ロギング モードを設定します。
		• [txpower]：802.11 送信電力変更ロギング モードを設定します。

ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 統計情報の監視の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**} 例： `Device(config)#ap dot11 24ghz rrm monitor channel-list all`	noise/interference/rogue などのパラメータに 802.11 監視チャネル リストを設定します。 • [all]：すべてのチャネルを監視します。 • [country]：設定された国コードで使用するチャネルを監視します。 • [dca]：動的なチャネル割り当てで使用されるチャネルを監視します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm monitor coverage** 間隔 例： `Device(config)#ap dot11 24ghz rrm monitor coverage 600`	802.11 のカバレッジ測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 4	**ap dot11 24ghz | 5ghz rrm monitor load** 間隔 例： `Device(config)#ap dot11 24ghz rrm monitor load 180`	802.11 負荷測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm monitor noise** 間隔 例： `Device(config)#ap dot11 24ghz rrm monitor noise 360`	802.11 のノイズ測定間隔（チャネル スキャン間隔）を、60 ～ 3600 秒の範囲で設定します。
ステップ 6	**ap dot11 24ghz | 5ghz rrm monitor signal** 間隔 例：	802.11 の信号測定間隔（ネイバーパケットの頻度）を、60 ～ 3600 秒の範囲で設定します。

	コマンドまたはアクション	目的
	`Device(config)#ap dot11 24ghz rrm monitor signal 480`	
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 パフォーマンス プロファイルの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile clients 20`	802.11 Cisco AP クライアント数のしきい値を、1 ～ 75 の範囲で設定します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile foreign 50`	802.11 外部干渉のしきい値を、0 ～ 100 % の範囲で設定します。
ステップ 4	**ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile noise -65`	802.11 外部ノイズのしきい値を、-127 ～ 0 dBm の範囲で設定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile throughput 10000`	802.11 Cisco AP スループットのしきい値を、1000 ～ 10000000 バイト/秒の範囲で設定します。

	コマンドまたはアクション	目的
ステップ 6	**ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile utilization 75`	802.11 RF 使用率のしきい値を、0 ～ 100% の範囲で設定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RF グループ内の不正アクセス ポイント検出の設定

RF グループ内の不正アクセス ポイント検出の設定（CLI）

始める前に

RF グループ内の各 Cisco WLC に同じ RF グループ名が設定されていることを確認します。

（注） この名前は、すべてのビーコン フレーム内の認証 IE を検証するために使用されます。Cisco WLC に異なる名前が設定されている場合は、誤ったアラームが生成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *Cisco_AP* **mode** {**local** | **monitor**} 例： `Device# ap name ap1 mode local`	ローカル（通常）モードまたはモニタ（リッスン専用）モードの特定アクセス ポイントを設定します。Cisco WLC に接続されたすべてのアクセス ポイントについて、次の手順を実行します。
ステップ 2	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**wireless wps ap-authentication** 例： `Device (config)# wireless wps ap-authentication`	不正なアクセスポイントの検出をイネーブルにします。
ステップ 5	**wireless wps ap-authentication threshold** *value* 例： `Device (config)# wireless wps ap-authentication threshold 50`	不正アクセス ポイント アラームが生成されるタイミングを指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。 しきい値の有効範囲は 1 ～ 255 で、デフォルトのしきい値は1です。アラームの誤判定を防止するには、しきい値を高い値に設定してください。 （注） RF グループ内のすべての Cisco WLC で、不正アクセス ポイントの検出としきい値をイネーブルにします。 （注） RF グループ内のすべての Cisco WLC で不正アクセス ポイントの検出がイネーブルになっていない場合、この機能がディセーブルになっている Cisco WLC のアクセス ポイントは不正として報告されます。

RF グループ内の不正アクセス ポイント検出の有効化（GUI）

手順

ステップ 1 RF グループ内の各 Cisco WLC に同じ RF グループ名が設定されていることを確認します。

（注） この名前は、すべてのビーコンフレーム内の認証IEを検証するために使用されます。Cisco WLCに異なる名前が設定されている場合は、誤ったアラームが生成されます。

ステップ 2 **[Configuration]** > **[Wireless]** > **[Access Points]** > **[All APs]** を選択して、[All APs] ページを開きます。

ステップ 3 アクセス ポイントの名前をクリックして、[All APs] > [Edit] ページを開きます。

ステップ 4 [AP Mode] ドロップダウン リストから [local] または [monitor] を選択し、[Apply] をクリックして変更を確定します。

ステップ 5 [Save Configuration] をクリックして、変更を保存します。

ステップ 6 Cisco WLC に接続されているすべてのアクセス ポイントについて、ステップ 2 からステップ 5 を繰り返します。

ステップ 7 **[Configuration]** > **[Security]** > **[Wireless Protection Policies]** > **[AP Authentication/MFP]** を選択して、[AP Authentication Policy] ページを開きます。

この Cisco WLC が属する RF グループの名前は、ページの上部に表示されます。

ステップ 8 [Protection Type] ドロップダウン リストから [AP Authentication] を選択して、不正アクセス ポイントの検出を有効にします。

ステップ 9 [Alarm Trigger Threshold] 編集ボックスに数値を入力して、不正アクセス ポイントに関するアラームがいつ生成されるようにするかを指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。

（注） しきい値の有効範囲は 1 ～ 255 で、デフォルト値は 1 です。アラームの誤判定を防止するには、しきい値を高い値に設定してください。

ステップ 10 [Apply] をクリックして、変更を確定します。

ステップ 11 [Save Configuration] をクリックして、変更を保存します。

ステップ 12 RF グループ内のすべての Cisco WLC について、この手順を繰り返します。

（注） RF グループ内のすべての Cisco WLC で不正アクセス ポイントの検出がイネーブルになっていない場合、この機能がディセーブルになっている Cisco WLC のアクセス ポイントは不正として報告されます。

RRM パラメータと RF グループ ステータスの監視

RRM パラメータの監視

表 *101 :* 無線リソース管理を監視するためのコマンド

コマンド	説明
show ap dot11 24ghz ccx	すべての Cisco AP に対して 802.11b CCX 情報を表示します。
show ap dot11 24ghz channel	802.11b チャネル割り当ての設定および統計情報を表示します。
show ap dot11 24ghz coverage	802.11b カバレッジの設定と統計情報を表示します。
show ap dot11 24ghz group	802.11b グループ化の設定と統計情報を表示します。

コマンド	説明
show ap dot11 24ghz l2roam	802.11b l2roam 情報を表示します。
show ap dot11 24ghz logging	802.11b イベント ロギングの設定と統計情報を表示します。
show ap dot11 24ghz monitor	802.11b モニタリングの設定および統計情報を表示します。
show ap dot11 24ghz profile	すべての Cisco AP の 802.11b プロファイル情報を表示します。
show ap dot11 24ghz receiver	802.11b レシーバの設定と統計情報を表示します。
show ap dot11 24ghz summary	802.11b Cisco AP の設定と統計情報を表示します。
show ap dot11 24ghz txpower	802.11b 送信電力制御の設定と統計情報を表示します。
show ap dot11 5ghz ccx	すべての Cisco AP の 802.11a CCX 情報を表示します。
show ap dot11 5ghz channel	802.11aチャネル割り当ての設定および統計情報を表示します。
show ap dot11 5ghz coverage	802.11a カバレッジの設定と統計情報を表示します。
show ap dot11 5ghz group	802.11a グループ化の設定と統計情報を表示します。
show ap dot11 5ghz l2roam	802.11a l2roam 情報を表示します。
show ap dot11 5ghz logging	802.11a イベント ロギングの設定と統計情報を表示します。
show ap dot11 5ghz monitor	802.11a モニタリングの設定および統計情報を表示します。
show ap dot11 5ghz profile	すべての Cisco AP の 802.11a プロファイル情報を表示します。
show ap dot11 5ghz receiver	802.11a レシーバの設定と統計情報を表示します。
show ap dot11 5ghz summary	802.11a Cisco AP の設定と統計情報を表示します。
show ap dot11 5ghz txpower	802.11a 送信電力制御の設定と統計情報を表示します。

RF グループ ステータスの監視（CLI）

ここでは、RF グループ ステータスの新しいコマンドについて説明します。

次のコマンドがの RF グループ ステータスを監視するために使用できます。

表 *102 :* アグレッシブ ロード バランシング コマンドの監視

コマンド	目的
show ap dot11 5ghz group	802.11a RF ネットワークの RF グループ リーダーである Cisco WLC の名前が表示されます。

show ap dot11 24ghz group	802.11b/g RF ネットワークの RF グループ リーダーである Cisco WLC の名前が表示されます。

RF グループ ステータスの監視（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[802.11a/n]** > または **[802.11b/g/n]** > **[RRM]** > **[RF Grouping]** を選択して、[RF Grouping Algorithm] ページを開きます。

このページは RF グループの詳細を示し、設定可能なパラメータ **[Group mode]**、この Cisco WLC の **[Group role]**、**[Group Update Interval]**、およびこの Cisco WLC の **[Group Leader]** の Cisco WLC 名と IP アドレスを表示します。

（注） RF グループ化モードは、[Group Mode] ドロップダウン リストを使用して設定できます。

ヒント：一度 Cisco WLC がスタティック メンバとして join してから、グループ化モードを変更する場合は、メンバを設定したスタティック リーダーからそのメンバを削除することをお勧めします。メンバの Cisco WLC が複数のスタティック リーダーでメンバになるように設定されていないことも確認してください。これは、1 つまたは複数の RF スタティック リーダーから join 試行が繰り返されるのを回避します。

ステップ 2 （任意）選択しなかったネットワーク タイプ（802.11a/n または 802.11b/g/n）について、この手順を繰り返します。

例：RF グループの設定

次に、RF グループ名を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless rf-network test1
Device(config)# ap dot11 24ghz shutdown
Device(config)# end
Device # show network profile 5
```

次に、RF グループ内の不正アクセス ポイントの検出を設定する例を示します。

```
Device# ap name ap1 mode local
Device# end
Device# configure terminal
Device(config)# wireless wps ap-authentication
Device(config)# wireless wps ap-authentication threshold 50
Device(config)# end
```

ED-RRM について

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャネル、またはある範囲内のチャネルが完全に妨害を受けます。Cisco CleanAir の Event Driven RRM（EDRRM）機能を使用すると、電波品質（AQ）に対してしきい値を設定できます。しきい値を超過した場合には、影響を受けたアクセスポイントに対してチャネル変更がただちに行われます。ほとんどの RF 管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAir では AQ 測定値を使用してスペクトラムを連続的に評価するため、対応策を 30 秒以内に実行します。たとえば、アクセス ポイントがビデオ カメラからの干渉を受けた場合は、そのカメラが動作し始めてから 30 秒以内にチャネル変更によってアクセス ポイントを回復させることができます。Cisco CleanAir では干渉源の識別と位置の特定も行うため、後からその装置の永続的な緩和処理も実行できます。

Cisco ワイヤレス LAN コントローラで ED-RRM の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、Cisco CleanAir 対応のアクセス ポイントで非常に高いレベルの干渉が検出された場合に、Event Driven Radio Resource Management（RRM）の実行がトリガーされるよう設定します。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event** ：802.11 の Cisco Lightweight アクセス ポイントの CleanAir による RRM パラメータを設定します。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}：802.11 の Cisco Lightweight アクセス ポイントの CleanAir による RRM 感度を設定します。デフォルトの選択は、[Medium] です。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution**：不正コントリビューションを有効にします。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contributionduty-cycle** *thresholdvalue*：不正コントリビューションのしきい値を設定します。値の範囲は 1 ～ 99 で、デフォルトの値は 80 です。

ステップ 2 次のコマンドを入力して、変更を保存します。

write memory

ステップ 3 次のコマンドを入力して、802.11a/n/ac または 802.11b/g/n ネットワークに対する CleanAir の設定を確認します。

show ap dot11 {**24ghz** | **5ghz**} **cleanairconfig**

以下に類似した情報が表示されます。

```
AdditionalClean Air Settings:
```

```
CleanAir Event-driven RRM State............. : Enabled
CleanAir Driven RRM Sensitivity............. : LOW
CleanAir Event-driven RRM Rogue Option...... : Enabled
CleanAir Event-driven RRM Rogue Duty Cycle... : 80
CleanAir Persistent Devices state........... : Disabled
CleanAir Persistent Device Propagation...... : Disabled
```

ED-RRM の設定（GUI）

手順

ステップ 1 **[Configure]** > **[Radio Configurations]** > **[2.4 GHZ or 5 GHZ]** > **[RRM]** > **[DCA]** の順に選択して、[ED-RRM] ページを開きます。

（注） ED-RRM をイネーブルにする前に、**[Configure]** > **[Radio Configurations]** > **[2.4 GHZ or 5 GHZ]** > **[Network]** > **[General]** ページから [Network Status] を無効にする必要があります。ED-RRM の設定後に、ネットワークを再度有効にします。

ステップ 2 [Event Driven RRM] セクションで、ED-RRM パラメータを表示するには、[EDRRM] チェックボックスをオンにします。

ステップ 3 [Sensitivity Threshold] のドロップダウンから値を選択します。

オプション：[Low]、[Medium]、[High]。デフォルトの選択は、[Medium] です。

ステップ 4 不正なデューティ サイクル パラメータを表示するには、[Rogue Contribution] チェックボックスをオンにします。

ステップ 5 テキストボックスに、[Rogue Duty Cycle] の値を入力します。

値の範囲は 1 ～ 99 で、デフォルトの値は 80 です。

ステップ 6 [Apply] をクリックします。

ステップ 7 [Save Configuration] をクリックします。

無線リソース管理に関するその他の参考ドキュメント

関連資料

関連項目	マニュアル タイトル
RRM コマンドと詳細	『*RRM Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

無線リソース管理の設定を行うための機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 84 章

Cisco 2800/3800 シリーズ アクセス ポイントの XOR スロットの設定

- XOR 無線に関する情報 （1711 ページ）
- XOR 無線の設定（GUI） （1711 ページ）
- XOR 無線の設定（CLI） （1712 ページ）
- XOR 無線パラメータのモニタリング （1713 ページ）

XOR 無線に関する情報

デュアルバンド（XOR）無線は、2.4-GHz と 5-GHz のどちらのバンドでも利用できる機能や同じアクセス ポイント上で両方のバンドを受動的に監視する機能を提供します。2800/3800 シリーズ アクセス ポイント モデルは、専用のマクロ/マイクロ アーキテクチャをサポートする I モデルとマクロ/マクロをサポートする E および P モデルによってデュアル 5-GHz 帯域の動作に対応できるように設計されています。

マクロ/マイクロおよびマクロ/マクロ アーキテクチャの詳細については、「*FRA とデュアル 5 GHz の動作*」を参照してください。

XOR 無線の設定（GUI）

XOR 無線の設定：

手順

ステップ 1 [Configure] > [Access Points] > [All APs] の順に選択します。

ステップ 2 2800/3800 シリーズ アクセス ポイントのいずれかをクリックします。

ステップ 3 [Configure] をクリックします。

[XOR] タブが表示されます。XOR で更新を行う前に、[General] タブで管理者ステータスを無効にする必要があります。

XOR 無線の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、指定したアクセス ポイントでアンテナを有効にします。

ap name <Cisco AP> dot11 dual-band dot11 antenna {A | B | C | D}

ステップ 2 次のコマンドを入力して、指定したアクセス ポイントでアンテナを無効にします。

ap name <Cisco AP> no dot11 dual-band dot11 antenna {A | B | C | D}

ステップ 3 指定したアクセス ポイントに、802.11 デュアルバンド外部アンテナのゲインを設定します。

ap name <Cisco AP> dot11 dual-band antenna gain <external antenna gain value>

外部アンテナのゲイン値の範囲は 0 ～ 40 です。

（注） 外部アンテナのゲイン値を .5 dBi 単位で入力します（整数値 4 は 4 x 0.5 = 2 dBi のゲインになります）。

ステップ 4 指定したアクセス ポイントに周波数帯域を設定します。

ap name cisco1 dot11 dual-band band {24ghz | 5ghz}

ステップ 5 指定したアクセス ポイントにチャネル幅を設定します。

ap name cisco1 dot11 dual-band channel width {20 | 40 |80 | 160}

ステップ 6 指定したアクセス ポイントのチャネル数を自動に設定するか、カスタムの数に設定します。

ap name cisco1 dot11 dual-band channel {<channel number> | auto | width}

（注）
- <channel number>：範囲は 1 ～ 165 になります。
- auto：**auto** オプションを使用して、自動チャネル割り当てを有効にします。
- width：**width** オプションを使用して、802.11 デュアルバンドのチャネル幅を設定します。

ステップ 7 指定したアクセス ポイント用に指定したバンドで CleanAir を有効にします。

ap name cisco1 dot11 dual-band cleanair band {24Ghz | 5Ghz}

ステップ 8 指定したアクセス ポイント用に指定したバンドで CleanAir を無効にします。

ap name cisco1 no dot11 dual-band cleanair band {24Ghz | 5Ghz}

ステップ 9 指定したアクセス ポイントでデュアル バンド無線を無効にします。

ap name cisco1 dot11 dual-band shutdown

ステップ 10 指定したアクセス ポイントでデュアル バンド無線を有効にします。

ap name cisco1 no dot11 dual-band shutdown

ステップ 11 指定したアクセス ポイントのデュアル バンド無線の役割を設定します。

ap name cisco1 dot11 dual-band role {auto | manual {client-serving | monitor}}

（注）
- auto：無線の役割の選択を自動に切り替えます。
- manual：無線の役割の選択を手動に切り替えます。
- client-serving：client-serving モードに切り替えます。
- monitor：モニタ モードに切り替えます。

ステップ 12 指定したアクセス ポイントの RTS しきい値を設定します。

ap name cisco1 dot11 dual-band rts threshold <0-4000>

（注） <0-4000> にはしきい値をバイト単位で指定します。メッシュ アクセス ポイントの RTS しきい値のみ設定できます。

ステップ 13 指定したアクセスポイントの送信電力レベルを自動に設定するか、カスタムのレベルを設定します。

ap name cisco1 dot11 dual-band txpower {<1-8> | auto}

（注） <1-8> には送信電力レベルを指定します。

XOR 無線パラメータのモニタリング

表 *103 : XOR* 無線をモニタするコマンド

コマンド	説明
show ap name *Cisco AP* config dot11 dual-band	指定したアクセスポイント上のすべてのデュアルバンド無線の詳細情報を表示します。
show ap name *Cisco AP* auto-rf dot11 dual-band	指定したアクセス ポイントの自動 RF 情報を表示します。
show ap name *Cisco AP* wlan dot11 dual-band	指定したアクセス ポイントの WLAN 情報を表示します。

コマンド	説明
show ap config dot11 dual-band summary	すべてのデュアルバンド無線に関する詳細な情報を表示します。

第 85 章

Cisco 2800/3800 シリーズ アクセス ポイントの Flexible Radio Assignment の設定

- Flexible Radio Assignment（FRA）に関する情報 （1715 ページ）
- カバレッジ オーバーラップ ファクタ（COF） （1716 ページ）
- 無線の役割の割り当て（Radio Role Assignment） （1717 ページ）
- クライアントネットワーク設定 （1717 ページ）
- 定常状態の動作 （1718 ページ）
- FRA とデュアル 5-GHz の動作 （1718 ページ）
- Flexible Radio Assignment の設定（CLI） （1719 ページ）
- クライアント ネットワーク設定（CLI）の構成 （1720 ページ）
- Flexible Radio Assignment のリセット（CLI） （1720 ページ）
- マイクロ/マクロ モードの設定（CLI） （1721 ページ）
- マクロ/マイクロ遷移しきい値のモニタリング（CLI） （1721 ページ）
- プローブ抑制の設定（CLI） （1722 ページ）
- Flexible Radio Assignment のデバッグ（CLI） （1723 ページ）

Flexible Radio Assignment（FRA）に関する情報

Flexible Radio Assignment（FRA）は、NDP の測定値を分析するために RRM に追加された新しいコア アルゴリズムで、新しいフレキシブル無線がネットワークで果たす役割（2.4-GHz、5-GHz、Monitor）を決定するために使われるハードウェアを管理します。

FRA の役割：

- 2.4-GHz の無線について、冗長性の測定値を計算して保持し、カバレッジ オーバーラップ ファクタ（COF）と呼ばれる新しい測定メトリックとして示す。
- 冗長インターフェイスとしてマークされているインターフェイスに対する無線の役割の割り当て、または再割り当てを管理する。
- マクロ/マイクロ実装（Cisco Aironet 2800/3800 I モデル）FRA 用のデュアル 5-GHz インターフェイス間のクライアント ロード バランシング（マクロ/マイクロ遷移）を管理する。

FRA は従来の AP との混在環境で実行できるように、既存の RRM に統合されています。新しい運用方法を理解するためには、若干の新しい命名規則と動作を理解する必要があります。既存の AP のモードの概念についても変更点があります。既存のモード選択では、AP 全体（slot0 および slot1）が以下を含む複数の動作モードのいずれかに設定されます。

- Local Mode
- Monitor Mode
- Flex Connect Mode
- Sniffer Mode
- Spectrum Connect Mode

slot0 にフレキシブル（XOR）な無線を追加することによって、以前のモードの多くで無線インターフェイスごとの運用が可能になりました。AP 全体を 1 つのモードにする必要はありません。この概念を単一の無線レベルで適用するときに、これは「役割」と呼ばれます。製品リリースの時点で割り当てられる 3 つの役割は次のとおりです。

- Client Serving：2.4-GHz または 5-GHz
- Monitor：モニター モード

（注） ここで、Client Serving は、無線が選択されているバンドでクライアントをサポートするという点で Local Mode と同じです。

注意事項：

モード：AP 全体（slot0/1）に割り当てられます。

役割：単一の無線インターフェイス（slot0）に割り当てられます。

カバレッジ オーバーラップ ファクタ（COF）

FRA がカバレッジ オーバーラップ ファクタ（COF）を実行する方法とその内容について詳しく説明します。

FRA は 2.4 GHz のカバレッジのみを評価し、オーバーラップして干渉を生じさせるカバレッジの有無を判断します。デフォルトにより、Cisco Aironet 3800/2800 シリーズ AP は、1*2.4-GHz のインターフェイスと 1*5-GHz のインターフェイスを初期化します。これは従来の AP と同じ動作です。FRA が分析を完了すると、ネットワーク目標に対応するために、冗長であることがわかった無線を別のさらに有益な役割に割り当てます。

FRA は、確立済みの Neighbor Discovery Protocol（NDP）の出力を RPM から取得し、それを基に RF 範囲で各無線の位置を探し、セルごとにカバレッジのオーバーラップを評価します。FRA は、AP から得た NDP の測定値を使用して、ソリューション セットに含まれる他のすべての AP（AP グループ、物理ネイバー）との相対的な位置関係を X Y 座標に描画します。各セルの

円周は、各 AP のその時点の送信電力レベルに基づいて計算されます。これにより、AP のカバレッジの交差の論理マトリックスが生成されます。

計算されたカバレッジが FRA の感度のしきい値に一致もしくは超える場合に、無線は冗長としてマークされます。

- **低**：100% COF
- **中**：95% COF
- **高**：90% COF

COF の詳細については、『Radio Resource Management に関するホワイトペーパー』を参照してください。

無線の役割の割り当て（Radio Role Assignment）

無線が冗長としてマークされると、無線の設定によって次のステップが決定されます。フレキシブル無線は、以下の 2 つの動作状態に割り当てることができます。

- **自動**：デフォルトの動作状態です。無線はユーザの介入なしで、計算された COF に基づく FRA または DCA によって直接この状態に割り当てられます。
- **手動**：動作状態が手動でも、FRA は無線の COF を生成します。ただし、無線の割り当てはユーザが手動で完全に制御します。

無線の役割の割り当ての詳細については、『Radio Resource Management に関するホワイトペーパー』を参照してください。

クライアントネットワーク設定

クライアントネットワーク設定では、RRM の動作の優先順位付けの方法を設定できます。FRA には次のようなエントリがあります。

2.4-GHz インターフェイスに接続されているクライアントを 5-GHz インターフェイスに変更するとどうなるか見てみましょう。オプションは3つあり、FRA はデフォルトにより [Connectivity] 設定を使用します。

その 3 つのオプションは次のとおりです。

- **Connectivity**：接続に基づく設定
- **Default**：クライアントネットワーク設定を適用しない
- **Throughput**：スループットに基づく設定

無線は、CLI で元に戻すか、GUI または CLI で手動設定しない限り、2.4-GHz に戻ります。

クライアント ネットワーク設定の詳細については、『Radio Resource Management に関するホワイトペーパー』を参照してください。

定常状態の動作

FRA は 2.4-GHz スペクトラムの過密状態を評価して修復するように設計されています。5-GHz を最適化するようにネットワークを設計する場合は、冗長 2.4-GHz インターフェイスを確立します。FRA は冗長無線の選択、遷移、割り当てを管理します。

ネットワーク設計と AP の数が変わらない場合、FRA はモニタリング以外に実行することはほとんどありません。2.4-GHz の役割で利用できない AP の COF は表示できません。ただし、役割の選択と DCA はアクティブなままです。つまり、AP の追加や使用する帯域幅の変更を行う場合、5-GHz を割り当てても、FRA はフレキシブル無線に異なる役割を選択できます。こうなると、稼働中の多数のインターフェイスの安定を保つのが難しくなります。5-GHz インターフェイスがモニタ モードに変更される可能性があります。無線を手動に変更してロックをかければ、FRA がさらにアクションを実行するのを防ぐことができます。

だたし、この操作を行うと、帯域幅の変更などスペクトルのバランスを変えるような変更をする際に問題が発生する可能性があるため、メジャーなアップグレードとして対処する必要があります。

このように、2.4-GHz の役割を含まないどのフレキシブルインターフェイスでも、しばらくすると COF が利用できなくなります。

FRA とデュアル 5-GHz の動作

FRA はデュアル 5 GHz セルを管理します。デュアル 5-GHz アクセス ポイントの 2 つの動作モードは次のとおりです。

- **マクロ/マイクロ**：より小さなセルが内部にある大きなセル。単一セルの範囲内でキャパシティを倍にします。
- **マクロ/マクロ**：独立した 5-GHz のデュアル セル。単一の従来のデュアルバンド アクセス ポイントのカバレッジを倍にします。

マクロ/マイクロを使用できるのは、Cisco Aironet 3800/2800 シリーズ I モデルのみです。この AP のアンテナは、セル配置内のセルをサポートするように設計されています。

FRA と DCA では、デュアル 5-GHz マクロ/マイクロとして動作する場合、以下の設定要件が適用されます。

- 最小 100MHz でチャネルを分離（周波数の多様性）
- マイクロセル電力を最小に制限
- 各セルで同じ SSID

また、FRA は 2 つのセルを監視し、2 つのセル間のクライアント接続を最適化します。このように、パフォーマンスが同様のクライアント間で引き継ぐことで、スループットを最大化します。クライアントをマクロ セルとマイクロ セル間で移動または遷移させる方法には、以下の 3 つがあります。

- 802.11v BSS Transition
- 802.11k
- プローブ抑制

802.11v BSS Transition、802.11k、プローブ抑制の詳細については、『Radio Resource Management に関するホワイトペーパー』を参照してください。

Flexible Radio Assignment の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ap fra {interval | sensitivity {high | low | medium}}**
	例：
	`Device(config)#ap fra interval 2`
		すべてのシスコのアクセス ポイントに FRA を設定します。
		• **interval**：FRA の間隔を時間単位で設定します。範囲は 1 ～ 24 時間です。デフォルト値は 1 時間です。
		• **sensitivity**：FRA の感度レベルを設定します。
		  • **[high]**：最高の感度を指定します。
		  • **[low]**：最低の感度を指定します。
		  • **[medium]**：中間の感度を指定します。

ステップ 3	**show ap fra**	FRA の設定とオーバーラップ ファクタを表示します。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config)# end`	ンフィギュレーション モードを終了できます。

クライアント ネットワーク設定（CLI）の構成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz** } **client-network-preference** {**connectivity**| **throughput**} 例： `Device(config)#ap dot11 24 client-network-preference connectivity`	クライアント ネットワーク設定を構成します。 • **接続**：接続に基づく設定をします。 • **スループット**：スループットに基づく設定をします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Flexible Radio Assignment のリセット（CLI）

- 次のコマンドを入力して、無線を元に戻します。

  ap fra revert {**all** | **auto-only**}

  ```
  ap fra revert all
  ```

  - **all**：すべての XOR 無線を元に戻します。
  - **auto-only**：現在自動バンド選択になっている XOR 無線のみを元に戻します。

（注） 元に戻すモードで **all** または **auto-only** を選択した場合、以下のいずれかのオプションも選択する必要があります。

- **auto**：XOR 無線を自動バンド選択モードにします。
- **static**：XOR 無線をスタティック 2.4-GHz バンドにします。

マイクロ/マクロ モードの設定（CLI）

Cisco Aironet 2800/3800 I シリーズ アクセス ポイント モデルの XOR 無線を 5 GHz 帯域で動作するように変更すると、コントローラは slot0 を最も低い電力レベルにします。このため、マイクロ/マクロセルが形成されます。

マイクロ/マクロ モードを設定するには、次の手順に従います。

手順

ステップ 1 次のコマンドを入力し、シスコのアクセス ポイントでデュアルバンド無線を無効にします。

ap name *ap-name* **dot11 dual-band shutdown**

ステップ 2 無線の役割が**auto** または **manual** の場合は、次のコマンドを入力して **client-serving** に役割を変更する必要があります。

ap name *ap-name* **dot11 dual-band role manual client-serving**

ステップ 3 次のコマンドを入力し、動作帯域（5-GHz）を設定します。

ap name *ap-name* **dot11 dual-band band 5ghz**

ステップ 4 次のコマンドを入力し、シスコのアクセス ポイントでデュアルバンド無線を有効にします。

ap name *ap-name* **no dot11 dual-band shutdown**

マクロ/マイクロ遷移しきい値のモニタリング（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**wireless macro-micro steering transition-threshold** {**balancing-window** *no_of_clients*| **client count** *no_of_clients*| **macro-to-micro** *RSSI_in_dBm*| **micro-to-macro** *RSSI_in_dBm*} 例： `Device(config)#wireless macro-micro steering transition-threshold balancing-window 1000`	マイクロ/マクロ遷移しきい値を設定します。 • **balancing-window**：マイクロ/マクロ クライアント ロード バランシングの範囲を設定します。*no_of_clients* の値の範囲は 0 ～ 65535 です。 • **client**：マイクロ/マクロ クライアント パラメータを設定します。*no_of_clients* の値の範囲は 0 ～ 65535 です。 • **macro-to-micro**：マクロ/マイクロ遷移の RSSI を設定します。*RSSI_in_dBm* の値の範囲は -128 ～ 0 です。 • **micro-to-macro**：マイクロ/マクロ遷移の RSSI を設定します。*RSSI_in_dBm* の値の範囲は -128 ～ 0 です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

プローブ抑制の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless macro-micro steering probe-suppression** {**aggressiveness** *no_of_cycles*| **hysteresis** *RSSI_in_dBm*| **probe-auth** | **probe-only** }	マイクロ/マクロ プローブ抑制を設定します。

	コマンドまたはアクション	目的
	例： `Device(config)#wireless macro-micro steering probe-suppression probe-only`	• **aggressiveness**：抑制するプローブサイクルを設定します。*no_of_cycles* の値の範囲は 0 ～ 255 です。 • **hysteresis**：ヒステリシスを設定します。*RSSI_in_dBm* の値の範囲は -6 ～ -3 です。 • **probe-auth**：プローブと single auth の両方を抑制します。 • **probe-only**：プローブのみを抑制します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Flexible Radio Assignment のデバッグ（CLI）

- 次のコマンドを入力して、FRA のデバッグを実行します。

  set platform software trace wireless switch active R0 rrm-fra {**noise | verbose**}

  ```
  set platform software trace wireless switch active R0 rrm-fra noise
  ```

  - **noise**：可能性のある最大メッセージ
  - **verbose**：詳細デバッグ メッセージ

第 86 章

設定の最適化されたローミング

- ローミングの最適化について （1725 ページ）
- ローミングの最適化の制約事項 （1726 ページ）
- ローミングの最適化の設定（CLI） （1726 ページ）

ローミングの最適化について

ローミングの最適化は、遠隔地のアクセスポイントに長時間アソシエートし続けているクライアントや、接続が不安定な Wi-Fi ネットワークに接続を試みるアウトバウンドクライアントの問題を解決します。この機能は、クライアント データ パケットの RSSI とデータ レートに基づいてクライアントをアソシエート解除します。クライアントは、RSSI アラーム条件が満たされ、現在のデータ レートが最適化ローミング データ レートのしきい値を下回っている場合にアソシエート解除されます。データ レート オプションを無効にして、RSSI のみをクライアントのアソシエート解除に使用するようにできます。

ローミングの最適化は、クライアントの RSSI が低いときにもクライアント アソシエーションを阻止します。この機能は、RSSI しきい値に照らして受信クライアントの RSSI をチェックします。このチェックで、クライアントに有効な接続がない限り、クライアントの Wi-Fi ネットワークへの接続が阻止されます。クライアントはビーコンを受信して Wi-Fi ネットワークに接続できても、信号が弱いために安定した接続をサポートできない場合がよくあります。

ローミングの最適化を使用することによって、無線に対してクライアント カバレッジ レポート間隔を設定することもできます。クライアント カバレッジの統計情報には、データ パケット RSSI、カバレッジ ホールの検出および軽減（CHDM）の事前アラーム障害、再送信要求と現在のデータ レートが含まれます。

最適化されたローミングは、以下のシナリオで実行します。

- クライアントのしつこいアクセス操作に対処して、事前にクライアントを切断する。
- データ RSSI パケットを能動的に監視する。
- RSSI が、設定されたしきい値よりも低くなるとクライアントのアソシエーションを解除する。

ローミングの最適化の制約事項

- 802.11a/b ネットワークを無効にするまで、ローミングの最適化の間隔を設定できません。

ローミングの最適化の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、ローミングの最適化を有効にします。

ap dot11 5ghz rrm optimized-roam

デフォルトでは、ローミングの最適化は無効になっています。

ステップ 2 次のコマンドを入力して、802.11a ネットワークのクライアント カバレッジのレポート間隔を設定します。

ap dot11 5ghz rrm optimized-roam reporting-interval *interval-seconds*

範囲は 5 ～ 90 秒です。デフォルト値は 90 秒です。

（注） ローミングの最適化のレポート間隔を設定する前に、802.11a ネットワークを無効にする必要があります。

ステップ 3 次のコマンドを入力して、802.11a ネットワークのしきい値データ レートを設定します。

ap dot11 5ghz rrm optimized-roam data-rate-threshold *mbps*

802.11a の場合、設定可能なデータ レートは、1、2、5.5、6、9、11、12、18、24、36、48、および 54 です。データ レートを無効にするには DISABLED を設定します。

ステップ 4 このコマンドを入力して、各帯域のローミングの最適化の情報を表示します。

show ap dot11 5ghz optimized-roaming

```
(Cisco Controller) > show ap dot11 5ghz optimized-roaming
802.11a OptimizedRoaming

  Mode                                  : Disabled
  Reporting Interval                    : 90 seconds
  Rate Threshold                        : Disabled
```

ステップ 5 次のコマンドを入力して、最適なローミング統計に関する情報を表示します。

show ap dot11 5ghz optimized-roaming statistics

```
(Cisco Controller) > show ap dot11 5ghz optimized-roaming statistics
802.11a OptimizedRoaming statistics

  Disassociations                       : 0
```

```
Rejections                          : 0
```

第 87 章

設定の Rx SOP

- Rx-SOP に関する情報 （1729 ページ）
- Rx SOP の設定（CLI） （1729 ページ）

Rx-SOP に関する情報

レシーバのパケット検出開始しきい値（Rx SOP）は、アクセス ポイントの無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。Wi-Fi レベルが上がると、無線の受信感度が下がり、レシーバのセル サイズが小さくなります。セル サイズの減少は、ネットワークのクライアントの分散に影響します。

RF リンクが脆弱なクライアント、つなぎっぱなしのクライアント、およびアクセス ポイント全体で負荷分散しているクライアントに対処するために Rx SOP が使用されます。Rx SOP は、アクセス ポイントが最も近くにある最も強力なクライアントを最適化する必要のあるスタジアムやホールなどの高密度展開でネットワーク性能を最大限引き出すのに役立ちます。

Rx SOP の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、Rx SOP モードを設定します。

ap dot11 {24ghz | 5ghz} rx-sop threshold {auto | high | low | medium}

ステップ 2 Rx SOP の高密度パラメータを確認します。

show ap dot11 24ghz high-density

```
Controller# show ap dot11 24ghz high-density
Receiver Start-of-Packet threshold: auto
Multicast Data Rate: auto
AP Name : AP5475.d064.0552
```

```
Receiver Start-of-Packet threshold: auto
Multicast Data Rate: auto 2:33 PM
```

第 88 章

AirTime Fairness の設定

- Air Time Fairness について （1731 ページ）
- AirTime Fairness の設定、表示、および変更 （1733 ページ）

Air Time Fairness について

Cisco High Density Experience（HDX）向けの Cisco Air Time Fairness（ATF）は、ダウンリンクの通信時間を調整するワイヤレス Quality of Service（QoS）として機能します。この機能を使用して、ネットワーク管理者は、一部のグループが他のグループよりも頻繁に WLAN からトラフィックを受信できるようにするポリシーを作成して適用できます。

Cisco ATF には次の機能があります。

- ユーザ グループまたはデバイス カテゴリに対して Wi-Fi の通信時間を割り当てる。
- Cisco ATF は、ネットワークではなくネットワーク管理者が定義する。
- 簡単な仕組みで通信時間を割り当てることができる。
- WLAN の状態の変化に動的に対応できる。
- サービス レベル契約を効率的に実行できる。
- 各種の標準規格に準拠した Wi-Fi QoS のメカニズムを強化できる。

環境内でクライアント グループごとの通信中時間面の公平さの意味するものを定義する能力をネットワーク マネージャに与えることで、トラフィック量も制御することができます。

ポリシーは、ネットワーク内のデータ パケットを許可、回避、および優先順位付けするために作成されます。作成されるすべてのポリシーには、ネットワークでのそのポリシーの重要性を示す重み値を設定する必要があります。重み値は、5 ～ 100 の範囲で割り当てることができます。WLAN にポリシーが割り当てられていない場合は、重み値 10 が設定されたデフォルトのポリシー（ポリシー ID 0）がシステムによって割り当てられます。重み値は、ポリシーに割り当てられる通信時間のパーセンテージに影響します。通信時間のパーセンテージは、ユーザによる操作なしでシステムによって計算されます。したがって、WLAN およびポリシーがネットワークに追加されたりネットワークから削除されると、通信時間のパーセンテージは自動的に変更されます。

（注） パーセンテージが変化すると、変更された値が新しいトラフィックに最適でない場合があります。

たとえば、ネットワークにポリシー値 5、10、および 35 を持つ WLAN が 3 つある場合、通信時間パーセンテージの計算は、重み値 5 の場合は 10% となり、重み値 10 と 35 の場合はそれぞれ 20% と 70% の通信時間となります。重み 15 の新しいポリシーを追加すると、システムは 7.7%、15.38%、23.07%、および 53.84% として、つまり重み値をそれぞれ 5、10、15、35 として通信時間のパーセンテージを計算し直します。

Cisco ATF には 3 つのモードがあり、モードごとに 3 つのレベルに分割できるため、設定時に柔軟性が得られます。3 つのモードは次のとおりです。

- 無効モード：ATF が Cisco WLC で無効になります。デフォルトのオプションは [Disable] です。
- モニタ モード：ユーザは次の操作を実行できます。
  - 通信時間の表示
  - すべての AP 送信の通信時間の報告
  - レポートの表示
    - SSID/WLAN 単位
    - AP グループ単位
    - AP 単位
  - 通信時間の使用量の定期報告
  - ブロック ACK は報告しません
  - モニタ モードの一部としての適用は無効です
- 適用ポリシー モード：ユーザは次の機能を実行できます。
  - 設定したポリシーに基づいて通信時間を適用
  - 次の項目に通信時間を適用
    - 単独の WLAN
    - Cisco WLC ネットワーク内で接続されているすべての AP
    - 単独の AP グループ
    - AP
  - WLAN ごとの厳密な適用：無線の WLAN で使用される通信時間はポリシーの設定制限まで厳密に適用されます。

- WLAN 単位の最適な適用：割り当てられている通信時間を使用していない他の SSID から未使用の通信時間を共有します。

（注） AP グループ グローバル設定と AP レベルごとの特権 EXEC コマンドは、WLAN に適用されているポリシーと無線レベルで適用されている Air Time Fairness モードを上書きできます。

AirTime Fairness の設定、表示、および変更

Cisco Air Time Fairness の設定（CLI）

Cisco Air Time Fairness（ATF）機能は、次の CLI を使用して設定できます。

- Cisco ATF をポリシー適用モードまたはモニタ モードで有効にするには、次のコマンドを入力します。

  ap dot11 {**24ghz** | **5ghz**} **airtime-fairness mode** {**enforce-policy** | **monitor**}

- Cisco ATF をポリシー適用モードまたはモニタ モードで無効にするには、次のコマンドを入力します。

  no ap dot11 {**24ghz** | **5ghz**} **airtime-fairness mode** {**enforce-policy** | **monitor**}

- 新しい ATF ポリシーを作成し、ポリシーの重みを適用するには、次のコマンドを入力します。

  1. **controller#configure terminal**
  2. **controller(config)# ap dot11 airtime-fairness policy-name** *policy-name policy-id*
  3. **controller(config-airtime-fairness policy)# policy-weight** *policy-weight*

  ポリシーの重みの範囲は 05 ～ 100 です。対応する WLAN にポリシーが適用されていない場合は、デフォルト値 10 が適用されます。

- ポリシーを削除するには、次のコマンドを入力します。

  no ap dot11 airtime-fairness policy-name *policy-name*

- WLAN に Cisco ATF ポリシーを設定するには、次のコマンドを使用します。

  1. **controller#configure terminal**
  2. **controller(config)# wlan** *wlan-name*
  3. **controller(config-wlan)# airtime-fairness policy** *policy-name*

- AP グループに Cisco ATF モードを設定するには、次のコマンドを使用します。

  1. **controller#configure terminal**
  2. **controller(config)# ap group** *apgroup-name*
  3. **controller(config-apgroup)#** no **airtime-fairness dot11** {**24ghz** | **5ghz**} **mode** {**enforce-policy** | **monitor**}

- AP グループに Cisco ATF の最適化を設定するには、次のコマンドを使用します。
  1. **controller#configure terminal**
  2. **controller(config)# ap group** *apgroup-name*
  3. **controller(config-apgroup)#** no **airtime-fairness dot11** {**24ghz** | **5ghz**} **optimization**
- AP 固有の WLAN リスト経由で WLAN に適用済みポリシーのオーバーライドを設定するには、次のコマンドを使用します。
  1. **controller#configure terminal**
  2. **controller(config)# ap group** *apgroup-name*
  3. **controller(config-apgroup)# wlan** *wlan-name*
  4. **controller(config-wlan-apgroup)#** no **airtime-fairness dot11** {**24ghz** | **5ghz**} **policy** *policy-name*
- WLAN に Cisco ATF ポリシーを設定するには、次のコマンドを使用します。
  1. **controller# configure terminal**
  2. **controller(config)# wlan** *wlan-name*
  3. **controller(config-wlan)# airtime-fairness policy** *policy-name*
- ワイヤレス ATF の統計情報をクリアするには、次のコマンドを入力します。
  1. **controller# clear wireless airtime-fairness statistics**

Cisco Air Time Fairness の表示（CLI）

Cisco Air Time Fairness（ATF）機能の設定は、次の CLI を使用して表示できます。

- 設定されたすべてのポリシーを表示するには、次のコマンドを入力します。

  show ap airtime-fairness policy
- 設定済み WLAN のリストと、適用された ATF ポリシーを表示するには、次のコマンドを入力します。

  show ap airtime-fairness wlan
- 特定の AP グループの ATF 設定を表示するには、次のコマンドを入力します。

  show ap airtime-fairness ap-group *group-name*
- 無線ごとの ATF 設定を含む AP リストを表示するには、次のコマンドを入力します。

  show ap airtime-fairness
- 2.4-GHz および 5-GHz 無線に設定された ATF を含む AP リストを表示するには、次のコマンドを入力します。

  show ap dot11 {**24ghz** | **5ghz**} **airtime-fairness**
- 特定の AP の ATF 設定を表示します

  show ap name *ap-name***airtime-fairness**
- 指定された ATF ポリシーの統計情報を表示します

show ap name *ap-name***dot11** {**24ghz** | **5ghz**} **airtime-fairness policy** *policy-name* **statistics**

- 特定の AP でアクティブな指定された WLAN の ATF 統計情報を表示します

  show ap name *ap-name***dot11** {**24ghz** | **5ghz**} **airtime-fairness wlan name** *wlan-name***statistics**

- WLAN ごとの ATF 統計情報を表示します

  show ap name *ap-name***dot11** {**24ghz** | **5ghz**} **airtime-fairness summary**

AP の AirTime Fairness パラメータの変更（CLI）

次のコマンドでは、特定の AP ATF パラメータの変更ができます。ユーザは、これらのコマンドを使用して、AP ごとに ATF ポリシーの有効化、無効化、変更、または上書きを行うことができます。

- 特定の AP に対し、ATF をポリシー適用モードまたはモニタ モードで有効にします。

  ap name *ap-name***dot11** {**24ghz** | **5ghz**} **airtime-fairness mode** {**enforce-policy** | **monitor**}

- 特定の AP に対し、ATF をポリシー適用モードまたはモニタ モードで無効にします。

  ap name *ap-name***no dot11** {**24ghz** | **5ghz**} **airtime-fairness mode** {**enforce-policy** | **monitor**}

- 特定の AP の ATF 最適化を有効にします。

  ap name *ap-name***dot11** {**24ghz** | **5ghz**} **airtime-fairness optimization**

- 特定の AP の ATF 最適化を無効にします。

  ap name *ap-name***no dot11** {**24ghz** | **5ghz**} **airtime-fairness optimization**

- 1 つの AP に固有の WLAN でポリシーを上書きします

  ap name *ap-name***dot11** {**24ghz** | **5ghz**} **airtime-fairness wlan-name** *wlan-name***policy-name** *policy-name*

- WLAN に固有の WLAN で ATF ポリシーのオーバーライドを無効にします

  ap name *ap-name***no dot11** {**24ghz** | **5ghz**} **airtime-fairness wlan-name** *wlan-name*

第 89 章

CA での RF プロファイルの設定

- CA での RF プロファイルの前提条件 （1737 ページ）
- CA での RF プロファイルの制約事項 （1737 ページ）
- CA での RF プロファイルについて （1738 ページ）
- RF プロファイルのカスタマイズ （1739 ページ）
- CA での RF プロファイルの設定方法 （1741 ページ）

CA での RF プロファイルの前提条件

最新の RF プロファイル設定が AP グループ（新規または変更済み）に適用されます。AP グループの各コントローラに適用されるものと同じ RF プロファイルのルールが適用されます。そうでないと、アクティベーションはそのコントローラで失敗します。

（注） 同じ RF プロファイルを複数の AP グループに割り当てることができます。

CA での RF プロファイルの制約事項

- 一元化モードを有効にすると、再起動時に設定が失われるので、再設定する必要があります。

  （注） Cisco Communications Media Module（CMM）機能は廃止される予定です。

- 設定は、MC およびすべての MA で全く同じである必要があります。
- AP のカスタム電源設定はサポートされていません。
- RF プロファイルは、チャネルおよび送信電力（TPC）がすべての AP で RRM によって管理されている場合にのみアクティブになります。

- AP グループに適用される RF プロファイルは削除できません。
- 設定を変更するには、AP グループに割り当てられている RF プロファイルをシャットダウンする必要があります。
- どちらかのバンドで AP グループ内の RF プロファイルの割り当てを変更すると、AP がリブートします。

CA での RF プロファイルについて

コンバージド アクセス（CA）で RF プロファイル（ローカル モードのみ）を使用すると、一般的な無線設定を共有する AP グループをカスタマイズできます。特別な RF プロファイルは 802.11 帯域ごとに作成できます。これらの RF プロファイルには、既存のすべての RF パラメータのデフォルト設定、および追加の新しい設定があります。

最近インストールされた AP は、「デフォルト グループ」の AP グループにデフォルトで割り当てられます。無線は、RF 干渉を除去するために無効になっています。新しい AP に RF プロファイル設定を適用する必要がある場合は、手動で AP グループに追加する必要があります。

RF プロファイルは、AP グループに属するすべての AP に適用され、そのグループ内のすべての AP に同じプロファイルが設定されます。RF プロファイルがアタッチされている AP グループ内の AP の設定の優先順位は次のとおりです。

1. AP 固有。
2. RF プロファイル。
3. 国際窓口：

Rx SOP とマルチキャスト データ レートのプライオリティは、この優先順位に従いません。これらは次のルールに従います。

- AP が RF プロファイルがアタッチされている AP グループ内にあり、RF プロファイル設定と AP 固有の設定の間である場合、最後に行われた設定が優先されます。
- AP が AP グループにない場合、または AP グループに RF プロファイルがなく、グローバル コンフィギュレーションと AP 固有の設定の間である場合、最後に行われた設定が優先されます。
- RF プロファイルが削除されると、最後の RF のプロファイル設定が AP に保存されます。この保存された設定は、AP が再度追加された場合に適用されます。

CA での RF プロファイル機能によって、次の設定をカスタマイズできます。

- バンド選択設定。
- カバレッジ ホール軽減設定。
- 動的チャネル割り当て（DCA）設定。
- 高密度設定。

- ロード バランシング設定。
- スタジアム ビジョン設定。
- 伝送パワー コントロール（TPC）設定。

RF プロファイルのカスタマイズ

バンド選択設定

この設定は、クライアント機能を確認することで、2.4-GHz 帯域と 5-GHz 帯域の間のクライアント分散に対処します。WLAN で帯域選択を有効にすると、2.4 GHz 帯域を AP に抑制させ、デュアルバンドクライアントを 5 GHz 帯域に移動することができます。次の帯域選択パラメータを AP グループごとに設定できます。

- プローブ応答：クライアントへのプローブ応答。この機能は有効または無効にすることができます。
- プローブ サイクル回数：RF プロファイルのプローブ サイクル回数。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。
- サイクルしきい値：RF プロファイル帯域選択を新しくスキャンするサイクル期間の時間しきい値。この設定は、クライアントからの新しいプルーブ要求が新しいスキャン サイクルで送信される間の時間しきい値を決定します。
- 失効抑制期間：以前に認識されていた 802.11b/g クライアントをプルーニングするための期限切れ時間。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
- デュアルバンドの失効：以前に認識されていたデュアルバンドクライアントをプルーニングするための期限切れ時間。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
- クライアント RSSI：クライアントがプローブに応答するための最小 RSSI。

カバレッジ ホール軽減設定

カバレッジ ホールを軽減するために、次のパラメータをこの機能の下に設定できます。

- データ RSSI：アクセス ポイントで受信されたデータ パケットの最小の受信信号強度インジケータ（RSSI）値。入力する値は、ネットワーク内のカバレッジ ホール（またはカバレッジが不完全な領域）を特定するのに使用されます。
- Voice RSSI：アクセス ポイントで受信された音声パケットの最小の受信信号強度インジケータ（RSSI）値。

- カバレッジ例外：アクセスポイント上で、信号レベルが低くなっているにもかかわらず、別のアクセス ポイントにローミングできないクライアントの割合。アクセス ポイントに設定されたカバレッジ レベルよりも多くこのようなクライアントが存在する場合、カバレッジ ホール イベントがトリガーされます。
- カバレッジ レベル：カバレッジ ホール例外をトリガーする、データまたは音声 RSSI しきい値以下の RSSI 値を持つアクセス ポイント上のクライアントの最小数。

動的チャネル割り当て設定

動的チャネル割り当て（DCA）では、次のパラメータをこの機能の下に設定できます。

- Avoid foreign AP interference：DCA アルゴリズムは、外部 802.11 トラフィックのアクセスポイントから検出されたトラフィックや干渉など、複数の入力での最適化に基づいています。各アクセス ポイントでは定期的に干渉、ノイズ レベル、外部干渉および負荷を測定し、ネイバー AP のリストを管理します。外部 AP 干渉は、802.11 非ネイバーから受信されるものです。この干渉は、ノイズ レベルと同じメカニズムを使用して測定されます。
- Channel width：次のチャネル幅のオプションのいずれかを選択して、5 GHz 帯域のすべての 802.11n および 802.11ac 無線でサポートするチャネル帯域幅を指定できます。
  - [20 MHz]：20 MHz は、2.4 GHz に許可された最大チャネル幅でもあります。これは、チャネル幅のデフォルト値です。
  - [40 MHz]：40 MHz のチャネル帯域幅。
  - [80 MHz]：80 MHz のチャネル帯域幅。
- DCA channel list：DCA がアクセス ポイント無線にチャネルの 1 つを割り当てるために使用するチャネル セットを選択できます。RF プロファイル用に選択されるチャネル セットは、DCA グローバル チャネル リストのサブセットにする必要があります。利用可能なチャネルはグローバルに設定された国に基づいて事前に選択されます。DCA は、これらのチャネル上で測定されるメトリックを比較して、最適なチャネルを選択します。
- Trap thresholds：トラップのプロファイルしきい値は、RF プロファイルに基づいて特定の AP グループに対して設定できます。

高密度設定

密集ワイヤレス ネットワークの RF 環境を最適化するために、次の設定を使用できます。

- WLAN または無線ごとのクライアントの制限：高密度環境の AP と通信できるクライアントの最大数。
- クライアント トラップしきい値：アクセス ポイントにアソシエートされるクライアント数のしきい値。この値以降、SNMP トラップがコントローラと Cisco Prime Infrastructure に送信されます。

ロード バランシング設定

ロード バランシングは、AP にわたるクライアントの適正な分散を維持します。次のパラメータを設定できます。

- ウィンドウ：ロード バランシングは、クライアントのウィンドウ サイズを適用することによって、クライアント アソシエーションの制限を設定します。
- 拒否：拒否数は、ロードバランシング中のアソシエーション拒否の最大数を設定します。

スタジアム ビジョン設定

スタジアム ビジョンの場合、次のパラメータをこの機能の下に設定できます。

- マルチキャスト データ レート：AP の RF 条件に基づく、設定可能なマルチキャスト トラフィックのデータ レート。

伝送パワー コントロール設定

伝送パワー コントロール（TPC）では、次のパラメータをこの機能の下に設定できます。

- 最小電力：RF プロファイルが適用される AP グループに属する AP に許可された最小電力。
- 最大電力：RF プロファイルが適用される AP グループに属する AP に許可された最大電力。
- しきい値：最も強力なネイバーの電力が設定したしきい値を上回ると、RRM は RF プロファイルが適用されている AP グループ内の AP に対して実行されます。

CA での RF プロファイルの設定方法

RF プロファイル パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**ap dot11 24ghz rf-profile** *profile-name* 例： `Device(config)# ap dot11 24ghz rf-profile doctest`	選択されたバンドの RF プロファイルの設定。

	コマンドまたはアクション	目的
ステップ 2	**band-select client rssi** *value* 例： `Device(config-rf-profile)#band-select client rssi -50`	プローブを開始またはプローブに応答するための、バンド選択クライアントしきい値を最小dBmでクライアントに設定します。 （注） このオプションは 2.4GHz 帯域でのみ使用できます。
ステップ 3	**channel add** *channel#* 例： `Device(config-rf-profile)# channel add 2`	このコマンドは、RFプロファイルDCAチャネル リストにデフォルト以外のチャネルを追加します。
ステップ 4	**channel delete** *channel#* 例： `Device(config-rf-profile)# channel delete 2`	delete コマンドを使用すると、RF プロファイル DCA チャネル リストからデフォルトのチャネルが削除されます。
ステップ 5	**channel width** *value* 例： `Device(config-rf-profile)# channel width 40`	RF プロファイル DCA チャネル幅を設定します。 （注） このオプションは 5GHz 帯域でのみ使用できます。
ステップ 6	**coverage voice rssi threshold** *value* 例： `Device(config-rf-profile)# coverage voice rssi threshold -50`	音声パケットのカバレッジホール検出用の RF プロファイル カバレッジおよび RSSI しきい値を設定します。
ステップ 7	**coverage exception** *value* 例： `Device(config-rf-profile)# coverage exception 60`	Cisco AP カバレッジの例外レベルを設定します。
ステップ 8	**dot11n-only** 例： `Device(config-rf-profile)# channel dot11n-only`	RF プロファイルの 802.11n クライアント専用モードを有効にします。

	コマンドまたはアクション	目的
ステップ 9	**load-balancing denial** *value* 例： `Device(config-rf-profile)# load-balancing denial 8`	RF プロファイルのロード バランスおよびロードバランシングの拒否数を設定します。
ステップ 10	**high-density clients count** *value* 例： `Device(config-rf-profile)# high-density clients count 160`	RF プロファイル高密度クライアントカウントの値を設定します。
ステップ 11	**rate** *rate* **disable** 例： `Device(config-rf-profile)# rate RATE_1M disable`	選択されたレートプロファイルに対し 802.11 運用レートを無効にします。
ステップ 12	**trap threshold clients** *value* 例： `Device(config-rf-profile)# trap threshold clients 145`	トラップが設定された後、AP に関連付けられているクライアント数への RF プロファイル トラップしきい値を設定します。
ステップ 13	**tx-power min** *value* 例： `Device(config-rf-profile)# tx-power min -10`	最小送信電力レベルを設定します。
ステップ 14	**Shutdown** 例： `Device(config-rf-profile)# Shutdown`	プロファイルをシャットダウンし、ネットワークを無効にします。
ステップ 15	**ap group** *group-name* 例： `Device(config)# ap group docgroup`	AP グループに RF プロファイルを設定します。
ステップ 16	**remote-lan** *rlan-name* 例： `Device(config-apgroup)#remote-lan labtest`	AP グループへのリモート LAN の設定。

	コマンドまたはアクション	目的
ステップ 17	**wlan** *wlan-name* 例： `Device(config-apgroup)#wlan labwantest`	AP グループへの WLAN の設定。
ステップ 18	**rf-profile dot11 24ghz** *profile-name* 例： `Device(config-apgroup)#rf-profile dot11 24ghz doctest`	AP グループへの 802.11b RF プロファイルの設定。
ステップ 19	**rf-profile dot11 5ghz** *profile-name* 例： `Device(config-apgroup)#rf-profile dot11 5ghz doc5test`	AP グループへの 802.11a RF プロファイルの設定。
ステップ 20	**show ap rf-profile name** *profile-name* **detail** 例： `Device#show ap rf-profile name doctest detail`	RF プロファイル設定の詳細を表示します。
ステップ 21	**show ap rf-profile summary** 例： `Device#show ap rf-profile summary`	RF プロファイルの要約を表示します。
ステップ 22	**show ap groups** 例： `Device#show ap groups`	ap グループの概要を表示します。

第 XVI 部

ルーティング

- 双方向フォワーディング検出の設定 （1747 ページ）
- MSDP の設定 （1773 ページ）
- IP ユニキャスト ルーティングの設定 （1803 ページ）

第 90 章

双方向フォワーディング検出の設定

- 双方向フォワーディング検出 （1747 ページ）

双方向フォワーディング検出

このマニュアルでは、双方向フォワーディング検出（BFD）プロトコルをイネーブルにする方法について説明します。BFDはあらゆるメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。

BFDは高速転送パス障害検出に加えて、ネットワーク管理者向けの整合性のある障害検出方法を提供します。ネットワーク管理者はBFDを使用して、さまざまなルーティング プロトコルの helloメカニズムで、変動速度ではなく一定速度で転送パスの障害を検出できるため、ネットワークプロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

双方向フォワーディング検出の前提条件

- シスコ エクスプレス フォワーディングおよび IP ルーティングが、関連するすべてのスイッチでイネーブルになっていること。

- BFD を導入する前に、BFD でサポートされる IP ルーティング プロトコルのいずれかをスイッチで設定しておくこと。使用しているルーティングプロトコルの高速コンバージェンスを実装する必要があります。高速コンバージェンスの設定については、お使いのバージョンの Cisco IOS ソフトウェアの IP ルーティングのマニュアルを参照してください。Cisco IOS ソフトウェアの BFD ルーティング プロトコルのサポートの詳細については、「双方向フォワーディング検出の制約事項」の項を参照してください。

双方向フォワーディング検出の制約事項

- BFD は直接接続されたネイバーだけに対して動作します。BFD のネイバーは 1 ホップ以内に限られます。マルチホップのコンフィギュレーションはサポートされません。
- プラットフォームおよびインターフェイスによっては、BFDサポートを利用できないものがあります。特定のプラットフォームまたはインターフェイスで BFD のサポートについて確認し、プラットフォームとハードウェアの正確な制約事項を入手するには、お使いのソフトウェア バージョンの Cisco IOS ソフトウェアのリリース ノートを参照してください。
- BFD パケットは自己生成パケットの QoS ポリシーでは一致しません。
- BFD パケットは **classclass-default** コマンドで一致します。そのため、ユーザは適切な帯域幅の可用性を確認して、オーバーサブスクリプションによる BFD パケットのドロップを防ぐ必要があります。
- BFD HA のサポートは、Cisco Denali IOS XE 16.3.1 では使用できません。

双方向フォワーディング検出について

BFD の動作

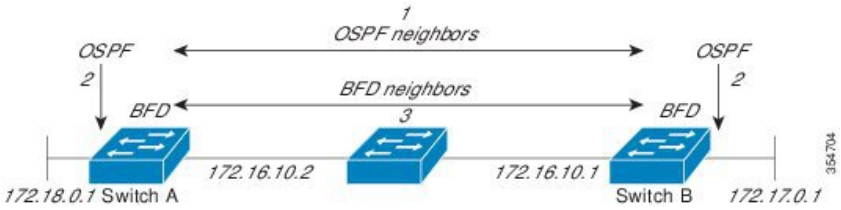
BFD は、インターフェイス、データリンク、および転送プレーンを含めて、2 つの隣接ルータ間の転送パスで、オーバーヘッドの少ない短期間の障害検出方法を提供します。

BFD はインターフェイス レベルおよびルーティング プロトコル レベルでイネーブルにする検出プロトコルです。シスコではBFD非同期モードをサポートしています。このモードは、2 台のシステム間で BFD 制御パケットを送信することでルータ間の BFD ネイバー セッションをアクティブ化して維持します。したがって、BFDセッションを作成するには、両方のシステムで（または BFD ピアで）BFD を設定する必要があります。適切なルーティング プロトコルに対して、インターフェイス レベルおよびルータ レベルで BFD がイネーブルになっている場合、BFD セッションが作成されて BFD タイマーがネゴシエートされ、ネゴシエートされた間隔で BFD ピアが互いに BFD 制御パケットの送信を開始します。

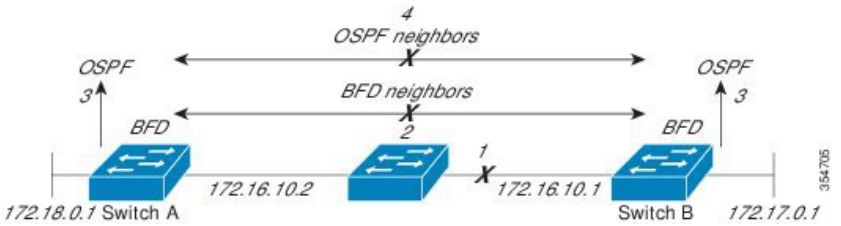
ネイバー関係

BFD はあらゆるメディア タイプ、カプセル化、トポロジ、ルーティング プロトコル BGP、EIGRP、IS-IS、および OSPF の個別の高速 BFD ピア障害検出時間を提供します。ローカル ルー

タのルーティング プロトコルに高速障害検出通知を送信して、ルーティング テーブル再計算プロセスを開始すると、BFD はネットワーク コンバージェンス時間全体を大幅に短縮できます。下の図に、OSPF と BFD を実行する 2 台のルータがある単純なネットワークを示します。OSPF がネイバー（1）を検出すると、OSPF ネイバー ルータ（2）で BFD ネイバー セッションを開始する要求が、ローカル BFD プロセスに送信されます。OSPF ネイバー ルータでの BFD ネイバー セッションが確立されます（3）。



以下の図に、ネットワークで障害が発生した場合を示します（1）。OSPF ネイバー ルータでの BFD ネイバー セッションが停止されます（2）。BFD はローカル OSPF プロセスに BFD ネイバーに接続できなくなったことを通知します（3）。ローカル OSPF プロセスは OSPF ネイバー関係を解除します（4）。代替パスを使用できる場合、ルータはただちにコンバージェンスを開始します。



ルーティング プロトコルでは、取得したネイバーそれぞれについて、BFD で登録する必要があります。ネイバーが登録されると、セッションがまだ存在していない場合、BFD によって、ネイバーとのセッションが開始されます。

次のとき、OSPF では、BFD を使用して登録が行われます。

- ネイバーの有限状態マシン（FSM）は、Full ステートに移行します。
- OSPF BFD と BFD の両方がイネーブルにされます。

ブロードキャスト インターフェイスでは、OSPF によって、指定ルータ（DR）とバックアップ指定ルータ（BDR）とともにのみ、BFD セッションが確立されますが、DROTHER ステートのすべての 2 台のルータ間では確立されません。

BFD の障害検出

BFD セッションが確立され、タイマーの取り消しが完了すると、BFD ピアは IGP hello プロトコルと同様に動作する（ただし、より高速な）、BFD 制御パケットを送信して状態を検出します。次の点に注意する必要があります。

- BFD はフォワーディング パスの障害検出プロトコルです。BFD は障害を検出しますが、障害が発生したピアをバイパスするには、ルーティング プロトコルがアクションを実行する必要があります。

- Cisco IOS XE Denali 16.3.1 では、シスコ デバイスは BFD バージョン 0 をサポートします。このバージョンでは、デバイスは実装時に複数のクライアント プロトコルに 1 つの BFD セッションを使用します。たとえば、同じピアへの同じリンクを介してネットワークで OSPF および EIGRP を実行している場合、1 つの BFD セッションだけが確立され、BFD で両方のルーティング プロトコルとセッション情報を共有します。

BFD バージョンの相互運用性

デフォルトでは、すべての BFD セッションがバージョン 1 で実行され、バージョン 0 と相互運用可能です。システムで自動的に FD バージョン検出が実行される場合、ネイバー間の BFD セッションがネイバー間の最も一般的な BFD バージョンで実行されます。たとえば、BFD ネイバーが BFD バージョン 0 を実行し、他の BFD ネイバーがバージョン 1 を実行している場合、セッションで BFD バージョン 0 が実行されます。**showbfdneighbors** [**details**] コマンドの出力で、BFD ネイバーが実行している BFD バージョンを確認できます。

BFD バージョンの検出の例については、エコー モードがデフォルトでイネーブルになった EIGRP ネットワークでの BFD の設定の例を参照してください。

BFD セッションの制限

Cisco IOS XE Denali 16.3.1 では、作成できる BFD セッションの数が 100 に増えました。

非ブロードキャスト メディア インターフェイスに対する BFD サポート

Cisco IOS XE Denali 16.3.1 では、BFD 機能は、ルーティングされた SVI と L3 ポート チャネルでサポートされます。

bfd interval コマンドは、BFD モニタリングを開始するインターフェイスで設定する必要があります。

ステートフル スイッチオーバーでのノンストップ フォワーディングの BFD サポート

通常、ネットワーキング デバイスを再起動すると、そのデバイスのすべてのルーティング ピアがデバイスの終了および再起動を検出します。この遷移によってルーティング フラップが発生し、そのために複数のルーティング ドメインに分散される可能性があります。ルーティングの再起動によって発生したルーティング フラップによって、ルーティングが不安定になります。これはネットワーク全体のパフォーマンスに悪影響を及ぼします。ノンストップ フォワーディング（NSF）は、ステートフル スイッチオーバー（SSO）がイネーブルになっているデバイスのルーティング フラップを抑制するのに役立ち、それによってネットワークの不安定さが減少します。

NSF では、ルーティング プロトコル情報がスイッチオーバー後に保存されるとき、既知のルータでデータ パケットのフォワーディングを継続できます。NSF を使用すると、ピア ネットワーキング デバイスでルーティング フラップが発生しません。データ トラフィックはインテリジェント ラインカードまたはデュアル フォワーディング プロセッサを介して転送されますが、スタンバイ RP では、スイッチオーバー中に障害が発生したアクティブな RP からの制御と見なされます。ラインカードおよびフォワーディング プロセッサの機能はスイッチオーバーによって維持され、アクティブな RP の転送情報ベース（FIB）が NSF 動作で最新状態が維持されます。

デュアル RP をサポートするデバイスでは、SSO が RP の 1 つをアクティブなプロセッサとして確立し、他の RP はスタンバイ プロセッサに割り当てられ、それらの間で情報が同期されます。アクティブな RP に障害が発生したとき、ネットワーキング デバイスから削除されたとき、または手動でメンテナンスから排除されたときに、アクティブなプロセッサとスタンバイ プロセッサからのスイッチオーバーが発生します。

ステートフル スイッチオーバーの BFD サポート

BFD プロトコルでは、隣接するフォワーディング エンジン間でパスに短期間の障害検出が行われます。デュアル RP ルータまたはスイッチ（冗長性のため）を使用するネットワーク導入では、ルータにグレースフル リスタート メカニズムがあり、アクティブな RP とスタンバイ RP の間のスイッチオーバー時にフォワーディング状態が保護されます。

ハードウェアの通信障害を検出する機能に応じて、デュアル RP のスイッチオーバー回数が異なります。BFD が RP で稼働している場合、一部のプラットフォームでは BFD プロトコルがタイムアウトになる前にスイッチオーバーを検出することはできません。このようなプラットフォームは低速スイッチオーバー プラットフォームと呼ばれます。

スタティック ルーティングの BFD サポート

OSPF や BGP などの動的なルーティング プロトコルとは異なり、スタティック ルーティングにはピア検出の方法がありません。したがって、BFD が設定されると、ゲートウェイの到達可能性は完全に指定されたネイバーへの BFD セッションの状態に依存します。BFD セッションが開始されない限り、スタティック ルートのゲートウェイは到達不能と見なされ、したがって、影響を受けるルートが適切なルーティング情報ベース（RIB）にインストールされません。

BFD セッションが正常に確立されるように、ピア上のインターフェイスで BFD を設定し、ピア上の BFD クライアントに BFD ネイバーのアドレスを登録する必要があります。インターフェイスがダイナミック ルーティング プロトコルで使用される場合、後者の要件は通常、BFD の各ネイバーでルーティング プロトコル インスタンスを設定することによって満たされます。インターフェイスがスタティック ルーティングに排他的に使用される場合、この要件はピア上でスタティック ルートを設定することによって満たす必要があります。

BFD セッションが起動状態のときに BFD 設定がリモート ピアから削除された場合、BFD セッションの最新状態が IPv4 スタティックに送信されません。その結果、スタティック ルートが RIB に残ります。唯一の回避策は、IPv4 スタティック BFD ネイバー設定を削除して、スタティック ルートが BFD セッション状態を追跡しないようにすることです。また、シリアル インターフェイスのカプセル化のタイプを BFD でサポートされていないタイプに変更する場合、このインターフェイスで BFD がダウン状態になります。回避策はインターフェイスをシャットダウンし、サポートされているカプセル化のタイプに変更してから、BFD を再設定することです。

IPv4 スタティック クライアントでは 1 つの BFD セッションを使用して、特定のインターフェイスを通るネクスト ホップの到達可能性を追跡できます。一連の BFD 追跡対象スタティック ルートに対して BFD グループを割り当てることができます。各グループには 1 つのアクティブ スタティック BFD 設定、1 つ以上のパッシブ BFD 構成、および対応する BFD 追跡対象スタティック ルートが必要です。nongroup エントリは、BFD グループが割り当てられていない BFD 追跡対象スタティック ルートです。BFD グループは、さまざまな VRF の一部として構成

可能なスタティック BFD 設定に対応する必要があります。実際には、パッシブ スタティック BFD 設定は、アクティブな設定と同じ VRF に構成する必要はありません。

BFD グループごとに存在するアクティブなスタティック BFD セッションは 1 つだけです。スタティック BFD 設定とその BFD 設定を使用する対応のスタティック ルートを追加して、アクティブ BFD セッションを設定できます。アクティブなスタティック BFD 構成とそのスタティック BFD 設定を使用するスタティック ルートがある場合にのみ、グループの BFD セッションが作成されます。アクティブなスタティック BFD 設定またはアクティブなスタティック ルートが BFD グループから削除されると、パッシブなスタティック ルートがすべて RIB から削除されます。実際には、すべてのパッシブなスタティック ルートは、アクティブなスタティック BFD 設定と、アクティブな BFD セッションで追跡されるスタティック ルートがグループで設定されるまでは非アクティブです。

同様に、BFD グループごとに 1 つ以上のパッシブなスタティック BFD 設定と、対応する BFD 追跡対象スタティック ルートが存在します。パッシブなスタティック セッション ルートは、アクティブな BFD セッション状態が到達可能であるときだけ有効です。グループのアクティブな BFD セッション状態が到達可能であっても、対応するインターフェイスの状態がアップである場合にのみ、パッシブなスタティック ルートが RIB に追加されます。パッシブな BFD セッションがグループから削除されると、アクティブな BFD セッション（存在する場合）や BFD グループの到達可能性ステータスには影響しません。

障害検出に BFD を使用することの利点

機能を導入するときは、あらゆる代替策を検討し、トレードオフに注意することが重要です。

EIGRP、IS-IS、および OSPF の通常の導入で BFD に最も近い代替策は、EIGRP、IS-IS、および OSPF ルーティング プロトコルの変更された障害検出メカニズムを使用することです。

EIGRP の hello およびホールド タイマーを絶対最小値に設定する場合、EIGRP の障害検出速度が 1〜2 秒程度に下がります。

IS-IS または OSPF に fast hello を使用する場合、これらの Interior Gateway Protocol（IGP）プロトコルによって障害検出メカニズムが最小 1 秒に減少します。

ルーティング プロトコルの減少したタイマー メカニズムで BFD を実装すると、いくつかの利点があります。

- EIGRP、IS-IS、および OSPF タイマーによって 1 秒または 2 秒の最小検出タイマーを実現できますが、障害検出が 1 秒未満になる場合もあります。
- BFD は特定のルーティング プロトコルに関連付けられていないため、EIGRP、IS-IS、および OSPF の汎用の整合性のある障害検出メカニズムとして使用できます。
- BFD の一部をデータ プレーンに分散できるため、コントロール プレーンに全体が存在する分散 EIGRP、IS-IS、および OSPF タイマーよりも CPU の負荷を軽くすることができます。

双方向フォワーディング検出の設定方法

インターフェイスでの BFD セッション パラメータの設定

インターフェイスで BFD を設定するには、インターフェイスで BFD セッションの基本パラメータを設定する必要があります。BFD ネイバーに対して BFD セッションを実行するインターフェイスごとに、この手順を繰り返します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかの手順を実行します。
	• **ipaddress** *ipv4-address mask*
	• **ipv6address** *ipv6-address/mask*
	例：
	インターフェイスの IPv4 アドレスの設定：
	`Device(config-if)# ip address 10.201.201.1 255.255.255.0`
	インターフェイスの IPv6 アドレスの設定：
	`Device(config-if)# ipv6 address 2001:db8:1:1::1/32`
		インターフェイスに IP アドレスを設定します。

ステップ 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* 例： `Device(config-if)# bfd interval 100 min_rx 100 multiplier 3`	インターフェイスで BFD をイネーブルにします。 BFD interval 設定は、それを設定したサブインターフェイスが削除されたときに削除されます。 BFD interval 設定は次のような場合には削除されません。

	コマンドまたはアクション	目的
		• IPv4 アドレスがインターフェイスから削除された場合 • IPv6 アドレスがインターフェイスから削除された場合 • IPv6 がインターフェイスからディセーブルにされた場合 • インターフェイスがシャットダウンされた場合 • インターフェイスで IPv4 CEF がグローバルまたはローカルでディセーブルにされた場合 • インターフェイスで IPv6 CEF がグローバルまたはローカルでディセーブルにされた場合
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ダイナミック ルーティング プロトコルに対する BFD サポートの設定

eBGP に対する BFD サポートの設定

ここでは、BGP が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、BGP に対する BFD サポートを設定する手順について説明します。

始める前に

e BGP は、関連するすべてのルータで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」の項を参照してください。

（注） **showbfdneighborsdetails** コマンドの出力には、設定された間隔が表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**routerbgp** *as-tag* 例： `Device(config)# router bgp tag1`	BGP プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **fall-overbfd** 例： `Device(config-router)# neighbor 172.16.10.2 fall-over bfd`	フェールオーバーに対する BFD サポートをイネーブルにします。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**showbfdneighbors**[**details**] 例： `Device# show bfd neighbors detail`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されることを確認します。
ステップ 7	**showipbgpneighbor** 例： `Device# show ip bgp neighbor`	（任意）ネイバーへの BGP および TCP 接続についての情報を表示します。

EIGRP に対する BFD サポートの設定

ここでは、EIGRP が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、EIGRP に対する BFD サポートを設定する手順について説明します。EIGRP に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して、EIGRP がルーティングしているすべてのインターフェイスに対して BFD をイネーブルにできます。

- ルータ設定モードで **bfdinterface** *type number* コマンドを使用して、EIGRP がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

始める前に

EIGRP は、関連するすべてのルータで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでのBFDセッション パラメータの設定」の項を参照してください。

（注） **showbfdneighborsdetails** コマンドの出力には、設定された間隔が表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router eigrp** *as-number* 例： `Device(config)# router eigrp 123`	EIGRP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **bfdall-interfaces**
	• **bfdinterface** *type number*
	例：
	`Device(config-router)# bfd all-interfaces`
	例：
	`Device(config-router)# bfd interface GigabitFastEthernet 1/0/1`
		EIGRP ルーティング プロセスに関連付けられたすべてのインターフェイスで、BFD をグローバルにイネーブルにします。
		または
		EIGRP ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-router) end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**showbfdneighbors**[**details**] 例： `Device# show bfd neighbors details`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されることを確認します。
ステップ 7	**showipeigrpinterfaces** [*type number*] [*as-number*] [**detail**] 例： `Device# show ip eigrp interfaces detail`	（任意）EIGRP に対する BFD サポートがイネーブルになっているインターフェイスを表示します。

IS-IS に対する BFD サポートの設定

ここでは、IS-IS が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、IS-IS に対する BFD サポートを設定する手順について説明します。IS-IS に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfd all-interfaces** コマンドを使用して、IS-IS が IPv4 ルーティングをサポートしているすべてのインターフェイスに対して BFD をイネーブルにできます。次にインターフェイス コンフィギュレーション モードで **isisbfddisable** コマンドを使用すると、1 つ以上のインターフェイスに対して BFD をディセーブルにできます。
- インターフェイス コンフィギュレーション モードで **isisbfd** コマンドを使用すると、IS-IS がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

IS-IS に対する BFD サポートを設定するには、次のいずれかの手順に従います。

前提条件

IS-IS は、関連するすべてのルータで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」の項を参照してください。

（注） **showbfdneighborsdetails** コマンドの出力には、設定された間隔が表示されます。ハードウェアオフロードされた BFD セッションが 50 ms の倍数でない Tx および Rx 間隔で設定されていたために変更された間隔は出力に表示されません。

すべてのインターフェイスの *IS-IS* に対する *BFD* サポートの設定

IPv4 ルーティングをサポートするすべての IS-IS インターフェイスで BFD を設定するには、この項の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**routerisis** *area-tag* 例： `Device(config)# router isis tag1`	IS-IS プロセスを指定し、ルータ コンフィギュレーションモードを開始します。
ステップ 4	**bfdall-interfaces** 例： `Device(config-router)# bfd all-interfaces`	IS-IS ルーティング プロセスに関連付けられたすべてのインターフェイスで、BFD をグローバルにイネーブルにします。
ステップ 5	**exit** 例： `Device(config-router)# exit`	（任意）ルータでグローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *type number* 例： `Device(config)# interface fastethernet 6/0`	（任意）インターフェイス コンフィギュレーションモードを開始します。
ステップ 7	**iprouterisis** [*tag*] 例： `Device(config-if)# ip router isis tag1`	（任意）インターフェイスで IPv4 ルーティングのサポートをイネーブルにします。
ステップ 8	**isisbfd**[**disable**] 例：	（任意）IS-IS ルーティング プロセスに関連付けられた 1 つ以上のインター

	コマンドまたはアクション	目的
	`Device(config-if)# isis bfd`	フェイスに対して、インターフェイスごとに BFD をイネーブルまたはディセーブルにします。 （注） コンフィギュレーションモードで **bfdall-interfaces** コマンドを使用して IS-IS が関連付けられたすべてのインターフェイスで以前に BFD をイネーブルにしていた場合にのみ、**disable** キーワードを使用する必要があります。
ステップ 9	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 10	**showbfdneighbors**[**details**] 例： `Device# show bfd neighbors details`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されるかどうかの検証に使用できる情報を表示します。
ステップ 11	**showclnsinterface** 例： `Device# show clns interface`	（任意）IS-IS に対する BFD が、関連付けられた特定の IS-IS インターフェイスに対してイネーブルになっているかどうかを検証するために使用できる情報を表示します。

1 つ以上のインターフェイスの *IS-IS* に対する *BFD* サポートの設定

1 つ以上の IS-IS インターフェイスだけに BFD を設定するには、この項の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**interface** *type number* 例： `Device(config)# interface fastethernet 6/0`	インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	**iprouterisis** [*tag*] 例： `Device(config-if)# ip router isis tag1`	インターフェイスで IPv4 ルーティングのサポートをイネーブルにします。
ステップ 5	**isisbfd[disable]** 例： `Device(config-if)# isis bfd`	IS-IS ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルまたはディセーブルにします。 （注） ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して IS-IS が関連付けられたすべてのインターフェイスで BFD をイネーブルにした場合にだけ、**disable** キーワードを使用する必要があります。
ステップ 6	**end** 例： `Device(config-if)# end`	インターフェイスコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**showbfdneighbors**[**details**] 例： `Device# show bfd neighbors details`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されるかどうかの検証に使用できる情報を表示します。
ステップ 8	**showclnsinterface** 例： `Device# show clns interface`	（任意）IS-IS に対する BFD が、関連付けられた特定の IS-IS インターフェイスに対してイネーブルになっているかどうかを検証するために使用できる情報を表示します。

OSPF に対する BFD サポートの設定

ここでは、OSPF が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、OSPF に対する BFD サポートを設定する手順について説明します。すべてのインターフェイスでグローバルに OSPF に対する BFD を設定するか、または 1 つ以上のインターフェイスで選択的に設定することができます。

OSPF に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して、OSPF がルーティングしているすべてのインターフェイスに対して BFD をイネーブルにできます。インターフェイス コンフィギュレーション モードで **ipospfbfd** [**disable**] コマンドを使用して、個々のインターフェイスで BFD をディセーブルにできます。
- インターフェイス コンフィギュレーション モードで **ipospfbfd** コマンドを使用して、OSPF がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

OSPF に対する BFD サポートのタスクについては、次の項を参照してください。

すべてのインターフェイスの *OSPF* に対する *BFD* サポートの設定

すべての OSPF インターフェイスに BFD を設定するには、この項の手順に従います。

すべての OSPF インターフェイスに対して BFD を設定するのではなく、特定の 1 つ以上のインターフェイスに対して BFD サポートを設定する場合は、「1 つ以上のインターフェイスの OSPF に対する BFD サポートの設定」の項を参照してください。

始める前に

OSPF は、関連するすべてのルータで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」の項を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**routerospf** *process-id* 例： `Device(config)# router ospf 4`	OSPF プロセスを指定し、ルータ コンフィギュレーションモードを開始します。
ステップ 4	**bfdall-interfaces** 例： `Device(config-router)# bfd all-interfaces`	OSPF ルーティング プロセスに関連付けられたすべてのインターフェイスで、BFD をグローバルにイネーブルにします。
ステップ 5	**exit** 例： `Device(config-router)# exit`	（任意）デバイスでグローバル コンフィギュレーション モードに戻ります。ステップ 7 を実行して 1 つ以上のインターフェイスに対して BFD をディセーブルにする場合にだけ、このコマンドを入力します。
ステップ 6	**interface** *type number* 例： `Device(config)# interface fastethernet 6/0`	（任意）インターフェイス コンフィギュレーションモードを開始します。ステップ 7 を実行して 1 つ以上のインターフェイスに対して BFD をディセーブルにする場合にだけ、このコマンドを入力します。
ステップ 7	**ipospfbfd**[**disable**] 例： `Device(config-if)# ip ospf bfd disable`	（任意）OSPF ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をディセーブルにします。 （注） ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して OSPF が関連付けられたすべてのインターフェイスで BFD をイネーブルにした場合にだけ、**disable** キーワードを使用する必要があります。
ステップ 8	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**showbfdneighbors**[**details**] 例： `Device# show bfd neighbors detail`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されるかどうかの検証に使用できる情報を表示します。
ステップ 10	**showipospf** 例： `Device# show ip ospf`	（任意）OSPF に対して BFD がイネーブルになっているかどうかを検証するために使用できる情報を表示します。

1 つ以上のインターフェイスの *OSPF* に対する *BFD* サポートの設定

1 つ以上の OSPF インターフェイスで BFD を設定するには、この項の手順に従います。

始める前に

OSPF は、関連するすべてのルータで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでのBFDセッション パラメータの設定」の項を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface fastethernet 6/0`	インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	**ipospfbfd**[**disable**] 例： `Device(config-if)# ip ospf bfd`	OSPF ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD を

	コマンドまたはアクション	目的
		イネーブルまたはディセーブルにします。 （注） ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して OSPF が関連付けられたすべてのインターフェイスで BFD をイネーブルにした場合にだけ、**disable** キーワードを使用する必要があります。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**showbfdneighbors**[**details**] 例： `Device# show bfd neighbors details`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されるかどうかの検証に使用できる情報を表示します。
ステップ 7	**showipospf** 例： `Device# show ip ospf`	（任意）OSPF に対して BFD サポートがイネーブルになっているかどうかを検証するために使用できる情報を表示します。

HSRP に対する BFD サポートの設定

ホットスタンバイ ルータ プロトコル（HSRP）の BFD サポートをイネーブルにするには、次の作業を実行します。この手順のステップは、HSRP ピアに BFD セッションを実行する各インターフェイスで行ってください。

デフォルトでは、HSRP は BFD をサポートします。BFD に対する HSRP サポートが手動でディセーブルになっている場合、ルータ レベルで再びイネーブルにして、すべてのインターフェイスに対してグローバルに BFD サポートをイネーブルにするか、またはインターフェイス レベルでインターフェイスごとにイネーブルにすることができます。

始める前に

- HSRP は、関連するすべてのルータで実行する必要があります。
- シスコ エクスプレス フォワーディングをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipcef**[**distributed**] 例： `Device(config)# ip cef`	シスコエクスプレスフォワーディングまたは分散型シスコエクスプレスフォワーディングをイネーブルにします。
ステップ 4	**interface** *type number* 例： `Device(config)# interface FastEthernet 6/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ipaddress** *ip-address mask* 例： `Device(config-if)# ip address 10.1.0.22 255.255.0.0`	インターフェイスにIPアドレスを設定します。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# standby 1 ip 10.0.0.11`	HSRP をアクティブにします。
ステップ 7	**standbybfd** 例： `Device(config-if)# standby bfd`	（任意）インターフェイスでBFDに対する HSRP をイネーブルにします。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 9	**standbybfdall-interfaces** 例： `Device(config)# standby bfd all-interfaces`	（任意）すべてのインターフェイスで BFD に対する HSRP をイネーブルにします。
ステップ 10	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**showstandby neighbors** 例： `Device# show standby neighbors`	（任意）BFD に対する HSRP サポートについての情報を表示します。

スタティック ルーティングに対する BFD サポートの設定

スタティック ルーティングのための BFD サポートを設定するには、このタスクを実行します。各 BFD ネイバーに対してこの手順を繰り返します。詳細については、「例：スタティック ルーティングに対する BFD サポートの設定」の項を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface serial 2/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	次のいずれかの手順を実行します。 • **ipaddress** *ipv4-address mask* • **ipv6address** *ipv6-address/mask*	インターフェイスに IP アドレスを設定します。

	コマンドまたはアクション	目的

	例：
	インターフェイスの IPv4 アドレスの設定：
	`Device(config-if)# ip address 10.201.201.1 255.255.255.0`
	インターフェイスの IPv6 アドレスの設定：
	`Device(config-if)# ipv6 address 2001:db8:1:1::1/32`	

ステップ 5	**bfd interval** *milliseconds* **mix_rx** *milliseconds* **multiplier** *interval-multiplier* 例： `Device(config-if)# bfd interval 500 min_rx 500 multiplier 5`	インターフェイスで BFD をイネーブルにします。 bfd interval 設定は、それを設定したサブインターフェイスが削除されたときに削除されます。 bfd interval 設定は次のような場合には削除されません。 • IPv4 アドレスがインターフェイスから削除された場合 • IPv6 アドレスがインターフェイスから削除された場合 • IPv6 がインターフェイスからディセーブルにされた場合 • インターフェイスがシャットダウンされた場合 • インターフェイスで IPv4 CEF がグローバルまたはローカルでディセーブルにされた場合 • インターフェイスで IPv6 CEF がグローバルまたはローカルでディセーブルにされた場合
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**ip route static bfd** *interface-type interface-number ip-address* [**group** *group-name* [**passive**]] 例： `Device(config)# ip route static bfd TenGigabitEthernet1/0/1 10.10.10.2 group group1 passive`	スタティック ルートの BFD ネイバーを指定します。 • BFD が直接接続されたネイバーだけでサポートされているため、*interface-type*、*interface-number*、および *ip-address* 引数は必須です。
ステップ 8	**ip route** [**vrf** *vrf-name*] *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*] 例： `Device(config)# ip route 10.0.0.0 255.0.0.0`	スタティック ルートの BFD ネイバーを指定します。
ステップ 9	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**show ip static route** 例： `Device# show ip static route`	（任意）スタティック ルート データベース情報を表示します。
ステップ 11	**show ip static route bfd** 例： `Device# show ip static route bfd`	（任意）設定された BFD グループおよび nongroup エントリからスタティック BFD の設定に関する情報を表示します。
ステップ 12	**exit** 例： `Device# exit`	特権 EXEC モードを終了し、ユーザ EXEC モードに戻ります。

BFD エコー モードの設定

デフォルトでは BFD エコー モードがイネーブルになっていますが、方向ごとに個別に実行できるように、ディセーブルにすることもできます。

BFD エコー モードは非同期 BFD で動作します。エコー パケットはフォワーディング エンジンによって送信され、検出を実行するために、同じパスで転送されます。反対側の BFD セッションはエコー パケットの実際のフォワーディングに関与しません。エコー機能およびフォ

ワーディング エンジンが検出プロセスを処理するため、2 つの BFD ネイバー間で送信される BFD 制御パケットの数が減少します。また、フォワーディング エンジンが、リモート システムを介さずにリモート（ネイバー）システムの転送パスをテストするため、パケット内遅延が向上する可能性があり、それによって BFD バージョン 0 を BFD セッションの BFD 制御パケットで使用する場合に、障害検出時間を短縮できます。

エコー モードを両端で実行している（両方の BFD ネイバーがエコー モードを実行している）場合は、非対称性がないと表現されます。

前提条件

BFD は、関連するすべてのルータで実行する必要があります。

CPU 使用率の上昇を避けるために、BFD エコー モードを使用する前に、**noipredirects** コマンドを入力して、インターネット制御メッセージプロトコル（ICMP）リダイレクト メッセージの送信をディセーブルにする必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」の項を参照してください。

機能制限

BFD エコー モードは、ユニキャスト リバース パス転送（uRPF）の設定との組み合わせでは動作しません。BFD エコー モードと uRPF の設定がイネーブルの場合、セッションはフラップします。

非対称性のない BFD エコー モードのディセーブル化

この手順では、非対称性のない BFD エコー モードをディセーブルにする方法を示します。ルータからはエコー パケットが送信されず、ルータはネイバー ルータから受信する BFD エコー パケットを転送しません。

各 BFD ルータに対してこの手順を繰り返します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**no bfdecho** 例： `Router(config)# no bfd echo`	BFD エコー モードをディセーブルにします。 • **no** 形式を使用すると、BFD エコー モードをディセーブルにできます。
ステップ 4	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

BFD テンプレートの作成と設定

シングルホップ テンプレートは一連の BFD 間隔値を指定するために設定できます。BFD テンプレートの一部として指定される BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。

（注） bfd-template を設定すると、エコー モードが無効になります。

シングルホップ テンプレートの設定

BFD シングルホップ テンプレートを作成し、BFD インターバル タイマーを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bfd-templatesingle-hop** *template-name* 例： `Device(config)# bfd-template single-hop bfdtemplate1`	シングルホップ BFD テンプレートを作成し、BFD コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**intervalmin-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value* 例： `Device(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3`	BFD パケット間での送受信間隔を設定し、ピアが使用不能であると BFD が宣言する前に損失される連続的な BFD 制御パケット数を指定します。
ステップ 5	**end** 例： `Device(bfd-config)# end`	BFD コンフィギュレーション モードを終了し、デバイスを特権 EXEC モードに戻します。

BFD のモニタリングとトラブルシューティング

ここでは、維持とトラブルシューティングのために BFD 情報を取得する方法について説明します。必要に応じてこれらのタスクのコマンドを、正しい順序で入力します。

ここでは、次の Cisco プラットフォームに対する BFD のモニタリングとトラブルシューティングについて説明します。

BFD のモニタリングとトラブルシューティング

Catalyst 7600 シリーズ ルータのモニタリングとトラブルシューティングを実行するには、この項の 1 つ以上の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showbfdneighbors**[**details**] 例： `Router# show bfd neighbors details`	（任意）BFD 隣接関係データベースを表示します。 • **details** キーワードを指定すると、すべての BFD プロトコル パラメータとネイバーごとにタイマーが表示されます。
ステップ 3	**debugbfd**[**packet** | **event**] 例： `Router# debug bfd packet`	（任意）BFD パケットのデバッグ情報を表示します。

第 91 章

MSDP の設定

- 機能情報の確認 （1773 ページ）
- MSDP の設定について （1773 ページ）
- MSDP の設定方法 （1776 ページ）
- MSDP のモニタリングおよびメンテナンス （1799 ページ）
- MSDP の設定例 （1800 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

MSDP の設定について

このセクションでは、スイッチに Multicast Source Discovery Protocol（MSDP）を設定する方法について説明します。MSDP によって、複数の Protocol-Independent Multicast Sparse-Mode（PIM-SM）ドメインが接続されます。

このソフトウェア リリースでは、MSDP と連携して動作する Multicast Border Gateway Protocol（MBGP）がサポートされていないため、MSDP は完全にはサポートされていません。ただし、MBGP が動作していない場合、MSDP と連携して動作するデフォルト ピアを作成できます。

（注） この機能を使用するには、アクティブ スイッチ上で IP Services フィーチャー セットが稼働している必要があります。

MSDP の概要

MSDP を使用すると、さまざまなドメイン内のすべてのランデブー ポイント（RP）に、グループのマルチキャスト送信元を通知できます。各 PIM-SM ドメインでは独自の RP が使用され、他のドメインの RP には依存しません。RP は伝送制御プロトコル（TCP）を通じて MSDP を実行し、他のドメイン内のマルチキャスト送信元を検出します。

PIM-SM ドメイン内の RP は、他のドメイン内の MSDP 対応デバイスと MSDP ピアリング関係にあります。ピアリング関係は TCP 接続を通じて発生します。主に、マルチキャスト グループを送信する送信元のリストを交換します。RP 間の TCP 接続は、基本的なルーティング システムによって実現されます。受信側の RP では、送信元リストを使用して送信元のパスが確立されます。

このトポロジの目的は、ドメインから、他のドメイン内のマルチキャスト送信元を検出することです。マルチキャスト送信元がレシーバーのあるドメインを対象としている場合、マルチキャストデータはPIM-SMの通常の送信元ツリー構築メカニズムを通じて配信されます。MSDP は、グループを送信する送信元のアナウンスにも使用されます。これらのアナウンスは、ドメインの RP で発信する必要があります。

MSDP のドメイン間動作は、Border Gateway Protocol（BGP）または MBGP に大きく依存します。ドメイン内の RP（インターネットへのアナウンス対象であるグローバル グループを送信する送信元用の RP）で、MSDP を実行してください。

MSDP の動作

送信元が最初のマルチキャスト パケットを送信すると、送信元に直接接続された先頭ホップ ルータ（指定ルータまたは RP）によって RP に PIM 登録メッセージが送信されます。RP は登録メッセージを使用し、アクティブな送信元を登録したり、ローカル ドメイン内の共有ツリーの下方向にマルチキャスト パケットを転送します。MSDP が設定されている場合は、Source-Active（SA）メッセージも、すべての MSDP ピアに転送します。送信元、送信元からの送信先であるグループ、および RP のアドレスまたは発信元 ID（RP アドレスとして使用されるインターフェイスの IP アドレス）が設定されている場合は、SA メッセージによってこれらが識別されます。

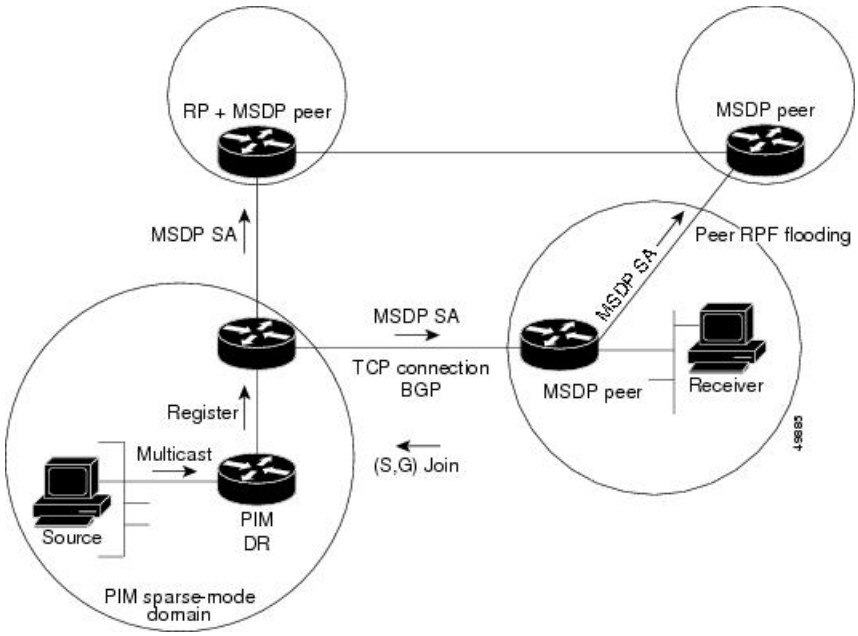
各 MSDP ピアは SA メッセージを発信元の RP から受信して転送し、ピア Reverse-Path Forwarding（RPF）フラッディングを実現します。MSDP デバイスは、BGP または MBGP ルーティング テーブルを調べ、どのピアが SA メッセージの発信元 RP へのネクスト ホップであるかを検出します。このようなピアは *RPF* ピアと呼ばれます。MSDP デバイスでは、RPF ピア以外のすべての MSDP ピアにメッセージが転送されます。BGP および MBGP がサポートされていない場合に MSDP を設定する方法については、デフォルトの MSDP ピアの設定（1776 ページ）を参照してください。

MSDP ピアは、非 RPF ピアから発信元 RP へ向かう同じ SA メッセージを受信すると、そのメッセージをドロップします。それ以外の場合、すべての MSDP ピアにメッセージが転送されます。

ドメインの RP ピアは MSDP ピアから SA メッセージを受信します。この RP が SA メッセージに記述されているグループへの加入要求を持ち、空でない発信インターフェイス リストに（*,G）エントリが含まれている場合、そのグループはドメインの対象となり、RP から送信元方向に（S,G）Join メッセージが送信されます。（S,G）Join メッセージが送信元の DR に到達してからは、送信元からリモート ドメイン内の RP への送信元ツリーのブランチが構築されています。この結果、マルチキャスト トラフィックを送信元から送信元ツリーを経由して RP へ、そしてリモート ドメイン内の共有ツリーを下ってレシーバへと送信できます。

図 *95 : RP* ピア間で動作する *MSDP*

この図に、2 つの MSDP ピアの間での MSDP の動作を示します。PIM では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP が使用されます。MSDP が設定されている場合は、次のシーケンスが発生します。



デフォルトでは、スイッチで受信された SA メッセージ内の送信元やグループのペアは、キャッシュに格納されません。また、MSDP SA 情報が転送される場合、この情報はメモリに格納されません。したがって、ローカル RP で SA メッセージが受信された直後にメンバーがグループに加入した場合、そのメンバーは、その次の SA メッセージによって送信元に関する情報が取得されるまで、待機する必要があります。この遅延は加入遅延と呼ばれます。

ローカル RP では、SA 要求を送信し、指定されたグループに対するすべてのアクティブな送信元の要求をすぐに取得できます。デフォルトでは、新しいメンバーがグループに加入してマルチキャスト トラフィックを受信する必要が生じた場合、スイッチは MSDP ピアに SA 要求メッセージを送信しません。新しいメンバーは次の定期的な SA メッセージを受信する必要があります。

グループへの送信元である接続 PIM SM ドメイン内のアクティブなマルチキャスト送信元を、グループの新しいメンバーが学習する必要がある場合は、新しいメンバーがグループに加入したときに、指定された MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定します。

MSDP の利点

MSDP には次の利点があります。

- 共有されたマルチキャスト配信ツリーが分割され、共有ツリーがドメインに対してローカルになるように設定できます。ローカル メンバーはローカル ツリーに加入します。共有ツリーへの Join メッセージはドメインから脱退する必要はありません。
- PIM SM ドメインは独自の RP だけを信頼するため、他のドメインの RP に対する信頼度が低下します。このため、送信元の情報がドメイン外部に漏れないようにでき、セキュリティが高まります。
- レシーバーだけが配置されているドメインは、グループ メンバーシップをグローバルにアドバタイズしなくても、データを受信できます。
- グローバルな送信元マルチキャスト ルーティング テーブル ステートが不要になり、メモリが削減されます。

MSDP の設定方法

MSDP のデフォルト設定

MSDP はイネーブルになっていません。デフォルトの MSDP ピアはありません。

デフォルトの MSDP ピアの設定

始める前に

MSDP ピアを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp default-peer** *ip-address* | *name* [**prefix-list** *list*] 例： `Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a`	すべての MSDP SA メッセージの受信元となるデフォルト ピアを定義します。 • *ip-address* | *name* には、MSDP デフォルト ピアの IP アドレスまたはドメイン ネーム システム（DNS）サーバ名を入力します。 • （任意）**prefix-list** *list* を指定する場合は、リスト内のプレフィックス専用のデフォルト ピアとなるピアを指定するリスト名を入力します。プレフィックス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。 **prefix-list** キーワードが指定された **ip msdp default-peer** コマンドを複数入力すると、複数の RP プレフィックスに対してすべてのデフォルト ピアが同時に使用されます。この構文は通常、スタブ サイト クラウドに接続されたサービス プロバイダークラウドで使用されます。 **prefix-list** キーワードを指定せずに **ip msdp default-peer** コマンドを複数入力すると、単一のアクティブ ピアですべての SA メッセージが受信されます。このピアに障害がある場合は、次の設定済みデフォルト ピアですべての SA メッセージが受信されます。この構文は通常、スタブ サイトで使用されます。
ステップ 4	**ip prefix-list** *name* [**description** *string*] | **seq** *number* {**permit** | **deny**} *network length* 例：	（任意）ステップ 2 で指定された名前を使用し、プレフィックス リストを作成します。

	コマンドまたはアクション	目的
	`Router(config)# prefix-list site-a seq 3 permit 12 network length 128`	• （任意）**description** *string* には、このプレフィックス リストを説明する 80 文字以下のテキストを入力します。 • **seq** *number* には、エントリのシーケンス番号を入力します。指定できる範囲は 1 ～ 4294967294 です。 • **deny** キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。 • **permit** キーワードを指定すると、条件が一致した場合にアクセスが許可されます。 • *network length* には、許可または拒否されているネットワークの番号およびネットワーク マスク長（ビット単位）を指定します。
ステップ 5	**ip msdp description** {*peer-name* | *peer-address*} *text* 例： `Router(config)# ip msdp description peer-name site-b`	（任意）設定内で、または **show** コマンド出力内で簡単に識別できるように、指定されたピアの説明を設定します。 デフォルトでは、MSDP ピアに説明は関連付けられていません。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SA ステートのキャッシング

メモリを消費して送信元情報の遅延を短縮する場合は、SA メッセージをキャッシュに格納するようにデバイスを設定できます。送信元とグループのペアのキャッシングをイネーブルにするには、次の手順を実行します。

送信元とグループのペアのキャッシングをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp cache-sa-state** [**list** *access-list-number*] 例： `Device(config)# ip msdp cache-sa-state 100`	送信元とグループのペアのキャッシングをイネーブルにします（SA ステートを作成します）。アクセス リストを通過したこれらのペアがキャッシュに格納されます。 **list** *access-list-number* の範囲は 100 ～ 199 です。 （注） このコマンドの代わりに、**ip msdp sa-reques** グローバル コンフィギュレーション コマンドを使用できます。この代替コマンドを使用すると、グループの新しいメンバがアクティブになった場合に、SA 要求メッセージがデバイスから MSDP ピアに送信されます。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* 例：	IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。

	コマンドまたはアクション	目的
	`Device(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255`	• *access-list-number* の範囲は 100 ～ 199 です。ステップ 2 で作成した番号と同じ値を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には1を設定します。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には1を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MSDP ピアからの送信元情報の要求

グループへの送信元である接続 PIM SM ドメイン内のアクティブなマルチキャスト送信元を、グループの新しいメンバが学習する必要がある場合は、新しいメンバがグループに加入したときに、指定された MSDP ピアに SA 要求メッセージがデバイスから送信されるようにこのタスクを実行します。ピアは SA キャッシュ内の情報に応答します。ピアにキャッシュが設定されていない場合、このコマンドを実行しても何も起こりません。この機能を設定すると加入遅延は短縮されますが、メモリが消費されます。

新しいメンバがグループに加入し、マルチキャスト トラフィックを受信する必要が生じた場合、MSDP ピアに SA 要求メッセージを送信するようにデバイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp sa-request** {*ip-address* | *name*} 例： `Device(config)# ip msdp sa-request 171.69.1.1`	指定された MSDP ピアに SA 要求メッセージを送信するようにデバイスを設定します。 *ip-address* | *name* を指定する場合は、グループの新しいメンバがアクティブになるときにローカル デバイスの SA メッセージの要求元になる MSDP ピアの IP アドレス、または名前を入力します。

	コマンドまたはアクション	目的
		SA メッセージを送信する必要がある MSDP ピアごとに、このコマンドを繰り返します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチから発信される送信元情報の制御

デバイスから発信されるマルチキャスト送信元情報を制御できます。

- アドバタイズ対象の送信元（送信元ベース）
- 送信元情報のレシーバー（要求元認識ベース）

詳細については、送信元の再配信 （1782 ページ）およびSA 要求メッセージのフィルタリング（1785 ページ）を参照してください。

送信元の再配信

SA メッセージは、送信元が登録されている RP で発信されます。デフォルトでは、RP に登録されているすべての送信元がアドバタイズされます。送信元が登録されている場合は、RP に *A* フラグが設定されています。このフラグは、フィルタリングされる場合を除き、送信元が SA に格納されてアドバタイズされることを意味します。

アドバタイズされる登録済みの送信元をさらに制限するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp redistribute** [**list** *access-list-name*] [**asn** *aspath-access-list-number*] [**route-map** *map*] 例： `Device(config)# ip msdp redistribute list 21`	SA メッセージに格納されてアドバタイズされる、マルチキャスト ルーティング テーブル内の（S,G）エントリを設定します。 デフォルトでは、ローカル ドメイン内の送信元だけがアドバタイズされます。 • （任意）**list** *access-list-name*：IP 標準または IP 拡張アクセス リストの名前または番号を入力します。標準アクセス リストの範囲は 1 ～ 99、拡張アクセス リストの範囲は 100 ～ 199 です。アクセス リストによって、アドバタイズされるローカルな送信元、および送信されるグループが制御されます。 • （任意）**asn** *aspath-access-list-number*：1 ～ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、**ip as-path access-list** コマンドでも設定する必要があります。 • （任意）**route-map** *map*：1 ～ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、**ip as-path access-list** コマンドでも設定する必要があります。

	コマンドまたはアクション	目的
		アクセス リストまたは自律システム パス アクセス リストに従って、デバイスが（S, G）ペアをアドバタイズします。

ステップ 4	次のいずれかを使用します。
	• `access-list` *access-list-number* `{deny|permit}` *source* [*source-wildcard*]
	• `access-list` *access-list-number* `{deny|permit}` *protocol source source-wildcard destination destination-wildcard*
	例：
	`Device(config)# access list 21 permit 194.1.22.0`
	または
	`Device(config)# access list 21 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1`
		IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。
		または
		IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。
		• *access-list-number*：ステップ 2 で作成した同じ番号を入力します。標準アクセス リストの範囲は 1 ～ 99、拡張アクセス リストの範囲は 100 ～ 199 です。
		• **deny**：条件に合致している場合、アクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。
		• *protocol*：プロトコル名として **ip** を入力します。
		• *source*：パケットの送信元であるネットワークまたはホストの番号を入力します。
		• *source-wildcard*：送信元に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。
		• *destination*：パケットの宛先であるネットワークまたはホストの番号を入力します。
		• *destination-wildcard*：宛先に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には1を設定します。

	コマンドまたはアクション	目的
		アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SA 要求メッセージのフィルタリング

デフォルトでは、SA情報をキャッシングしているデバイスだけが、SA要求に応答できます。このようなデバイスでは、デフォルトで MSDP ピアからのすべての SA 要求メッセージが採用され、アクティブな送信元の IP アドレスが取得されます。

ただし、MSDP ピアからの SA 要求をすべて無視するように、デバイスを設定できます。標準アクセス リストに記述されたグループのピアからの SA 要求メッセージだけを採用することもできます。アクセス リスト内のグループが指定された場合は、そのグループのピアからの SA 要求メッセージが受信されます。他のグループのピアからの他のメッセージは、すべて無視されます。

デフォルトの設定に戻すには、**no ip msdp filter-sa-request** {*ip-address*| *name*} グローバル コンフィギュレーション コマンドを使用します。

これらのオプションのいずれかを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • `ip msdp filter-sa-request` {*ip-addressname*} • `ip msdp filter-sa-request` {*ip-addressname*} `list` *access-list-number* 例： `Device(config)# ip msdp filter sa-request 171.69.2.2`	指定された MSDP ピアからの SA 要求メッセージをすべてフィルタリングします。 または 標準アクセス リストを通過したグループに対して、指定された MSDP ピアからの SA 要求メッセージをフィルタリングします。アクセス リストには、複数のグループ アドレスが記述されています。access-list-number の範囲は 1 ～ 99 です。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 1 permit 192.4.22.0 0.0.0.255`	IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。

	コマンドまたはアクション	目的
		アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチで転送される送信元情報の制御

デフォルトでは、デバイスで受信されたすべての SA メッセージが、すべての MSDP ピアに転送されます。ただし、フィルタリングするか、または存続可能時間（TTL）値を設定し、発信メッセージがピアに転送されないようにできます。

フィルタの使用法

フィルタを作成すると、次のいずれかの処理を実行できます。

- すべての送信元とグループのペアのフィルタリング
- 特定の送信元とグループのペアだけが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかを使用します。
	• **ip msdp sa-filter out** {*ip-address name*}
	• **ip msdp sa-filter out** {*ip-address name*} `list` *access-list-number*
	• **ip msdp sa-filter out** {*ip-address name*} `route-map` *map-tag*
	例：
	`Device(config)# ip msdp sa-filter out switch.cisco.com`
	または
	`Device(config)# ip msdp sa-filter out list 100`
	または
	`Device(config)# ip msdp sa-filter out switch.cisco.com route-map 22`
		• 指定された MSDP ピアへの SA メッセージをフィルタリングします。
		• 指定したピアに対する IP 拡張アクセス リストを通過した SA メッセージのみを渡します。拡張アクセスリスト番号の範囲は 100 ～ 199 です。
		list と **route-map** の両方のキーワードを使用すると、すべての条件に一致しなければ、発信 SA メッセージ内のいずれの（S,G）ペアも通過できません。
		• 指定された MSDP ピアへのルート マップ *map-tag* で一致基準を満たす SA メッセージのみを渡します。
		すべての一致条件を満たす場合、ルート マップに **permit** が指定されていれば、ルートはフィルタを通過します。**deny** が指定されていれば、ルートはフィルタリングされます。

ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* 例： `Device(config)# access list 100 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1`	（任意）IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。

	コマンドまたはアクション	目的
		• *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には1を設定します。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には1を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限

TTL 値を使用して、各送信元の最初の SA メッセージにカプセル化されるデータを制御できます。IP ヘッダー TTL 値が *ttl* 引数以上であるマルチキャスト パケットだけが、指定された MSDP ピアに送信されます。たとえば、内部トラフィックの TTL 値を 8 に制限できます。他のグループを外部に送信する場合は、これらのパケットの TTL を 8 より大きく設定して送信する必要があります。

TTL しきい値を確立するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp ttl-threshold** {*ip-address* | *name*} *ttl* 例： `Device(config)# ip msdp ttl-threshold switch.cisco.com 0`	指定された MSDP ピア宛ての最初の SA メッセージにカプセル化されるマルチキャスト データを制限します。 • *ip-address* | *name* には、TTL の制限が適用される MSDP ピアの IP アドレスまたは名前を入力します。 • *ttl* には、TTL 値を入力します。デフォルトは 0 です。この場合、すべてのマルチキャスト データ パケットは、TTL がなくなるまでピアに転送されます。指定できる範囲は 0 ～ 255 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチで受信される送信元情報の制御

デフォルトでは、デバイスは、MSDP の RPF ピアによって送信されたすべての SA メッセージを受信します。ただし、着信 SA メッセージをフィルタリングし、MSDP ピアから受信する送信元情報を制御できます。つまり、特定の着信 SA メッセージを受信しないようにデバイスを設定できます。

次のいずれかの処理を実行できます。

- MSDP ピアからのすべての着信 SA メッセージのフィルタリング
- 特定の送信元とグループのペアが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **ip msdp sa-filter in** {*ip-address name*}	• 指定された MSDP ピアへの SA メッセージをフィルタリングします。 • IP 拡張アクセス リストを通過する、指定されたピアからの SA メッ

	コマンドまたはアクション	目的
	• **ip msdp sa-filter in** {*ip-address name*} `list` *access-list-number* • **ip msdp sa-filter in** {*ip-address name*} `route-map` *map-tag* 例： `Device(config)#` **`ip msdp sa-filter in switch.cisco.com`** または `Device(config)#` **`ip msdp sa-filter in list 100`** または `Device(config)#` **`ip msdp sa-filter in switch.cisco.com route-map 22`**	セージのみを通過させます。拡張アクセス リスト *access-list-number* の範囲は 100 ～ 199 です。 **list** と **route-map** の両方のキーワードを使用すると、すべての条件に一致しなければ、発信 SA メッセージ内のいずれの（S,G）ペアも通過できません。 • ルート マップ *map-tag* 内の一致条件を満たす、指定された MSDP ピアからの SA メッセージのみを通過させます。 すべての一致条件を満たす場合、ルート マップに **permit** が指定されていれば、ルートはフィルタを通過します。**deny** が指定されていれば、ルートはフィルタリングされます。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* 例： `Device(config)#` **`access list 100 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1`**	（任意）IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *Access-list-number* には、ステップ 2 で指定した番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。

	コマンドまたはアクション	目的
		• *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には1を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MSDP メッシュ グループの設定

MSDP メッシュ グループは、MSDP によって完全なメッシュ型に相互接続された MSDP スピーカーのグループです。メッシュ グループ内のピアから受信された SA メッセージは、同じメッシュ グループ内の他のピアに転送されません。したがって、SA メッセージのフラッディングが削減され、ピア RPF フラッディングが簡素化されます。ドメイン内に複数の RP がある場合は、**ip msdp mesh-group** グローバル コンフィギュレーション コマンドを使用します。特に、ドメインを越えて SA メッセージを送信する場合に使用します。単一のデバイスに複数のメッシュ グループを（異なる名前で）設定できます。

メッシュ グループを作成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp mesh-group** *name* {*ip-address* | *name*} 例： `Device(config)# ip msdp mesh-group 2 switch.cisco.com`	MSDP メッシュ グループを設定し、そのメッシュ グループに属する MSDP ピアを指定します。 デフォルトでは、MSDP ピアはメッシュ グループに属しません。 • *name* には、メッシュ グループの名前を入力します。 • *ip-address* | *name* には、メッシュ グループのメンバーになる MSDP ピアの IP アドレスまたは名前を入力します。 グループ内の MSDP ピアごとに、この手順を繰り返します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

MSDP ピアのシャットダウン

複数のMSDPコマンドが設定された単一のピアをアクティブにしない場合は、ピアをシャットダウンしてから、あとで起動できます。ピアがシャットダウンすると、TCP接続が終了し、再起動されません。ピアの設定情報を保持したまま、MSDPセッションをシャットダウンすることもできます。

ピアをシャットダウンするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp shutdown** {*peer-name* | *peer address*} 例： `Device(config)# ip msdp shutdown switch.cisco.com`	設定情報を保持したまま、指定された MSDP ピアをシャットダウン状態にします。 *peer-name* | *peer address* を指定する場合は、シャットダウンする MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

境界 PIM デンス モード領域の MSDP への包含

デンス モード（DM）領域と PIM スパース モード（SM）領域の境界となるデバイスに MSDP を設定します。デフォルトでは、DM 領域のアクティブな送信元は MSDP に加入しません。

（注） **ip msdp border sa-address** グローバル コンフィギュレーション コマンドの使用は推奨できません。DM ドメイン内の送信元が SM ドメイン内の RP にプロキシ登録されるように SM ドメイン内の境界ルータを設定し、標準 MSDP 手順でこれらの送信元をアドバタイズするように SM ドメインを設定してください。

ip msdp originator-id グローバル コンフィギュレーション コマンドを実行すると、RP アドレスとして使用されるインターフェイスも識別されます。**ip msdp border sa-address** と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスが RP アドレスを指定します。

DM 領域でアクティブな送信元の SA メッセージを MSDP ピアに送信するように境界ルータを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp border sa-address** *interface-id* 例：	DM 領域内のアクティブな送信元に関する SA メッセージを送信するように、

	コマンドまたはアクション	目的
	`Device(config)# ip msdp border sa-address 0/1`	DM 領域と SM 領域の境界スイッチを設定します。 *interface-id* には、SA メッセージ内の RP アドレスとして使用される、IP アドレスの配信元となるインターフェイスを指定します。 インターフェイスの IP アドレスは、SA メッセージ内の RP フィールド [Originator-ID] の値として使用されます。
ステップ 4	**ip msdp redistribute** [**list** *access-list-name*] [**asn** *aspath-access-list-number*] [**route-map** *map*] 例： `Device(config)# ip msdp redistribute list 100`	SA メッセージに格納されてアドバタイズされる、マルチキャスト ルーティング テーブル内の（S,G）エントリを設定します。 詳細については、送信元の再配信（1782 ページ）を参照してください。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

RP アドレス以外の発信元アドレスの設定

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用する場合は、送信元 ID を変更します。次のいずれかの場合に送信元 ID を変更できます。

- MSDP メッシュ グループ内の複数のデバイス上で、論理 RP を設定する場合。
- PIM SM ドメインと DM ドメインの境界となるデバイスがある場合。サイトの DM ドメインの境界となるデバイスがあり、SM がその外部で使用されている場合は、DM の送信元を外部に通知する必要があります。このデバイスはRPでないため、SA メッセージで使用される RP アドレスはありません。したがって、このコマンドではインターフェイスのアドレスを指定し、RP アドレスを提供します。

ip msdp bordersa-address と **ip msdp originator-id** グローバル コンフィギュレーション コマンドの両方が設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスが RP アドレスを指定します。

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用できるようにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp originator-id** *interface-id* 例： `Device(config)# ip msdp originator-id 0/1`	発信元デバイスのインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。 *Interface-id* には、ローカルデバイスのインターフェイスを指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MSDP のモニタリングおよびメンテナンス

MSDP SA メッセージ、ピア、状態、ピアのステータスをモニタするコマンドは以下のとおりです。

表 *104 : MSDP* のモニタおよびメンテナンスのためのコマンド

コマンド	目的
debug ip msdp [*peer-address* | *name*] [**detail**] [**routes**]	MSDP アクティビティをデバッグします。
debug ip msdp resets	MSDP ピアのリセット原因をデバッグします。
show ip msdp count [*autonomous-system-number*]	SA メッセージに格納され、各自律システムから発信された送信元およびグループの個数を表示します。**ip msdp cache-sa-state** コマンドは、このコマンドによって出力が生成されるように設定する必要があります。
show ip msdp peer [*peer-address* | *name*]	MSDP ピアに関する詳細情報を表示します。
show ip msdp sa-cache [*group-address* | *source-address* | *group-name* | *source-name*] [*autonomous-system-number*]	MSDP ピアから学習した（S,G）ステートを表示します。
show ip msdp summary	MSDP ピア ステータスおよび SA メッセージ数を表示します。

MSDP 接続、統計情報、SA キャッシュ エントリをクリアするコマンドは以下のとおりです。

表 *105 : MSDP* 接続、統計情報、または *SA* キャッシュ エントリをクリアするためのコマンド

コマンド	目的
clear ip msdp peer *peer-address* | *name*	指定された MSDP ピアへの TCP 接続をクリアし、すべての MSDP メッセージ カウンタをリセットします。

コマンド	目的
clear ip msdp statistics [*peer-address* | *name*]	セッションをリセットせずに、1 つまたはすべての MSDP ピア統計情報カウンタをクリアします。
clear ip msdp sa-cache [*group-address* | *name*]	すべてのエントリの SA キャッシュ エントリ、特定のグループのすべての送信元、または特定の送信元とグループのペアのすべてのエントリをクリアします。

MSDP の設定例

デフォルト MSDP ピアの設定：例

次に、ルータ A およびルータ C の部分的な設定の例を示します 。これらの ISP にはそれぞれに複数のカスタマー（カスタマーと同様）がおり、 デフォルトのピアリング（BGP または MBGP なし）を使用しています。この場合、両方の ISP で類似した設定となります。つまり、両方の ISP では、対応するプレフィックス リストで SA が許可されている場合、デフォルト ピアからの SA だけが受信されます。

ルータ A

```
Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

ルータ C

```
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

SA ステートのキャッシング：例

次に、グループ 224.2.0.0/16 への送信元である 171.69.0.0/16 のすべての送信元のキャッシュ ステートをイネーブルにする例を示します。

```
Device(config)# ip msdp cache-sa-state 100
Device(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

MSDP ピアからの送信元情報の要求：例

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定する例を示します。

```
Device(config)# ip msdp sa-request 171.69.1.1
```

スイッチから発信される送信元情報の制御：例

次に、171.69.2.2 の MSDP ピアからの SA 要求メッセージをフィルタリングするように、スイッチを設定する例を示します。ネットワーク 192.4.22.0 の送信元からの SA 要求メッセージはアクセス リスト 1 に合格して、受信されます。その他のすべてのメッセージは無視されます。

```
Device(config)# ip msdp filter sa-request 171.69.2.2 list 1
Device(config)# access-list 1 permit 192.4.22.0 0.0.0.255
```

スイッチから転送される送信元情報の制御：例

次に、アクセス リスト 100 を通過する（S,G）ペアだけが SA メッセージに格納され、*switch.cisco.com* という名前のピアに転送されるように設定する例を示します。

```
Device(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
Device(config)# ip msdp sa-filter out switch.cisco.com list 100
Device(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

スイッチで受信される送信元情報の制御：例

次に、*switch.cisco.com* という名前のピアからのすべての SA メッセージをフィルタリングする例を示します。

```
Device(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
Device(config)# ip msdp sa-filter in switch.cisco.com
```

第 92 章

IP ユニキャスト ルーティングの設定

- 機能情報の確認 （1804 ページ）
- IP ユニキャスト ルーティングの設定に関する情報 （1804 ページ）
- IP ルーティングに関する情報 （1804 ページ）
- IP ルーティングの設定方法 （1813 ページ）
- IP アドレッシングの設定方法 （1814 ページ）
- IP アドレスのモニタリングおよびメンテナンス （1834 ページ）
- IP ユニキャスト ルーティングの設定方法 （1836 ページ）
- RIP 情報 （1837 ページ）
- RIP の設定方法 （1838 ページ）
- サマリー アドレスおよびスプリット ホライズンの設定例 （1847 ページ）
- OSPF に関する情報 （1847 ページ）
- OSPF の設定方法 （1852 ページ）
- OSPF の監視 （1864 ページ）
- OSPF の設定例 （1865 ページ）
- EIGRP に関する情報 （1866 ページ）
- EIGRP の設定方法 （1870 ページ）
- EIGRP のモニタリングおよびメンテナンス （1878 ページ）
- BGP に関する情報 （1878 ページ）
- BGP の設定方法 （1888 ページ）
- BGP のモニタリングおよびメンテナンス （1915 ページ）
- BGP の設定例 （1916 ページ）
- ISO CLNS ルーティングに関する情報 （1918 ページ）
- ISO CLNS ルーティングの設定方法 （1922 ページ）
- ISO IGRP と IS-IS のモニタリングおよびメンテナンス （1933 ページ）
- ISO CLNS ルーティングの設定例 （1935 ページ）
- Multi-VRF CE に関する情報 （1936 ページ）
- Multi-VRF CE の設定方法 （1940 ページ）
- Multi-VRF CE の設定例 （1956 ページ）
- ユニキャスト リバース パス転送の設定 （1960 ページ）

• プロトコル独立機能 （1961 ページ）
• IP ネットワークのモニタリングおよびメンテナンス （1986 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IP ユニキャスト ルーティングの設定に関する情報

このモジュールでは、スイッチで IP Version 4（IPv4）ユニキャスト ルーティングを設定する方法について説明します。

（注） LAN ベース フィーチャを実行しているスイッチでは、VLAN でのスタティック ルーティングのみがこのリリースでサポートされます。

スイッチ スタックは、ネットワーク内のそれ以外のルータに対して、単一のルータとして動作し、認識されます。スタティック ルーティング、Routing Information Protocol（RIP）などの基本的なルーティング機能は、IP Base フィーチャ セットおよび IP Services フィーチャ セットの両方で使用できます。拡張ルーティング機能およびその他のルーティング プロトコルを使用するには、スタンドアロン スイッチやアクティブ スイッチで IP サービス フィーチャ セットをイネーブルにする必要があります。

（注） IPv4 トラフィックに加えて、スイッチまたはスイッチ スタックが IP ベースまたは IP サービス フィーチャ セットを実行している場合、IP バージョン 6（IPv6）ユニ キャストルーティングをイネーブルにし、IPv6 トラフィックを転送するようにインターフェイスを設定できます。

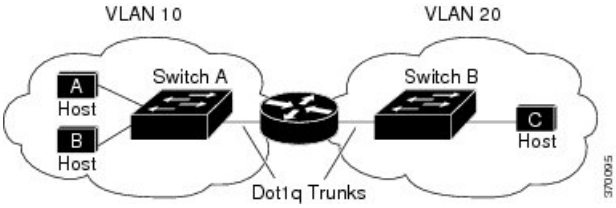
IP ルーティングに関する情報

一部のネットワーク環境で、VLAN（仮想LAN）は各ネットワークまたはサブネットワークに関連付けられています。IP ネットワークで、各サブネットワークは 1 つの VLAN に対応しています。VLAN を設定すると、ブロードキャスト ドメインのサイズを制御し、ローカル トラ

フィックをローカル内にとどめることができます。ただし、異なる VLAN 内のネットワークデバイスが相互に通信するには、VLAN間でトラフィックをルーティング（VLAN間ルーティング）するレイヤ3デバイス（ルータ）が必要です。VLAN 間ルーティングでは、適切な宛先 VLAN にトラフィックをルーティングするため、1 つまたは複数のルータを設定します。

図 *96 :* ルーティング トポロジの例

次の図に基本的なルーティング トポロジを示します。スイッチ A は VLAN 10 内、スイッチ B は VLAN 20 内にあります。ルータには各 VLAN のインターフェイスが備わっています。



VLAN 10 内のホスト A が VLAN 10 内のホスト B と通信する場合、ホスト A はホスト B 宛にアドレス指定されたパケットを送信します。スイッチAはパケットをルータに送信せず、ホスト B に直接転送します。

ホスト A から VLAN 20 内のホスト C にパケットを送信する場合、スイッチ A はパケットをルータに転送し、ルータは VLAN 10 インターフェイスでトラフィックを受信します。ルータはルーティング テーブルを調べて正しい発信インターフェイスを判別し、VLAN 20 インターフェイスを経由してパケットをスイッチ B に送信します。スイッチ B はパケットを受信し、ホスト C に転送します。

ルーティング タイプ

ルータおよびレイヤ 3 スイッチは、次の方法でパケットをルーティングできます。

- デフォルト ルーティング
- 事前にプログラミングされているトラフィックのスタティック ルートの使用
- ルーティング プロトコルによるルートの動的な計算

デフォルトルーティングとは、宛先がルータにとって不明であるトラフィックをデフォルトの出口または宛先に送信することです。

スタティック ユニキャスト ルーティングの場合、パケットは事前に設定されたポートから単一のパスを通り、ネットワークの内部または外部に転送されます。スタティック ルーティングは安全で、帯域幅をほとんど使用しません。ただし、リンク障害などのネットワークの変更には自動的に対応しないため、パケットが宛先に到達しないことがあります。ネットワークが拡大するにつれ、スタティック ルーティングの設定は煩雑になります。

LAN ベース フィーチャ セットを実行しているスイッチは、管理インターフェイスで使用するデフォルト ルートに加えて、ユーザが設定した 16 のスタティック ルートをサポートしています。LAN ベース イメージは、SVI でのみスタティック ルーティングをサポートしています。

ルータでは、トラフィックを転送する最適ルートを動的に計算するため、ダイナミック ルーティング プロトコルが使用されます。ダイナミック ルーティング プロトコルには次の 2 つのタイプがあります。

- ディスタンスベクトル プロトコルを使用するルータでは、ネットワーク リソースの距離の値を使用してルーティングテーブルを保持し、これらのテーブルをネイバーに定期的に渡します。ディスタンスベクトルプロトコルは1つまたは複数のメトリックを使用し、最適なルートを計算します。これらのプロトコルは、簡単に設定、使用できます。
- リンクステート プロトコルを使用するルータでは、ルータ間のリンクステート アドバタイズメント（LSA）の交換に基づき、ネットワーク トポロジに関する複雑なデータベースを保持します。LSA はネットワークのイベントによって起動され、コンバージェンス時間、またはこれらの変更への対応時間を短縮します。リンクステートプロトコルはトポロジの変更にすばやく対応しますが、ディスタンスベクトルプロトコルよりも多くの帯域幅およびリソースが必要になります。

スイッチでサポートされているディスタンスベクトルプロトコルは、Routing Information Protocol（RIP）および Border Gateway Protocol（BGP）です。RIP は最適パスを決定するために単一の距離メトリック（コスト）を使用し、BGP はパス ベクトル メカニズムを追加します。また、Open Shortest Path First（OSPF）リンクステート プロトコル、および従来の Interior Gateway Routing Protocol（IGRP）にリンクステート ルーティング機能の一部を追加して効率化を図った Enhanced IGRP（EIGRP）もサポートされています。

（注） スイッチまたはスイッチ スタックでサポートされるプロトコルは、アクティブ スイッチ上で稼働しているソフトウェアによって決まります。アクティブ スイッチ上で IP ベース フィーチャ セットが稼働している場合は、デフォルトのルーティング、スタティック ルーティング、および RIP だけがサポートされます。スイッチで LAN ベース フィーチャ セットが稼働している場合、SVI では 16 のスタティック ルートを設定できます。その他のすべてのルーティング プロトコルには、IP サービス フィーチャ セットが必要です。

IP ルーティングおよびスイッチ スタック

スタックのスイッチがルーティング ピアに接続されているかどうかに関係なく、スイッチ スタックはネットワークからは単一のスイッチとして認識されます。

アクティブ スイッチにより、次の機能が実行されます。

- ルーティング プロトコルを初期化し、設定します。
- ルーティング プロトコル メッセージおよびアップデートを他のルータに送信します。
- ピア ルータから受信したルーティング プロトコル メッセージおよびアップデートを処理します。

- distributed Cisco Express Forwarding（dCEF）データベースを生成および維持し、すべてのスタック メンバーに配信します。このデータベースに基づいて、スタック内のすべてのスイッチにルートがプログラミングされます。
- アクティブ スイッチの MAC アドレスはスタック全体のルータ MAC アドレスとして使用され、すべての外部デバイスはこのアドレスを使用して IP パケットをスタックに送信します。
- ソフトウェア転送またはソフトウェア処理を必要とするすべての IP パケットは、アクティブ スイッチの CPU を通ります。

スタック メンバーは、次に示す機能を実行します。

- ルーティング スタンバイ スイッチとして機能します。アクティブ スイッチに障害が発生し、新規アクティブ スイッチとして選択された場合に、処理を引き継ぐことができます。
- ルートをハードウェアにプログラムします。

アクティブ スイッチに障害が発生すると、スタックはアクティブ スイッチがダウンしていることを検出し、スタック メンバの 1 つを新規アクティブ スイッチとして選択します。この期間中に、ハードウェアは一時的な中断を除き、アクティブなプロトコルがない状態でパケットの転送を継続します。

ただし、スイッチ スタックが障害のあとハードウェア ID を維持していても、アクティブ スイッチの再起動前の短い中断の間にルータ ネイバーのルーティング プロトコルがフラップすることがあります。OSPF や EIGRP などのルーティング プロトコルは、ネイバーの移行を認識する必要があります。ルータは、次の 2 つのレベルの Nonstop Forwarding（NSF）を使用して、スイッチオーバーの検出、ネットワーク トラフィックの転送の継続、およびピア デバイスから情報の回復を行います。

- NFS 認識ルータによるネイバー ルータ障害の許容。ネイバー ルータの再起動後、NFS 認識ルータは要求を受けて自身のステート情報とルートの隣接情報を提供します。
- NFS 対応ルータによる NSF のサポート。NSF 対応ルータは、アクティブ スイッチの変更を検出した場合、NSF 認識ネイバーまたは NSF 対応ネイバーからの情報でルーティング情報を再構築します。再起動を待つことはしません。

スイッチ スタックは NSF 対応ルーティングを OSPF および EIGRP に対してサポートします。

新規アクティブ スイッチは、選択されたときに次の機能を実行します。

- ルーティング アップデートの生成、受信、および処理を開始します。
- ルーティング テーブルを構築し、CEF データベースを生成して、スタック メンバーに配信します。
- ルータ MAC アドレスとして自身の MAC アドレスを使用します。新規 MAC アドレスのネットワーク ピアに通知するために、新規ルータ MAC アドレスを使用して余分の ARP 応答を定期的に（5 分間の間、数秒おきに）送信します。

（注） 固定 MAC アドレス機能をスタックに設定していて、アクティブ スイッチに変更があった場合、設定された時間スタック MAC アドレスは変更されません。この期間に前のアクティブ スイッチがメンバスイッチとしてスタックに再加入する場合、スタック MAC アドレスは前のアクティブ スイッチの MAC アドレスのままになります。

- ARP 要求をプロキシ ARP IP アドレスに送信し、ARP 応答を受信して、各プロキシ ARP エントリの到達可能性を判別しようとします。到達可能なプロキシ ARP IP アドレスごとに、新規ルータ MAC アドレスを使用して gratuitous ARP 応答を生成します。このプロセスは、新規アクティブ スイッチが選択されたあと、5 分間繰り返されます。

（注） アクティブ スイッチが IP サービス フィーチャ セットを実行している場合は、スタックは、Open Shortest Path First（OSPF）、Enhanced IGRP（EIGRP）、およびボーダー ゲートウェイ プロトコル（BGP）を含む、サポートされるすべてのプロトコルを実行できます。アクティブ スイッチに障害が発生し、新規に選択されたアクティブ スイッチ上で IP ベースまたは LAN ベース フィーチャ セットが稼働している場合、これらのプロトコルはスタック内で稼働しなくなります。

注意 スイッチ スタックを複数のスタックに分割すると、ネットワークが適切に動作しなくなる場合があります。

スイッチがリロードされると、NSF/SSO 機能である場合でも、そのスイッチのポートがすべてダウンし、ルーティングに関わるインターフェイスにトラフィックの損失が発生します。

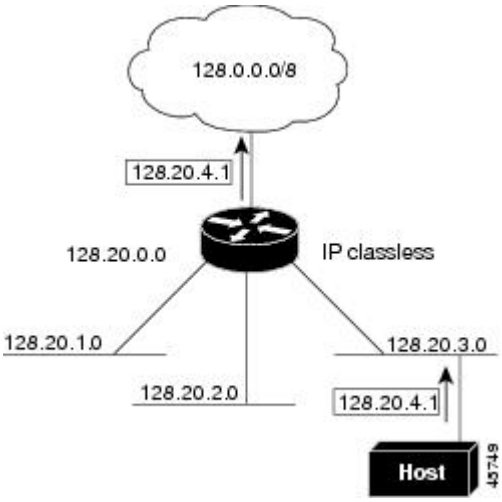
クラスレス ルーティング

ルーティングを行うように設定されたデバイスで、クラスレスルーティング動作はデフォルトでイネーブルとなっています。クラスレスルーティングがイネーブルの場合、デフォルトルートがないネットワークのサブネット宛てパケットをルータが受信すると、ルータは最適なスーパーネットルートにパケットを転送します。スーパーネットは、単一の大規模アドレス空間をシミュレートするために使用されるクラス C アドレス空間の連続ブロックで構成されています。スーパーネットは、クラス B アドレス空間の急速な枯渇を回避するために設計されました。

図では、クラスレスルーティングがイネーブルとなっています。ホストがパケットを 128.20.4.1 に送信すると、ルータはパケットを廃棄せずに、最適なスーパーネットルートに転送します。

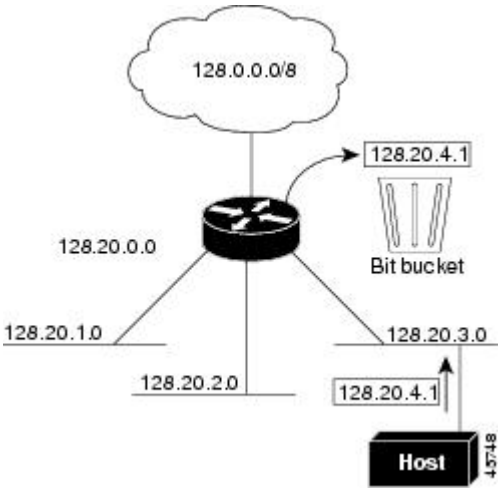
クラスレス ルーティングがディセーブルの場合、デフォルト ルートがないネットワークのサブネット宛てパケットを受信したルータは、パケットを廃棄します。

図 *97 : IP* クラスレス ルーティングがイネーブルの場合



図では、ネットワーク 128.20.0.0 のルータはサブネット 128.20.1.0、128.20.2.0、128.20.3.0 に接続されています。ホストがパケットを 128.20.4.1 に送信した場合、ネットワークのデフォルト ルートが存在しないため、ルータはパケットを廃棄します。

図 *98 : IP* クラスレス ルーティングがディセーブルの場合



デバイスが認識されないサブネット宛てのパケットを最適なスーパーネット ルートに転送しないようにするには、クラスレス ルーティング動作をディセーブルにします。

アドレス解決

インターフェイス固有の IP 処理方法を制御するには、アドレス解決を行います。IP を使用するデバイスには、ローカル セグメントまたは LAN 上のデバイスを一意に定義するローカル ア

ドレス（MAC アドレス）と、デバイスが属するネットワークを特定するネットワーク アドレスがあります。

（注） スイッチスタックでは、スタックの単一のMACアドレスおよびIPアドレスを使用して、ネットワーク通信を行います。

ローカルアドレス（MAC アドレス）は、パケット ヘッダーのデータ リンク層（レイヤ 2）セクションに格納されて、データ リンク（レイヤ2）デバイスによって読み取られるため、データ リンク アドレスと呼ばれます。ソフトウェアがイーサネット上のデバイスと通信するには、デバイスの MAC アドレスを学習する必要があります。IP アドレスから MAC アドレスを学習するプロセスを、アドレス解決と呼びます。MAC アドレスから IP アドレスを学習するプロセスを、逆アドレス解決と呼びます。

デバイスでは、次の形式のアドレス解決を行うことができます。

- ARP：IP アドレスを MAC アドレスと関連付けるために使用されます。ARP は IP アドレスを入力と解釈し、対応する MAC アドレスを学習します。次に、IP アドレス/MAC アドレス アソシエーションを ARP キャッシュにストアし、すぐに取り出せるようにします。その後、IPデータグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化、および ARP 要求や応答については、サブネットワーク アクセス プロトコル（SNAP）で規定されています。
- プロキシ ARP：ルーティング テーブルを持たないホストで、他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにします。デバイス（ルータ）が送信元と異なるインターフェイス上のホストに宛てたARP要求を受信した場合、そのルータに他のインターフェイスを経由してそのホストに至るすべてのルートが格納されていれば、ルータは自身のローカル データ リンク アドレスを示すプロキシ ARP パケットを生成します。ARP 要求を送信したホストはルータにパケットを送信し、ルータはパケットを目的のホストに転送します。

デバイスでは、ARP と同様の機能（ローカル MAC アドレスでなく IP アドレスを要求する点を除く）を持つ Reverse Address Resolution Protocol（RARP）を使用することもできます。RARP を使用するには、ルータ インターフェイスと同じネットワーク セグメント上に RARP サーバを設置する必要があります。サーバを識別するには、**ip rarp-server** *address* インターフェイス コンフィギュレーション コマンドを使用します。

RARP の詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』を参照してください。

プロキシ ARP

プロキシ ARP は、他のルートを学習する場合の最も一般的な方法です。プロキシ ARP を使用すると、ルーティング情報を持たないイーサネット ホストと、他のネットワークまたはサブネット上のホストとの通信が可能になります。このホストでは、すべてのホストが同じローカルイーサネット上にあり、ARP を使用して MAC アドレスを学習すると想定されています。デ

バイスが送信元と異なるネットワーク上にあるホストに宛てた ARP 要求を受信した場合、デバイスはそのホストへの最適なルートがあるかどうかを調べます。最適なルートがある場合、スイッチはデバイス自身のイーサネット MAC アドレスが格納された ARP 応答パケットを送信します。要求の送信元ホストはパケットをスイッチに送信し、スイッチは目的のホストにパケットを転送します。プロキシ ARP は、すべてのネットワークをローカルな場合と同様に処理し、IP アドレスごとに ARP 処理を実行します。

ICMP Router Discovery Protocol

ルータ ディスカバリを使用すると、デバイスは ICMP Router Discovery Protocol（IRDP）を使用し、他のネットワークへのルートを動的に学習します。ホストは IRDP を使用し、ルータを特定します。クライアントとして動作しているデバイスは、ルータ ディスカバリ パケットを生成します。ホストとして動作しているデバイスは、ルータ ディスカバリ パケットを受信します。デバイスは Routing Information Protocol（RIP）ルーティングのアップデートを受信し、この情報を使用してルータの場所を推測することもできます。実際のところ、ルーティングデバイスによって送信されたルーティングテーブルは、デバイスにストアされません。どのシステムがデータを送信しているのかが記録されるだけです。IRDP を使用する利点は、プライオリティと、パケットが受信されなくなってからデバイスがダウンしていると見なされるまでの期間の両方をルータごとに指定できることです。

検出された各デバイスは、デフォルト ルータの候補となります。現在のデフォルト ルータがダウンしたと宣言された場合、または再送信が多すぎて TCP 接続がタイムアウトになりつつある場合、プライオリティが上位のルータが検出されると、最も高いプライオリティを持つ新しいルータが選択されます。

UDP ブロードキャスト パケットおよびプロトコル

ユーザ データグラム プロトコル（UDP）は IP のホスト間レイヤ プロトコルで、TCP と同様です。UDP はオーバーヘッドが少ない、コネクションレスのセッションを 2 つのエンド システム間に提供しますが、受信されたデータグラムの確認応答は行いません。場合に応じてネットワーク ホストは UDP ブロードキャストを使用し、アドレス、コンフィギュレーション、名前に関する情報を検索します。このようなホストが、サーバを含まないネットワーク セグメント上にある場合、通常 UDP ブロードキャストは転送されません。この状況を改善するには、特定のクラスのブロードキャストをヘルパー アドレスに転送するように、ルータのインターフェイスを設定します。インターフェイスごとに、複数のヘルパー アドレスを使用できます。

UDP 宛先ポートを指定し、転送される UDP サービスを制御できます。複数の UDP プロトコルを指定することもできます。旧式のディスクレス Sun ワークステーションおよびネットワーク セキュリティ プロトコル SDNS で使用される Network Disk（ND）プロトコルも指定できます。

ヘルパー アドレスがインターフェイスに定義されている場合、デフォルトでは UDP と ND の両方の転送がイネーブルになっています。『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』の **ip forward-protocol** インターフェイス コンフィギュレーション コマンドの説明には、UDP ポートを指定しない場合にデフォルトで転送されるポートがリストされています。

ブロードキャスト パケットの処理

IPインターフェイスアドレスを設定したあとで、ルーティングをイネーブルにしたり、1つまたは複数のルーティング プロトコルを設定したり、ネットワーク ブロードキャストへのデバイスの応答方法を設定したりできます。ブロードキャストは、物理ネットワーク上のすべてのホスト宛てのデータ パケットです。デバイスでは、2種類のブロードキャストがサポートされています。

- ダイレクト ブロードキャスト パケット：特定のネットワークまたは一連のネットワークに送信されます。ダイレクト ブロードキャスト アドレスには、ネットワークまたはサブネット フィールドが含まれます。
- フラッディング ブロードキャスト パケット：すべてのネットワークに送信されます。

（注） **storm-control** インターフェイス コンフィギュレーション コマンドを使用して、トラフィック抑制レベルを設定し、レイヤ 2 インターフェイスでブロードキャスト、ユニキャスト、マルチキャスト トラフィックを制限することもできます。

ルータはローカル ケーブルまでの範囲を制限して、ブロードキャスト ストームを防ぎます。ブリッジ（インテリジェントなブリッジを含む）はレイヤ 2 デバイスであるため、ブロードキャストはすべてのネットワーク セグメントに転送され、ブロードキャスト ストームを伝播します。ブロードキャストストーム問題を解決する最善の方法は、ネットワーク上で単一のブロードキャスト アドレス方式を使用することです。最新の IP 実装機能ではほとんどの場合、アドレスをブロードキャスト アドレスとして使用するように設定できます。デバイスをはじめ、多数の実装機能では、ブロードキャストメッセージを転送するためのアドレス方式が複数サポートされています。

IP ブロードキャストのフラッディング

IPブロードキャストをインターネットワーク全体に、制御可能な方法でフラッディングできるようにするには、ブリッジングSTPで作成されたデータベースを使用します。この機能を使用すると、ループを回避することもできます。この機能を使用できるようにするには、フラッディングが行われるインターフェイスごとにブリッジングを設定する必要があります。ブリッジングが設定されていないインターフェイス上でも、ブロードキャストを受信できます。ただし、ブリッジングが設定されていないインターフェイスでは、受信したブロードキャストが転送されません。また、異なるインターフェイスで受信されたブロードキャストを送信する場合、このインターフェイスは使用されません。

IPヘルパーアドレスのメカニズムを使用して単一のネットワーク アドレスに転送されるパケットを、フラッディングできます。各ネットワーク セグメントには、パケットのコピーが1つだけ送信されます。

フラッディングを行う場合、パケットは次の条件を満たす必要があります（これらの条件は、IP ヘルパー アドレスを使用してパケットを転送するときの条件と同じです）。

- パケットは MAC レベルのブロードキャストでなければなりません。
- パケットは IP レベルのブロードキャストでなければなりません。
- パケットは Trivial File Transfer Protocol（TFTP）、ドメイン ネーム システム（DNS）、Time、NetBIOS、ND、または BOOTP パケット、または **ip forward-protocol udp** グローバル コンフィギュレーション コマンドで指定された UDP でなければなりません。
- パケットの存続可能時間（TTL）値は 2 以上でなければなりません。

フラッディングされた UDP データグラムには、出力インターフェイスで **ip broadcast-address** インターフェイス コンフィギュレーション コマンドによって指定された宛先アドレスが表示されます。宛先アドレスを、任意のアドレスに設定できます。このため、データグラムがネットワーク内に伝播されるにつれ、宛先アドレスが変更されることもあります。送信元アドレスは変更されません。TTL 値が減ります。

フラッディングされた UDP データグラムがインターフェイスから送信されると（場合によっては宛先アドレスが変更される）、データグラムは通常の IP 出力ルーチンに渡されます。このため、出力インターフェイスにアクセス リストがある場合、データグラムはその影響を受けます。

デバイスでは、パケットの大部分がハードウェアで転送され、デバイスの CPU を経由しません。CPU に送信されるパケットの場合は、ターボフラッディングを使用し、スパニングツリーベースの UDP フラッディングを約 4 ～ 5 倍高速化します。この機能は、ARP カプセル化用に設定されたイーサネット インターフェイスでサポートされています。

IP ルーティングの設定方法

デバイス上で、IP ルーティングはデフォルトでディセーブルとなっているため、ルーティングを行う前に、IP ルーティングをイネーブルにする必要があります。IP ルーティングに関する設定情報については、『*Cisco IOS IP Configuration Guide*』を参照してください。

次の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。

- ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドを使用し、レイヤ 3 ポートとして設定された物理ポートです。
- スイッチ仮想インターフェイス（SVI）：**interface vlan** *vlan_id* グローバル コンフィギュレーション コマンドによって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。

（注） IP ルーティングを有効にすると、SVI として設定されている VLAN もまた、自分宛先ではないブロードキャスト ARP 要求を学習します。

- レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイス

をチャネル グループにバインドして作成されたポートチャネル論理インターフェイス。詳細については、『Layer 2 Configuration Guide』の「Configuring Layer 3 EtherChannels」の章を参照してください。

（注） スイッチは、ユニキャスト ルーテッド トラフィックのトンネル インターフェイスをサポートしません。

ルーティングが発生するすべてのレイヤ3インターフェイスに、IPアドレスを割り当てる必要があります。

（注） スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。

設定できるルーテッド ポートおよび SVI の個数は 128 に制限されています。推奨個数と実装されている機能の数量を超えると、ハードウェアによって制限されるため、CPU利用率が影響を受けることがあります。

ルーティングを設定するための主な手順は次のとおりです。

- VLANインターフェイスをサポートするには、デバイスまたはスイッチ スタックでVLANを作成および設定し、レイヤ 2 インターフェイスに VLAN メンバーシップを割り当てます。詳細については、『VLAN Configuration Guide』の「Configuring VLANs」の章を参照してください。
- レイヤ 3 インターフェイスを設定します。
- スイッチ上で IP ルーティングをイネーブルに設定します。
- レイヤ 3 インターフェイスに IP アドレスを割り当てます。
- 選択したルーティング プロトコルをスイッチ上でイネーブルにします。
- ルーティング プロトコル パラメータを設定します（任意）。

IP アドレッシングの設定方法

IP ルーティングを設定するには、レイヤ 3 ネットワーク インターフェイスに IP アドレスを割り当ててインターフェイスをイネーブルにし、IP を使用するインターフェイスを経由してホストとの通信を許可する必要があります。次の項では、さまざまな IP アドレス指定機能の設定方法について説明します。IPアドレスをインターフェイスに割り当てる手順は必須ですが、その他の手順は任意です。

- アドレス指定のデフォルト設定
- ネットワーク インターフェイスへの IP アドレスの割り当て

- アドレス解決方法の設定
- IP ルーティングがディセーブルの場合のルーティング支援機能
- ブロードキャスト パケットの処理方法の設定
- IP アドレスのモニタリングおよびメンテナンス

IP アドレス指定のデフォルト設定

表 *106 :* アドレス指定のデフォルト設定

機能	デフォルト設定
IP アドレス	未定義
『ARP』	ARP キャッシュに永続的なエントリはありません カプセル化：標準イーサネット形式の ARP 14400 秒（4 時間）
IP ブロードキャスト アドレス	255.255.255.255（すべて 1）
IP クラスレス ルーティング	イネーブル
IP デフォルト ゲートウェイ	ディセーブル
IP ダイレクト ブロードキャスト	ディセーブル（すべての IP ダイレクト ブロードキャストがドロップされます）
IP ドメイン	ドメイン リスト：ドメイン名は未定義 ドメイン検索：イネーブル ドメイン名：イネーブル
IP 転送プロトコル	ヘルパー アドレスが定義されているか、またはユーザ データグラム プロトコル（UDP）フラッディングが設定されている場合、デフォルト ポートでは UDP 転送がイネーブルとなります ローカル ブロードキャスト：ディセーブル スパニングツリー プロトコル（STP）：ディセーブル ターボフラッディング：ディセーブル
IP ヘルパー アドレス	ディセーブル

機能	デフォルト設定
IP ホスト	ディセーブル
ICMP Router Discovery Protocol（IRDP）	ディセーブル イネーブルの場合のデフォルト： • ブロードキャスト IRDP アドバタイズメント • アドバタイズメント間の最大インターバル：600 秒 • アドバタイズ間の最小インターバル：最大インターバルの 0.75 倍 • プリファレンス：0
IP プロキシ ARP	イネーブル
IP ルーティング	ディセーブル
IP サブネットゼロ	ディセーブル

ネットワーク インターフェイスへの IP アドレスの割り当て

IP アドレスは IP パケットの送信先を特定します。一部の IP アドレスは特殊な目的のために予約されていて、ホスト、サブネット、またはネットワーク アドレスには使用できません。RFC 1166 の『Internet Numbers』には IP アドレスに関する公式の説明が記載されています。

インターフェイスには、1 つのプライマリ IP アドレスを設定できます。マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。マスクを使用してネットワークをサブネット化する場合、そのマスクをサブネット マスクと呼びます。割り当てられているネットワーク番号については、インターネット サービス プロバイダーにお問い合わせください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**no switchport** 例： `Device(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 5	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 10.1.5.1 255.255.255.0`	IP アドレスおよび IP サブネット マスクを設定します。
ステップ 6	**no shutdown** 例： `Device(config-if)# no shutdown`	物理インターフェイスをイネーブルにします。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip route** 例： `Device# show ip route`	入力を確認します。
ステップ 9	**show ip interface** [*interface-id*] 例： `Device# show ip interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 10	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

サブネット ゼロの使用

サブネット アドレスがゼロであるサブネットを作成しないでください。同じアドレスを持つネットワークおよびサブネットがある場合に問題が発生することがあります。たとえば、ネットワーク 131.108.0.0 のサブネットが 255.255.255.0 の場合、サブネット ゼロは 131.108.0.0 と記述され、ネットワーク アドレスと同じとなってしまいます。

すべてが 1 のサブネット（131.108.255.0）は使用可能です。また、IP アドレス用にサブネットスペース全体が必要な場合は、サブネット ゼロの使用をイネーブルにできます（ただし推奨できません）。

デフォルトに戻して、サブネット ゼロの使用をディセーブルにするには、**no ip subnet-zero** グローバル コンフィギュレーション コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip subnet-zero** 例： `Device(config)# ip subnet-zero`	インターフェイス アドレスおよびルーティングのアップデート時にサブネット ゼロの使用をイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

クラスレス ルーティングのディセーブル化

デバイスが認識されないサブネット宛てのパケットを最適なスーパーネットルートに転送しないようにするには、クラスレス ルーティング動作をディセーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ip classless** 例： `Device(config)#no ip classless`	クラスレスルーティング動作をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

アドレス解決方法の設定

アドレス解決を設定するために必要な作業は次のとおりです。

スタティック ARP キャッシュの定義

ARP および他のアドレス解決プロトコルを使用すると、IP アドレスと MAC アドレス間をダイナミックにマッピングできます。ほとんどのホストではダイナミック アドレス解決がサポートされているため、通常の場合、スタティック ARP キャッシュ エントリを指定する必要はありません。スタティック ARP キャッシュ エントリを定義する必要がある場合は、グローバルにそれを定義できます。グローバルに定義すると、IP アドレスを MAC アドレスに変換するためにデバイスが使用するARP キャッシュに永続的なエントリをインストールします。また、指定された IP アドレスに属しているかのように、デバイスが ARP 要求に応答するように指定することもできます。ARP エントリを永続的なエントリにしない場合は、ARP エントリのタイムアウト期間を指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**arp** *ip-address hardware-address type* 例：	ARP キャッシュ内で IP アドレスを MAC（ハードウェア）アドレスに関連付け、次に示すカプセル化タイプのいずれかを指定します。

	コマンドまたはアクション	目的
	`Device(config)# ip 10.1.5.1 c2f3.220a.12f4 arpa`	• **arpa**：ARP カプセル化（イーサネット インターフェイス用） • **snap**：SNAP カプセル化（トークン リングおよび FDDI インターフェイス用） • **sap**：HP の ARP タイプ
ステップ 4	**arp** *ip-address hardware-address type* [**alias**] 例： `Device(config)# ip 10.1.5.3 d7f3.220d.12f5 arpa alias`	（任意）指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定します。
ステップ 5	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するインターフェイスを指定します。
ステップ 6	**arp** *timeout seconds* 例： `Device(config-if)# arp 20000`	（任意）ARP キャッシュ エントリがキャッシュに保持される期間を設定します。デフォルト値は 14400 秒（4 時間）です。指定できる範囲は 0 ～ 2147483 秒です。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** [*interface-id*] 例： `Device# show interfaces gigabitethernet 1/0/1`	すべてのインターフェイスまたは特定のインターフェイスで使用される ARP のタイプおよびタイムアウト値を確認します。
ステップ 9	**show arp** 例： `Device# show arp`	ARP キャッシュの内容を表示します。
ステップ 10	**show ip arp** 例：	ARP キャッシュの内容を表示します。

	コマンドまたはアクション	目的
	`Device# show ip arp`	
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ARP のカプセル化の設定

IP インターフェイスでは、イーサネット ARP カプセル化（**arpa** キーワードで表される）がデフォルトでイネーブルに設定されています。ネットワークの必要性に応じて、カプセル化方法を SNAP に変更できます。

カプセル化タイプをディセーブルにするには、**no arp arpa** または **no arp snap** インターフェイス コンフィギュレーション コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	インターフェイスコンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**arp** {**arpa** | **snap**} 例： `Device(config-if)# arp arpa`	ARP カプセル化方法を指定します。 • **arpa**：Address Resolution Protocol • **snap**：Subnetwork Address Protocol

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*] 例： `Device# show interfaces`	すべてのインターフェイスまたは指定されたインターフェイスの ARP カプセル化設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

プロキシ ARP のイネーブル化

デフォルトでは、プロキシ ARP がデバイスで使用されます。ホストが他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにするためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	インターフェイスコンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip proxy-arp** 例：	インターフェイス上でプロキシ ARP をイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config-if)# ip proxy-arp`	
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip interface** [*interface-id*] 例： `Device# show ip interface gigabitethernet 1/0/2`	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ルーティングがディセーブルの場合のルーティング支援機能

次のメカニズムを使用することで、デバイスは IP ルーティングがイネーブルでない場合、別のネットワークへのルートを学習できます。

- 『Proxy ARP』
- デフォルト ゲートウェイ
- ICMP Router Discovery Protocol（IRDP）

プロキシ ARP

プロキシ ARP は、デフォルトでイネーブルに設定されています。ディセーブル化されたプロキシ ARP をイネーブルにするには、「プロキシ ARP のイネーブル化」の項を参照してください。プロキシ ARP は、他のルータでサポートされているかぎり有効です。

デフォルト ゲートウェイ

ルートを特定するもう 1 つの方法は、デフォルト ルータ、つまりデフォルト ゲートウェイを定義する方法です。ローカルでないすべてのパケットはこのルータに送信されます。このルータは適切なルーティングを行う、または IP 制御メッセージプロトコル（ICMP）リダイレクトメッセージを返信するという方法で、ホストが使用するローカルルータを定義します。デバイスはリダイレクトメッセージをキャッシュに格納し、各パケットをできるだけ効率的に転送し

ます。この方法には、デフォルト ルータがダウンした場合、または使用できなくなった場合に、検出が不可能となる制限があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip default-gateway** *ip-address* 例： `Device(config)# ip default gateway 10.1.5.1`	デフォルト ゲートウェイ（ルータ）を設定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip redirects** 例： `Device# show ip redirects`	設定を確認するため、デフォルト ゲートウェイ ルータのアドレスを表示します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ICMP Router Discovery Protocol（IRDP）

インターフェイスでIRDPルーティングを行う場合は、インターフェイスでIRDP処理をイネーブルにしてください。IRDP 処理をイネーブルにすると、デフォルトのパラメータが適用されます。

これらのパラメータを変更することもできます。**maxadvertinterval** 値を変更すると、**holdtime** 値および **minadvertinterval** 値も変更されます。最初に **maxadvertinterval** 値を変更し、次に **holdtime** 値または **minadvertinterval** 値のいずれかを手動で変更することが重要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip irdp** 例： `Device(config-if)# ip irdp`	インターフェイスでIRDP処理をイネーブルにします。
ステップ 5	**ip irdp multicast** 例： `Device(config-if)# ip irdp multicast`	（任意）IP ブロードキャストの代わりとして、マルチキャスト アドレス（224.0.0.1）に IRDP アドバタイズを送信します。 （注） このコマンドを使用すると、IRDP パケットをマルチキャストとして送信するサンマイクロシステムズ社の Solaris との互換性を維持できます。実装機能の中には、これらのマルチキャストを受信できないものも多くあります。このコマンドを使用する前に、エンドホストがこの機能に対応していることを確認してください。

	コマンドまたはアクション	目的
ステップ 6	**ip irdp holdtime** *seconds* 例： `Device(config-if)# ip irdp holdtime 1000`	（任意）アドバタイズが有効である IRDP 期間を設定します。デフォルト値は **maxadvertinterval** 値の 3 倍です。**maxadvertinterval** 値よりも大きな値（9000 秒以下）を指定する必要があります。**maxadvertinterval** 値を変更すると、この値も変更されます。
ステップ 7	**ip irdp maxadvertinterval** *seconds* 例： `Device(config-if)# ip irdp maxadvertinterval 650`	（任意）アドバタイズメントの IRDP 最大間隔を設定します。デフォルトは 600 秒です。
ステップ 8	**ip irdp minadvertinterval** *seconds* 例： `Device(config-if)# ip irdp minadvertinterval 500`	（任意）アドバタイズ間の IRDP の最小インターバルを設定します。デフォルト値は **maxadvertinterval** 値の 0.75 倍です。**maxadvertinterval** を変更すると、この値も新しいデフォルト値（**maxadvertinterval** の 0.75 倍）に変更されます。
ステップ 9	**ip irdp preference** *number* 例： `Device(config-if)# ip irdp preference 2`	（任意）デバイスの IRDP プリファレンス レベルを設定します。指定できる範囲は -231 ～ 231 です。デフォルトは 0 です。大きな値を設定すると、ルータのプリファレンス レベルも高くなります。
ステップ 10	**ip irdp address** *address* [*number*] 例： `Device(config-if)# ip irdp address 10.1.10.10`	（任意）プロキシアドバタイズを行うための IRDP アドレスとプリファレンスを設定します。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show ip irdp** 例： `Device# show ip irdp`	IRDP 値を表示し、設定を確認します。

	コマンドまたはアクション	目的
ステップ 13	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ブロードキャスト パケットの処理方法の設定

これらの方式をイネーブルにするには、次に示す作業を実行します。

- ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化
- UDP ブロードキャスト パケットおよびプロトコルの転送
- IP ブロードキャスト アドレスの確立
- IP ブロードキャストのフラッディング

ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化

デフォルトでは、IP ダイレクト ブロードキャストがドロップされるため、転送されることはありません。IP ダイレクト ブロードキャストがドロップされると、ルータが DoS 攻撃（サービス拒絶攻撃）にさらされる危険が少なくなります。

ブロードキャストが物理（MAC レイヤ）ブロードキャストになるインターフェイスでは、IP ダイレクト ブロードキャストの転送をイネーブルにできます。**ip forward-protocol** グローバル コンフィギュレーション コマンドを使用し、設定されたプロトコルだけを転送できます。

転送するブロードキャストを制御するアクセス リストを指定できます。アクセス リストを指定すると、アクセス リストで許可されている IP パケットだけが、ダイレクト ブロードキャストから物理ブロードキャストに変換できるようになります。アクセス リストの詳細については、『Security Configuration Guide』の「Information about Network Security with ACLs」の項を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	インターフェイス コンフィギュレーションモードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ip directed-broadcast** [*access-list-number*] 例： `Device(config-if)# ip directed-broadcast 103`	インターフェイス上で、ダイレクトブロードキャストから物理ブロードキャストへの変換をイネーブルにします。転送するブロードキャストを制御するアクセスリストを指定できます。アクセスリストを指定すると、アクセスリストで許可されているIPパケットだけが変換可能になります。 （注） **ip directed-broadcast** インターフェイス コンフィギュレーション コマンドは VPN ルーティングおよび転送（VRF）インターフェイスで設定でき、こうすると VRF 対応になります。ダイレクトブロードキャスト トラフィックが VRF 内でだけルーティングされます。
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーションモードに戻ります。
ステップ 6	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**} 例： `Device(config)# ip forward-protocol nd`	ブロードキャストパケットを転送するとき、ルータによって転送されるプロトコルおよびポートを指定します。 • **udp**：UPD データグラムを転送します。 port：（任意）転送される UDP サービスを制御する宛先ポートです。 • **nd**：ND データグラムを転送します。

	コマンドまたはアクション	目的
		• **sdns**：SDNS データグラムを転送します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip interface** [*interface-id*] 例： `Device# show ip interface`	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

UDP ブロードキャスト パケットおよびプロトコルの転送

UDPブロードキャストの転送を設定するときにUDPポートを指定しないと、ルータはBOOTPフォワーディング エージェントとして動作するように設定されます。BOOTP パケットは Dynamic Host Configuration Protocol（DHCP）情報を伝達します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip helper-address** *address* 例： `Device(config-if)# ip helper address 10.1.10.1`	転送をイネーブルにし、BOOTP などの UDP ブロードキャストパケットを転送するための宛先アドレスを指定します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーションモードに戻ります。
ステップ 6	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**} 例： `Device(config)# ip forward-protocol sdns`	ブロードキャストパケットを転送するときに、ルータによって転送されるプロトコルを指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip interface** [*interface-id*] 例： `Device# show ip interface gigabitethernet 1/0/1`	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例：	（任意）コンフィギュレーションファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

IP ブロードキャスト アドレスの確立

最も一般的な（デフォルトの）IP ブロードキャスト アドレスは、すべて 1 で構成されているアドレス（255.255.255.255）です。ただし、任意の形式の IP ブロードキャスト アドレスを生成するようにデバイスを設定することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイスコンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ip broadcast-address** *ip-address* 例： `Device(config-if)# ip broadcast-address 128.1.255.255`	デフォルト値と異なるブロードキャスト アドレス（128.1.255.255 など）を入力します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show ip interface** [*interface-id*] 例： `Device# show ip interface`	指定されたインターフェイスまたはすべてのインターフェイスのブロードキャスト アドレスを確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ブロードキャストのフラッディング

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip forward-protocol spanning-tree** 例： `Device(config)# ip forward-protocol spanning-tree`	ブリッジング スパニングツリーデータベースを使用し、UDPデータグラムをフラッディングします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。
ステップ 7	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 8	**ip forward-protocol turbo-flood** 例： `Device(config)# ip forward-protocol turbo-flood`	スパニングツリーデータベースを使用し、UDPデータグラムのフラッディングを高速化します。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

IP アドレスのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容が無効になっている場合、または無効である可能性がある場合は、**clear** 特権 EXEC コマンドを使用し、すべての内容を削除できます。次の表に、内容をクリアするために使用するコマンドを示します。

表 *107*：キャッシュ、テーブル、データベースをクリアするコマンド

clear arp-cache	IP ARP キャッシュおよび高速スイッチング キャッシュをクリアします。
clear host {*name* | *}	ホスト名およびアドレス キャッシュから 1 つまたはすべてのエントリを削除します。
clear ip route {**network** [*mask*] | *}	IP ルーティング テーブルから 1 つまたは複数のルートを削除します。

IP ルーティング テーブル、キャッシュ、データベースの内容、ノードへの到達可能性、ネットワーク内のパケットのルーティング パスなど、特定の統計情報を表示できます。次の表に、IP 統計情報を表示するために使用する特権 EXEC コマンドを示します。

表 *108*：キャッシュ、テーブル、データベースを表示するコマンド

show arp	ARP テーブル内のエントリを表示します。
show hosts	デフォルトのドメイン名、検索サービスの方式、サーバ ホスト名、およびキャッシュに格納されているホスト名とアドレスのリストを表示します。
show ip aliases	TCP ポートにマッピングされた IP アドレスを表示します（エイリアス）。
show ip arp	IP ARP キャッシュを表示します。
show ip interface [*interface-id*]	インターフェイスの IP ステータスを表示します。
show ip irdp	IRDP 値を表示します。
show ip masks *address*	ネットワーク アドレスに対して使用されるマスクおよび各マスクを使用するサブネット番号を表示します。
show ip redirects	デフォルト ゲートウェイのアドレスを表示します。
show ip route [*address* [*mask*]] | [*protocol*]	ルーティング テーブルの現在の状態を表示します。
show ip route summary	サマリー形式でルーティング テーブルの現在のステータスを表示します。

IP ユニキャスト ルーティングの設定方法

IP ユニキャスト ルーティングのイネーブル化

デフォルトで、デバイスはレイヤ 2 スイッチング モード、IP ルーティングはディセーブルとなっています。デバイスのレイヤ3機能を使用するには、IPルーティングをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip routing** 例： `Device(config)# ip routing`	IPルーティングをイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

IP ルーティングのイネーブル化の例

次に、ルーティング プロトコルとして RIP を使用し、 上で IP ルーティングをイネーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip routing
Device(config)# router rip
Device(config-router)# network 10.0.0.0
Device(config-router)# end
```

次の作業

ここで、選択したルーティング プロトコルのパラメータを設定できます。具体的な手順は次のとおりです。

- RIP
- OSPF
- EIGRP
- BGP
- ユニキャスト Reverse Path Forwarding
- プロトコル独立機能（任意）

RIP 情報

RIP は、小規模な同種ネットワーク間で使用するために作成された Interior Gateway Protocol（IGP）です。RIP は、ブロードキャスト ユーザ データグラム プロトコル（UDP）データ パケットを使用してルーティング情報を交換するディスタンスベクトル ルーティング プロトコルです。このプロトコルは RFC 1058 に文書化されています。RIP の詳細については、『*IP Routing Fundamentals*』（Cisco Press 刊）を参照してください。

（注） RIP は IP ベース でサポートされています。

デバイスはRIPを使用し、30秒ごとにルーティング情報アップデート（アドバタイズメント）を送信します。180秒以上を経過しても別のルータからアップデートがルータに届かない場合、

該当するルータから送られたルートは使用不能としてマークされます。240 秒後もまだ更新がない場合、ルータは更新のないルータのルーティングテーブルエントリをすべて削除します。

RIP では、各ルートの値を評価するためにホップ カウントが使用されます。ホップ カウントは、ルート内で経由されるルータ数です。直接接続されているネットワークのホップ カウントは 0 です。ホップ カウントが 16 のネットワークに到達できません。このように範囲（0 ～ 15）が狭いため、RIP は大規模ネットワークには適していません。

ルータにデフォルトのネットワーク パスが設定されている場合、RIP はルータを疑似ネットワーク 0.0.0.0 にリンクするルートをアドバタイズします。0.0.0.0 ネットワークは存在しません。RIP はデフォルトのルーティング機能を実行するためのネットワークとして、このネットワークを処理します。デフォルト ネットワークが RIP によって学習された場合、またはルータにラスト リゾート ゲートウェイがあり、RIP がデフォルトのメトリックによって設定されている場合、デバイスはデフォルト ネットワークをアドバタイズします。RIP は指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイスのネットワークを指定しなければ、RIP のアップデート中にアドバタイズされません。

サマリー アドレスおよびスプリット ホライズン

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティング ループの発生を抑えるために、スプリット ホライズン メカニズムが使用されます。スプリット ホライズンは、ルートに関する情報の発信元であるインターフェイス上の、ルータによって、その情報がアドバタイズされないようにします。この機能を使用すると、通常の場合は複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。

RIP の設定方法

RIP のデフォルト設定

表 *109 : RIP* のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル
デフォルト情報送信元	ディセーブル
デフォルト メトリック	自動メトリック変換（組み込み）
IP RIP 認証キーチェーン	認証なし 認証モード：クリア テキスト
IP RIP の起動	ディセーブル

機能	デフォルト設定
IP スプリット ホライズン	メディアにより異なる
Neighbor	未定義
ネットワーク	指定なし
オフセット リスト	ディセーブル
出力遅延	0 ミリ秒
タイマー基準	• 更新：30 秒 • 無効：180 秒 • ホールドダウン：180 秒 • フラッシュ：240 秒
アップデート送信元の検証	イネーブル
Version	RIP バージョン 1 およびバージョン 2 パケットを受信し、バージョン 1 パケットを送信します。

基本的な RIP パラメータの設定

RIP を設定するには、ネットワークに対して RIP ルーティングをイネーブルにします。他のパラメータを設定することもできます。デバイスでは、ネットワーク番号を設定するまでRIP コンフィギュレーション コマンドは無視されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip routing** 例： `Device(config)# ip routing`	IP ルーティングをイネーブルにします。（IP ルーティングがディセーブルになっている場合だけ、必須です）。
ステップ 4	**router rip** 例： `Device(config)# router rip`	RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 5	**network** *network number* 例： `Device(config)# network 12`	ネットワークを RIP ルーティング プロセスと関連付けます。複数の **network** コマンドを指定できます。RIP ルーティング アップデートの送受信は、これらのネットワークのインターフェイスを経由する場合だけ可能です。 （注） RIP コマンドを有効にするには、ネットワーク番号を設定する必要があります。
ステップ 6	**neighbor** *ip-address* 例： `Device(config)# neighbor 10.2.5.1`	（任意）ルーティング情報を交換する隣接ルータを定義します。このステップを使用すると、RIP（通常はブロードキャストプロトコル）からのルーティング アップデートが非ブロードキャスト ネットワークに到達するようになります。
ステップ 7	**offset-list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*] 例： `Device(config)# offset-list 103 in 10`	（任意）オフセット リストをルーティング メトリックに適用し、RIP によって取得したルートへの着信および発信メトリックを増加します。アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。
ステップ 8	**timers basic** *update invalid holddown flush* 例： `Device(config)# timers basic 45 360 400 300`	（任意）ルーティング プロトコル タイマーを調整します。すべてのタイマーの有効範囲は 0 ～ 4294967295 秒です。 • *update*：ルーティング アップデートの送信間隔。デフォルトは 30 秒です。

	コマンドまたはアクション	目的
		• *invalid*：ルートが無効と宣言されるまでの時間。デフォルト値は180秒です。 • *holddown*：ルートがルーティングテーブルから削除されるまでの時間。デフォルト値は 180 秒です。 • *flush*：ルーティング アップデートが延期される時間。デフォルトは 240 秒です。
ステップ 9	**version** {**1** | **2**} 例： `Device(config)# version 2`	（任意）RIP バージョン 1 または RIP バージョン 2 のパケットだけを送受信するようにスイッチを設定します。デフォルトの場合、スイッチではバージョン 1 および 2 を受信しますが、バージョン 1 だけを送信します。インターフェイス コマンド **ip rip** {**send** | **receive**} **version 1** | **2** | **1 2**} を使用し、インターフェイスでの送受信に使用するバージョンを制御することもできます。
ステップ 10	**no auto summary** 例： `Device(config)# no auto summary`	（任意）自動要約をディセーブルにします。デフォルトでは、クラスフルネットワーク境界を通過するときにサブプレフィックスがサマライズされます。サマライズをディセーブルにし（RIP バージョン 2 だけ）、クラスフルネットワーク境界にサブネットおよびホストルーティング情報をアドバタイズします。
ステップ 11	**no validate-update-source** 例： `Device(config)# no validdate-update-source`	（任意）着信 RIP ルーティング アップデートの送信元 IP アドレスの検証をディセーブルにします。デフォルトでは、スイッチが着信 RIP ルーティング アップデートの送信元IPアドレスを検証します。送信元アドレスが無効な場合は、アップデートが廃棄されます。通常の環境で使用する場合は、この機能をディセーブルにしないでください。ただし、ネットワークに接続されていないルータがあり、そのルータの

	コマンドまたはアクション	目的
		アップデートを受信する場合は、このコマンドを使用できます。
ステップ 12	**output-delay** *delay* 例： `Device(config)# output-delay 8`	（任意）送信する RIP アップデートにパケット間遅延を追加します。デフォルトでは、複数のパケットからなるRIPアップデートのパケットに、パケット間遅延が追加されません。パケットを低速なデバイスに送信する場合は、8～50 ミリ秒のパケット間遅延を追加できます。
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show ip protocols** 例： `Device# show ip protocols`	入力を確認します。
ステップ 15	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

RIP 認証の設定

RIP Version 1 は認証をサポートしていません。RIP バージョン 2 のパケットを送受信する場合は、インターフェイスでRIP認証をイネーブルにできます。インターフェイスで使用できる一連のキーは、キー チェーンによって指定されます。キー チェーンが設定されていないと、デフォルトの場合でも認証は実行されません。

RIP 認証がイネーブルであるインターフェイスでは、プレーン テキストと MD5 という 2 つの認証モードがデバイスでサポートされます。デフォルトはプレーン テキストです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ip rip authentication key-chain** *name-of-chain* 例： `Device(config-if)# ip rip authentication key-chain trees`	RIP 認証をイネーブルにします。
ステップ 5	**ip rip authentication mode {text | md5}** 例： `Device(config-if)# ip rip authentication mode md5`	プレーン テキスト認証（デフォルト）または MD5 ダイジェスト認証を使用するように、インターフェイスを設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

サマリー アドレスおよびスプリット ホライズンの設定

（注） ルートを適切にアドバタイズするため、アプリケーションがスプリット ホライズンをディセーブルにする必要がある場合を除き、通常はこの機能をディセーブルにしないでください。

ダイヤルアップ クライアント用のネットワーク アクセス サーバで、サマライズされたローカル IP アドレス プールをアドバタイズするように、RIP が動作しているインターフェイスを設定する場合は、**ip summary-address rip** インターフェイス コンフィギュレーション コマンドを使用します。

（注） スプリット ホライズンがイネーブルの場合、自動サマリーとインターフェイス IP サマリー アドレスはともにアドバタイズされません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイスコンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 10.1.1.10 255.255.255.0`	IP アドレスおよび IP サブネットを設定します。
ステップ 5	**ip summary-address rip ip address** *ip-network mask* 例：	サマライズする IP アドレスおよび IP ネットワーク マスクを設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip summary-address rip ip address 10.1.1.30 255.255.255.0`	
ステップ 6	**no ip split horizon** 例： `Device(config-if)# no ip split horizon`	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip interface** *interface-id* 例： `Device# show ip interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティング ループの発生を抑えるために、スプリット ホライズン メカニズムが使用されます。スプリット ホライズンは、ルートに関する情報の発信元であるインターフェイス上の、ルータによって、その情報がアドバタイズされないようにします。この機能を使用すると、複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。

（注） ルートを適切にアドバタイズするために、アプリケーションがスプリット ホライズンをディセーブルにする必要がある場合を除き、通常この機能をディセーブルにしないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイスコンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 10.1.1.10 255.255.255.0`	IP アドレスおよび IP サブネットを設定します。
ステップ 5	**no ip split-horizon** 例： `Device(config-if)# no ip split-horizon`	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip interface** *interface-id* 例： `Device# show ip interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

サマリーアドレスおよびスプリットホライズンの設定例

次の例では、主要ネットは 10.0.0.0 です。自動サマリー アドレス 10.0.0.0 はサマリー アドレス 10.2.0.0 によって上書きされるため、10.2.0.0 はインターフェイス ギガビット イーサネット ポート 2 からアドバタイズされますが、10.0.0.0 はアドバタイズされません。次の例では、インターフェイスがまだレイヤ 2 モード（デフォルト）の場合、**no switchport** インターフェイス コンフィギュレーション コマンドを入力してから、**ip address** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

（注） スプリット ホライズンがイネーブルである場合、（**ip summary-address rip** ルータ コンフィギュレーション コマンドによって設定される）自動サマリーとインターフェイス サマリー アドレスはともにアドバタイズされません。

```
Device(config)# router rip
Device(config-router)# interface gigabitethernet1/0/2
Device(config-if)# ip address 10.1.5.1 255.255.255.0
Device(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Device(config-if)# no ip split-horizon
Device(config-if)# exit
Device(config)# router rip
Device(config-router)# network 10.0.0.0
Device(config-router)# neighbor 2.2.2.2 peer-group mygroup
Device(config-router)# end
```

OSPF に関する情報

OSPF は IP ネットワーク専用の IGP で、IP サブネット化、および外部から取得したルーティング情報のタグ付けをサポートしています。OSPF を使用するとパケット認証も可能になり、パケットを送受信するときに IP マルチキャストが使用されます。シスコの実装では、RFC1253 の OSPF 管理情報ベース（MIB）がサポートされています。

（注） OSPF は IP ベースではサポートされません。

シスコの実装は、次の主要機能を含む OSPF バージョン 2 仕様に準拠します。

- スタブ エリアの定義がサポートされています。
- 任意の IP ルーティング プロトコルによって取得されたルートは、別の IP ルーティング プロトコルに再配信されます。つまり、ドメイン内レベルで、OSPF は EIGRP および RIP

によって取得したルートを取り込むことができます。OSPF ルートを RIP に伝達することもできます。

- エリア内の隣接ルータ間でのプレーン テキスト認証および MD5 認証がサポートされています。
- 設定可能なルーティング インターフェイス パラメータには、インターフェイス出力コスト、再送信インターバル、インターフェイス送信遅延、ルータ プライオリティ、ルータのデッド インターバルと hello インターバル、認証キーなどがあります。
- 仮想リンクがサポートされています。
- RFC 1587 に基づく Not-So-Stubby-Area（NSSA）がサポートされています。

通常、OSPF を使用するには、多くの内部ルータ、複数のエリアに接続された Area Border Router（ABR;エリア境界ルータ）、および自律システム境界ルータ（ASBR）間で調整する必要があります。最小設定では、すべてのデフォルトパラメータ値、エリアに割り当てられたインターフェイスが使用され、認証は行われません。環境をカスタマイズする場合は、すべてのルータの設定を調整する必要があります。

OSPF NSF

デバイスまたはスイッチ スタックは 2 つのレベルのノンストップ フォワーディング（NSF）をサポートしています。

- OSPF NSF 認識 （1848 ページ）
- OSPF NSF 対応 （1848 ページ）

OSPF NSF 認識

IP サービス フィーチャ セットは、OSPF NSF 認識を IPv4 に対してサポートしています。隣接ルータが NSF 対応である場合、レイヤ 3 デバイスでは、ルータに障害（クラッシュ）が発生してプライマリ ルート プロセッサ（RP）がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能をディセーブルにできません。

OSPF NSF 対応

IP サービス フィーチャ セットでは、前のリリースでサポートされていた OSPFv2 NSF Cisco フォーマットに加えて、OSPFv2 NSF IETF フォーマットもサポートされます。この機能の詳細については、『*NSF—OSPF (RFC 3623 OSPF Graceful Restart)*』を参照してください。

IP サービス フィーチャ セットは、OSPF NSF 対応ルーティングも IPv4 に対してサポートし、スタック マスター変更後のコンバージェンスの向上と、トラフィック損失の低減を実現します。OSPF NSF 対応スタックでスタック マスターの変更が生じた場合、新しいスタック マス

ターは自身のリンクステート データベースを OSPF ネイバーと再同期化するために、次の 2 つの処理をする必要があります。

- ネイバー関係をリセットせずにネットワーク上の使用可能な OSPF ネイバーを解放します。
- ネットワークのリンクステート データベースの内容を再取得します。

スタック マスターの変更後、新しいマスターは隣接する NSF 認識デバイスに OSPF NSF 信号を送信します。デバイスはこの信号を、スタックとのネイバー関係をリセットしない指示として認識します。NSF 対応スタック マスターは、ネットワーク上の他のルータから信号を受け取ると、自身のネイバー リストの再構築を開始します。

NSF 対応スタック マスターはネイバー関係を再確立すると、自身のデータベースを NSF 認識ネイバーと再同期化し、OSPF ネイバー間でルーティング情報を交換します。新しいスタック マスターはこのルーティング情報を使用して、新しい情報を基に古いルートの削除、ルーティング情報ベース（RIB）の更新、転送情報ベース（FIB）のアップデートを行います。これで OSPF プロトコルは完全に収束します。

（注） OSPF NSF では、すべてのネイバー ネットワーク デバイスが NSF 認識である必要があります。ネットワーク セグメント上に非 NSF 認識ネイバーが検出された場合、NSF 対応ルータはそのセグメントに対する NSF 機能をディセーブルにします。すべてのデバイスが NSF 認識または NSF 対応デバイスとなっているその他のネットワーク セグメントでは、NSF 対応機能が継続して提供されます。

OSPF NSF ルーティングをイネーブルにするには、**nsf** OSPF ルーティング コンフィギュレーション コマンドを使用します。OSPF NSF ルーティングがイネーブルになっていることを確認するには、**show ip ospf** 特権 EXEC コマンドを使用します。

詳細については、次の URL の『*Cisco Nonstop Forwarding*』を参照してください。
http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-nonstp_fwdg.html

OSPF エリア パラメータ

複数の OSPF エリア パラメータを設定することもできます。設定できるパラメータには、エリア、スタブ エリア、および NSSA への無許可アクセスをパスワードによって阻止する認証用パラメータがあります。スタブ エリアは、外部ルートの情報が送信されないエリアです。が、代わりに、自律システム（AS）外の宛先に対するデフォルトの外部ルートが、ABR によって生成されます。NSSA ではコアからそのエリアへ向かう LSA の一部がフラッディングされませんが、再配信することによって、エリア内の AS 外部ルートをインポートできます。

経路集約は、アドバタイズされたアドレスを、他のエリアでアドバタイズされる単一のサマリー ルートに統合することです。ネットワーク番号が連続する場合は、**area range** ルータ コンフィギュレーション コマンドを使用し、範囲内のすべてのネットワークを対象とするサマリー ルートをアドバタイズするように ABR を設定できます。

その他の OSPF パラメータ

ルータ コンフィギュレーション モードで、その他の OSPF パラメータを設定することもできます。

- ルート集約：他のプロトコルからルートを再配信すると、各ルートは外部 LSA 内で個別にアドバタイズされます。OSPF リンク ステート データベースのサイズを小さくするには、**summary-address** ルータ コンフィギュレーション コマンドを使用し、指定されたネットワーク アドレスおよびマスクに含まれる、再配信されたすべてのルートを単一のルータにアドバタイズします。
- 仮想リンク：OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンが不連続である場合に仮想リンクを確立するには、2 つの ABR を仮想リンクのエンドポイントとして設定します。設定情報には、他の仮想エンドポイント（他の ABR）の ID、および 2 つのルータに共通する非バックボーン リンク（通過エリア）などがあります。仮想リンクをスタブ エリアから設定できません。
- デフォルト ルート：OSPF ルーティング ドメイン内へのルート再配信を設定すると、ルータは自動的に自律システム境界ルータ（ASBR）になります。ASBR を設定し、強制的に OSPF ルーティング ドメインにデフォルト ルートを生成できます。
- すべての OSPF **show** 特権 EXEC コマンドで使用されるドメイン ネーム サーバ（DNS）名を使用すると、ルータ ID やネイバー ID を指定して表示する場合に比べ、ルータを簡単に特定できます。
- デフォルト メトリック：OSPF は、インターフェイスの帯域幅に従ってインターフェイスの OSPF メトリックを計算します。メトリックは、帯域幅で分割された *ref-bw* として計算されます。ここでの *ref* のデフォルト値は 10 で、帯域幅（*bw*）は **bandwidth** インターフェイス コンフィギュレーション コマンドによって指定されます。大きな帯域幅を持つ複数のリンクの場合は、大きな数値を指定し、これらのリンクのコストを区別できます。
- アドミニストレーティブ ディスタンスは、ルーティング情報送信元の信頼性を表す数値です。0 ～ 255 の整数を指定でき、値が大きいほど信頼性は低下します。アドミニストレーティブ ディスタンスが 255 の場合はルーティング情報の送信元をまったく信頼できないため、無視する必要があります。OSPF では、エリア内のルート（エリア内）、別のエリアへのルート（エリア間）、および再配信によって学習した別のルーティング ドメインからのルート（外部）の 3 つの異なるアドミニストレーティブ ディスタンスが使用されます。どのアドミニストレーティブ ディスタンスの値でも変更できます。
- 受動インターフェイス：イーサネット上の 2 つのデバイス間のインターフェイスは 1 つのネットワーク セグメントしか表しません。このため、OSPF が送信側インターフェイスに hello パケットを送信しないようにするには、送信側デバイスを受動インターフェイスに設定する必要があります。両方のデバイスは受信側インターフェイス宛ての hello パケットを使用することで、相互の識別を可能にします。
- ルート計算タイマー：OSPF がトポロジ変更を受信してから SPF 計算を開始するまでの遅延時間、および 2 つの SPF 計算の間のホールド タイムを設定できます。

- ネイバー変更ログ：OSPF ネイバー ステートが変更されたときに Syslog メッセージを送信するようにルータを設定し、ルータの変更を詳細に表示できます。

LSA グループ ペーシング

OSPF LSA グループ ペーシング機能を使用すると、OSPF LSA をグループ化し、リフレッシュ、チェックサム、エージング機能の同期を取って、ルータをより効率的に使用できるようになります。デフォルトでこの機能はイネーブルとなっています。デフォルトのペーシング インターバルは 4 分間です。通常は、このパラメータを変更する必要はありません。最適なグループ ペーシング インターバルは、ルータがリフレッシュ、チェックサム、エージングを行う LSA 数に反比例します。たとえば、データベース内に約 10000 個の LSA が格納されている場合は、ペーシング インターバルを短くすると便利です。小さなデータベース（40 ～ 100 LSA）を使用する場合は、ペーシング インターバルを長くし、10 ～ 20 分に設定してください。

ループバック インターフェイス

OSPF は、インターフェイスに設定されている最大の IP アドレスをルータ ID として使用します。このインターフェイスがダウンした場合、または削除された場合、OSPF プロセスは新しいルータ ID を再計算し、すべてのルーティング情報をそのルータのインターフェイスから再送信します。ループバック インターフェイスが IP アドレスによって設定されている場合、他のインターフェイスにより大きな IP アドレスがある場合でも、OSPF はこの IP アドレスをルータ ID として使用します。ループバック インターフェイスに障害は発生しないため、安定性は増大します。OSPF は他のインターフェイスよりもループバック インターフェイスを自動的に優先し、すべてのループバック インターフェイスの中で最大の IP アドレスを選択します。

OSPF の設定方法

OSPF のデフォルト設定

表 *110 : OSPF* のデフォルト設定

機能	デフォルト設定
インターフェイス パラメータ	コスト：1 再送信インターバル：5 秒 送信遅延：1 秒 プライオリティ：1 hello インターバル：10 秒 デッド インターバル：hello インターバルの 4 倍 認証なし パスワードの指定なし MD5 認証はディセーブル
エリア	認証タイプ：0（認証なし） デフォルト コスト：1 範囲：ディセーブル スタブ：スタブ エリアは未定義 NSSA：NSSA エリアは未定義
自動コスト	100 Mb/s
デフォルト情報送信元	ディセーブルイネーブルの場合、デフォルトのメトリック設定は10で、外部ルートタイプのデフォルトはタイプ 2 です。
デフォルト メトリック	各ルーティング プロトコルに適切な、組み込みの自動メトリック変換
距離 OSPF	dist1（エリア内のすべてのルート）：110。dist2（エリア間のすべてのルート）：110。および dist3（他のルーティング ドメインからのルート）：110。

機能	デフォルト設定
OSPF データベース フィルタ	ディセーブルすべての発信 LSA がインターフェイスにフラッディングされます。
IP OSPF 名検索	ディセーブル
隣接関係変更ログ	イネーブル
Neighbor	指定なし
ネイバー データベース フィルタ	ディセーブルすべての発信 LSA はネイバーにフラッディングされます。
ネットワーク エリア	ディセーブル
ノンストップ フォワーディング（NSF）認識	イネーブルレイヤ3スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
NSF 対応	ディセーブル （注） スイッチ スタックは OSPF NSF 対応ルーティングを IPv4 に対してサポートします。
ルータ ID	OSPF ルーティング プロセスは未定義
サマリー アドレス	ディセーブル
タイマー LSA グループのペーシング	240 秒
タイマー Shortest Path First（SPF）	spf 遅延：5 秒; spf ホールドタイム：10 秒
仮想リンク	エリア ID またはルータ ID は未定義 hello インターバル：10 秒 再送信インターバル：5 秒 送信遅延：1 秒 デッド インターバル：40 秒 認証キー：キーは未定義 メッセージダイジェスト キー（MD5）：キーは未定義

基本的な OSPF パラメータの設定

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、そのルーティング プロセスに関連付けられる IP アドレスの範囲を指定し、その範囲に関連付けられるエリア ID を割り当てます。IP サービス イメージを実行しているスイッチでは、Cisco OSPFv2 NSF フォーマットまたは IETF OSPFv2 NSF フォーマットのいずれかを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** process-id 例： `Device(config)# router ospf 15`	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。プロセス ID はローカルに割り当てられ、内部で使用される識別パラメータで、任意の正の整数を指定できます。各 OSPF ルーティング プロセスには一意の値があります。 （注） OSPF for Routed Access は、OSPFv2 インスタンスと OSPFv3 インスタンスをそれぞれ 1 つずつと、最大 200 のダイナミックに学習されるルートをサポートします。
ステップ 3	**nsf cisco** [**enforce global**] 例： `Device(config)# nsf cisco enforce global`	（任意）OSPF での Cisco NSF 動作をイネーブルにします。**enforce global** キーワードを指定すると、非 NSF 認識のネイバー ネットワーキング デバイスが検出されたときに NSF 再起動がキャンセルされます。 （注） ステップ 3 またはステップ 4 でコマンドを入力し、ステップ 5 に進みます。
ステップ 4	**nsf ietf** [**restart-interval** *seconds*] 例：	（任意）OSPF での IETF NSF 動作をイネーブルにします。**restart-interval** キーワードでは、グレースフル リスタート

	コマンドまたはアクション	目的
	`Device(config)# nsf ietf restart-interval 60`	間隔の長さを秒単位で指定します。範囲は 1 ～ 1800 です。デフォルトは 120 です。 （注） ステップ 3 またはステップ 4 でコマンドを入力し、ステップ 5 に進みます。
ステップ 5	**network** address wildcard-mask **area** area-id 例： `Device(config)# network 10.1.1.1 255.240.0.0 area 20`	OSPF が動作するインターフェイス、およびそのインターフェイスのエリア ID を定義します。単一のコマンドにワイルドカードマスクを指定し、特定の OSPF エリアに関連付けるインターフェイスを 1 つまたは複数定義できます。エリア ID には 10 進数または IP アドレスを指定できます。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip protocols** 例： `Device# show ip protocols`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF インターフェイスの設定

ip ospf インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイス固有の OSPF パラメータを変更できます。これらのパラメータを変更する必要はありませんが、一部のインターフェイスパラメータ（hello インターバル、デッドインターバル、認証キーなど）については、接続されたネットワーク内のすべてのルータで統一性を維持する必要があります。これらのパラメータを変更した場合は、ネットワーク内のすべてのルータの値も同様に変更してください。

（注） **ip ospf** インターフェイス コンフィギュレーション コマンドはすべてオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** interface-id 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip ospf** cost 例： `Device(config-if)# ip ospf 8`	（任意）インターフェイスでパケットを送信するコストを明示的に指定します。
ステップ 4	**ip ospf retransmit-interval** seconds 例： `Device(config-if)# ip ospf transmit-interval 10`	（任意）LSA 送信間隔を秒数で指定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 5 秒です。
ステップ 5	**ip ospf transmit-delay** seconds 例： `Device(config-if)# ip ospf transmit-delay 2`	（任意）リンク ステートアップデートパケットを送信するまでの予測待機時間を秒数で設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 1 秒です。
ステップ 6	**ip ospf priority** number 例： `Device(config-if)# ip ospf priority 5`	（任意）ネットワークに対して、OSPF で指定されたルータを検索するときに役立つプライオリティを設定します。有効な範囲は 0 ～ 255 です。デフォルトは 1 です。
ステップ 7	**ip ospf hello-interval** seconds 例： `Device(config-if)# ip ospf hello-interval 12`	（任意）OSPF インターフェイスで hello パケットの送信間隔を秒数で設定します。ネットワークのすべてのノードで同じ値を指定する必要があります。指

	コマンドまたはアクション	目的
		定できる範囲は 1 ～ 65535 秒です。デフォルトは 10 秒です。
ステップ 8	**ip ospf dead-interval** seconds 例： `Device(config-if)# ip ospf dead-interval 8`	（任意）最後のデバイスで hello パケットが確認されてから、OSPF ルータがダウンしていることがネイバーによって宣言されるまでの時間を秒数で設定します。ネットワークのすべてのノードで同じ値を指定する必要があります。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は hello インターバルの 4 倍です。
ステップ 9	**ip ospf authentication-key** キー 例： `Device(config-if)# ip ospf authentication-key password`	（任意）隣接 OSPF ルータで使用されるパスワードを割り当てます。パスワードには、キーボードから入力した任意の文字列（最大 8 バイト長）を指定できます。同じネットワーク上のすべての隣接ルータには、OSPF 情報を交換するため、同じパスワードを設定する必要があります。
ステップ 10	**ip ospf message digest-key** keyid **md5** key 例： `Device(config-if)# ip ospf message digest-key 16 md5 your1pass`	（任意）MDS 認証をイネーブルにします。 • *keyid*：1 ～ 255 の ID。 • *key*：最大 16 バイトの英数字パスワード
ステップ 11	**ip ospf database-filter all out** 例： `Device(config-if)# ip ospf database-filter all out`	（任意）インターフェイスへの OSPF LSA パケットのフラッディングを阻止します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show ip ospf interface** [*interface-name*] 例：	OSPF に関連するインターフェイス情報を表示します。

	コマンドまたはアクション	目的
	`Device# show ip ospf interface`	
ステップ 14	**show ip ospf neighbor detail** 例： `Device# show ip ospf neighbor detail`	ネイバー スイッチの NSF 認証ステータスを表示します。出力には、次のいずれかが表示されます。 • *Options is 0x52* *LLS Options is 0x1 (LR)* これらの行の両方が表示される場合、ネイバー スイッチが NSF 認識です。 • *Options is 0x42*：ネイバー スイッチが NSF 認識でないことを示します。
ステップ 15	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF エリア パラメータの設定

始める前に

（注） OSPF **area** ルータ コンフィギュレーション コマンドはすべて任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**router ospf** process-id 例： `Device(config)# router ospf 109`	OSPF ルーティングを有効にし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**area** *area-id***authentication** 例： `Device(config-router)# area 1 authentication`	（任意）特定のエリアへの無許可アクセスに対して、パスワードベースの保護を可能にします。ID には 10 進数または IP アドレスのいずれかを指定できます。
ステップ 4	**area** *area-id***authentication message-digest** 例： `Device(config-router)# area 1 authentication message-digest`	（任意）エリアに関して MD5 認証を有効にします。
ステップ 5	**area** *area-id***stub** [**no-summary**] 例： `Device(config-router)# area 1 stub`	（任意）エリアをスタブエリアとして定義します。**no-summary** キーワードを指定すると、ABR はサマリー リンク アドバタイズメントをスタブ エリアに送信できなくなります。
ステップ 6	**area** *area-id***nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**] 例： `Device(config-router)# area 1 nssa default-information-originate`	（任意）エリアを NSSA として定義します。同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。次のキーワードのいずれかを選択します。 • **no-redistribution**：ルータが NSSA ABR の場合、**redistribute** コマンドを使用して、ルートを NSSA エリアでなく通常のエリアに取り込む場合に使用します。 • **default-information-originate**：LSA タイプ 7 を NSSA に取り込めるようにする場合に、ABR で選択します。 • **no-redistribution**：サマリー LSA を NSSA に送信しない場合に選択します。
ステップ 7	**area** *area-id***range** *address mask* 例：	（任意）単一のルートをアドバタイズするアドレス範囲を指定します。この

	コマンドまたはアクション	目的
	`Device(config-router)# area 1 range 255.240.0.0`	コマンドは、ABR に対してだけ使用します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip ospf** [*process-id*] 例： `Device# show ip ospf`	設定を確認するため、一般的な OSPF ルーティングプロセスまたは特定のプロセス ID に関する情報を表示します。
ステップ 10	**show ip ospf** [*process-id* [*area-id*]] **database** 例： `Device# show ip osfp database`	特定のルータの OSPF データベースに関連する情報のリストを表示します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

その他の OSPF パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id* 例： `Device(config)# router ospf 10`	OSPF ルーティングを有効にし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**summary-address** *address mask* 例：	（任意）1 つのサマリー ルートだけがアドバタイズされるように、再配信さ

	コマンドまたはアクション	目的
	`Device(config)# summary-address 10.1.1.1 255.255.255.0`	れたルートのアドレスおよび IP サブネット マスクを指定します。
ステップ 4	**area** *area-id router-id* [*seconds*] [*seconds*] [] [[*key*] | *keyid* *key*] **authentication** **transmit-delay** **retransmit-interval** **authentication-key** **message-digest-key** **hello-interval** 5 例： `Device(config)# area 2 virtual-link 192.168.255.1 hello-interval 5`	（任意）仮想リンクを確立し、パラメータを設定します。
ステップ 5	**default-information originate** [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*] 例： `Device(config)# default-information originate metric 100 metric-type 1`	（任意）強制的に OSPF ルーティングドメインにデフォルトルートを生成するように ASBR を設定します。パラメータはすべて任意です。
ステップ 6	**ip ospf name-lookup** 例： `Device(config)# ip ospf name-lookup`	（任意）DNS名検索を設定します。デフォルトではディセーブルになっています。
ステップ 7	**ip auto-cost reference-bandwidth** *ref-bw* 例： `Device(config)# ip auto-cost reference-bandwidth 5`	（任意）単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8	**distance ospf** {[**inter-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]} 例： `Device(config)# distance ospf inter-area 150`	（任意）OSPF の距離の値を変更します。各タイプのルートのデフォルト距離は 110 です。指定できる範囲は 1 ～ 255 です。
ステップ 9	**passive-interface** *type number* 例： `Device(config)# passive-interface gigabitethernet 1/0/6`	（任意）指定されたインターフェイス経由の hello パケットの送信を抑制します。
ステップ 10	**timers throttle spf** *spf-delay spf-holdtime spf-wait* 例：	（任意）ルート計算タイマーを設定します。

	コマンドまたはアクション	目的
	`Device(config)# timers throttle spf 200 100 100`	• *spf-delay*：SPF 計算の変更を受信する間の遅延。指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-holdtime*：最初と 2 番目の SPF 計算の間の遅延。指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-wait*：SPF 計算の最大待機時間（ミリ秒）。指定できる範囲は 1 ～ 600000 ミリ秒です。
ステップ 11	**ospf log-adj-changes** 例： `Device(config)# ospf log-adj-changes`	（任意）ネイバーステートが変更されたとき、syslog メッセージを送信します。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show ip ospf** [*process-id* [*area-id*]] **database** 例： `Device# show ip ospf database`	特定のルータの OSPF データベースに関連する情報のリストを表示します。
ステップ 14	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

LSA グループ ペーシングの変更

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**router ospf** *process-id* 例： `Device(config)# router ospf 25`	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**timers lsa-group-pacing** *seconds* 例： `Device(config-router)# timers lsa-group-pacing 15`	LSA の グループ ペーシングを変更します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ループバック インターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface loopback 0** 例： `Device(config)# interface loopback 0`	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip address** address mask 例： `Device(config-if)# ip address 10.1.1.5 255.255.240.0`	このインターフェイスに IP アドレスを割り当てます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip interface** 例： `Device# show ip interface`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF の監視

IP ルーティング テーブルの内容、キャッシュの内容、およびデータベースの内容など、特定の統計情報を表示できます。

表 *111 : IP OSPF* 統計情報の表示コマンド

show ip ospf [*process-id*]	OSPF ルーティング プロセスに関する一般情報を表示します。

show ip ospf [*process-id*] **database** [**router**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**router**] [**self-originate**] **show ip ospf** [*process-id*] **database** [**router**] [**adv-router** [*ip-address*]] **show ip ospf** [*process-id*] **database** [**network**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**asbr-summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**external**] [*link-state-id*] **show ip ospf** [*process-id area-id*] **database** [**database-summary**]	OSPF データベースに関連する情報のリストを表示します。
show ip ospf border-routes	内部の OSPF ルーティング ABR および ASBR テーブル エントリを表示します。
show ip ospf interface [*interface-name*]	OSPF に関連するインターフェイス情報を表示します。
show ip ospf neighbor [*interface-name*] [*neighbor-id*] **detail**	OSPF インターフェイス ネイバー情報を表示します。
show ip ospf virtual-links	OSPF に関連する仮想リンク情報を表示します。

OSPF の設定例

例：基本的な OSPF パラメータの設定

次に、OSPF ルーティング プロセスを設定し、プロセス番号 109 を割り当てる例を示します。

```
Device(config)# router ospf 109
Device(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

EIGRP に関する情報

EIGRP は IGRP のシスコ独自の拡張バージョンです。EIGRP は IGRP と同じディスタンス ベクトル アルゴリズムおよび距離情報を使用しますが、EIGRP では収束性および動作効率が大幅に改善されています。

コンバージェンステクノロジーには、拡散更新アルゴリズム（DUAL）と呼ばれるアルゴリズムが採用されています。DUAL を使用すると、ルート計算の各段階でループが発生しなくなり、トポロジの変更に関連するすべてのデバイスを同時に同期できます。トポロジ変更の影響を受けないルータは、再計算に含まれません。

IP EIGRP を導入すると、ネットワークの幅が広がります。RIP の場合、ネットワークの最大幅は 15 ホップです。EIGRP メトリックは数千ホップをサポートするほど大きいため、ネットワークを拡張するときに問題となるのは、トランスポート レイヤのホップ カウンタだけです。IP パケットが 15 台のルータを経由し、宛先方向のネクスト ホップが EIGRP によって取得されている場合だけ、EIGRP は転送制御フィールドの値を増やします。RIP ルートを宛先へのネクスト ホップとして使用する場合、転送制御フィールドでは、通常どおり値が増加します。

EIGRP の機能

EIGRP には次の機能があります。

- 高速コンバージェンス
- 差分更新：宛先のステートが変更された場合、ルーティングテーブルの内容全体を送信する代わりに差分更新を行い、EIGRP パケットに必要な帯域幅を最小化します。
- 低い CPU 使用率：完全更新パケットを受信ごとに処理する必要がないため、CPU 使用率が低下します。
- プロトコルに依存しないネイバー探索メカニズム：このメカニズムを使用し隣接ルータに関する情報を取得します。
- 可変長サブネット マスク（VLSM）
- 任意のルート集約
- 大規模ネットワークへの対応

EIGRP コンポーネント

EIGRP には次に示す 4 つの基本コンポーネントがあります。

- ネイバー探索および回復：直接接続されたネットワーク上の他のルータに関する情報を動的に取得するために、ルータで使用されるプロセスです。また、ネイバーが到達不能または動作不能になっていることを検出するためにも使用されます。ネイバー探索および回復は、サイズの小さな hello パケットを定期的に送信することにより、わずかなオーバーヘッ

ドで実現されます。hello パケットが受信されているかぎり、Cisco ISO ソフトウェアは、ネイバーが有効に機能していると学習します。このように判別された場合、隣接ルータはルーティング情報を交換できます。

- Reliable Transport Protocol：EIGRP パケットをすべてのネイバーに確実に、順序どおりに配信します。マルチキャスト パケットとユニキャスト パケットが混在した伝送もサポートされます。EIGRP パケットには確実に送信する必要があるものと、そうでないものがあります。効率化のため、信頼性は必要時にのみ提供されます。たとえば、マルチキャスト機能があるマルチアクセスネットワーク（イーサネットなど）では、すべてのネイバーにそれぞれ hello パケットを確実に送信する必要はありません。そのため、EIGRP は、1 つのマルチキャスト hello を送信し、パケットに確認応答が必要ないという通知をそのパケットに含めます。他のタイプのパケット（アップデートなど）の場合は、確認応答（ACK パケット）を要求します。信頼性の高い伝送であれば、ペンディング中の未確認応答パケットがある場合、マルチキャストパケットを迅速に送信できます。このため、リンク速度が変化する場合でも、コンバージェンス時間を短く保つことができます。

- DUAL 有限状態マシンには、すべてのルート計算の決定プロセスが組み込まれており、すべてのネイバーによってアドバタイズされたすべてのルートが追跡されます。DUAL は距離情報（メトリックともいう）を使用して、効率的な、ループのないパスを選択し、さらに DUAL は適切な後継ルータに基づいて、ルーティング テーブルに挿入するルートを選択します。後継ルータは、宛先への最小コスト パス（ルーティング ループに関連しないことが保証されている）を持つ、パケット転送に使用される隣接ルータです。適切な後継ルータが存在しなくても、宛先にアドバタイズするネイバーが存在する場合は再計算が行われ、この結果、新しい後継ルータが決定されます。ルートの再計算に要する時間によって、コンバージェンス時間が変わります。再計算はプロセッサに負荷がかかるため、必要でない場合は、再計算しないようにしてください。トポロジが変更されると、DUAL はフィジブル サクセサの有無を調べます。適切なフィジブル サクセサが存在する場合は、それらを探して使用し、不要な再計算を回避します。

- プロトコル依存モジュールは、ネットワーク層プロトコル固有のタスクを実行します。たとえば、IP EIGRP モジュールは、IP でカプセル化された EIGRP パケットを送受信します。また、EIGRP パケットを解析したり、DUAL に受信した新しい情報を通知したりします。EIGRP は DUAL にルーティング決定を行うように要求しますが、結果は IP ルーティング テーブルに格納されます。EIGRP は、他の IP ルーティング プロトコルによって取得したルートの再配信も行います。

（注） EIGRP をイネーブルにするには、デバイスまたはスタック マスター上で IP サービス フィーチャ セットが稼働している必要があります。

EIGRP NSF

デバイススタックは、次の 2 つのレベルの EIGRP ノンストップ フォワーディングをサポートします。

- EIGRP NSF 認識
- EIGRP NSF 対応

EIGRP NSF 認識

IP サービス フィーチャ セットは、EIGRP NSF 認識を IPv4 に対してサポートしています。隣接ルータが NSF 対応である場合、レイヤ 3 デバイスでは、ルータに障害が発生してプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェアアップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能をディセーブルにできません。この機能の詳細については、『*Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*』の「EIGRP Nonstop Forwarding (NSF) Awareness」を参照してください。

EIGRP NSF 対応

IP サービス フィーチャ セットでは、EIGRP Cisco NSF ルーティングがサポートされています。それにより、コンバージェンスの時間が短くなり、スタック マスター変更後のトラフィック損失がなくなります。この NSF 機能の詳細については、『*High Availability Configuration Guide, Cisco IOS XE Release 3S*』の「Configuring Nonstop Forwarding」を参照してください。

IP サービス フィーチャ セットは、EIGRP NSF 対応ルーティングも IPv4 に対してサポートし、スタック マスター変更後のコンバージェンスの向上と、トラフィック損失の低減を実現します。EIGRP NSF 対応のスタック マスターが再起動したとき、または新しいスタック マスターが起動して NSF が再起動したとき、このデバイスにはネイバーが存在せず、トポロジ テーブルは空の状態です。デバイスは、デバイス スタックに対するトラフィックを中断することなく、インターフェイスの起動、ネイバーの再取得、およびトポロジ テーブルとルーティング テーブルの再構築を行う必要があります。EIGRP ピア ルータは新しいスタック マスターから学習したルートを維持し、NSF の再起動処理の間トラフィックの転送を継続します。

ネイバーによる隣接リセットを防ぐために、新しいスタック マスターは EIGRP パケット ヘッダーの新しい Restart（RS）ビットを使用して再起動を示します。これを受信したネイバーは、ピア リスト内のスタックと同期を取り、スタックとの隣接関係を維持します。続いてネイバーは、RS ビットがセットされているスタック マスターにトポロジ テーブルを送信して、自身が NSF 認識デバイスであることおよび新しいスタック マスターを補助していることを示します。

スタックのピア ネイバーの少なくとも 1 つが NFS 認識デバイスであれば、スタック マスターはアップデート情報を受信してデータベースを再構築します。各 NSF 認識ネイバーは、最後のアップデート パケットに End of Table（EOT）マーカーを付けて送信して、テーブル情報の最後であることを示します。スタック マスターは、EOT マーカーを受信したときにコンバージェンスを認識し、続いてアップデートの送信を始めます。スタック マスターがネイバーからすべての EOT マーカーを受信した場合、または NSF コンバージ タイマーが期限切れになった場合、EIGRP は RIB にコンバージェンスを通知し、すべての NSF 認識ピアにトポロジ テーブルをフラッディングします。

EIGRP スタブ ルーティング

EIGRP スタブ ルーティング機能は、すべてのフィーチャ セットで使用でき、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を低減させます。

（注） IP Base フィーチャ セットに含まれる EIGRP スタブ ルーティング機能では、ルーティング テーブルからの接続ルートまたはサマリー ルートをネットワーク内の他の デバイス にアドバタイズすることだけを行います。デバイスはアクセス レイヤで EIGRP スタブ ルーティングを使用することにより、ほかのタイプのルーティング アドバタイズメントの必要性を排除しています。拡張機能および完全な EIGRP ルーティングを使用するには、デバイス で IP ベース フィーチャ セットを稼働させる必要があります。IP ベース フィーチャ セットが稼働する デバイス上で、Multi-VRF-CE と EIGRP スタブ ルーティングを同時に設定しようとすると、設定は許可されません。IPv6 EIGRP スタブ ルーティングは、IP ベース フィーチャ セットではサポートされません。

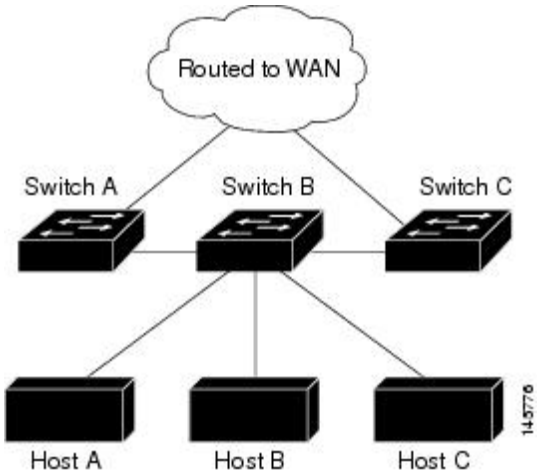
EIGRP スタブ ルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、EIGRP スタブ ルーティングを設定しているデバイス経由です。デバイスは、ユーザインターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRP スタブ ルーティングを使用しているときは、EIGRP を使用してデバイスだけをスタブとして設定するように、分散ルータおよびリモートルータを設定する必要があります。指定したルートだけがデバイスから伝播されます。デバイスは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブ ルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブ ルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。スタブ ルータは、ディストリビューション ルータを使用して適切なアップデートをすべてのピアに送信します。

次の図では、デバイス B は EIGRP スタブ ルータとして設定されています。デバイス A および C は残りの WAN に接続されています。デバイス B は、接続ルート、スタティック ルート、再配信ルート、およびサマリー ルートをデバイス A と C にアドバタイズします。デバイス B はデバイス A から学習したルートをアドバタイズしません（逆の場合も同様です）。

図 *99 : EIGRP* スタブ ルータ設定



EIGRP スタブ ルーティングの詳細については、『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols*』の「Configuring EIGRP Stub Routing」の項を参照してください。

EIGRP の設定方法

EIGRP ルーティング プロセスを作成するには、EIGRP をイネーブルにし、ネットワークを関連付ける必要があります。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイス ネットワークを指定しないと、どの EIGRP アップデートでもアドバタイズされません。

（注） ネットワーク上に IGRP 用に設定されているルータがあり、この設定を EIGRP に変更する場合は、IGRP と EIGRP の両方が設定された移行ルータを指定する必要があります。この場合は、この次の項に記載されているステップ 1 ～ 3 を実行し、さらに「スプリット ホライゾンの設定」も参照してください。ルートを自動的に再配信するには、同じ AS 番号を使用する必要があります。

EIGRP のデフォルト設定

表 *112 : EIGRP* のデフォルト設定

機能	デフォルト設定
自動サマリー	ディセーブル
デフォルト情報	再配信中は外部ルートが許可され、EIGRP プロセス間でデフォルト情報が渡されます。

機能	デフォルト設定
デフォルト メトリック	デフォルト メトリックなしで再配信できるのは、接続されたルートおよびインターフェイスのスタティック ルートだけです。デフォルト メトリックは次のとおりです。 • 帯域幅：0 以上の kb/s • 遅延（10 マイクロ秒）：0 または 39.1 ナノ秒の倍数である任意の正の数値 • 信頼性：0 ～ 255 の任意の数値（255 の場合は信頼性が 100%） • 負荷：0 ～ 255 の数値で表される有効帯域幅（255 の場合は 100% の負荷） • MTU：バイトで表されたルートの MTU サイズ（0 または任意の正の整数）
ディスタンス	内部距離：90 外部距離：170
EIGRP の隣接関係変更ログ	ディセーブル隣接関係の変更はロギングされません。
IP 認証キーチェーン	認証なし
IP 認証モード	認証なし
IP 帯域幅比率	50%
IP hello 間隔	低速非ブロードキャスト マルチアクセス（NBMA）ネットワークの場合：60 秒、それ以外のネットワークの場合：5 秒
IP ホールドタイム	低速 NBMA ネットワークの場合：180 秒、それ以外のネットワークの場合：15 秒
IP スプリットホライズン	イネーブル
IP サマリー アドレス	サマリー集約アドレスは未定義
メトリック重み	tos：0、k1 および k3：1、k2、k4、および k5：0
ネットワーク	指定なし

機能	デフォルト設定
ノンストップ フォワーディング（NSF）認識	IP サービス フィーチャ セットを実行するスイッチ上で IPv4 対してイネーブルになっています。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
NSF 対応	ディセーブル （注） デバイスは EIGRP NSF 対応ルーティングを IPv4 に対してサポートします。
オフセットリスト	ディセーブル
ルータ EIGRP	ディセーブル
メトリック設定	ルート マップにはメトリック設定なし
トラフィック共有	メトリックの比率に応じて配分
バリアンス	1（等コスト ロード バランシング）

基本的な EIGRP パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** autonomous-system 例： `Device(config)# router eigrp 10`	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。AS 番号によって他の EIGRP ルータへのルートを特定し、ルーティング情報をタグ付けします。
ステップ 3	**nsf** 例：	（任意）EIGRP NSF をイネーブルにします。スタック マスターおよびそのす

	コマンドまたはアクション	目的
	`Device(config)# nsf`	べてのピア上でこのコマンドを入力します。
ステップ 4	**network** network-number 例： `Device(config)# network 192.168.0.0`	ネットワークを EIGRP ルーティングプロセスに関連付けます。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。
ステップ 5	**eigrp log-neighbor-changes** 例： `Device(config)# eigrp log-neighbor-changes`	（任意）EIGRP 隣接関係変更のロギングをイネーブルにし、ルーティングシステムの安定性をモニタします。
ステップ 6	**metric weights** *tos k1 k2 k3 k4 k5* 例： `Device(config)# metric weights 0 2 0 2 0 0`	（任意）EIGRP メトリックを調整します。デフォルト値はほとんどのネットワークで適切に動作するよう入念に設定されていますが、調整することも可能です。 **注意** メトリックを設定する作業は複雑です。熟練したネットワーク設計者の指導がない場合は、行わないでください。
ステップ 7	**offset-list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*] 例： `Device(config)# offset-list 21 out 10`	（任意）オフセットリストをルーティング メトリックに適用し、EIGRP によって取得したルートへの着信および発信メトリックを増加します。アクセスリストまたはインターフェイスを使用し、オフセットリストを制限できます。
ステップ 8	**auto-summary** 例： `Device(config)# auto-summary`	（任意）ネットワークレベルルートへのサブネットルートの自動サマライズをイネーブルにします。
ステップ 9	**ip summary-address eigrp** *autonomous-system-number address mask* 例： `Device(config)# ip summary-address eigrp 1 192.168.0.0 255.255.0.0`	（任意）サマリー集約を設定します。

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show ip protocols** 例： `Device# show ip protocols`	入力を確認します。 NSF 認識の場合、出力に次のように表示されます。 *** IP Routing is NSF aware *** EIGRP NSF enabled
ステップ 12	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

EIGRP インターフェイスの設定

インターフェイスごとに、他の EIGRP パラメータを任意で設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip bandwidth-percent eigrp** *percent* 例： `Device(config-if)# ip bandwidth-percent eigrp 60`	（任意）インターフェイスで EIGRP が使用できる帯域幅の割合を設定します。デフォルト値は 50% です。

	コマンドまたはアクション	目的
ステップ 4	**ip summary-address eigrp** *autonomous-system-number address mask* 例： `Device(config-if)# ip summary-address eigrp 109 192.161.0.0 255.255.0.0`	（任意）指定されたインターフェイスのサマリー集約アドレスを設定します（auto-summary がイネーブルの場合は、通常設定する必要はありません）。
ステップ 5	**ip hello-interval eigrp** *autonomous-system-number seconds* 例： `Device(config-if)# ip hello-interval eigrp 109 10`	（任意）EIGRP ルーティング プロセスの hello タイム インターバルを変更します。指定できる範囲は 1 ～ 65535 秒です。低速 NBMA ネットワークの場合のデフォルト値は 60 秒、その他のすべてのネットワークでは 5 秒です。
ステップ 6	**ip hold-time eigrp** *autonomous-system-number seconds* 例： `Device(config-if)# ip hold-time eigrp 109 40`	（任意）EIGRP ルーティング プロセスのホールドタイムインターバルを変更します。指定できる範囲は 1 ～ 65535 秒です。低速 NBMA ネットワークの場合のデフォルト値は 180 秒、その他のすべてのネットワークでは 15 秒です。 **注意** ホールドタイムを調整する前に、シスコのテクニカルサポートにお問い合わせください。
ステップ 7	**no ip split-horizon eigrp** *autonomous-system-number* 例： `Device(config-if)# no ip split-horizon eigrp 109`	（任意）スプリットホライズンをディセーブルにし、ルート情報が情報元インターフェイスからルータによってアドバタイズされるようにします。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip eigrp interface** 例： `Device# show ip eigrp interface`	EIGRP がアクティブであるインターフェイス、およびそれらのインターフェイスに関連する EIGRP の情報を表示します。
ステップ 10	**copy running-config startup-config** 例：	（任意）コンフィギュレーションファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

EIGRP ルート認証の設定

EIGRP ルート認証を行うと、EIGRP ルーティング プロトコルからのルーティング アップデートに関する MD5 認証が可能になり、承認されていない送信元から無許可または問題のあるルーティング メッセージを受け取ることがなくなります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** interface-id 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip authentication mode eigrp** *autonomous-system***md5** 例： `Device(config-if)# ip authentication mode eigrp 104 md5`	IP EIGRP パケットの MD5 認証をイネーブルにします。
ステップ 4	**ip authentication key-chain eigrp** *autonomous-system key-chain* 例： `Device(config-if)# ip authentication key-chain eigrp 105 chain1`	IP EIGRP パケットの認証をイネーブルにします。
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**key chain** *name-of-chain* 例： `Device(config)# key chain chain1`	キーチェーンを識別し、キーチェーンコンフィギュレーションモードを開始します。ステップ 4 で設定した名前を指定します。
ステップ 7	**key** *number* 例： `Device(config-keychain)# key 1`	キーチェーンコンフィギュレーションモードで、キー番号を識別します。
ステップ 8	**key-string** *text* 例： `Device(config-keychain-key)# key-string key1`	キーチェーンコンフィギュレーションモードで、キーストリングを識別します。
ステップ 9	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} 例： `Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200`	（任意）キーを受信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 10	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} 例： `Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600`	（任意）キーを送信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 12	**show key chain** 例： `Device# show key chain`	認証キーの情報を表示します。
ステップ 13	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

EIGRP のモニタリングおよびメンテナンス

ネイバー テーブルからネイバーを削除できます。さらに、各種 EIGRP ルーティング統計情報を表示することもできます。下の図に、ネイバーを削除し、統計情報を表示する特権 EXEC コマンドを示します。表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

表 *113：IP EIGRP の clear および show コマンド*

clear ip eigrp neighbors [*if-address* | *interface*]	ネイバーテーブルからネイバーを削除します。
show ip eigrp interface [*interface*] [*as number*]	EIGRP に設定されているインターフェイスに関する情報を表示します。
show ip eigrp neighbors [*type-number*]	EIGRP によって検出されたネイバーを表示します。
show ip eigrp topology [*autonomous-system-number*] | [[*ip-address*] *mask*]]	指定されたプロセスの EIGRP トポロジテーブルを表示します。
show ip eigrp traffic [*autonomous-system-number*]	すべてまたは指定された EIGRP プロセスの送受信パケット数を表示します。

BGP に関する情報

ボーダー ゲートウェイ プロトコル（BGP）は、Exterior Gateway Protocol です。自律システム間で、ループの発生しないルーティング情報交換を保証するドメイン間ルーティング システムを設定するために使用されます。自律システムは、同じ管理下で動作して RIP や OSPF などの Interior Gateway Protocol（IGP）を境界内で実行し、Exterior Gateway Protocol（EGP）を使用して相互接続されるルータで構成されます。BGP バージョン 4 は、インターネット内でドメイン

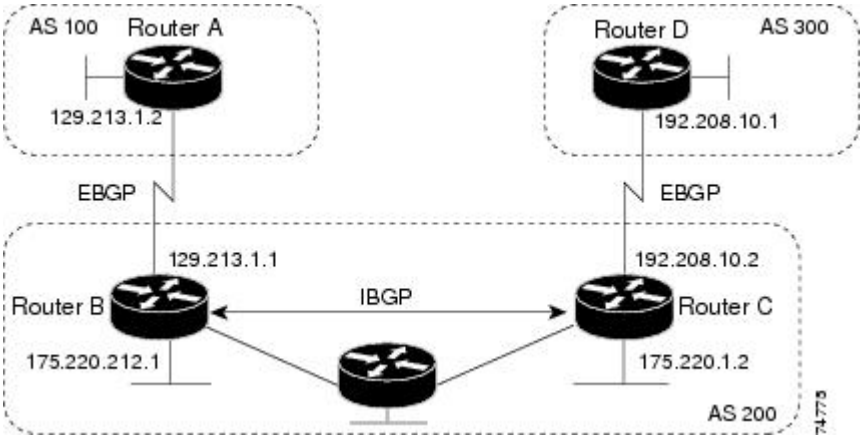
間ルーティングを行うための標準 EGP です。このプロトコルは、RFC 1163、1267、および 1771 で定義されています。BGP の詳細については、『*Internet Routing Architectures*』（Cisco Press 刊）、および『*Cisco IP and IP Routing Configuration Guide*』の「Configuring BGP」を参照してください。

BGP コマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』の「IP Routing Protocols」を参照してください。

BGP ネットワーク トポロジ

同じ自律システム（AS）に属し、BGP アップデートを交換するルータは内部BGP（IBGP）を実行し、異なる自律システムに属し、BGPアップデートを交換するルータは外部BGP（EBGP）を実行します。大部分のコンフィギュレーション コマンドは、EBGP と IBGP で同じですが、ルーティング アップデートが自律システム間で交換されるか（EBGP）、または AS 内で交換されるか（IBGP）という点で異なります。下の図に、EBGP と IBGP の両方を実行しているネットワークを示します。

図 *100 : EBGP*、*IBGP*、および複数の自律システム



外部 AS と情報を交換する前に、BGP は AS 内のルータ間で内部 BGP ピアリングを定義し、IGRP や OSPF など AS 内で稼働する IGP に BGP ルーティング情報を再配信して、AS 内のネットワークに到達することを確認します。

BGP ルーティング プロセスを実行するルータは、通常 BGP スピーカーと呼ばれます。BGP はトランスポート プロトコルとして伝送制御プロトコル（TCP）を使用します（特にポート 179）。ルーティング情報を交換するため相互に TCP 接続された 2 つの BGP スピーカーを、ピアまたはネイバーと呼びます。上の図では、ルータ A と B が BGP ピアで、ルータ B と C、ルータ C と D も同様です。ルーティング情報は、宛先ネットワークへの完全パスを示す一連の AS 番号です。BGP はこの情報を使用し、ループのない自律システム マップを作成します。

このネットワークの特徴は次のとおりです。

- ルータ A および B では EBGP が、ルータ B および C では IBGP が稼働しています。EBGP ピアは直接接続されていますが、IBGP ピアは直接接続されていないことに注意してくだ

さい。IGP が稼働し、2 つのネイバーが相互に到達するかぎり、IBGP ピアを直接接続する必要はありません。

- AS 内のすべての BGP スピーカーは、相互にピア関係を確立する必要があります。つまり、AS 内の BGP スピーカーは、論理的な完全メッシュ型に接続する必要があります。BGP4 は、論理的な完全メッシュに関する要求を軽減する 2 つの技術（連合およびルートリフレクタ）を提供します。
- AS 200 は AS 100 および AS 300 の中継 AS です。つまり、AS 200 は AS 100 と AS 300 間でパケットを転送するために使用されます。

BGP ピアは完全な BGP ルーティング テーブルを最初に交換し、差分更新だけを送信します。BGP ピアはキープアライブ メッセージ（接続が有効であることを確認）、および通知メッセージ（エラーまたは特殊条件に応答）を交換することもできます。

BGP の場合、各ルートはネットワーク番号、情報が通過した自律システムのリスト（自律システム パス）、および他のパス属性リストで構成されます。BGP システムの主な機能は、AS パスのリストに関する情報など、ネットワークの到達可能性情報を他の BGP システムと交換することです。この情報は、AS が接続されているかどうかを判別したり、ルーティング ループをプルーニングしたり、AS レベル ポリシー判断を行うために使用できます。

Cisco IOS が稼働しているルータまたはデバイスが IBGP ルートを選択または使用するのは、ネクストホップ ルータで使用可能なルートがあり、IGP から同期信号を受信している（IGP 同期がディセーブルの場合は除く）場合です。複数のルートが使用可能な場合、BGP は属性値に基づいてパスを選択します。BGP 属性については、「BGP 判断属性の設定」の項を参照してください。

BGP バージョン 4 ではクラスレス ドメイン間ルーティング（CIDR）がサポートされているため、集約ルートを作成してスーパーネットを構築し、ルーティング テーブルのサイズを削減できます。CIDR は、BGP 内部のネットワーク クラスの概念をエミュレートし、IP プレフィックスのアドバタイズをサポートします。

NSF 認識

BGP NSF 認識は、IP サービス フィーチャ セットで IPv4 に対してサポートされます。BGP ルーティングでこの機能をイネーブルにするには、グレースフル リスタートをイネーブルにする必要があります。隣接ルータが NSF 対応で、この機能がイネーブルである場合、レイヤ 3 デバイスでは、ルータに障害が発生してプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能の詳細については、『*Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*』の「BGP Nonstop Forwarding (NSF) Awareness」を参照してください。

BGP ルーティングに関する情報

BGP ルーティングをイネーブルにするには、BGP ルーティング プロセスを確立し、ローカルネットワークを定義します。BGP はネイバーとの関係を完全に認識する必要があるため、BGP ネイバーも指定する必要があります。

BGP は、内部および外部の 2 種類のネイバーをサポートします。内部ネイバーは同じ AS 内に、外部ネイバーは異なる AS 内にあります。通常の場合、外部ネイバーは相互に隣接し、1 つのサブネットを共有しますが、内部ネイバーは同じ AS 内の任意の場所に存在します。

スイッチではプライベート AS 番号を使用できます。プライベート AS 番号は通常サービス プロバイダーによって割り当てられ、ルートが外部ネイバーにアドバタイズされないシステムに設定されます。プライベート AS 番号の範囲は 64512 ～ 65535 です。AS パスからプライベート AS 番号を削除するように外部ネイバーを設定するには、**neighbor remove-private-as** ルータ コンフィギュレーション コマンドを使用します。この結果、外部ネイバーにアップデートを渡すとき、AS パス内にプライベート AS 番号が含まれている場合は、これらの番号が削除されます。

AS が別の AS からさらに別の AS にトラフィックを渡す場合は、アドバタイズ対象のルートに矛盾が存在しないことが重要です。BGP がルートをアドバタイズしてから、ネットワーク内のすべてのルータが IGP を通してルートを学習した場合、AS は一部のルータがルーティングできなかったトラフィックを受信することがあります。このような事態を避けるため、BGP は IGP が AS に情報を伝播し、BGP が IGP と同期化されるまで、待機する必要があります。同期化は、デフォルトでイネーブルに設定されています。AS が特定の AS から別の AS にトラフィックを渡さない場合、または自律システム内のすべてのルータで BGP が稼働している場合は、同期化をディセーブルにし、IGP 内で伝送されるルート数を少なくして、BGP がより短時間で収束するようにします。

ルーティング ポリシーの変更

ピアのルーティング ポリシーには、インバウンドまたはアウトバウンド ルーティング テーブル アップデートに影響する可能性があるすべての設定が含まれます。BGP ネイバーとして定義された 2 台のルータは、BGP 接続を形成し、ルーティング情報を交換します。このあとで BGP フィルタ、重量、距離、バージョン、またはタイマーを変更する場合、または同様の設定変更を行う場合は、BGP セッションをリセットし、設定の変更を有効にする必要があります。

リセットには、ハード リセットとソフト リセットの 2 種類があります。Cisco IOS Release 12.1 以降では、事前に設定を行わなくても、ソフト リセットを使用できます。事前設定なしにソフト リセットを使用するには、両方の BGP ピアでソフト ルート リフレッシュ機能がサポートされていなければなりません。この機能は、ピアによって TCP セッションが確立されたときに送信される OPEN メッセージに格納されてアドバタイズされます。ソフト リセットを使用すると、BGP ルータ間でルート リフレッシュ要求およびルーティング情報を動的に交換したり、それぞれのアウトバウンド ルーティング テーブルをあとで再アドバタイズできます。

- ソフト リセットによってネイバーからインバウンド アップデートが生成された場合、このリセットはダイナミック インバウンド ソフト リセットといいます。

- ソフト リセットによってネイバーに一連のアップデートが送信された場合、このリセットはアウトバウンド ソフト リセットといいます。

ソフト インバウンド リセットが発生すると、新規インバウンド ポリシーが有効になります。ソフトアウトバウンドリセットが発生すると、BGPセッションがリセットされずに、新規ローカル アウトバウンド ポリシーが有効になります。アウトバウンド ポリシーのリセット中に新しい一連のアップデートが送信されると、新規インバウンドポリシーも有効になる場合があります。

下の表に、ハード リセットとソフト リセットの利点および欠点を示します。

表 *114*：ハード リセットとソフト リセットの利点および欠点

リセット タイプ	利点	欠点
ハード リセット	メモリ オーバーヘッドが発生しません。	ネイバーから提供された BGP、IP、および FIB テーブルのプレフィックスが失われます。推奨しません。
発信ソフト リセット	ルーティング テーブル アップデートが設定、保管されません。	インバウンド ルーティング テーブル アップデートがリセットされません。
ダイナミック インバウンド ソフト リセット	BGP セッションおよびキャッシュがクリアされません。 ルーティング テーブル アップデートを保管する必要がなく、メモリ オーバーヘッドが発生しません。	両方の BGP ルータでルート リフレッシュ機能をサポートする必要があります（Cisco IOS Release 12.1 以降）。

BGP 判断属性

BGP スピーカーが複数の自律システムから受信したアップデートが、同じ宛先に対して異なるパスを示している場合、BGP スピーカーはその宛先に到達する最適パスを 1 つ選択する必要があります。選択されたパスは BGP ルーティング テーブルに格納され、ネイバーに伝播されます。この判断は、アップデートに格納されている属性値、および BGP で設定可能な他の要因に基づいて行われます。

BGP ピアはネイバー AS からプレフィックスに対する 2 つの EBGP パスを学習するとき、最適パスを選択して IP ルーティング テーブルに挿入します。BGP マルチパス サポートがイネーブルで、同じネイバー自律システムから複数の EBGP パスを学習する場合、単一の最適パスの代わりに、複数のパスが IP ルーティング テーブルに格納されます。そのあと、パケット スイッチング中に、複数のパス間でパケット単位または宛先単位のロードバランシングが実行されます。maximum-paths**maximum-paths** ルータ コンフィギュレーション コマンドは、許可されるパス数を制御します。

これらの要因により、BGP が最適パスを選択するために属性を評価する順序が決まります。

1. パスで指定されているネクストホップが到達不能な場合、このアップデートは削除されます。BGP ネクストホップ属性（ソフトウェアによって自動判別される）は、宛先に到達するために使用されるネクストホップの IP アドレスです。EBGP の場合、通常このアドレスは **neighbor remote-as router** ルータ コンフィギュレーション コマンドで指定されたネイバーの IP アドレスです。ネクストホップの処理をディセーブルにするには、ルート マップまたは **neighbor next-hop-self** ルータ コンフィギュレーション コマンドを使用します。

2. 最大の重みのパスを推奨します（シスコ独自のパラメータ）。ウェイト属性はルータにローカルであるため、ルーティング アップデートで伝播されません。デフォルトでは、ルータ送信元のパスに関するウェイト属性は 32768 で、それ以外のパスのウェイト属性は 0 です。最大の重みのルートを推奨します。重みを設定するには、アクセス リスト、ルート マップ、または **neighbor weight** ルータ コンフィギュレーション コマンドを使用します。

3. ローカル プリファレンス値が最大のルートを推奨します。ローカル プリファレンスはルーティング アップデートに含まれ、同じ AS 内のルータ間で交換されます。ローカル初期設定属性のデフォルト値は 100 です。ローカルプリファレンスを設定するには、**bgp default local-preference** ルータ コンフィギュレーション コマンドまたはルート マップを使用します。

4. ローカル ルータ上で稼働する BGP から送信されたルートを推奨します。

5. AS パスが最短のルートを推奨します。

6. 送信元タイプが最小のルートを推奨します。内部ルートまたは IGP は、EGP によって学習されたルートよりも小さく、EGP で学習されたルートは、未知の送信元のルートまたは別の方法で学習されたルートよりも小さくなります。

7. 想定されるすべてのルートについてネイバー AS が同じである場合は、MED メトリック属性が最小のルートを推奨します。MED を設定するには、ルート マップまたは **default-metric** ルータ コンフィギュレーション コマンドを使用します。IBGP ピアに送信されるアップデートには、MED が含まれます。

8. 内部（IBGP）パスより、外部（EBGP）パスを推奨します。

9. 最も近い IGP ネイバー（最小の IGP メトリック）を通って到達できるルートを推奨します。ルータは、AS 内の最短の内部パス（BGP のネクストホップへの最短パス）を使用し、宛先に到達するためです。

10. 次の条件にすべて該当する場合は、このパスのルートを IP ルーティング テーブルに挿入してください。

    最適ルートと目的のルートがともに外部ルートである

    最適ルートと目的のルートの両方が、同じネイバー自律システムからのルートである

    maximum-paths がイネーブルである

11. マルチパスがイネーブルでない場合は、BGP ルータ ID の IP アドレスが最小であるルートを推奨します。通常、ルータ ID はルータ上の最大の IP アドレスまたはループバック（仮想）アドレスですが、実装に依存することがあります。

ルート マップ

BGP 内でルート マップを使用すると、ルーティング情報を制御、変更したり、ルーティングドメイン間でルートを再配信する条件を定義できます。ルート マップの詳細については、「Using Route Maps to Redistribute Routing Information」の項を参照してください。各ルート マップには、ルート マップを識別する名前（マップ タグ）およびオプションのシーケンス番号が付いています。

BGP フィルタリング

BGP アドバタイズメントをフィルタリングするには、**as-path access-list** グローバル コンフィギュレーション コマンドや **neighbor filter-list** ルータ コンフィギュレーション コマンドなどの AS パス フィルタを使用します。**neighbor distribute-list** ルータ コンフィギュレーション コマンドとアクセス リストを併用することもできます。distribute-list フィルタはネットワーク番号に適用されます。**distribute-list** コマンドの詳細については、「ルーティング アップデートのアドバタイズおよび処理の制御」の項を参照してください。

ネイバー単位でルートマップを使用すると、アップデートをフィルタリングしたり、さまざまな属性を変更したりできます。ルート マップは、インバウンド アップデートまたはアウトバウンド アップデートのいずれかに適用できます。ルート マップを渡すルートだけが、アップデート内で送信または許可されます。着信および発信の両方のアップデートで、AS パス、コミュニティ、およびネットワーク番号に基づくマッチングがサポートされています。AS パスのマッチングには **match as-path access-list** ルート マップ コマンド、コミュニティに基づくマッチングには **match community-list** ルート マップ コマンド、ネットワークに基づくマッチングには **ip access-list** グローバル コンフィギュレーション コマンドが必要です。

BGP フィルタリングのプレフィックス リスト

neighbor distribute-list ルータ コンフィギュレーション コマンドを含む多数の BGP ルート フィルタリング コマンドでは、アクセス リストの代わりにプレフィックス リストを使用できます。プレフィックス リストを使用すると、大規模リストのロードおよび検索パフォーマンスが改善し、差分更新がサポートされ、コマンドライン インターフェイス（CLI）設定が簡素化され、柔軟性が増すなどの利点が生じます。

プレフィックス リストによるフィルタリングでは、アクセス リストの照合の場合と同様に、プレフィックス リストに記載されたプレフィックスとルートのプレフィックスが照合されます。一致すると、一致したルートが使用されます。プレフィックスが許可されるか、または拒否されるかは、次に示すルールに基づいて決定されます。

- 空のプレフィックス リストはすべてのプレフィックスを許可します。

- 特定のプレフィックスがプレフィックスリストのどのエントリとも一致しなかった場合、実質的に拒否されたものと見なされます。
- 指定されたプレフィックスと一致するエントリがプレフィックスリスト内に複数存在する場合は、シーケンス番号が最小であるプレフィックス リスト エントリが識別されます。

デフォルトでは、シーケンス番号は自動生成され、5 ずつ増分します。シーケンス番号の自動生成をディセーブルにした場合は、エントリごとにシーケンス番号を指定する必要があります。シーケンス番号を指定する場合の増分値に制限はありません。増分値が 1 の場合は、このリストに追加エントリを挿入できません。増分値が大きい場合は、値がなくなることがあります。

BGP コミュニティ フィルタリング

BGP コミュニティ フィルタリングは、COMMUNITIES 属性の値に基づいてルーティング情報の配信を制御する BGP の方法の 1 つです。この属性によって、宛先はコミュニティにグループ化され、コミュニティに基づいてルーティング判断が適用されます。この方法を使用すると、ルーティング情報の配信制御を目的とする BGP スピーカーの設定が簡単になります。

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。各宛先は複数のコミュニティに属します。AS 管理者は、宛先が属するコミュニティを定義できます。デフォルトでは、すべての宛先が一般的なインターネットコミュニティに属します。コミュニティは、過渡的でグローバルなオプションの属性である、COMMUNITIES 属性（1 ～ 4294967200 の数値）によって識別されます。事前に定義された既知のコミュニティの一部を、次に示します。

- **internet**：このルートをインターネットコミュニティにアドバタイズします。すべてのルータが所属します。
- **no-export**：EBGP ピアにこのルートをアドバタイズしません。
- **no-advertise**：どのピア（内部または外部）にもこのルートをアドバタイズしません。
- **local-as**：ローカルな AS 外部のピアにこのルートをアドバタイズしません。

コミュニティに基づき、他のネイバーに許可、送信、配信するルーティング情報を制御できます。BGP スピーカーは、ルートを学習、アドバタイズ、または再配信するときに、ルートのコミュニティを設定、追加、または変更します。ルートを集約すると、作成された集約内の COMMUNITIES 属性に、すべての初期ルートの全コミュニティが含まれます。

コミュニティ リストを使用すると、ルートマップの match 句で使用されるコミュニティ グループを作成できます。さらに、アクセス リストの場合と同様、一連のコミュニティ リストを作成することもできます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。

コミュニティに基づいて COMMUNITIES 属性および match 句を設定するには、「ルート マップによるルーティング情報の再配信」に記載されている **match community-list** および **set community** ルート マップ コンフィギュレーション コマンドを参照してください。

BGP ネイバーおよびピア グループ

通常、BGP ネイバーの多くは同じアップデート ポリシー（同じアウトバウンド ルート マップ、配信リスト、フィルタ リスト、アップデート送信元など）を使用して設定されます。アップデート ポリシーが同じネイバーをピア グループにまとめると設定が簡単になり、アップデートの効率が高まります。多数のピアを設定した場合は、この方法を推奨します。

BGP ピア グループを設定するには、ピア グループを作成し、そこにオプションを割り当てて、ピア グループ メンバーとしてネイバーを追加します。ピア グループを設定するには、**neighbor** ルータ コンフィギュレーション コマンドを使用します。デフォルトでは、ピア グループ メンバーは remote-as（設定されている場合）、version、update-source、out-route-map、out-filter-list、out-dist-list、minimum-advertisement-interval、next-hop-self など、ピア グループの設定オプションをすべて継承します。すべてのピア グループ メンバーは、ピア グループに対する変更を継承します。また、アウトバウンドアップデートに影響しないオプションを無効にするように、メンバーを設定することもできます。

集約ルート

クラスレス ドメイン間ルーティング（CIDR）を使用すると、集約ルート（またはスーパーネット）を作成して、ルーティング テーブルのサイズを最小化できます。BGP 内に集約ルートを設定するには、集約ルートを BGP に再配信するか、または BGP ルーティング テーブル内に集約エントリを作成します。BGP テーブル内に特定のエントリがさらに 1 つまたは複数存在する場合は、BGP テーブルに集約アドレスが追加されます。

ルーティング ドメイン コンフェデレーション

IBGP メッシュを削減する方法の 1 つは、自律システムを複数のサブ自律システムに分割して、単一の自律システムとして認識される単一の連合にグループ化することです。各自律システムは内部で完全にメッシュ化されていて、同じコンフェデレーション内の他の自律システムとの間には数本の接続があります。異なる自律システム内にあるピアでは EBGP セッションが使用されますが、ルーティング情報は IBGP ピアと同様な方法で交換されます。具体的には、ネクスト ホップ、MED、およびローカル プリファレンス情報は維持されます。すべての自律システムで単一の IGP を使用できます。

BGP ルート リフレクタ

BGP では、すべての IBGP スピーカーを完全メッシュ構造にする必要があります。外部ネイバーからルートを受信したルータは、そのルートをすべての内部ネイバーにアドバタイズする必要があります。ルーティング情報のループを防ぐには、すべての IBGP スピーカーを接続する必要があります。内部ネイバーは、内部ネイバーから学習されたルートを他の内部ネイバーに送信しません。

ルート リフレクタを使用すると、学習されたルートをネイバーに渡す場合に他の方法が使用されるため、すべての IBGP スピーカーを完全メッシュ構造にする必要はありません。IBGP ピアをルート リフレクタに設定すると、その IBGP ピアは IBGP によって学習されたルートを一

連のIBGPネイバーに送信するようになります。ルート リフレクタの内部ピアには、クライアント ピアと非クライアント ピア（AS内の他のすべてのルータ）の2つのグループがあります。ルート リフレクタは、これらの2つのグループ間でルートを反映させます。ルート リフレクタおよびクライアント ピアは、クラスタを形成します。非クライアント ピアは相互に完全メッシュ構造にする必要がありますが、クライアント ピアはその必要はありません。クラスタ内のクライアントは、そのクラスタ外のIBGPスピーカーと通信しません。

アドバタイズされたルートを受信したルートリフレクタは、ネイバーに応じて、次のいずれかのアクションを実行します。

- 外部BGPスピーカーからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズします。
- 非クライアント ピアからのルートをすべてのクライアントにアドバタイズします。
- クライアントからのルートをすべてのクライアントおよび非クライアントピアにアドバタイズします。したがって、クライアントを完全メッシュ構造にする必要はありません。

通常、クライアントのクラスタにはルート リフレクタが1つあり、クラスタはルート リフレクタのルータIDで識別されます。冗長性を高めて、シングル ポイントでの障害を回避するには、クラスタに複数のルートリフレクタを設定する必要があります。このように設定した場合は、ルート リフレクタが同じクラスタ内のルート リフレクタからのアップデートを認識できるように、クラスタ内のすべてのルート リフレクタに同じクラスタID（4バイト）を設定する必要があります。クラスタを処理するすべてのルートリフレクタは完全メッシュ構造にし、一連の同一なクライアント ピアおよび非クライアント ピアを設定する必要があります。

ルート ダンプニング

ルート フラップ ダンプニングは、インターネットワーク内でフラッピング ルートの伝播を最小化するためのBGP機能です。ルートの状態が使用可能、使用不可能、使用可能、使用不可能という具合に、繰り返し変化する場合、ルートはフラッピングと見なされます。ルートダンプニングがイネーブルの場合は、フラッピングしているルートにペナルティ値が割り当てられます。ルートの累積ペナルティが、設定された制限値に到達すると、ルートが稼働している場合であっても、BGPはルートのアドバタイズメントを抑制します。再使用限度は、ペナルティと比較される設定可能な値です。ペナルティが再使用限度より小さくなると、起動中の抑制されたルートのアドバタイズメントが再開されます。

IBGPによって取得されたルートには、ダンプニングが適用されません。このポリシーにより、IBGP ピアのペナルティがAS外部のルートよりも大きくなることはありません。

BGPの追加情報

BGP設定の詳しい説明については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Routing Protocols」にある「Configuring BGP」を参照してください。特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

BGP の設定方法

BGP のデフォルト設定

下の表に、BGP のデフォルト設定を示します。すべての特性の詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』の特定のコマンドを参照してください。

表 *115 : BGP* のデフォルト設定

機能	デフォルト設定
集約アドレス	ディセーブル：未定義
AS パス アクセス リスト	未定義
自動サマリー	ディセーブル
最適パス	• ルータはルートを選択する場合に *as-path* を考慮し、外部 BGP ピアからの類似ルートは比較しません。 • ルータ ID の比較：ディセーブル
BGP コミュニティ リスト	• 番号：未定義。コミュニティ番号を示す特定の値を許可すると、許可されていないその他すべてのコミュニティ番号は、暗黙の拒否にデフォルト設定されます。 • フォーマット：シスコデフォルト フォーマット（32 ビット番号）
BGP 連合 ID/ピア	• ID：未設定 • ピア：識別なし
BGP 高速外部フォールオーバー	イネーブル
BGP ローカル初期設定	100。指定できる範囲は 0～4294967295 です（大きな値を推奨）。
BGP ネットワーク	指定なし。バックドア ルートのアドバタイズなし

機能	デフォルト設定
BGP ルート ダンプニング	デフォルトでは、ディセーブルです。イネーブルの場合は、次のようになります。 • 半減期は 15 分 • 再使用は 750（10 秒増分） • 抑制は 2000（10 秒増分） • 最大抑制時間は半減期の 4 倍（60 分）
BGP ルータ ID	ループバック インターフェイスに IP アドレスが設定されている場合は、ループバック インターフェイスの IP アドレス、またはルータの物理インターフェイスに対して設定された最大の IP アドレス
デフォルトの情報送信元（プロトコルまたはネットワーク再配信）	ディセーブル
デフォルト メトリック	自動メトリック変換（組み込み）
ディスタンス	• 外部ルート アドミニストレーティブ ディスタンス：20（有効値は 1 ～ 255） • 内部ルート アドミニストレーティブ ディスタンス：200（有効値は 1 ～ 255） • ローカル ルート アドミニストレーティブ ディスタンス：200（有効値は 1 ～ 255）
ディストリビュート リスト	• 入力（アップデート中に受信されたネットワークをフィルタリング）：ディセーブル • 出力（アップデート中のネットワークのアドバタイズを抑制）：ディセーブル
内部ルート再配信	ディセーブル
IP プレフィックス リスト	未定義

機能	デフォルト設定
Multi Exit Discriminator（MED）	• 常に比較：ディセーブル。異なる自律システム内のネイバーからのパスに対して、MED を比較しません。 • 最適パスの比較：ディセーブル • 最悪パスである MED の除外：ディセーブル • 決定的な MED 比較：ディセーブル

機能	デフォルト設定
Neighbor	

機能	デフォルト設定
	• アドバタイズメント インターバル：外部ピアの場合は 30 秒、内部ピアの場合は 5 秒 • ロギング変更：イネーブル • 条件付きアドバタイズ：ディセーブル • デフォルト送信元：ネイバーに送信されるデフォルト ルートはなし • 説明：なし • ディストリビュート リスト：未定義 • 外部 BGP マルチホップ：直接接続されたネイバーだけを許可 • フィルタ リスト：使用しない • 受信したプレフィックスの最大数：制限なし • ネクスト ホップ（BGP ネイバーのネクスト ホップとなるルータ）：ディセーブル • パスワード：ディセーブル • ピア グループ：定義なし、割り当てメンバーなし • プレフィックス リスト：指定なし • リモート AS（ネイバー BGP テーブルへのエントリ追加）：ピア定義なし • プライベート AS 番号の削除：ディセーブル • ルート マップ：ピアへの適用なし • コミュニティ属性送信：ネイバーへの送信なし。 • シャットダウンまたはソフト再設定：ディセーブル • タイマー：60 秒、ホールドタイム：180 秒 • アップデート送信元：最適ローカル アドレス

機能	デフォルト設定
	• バージョン：BGP バージョン 4 • 重み：BGP ピアによって学習されたルート：0、ローカル ルータから取得されたルート：32768
NSF[6] 認識	ディセーブル状態の [7]。イネーブル状態の場合、レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
ルート リフレクタ	未設定
同期化（BGP および IGP）	ディセーブル
テーブル マップ アップデート	ディセーブル
タイマー	キープアライブ：60 秒、ホールドタイム：180 秒

[6] Nonstop Forwarding
[7] NSF 認識は、グレースフル リスタートをイネーブルにすることにより、IP サービス フィーチャ セットを実行するスイッチ上で IPv4 に対してイネーブルにできます

BGP ルーティングのイネーブル化

始める前に

（注） BGP をイネーブルにするには、スイッチまたはスタック マスター上で IP サービス フィーチャ セットが稼働している必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ip routing** 例： `Device(config)# ip routing`	IP ルーティングをイネーブルにします。
ステップ 3	**router bgp** *autonomous-system* 例： `Device(config)# router bgp 45000`	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータコンフィギュレーションモードを開始します。指定できる AS 番号は 1～65535 です。64512～65535 は、プライベート AS 番号専用です。
ステップ 4	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] 例： `Device(config)# network 10.108.0.0`	この AS に対してローカルとなるようにネットワークを設定し、BGP テーブルにネットワークを格納します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number* 例： `Device(config)# neighbor 10.108.1.2 remote-as 65200`	BGP ネイバー テーブルに設定を追加し、IP アドレスによって識別されるネイバーが、指定された AS に属することを示します。 EBGP の場合、通常ネイバーは直接接続されており、IP アドレスは接続のもう一方の端におけるインターフェイスのアドレスです。 IBGP の場合、IP アドレスにはルータインターフェイス内の任意のアドレスを指定できます。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remove-private-as** 例： `Device(config)# neighbor 172.16.2.33 remove-private-as`	（任意）発信ルーティング アップデート内の AS パスからプライベート AS 番号を削除します。
ステップ 7	**synchronization** 例： `Device(config)# synchronization`	（任意）BGP と IGP の同期化をイネーブルにします。
ステップ 8	**auto-summary** 例：	（任意）自動ネットワーク サマライズをイネーブルにします。IGP から BGP

	コマンドまたはアクション	目的
	`Device(config)# auto-summary`	にサブネットが再配信された場合、ネットワーク ルートだけが BGP テーブルに挿入されます。
ステップ 9	**bgp graceful-restart** 例： `Device(config)# bgp graceful-start`	（任意）NSF 認識をスイッチでイネーブルにします。NSF 認識はデフォルトではディセーブルです。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show ip bgp network** *network-number* 例： `Device# show ip bgp network 10.108.0.0`	設定を確認します。
ステップ 12	**show ip bgp neighbor** 例： `Device# show ip bgp neighbor`	NSF 認識（グレースフル リスタート）がネイバーでイネーブルにされていることを確認します。 スイッチおよびネイバーで NSF 認識がイネーブルである場合は、次のメッセージが表示されます。 グレースフル リスタート機能: アドバタイズおよび受信される スイッチで NSF 認識がイネーブルであり、ネイバーでディセーブルである場合は、次のメッセージが表示されます。 グレースフル リスタート機能: アドバタイズされる
ステップ 13	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング ポリシー変更の管理

BGP ピアがルート リフレッシュ機能をサポートするかどうかを学習して、BGP セッションをリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show ip bgp neighbors** 例： `Device# show ip bgp neighbors`	ネイバーがルート リフレッシュ機能をサポートするかどうかを表示します。サポートされている場合は、ルータに関する次のメッセージが表示されます。 *Received route refresh capability from peer*
ステップ 2	**clear ip bgp** {* | *address* | *peer-group-name*} 例： `Device# clear ip bgp *`	指定された接続上でルーティング テーブルをリセットします。 • すべての接続をリセットする場合は、アスタリスク（*）を入力します。 • 特定の接続をリセットする場合は、IP アドレスを入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 3	**clear ip bgp** {* | *address* | *peer-group-name*} **soft out** 例： `Device# clear ip bgp * soft out`	（任意）指定された接続上でインバウンド ルーティング テーブルをリセットするには、アウトバウンド ソフト リセットを実行します。このコマンドは、ルート リフレッシュがサポートされている場合に使用してください。 • すべての接続をリセットする場合は、アスタリスク（*）を入力します。 • 特定の接続をリセットする場合は、IP アドレスを入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。

	コマンドまたはアクション	目的
ステップ 4	**show ip bgp** 例： `Device# show ip bgp`	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 5	**show ip bgp neighbors** 例： `Device# show ip bgp neighbors`	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。

BGP 判断属性の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system* 例： `Device(config)# router bgp 4500`	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp best-path as-path ignore** 例： `Device(config-router)# bgp bestpath as-path ignore`	（任意）ルート選択中に AS パス長を無視するようにルータを設定します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self** 例： `Device(config-router)# neighbor 10.108.1.1 next-hop-self`	（任意）ネクストホップ アドレスの代わりに使用される特定の IP アドレスを入力し、ネイバーへの BGP アップデートに関するネクストホップの処理をディセーブルにします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **weight** *weight* 例： `Device(config-router)# neighbor 172.16.12.1 weight 50`	（任意）ネイバー接続に重みを割り当てます。指定できる値は 0 ～ 65535 です。最大の重みのルートを推奨します。別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ロー

	コマンドまたはアクション	目的
		カルルータから送信されたルートのデフォルトの重みは 32768 です。
ステップ 6	**default-metric** *number* 例： `Device(config-router)# default-metric 300`	（任意）推奨パスを外部ネイバーに設定するように MED メトリックを設定します。MED を持たないすべてのルータも、この値に設定されます。指定できる範囲は 1 ～ 4294967295 です。最小値を推奨します。
ステップ 7	**bgp bestpath med missing-as-worst** 例： `Device(config-router)# bgp bestpath med missing-as-worst`	（任意）MED がない場合は無限の値が指定されていると見なし、MED 値を持たないパスが最も望ましくないパスになるように、スイッチを設定します。
ステップ 8	**bgp always-compare med** 例： `Device(config-router)# bgp always-compare-med`	（任意）異なる AS 内のネイバーからのパスに対して、MED を比較するようにスイッチを設定します。デフォルトでは、MED は同じ AS 内のパス間でだけ比較されます。
ステップ 9	**bgp bestpath med confed** 例： `Device(config-router)# bgp bestpath med confed`	（任意）連合内の異なるサブ AS によってアドバタイズされたパスから特定のパスを選択する場合に、MED を考慮するようにスイッチを設定します。
ステップ 10	**bgp deterministic med** 例： `Device(config-router)# bgp deterministic med`	（任意）同じ AS 内の異なるピアによってアドバタイズされたルートから選択する場合に、MED 変数を考慮するようにスイッチを設定します。
ステップ 11	**bgp default local-preference** *value* 例： `Device(config-router)# bgp default local-preference 200`	（任意）デフォルトのローカル プリファレンス値を変更します。指定できる範囲は 0 ～ 4294967295 で、デフォルト値は 100 です。最大のローカル プリファレンス値を推奨します。
ステップ 12	**maximum-paths** *number* 例： `Device(config-router)# maximum-paths 8`	（任意）IP ルーティングテーブルに追加するパスの数を設定します。デフォルトでは、最適パスだけがルーティングテーブルに追加されます。指定できる範囲は 1 ～ 16 です。複数の値を指定すると、パス間のロードバランシングが可能になります。スイッチ ソフト

	コマンドまたはアクション	目的
		ウェア では最大 32 の等コスト ルートが許可されていますが、スイッチハードウェアはルートあたり 17 パス以上は使用しません。
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show ip bgp** 例： `Device# show ip bgp`	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 15	**show ip bgp neighbors** 例： `Device# show ip bgp neighbors`	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 16	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ルート マップによる BGP フィルタリングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map set-peer-address permit 10`	ルート マップを作成し、ルート マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**set ip next-hop** *ip-address* [*...ip-address*] [**peer-address**] 例： `Device(config)# set ip next-hop 10.1.1.3`	（任意）ネクストホップ処理をディセーブルにするようにルート マップを設定します。 • インバウンド ルート マップの場合は、一致するルートのネクストホップをネイバー ピア アドレスに設定し、サードパーティのネクストホップを上書きします。 • BGP ピアのアウトバウンド ルート マップの場合は、ネクスト ホップをローカル ルータのピア アドレスに設定して、ネクスト ホップ計算をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show route-map** [*map-name*] 例： `Device# show route-map`	設定を確認するため、設定されたすべてのルートマップ、または指定されたルート マップだけを表示します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ネイバーによる BGP フィルタリングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**router bgp** *autonomous-system* 例： `Device(config)# router bgp 109`	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** {*ip-address* | *peer-group name*} **distribute-list**{**access-list-number** | *name*} {**in** | **out**} 例： `Device(config-router)# neighbor 172.16.4.1 distribute-list 39 in`	（任意）アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。 （注） **neighbor prefix-list** ルータ コンフィギュレーション コマンドを使用して、アップデートをフィルタリングすることもできますが、両方のコマンドを使用して同じ BGP ピアを設定することはできません。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **route-map** *map-tag* {**in** | **out**} 例： `Device(config-router)# neighbor 172.16.70.24 route-map internal-map in`	（任意）ルート マップを適用し、着信または発信ルートをフィルタリングします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors** 例： `Device# show ip bgp neighbors`	設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス リストおよびネイバーによる BGP フィルタリングの設定

BGP 自律システム パスに基づいて着信および発信の両方のアップデートにアクセス リスト フィルタを指定して、フィルタリングすることもできます。各フィルタは、正規表現を使用するアクセス リストです。（正規表現の作成方法については、『*Cisco IOS Dial Technologies Command Reference, Release 12.4*』の付録「Regular Expressions」を参照してください）。この方法を使用するには、自律システム パスのアクセス リストを定義し、特定のネイバーとの間のアップデートに適用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip as-path access-list** *access-list-number* {**permit** | **deny**} *as-regular-expressions* 例： `Device(config)# ip as-path access-list 1 deny _65535_`	BGP-related アクセス リストを定義します。
ステップ 3	**router bgp** *autonomous-system* 例： `Device(config)# router bgp 110`	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **filter-list** {*access-list-number* | *name*} {**in** | **out** | **weight** *weight*} 例： `Device(config-router)# neighbor 172.16.1.1 filter-list 1 out`	アクセス リストに基づいて、BGP フィルタを確立します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors** [**paths** *regular-expression*] 例：	設定を確認します。

	コマンドまたはアクション	目的
	`Device# show ip bgp neighbors`	
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP フィルタリング用のプレフィックス リストの設定

コンフィギュレーションエントリを削除する場合は、シーケンス番号を指定する必要はありません。**Show** コマンドの出力には、シーケンス番号が含まれます。

コマンド内でプレフィックス リストを使用する場合は、あらかじめプレフィックス リストを設定しておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip prefix-list** *list-name* [**seq** *seq-value*] **deny** | **permit** *network/len* [**ge** *ge-value*] [**le** *le-value*] 例： `Device(config)# ip prefix-list BLUE permit 172.16.1.0/24`	一致条件に合わせてアクセスを拒否（**deny**）または許可（**permit**）するプレフィックス リストを作成します。シーケンス番号を指定することもできます。少なくとも 1 つの **permit** コマンドまたは **deny** コマンドを入力する必要があります。 • *network/len* は、ネットワーク番号およびネットワーク マスクの長さ（ビット単位）です。 • （任意）**ge** および **le** の値は、照合するプレフィックス長の範囲を指定します。指定された *ge-value* および *le-value* は、次の条件を満たす必要があります。*len* < *ge-value* < *le-value*< 32

	コマンドまたはアクション	目的
ステップ 3	**ip prefix-list** *list-name* **seq** *seq-value* **deny** | **permit** *network/len* [**ge** *ge-value*] [**le** *le-value*] 例： `Device(config)# ip prefix-list BLUE seq 10 permit 172.24.1.0/24`	（任意）プレフィックス リストにエントリを追加し、そのエントリにシーケンス番号を割り当てます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip prefix list** [**detail** | **summary**] *name* [*network/len*] [**seq** *seq-num*] [**longer**] [**first-match**] 例： `Device# show ip prefix list summary test`	プレフィックスリストまたはプレフィックス リスト エントリに関する情報を表示して、設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP コミュニティ フィルタリングの設定

デフォルトでは、COMMUNITIES 属性はネイバーに送信されません。COMMUNITIES 属性が特定の IP アドレスのネイバーに送信されるように指定するには、**neighbor send-community** ルータ コンフィギュレーション コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ip community-list** *community-list-number* {**permit** | **deny**} *community-number* 例： `Device(config)# ip community-list 1 permit 50000:10`	コミュニティリストを作成し、番号を割り当てます。 • *community-list-number* は 1 ～ 99 の整数です。この値は、コミュニティの 1 つ以上の許可または拒否グループを識別します。 • *community-number* は、**set community** ルートマップ コンフィギュレーション コマンドで設定される番号です。
ステップ 3	**router bgp** *autonomous-system* 例： `Device(config)# router bgp 108`	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **send-community** 例： `Device(config-router)# neighbor 172.16.70.23 send-community`	この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 5	**set comm-list** *list-num***delete** 例： `Device(config-router)# set comm-list 500 delete`	（任意）ルートマップで指定された標準または拡張コミュニティリストと一致する着信または発信アップデートのコミュニティ属性から、コミュニティを削除します。
ステップ 6	**exit** 例： `Device(config-router)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip bgp-community new-format** 例： `Device(config)# ip bgp-community new format`	（任意）AA:NN の形式で、BGP コミュニティを表示、解析します。 BGP コミュニティは、2 つの部分からなる 2 バイト長形式で表示されます。シスコのデフォルトのコミュニティ形式は、NNAA です。BGP に関する最新の RFC では、コミュニティは AA:NN の形式をとります。最初の部分は AS

	コマンドまたはアクション	目的
		番号で、その次の部分は 2 バイトの数値です。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp community** 例： `Device# show ip bgp community`	設定を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

BGP ネイバーおよびピア グループの設定

各ネイバーに設定オプションを割り当てるには、ネイバーの IP アドレスを使用し、次に示すルータ コンフィギュレーション コマンドのいずれかを指定します。ピア グループにオプションを割り当てるには、ピア グループ名を使用し、いずれかのコマンドを指定します。**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用すると、すべての設定情報を削除せずに、BGP ピアまたはピア グループをディセーブルにできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** *peer-group-name***peer-group**	BGP ピア グループを作成します。
ステップ 4	**neighbor** *ip-address***peer-group** *peer-group-name*	BGP ネイバーをピア グループのメンバにします。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*	BGP ネイバーを指定します。**remote-as** *number* を使用してピア グループが設定されていない場合は、このコマンドを使用し、EBGP ネイバーを含むピア グループを作成します。指定できる範囲は 1 ～ 65535 です。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **description** *text*	（任意）ネイバーに説明を関連付けます。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]	（任意）BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface*	（任意）内部 BGP セッションに、TCP 接続に関するすべての操作インターフェイスの使用を許可します。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop**	（任意）ネイバーがセグメントに直接接続されていない場合でも、BGP セッションを使用可能にします。マルチホップ ピア アドレスへの唯一のルートがデフォルト ルート（0.0.0.0）の場合、マルチホップ セッションは確立されません。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **local-as** *number*	（任意）ローカル AS として使用する AS 番号を指定します。指定できる範囲は 1 ～ 65535 です。
ステップ 12	**neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*	（任意）BGP ルーティング アップデートを送信する最小インターバルを設定します。
ステップ 13	**neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*]	（任意）ネイバーから受信できるプレフィックス数を制御します。指定できる範囲は 1 ～ 4294967295 です。*threshold*（任意）は、警告メッセージが生成される基準となる最大値（パー

	コマンドまたはアクション	目的
		センテージ）です。デフォルトは 75% です。
ステップ 14	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	（任意）ネイバー宛ての BGP アップデートに関して、ネクストホップでの処理をディセーブルにします。
ステップ 15	neighbor {*ip-address* | *peer-group-name*} password *string*	（任意）TCP 接続での MD5 認証を BGP ピアに設定します。両方の BGP ピアに同じパスワードを設定する必要があります。そうしないと、BGP ピア間に接続が作成されません。
ステップ 16	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}	（任意）着信または発信ルートにルート マップを適用します。
ステップ 17	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 18	**neighbor** {*ip-address* | *peer-group-name*} **timers** *keepalive holdtime*	（任意）ネイバーまたはピア グループ用のタイマーを設定します。 • *keepalive* インターバルは、キープアライブ メッセージがピアに送信される間隔です。指定できる範囲は 1 ～ 4294967295 秒です。デフォルト値は 60 秒です。 • *holdtime* は、キープアライブ メッセージを受信しなかった場合、ピアが非アクティブと宣言されるまでのインターバルです。指定できる範囲は 1 ～ 4294967295 秒です。デフォルト値は 180 秒です。
ステップ 19	**neighbor** {*ip-address* | *peer-group-name*} **weight** *weight*	（任意）ネイバーからのすべてのルートに関する重みを指定します。
ステップ 20	**neighbor** {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *name*} {**in** | **out**}	（任意）アクセスリストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。
ステップ 21	**neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out** | **weight** *weight*}	（任意）BGP フィルタを確立します。

	コマンドまたはアクション	目的
ステップ 22	**neighbor** {*ip-address* | *peer-group-name*} **version** *value*	（任意）ネイバーと通信するときに使用するBGPバージョンを指定します。
ステップ 23	**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**	（任意）受信したアップデートのストアを開始するようにソフトウェアを設定します。
ステップ 24	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 25	**show ip bgp neighbors**	設定を確認します。
ステップ 26	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ルーティング テーブルでの集約アドレスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system* 例： `Device(config)# router bgp 106`	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**aggregate-address** *address mask* 例： `Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0`	BGPルーティングテーブル内に集約エントリを作成します。集約ルートはASからのルートとしてアドバタイズされます。情報が失われた可能性があることを示すため、アトミック集約属性が設定されます。

	コマンドまたはアクション	目的
ステップ 4	**aggregate-address** *address mask***as-set** 例： `Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set`	（任意）AS 設定パス情報を生成します。このコマンドは、この前のコマンドと同じルールに従う集約エントリを作成します。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET です。多くのパスを集約するときは、このキーワードを使用しないでください。このルートは絶えず取り消され、アップデートされます。
ステップ 5	**aggregate-address** *address-mask***summary-only** 例： `Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only`	（任意）サマリーアドレスだけをアドバタイズします。
ステップ 6	**aggregate-address** *address mask***suppress-map** *map-name* 例： `Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0 suppress-map map1`	（任意）選択された、より具体的なルートを抑制します。
ステップ 7	**aggregate-address** *address mask***advertise-map** *map-name* 例： `Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0 advertise-map map2`	（任意）ルートマップによって指定された設定に基づいて集約を生成します。
ステップ 8	**aggregate-address** *address mask***attribute-map** *map-name* 例： `Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0 attribute-map map3`	（任意）ルートマップで指定された属性を持つ集約を生成します。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show ip bgp neighbors** [**advertised-routes**] 例： `Device# show ip bgp neighbors`	設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ルーティング ドメイン連合の設定

自律システムのグループの自律システム番号として機能する連合 ID を指定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system* 例： `Device(config)# router bgp 100`	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp confederation identifier** *autonomous-system* 例： `Device(config)# bgp confederation identifier 50007`	BGP 連合 ID を設定します。
ステップ 4	**bgp confederation peers** *autonomous-system* [*autonomous-system ...*] 例： `Device(config)# bgp confederation peers 51000 51001 51002`	連合に属する AS、および特殊な EBGP ピアとして処理する AS を指定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbor** 例： `Device# show ip bgp neighbor`	設定を確認します。
ステップ 7	**show ip bgp network** 例： `Device# show ip bgp network`	設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP ルート リフレクタの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system* 例： `Device(config)# router bgp 101`	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** {*ip-address* | *peer-group-name*} **route-reflector-client** 例： `Device(config-router)# neighbor 172.16.70.24 route-reflector-client`	ローカル ルータを BGP ルート リフレクタとして、指定されたネイバーをクライアントとして、それぞれ設定します。

	コマンドまたはアクション	目的
ステップ 4	**bgp cluster-id** *cluster-id* 例： `Device(config-router)# bgp cluster-id 10.0.1.2`	（任意）クラスタに複数のルート リフレクタが存在する場合、クラスタ ID を設定します。
ステップ 5	**no bgp client-to-client reflection** 例： `Device(config-router)# no bgp client-to-client reflection`	（任意）クライアント間のルート反映をディセーブルにします。デフォルトでは、ルート リフレクタ クライアントからのルートは、他のクライアントに反映されます。ただし、クライアントが完全メッシュ構造の場合、ルート リフレクタはルートをクライアントに反映させる必要がありません。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp** 例： `Device# show ip bgp`	設定を確認します。送信元 ID およびクラスタリスト属性を表示します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルート ダンプニングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**router bgp** *autonomous-system* 例： `Device(config)# router bgp 100`	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp dampening** 例： `Device(config-router)# bgp dampening`	BGP ルート ダンプニングをイネーブルにします。
ステップ 4	**bgp dampening** *half-life reuse suppress max-suppress* [**route-map** *map*] 例： `Device(config-router)# bgp dampening 30 1500 10000 120`	（任意）ルートダンプニング係数のデフォルト値を変更します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp flap-statistics** [{**regexp** *regexp*} | {**filter-list** *list*} | {*address mask* [**longer-prefix**]}] 例： `Device# show ip bgp flap-statistics`	（任意）フラッピングしているすべてのパスのフラップを監視します。ルートの抑制が終了し、安定状態になると、統計情報が削除されます。
ステップ 7	**show ip bgp dampened-paths** 例： `Device# show pi bgp dampened-paths`	（任意）抑制されるまでの時間を含めて、ダンプニングされたルートを表示します。
ステップ 8	**clear ip bgp flap-statistics** [{ *regexp*} | { *list*} | {*address mask* []}**regexpfilter-listlonger-prefix** 例： `Device# clear ip bgp flap-statistics`	（任意）BGP フラップ統計情報を消去して、ルートがダンプニングされる可能性を小さくします。
ステップ 9	**clear ip bgp dampening** 例： `Device# clear ip bgp dampening`	（任意）ルートダンプニング情報を消去して、ルートの抑制を解除します。

	コマンドまたはアクション	目的
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

BGP のモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。この作業は、特定の構造の内容が無効になる場合、または無効である疑いがある場合に必要となります。

BGP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。さらに、リソースの利用率を取得したり、ネットワーク問題を解決するための情報を使用することもできます。さらに、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のルーティング パスを検出することもできます。

下の図に、BGP を消去および表示するために使用する特権 EXEC コマンドを示します。表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

表 *116*： *IP BGP* の *clear* および *show* コマンド

clear ip bgp *address*	特定の BGP 接続をリセットします。
clear ip bgp *	すべての BGP 接続をリセットします。
clear ip bgp peer-group *tag*	BGP ピア グループのすべてのメンバを削除します。
show ip bgp *prefix*	プレフィックスがアドバタイズされるピア グループ、またはピア グループに含まれないピアを表示します。ネクスト ホップやローカル プレフィックスなどのプレフィックス属性も表示されます。
show ip bgp cidr-only	サブネットおよびスーパーネット ネットワーク マスクを含むすべての BGP ルートを表示します。
show ip bgp community [*community-number*] [**exact**]	指定されたコミュニティに属するルートを表示します。

show ip bgp community-list *community-list-number* [**exact-match**]	コミュニティ リストで許可されたルートを表示します。
show ip bgp filter-list *access-list-number*	指定された AS パス アクセス リストによって照合されたルートを表示します。
show ip bgp inconsistent-as	送信元の AS と矛盾するルートを表示します。
show ip bgp regexp *regular-expression*	コマンドラインに入力された特定の正規表現と一致する AS パスを持つルートを表示します。
show ip bgp	BGP ルーティング テーブルの内容を表示します。
show ip bgp neighbors [*address*]	各ネイバーとの BGP 接続および TCP 接続に関する詳細情報を表示します。
show ip bgp neighbors [*address*] [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** *regular-expression* | **received-routes** | **routes**]	特定の BGP ネイバーから取得されたルートを表示します。
show ip bgp paths	データベース内のすべての BGP パスを表示します。
show ip bgp peer-group [*tag*] [**summary**]	BGP ピア グループに関する情報を表示します。
show ip bgp summary	BGP 接続すべての状況を表示します。

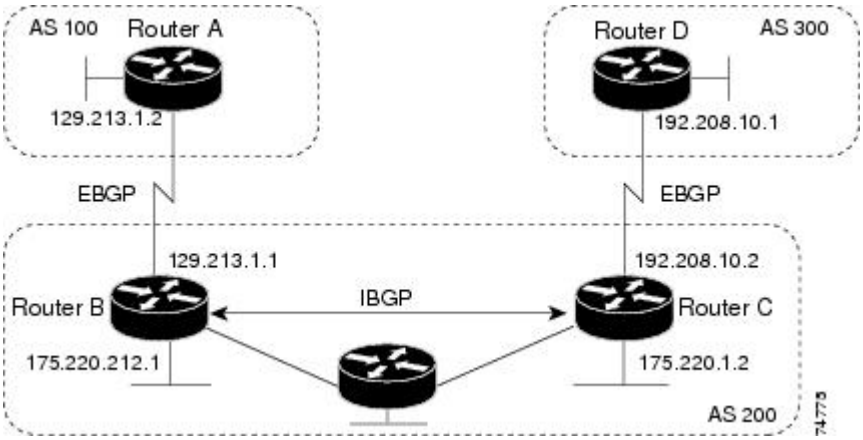
bgp log-neighbor changes コマンドは、デフォルトでイネーブルです。そのため、BGP ネイバーのリセット、起動、またはダウン時に生成されるメッセージをログに記録できます。

BGP の設定例

例：ルータでの BGP の設定

次に、下の図のルータでの BGP の設定例を示します。

図 *101 : EBGP*、*IBGP*、および複数の自律システム



ルータ A：

```
Device(config)# router bgp 100
Device(config-router)# neighbor 129.213.1.1 remote-as 200
```

ルータ B：

```
Device(config)# router bgp 200
Device(config-router)# neighbor 129.213.1.2 remote-as 100
Device(config-router)# neighbor 175.220.1.2 remote-as 200
```

ルータ C：

```
Device(config)# router bgp 200
Device(config-router)# neighbor 175.220.212.1 remote-as 200
Device(config-router)# neighbor 192.208.10.1 remote-as 300
```

ルータ D：

```
Device(config)# router bgp 300
Device(config-router)# neighbor 192.208.10.2 remote-as 200
```

BGP ピアが稼働していることを確認するには、show ip bgp neighbors 特権 EXEC コマンドを使用します。次に、ルータ A にこのコマンドを実行した場合の出力例を示します。

```
Device# show ip bgp neighbors

BGP neighbor is 129.213.1.1, remote AS 200, external link
 BGP version 4, remote router ID 175.220.212.1
 BGP state = established, table version = 3, up for 0:10:59
 Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
 Minimum time between advertisement runs is 30 seconds
 Received 2828 messages, 0 notifications, 0 in queue
 Sent 2826 messages, 0 notifications, 0 in queue
 Connections established 11; dropped 10
```

state = established 以外の情報が出力された場合、ピアは稼働していません。リモート ルータ ID は、ルータ（または最大のループバック インターフェイス）上の最大の IP アドレスです。テーブルが新規情報でアップデートされるたびに、テーブルのバージョン番号は増加します。

継続的にテーブルバージョン番号が増加している場合は、ルートがフラッピングし、ルーティング アップデートが絶えず発生しています。

外部プロトコルの場合、**network** ルータ コンフィギュレーション コマンドから IP ネットワークへの参照によって制御されるのは、アドバタイズされるネットワークだけです。これは、**network** コマンドを使用してアップデートの送信先を指定する IGP（EIGRP など）と対照的です。

BGP 設定の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Routing Protocols」を参照してください。特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

ISO CLNS ルーティングに関する情報

コネクションレス型ルーティング

国際標準化機構（ISO）コネクションレス型ネットワーク サービス（CLNS）プロトコルとは、オープン システム インターコネクション（OSI）モデルのネットワーク層の標準の 1 つです。ISO ネットワーク アーキテクチャ内のアドレスは、ネットワーク サービス アクセス ポイント（NSAP）アドレスおよび Network Entity Titles（NETs）と呼ばれます。OSI ネットワークの各ノードには、1 つ以上の NETs が含まれます。さらに、各ノードには、多数の NSAP アドレスが含まれます。

デバイス上で、**clns routing** グローバル コンフィギュレーション コマンドを使用してコネクションレス型ルーティングをイネーブルにすると、デバイスはルーティング関連の機能を果たさず、転送の決定だけを行います。ダイナミック ルーティングには、ルーティング プロトコルもイネーブルにする必要があります。デバイスは、Intermediate System-to-Intermediate System（IS-IS）ダイナミック ルーティング プロトコルをサポートします。このプロトコルは、ISO CLNS ネットワーク用の OSI ルーティング プロトコルに基づいています。

動的にルーティングを行う場合は、IS-IS を使用します。このルーティング プロトコルは、エリアの概念をサポートします。1つのエリア内部では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。エリア間では、ルータは適切なエリアに到達する方法を認識しています。IS-IS は、ステーション ルーティング（1つのエリア内）およびエリア ルーティング（エリア間）という 2 つのレベルのルーティングをサポートします。

ISO IGRP と IS-IS NSAP アドレス方式の主な違いは、エリア アドレスの定義にあります。両方ともレベル 1 ルーティング（1 つのエリア内）にはシステム ID を使用します。ただし、エリア ルーティングに関してアドレスが指定される方法が異なります。ISO IGRP NSAP アドレスには、ドメイン、エリア、およびシステム ID という 3 つの異なるフィールドが含まれます。IS-IS アドレスには、単一の連続的エリア フィールド（ドメイン フィールドおよびエリア フィールドから成る）とシステム ID という 2 つのフィールドが含まれます。

（注） ISO CLNS の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Configuration Guide, Release 12.4*』を参照してください。この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.4*』を参照するか、IOS コマンド リファレンス マスターインデックスを使用するか、オンライン検索を行ってください。

IS-IS ダイナミック ルーティング

IS-IS は、ISO ダイナミック ルーティング プロトコルの 1 つです（ISO 105890 で説明されている）。その他のルーティング プロトコルとは異なり、IS-IS をイネーブルするには、IS-IS ルーティング プロセスを作成し、それをネットワークではなく特定のインターフェイスに割り当てる必要があります。マルチエリア IS-IS コンフィギュレーション構文を使用することで、レイヤ 3 デバイスまたはルータごとに複数の IS-IS ルーティング プロトコルを指定できます。その後、IS-IS ルーティング プロセスのインスタンスごとにパラメータを設定します。

小規模の IS-IS ネットワークは、ネットワーク内にすべてのルータが含まれる単一のエリアとして構築されます。ネットワークの規模が大きくなるに従って、このネットワークは、すべてのエリアに属する、接続されたすべてのレベル 2 ルータのセットから構成されるバックボーンエリア内に再編成され、その後、このネットワークはローカルエリアに接続されます。ローカル エリア内部では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。エリア間では、ルータはバックボーンへの到達方法を認識しており、バックボーン ルータは他のエリアに到達する方法を認識しています。

ルータは、ローカルエリア内でルーティングを実行するために、レベル 1 の隣接関係を確立します（ステーション ルーティング）。ルータは、レベル 1 のエリア間でルーティングを実行するために、レベル 2 の隣接関係を確立します（エリア ルーティング）。

1 つの Cisco ルータは、最大 29 エリアのルーティングに参加でき、バックボーンでレベル 2 ルーティングを実行できます。一般に、ルーティング プロセスごとに 1 つのエリアに対応します。デフォルトでは、ルーティング プロセスの最初のインスタンスが、レベル 1 および レベル 2 両方のルーティングを実行するように設定されます。追加のルーティング インスタンスを設定できます。このインスタンスは、自動的にレベル 1 エリアとして扱われます。IS-IS ルーティング プロセスの各インスタンスごとに個別にパラメータを設定する必要があります。

IS-IS マルチエリア ルーティングでは、シスコの各装置に対して最大 29 個の レベル 1 エリアを定義できますが、レベル 2 ルーティングを実行するプロセスは 1 つだけ設定できます。レベル 2 ルーティングが任意のプロセス上に設定されている場合、追加のプロセスは、すべて自動的にレベル 1 に設定されます。同時に、このプロセスがレベル 1 ルーティングを実行するように設定することもできます。ルータ インスタンスにレベル 2 ルーティングが必要でない場合は、**is-type** グローバル コンフィギュレーション コマンドを使用してレベル 2 の機能を削除します。別のルータ インスタンスをレベル 2 ルータとして設定する場合にも **is-type** コマンドを使用します。

（注） IS-IS の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Routing Protocols」を参照してください。ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS IP Command Reference, Release 12.4*』を参照してください。

NSF 認識

統合型 IS-IS NSF 認識機能は IPv4G でサポートされています。この機能により、NSF を認識する顧客宅内装置（CPE）ルータが、NFS 対応ルータによるパケットのノンストップ転送を実現します。ローカル ルータでは、必ずしも NSF を実行している必要はありませんが、このルータが NSF を認識していると、スイッチオーバー プロセス時にルーティング データベースの整合性と精度、および隣接 NSF 対応ルータ上のリンクステート データベースが保持されます。

この機能は、自動的にイネーブルにされ、設定は必要ありません。この機能の詳細については、『*Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

IS-IS グローバル パラメータ

設定可能ないくつかのオプションの IS-IS グローバル パラメータを次に示します。

- ルート マップによって制御されるデフォルト ルートを設定することで、デフォルト ルートを IS-IS ルーティング ドメイン内に強制的に設定できます。ルート マップで設定可能な、その他のフィルタリング オプションも指定できます。
- 内部チェックサム エラーとともに受信された IS-IS LSP を無視したり、破損した LSP を消去するようにルータを設定できます。これにより、LSP の発信側は、LSP を再生成します。
- エリアおよびドメインにパスワードを割り当てられます。
- サマリー アドレスを使用して、ルーティング テーブル内に表示される集約アドレスを作成できます（経路集約）。他のルーティング プロトコルから学習したルートも集約できます。サマリーをアドバタイズするのに使用されるメトリックは、すべての個別ルートにおける最小のメトリックです。
- 過負荷ビットを設定できます。
- LSP リフレッシュ インターバルおよび LSP がリフレッシュなしでルータ データベース内にとどまることができる最大時間を設定できます。
- LSP 生成に対するスロットリング タイマー、最短パス優先計算、および部分ルート計算を設定できます。
- IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、デバイスがログ メッセージを生成するように設定できます。
- ネットワーク内のリンクが、1500 バイト未満の最大伝送単位（MTU）サイズの場合、それでもルーティングが行われるように LSP MTU の値を低くできます。

- パーティション回避ルータ コンフィギュレーション コマンドは、レベル1-2境界ルータ、隣接レベル 1 ルータ、およびエンド ホスト間で完全な接続が失われた場合に、エリアがパーティション化されるのを防ぎます。

IS-IS インターフェイス パラメータ

任意で、特定のインターフェイス固有の IS-IS パラメータを、付加されている他のルータとは別に設定できます。ただし、一部の値（乗数およびタイムインターバルなど）をデフォルトから変更する場合、複数のルータおよびインターフェイス上でもこれを変更する必要があります。ほとんどのインターフェイス パラメータは、レベル 1、レベル 2、またはその両方で設定できます。

次に、設定可能なインターフェイス レベル パラメータの一部を示します。

- インターフェイスのデフォルト メトリック：Quality of Service（QoS）ルーティングが実行されない場合に、IS-IS メトリックの値として使用され、割り当てられます。
- helloインターバル（インターフェイスから送信されるhelloパケットの間隔）またはデフォルトの hello パケット乗数：インターフェイス上で使用されて、IS-IS helloパケットで送信されるホールド タイムを決定します。ホールド タイムは、ネイバーがダウンしていると宣言するまでに、別の hello パケットを待機する時間を決定します。これにより、障害リンクまたはネイバーが検出される速さも決定し、ルートを再計算できるようになります。hello パケットが頻繁に失われ、IS-IS 隣接に無用な障害が発生する場合は、hello 乗数を変更してください。hello 乗数を大きくし、それに対応して hello インターバルを小さくすると、リンク障害を検出するのに必要な時間を増やすことなく、helloプロトコルの信頼性を高めることができます。
- その他のタイム インターバル：
  - Complete Sequence Number PDU（CSNP）インターバルCSNP は、指定ルータにより送信され、データベースの同期を維持します。
  - 再送信インターバルこれは、ポイントツーポイント リンクの IS-IS LSP の再送信間隔です。
  - IS-IS LSP 再送信スロットル インターバルこれは、IS-IS LSP がポイントツーポイント リンクで再送信される最大レート（パケット間のミリ秒数）です。このインターバルは、同じ LSP が連続する再送信間隔である再送信インターバルとは異なります。
- 指定ルータの選択プライオリティ：マルチアクセス ネットワークで必要な隣接数を削減し、その代わりに、ルーティング プロトコル トラフィックの量およびトポロジデータベースのサイズを削減できます。
- インターフェイス回線タイプ：指定されたインターフェイス上のネイバーに必要な隣接タイプです。
- インターフェイスのパスワード認証

ISO CLNS ルーティングの設定方法

IS-IS のデフォルト設定

表 *117 : IS-IS* のデフォルト設定

機能	デフォルト設定
リンクステート PDU（LSP）エラーを無視	イネーブル
IS-IS タイプ	従来型の IS-IS：ルータは、レベル 1（ステーション）とレベル 2（エリア） 両方のルータとして機能します。 マルチエリア IS-IS：IS-IS ルーティング プロセスの最初のインスタンスが レベル 1-2 ルータです。残りのインスタンスは、レベル1ルータです。
デフォルト情報送信元	ディセーブル
IS-IS 隣接関係のステート変更を記録	ディセーブル
LSP 生成スロットリング タイマー	連続で生成した2つの間の最大インターバル：5 秒 初期 LSP 生成遅延：50 ミリ秒 1 番目と 2 番目の LSP 生成間のホールド タイム：5000 ミリ秒
LSP 最大ライフ タイム（リフレッシュなし）	LSP パケットが削除されるまで 1200 秒（20 分）
LSP リフレッシュ インターバル	LSP リフレッシュを 900 秒（15 分）ごとに送信
最大 LSP パケット サイズ	1497 バイト
NSF 認識	イネーブルレイヤ3デバイスでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。

機能	デフォルト設定
部分ルート計算（PRC）スロットリング タイマー	最大 PRC 待機インターバル：5 秒 トポロジの変更後の初期 PRC 計算遅延：2000 ミリ秒 1 番目と 2 番目の PRC 計算間のホールド タイム：5000 ミリ秒
パーティション回避	ディセーブル
パスワード	エリアまたはドメインのパスワードが定義されておらず、認証はディセーブルになっています。
過負荷ビットの設定	ディセーブルイネーブルの際に引数が入力されない場合、過負荷ビットがただちに設定され、**no set-overload-bit** コマンドが入力されるまで設定されたままになります。
Shortest Path First（SPF）スロットリング タイマー	連続した SFP 間の最大インターバル：10 秒 トポロジの変更後の初期 SFP 計算：5500 ミリ秒 1 番目と 2 番目の SFP 計算間のホールド タイム：5500 ミリ秒
サマリー アドレス	ディセーブル

IS-IS ルーティングのイネーブル化

IS-IS をイネーブルにするには、各ルーティング プロセスに名前と NET を指定します。その後、インターフェイス上で IS-IS ルーティングをイネーブルにし、ルーティング プロセスの各インスタンスに対してエリアを指定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**clns routing** 例： `Device(config)# clns routing`	スイッチ上で ISO コネクションレス型ルーティングをイネーブルに設定します。
ステップ 3	**router isis** [*area tag*] 例： `Device(config)# router isis tag1`	指定したルーティングプロセスに対して IS-IS ルーティングをイネーブルにし、IS-IS ルーティング コンフィギュレーション モードを開始します。 （任意）*area tag* 引数を使用して、IS-IS ルータが割り当てられているエリアを特定します。複数の IS-IS エリアを設定する場合は、値を入力する必要があります。 最初に設定された IS-IS インスタンスは、デフォルトでレベル 1-2 です。後のインスタンスは、自動的にレベル 1 になります。**is-type** グローバル コンフィギュレーションコマンドを使用してルーティングのレベルを変更できます。
ステップ 4	**net** network-entity-title 例： `Device(config-router)# net 47.0004.004d.0001.0001.0c11.1111.00`	ルーティング プロセスに NET を設定します。マルチエリア IS-IS を設定する場合、各ルーティング プロセスに NET を指定します。NET およびアドレスの名前を指定できます。
ステップ 5	**is-type** {**level-1** | **level-1-2** | **level-2-only**} 例： `Device(config-router)# is-type level-2-only`	（任意）レベル 1（ステーション）ルータ、マルチエリアルーティング用のレベル 2（エリア）ルータ、または両方（デフォルト）として機能するようにルータを設定します。 • **level-1**：ステーション ルータとしてだけ機能します。 • **level-1-2**：ステーション ルータおよびエリア ルータの両方として機能します。 • **level 2**：エリア ルータとしてだけ機能します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-router)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	IS-IS をルーティングするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがまだレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力し、インターフェイスをレイヤ 3 モードにします。
ステップ 8	**ip router isis** [*area tag*] 例： `Device(config-if)# ip router isis tag1`	インターフェイス上の ISO CLNS に対して IS-IS ルーティング プロセスを設定し、ルーティング プロセスにエリア デジグネータを接続します。
ステップ 9	**clns router isis** [*area tag*] 例： `Device(config-if)# clns router isis tag1`	インターフェイス上で ISO CLNS をイネーブルにします。
ステップ 10	**ip address** *ip-address-mask* 例： `Device(config-if)# ip address 10.0.0.5 255.255.255.0`	インターフェイスの IP アドレスを定義します。インターフェイスのいずれかで IS-IS ルーティングが設定されている場合は、IS-IS がイネーブルになっているエリアに含まれるすべてのインターフェイスで IP アドレスが必要です。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show isis** [*area tag*] **database detail** 例： `Device# show isis database detail`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 13	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

IS-IS グローバル パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clns routing** 例： `Device(config)# clns routing`	スイッチ上で ISO コネクションレス型ルーティングをイネーブルに設定します。
ステップ 3	**router isis** 例： `Device(config)# router isis`	IS-IS ルーティング プロトコルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**default-information originate** [**route-map** *map-name*] 例： `Device(config-router)# default-information originate route-map map1`	（任意）デフォルトルートを IS-IS ルーティング ドメインに強制的に設定します。**route-map** *map-name* を入力すると、ルートマップが条件に一致している場合にルーティングプロセスによってデフォルトルートが生成されます。
ステップ 5	**ignore-lsp-errors** 例： `Device(config-router)# ignore-lsp-errors`	（任意）LSP を消去する代わりに、内部チェックサムにエラーがある LSP を無視するようにルータを設定します。このコマンドは、デフォルトでイネーブルになっています（破損した LSP はドロップされます）。破損した LSP を消去するには、**no ignore-lsp-errors** ルー

	コマンドまたはアクション	目的
		タ コンフィギュレーション コマンドを入力します。
ステップ 6	**area-password** *password* 例： `Device(config-router)# area-password 1password`	（任意）レベル 1（ステーション ルータ レベル）LSP に挿入されるエリア認証パスワードを設定します。
ステップ 7	**domain-password** *password* 例： `Device(config-router)# domain-password 2password`	（任意）レベル 2（エリア ルータ レベル）LSP に挿入されるルーティング ドメイン認証パスワードを設定します。
ステップ 8	**summary-address** *address mask* [**level-1** | **level-1-2** | **level-2**] 例： `Device(config-router)# summary-address 10.1.0.0 255.255.0.0 level-2`	（任意）所定のレベルのアドレスのサマリーを作成します。
ステップ 9	**set-overload-bit** [**on-startup** {*seconds* | **wait-for-bgp**}] 例： `Device(config-router)# set-overload-bit on-startup wait-for-bgp`	（任意）ルータに問題がある場合に、他のルータが最短パス優先（SPF）計算でこのルータを無視するように過負荷ビット（hippity ビット）を設定します。 • （任意）**on-startup**：起動時だけ過負荷ビットを設定します。**on-startup** が指定されない場合、過負荷ビットが即座に設定され、**no set-overload-bit** コマンドを入力するまで設定されたままになります。**on-startup** が指定された場合、秒数または **wait-for-bgp** を入力する必要があります。 • *seconds*：**on-startup** キーワードが設定されている場合、システム起動時に過負荷ビットが設定されて、この秒数の間設定されたままになります。指定できる範囲は 5 ～ 86400 秒です。 • **wait-for-bgp**：**on-startup** キーワードが設定されている場合、システ

	コマンドまたはアクション	目的
		ム起動時に過負荷ビットが設定されて、BGP が収束するまで設定されたままになります。BGP が収束されたことが IS-IS に通知されない場合、IS-IS は 10 分後に過負荷ビットをオフにします。
ステップ 10	**lsp-refresh-interval** *seconds* 例： `Device(config-router)# lsp-refresh-interval 1080`	（任意）LSP リフレッシュ インターバル（秒）を設定します。範囲は 1 ～ 65535 秒です。デフォルトでは、LSP リフレッシュを 900 秒（15 分）ごとに送信します。
ステップ 11	**max-lsp-lifetime** *seconds* 例： `Device(config-router)# max-lsp-lifetime 1000`	（任意）LSP パケットがリフレッシュされずにルータ データベース内に存続する最大時間を設定します。範囲は 1 ～ 65535 秒です。デフォルト値は 1200 秒（20 分）です。指定されたタイムインターバルのあと、LSP パケットは削除されます。
ステップ 12	**lsp-gen-interval** [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*] 例： `Device(config-router)# lsp-gen-interval level-2 2 50 100`	（任意）IS-IS 生成スロットリング タイマーを設定します。 • *lsp-max-wait*：2 つの連続する LSP 生成間の最大インターバル（秒）。指定できる範囲は 1 ～ 120 秒です。デフォルト値は 5 秒です。 • *lsp-initial-wait*：最初の LSP 生成遅延（ミリ秒）。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。 • *lsp-second-wait*：最初と 2 番目の LSP 生成間（ミリ秒）のホールドタイム。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
ステップ 13	**spf-interval** [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*] 例：	（任意）IS-IS SPF スロットリング タイマーを設定します。 • *spf-max-wait*：連続する SFP 間（秒）の最大インターバル。指定

	コマンドまたはアクション	目的
	`Device(config-router)# spf-interval level-2 5 10 20`	できる範囲は 1 ～ 120 で、デフォルトは 10 です。 • *spf-initial-wait*：トポロジ変更後の最初の SFP 計算（ミリ秒）。指定できる値の範囲は 1 ～ 10000 です。デフォルトは 5500 です。 • *spf-second-wait*：最初と 2 番目の SFP 計算間（ミリ秒）のホールドタイム。指定できる値の範囲は 1 ～ 10000 です。デフォルトは 5500 です。
ステップ 14	**prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*] 例： `Device(config-router)# prc-interval 5 10 20`	（任意）IS-IS PRC スロットリング タイマーを設定します。 • *prc-max-wait*：2 つの連続する PRC 計算間の最大インターバル（秒）。指定できる範囲は1～120 秒です。デフォルト値は 5 秒です。 • *prc-initial-wait*：トポロジ変更後の最初の PRC 計算遅延（ミリ秒）。指定できる範囲は 1 ～ 10,000 ミリ秒です。デフォルト値は 2000 ミリ秒です。 • *prc-second-wait*：最初と 2 番目の PRC 計算間（ミリ秒）のホールドタイム。指定できる範囲は 1 ～ 10,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
ステップ 15	**log-adjacency-changes** [**all**] 例： `Device(config-router)# log-adjacency-changes all`	（任意）IS-IS 隣接ステート変更をログするようルータを設定します。End System-to-Intermediate System PDU およびリンクステート パケット（LSP）など、IS-IS Hello に関連しないイベントにより生成されたすべての変更をログに含めるには、**all** を入力します。
ステップ 16	**lsp-mtu** *size* 例：	（任意）最大 LSP パケットサイズ（バイト）を指定します。指定できる範囲

	コマンドまたはアクション	目的
	`Device(config-router)# lsp mtu 1560`	は 128 ～ 4352 バイトです。デフォルト値は 1497 バイトです。 （注） ネットワーク内の任意のリンクで MTU サイズが縮小された場合、ネットワーク内のすべてのルータで LSP MTU サイズを変更する必要があります。
ステップ 17	**partition avoidance** 例： `Device(config-router)# partition avoidance`	（任意）境界ルータ、すべての隣接レベル 1 ルータ、およびエンド ホスト間で、フル接続が切断された場合、IS-IS レベル 1-2 境界ルータがレベル 1 エリア プレフィックスをレベル 2 バックボーンにアドバタイズしないようにします。
ステップ 18	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 19	**show clns** 例： `Device# show clns`	入力を確認します。
ステップ 20	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

IS-IS インターフェイス パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーションモードを開始します。インターフェイスがまだレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力し、インターフェイスをレイヤ 3 モードにします。
ステップ 3	**isis metric** *default-metric* [**level-1** | **level-2**] 例： `Device(config-if)# isis metric 15`	（任意）指定したインターフェイスにメトリック（またはコスト）を設定します。範囲は 0 ～ 63 です。デフォルトは 10 です。レベルが入力されない場合は、レベル 1 およびレベル 2 ルータの両方にデフォルト値が適用されます。
ステップ 4	**isis hello-interval** {*seconds* | **minimal**} [**level-1** | **level-2**] 例： `Device(config-if)# isis hello-interval minimal`	（任意）スイッチが hello パケットを送信する間隔を指定します。デフォルトでは、hello インターバル *seconds* の 3 倍の値が、送信される hello パケットの *holdtime* としてアドバタイズされます。hello インターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。 • **minimal**：ホールド タイムが 1 秒になるように、システムが hello 乗数に基づいて hello インターバルを計算するようにします。 • *seconds*：範囲は 1 ～ 65535 秒です。デフォルトは 10 秒です。
ステップ 5	**isis hello-multiplier** *multiplier* [**level-1** | **level-2**] 例： `Device(config-if)# isis hello-multiplier 5`	（任意）ルータが隣接装置のダウンを宣言するまでに、ネイバーが損失する IS-IS hello パケット数を指定します。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。hello 乗数を小さくすると、高速コンバージェンスとなりますが、ルーティングが不安定になる場合があります。

	コマンドまたはアクション	目的
ステップ 6	**isis csnp-interval** *seconds* [**level-1** | **level-2**] 例： `Device(config-if)# isis csnp-interval 15`	（任意）インターフェイスに IS-IS CSNP を設定します。範囲は 0 ～ 65535 です。デフォルトは 10 秒です。
ステップ 7	**isis retransmit-interval** *seconds* 例： `Device(config-if)# isis retransmit-interval 7`	（任意）ポイントツーポイントリンクの IS-IS LSP の再送信間隔（秒）を設定します。指定する値は、ネットワーク上の任意の 2 つのルータ間の予測ラウンドトリップ遅延よりも大きい整数である必要があります。範囲は 0 ～ 65535 です。デフォルトは 5 秒です。
ステップ 8	**isis retransmit-throttle-interval** *milliseconds* 例： `Device(config-if)# isis retransmit-throttle-interval 4000`	（任意）IS-IS LSP 再送信スロットルインターバルを設定します。これは、IS-IS LSP がポイントツーポイントリンク上で再送信される最大レート（パケット間のミリ秒数）です。範囲は 0 ～ 65535 です。デフォルト値は、**isis lsp-interval** コマンドにより決定します。
ステップ 9	**isis priority** *value* [**level-1** | **level-2**] 例： `Device(config-if)# isis priority 50`	（任意）指定ルータ選択で使用するプライオリティを設定します。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。
ステップ 10	**isis circuit-type** {**level-1** | **level-1-2** | **level-2-only**} 例： `Device(config-if)# isis circuit-type level-1-2`	（任意）指定されたインターフェイス上のネイバーで必要な隣接タイプを設定します（インターフェイスの回線タイプを指定します）。 • **level-1**：このノードとネイバーの両方に共通のエリアアドレスが少なくとも 1 つある場合、レベル 1 隣接関係が確立されます。 • **level-1-2**：ネイバーもレベル 1 およびレベル 2 の両方として設定されていて、少なくとも 1 つの共通のエリアがある場合、レベル 1 およびレベル 2 隣接関係が確立されます。共通のエリアがない場合は、レベル 2 隣接関係が確立されま

	コマンドまたはアクション	目的
		す。これはデフォルト設定です。これはデフォルトです。 • **level 2**：レベル 2 隣接関係が確立されます。ネイバールータがレベル 1 ルータである場合、隣接関係は確立されません。
ステップ 11	**isis password** *password* [**level-1** | **level-2**] 例： `Device(config-if)# isis password secret`	（任意）インターフェイスの認証パスワードを設定します。デフォルトでは、認証はディセーブルに設定されています。レベル 1 またはレベル 2 を指定すると、それぞれレベル 1 またはレベル 2 ルーティング用のパスワードだけがイネーブルになります。レベルを指定しない場合、デフォルトはレベル 1 およびレベル 2 です。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show clns interface** *interface-id* 例： `Device# show clns interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 14	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ISO IGRP と IS-IS のモニタリングおよびメンテナンス

CLNS キャッシュのすべての内容または特定のネイバーまたはルートの情報を削除できます。ルーティング テーブル、キャッシュ、およびデータベースの内容など、特定の CLNS または IS-IS の統計情報を表示できます。また、特定のインターフェイス、フィルタ、またはネイバーに関する情報も表示できます。

次の表に、ISO CLNS および IS-IS ルーティングを消去および表示するために使用する特権 EXEC コマンドを示します。出力フィールドの詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference,* 』を参照するか、Cisco IOS コマンド リファレンス マスター インデックスを使用するか、オンライン検索を行ってください。

表 *118 : ISO CLNS* と *IS-IS* の *clear* および *show* コマンド

コマンド	目的
clear clns cache	CLNS ルーティング キャッシュをクリアおよび再初期化します。
clear clns es-neighbors	隣接データベースから End System（ES）ネイバー情報を削除します。
clear clns is-neighbors	隣接データベースから Intermediate System（IS）ネイバー情報を削除します。
clear clns neighbors	隣接データベースから CLNS ネイバー情報を削除します。
clear clns route	動的に派生した CLNS ルーティング情報を削除します。
show clns	CLNS ネットワークに関する情報を表示します。
show clns cache	CLNS ルーティング キャッシュ内のエントリを表示します。
show clns es-neighbors	ES ネイバー エントリ（関連のあるエリアなど）を表示します。
show clns filter-expr	フィルタ式を表示します。
show clns filter-set	フィルタ セットを表示します。
show clns interface [*interface-id*]	各インターフェイスの CLNS 固有の情報または ES-IS 情報を表示します。
show clns neighbor	IS-IS ネイバーに関する情報を表示します。
show clns protocol	このルータの IS-IS または ISO IGRP ルーティング プロセスごとにプロトコル固有の情報を表示します。
show clns route	このルータが CLNS パケットをルーティングする方法を把握している宛先をすべて表示します。

コマンド	目的
show clns traffic	このルータで確認された CLNS パケットに関する情報を表示します。
show ip route isis	ISIS IP ルーティング テーブルの現在のステートを表示します。
show isis database	IS-IS リンクステート データベースを表示します。
show isis routes	IS-IS レベル 1 ルーティング テーブルを表示します。
show isis spf-log	IS-IS の Shortest Path First（SPF）計算の履歴を表示します。
show isis topology	すべてのエリアで接続済みルータのリストを表示します。
show route-map	設定されたすべてのルート マップ、または指定した 1 つのルートマップだけを表示します。
trace clns *destination*	ネットワークのパケットが指定された宛先までに経由するパスを検出します。
which-route {*nsap-address* | *clns-name*}	指定された CLNS の宛先が見つかったルーティング テーブルを表示します。

ISO CLNS ルーティングの設定例

例：IS-IS ルーティングの設定

次に、従来型の IS-IS を IP ルーティング プロトコルとして実行するために 3 つのルータを設定する方法を示します。従来型の IS-IS では、すべてのルータはレベル 1 およびレベル 2 のルータとして機能します（デフォルト）。

ルータ A：

```
Device(config)# clns routing
Device(config)# router isis
Device(config-router)# net 49.0001.0000.0000.000a.00
Device(config-router)# exit
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip router isis
Device(config-if)# clns router isis
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip router isis
```

```
Device(config-if)# clns router isis
Device(config-router)# exit
```

ルータ B：

```
Device(config)# clns routing
Device(config)# router isis
Device(config-router)# net 49.0001.0000.0000.000b.00
Device(config-router)# exit
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip router isis
Device(config-if)# clns router isis
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip router isis
Device(config-if)# clns router isis
Device(config-router)# exit
```

ルータ C：

```
Device(config)# clns routing
Device(config)# router isis
Device(config-router)# net 49.0001.0000.0000.000c.00
Device(config-router)# exit
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip router isis
Device(config-if)# clns router isis
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip router isis
Device(config-if)# clns router isis
Device(config-router)# exit
```

Multi-VRF CE に関する情報

バーチャル プライベート ネットワーク（VPN）は、ISP バックボーン ネットワーク上でお客様にセキュアな帯域幅共有を提供します。VPN は、共通ルーティング テーブルを共有するサイトの集合です。カスタマー サイトは、1 つまたは複数のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーは、VRF テーブルと呼ばれる VPN ルーティング テーブルと各インターフェイスを関連付けます。

スイッチ上で IP サービスまたは拡張 IP サービス フィーチャ セットが稼働している場合、スイッチはカスタマー エッジ（CE）デバイスの複数の VRF ルーティング/転送（Multi-VRF）インスタンスをサポートします（Multi-VRF CE）。サービス プロバイダーは、Multi-VRF CE により、重複する IP アドレスで複数の VPN をサポートできます。

（注） スイッチでは、VPN のサポートのためにマルチプロトコル ラベル スイッチング（MPLS）が使用されません。

Multi-VRF CE の概要

Multi-VRF CE は、サービス プロバイダーが複数の VPN をサポートし、VPN 間で IP アドレスを重複して使用できるようにする機能です。Multi-VRF CE は入力インターフェイスを使用して、さまざまな VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスと各 VRF を関連付けて仮想パケット転送テーブルを形成します。VRF 内のインターフェイスは、イーサネット ポートのように物理的なもの、または VLAN SVI のように論理的なものにもできますが、複数の VRF に属すことはできません。

（注） Multi-VRF CE インターフェイスは、レイヤ 3 インターフェイスである必要があります。

Multi-VRF CE には、次のデバイスが含まれます。

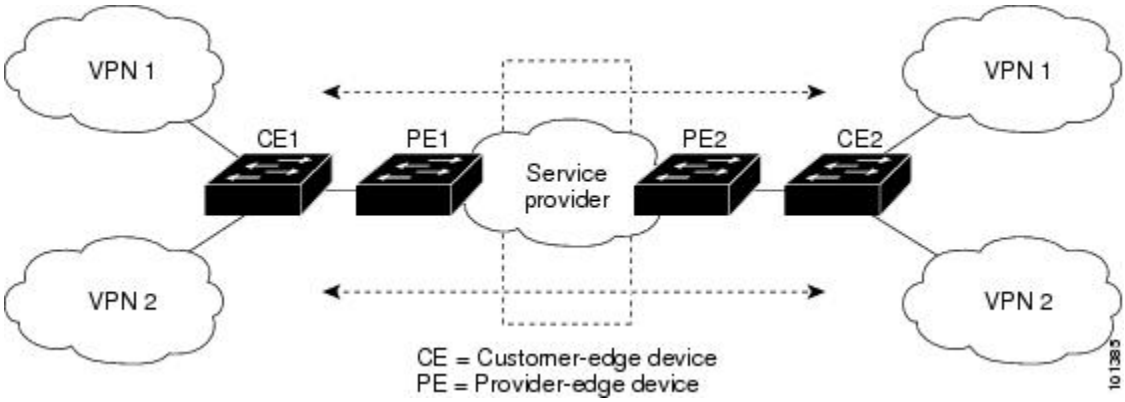
- お客様は、CE デバイスにより、1 つまたは複数のプロバイダー エッジ（PE）ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE デバイスは、サイトのローカル ルートをルータにアドバタイズし、リモート VPN ルートをそこから学習します。スイッチを CE に設定することができます。
- PE ルータは、スタティック ルーティング、または BGP、RIPv2、OSPF、EIGRP などのルーティング プロトコルを使用して、CE デバイスとルーティング情報を交換します。PE は、直接接続している VPN に対する VPN ルートのみを保守する必要があります。そのため、すべてのサービス プロバイダー VPN ルートを PE が保守する必要はありません。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に存在する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。PE ルータは、ローカル VPN ルートを CE から学習したあとで、IBGP を使用して別の PE ルータと VPN ルーティング情報を交換します。
- CE デバイスに接続していないサービス プロバイダー ネットワークのルータは、プロバイダー ルータやコア ルータになります。

Multi-VRF CE では、複数のお客様が 1 つの CE を共有でき、CE と PE の間で 1 つの物理リンクだけが使用されます。共有 CE は、お客様ごとに別々の VRF テーブルを維持し、独自のルーティングテーブルに基づいて、お客様ごとにパケットをスイッチングまたはルーティングします。Multi-VRF CE は、制限付きの PE 機能を CE デバイスに拡張して、別々の VRF テーブルを維持し、VPN のプライバシーおよびセキュリティをブランチ オフィスに拡張します。

ネットワーク トポロジ

次の図に、スイッチを複数の仮想 CE として使用した構成例を示します。このシナリオは、中小企業など、VPN サービスの帯域幅要件の低いお客様に適しています。この場合、スイッチにはマルチ VRF CE のサポートが必要です。Multi-VRF CE はレイヤ 3 機能なので、VRF のそれぞれのインターフェイスはレイヤ 3 インターフェイスである必要があります。

図 *102 :* 複数の仮想 *CE* として機能するスイッチ



CE スイッチは、レイヤ3インターフェイスを VRF に追加するコマンドを受信すると、Multi-VRF CE 関連のデータ構造で VLAN ID と Policy Label（PL）の間に適切なマッピングを設定し、VLAN ID と PL を VLAN データベースに追加します。

Multi-VRF CE を設定すると、レイヤ 3 フォワーディング テーブルは、次の 2 つのセクションに概念的に分割されます。

- Multi-VRF CE ルーティング セクションには、さまざまな VPN からのルートが含まれます。
- グローバル ルーティング セクションには、インターネットなど、VPN 以外のネットワークへのルートが含まれます。

さまざまな VRF の VLAN ID はさまざまな PL にマッピングされ、処理中に VRF を区別するために使用されます。レイヤ 3 設定機能では、学習した新しい VPN ルートごとに、入力ポートの VLAN ID を使用して PL を取得し、Multi-VRF CE ルーティング セクションに PL および新しいルートを挿入します。ルーテッド ポートからパケットを受信した場合は、ポート内部 VLAN ID 番号が使用されます。SVI からパケットを受信した場合は、VLAN 番号が使用されます。

パケット転送処理

Multi-VRF CE 対応ネットワークのパケット転送処理は次のとおりです。

- スイッチは、VPN からパケットを受信すると、入力 PL 番号に基づいてルーティング テーブルを検索します。ルートが見つかると、スイッチはパケットを PE に転送します。
- 入力 PE は、CE からパケットを受信すると、VRF 検索を実行します。ルートが見つかると、ルータは対応する MPLS ラベルをパケットに追加し、MPLS ネットワークに送信します。
- 出力 PE は、ネットワークからパケットを受信すると、ラベルを除去してそのラベルを使用し、正しい VPN ルーティング テーブルを識別します。次に、通常のルート検索を実行します。ルートが見つかると、パケットを正しい隣接デバイスに転送します。

- CE は、出力 PE からパケットを受信すると、入力 PL を使用して正しい VPN ルーティング テーブルを検索します。ルートが見つかると、パケットを VPN 内で転送します。

ネットワーク コンポーネント

VRF を設定するには、VRF テーブルを作成し、VRF に関連するレイヤ 3 インターフェイスを指定します。次に、VPN、および CE と PE 間でルーティング プロトコルを設定します。プロバイダーのバックボーンで VPN ルーティング情報を配信する場合は、BGP が優先ルーティング プロトコルです。Multi-VRF CE ネットワークには、次の 3 つの主要コンポーネントがあります。

- VPN ルート ターゲット コミュニティ：VPN コミュニティのその他すべてのメンバのリスト。VPN コミュニティ メンバーごとに VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング：VPN コミュニティのすべてのメンバーに VRF 到達可能性情報を伝播します。VPN コミュニティのすべての PE ルータで BGP ピアリングを設定する必要があります。
- VPN 転送：VPN サービス プロバイダー ネットワークを介し、全 VPN コミュニティ メンバー間で、全トラフィックを伝送します。

VRF 認識サービス

IP サービスはグローバル インターフェイスに設定可能で、グローバル ルーティング インスタンスで稼働します。IP サービスは複数のルーティング インスタンス上で稼働するように拡張されます。これが、VRF 認識です。システム内の任意の設定済み VRF であればいずれも、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームに依存しないモジュールに実装されます。VRF とは、Cisco IOS 内の複数のルーティング インスタンスを意味します。各プラットフォームには、サポートする VRF 数に関して独自の制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに ping を実行できます。
- ARP エントリは、個別の VRF で学習されます。ユーザは、特定の VRF の ARP エントリを表示できます。

Multi-VRF CE の設定方法

Multi-VRF CE のデフォルト設定

表 *119 : VRF* のデフォルト設定

機能	デフォルト設定
VRF	ディセーブルVRF は定義されていません。
マップ	インポート マップ、エクスポート マップ、ルート マップは定義されていません。
VRF 最大ルート数	ファスト イーサネット スイッチ：8000 ギガビット イーサネット スイッチ：12000
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブルです。

Multi-VRF CE の設定時の注意事項

（注）

Multi-VRF CE を使用するには、スイッチで IP サービスまたは拡張 IP サービス フィーチャ セットをイネーブルにする必要があります。

- Multi-VRF CE を含むスイッチは複数のお客様によって共有され、各お客様には独自のルーティング テーブルがあります。
- お客様は別々の VRF テーブルを使用するので、同じ IP アドレスを再利用できます。別々の VPN では IP アドレスの重複が許可されます。
- Multi-VRF CE では、複数のお客様が、PE と CE の間で同じ物理リンクを共有できます。複数の VLAN を持つトランク ポートでは、パケットがお客様間で分離されます。それぞれのお客様には独自の VLAN があります。
- Multi-VRF CE ではサポートされない MPLS-VRF 機能があります。ラベル交換、LDP 隣接関係、ラベル付きパケットはサポートされません。
- PE ルータの場合、Multi-VRF CE の使用と複数の CE の使用に違いはありません。図 41-6 では、複数の仮想レイヤ 3 インターフェイスが Multi-VRF CE デバイスに接続されています。
- スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合わせを使用して、VRF を設定できます。SVI は、アクセス ポートまたはトランク ポートで接続できます。
- お客様は、別のお客様と重複しないかぎり、複数の VLAN を使用できます。お客様の VLAN は、スイッチに保存されている適切なルーティング テーブルの識別に使用される特定のルーティング テーブル ID にマッピングされます。
- スイッチは、1 つのグローバル ネットワークおよび最大 26 の VRF をサポートします。
- CE と PE の間では、ほとんどのルーティング プロトコル（BGP、OSPF、RIP、およびスタティック ルーティング）を使用できます。ただし、次の理由から External BGP（EBGP）を使用することを推奨します。
  - BGP では、複数の CE とのやり取りに複数のアルゴリズムを必要としません。
  - BGP は、さまざまな管理者によって稼働するシステム間でルーティング情報を渡すように設計されています。
  - BGP では、ルートの属性を CE に簡単に渡すことができます。
- Multi-VRF CE は、パケットのスイッチング レートに影響しません。
- VPN マルチキャストはサポートされません。
- プライベート VLAN で VRF をイネーブルにできます（逆も同様です）。
- インターフェイスでポリシーベース ルーティング（PBR）がイネーブルになっている場合は、VRF をイネーブルにできません（逆も同様です）。
- インターフェイスで Web Cache Communication Protocol（WCCP）がイネーブルになっている場合は、VRF をイネーブルにできません（逆も同様です）。

VRF の設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference*』を参照してください。

（注） スタック スイッチで VRF 設定を変更した場合は、スタック全体をリロードすることをお勧めします。これは、CEF と VRF コントロール プレーン間の整合性を維持し、マスター スイッチオーバーの場合に不整合により表示されるエラー メッセージを避けるために不可欠です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： `Device(config)# ip routing`	IP ルーティングをイネーブルにします。
ステップ 3	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf vpn1`	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:2`	ルート識別子を指定して VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route-target both 100:2`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同一にする必要があります。

	コマンドまたはアクション	目的
ステップ 6	**import map** ルート マップ 例： `Device(config-vrf)# import map importmap1`	（任意）VRF にルート マップを対応付けます。
ステップ 7	**interface** *interface-id* 例： `Device(config-vrf)# interface gigabitethernet 1/0/1`	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスにはルーテッド ポートまたは SVI を設定できます。
ステップ 8	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding vpn1`	VRF をレイヤ 3 インターフェイスに対応付けます。 （注） **ip vrf forwarding** が管理インターフェイスで有効になっている場合、アクセス ポイントは加入しません。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： `Device# show ip vrf interfaces vpn1`	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VRF 認識サービスの設定

次のサービスは、VRF 認識です。

- 『ARP』
- ping

- 簡易ネットワーク管理プロトコル（SNMP）
- ユニキャスト RPF（uRPF）
- Syslog
- traceroute
- FTP および TFTP

（注） このスイッチでは、ユニキャスト RPF（uRPF）およびネットワーク タイム プロトコル（NTP）に対して VRF 認識のサービスはサポートされません。

ARP 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**show ip arp vrf** *vrf-name* 例： `Device# show ip arp vrf vpn1`	指定された VRF 内の ARP テーブルを表示します。

ping 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**ping vrf***vrf-name***ip-host** 例： `Device# ping vrf vpn1 ip-host`	指定された VRF 内の ARP テーブルを表示します。

SNMP 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server trap authentication vrf** 例： `Device(config)# snmp-server trap authentication vrf`	VRF で、パケットに対して SNMP トラップをイネーブルにします。
ステップ 3	**snmp-server engineID remote** *host* **vrf** *vpn-instance engine-id string* 例： `Device(config)# snmp-server engineID remote 172.16.20.3 vrf vpn1 80000009030000B064EFE100`	スイッチ上で、リモート SNMP エンジンの名前を設定します。
ステップ 4	**snmp-server host** *host* **vrf** *vpn-instance* **traps** *community* 例： `Device(config)# snmp-server host 172.16.20.3 vrf vpn1 traps comaccess`	SNMP トラップ動作の受信側、および SNMP トラップの送信に使用される VRF テーブルを指定します。
ステップ 5	**snmp-server host** *host* **vrf** *vpn-instance* **informs** *community* 例： `Device(config)# snmp-server host 172.16.20.3 vrf vpn1 informs comaccess`	SNMP 通知動作の受信先を指定し、SNMP 通知の送信に使用される VRF テーブルを指定します。
ステップ 6	**snmp-server user** *user group* **remote** *host* **vrf** *vpn-instance security model* 例： `Device(config)# snmp-server user abcd`	SNMP アクセス用に、VRF 上にあるリモート ホストの SNMP グループにユーザを追加します。

	コマンドまたはアクション	目的
	`remote 172.16.20.3 vrf vpn1 priv v2c 3des secure3des`	
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

uRPF 用 VRF 認識サービスの設定

uRPF は、VRF に割り当てられたインターフェイス上で設定でき、送信元検索が VRF テーブルで実行されます。

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no switchport** 例： `Device(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding vpn2`	インターフェイス上で VRF を設定します。
ステップ 5	**ip address** *ip-address* 例：	インターフェイスの IP アドレスを入力します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip address 10.1.5.1`	
ステップ 6	**ip verify unicast reverse-path** 例： `Device(config-if)# ip verify unicast reverse-path`	インターフェイス上でuRPFをイネーブルにします。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

VRF 認識 RADIUS の設定

VRF 認識 RADIUS を設定するには、まず RADIUS サーバ上で AAA をイネーブルにする必要があります。『Per VRF AAA Feature Guide』で説明されているとおり、スイッチで **ip vrf forwarding** *vrf-name* サーバグループ コンフィギュレーション コマンドと **ip radius source-interface** グローバル コンフィギュレーション コマンドがサポートされます。

syslog 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging on** 例： `Device(config)# logging on`	ストレージルータ イベント メッセージのロギングを、イネーブルまたは一時的にディセーブルにします。
ステップ 3	**logging host** *ip-address* **vrf** *vrf-name* 例：	ロギング メッセージが送信される Syslog サーバのホストアドレスを指定します。

	コマンドまたはアクション	目的
	`Device(config)# logging host 10.10.1.0 vrf vpn1`	
ステップ 4	**logging buffered** *logging buffered size***debugging** 例： `Device(config)# logging buffered critical 6000 debugging`	メッセージを内部バッファにロギングします。
ステップ 5	**logging trap debugging** 例： `Device(config)# logging trap debugging`	Syslog サーバに送信されるロギング メッセージを制限します。
ステップ 6	**logging facility** *facility* 例： `Device(config)# logging facility user`	ロギング ファシリティにシステム ロギング メッセージを送信します。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

traceroute 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『Cisco IOS Switching Services Command Reference, Release 12.4』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**traceroute vrf** *vrf-name ipaddress* 例： `Device(config)# traceroute vrf vpn2 10.10.1.1`	宛先アドレスを取得する VPN VRF の名前を指定します。

FTP および TFTP 用 VRF 認識サービスの設定

FTP および TFTP を VRF 認識とするには、いくつかの FTP/TFTP CLI を設定する必要があります。たとえば、インターフェイスに付加される VRF テーブルを使用する場合、E1/0 であれば、ip tftp source-interface E1/0 コマンドまたは ip ftp source-interface E1/0 コマンドを設定して、特定のルーティング テーブルを使用するように TFTP または FTP サーバに通知する必要があります。この例では、VRF テーブルが宛先 IP アドレスを検索するのに使用されます。これらの変更には下位互換性があり、既存の動作には影響を及ぼしません。つまり、VRF がそのインターフェイスに設定されていない場合でも、送信元インターフェイス CLI を使用して、特定のインターフェイスにパケットを送信できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip ftp source-interface** *interface-type interface-number* 例： `Device(config)# ip ftp source-interface gigabitethernet 1/0/2`	FTP 接続の発信元 IP アドレスを指定します。
ステップ 3	**end** 例： `Device(config)#end`	特権 EXEC モードに戻ります。
ステップ 4	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 5	**ip tftp source-interface** *interface-type interface-number* 例： `Device(config)# ip tftp source-interface gigabitethernet 1/0/2`	TFTP 接続用の送信元 IP アドレスを指定します。
ステップ 6	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	

マルチキャスト VRF の設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS IP Multicast Command Reference*』を参照してください。

Multi-VRF CE 内でのマルチキャスト設定の詳細については、『*IP Routing: Protocol-Independent Configuration Guide, Cisco IOS Release 15S*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： `Device(config)# ip routing`	IP ルーティング モードをイネーブルにします
ステップ 3	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf vpn1`	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:2`	ルート識別子を指定して VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:2`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* は、ステップ 4 で入力した

	コマンドまたはアクション	目的
		route-distinguisher と同一にする必要があります。
ステップ 6	**import map** ルート マップ 例： `Device(config-vrf)# import map importmap1`	（任意）VRF にルートマップを対応付けます。
ステップ 7	**ip multicast-routing vrf** *vrf-name***distributed** 例： `Device(config-vrf)# ip multicast-routing vrf vpn1 distributed`	（任意）VRF テーブルでグローバルマルチキャストルーティングをイネーブルにします。
ステップ 8	**interface** *interface-id* 例： `Device(config-vrf)# interface gigabitethernet 1/0/2`	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。インターフェイスはルーテッドポートまたは SVI に設定できます。
ステップ 9	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding vpn1`	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 10	**ip address** *ip-address***mask** 例： `Device(config-if)# ip address 10.1.5.1 255.255.255.0`	レイヤ 3 インターフェイスの IP アドレスを設定します。
ステップ 11	**ip pim sparse-dense mode** 例： `Device(config-if)# ip pim sparse-dense mode`	VRF に関連付けられているレイヤ 3 インターフェイス上で、PIM をイネーブルにします。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 13	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： `Device# show ip vrf detail vpn1`	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 14	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされている任意のルーティング プロトコル（RIP、OSPF、EIGRP、BGP）、またはスタティック ルーティングで設定できます。ここで説明する設定は OSPF のものですが、その他のプロトコルでも手順は同じです。

（注） VRF インスタンス内で EIGRP ルーティング プロセスが実行されるように設定するには、**autonomous-system** *autonomous-system-number* アドレス ファミリ コンフィギュレーション モード コマンドを入力して、自律システム番号を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id* **vrf** *vrf-name* 例： `Device(config)# router ospf 1 vrf vpn1`	OSPF ルーティングをイネーブルにして VPN 転送テーブルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**log-adjacency-changes** 例： `Device(config-router)# log-adjacency-changes`	（任意）隣接ステートの変更を記録します。これは、デフォルトの状態です。

	コマンドまたはアクション	目的
ステップ 4	**redistribute bgp** *autonomous-system-number***subnets** 例： `Device(config-router)# redistribute bgp 10 subnets`	BGP ネットワークから OSPF ネットワークに情報を再配布するようにスイッチを設定します。
ステップ 5	**network** *network-number***area** *area-id* 例： `Device(config-router)# network 1 area 2`	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip ospf** *process-id* 例： `Device# show ip ospf 1`	OSPF ネットワークの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP PE/CE ルーティング セッションの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 2`	その他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**network** *network-number* **mask** *network-mask* 例： `Device(config-router)# network 5 mask 255.255.255.0`	BGP を使用してアナウンスするネットワークおよびマスクを指定します。
ステップ 4	**redistribute ospf** *process-id* **match internal** 例： `Device(config-router)# redistribute ospf 1 match internal`	OSPF 内部ルートを再配布するようにスイッチを設定します。
ステップ 5	**network** *network-number* **area** *area-id* 例： `Device(config-router)# network 5 area 2`	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**address-family ipv4 vrf** *vrf-name* 例： `Device(config-router)# address-family ipv4 vrf vpn1`	PE/CE ルーティング セッションの BGP パラメータを定義し、VRF アドレス ファミリ モードを開始します。
ステップ 7	**neighbor** *address* **remote-as** *as-number* 例： `Device(config-router)# neighbor 10.1.1.2 remote-as 2`	PE と CE ルータの間の BGP セッションを定義します。
ステップ 8	**neighbor** *address* **activate** 例： `Device(config-router)# neighbor 10.2.1.1 activate`	IPv4 アドレス ファミリのアドバタイズメントをアクティブ化します。
ステップ 9	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip bgp** [**ipv4**] [**neighbors**] 例： `Device# show ip bgp ipv4 neighbors`	BGP 設定を確認します。

	コマンドまたはアクション	目的
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

Multi-VRF CE のモニタリング

表 *120 : Multi-VRF CE* 情報を表示するコマンド

show ip protocols vrf *vrf-name*	VRF に対応付けられたルーティング プロトコル情報を表示します。
show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**] [**supernets-only**]	VRF に対応付けられた IP ルーティング テーブル情報を表示します。
show ip vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]	定義された VRF インスタンスに関する情報を表示します。

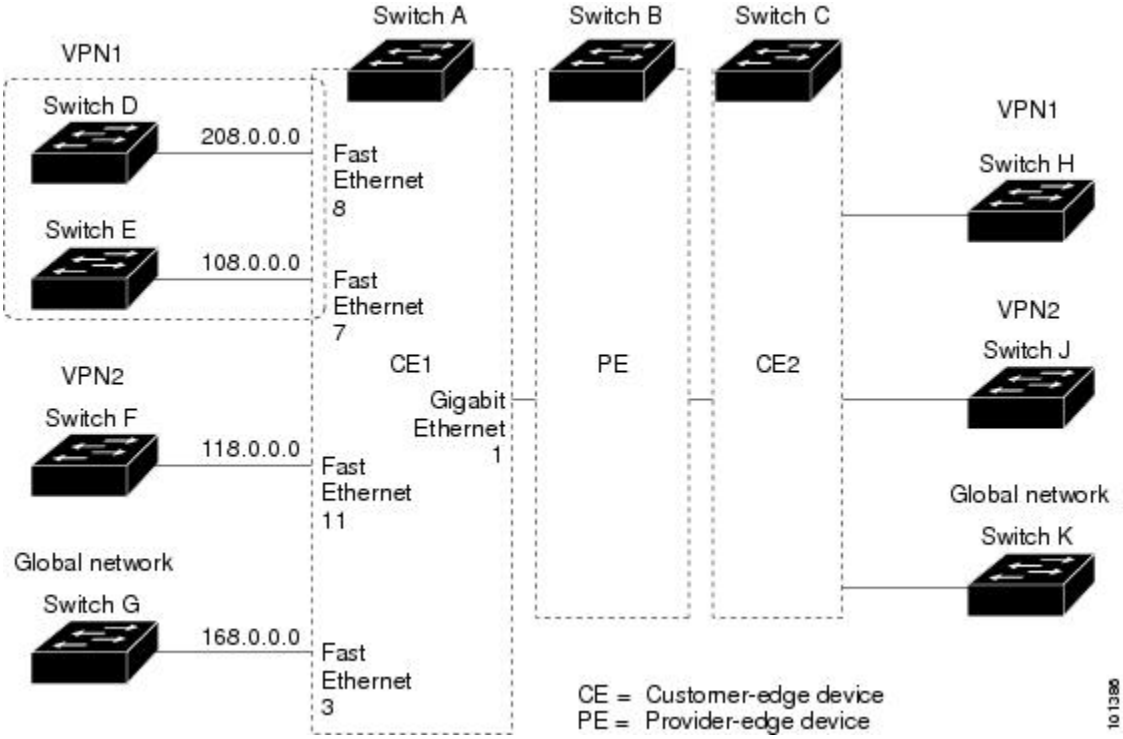
表示される情報の詳細については、『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

Multi-VRF CE の設定例

Multi-VRF CE の設定例

VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。CE/PE 接続には BGP が使用されます。図のあとに続く出力は、スイッチを CE スイッチ A として設定する例、およびカスタマー スイッチ D と F の VRF 設定を示しています。CE スイッチ C とその他のカスタマー スイッチを設定するコマンドは含まれていませんが、内容は同様です。この例には、PE ルータとして動作する Catalyst 6000 スイッチまたは Catalyst 6500 スイッチのスイッチ A へのトラフィックを設定するコマンドも含まれています。

図 *103 : Multi-VRF CE* の設定例



スイッチ A では、ルーティングをイネーブルにして VRF を設定します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip routing
Device(config)# ip vrf v11
Device(config-vrf)# rd 800:1
Device(config-vrf)# route-target export 800:1
Device(config-vrf)# route-target import 800:1
Device(config-vrf)# exit
Device(config)# ip vrf v12
Device(config-vrf)# rd 800:2
Device(config-vrf)# route-target export 800:2
Device(config-vrf)# route-target import 800:2
Device(config-vrf)# exit
```

スイッチAのループバックおよび物理インターフェイスを設定します。ギガビットイーサネット ポート 1 は PE へのトランク接続です。ギガビット イーサネット ポート 8 と 11 は VPN に接続されます。

```
Device(config)# interface loopback1
Device(config-if)# ip vrf forwarding v11
Device(config-if)# ip address 8.8.1.8 255.255.255.0
Device(config-if)# exit

Device(config)# interface loopback2
Device(config-if)# ip vrf forwarding v12
Device(config-if)# ip address 8.8.2.8 255.255.255.0
Device(config-if)# exit
```

```
Device(config)# interface gigabitethernet1/0/5
Device(config-if)# switchport trunk encapsulation dot1q
Device(config-if)# switchport mode trunk
Device(config-if)# no ip address
Device(config-if)# exit
Device(config)# interface gigabitethernet1/0/8
Device(config-if)# switchport access vlan 208
Device(config-if)# no ip address
Device(config-if)# exit
Device(config)# interface gigabitethernet1/0/11
Device(config-if)# switchport trunk encapsulation dot1q
Device(config-if)# switchport mode trunk
Device(config-if)# no ip address
Device(config-if)# exit
```

スイッチ A で使用する VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。VLAN 118 と 208 は、それぞれスイッチ F とスイッチ D を含む VPN に使用されます。

```
Device(config)# interface vlan10
Device(config-if)# ip vrf forwarding v11
Device(config-if)# ip address 38.0.0.8 255.255.255.0
Device(config-if)# exit
Device(config)# interface vlan20
Device(config-if)# ip vrf forwarding v12
Device(config-if)# ip address 83.0.0.8 255.255.255.0
Device(config-if)# exit
Device(config)# interface vlan118
Device(config-if)# ip vrf forwarding v12
Device(config-if)# ip address 118.0.0.8 255.255.255.0
Device(config-if)# exit
Device(config)# interface vlan208
Device(config-if)# ip vrf forwarding v11
Device(config-if)# ip address 208.0.0.8 255.255.255.0
Device(config-if)# exit
```

VPN1 と VPN2 で OSPF ルーティングを設定します。

```
Device(config)# router ospf 1 vrf vl1
Device(config-router)# redistribute bgp 800 subnets
Device(config-router)# network 208.0.0.0 0.0.0.255 area 0
Device(config-router)# exit
Device(config)# router ospf 2 vrf vl2
Device(config-router)# redistribute bgp 800 subnets
Device(config-router)# network 118.0.0.0 0.0.0.255 area 0
Device(config-router)# exit
```

CE/PE ルーティングに BGP を設定します。

```
Device(config)# router bgp 800
Device(config-router)# address-family ipv4 vrf vl2
Device(config-router-af)# redistribute ospf 2 match internal
Device(config-router-af)# neighbor 83.0.0.3 remote-as 100
Device(config-router-af)# neighbor 83.0.0.3 activate
Device(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Device(config-router-af)# exit
Device(config-router)# address-family ipv4 vrf vl1
Device(config-router-af)# redistribute ospf 1 match internal
Device(config-router-af)# neighbor 38.0.0.3 remote-as 100
Device(config-router-af)# neighbor 38.0.0.3 activate
```

```
Device(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Device(config-router-af)# end
```

スイッチ D は VPN 1 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip routing
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)# ip address 208.0.0.20 255.255.255.0
Device(config-if)# exit

Device(config)# router ospf 101
Device(config-router)# network 208.0.0.0 0.0.0.255 area 0
Device(config-router)# end
```

スイッチ F は VPN 2 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip routing
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport trunk encapsulation dot1q
Device(config-if)# switchport mode trunk
Device(config-if)# no ip address
Device(config-if)# exit

Device(config)# interface vlan118
Device(config-if)# ip address 118.0.0.11 255.255.255.0
Device(config-if)# exit

Device(config)# router ospf 101
Device(config-router)# network 118.0.0.0 0.0.0.255 area 0
Device(config-router)# end
```

このコマンドをスイッチ B（PE ルータ）で使用すると、CE デバイス、スイッチ A に対する接続だけが設定されます。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit
Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
```

```
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/1/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/1/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf vl
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end
```

ユニキャスト リバース パス転送の設定

ユニキャスト リバース パス転送（ユニキャスト RPF）機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造（スプーフィングされた）送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。たとえば、Smurf や Tribal Flood Network（TFN）など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタすることを攻撃者が阻止できるようにします。パブリック アクセスを提供するインターネット サービス プロバイダー（ISP）の場合、uRPF が IP ルーティング テーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、そのような攻撃をそらします。この処理により、ISP のネットワーク、その顧客、および残りのインターネットが保護されます。

（注）

- uRPF は、IP サービス でサポートされます。
- スイッチが複数のスイッチ タイプが混在する混合ハードウェア スタック内にある場合は、ユニキャスト RPF を設定しないでください。たとえば、Catalyst 3750-X、Catalyst 3750-E、Catalyst 3750 スイッチです。

IP uRPF 設定の詳細については、『*Cisco IOS Security Configuration Guide*』の「*Other Security Features*」の章を参照してください。

プロトコル独立機能

この項では、IP ルーティング プロトコルに依存しない機能について説明します。これらの機能は、IP ベースまたは IP サービス フィーチャ セットが稼働するスイッチ上で使用できますが、IP ベース フィーチャ セット付属のプロトコル関連機能は RIP でだけ使用できます。この章の IP ルーティング プロトコル独立コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』の「IP Routing Protocol-Independent Commands」の章を参照してください。

分散型シスコ エクスプレス フォワーディング

シスコ エクスプレス フォワーディングに関する情報

シスコ エクスプレス フォワーディング（CEF）は、ネットワーク パフォーマンスを最適化するために使用されるレイヤ 3 IP スイッチング技術です。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に割り当てることができます。スイッチ スタックでは、ハードウェアによって distributed CEF（dCEF）が使用されます。動的なネットワークでは、ルーティングの変更によって、高速スイッチング キャッシュ エントリが頻繁に無効になります。高速スイッチングキャッシュエントリが無効になると、トラフィックがルートキャッシュによって高速スイッチングされずに、ルーティング テーブルによってプロセス スイッチングされることがあります。CEF および dCEF は転送情報ベース（FIB）検索テーブルを使用して、宛先ベースの IP パケット スイッチングを実行します。

CEF および dCEF での 2 つの主要なコンポーネントは、分散 FIB と分散隣接テーブルです。

- FIB はルーティング テーブルや情報ベースと同様、IP ルーティング テーブルに転送情報のミラーイメージが保持されます。ネットワーク内でルーティングまたはトポロジが変更されると、IP ルーティング テーブルがアップデートされ、これらの変更が FIB に反映されます。FIB には、IP ルーティングテーブル内の情報に基づいて、ネクストホップのアドレス情報が保持されます。FIB にはルーティングテーブル内の既知のルートがすべて格納されているため、CEF はルート キャッシュをメンテナンスする必要がなく、トラフィックのスイッチングがより効率化され、トラフィック パターンの影響も受けません。
- リンク層上でネットワーク内のノードが 1 ホップで相互に到達可能な場合、これらのノードは隣接関係にあると見なされます。CEF は隣接テーブルを使用し、レイヤ 2 アドレッシング情報を付加します。隣接テーブルには、すべての FIB エントリに対する、レイヤ 2 のネクストホップのアドレスが保持されます。

スイッチまたはスイッチスタックは、ギガビット速度の回線レート IP トラフィックを達成するため特定用途向け集積回路（ASIC）を使用しているので、CEF または dCEF 転送はソフトウェア転送パス（CPU により転送されるトラフィック）にだけ適用されます。

シスコ エクスプレス フォワーディングの設定方法

デフォルトで、CEF または dCEF はグローバルにイネーブルに設定されています。何らかの理由でこれがディセーブルになった場合は、**ip cef** または **ip cef distributed** グローバル コンフィギュレーション コマンドを使用し、再度イネーブルに設定できます。

デフォルト設定では、すべてのレイヤ 3 インターフェイスで CEF または dCEF がイネーブルです。**no ip route-cache cef** インターフェイス コンフィギュレーション コマンドを入力すると、ソフトウェアが転送するトラフィックに対して CEF がディセーブルになります。このコマンドは、ハードウェア転送パスには影響しません。CEF をディセーブルにして **debug ip packet detail** 特権 EXEC コマンドを使用すると、ソフトウェア転送トラフィックをデバッグするのに便利です。ソフトウェア転送パス用のインターフェイスで CEF をイネーブルにするには、**ip route-cache cef** インターフェイス コンフィギュレーション コマンドを使用します。

⚠

注意 CLI には、インターフェイス上で CEF をディセーブルにする **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドが表示されますが、デバッグ以外の目的でインターフェイス上で CEF または dCEF をディセーブルにしないようにしてください。

ディセーブルである CEF または dCEF をグローバルにイネーブルにしたり、ソフトウェア転送トラフィックのインターフェイス上でイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip cef** 例： `Device(config)# ip cef`	非スタッキング スイッチで CEF の動作をイネーブルにします。 ステップ 4 に進みます。
ステップ 3	**ip cef distributed** 例： `Device(config)# ip cef distributed`	アクティブ スイッチで CEF の動作をイネーブルにします。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 5	**ip route-cache cef** 例： `Device(config-if)# ip route-cache cef`	ソフトウェア転送トラフィック用のインターフェイスでCEFをイネーブルにします。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip cef** 例： `Device# show ip cef`	すべてのインターフェイスの CEF ステータスを表示します。
ステップ 8	**show cef linecard** [**detail**] 例： `Device# show cef linecard detail`	（任意）非スタッキング スイッチの CEF 関連インターフェイス情報を表示します。
ステップ 9	**show cef linecard** [*slot-number*] [**detail**] 例： `Device# show cef linecard 5 detail`	（任意）スタック内のすべてのスイッチ、または指定されたスイッチに対して、スイッチのCEF関連インターフェイス情報をスタック メンバ別に表示します。 （任意）*slot-number* には、スタック メンバーのスイッチ番号を入力します。
ステップ 10	**show cef interface** [*interface-id*] 例： `Device# show cef interface gigabitethernet 1/0/1`	すべてのインターフェイスまたは指定されたインターフェイスの詳細な CEF 情報を表示します。
ステップ 11	**show adjacency** 例： `Device# show adjacency`	CEF の隣接テーブル情報を表示します。
ステップ 12	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

等コスト ルーティング パスの個数

等コスト ルーティング パスに関する情報

同じネットワークへ向かう同じメトリックのルートが複数ルータに格納されている場合、これらのルートは等価コストを保有していると見なされます。ルーティングテーブルに複数の等コスト ルートが含まれる場合は、これらをパラレル パスと呼ぶこともあります。ネットワークへの等コスト パスがルータに複数格納されている場合、ルータはこれらを同時に使用できます。パラレルパスを使用すると、パスに障害が発生した場合に冗長性を確保できます。また、使用可能なパスにパケットの負荷を分散し、使用可能な帯域幅を有効利用することもできます。等コスト ルートは、スタック内の各スイッチでサポートされます。

等コスト ルートはルータによって自動的に取得、設定されますが、ルーティング テーブルの IP ルーティング プロトコルでサポートされるパラレル パスの最大数は制御可能です。スイッチ ソフトウェア では最大 32 の等コスト ルーティングが許可されていますが、スイッチ ハードウェアはルートあたり 17 パス以上は使用しません。

等コスト ルーティング パスの設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **ospf** | **eigrp**} 例： `Device(config)# router eigrp`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**maximum-paths** *maximum* 例： `Device(config-router)# maximum-paths 2`	プロトコル ルーティング テーブルのパラレル パスの最大数を設定します。指定できる範囲は 1 ～ 16 です。ほとんどの IP ルーティング プロトコルでデフォルトは 4 ですが、BGP の場合だけ 1 です。
ステップ 4	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols** 例：	*Maximum path* フィールドの設定を確認します。

	コマンドまたはアクション	目的
	`Device# show ip protocols`	
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スタティック ユニキャスト ルート

スタティック ユニキャスト ルートに関する情報

スタティック ユニキャスト ルートは、特定のパスを通過して送信元と宛先間でパケットを送受信するユーザ定義のルートです。ルータが特定の宛先へのルートを構築できない場合、スタティック ルートは重要で、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

ユーザによって削除されるまで、スタティック ルートはスイッチに保持されます。ただし、アドミニストレーティブ ディスタンスの値を割り当て、スタティック ルートをダイナミック ルーティング情報で上書きできます。各ダイナミック ルーティング プロトコルには、デフォルトのアドミニストレーティブ ディスタンスが設定されています（表 10 を参照）。ダイナミック ルーティング プロトコルの情報でスタティック ルートを上書きする場合は、スタティック ルートのアドミニストレーティブ ディスタンスがダイナミック プロトコルのアドミニストレーティブ ディスタンスよりも大きな値になるように設定します。

表 *121*：ダイナミック ルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルト距離
接続されているインターフェイス	0
スタティック ルート	1
EIGRP サマリー ルート	5
外部 BGP	20
内部 EIGRP	90
IGRP	100
OSPF	110
内部 BGP	200
不明（Unknown）	225

インターフェイスを指し示すスタティック ルートは、RIP、IGRP、およびその他のダイナミック ルーティング プロトコルを通してアドバタイズされます。**redistribute** スタティック ルータ コンフィギュレーション コマンドが、これらのルーティング プロトコルに対して指定されているかどうかは関係ありません。これらのスタティック ルートがアドバタイズされるのは、インターフェイスを指し示すスタティック ルートが接続された結果、静的な性質を失ったとルーティング テーブルで見なされるためです。ただし、network コマンドで定義されたネットワーク以外のインターフェイスに対してスタティック ルートを定義する場合は、ダイナミック ルーティング プロトコルに **redistribute** スタティック コマンドを指定しない限り、ルートはアドバタイズされません。

インターフェイスがダウンすると、ダウンしたインターフェイスを経由するすべてのスタティック ルートが IP ルーティング テーブルから削除されます。転送ルータのアドレスとして指定されたアドレスへ向かう有効なネクストホップがスタティック ルート内に見つからない場合は、IP ルーティング テーブルからそのスタティック ルートも削除されます。

スタティック ユニキャスト ルートの設定

スタティック ユニキャスト ルートは、特定のパスを通過して送信元と宛先間でパケットを送受信するユーザ定義のルートです。ルータが特定の宛先へのルートを構築できない場合、スタティック ルートは重要で、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

スタティック ルートを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip route prefix mask** {*address* | *interface*} [*distance*] 例： `Device(config)# ip route prefix mask gigabitethernet 1/0/4`	スタティック ルートを確立します。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 5	**show ip route** 例： `Device# show ip route`	設定を確認するため、ルーティングテーブルの現在の状態を表示します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

スタティック ルートを削除するには、**no ip route** *prefix mask* {*address*| *interface*} グローバル コンフィギュレーション コマンドを使用します。ユーザによって削除されるまで、スタティック ルートはデバイスに保持されます。

デフォルトのルートおよびネットワーク

デフォルトのルートおよびネットワークに関する情報

ルータは、他のすべてのネットワークへのルートを学習できません。完全なルーティング機能を実現するには、一部のルータをスマート ルータとして使用し、それ以外のルータのデフォルト ルートをスマート ルータ宛てに指定します（スマート ルータにはインターネットワーク全体のルーティング テーブルに関する情報が格納されます）。これらのデフォルト ルートは動的に学習できますが、ルータごとに設定することもできます。ほとんどのダイナミックな内部ルーティング プロトコルには、スマート ルータを使用してデフォルト情報を動的に生成し、他のルータに転送するメカニズムがあります。

指定されたデフォルト ネットワークに直接接続されたインターフェイスがルータに存在する場合は、そのデバイス上で動作するダイナミック ルーティング プロトコルによってデフォルト ルートが生成されます。RIP の場合は、疑似ネットワーク 0.0.0.0 がアドバタイズされます。

ネットワークのデフォルトを生成しているルータには、そのルータ自身のデフォルト ルートも指定する必要があります。ルータが自身のデフォルト ルートを生成する方法の 1 つは、適切なデバイスを経由してネットワーク 0.0.0.0 に至るスタティック ルートを指定することです。

ダイナミック ルーティング プロトコルによってデフォルト情報を送信するときは、特に設定する必要はありません。ルーティング テーブルは定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。IGRP ネットワークでは、システムのデフォルト ネットワークの候補が複数存在する場合もあります。Cisco ルータでは、デフォル

ト ルートまたは最終ゲートウェイを設定するため、アドミニストレーティブ ディスタンスおよびメトリック情報を使用します。

ダイナミックなデフォルト情報がシステムに送信されない場合は、**ip default-network** グローバル コンフィギュレーション コマンドを使用し、デフォルト ルートの候補を指定します。このネットワークが任意の送信元のルーティング テーブルに格納されている場合は、デフォルト ルートの候補としてフラグ付けされます。ルータにデフォルト ネットワークのインターフェイスが存在しなくても、そこへのパスが格納されている場合、そのネットワークは1つの候補と見なされ、最適なデフォルト パスへのゲートウェイが最終ゲートウェイになります。

デフォルトのルートおよびネットワークの設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip default-network** *network number* 例： `Device(config)# ip default-network 1`	デフォルト ネットワークを指定します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ip route** 例： `Device# show ip route`	最終ゲートウェイで選択されたデフォルト ルートを表示します。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング情報を再配信するためのルート マップ

ルート マップの概要

スイッチでは複数のルーティング プロトコルを同時に実行し、ルーティング プロトコル間で情報を再配信できます。ルーティング プロトコル間での情報の再配信は、サポートされているすべての IP ベース ルーティング プロトコルに適用されます。

2 つのドメイン間で拡張パケット フィルタまたはルート マップを定義することにより、ルーティング ドメイン間でルートの再配信を条件付きで制御することもできます。**match** および **set** ルート マップ コンフィギュレーション コマンドは、ルート マップの条件部を定義します。**match** コマンドは、条件が一致する必要があることを指定しています。**set** コマンドは、ルーティング アップデートが match コマンドで定義した条件を満たす場合に行われる処理を指定します。再配信はプロトコルに依存しない機能ですが、**match** および **set** ルート マップ コンフィギュレーション コマンドの一部は特定のプロトコル固有のものです。

match コマンドのあとに、**set** コマンドおよび **route-map** コマンドをそれぞれ 1 つまたは複数指定します。**match** コマンドを指定しない場合は、すべて一致すると見なされます。**set** コマンドを指定しない場合、一致以外の処理はすべて実行されません。このため、少なくとも 1 つの **match** または **set** コマンドを指定する必要があります。

（注） **set** ルート マップ コンフィギュレーション コマンドを使用しないルート マップは、CPU に送信されるので、CPU の使用率が高くなります。

ルートマップ ステートメントは、**permit** または **deny** として識別することもできます。ステートメントが拒否としてマークされている場合、一致基準を満たすパケットは通常の転送チャネルを通じて送り返されます（宛先ベース ルーティング）、ステートメントが許可としてマークされている場合は、一致基準を満たすパケットに set コマンドが適用されます。一致基準を満たさないパケットは、通常のルーティング チャネルを通じて転送されます。

ルート マップの設定方法

次に示すステップ 3 ～ 14 はそれぞれ任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

（注） キーワードは、ルート配信を制御する手順で定義されているものと同じです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map***map-tag* [**permit** | **deny**] [*sequence number*] 例： `Device(config)# route-map rip-to-ospf permit 4`	再配信を制御するために使用するルート マップを定義し、ルート マップ コンフィギュレーション モードを開始します。 *map-tag*：ルートマップ用のわかりやすい名前を指定します。**redistribute** ルータ コンフィギュレーション コマンドはこの名前を使用して、このルートマップを参照します。複数のルートマップで同じマップ タグ名を共有できます。 （任意）**permit** が指定され、このルートマップの一致条件が満たされている場合は、set アクションの制御に従ってルートが再配信されます。**deny** が指定されている場合、ルートは再配信されません。 *sequence number*（任意）：同じ名前によってすでに設定されているルートマップのリスト内で、新しいルートマップの位置を指定する番号です。
ステップ 3	**match as-path** *path-list-number* 例： `Device(config-route-map)#match as-path 10`	BGP AS パス アクセス リストと照合します。
ステップ 4	**match community-list** *community-list-number* [**exact**] 例： `Device(config-route-map)# match community-list 150`	BGP コミュニティ リストのマッチングを行います。

	コマンドまたはアクション	目的
ステップ 5	**match ip address** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*] 例： `Device(config-route-map)# match ip address 5 80`	名前または番号を指定し、標準アクセス リストと照合します。1 ～ 199 の整数を指定できます。
ステップ 6	**match metric** metric-value 例： `Device(config-route-map)# match metric 2000`	指定されたルートメトリックと一致させます。*metric-value* には、0 ～ 4294967295 の値が指定された、EIGRP のメトリックを指定できます。
ステップ 7	**match ip next-hop** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*] 例： `Device(config-route-map)# match ip next-hop 8 45`	指定されたアクセス リスト（番号 1 ～ 199）のいずれかで送信される、ネクストホップのルータ アドレスと一致させます。
ステップ 8	**match tag** *tag value* [*...tag-value*] 例： `Device(config-route-map)# match tag 3500`	1 つまたは複数のルート タグ値からなるリスト内の指定されたタグ値と一致させます。0 ～ 4294967295 の整数を指定できます。
ステップ 9	**match interface***type number* [*...type-number*] 例： `Device(config-route-map)# match interface gigabitethernet 1/0/1`	指定されたインターフェイスの 1 つから、指定されたネクスト ホップへのルートと一致させます。
ステップ 10	**match ip route-source** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*] 例： `Device(config-route-map)# match ip route-source 10 30`	アドバタイズされた指定のアクセス リストによって指定したアドレスに一致します。
ステップ 11	**match route-type** {**local** | **internal** | **external** [**type-1** | **type-2**]} 例：	指定された **route-type** と一致させます。 • **local**：ローカルに生成された BGP ルート。

	コマンドまたはアクション	目的
	`Device(config-route-map)# match route-type local`	• **internal**：OSPF エリア内およびエリア間ルート、またはEIGRP内部ルート。 • **external**：OSPF 外部ルート（タイプ 1 またはタイプ 2）または EIGRP 外部ルート。
ステップ 12	**set dampening** *halflife reuse suppress max-suppress-time* 例： `Device(config-route-map)# set dampening 30 1500 10000 120`	BGP ルート ダンプニング係数を設定します。
ステップ 13	**set local-preference** *value* 例： `Device(config-route-map)# set local-preference 100`	ローカル BGP パスに値を割り当てます。
ステップ 14	**set origin** {**igp** | **egp** *as* | **incomplete**} 例： `Device(config-route-map)#set origin igp`	BGP 送信元コードを設定します。
ステップ 15	**set as-path** {**tag** | **prepend** *as-path-string*} 例： `Device(config-route-map)# set as-path tag`	BGP の自律システム パスを変更します。
ステップ 16	**set level** {**level-1** | **level-2** | **level-1-2** | **stub-area** | **backbone**} 例： `Device(config-route-map)# set level level-1-2`	ルーティング ドメインの指定エリアにアドバタイズされるルートのレベルを設定します。**stub-area** および **backbone** は、OSPF NSSA およびバックボーンエリアです。
ステップ 17	**set metric** *metric value* 例： `Device(config-route-map)# set metric 100`	再配布されるルートを指定するためのメトリック値を設定します（EIGRP のみ）。*metric value* は -294967295 ～ 294967295 の整数です。

	コマンドまたはアクション	目的
ステップ 18	**set metric***bandwidth delay reliability loading mtu* 例： `Device(config-route-map)# set metric 10000 10 255 1 1500`	再配布されるルートを指定するためのメトリック値を設定します（EIGRP のみ）。 • *bandwidth*：0 ～ 4294967295 の範囲のルートのメトリック値または IGRP 帯域幅（キロビット/秒単位）。 • *delay*：0 ～ 4294967295 の範囲のルート遅延（10 マイクロ秒単位）。 • *reliability*：0 ～ 255 の数値で表されるパケット伝送の成功可能性。255 は信頼性が 100% であること、0 は信頼性がないことを意味します。 • *loading*：0 ～ 255 の数値で表されるルートの有効帯域幅（255 は 100% の負荷）。 • *mtu*：ルートの MTU の最小サイズ（バイト単位）。範囲は 0 ～ 4294967295 です。
ステップ 19	**set metric-type {type-1 | type-2}** 例： `Device(config-route-map)# set metric-type type-2`	再配信されるルートに OSPF 外部メトリック タイプを設定します。
ステップ 20	**set metric-type internal** 例： `Device(config-route-map)# set metric-type internal`	ネクストホップの IGP メトリックと一致するように、EBGP ネイバーにアドバタイズされるプレフィックスの Multi-Exit 識別子（MED）値を設定します。
ステップ 21	**set weight** *number* 例： `Device(config-route-map)# set weight 100`	ルーティング テーブルの BGP 重みを設定します。指定できる値は 1 ～ 65535 です。
ステップ 22	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-route-map)# end`	
ステップ 23	**show route-map** 例： `Device# show route-map`	設定を確認するため、設定されたすべてのルートマップ、または指定されたルート マップだけを表示します。
ステップ 24	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ルート配信の制御方法

次に示すステップ 3 ～ 14 はそれぞれ任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

（注） キーワードは、再配信用にルート マップを設定する手順で定義されているものと同じです。

ルーティング プロトコルのメトリックを、必ずしも別のルーティング プロトコルのメトリックに変換する必要はありません。たとえば、RIP メトリックはホップ カウントで、IGRP メトリックは5つの特性の組み合わせです。このような場合は、メトリックを独自に設定し、再配信されたルートに割り当てます。ルーティング情報を制御せずにさまざまなルーティングプロトコル間で交換するとルーティングループが発生し、ネットワーク動作が著しく低下することがあります。

メトリック変換の代わりに使用されるデフォルトの再配信メトリックが定義されていない場合は、ルーティング プロトコル間で自動的にメトリック変換が発生することがあります。

- RIP はスタティック ルートを自動的に再配信できます。スタティック ルートにはメトリック 1（直接接続）が割り当てられます。
- デフォルト モードになっている場合、どのプロトコルも他のルーティング プロトコルを再配信できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**router** {**rip** | **ospf** | **eigrp**} 例： `Device(config)# router eigrp 10`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric** *metric-value*] [**metric-type** *type-value*] [**match internal** | **external** *type-value*] [**tag** *tag-value*] [**route-map** *map-tag*] [**weight** *weight*] [**subnets**] 例： `Device(config-router)# redistribute eigrp 1`	ルーティング プロトコル間でルートを再配信します。route-map を指定しないと、すべてのルートが再配信されます。キーワード **route-map** に *map-tag* を指定しないと、ルートは配信されません。
ステップ 4	**default-metric** *number* 例： `Device(config-router)# default-metric 1024`	現在のルーティング プロトコルが、再配信されたすべてのルートに対して同じメトリック値を使用するように設定します（RIP、OSPF）。
ステップ 5	**default-metric** bandwidth delay reliability loading mtu 例： `Device(config-router)# default-metric 1000 100 250 100 1500`	EIGRP ルーティング プロトコルが、EIGRP 以外で再配信されたすべてのルートに対して同じメトリック値を使用するように設定します。
ステップ 6	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show route-map** 例： `Device# show route-map`	設定を確認するため、設定されたすべてのルートマップ、または指定されたルート マップだけを表示します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Policy-Based Routing：ポリシーベース ルーティング

ポリシーベース ルーティングの概要

PBR を使用すると、トラフィック フローに定義済みポリシーを設定できます。PBR を使用してルーティングをより細かく制御するには、ルーティング プロトコルから取得したルートの信頼度を小さくします。PBR は、次の基準に基づいて、パスを許可または拒否するルーティング ポリシーを設定したり、実装したりできます。

- 特定のエンド システムの ID
- アプリケーション
- プロトコル

PBR を使用すると、等価アクセスや送信元依存ルーティング、インタラクティブ対バッチ トラフィックに基づくルーティング、専用リンクに基づくルーティングを実現できます。たとえば、在庫記録を本社に送信する場合は高帯域で高コストのリンクを短時間使用し、電子メールなど日常的に使用するアプリケーションデータは低帯域で低コストのリンクで送信できます。

PBR がイネーブルの場合は、アクセス コントロール リスト（ACL）を使用してトラフィックを分類し、各トラフィックがそれぞれ異なるパスを経由するようにします。PBR は着信パケットに適用されます。PBR がイネーブルのインターフェイスで受信されたすべてのパケットは、ルート マップを通過します。ルート マップで定義された基準に基づいて、パケットは適切なネクスト ホップに転送（ルーティング）されます。

- 許可とマークされているルート マップ文は次のように処理されます。
  - match コマンドは長さまたは複数の ACL で照合できます。ルート マップ文には複数の match コマンドを含めることができます。論理関数またはアルゴリズム関数は、許可または拒否の決定がされるまで、すべての match コマンドで実行されます。

    次に例を示します。

    match length A B

    match ip address acl1 acl2

    match ip address acl3

  パケットは、match length A B または acl1 または acl2 または acl3 により許可される場合に許可されます。

  - 決定が許可の場合は、set コマンドで指定されたアクションがパケットで適用されます。
  - 下された決定が拒否の場合は、PBR アクション（set コマンドで指定された）が適用されません。代わりに、処理ロジックが、シーケンス内の次のルートマップ文（シーケンス番号が次に高い文）に移動します。次の文が存在しない場合は、PBR 処理が終了し、パケットがデフォルトの IP ルーティング テーブルを使用してルーティングされます。

- PBR では、拒否としてマークされているルートマップ ステートメントはサポートされません。

標準 IP ACL を使用すると、アプリケーション、プロトコル タイプ、またはエンド ステーションに基づいて一致基準を指定するように、送信元アドレスまたは拡張 IP ACL の一致基準を指定できます。一致が見つかるまで、ルートマップにこのプロセスが行われます。一致が見つからない場合、通常の宛先ベースルーティングが行われます。match ステートメント リストの末尾には、暗黙の拒否ステートメントがあります。

match 句が満たされた場合は、set 句を使用して、パス内のネクスト ホップ ルータを識別する IP アドレスを指定できます。

PBR コマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』を参照してください。

PBR の設定方法

- PBR を使用するには、スイッチまたはスタック マスター上で IP Base フィーチャ セットをイネーブルにしておく必要があります。
- マルチキャスト トラフィックには、ポリシーによるルーティングが行われません。PBR が適用されるのはユニキャスト トラフィックだけです。
- ルーテッド ポートまたは SVI 上で、PBR をイネーブルにできます。
- スイッチは一致長に基づき PBR をサポートします。
- レイヤ 3 モードの EtherChannel ポート チャネルにはポリシー ルート マップを適用できますが、EtherChannel のメンバーである物理インターフェイスには適用できません。適用しようとすると、コマンドが拒否されます。ポリシー ルート マップが適用されている物理インターフェイスは、EtherChannel のメンバーになることができません。
- スイッチまたはスイッチ スタックには最大 128 個の IP ポリシー ルート マップを定義できます。
- スイッチまたはスイッチ スタックには、PBR 用として最大 512 個のアクセス コントロール エントリ（ACE）を定義できます。
- ルート マップに一致基準を設定する場合は、次の注意事項に従ってください。
  - ローカル アドレス宛てのパケットを許可する ACL と照合させないでください。
- VRF と PBR は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、VRF をイネーブルにはできません。その反対の場合も同じで、VRF がインターフェイスでイネーブルになっているときは、PBR をイネーブルにできません。
- WCCP と PBR は、スイッチ インターフェイスで相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、WCCP をイネーブルにできません。その反対の場合も同じで、WCCP がインターフェイスでイネーブルになっているときは、PBR をイネーブルにできません。

- PBR で使用されるハードウェア エントリ数は、ルート マップ自体、使用される ACL、ACL およびルート マップ エントリの順序によって異なります。
- TOS、DSCP、および IP Precedence に基づく PBR はサポートされません。
- set interface、set default next-hop、および set default interface はサポートされません。
- **ip next-hop recursive** および **ip next-hop verify availability** 機能は使用できません。next-hop は、直接接続される必要があります。
- set アクションのないポリシー マップはサポートされます。一致パケットは通常どおりにルーティングされます。
- match 句のないポリシー マップはサポートされます。set アクションはすべてのパケットに適用されます。

デフォルトでは、PBR はスイッチ上でディセーブルです。PBR を有効にするには、一致基準および結果アクションを指定するルートマップを作成する必要があります。次に、特定のインターフェイスでそのルート マップ用の PBR をイネーブルにします。指定したインターフェイスに着信したパケットのうち、match 句と一致したものはすべて PBR の対象になります。

スイッチで生成されたパケットまたはローカル パケットは、通常どおりにポリシー ルーティングされません。スイッチ上でローカルPBRをグローバルにイネーブルにすると、そのスイッチから送信されたすべてのパケットがローカル PBR の影響を受けます。ローカル PBR は、デフォルトでディセーブルに設定されています。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map** *map-tag* [**permit**] [*sequence number*] 例： `Device(config)# route-map pbr-map permit`	パケットの出力場所を制御するために使用するルートマップを定義し、ルート マップのコンフィギュレーション モードを開始します。 • *map-tag* – ルート マップ用のわかりやすい名前。 **ip policy route-map** インターフェイス コンフィギュレーション コマンドは、この名前を使用して、このルート マップを参照します。同じ map-tag がある複数の route-map 文は、1 つの route-map を定義します。 • （任意） **permit** – **permit** が指定され、このルート マップの一致

	コマンドまたはアクション	目的
		条件が満たされている場合は、set アクションの制御に従ってルートがポリシー ルーティングされます。 • （任意） *sequence number* – シーケンス番号は、特定のルートマップ内の route-map ステートメントの位置を示します。
ステップ 3	**match ip address** {*access-list-number* | *access-list-name*} [*access-list-number* |...*access-list-name*] 例： `Device(config-route-map)# match ip address 110 140`	1 つ以上の標準または拡張アクセス リストで許可されている送信元および宛先 IP アドレスを照合します。ACL は、複数の送信元および宛先 IP アドレスでも照合できます。 **match** コマンドを指定しない場合、ルートマップはすべてのパケットに適用されます。
ステップ 4	**match length min max** 例： `Device(config-route-map)# match length 64 1500`	パケット長と照合します。
ステップ 5	**set ip next-hop** *ip-address* [...*ip-address*] 例： `Device(config-route-map)# set ip next-hop 10.1.6.2`	基準と一致するパケットの動作を指定します。パケットのルーティング先となるネクストホップを設定します（ネクストホップは隣接している必要があります）。
ステップ 6	**exit** 例： `Device(config-route-map)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するインタフェースを指定します。
ステップ 8	**ip policy route-map** *map-tag* 例： `Device(config-if)# ip policy route-map pbr-map`	レイヤ 3 インターフェイス上で PBR を有効にし、使用するルートマップを識別します。1 つのインターフェイスに設定できるルート マップは、1 つだけです。ただし、異なるシーケンス番号を持つ複数のルートマップエントリを

	コマンドまたはアクション	目的
		設定できます。これらのエントリは、最初の一致が見つかるまで、シーケンス番号順に評価されます。一致が見つからない場合、パケットは通常どおりにルーティングされます。
ステップ 9	**ip route-cache policy** 例： `Device(config-if)# ip route-cache policy`	（任意）PBR の高速スイッチングを有効にします。PBR の高速スイッチングを有効にするには、PBR を有効にする必要があります。
ステップ 10	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**ip local policy route-map** *map-tag* 例： `Device(config)# ip local policy route-map local-pbr`	（任意）ローカルPBRを有効にして、スイッチから送信されるパケットにPBRを実行します。ローカルPBRは、スイッチによって生成されるパケットに適用されます。着信パケットには適用されません。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show route-map** [*map-name*] 例： `Device# show route-map`	（任意）設定を確認するため、設定されたすべてのルートマップ、または指定されたルートマップだけを表示します。
ステップ 14	**show ip policy** 例： `Device# show ip policy`	（任意）インターフェイスに付加されたポリシー ルート マップを表示します。
ステップ 15	**show ip local policy** 例： `Device# show ip local policy`	（任意）ローカルPBRが有効であるかどうか、および有効である場合は使用されているルート マップを表示します。

ルーティング情報のフィルタリング

ルーティング プロトコル情報をフィルタリングする場合は、以下の作業を実行します。

（注） OSPF プロセス間でルートが再配信される場合、OSPF メトリックは保持されません。

受動インターフェイスの設定

ローカル ネットワーク上の他のルータが動的にルートを取得しないようにするには、**passive-interface** ルータ コンフィギュレーション コマンドを使用し、ルーティング アップデートメッセージがルータインターフェイスから送信されないようにします。OSPF プロトコルでこのコマンドを使用すると、パッシブに指定したインターフェイスアドレスが OSPF ドメインのスタブ ネットワークとして表示されます。OSPF ルーティング情報は、指定されたルータインターフェイスから送受信されません。

多数のインターフェイスが存在するネットワークで、インターフェイスを手動でパッシブに設定する作業を回避するには、**passive-interface default** ルータ コンフィギュレーション コマンドを使用し、すべてのインターフェイスをデフォルトでパッシブになるように設定します。このあとで、隣接関係が必要なインターフェイスを手動で設定します。

パッシブとしてイネーブルにしたインターフェイスを確認するには、**show ip ospf interface** などのネットワーク モニタリング用特権 EXEC コマンドを使用します。アクティブとしてイネーブルにしたインターフェイスを確認するには、**show ip interface** 特権 EXEC コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**rip** | **ospf** | **eigrp**} 例： `Device(config)# router ospf`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**passive-interface** *interface-id* 例： `Device(config-router)# passive-interface gigabitethernet 1/0/1`	指定されたレイヤ3インターフェイス経由のルーティング アップデートの送信を抑制します。
ステップ 4	**passive-interface default** 例： `Device(config-router)# passive-interface default`	（任意）すべてのインターフェイスを、デフォルトでパッシブとなるように設定します。

	コマンドまたはアクション	目的
ステップ 5	**no passive-interface** *interface type* 例： `Device(config-router)# no passive-interface gigabitethernet1/0/3 gigabitethernet 1/0/5`	（任意）隣接関係を送信する必要があるインターフェイスだけをアクティブにします。
ステップ 6	**network** *network-address* 例： `Device(config-router)# network 10.1.1.1`	（任意）ルーティングプロセス用のネットワーク リストを指定します。*network-address* は IP アドレスです。
ステップ 7	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング アップデートのアドバタイズおよび処理の制御

アクセス コントロール リストと **distribute-list** ルータ コンフィギュレーション コマンドを組み合わせて使用すると、ルーティングアップデート中にルートのアドバタイズを抑制し、他のルータが 1 つまたは複数のルートを取得しないようにできます。この機能を OSPF で使用した場合は外部ルートにだけ適用されるため、インターフェイス名を指定できません。

distribute-list ルータ コンフィギュレーション コマンドを使用し、着信したアップデートのリストのうち特定のルートを処理しないようにすることもできます。（OSPF にこの機能は適用されません）。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**rip** | **eigrp**} 例：	ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# router eigrp 10`	
ステップ 3	**distribute-list** {*access-list-number* | *access-list-name*} **out** [*interface-name* | *routing process* | *autonomous-system-number*] 例： `Device(config-router)# distribute 120 out gigabitethernet 1/0/7`	アクセス リスト内のアクションに応じて、ルーティングアップデート内のルートのアドバタイズを許可または拒否します。
ステップ 4	**distribute-list** {*access-list-number* | *access-list-name*} **in** [*type-number*] 例： `Device(config-router)# distribute-list 125 in`	アップデートにリストされたルートの処理を抑制します。
ステップ 5	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング情報の送信元のフィルタリング

一部のルーティング情報が他の情報よりも正確な場合があるため、フィルタリングを使用して、さまざまな送信元から送られる情報にプライオリティを設定できます。「アドミニストレーティブディスタンス」は、ルータやルータのグループなど、ルーティング情報の送信元の信頼性を示す数値です。大規模ネットワークでは、他のルーティングプロトコルよりも信頼できるルーティング プロトコルが存在する場合があります。アドミニストレーティブ ディスタンスの値を指定すると、ルータはルーティング情報の送信元をインテリジェントに区別できるようになります。常にルーティング プロトコルのアドミニストレーティブ ディスタンスが最短（値が最小）であるルートが選択されます。

各ネットワークには独自の要件があるため、アドミニストレーティブディスタンスを割り当てる一般的な注意事項はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**rip** | **ospf** | **eigrp**} 例： `Device(config)# router eigrp 10`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**distance** *weight* {*ip-address* {*ip-address mask*}} [*ip access list*] 例： `Device(config-router)# distance 50 10.1.5.1`	アドミニストレーティブ ディスタンスを定義します。 *weight*：アドミニストレーティブディスタンスは 10 ～ 255 の整数です。単独で使用した場合、*weight* はデフォルトのアドミニストレーティブ ディスタンスを指定します。ルーティング情報の送信元に他の指定がない場合に使用されます。アドミニストレーティブ ディスタンスが 255 のルートはルーティング テーブルに格納されません。 （任意）*ip access list*：着信ルーティング アップデートに適用される IP 標準または IP 拡張アクセス リストです。
ステップ 4	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols** 例： `Device# show ip protocols`	指定されたルーティング プロセス用のデフォルトのアドミニストレーティブ ディスタンスを表示します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

認証キーの管理

キー管理を使用すると、ルーティングプロトコルで使用される認証キーを制御できます。一部のプロトコルでは、キー管理を使用できません。認証キーは EIGRP および RIP バージョン 2 で使用できます。

前提条件

認証キーを管理する前に、認証をイネーブルにする必要があります。プロトコルに対して認証をイネーブルにする方法については、該当するプロトコルについての説明を参照してください。認証キーを管理するには、キー チェーンを定義してそのキー チェーンに属するキーを識別し、各キーの有効期間を指定します。各キーには、ローカルにストアされる独自のキー ID（**key** *number* キー チェーン コンフィギュレーション コマンドで指定）があります。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5（MD5）認証キーが一意に識別されます。

認証キーの設定方法

有効期間が指定された複数のキーを設定できます。存在する有効なキーの数にかかわらず、送信される認証パケットは1つだけです。最小の番号から順にキー番号が調べられ、最初に見つかった有効なキーが使用されます。キー変更中は、有効期間が重なっても問題ありません。これらの有効期間は、ルータに通知する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**key chain** *name-of-chain* 例： `Device(config)# key chain key10`	キー チェーンを識別し、キーチェーン コンフィギュレーション モードを開始します。
ステップ 3	**key** *number* 例： `Device(config-keychain)# key 2000`	キー番号を識別します。指定できる範囲は 0 ～ 2147483647 です。
ステップ 4	**key-string** *text* 例： `Device(config-keychain)# Room 20, 10th floor`	キー ストリングを確認します。ストリングには 1 ～ 80 文字の大文字および小文字の英数字を指定できますが、最初の文字に数字を指定できません。

	コマンドまたはアクション	目的
ステップ 5	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} 例： `Device(config-keychain)# accept-lifetime 12:30:00 Jan 25 1009 infinite`	（任意）キーを受信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 6	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} 例： `Device(config-keychain)# accept-lifetime 23:30:00 Jan 25 1019 infinite`	（任意）キーを送信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 7	**end** 例： `Device(config-keychain)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show key chain** 例： `Device# show key chain`	認証キーの情報を表示します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ネットワークのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定の統計情報を表示することもできます。

表 *122 : IP* ルートの削除またはルート ステータスの表示を行うコマンド

clear ip route {*network* [*mask* | *****]}	1 つまたは複数のルートを IP ルーティング テーブルから消去します。
show ip protocols	アクティブなルーティング プロトコル プロセスのパラメータおよびステートを表示します。
show ip route [*address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]]	ルーティング テーブルの現在の状態を表示します。
show ip route summary	サマリー形式でルーティング テーブルの現在のステータスを表示します。
show ip route supernets-only	スーパーネットを表示します。
show ip cache	IP トラフィックのスイッチングに使用されるルーティング テーブルを表示します。
show route-map [*map-name*]	設定されたすべてのルート マップ、または指定した1つのルートマップだけを表示します。

第 XVII 部

セキュリティ

- 不正アクセスの防止 （1991 ページ）
- パスワードおよび権限レベルによるスイッチ アクセスの制御 （1993 ページ）
- 「Configuring TACACS+」 （2013 ページ）
- MACsec の暗号化 （2029 ページ）
- RADIUS の設定 （2075 ページ）
- RADIUS over DTLS の設定 （2127 ページ）
- Kerberos の設定 （2133 ページ）
- ローカル認証および許可の設定 （2141 ページ）
- セキュア シェル（SSH）の設定 （2147 ページ）
- SSH 認証の X.509v3 証明書 （2159 ページ）
- Secure Socket Layer HTTP の設定 （2169 ページ）
- IPv4 ACL の設定 （2185 ページ）
- IPv6 ACL の設定 （2243 ページ）
- DHCP の設定 （2261 ページ）
- IP ソース ガードの設定 （2285 ページ）
- ダイナミック ARP インスペクションの設定 （2295 ページ）
- IEEE 802.1x ポートベースの認証の設定 （2335 ページ）
- Web ベース認証の設定 （2433 ページ）
- ポート単位のトラフィック制御の設定 （2459 ページ）
- IPv6 ファースト ホップ セキュリティの設定 （2505 ページ）
- Cisco TrustSec の設定 （2553 ページ）

- コントロール プレーン ポリシングの設定 （2559 ページ）
- ワイヤレス ゲスト アクセスの設定 （2575 ページ）
- 不正なデバイスの管理 （2601 ページ）
- 不正なアクセス ポイントの分類 （2623 ページ）
- wIPS の設定 （2633 ページ）
- 侵入検知システムの設定 （2645 ページ）

第 93 章

不正アクセスの防止

- 機能情報の確認 （1991 ページ）
- 不正アクセスの防止 （1991 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

不正アクセスの防止

不正ユーザによる、スイッチの再設定や設定情報の閲覧を防止できます。一般的には、ネットワーク管理者からスイッチへのアクセスを許可する一方、非同期ポートを用いてネットワーク外からダイヤルアップ接続するユーザや、シリアル ポートを通じてネットワーク外から接続するユーザ、またはローカル ネットワーク内の端末またはワークステーションから接続するユーザによるアクセスを制限します。

スイッチへの不正アクセスを防止するには、次のセキュリティ機能を 1 つまたは複数設定します。

- 最低限のセキュリティとして、各スイッチ ポートでパスワードおよび権限を設定します。このパスワードは、スイッチにローカルに保存されます。ユーザがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。
- 追加のセキュリティ レイヤとして、ユーザ名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。このペアは回線またはポートに割り当てられ、

各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

- ユーザ名とパスワードのペアを使用したいが、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティ サーバ上のデータベースに保存できます。これにより、複数のネットワーキング デバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。
- また、失敗したログイン試行をログに記録するログイン拡張機能もイネーブルにすることもできます。ログイン拡張は、設定した回数のログインが失敗したあとに、それ以降のログイン試行をブロックするために設定することもできます。詳細については、『Cisco IOS Login Enhancements』マニュアルを参照してください。

関連トピック

ユーザ名とパスワードのペアの設定 （2004 ページ）
TACACS+ およびスイッチ アクセス （2015 ページ）
端末回線に対する Telnet パスワードの設定 （2002 ページ）

第 94 章

パスワードおよび権限レベルによるスイッチ アクセスの制御

- 機能情報の確認 （1993 ページ）
- パスワードおよび権限によるスイッチ アクセスの制御の制約事項 （1993 ページ）
- パスワードおよび権限レベルに関する情報 （1994 ページ）
- パスワードおよび権限レベルでスイッチ アクセスを制御する方法 （1997 ページ）
- スイッチ アクセスのモニタリング （2009 ページ）
- パスワードおよび権限レベルの設定例 （2009 ページ）
- その他の参考資料 （2011 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

パスワードおよび権限によるスイッチアクセスの制御の制約事項

パスワードおよび権限によるスイッチ アクセスの制御の制約事項は、次のとおりです。

- パスワード回復のディセーブル化は、**boot manual** グローバル コンフィギュレーション コマンドを使用して手動でブートするようにスイッチを設定している場合は無効です。この

コマンドは、スイッチの電源の再投入後、ブートローダプロンプト（*switch:*）を表示させます。

関連トピック

パスワード回復のディセーブル化 （2001 ページ）
パスワードの回復 （1995 ページ）

パスワードおよび権限レベルに関する情報

デフォルトのパスワードおよび権限レベル設定

ネットワークで端末のアクセスコントロールを行う簡単な方法は、パスワードを使用して権限レベルを割り当てることです。パスワード保護によって、ネットワークまたはネットワークデバイスへのアクセスが制限されます。権限レベルによって、ネットワークデバイスにログイン後、ユーザがどのようなコマンドを使用できるかが定義されます。

次の表に、デフォルトのパスワードおよび権限レベル設定を示します。

表 *123 :* デフォルトのパスワードおよび権限レベル設定

機能	デフォルト設定
イネーブルパスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です（特権 EXEC レベル）。パスワードは、コンフィギュレーション ファイル内では暗号化されていない状態です。
イネーブル シークレット パスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です（特権 EXEC レベル）。パスワードは、暗号化されてからコンフィギュレーション ファイルに書き込まれます。
回線パスワード	パスワードは定義されていません。

追加のパスワード セキュリティ

追加のセキュリティ レイヤを、特にネットワークを越えるパスワードや Trivial File Transfer Protocol（TFTP）サーバに保存されているパスワードに対して設定する場合には、**enable password** または **enable secret** グローバル コンフィギュレーション コマンドを使用できます。コマンドの作用はどちらも同じです。このコマンドにより、暗号化されたパスワードを設定できます。特権EXECモード（デフォルト設定）または特定の権限レベルにアクセスするユーザは、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムが使用されるので、**enable secret** コマンドを使用することを推奨します。

enable secret コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

パスワードの暗号化をイネーブルにすると、ユーザ名パスワード、認証キー パスワード、イネーブル コマンド パスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

関連トピック

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 （1998 ページ）
例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 （2010 ページ）

パスワードの回復

スイッチに物理的にアクセスできるエンドユーザは、デフォルトで、スイッチの電源投入時にブート プロセスに割り込み、新しいパスワードを入力することによって、失われたパスワードを回復できます。

パスワード回復ディセーブル化機能では、この機能の一部をディセーブルにすることによりスイッチのパスワードへのアクセスを保護できます。この機能がイネーブルの場合、エンドユーザは、システムをデフォルト設定に戻すことに同意した場合に限り、ブート プロセスに割り込むことができます。パスワード回復をディセーブルにしても、ブート プロセスに割り込んでパスワードを変更できますが、コンフィギュレーション ファイル（config.text）および VLAN データベース ファイル（vlan.dat）は削除されます。

パスワード回復をディセーブルにする場合は、エンド ユーザがブート プロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。VTP（VLAN トランキング プロトコル）トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

パスワードの回復を再びイネーブルにするには、service password-recovery**service password-recovery**グローバル コンフィギュレーション コマンドを使用します。

関連トピック

パスワード回復のディセーブル化 （2001 ページ）
パスワードおよび権限によるスイッチ アクセスの制御の制約事項 （1993 ページ）

端末回線の Telnet 設定

初めてスイッチに電源を投入すると、自動セットアップ プログラムが起動して IP 情報を割り当て、この後続けて使用できるようにデフォルト設定を作成します。さらに、セットアップ プログラムは、パスワードによる Telnet アクセス用にスイッチを設定することを要求します。

セットアッププログラムの実行中にこのパスワードを設定しなかった場合は、端末回線に対する Telnet パスワードを設定するときに設定できます。

関連トピック

端末回線に対する Telnet パスワードの設定 （2002 ページ）
例：端末回線に対する Telnet パスワードの設定 （2010 ページ）

ユーザ名とパスワードのペア

ユーザ名とパスワードのペアを設定できます。このペアはスイッチ上でローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

関連トピック

ユーザ名とパスワードのペアの設定 （2004 ページ）

権限レベル

Cisco スイッチ（および他のデバイス）では、権限レベルを使用して、スイッチ動作の異なるレベルに対してパスワードセキュリティを提供します。デフォルトでは、Cisco IOS ソフトウェアは、パスワード セキュリティの 2 つのモード（権限レベル）で動作します。ユーザ EXEC（レベル 1）および特権 EXEC（レベル 15）です。各モードに、最大 16 個の階層レベルからなるコマンドを設定できます。複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

回線の権限レベル

ユーザは、回線にログインし、別の権限レベルを有効に設定することにより、**privilege level** ライン コンフィギュレーション コマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっていれば、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

たとえば、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 のセキュリティを割り当て、レベル 2 のパスワードを広範囲のユーザに配布できます。また、**configure** コマンドへのアクセス制限を強化する場合は、レベル 3 のセキュリティを割り当て、そのパスワードを限られたユーザ グループに配布することもできます。

コマンド権限レベル

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。たとえば、**show ip traffic** コマンドをレベル 15 に設定すると、**show** コマンドおよび **show ip** コマンドは、それぞれ別のレベルに設定しない限り、自動的にレベル 15 に設定されます。

関連トピック

コマンドの特権レベルの設定 （2006 ページ）
例：コマンドの権限レベルの設定 （2010 ページ）
回線のデフォルト特権レベルの変更 （2007 ページ）
権限レベルへのログインおよび終了 （2008 ページ）

パスワードおよび権限レベルでスイッチアクセスを制御する方法

スタティック イネーブル パスワードの設定または変更

イネーブルパスワードは、特権EXECモードへのアクセスを制御します。スタティック イネーブル パスワードを設定または変更するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**enable password** *password* 例： `Device(config)# enable password secret321`	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 デフォルトでは、パスワードは定義されません。 *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符（?）は、パスワードを作成する場合に、疑問符の前に Ctrl+v を入力す

	コマンドまたはアクション	目的
		れば使用できます。たとえば、パスワード abc?123 を作成するときは、次のようにします。 **1.** **abc** を入力します。 **2.** Ctrl+v を入力します。 **3.** **?123** を入力します。 システムからイネーブル パスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：スタティック イネーブル パスワードの設定または変更 （2009 ページ）

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

特権 EXEC モード（デフォルト）または指定された特権レベルにアクセスするためにユーザが入力する必要がある暗号化パスワードを確立するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかを使用します。
	• `enable password [level` *level*`]` {*password encryption-type encrypted-password*}
	• `enable secret [level` *level*`]` {*password encryption-type encrypted-password*}
	例：
	`Device(config)# enable password example102`
	または
	`Device(config)# enable secret level 1 password secret123sample`
		• 特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。
		• シークレット パスワードを定義します。これは非可逆的な暗号化方式を使用して保存されます。
		• （任意）*level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です（特権 EXEC モード権限）。
		• *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
		• （任意）*encryption-type* には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか使用できません。暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、

	コマンドまたはアクション	目的
		別のスイッチの設定からコピーします。 （注） 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。
ステップ 4	**service password-encryption** 例： `Device(config)# service password-encryption`	（任意）パスワードの定義時または設定の書き込み時に、パスワードを暗号化します。 暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

追加のパスワード セキュリティ （1994 ページ）
例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 （2010 ページ）

パスワード回復のディセーブル化

パスワードの回復をディセーブルにしてスイッチのセキュリティを保護するには、次の手順を実行します。

始める前に

パスワード回復をディセーブルにする場合は、エンド ユーザがブート プロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。VTP（VLAN トランキング プロトコル）トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**system disable password recovery switch** {*all* | *<1-9>*} 例： `Device(config)# system disable password recovery switch all`	パスワード回復をディセーブルにします。 • *all*：スタック内のスイッチで設定を行います。 • *<1-9>*：選択したスイッチ番号で設定を行います。 この設定は、フラッシュ メモリの中で、ブートローダおよび Cisco IOS イメージがアクセスできる領域に保存されますが、ファイル システムには含まれません。また、ユーザがアクセスすることはできません。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

次のタスク

disable password recovery を削除するには、**no system disable password recovery switch all** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

パスワードの回復 （1995 ページ）
パスワードおよび権限によるスイッチ アクセスの制御の制約事項 （1993 ページ）

端末回線に対する Telnet パスワードの設定

接続された端末回線に対する Telnet パスワードを設定するには、ユーザ EXEC モードで次の手順を実行します。

始める前に

- エミュレーション ソフトウェアを備えた PC またはワークステーションをスイッチ コンソール ポートに接続するか、または PC をイーサネット管理ポートに接続します。
- コンソール ポートのデフォルトのデータ特性は、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなしです。コマンドライン プロンプトが表示されるまで、Return キーを何回か押す必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	（注） パスワードが特権 EXEC モードへのアクセスに必要な場合は、その入力が求められます。 特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**line vty 0 15** 例： `Device(config)# line vty 0 15`	Telnet セッション（回線）の数を設定し、ライン コンフィギュレーション モードを開始します。 コマンド対応Deviceでは、最大16のセッションが可能です。0 および 15 を指定すると、使用できる 16 の Telnet セッションすべてを設定することになります。
ステップ 4	**password** *password* 例： `Device(config-line)# password abcxyz543`	1 つまたは複数の回線に対応する Telnet パスワードを設定します。 *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ 5	**end** 例： `Device(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

パスワードおよび権限レベルに関する情報
不正アクセスの防止 （1991 ページ）
端末回線の Telnet 設定 （1995 ページ）
例：端末回線に対する Telnet パスワードの設定 （2010 ページ）

ユーザ名とパスワードのペアの設定

ユーザ名とパスワードのペアを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}
	例：
	`Device(config)# username adamsample privilege 1 password secret456`
	`Device(config)# username 111111111111 mac attribute`
		各ユーザのユーザ名、権限レベル、パスワードを設定します。
		• *name* には、ユーザ ID を 1 ワードで指定するか、または MAC アドレスを指定します。スペースと引用符は使用できません。
		• ユーザ名と MAC フィルタの両方に対し、最大 12000 のクライアントを個別に設定できます。
		• （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。
		• *encryption-type* には、暗号化されていないパスワードが後ろに続く場合は 0 を入力します。暗号化されたパスワードが後ろに続く場合は 7 を指定します。
		• *password* には、Device にアクセスするためにユーザが入力しなければならないパスワードを指定します。パ

	コマンドまたはアクション	目的
		スワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。

ステップ 4	次のいずれかを使用します。
	• **line console 0**
	• **line vty 0 15**
	例：
	`Device(config)# line console 0`
	または
	`Device(config)# line vty 15`
		ライン コンフィギュレーション モードを開始し、コンソール ポート（回線 0）または VTY 回線（回線 0 ～ 15）を設定します。

ステップ 5	**login local** 例： `Device(config-line)# login local`	ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 3 で指定されたユーザ名に基づきます。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

パスワードおよび権限レベルに関する情報
不正アクセスの防止 （1991 ページ）
ユーザ名とパスワードのペア （1996 ページ）

コマンドの特権レベルの設定

コマンドの権限レベルを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**privilege** *mode* **level** *level command* 例： `Device(config)# privilege exec level 14 configure`	コマンドの特権レベルを設定します。 • *mode* には、グローバル コンフィギュレーション モードの場合は **configure** を、EXEC モードの場合は **exec** を、インターフェイス コンフィギュレーション モードの場合は **interface** を、ライン コンフィギュレーション モードの場合は **line** をそれぞれ入力します。 • *level* の範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセスレベルです。 • *command* には、アクセスを制限したいコマンドを指定します。
ステップ 4	**enable password level** *level password* 例： `Device(config)# enable password level 14 SecretPswd14`	権限レベルをイネーブルにするためのパスワードを指定します。 • *level* の範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。 • *password* には、1 ～ 25 文字の英数字のストリングを指定します。スト

	コマンドまたはアクション	目的
		リングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

権限レベル （1996 ページ）
例：コマンドの権限レベルの設定 （2010 ページ）

回線のデフォルト特権レベルの変更

指定した回線のデフォルトの権限レベルを変更するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**line vty** *line* 例： `Device(config)# line vty 10`	アクセスを制限する仮想端末回線を選択します。
ステップ 4	**privilege level** *level* 例： `Device(config)# privilege level 15`	回線のデフォルト特権レベルを変更します。 *level* の範囲は 0 ～ 15 です。 レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

ユーザは、回線にログインし、別の権限レベルをイネーブルに設定することにより、**privilege level** ライン コンフィギュレーション コマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっていれば、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

関連トピック

権限レベル （1996 ページ）

権限レベルへのログインおよび終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、ユーザEXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** *level* 例： `Device> enable 15`	指定された特権レベルにログインします。 この例で、レベル 15 は特権 EXEC モードです。 *level* に指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable** *level* 例： `Device# disable 1`	指定した特権レベルを終了します。 この例で、レベル 1 はユーザ EXEC モードです。 *level* に指定できる範囲は 0 ～ 15 です。

関連トピック

権限レベル （1996 ページ）

スイッチ アクセスのモニタリング

表 *124 : DHCP* 情報を表示するためのコマンド

show privilege	権限レベルの設定を表示します。

パスワードおよび権限レベルの設定例

例：スタティック イネーブル パスワードの設定または変更

次に、イネーブルパスワードを*l1u2c3k4y5*に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モード アクセス）。

```
Device(config)# enable password l1u2c3k4y5
```

関連トピック

スタティック イネーブル パスワードの設定または変更 （1997 ページ）

例：暗号化によるイネーブルおよびイネーブルシークレットパスワードの保護

次に、権限レベル 2 に対して暗号化パスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

```
Device(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

関連トピック

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 （1998 ページ）
追加のパスワード セキュリティ （1994 ページ）

例：端末回線に対する Telnet パスワードの設定

次に、Telnet パスワードを *let45me67in89* に設定する例を示します。

```
Device(config)# line vty 10
Device(config-line)# password let45me67in89
```

関連トピック

端末回線に対する Telnet パスワードの設定 （2002 ページ）
端末回線の Telnet 設定 （1995 ページ）

例：コマンドの権限レベルの設定

configure コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして *SecretPswd14* を定義する例を示します。

```
Device(config)# privilege exec level 14 configure
Device(config)# enable password level 14 SecretPswd14
```

関連トピック

コマンドの特権レベルの設定 （2006 ページ）
権限レベル （1996 ページ）

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 95 章

「Configuring TACACS+」

- 機能情報の確認 （2013 ページ）
- TACACS+ の前提条件 （2013 ページ）
- TACACS+ の概要 （2015 ページ）
- TACACS+ を設定する方法 （2019 ページ）
- TACACS+ のモニタリング （2027 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

TACACS+ の前提条件

TACACS+によるスイッチアクセスのセットアップと設定の前提条件は、次のとおりです（示されている順序で実行する必要があります）。

1. スイッチに TACACS+ サーバ アドレスとスイッチを設定します。
2. 認証キーを設定します。
3. TACACS+ サーバでステップ 2 からキーを設定します。
4. 認証、許可、アカウンティング（AAA）をイネーブルにする。
5. ログイン認証方式リストを作成します。

6. 端末回線にリストを適用します。
7. 認証およびアカウンティング方式のリストを作成します。

TACACS+ によるスイッチ アクセスの制御の前提条件は、次のとおりです。

- スイッチ上で TACACS+ 機能を設定するには、設定済みの TACACS+ サーバにアクセスする必要があります。また、通常 LINUX または Windows ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されている TACACS+ サービスにもアクセスする必要があります。
- スイッチ スタックと TACACS+ サーバとの間に冗長接続を設定することを推奨します。これによって、接続済みのスタック メンバの 1 つがスイッチ スタックから削除された場合でも、TACACS+ サーバにアクセスできます。
- スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼働するシステムが必要です。
- TACACS+ を使用するには、それをイネーブルにする必要があります。
- 許可は、使用するスイッチでイネーブルにする必要があります。
- ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
- この項または他の項で示す AAA コマンドを使用するには、まず **aaa new-model** コマンドを使用して AAA をイネーブルにする必要があります。
- 最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウンティングの方式リストを定義できます。
- 方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。
- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。

関連トピック

TACACS+ の概要 （2015 ページ）
TACACS+ の動作 （2017 ページ）
TACACS+ を設定する方法 （2019 ページ）
方式リスト （2018 ページ）
TACACS+ ログイン認証の設定 （2021 ページ）

TACACS+ ログイン認証 （2018 ページ）
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定 （2024 ページ）
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可 （2018 ページ）

TACACS+ の概要

TACACS+ およびスイッチ アクセス

ここでは、TACACS+ について説明します。TACACS+ は詳細なアカウンティング情報を提供し、認証と許可のプロセスを柔軟に管理します。TACACS+ は、認証、許可、アカウンティング（AAA）機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用する必要があります。

関連トピック

パスワードおよび権限レベルに関する情報
不正アクセスの防止 （1991 ページ）
スイッチのローカル認証および許可の設定 （2141 ページ）
SSH サーバ、統合クライアント、およびサポートされているバージョン （2149 ページ）

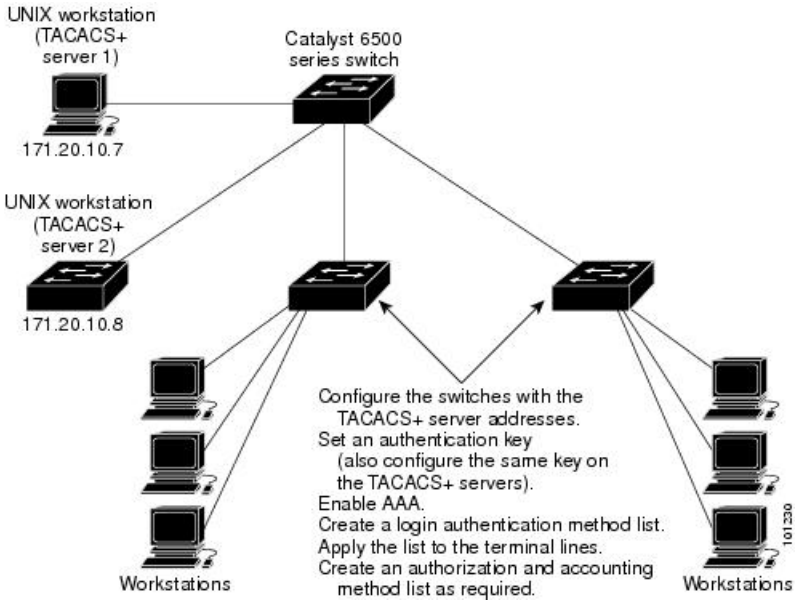
TACACS+ の概要

TACACS+は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）が各サービス（認証、許可、およびアカウンティング）を別個に提供します。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ の目的は、1 つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他の Cisco ルータやアクセス サーバとともにネットワーク アクセス サーバにできます。

図 *104*：一般的な *TACACS+* ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワードダイアログ、チャレンジおよび応答、メッセージサポートによって認証の完全制御を行います。

  認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードが入力された後、自宅の住所、母親の旧姓、サービスタイプ、社会保険番号などのいくつかの質問をすることによりユーザを試します）。TACACS+認証サービスは、ユーザ画面にメッセージを送信することもできます。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。

- 許可：autocommand、アクセス コントロール、セッション期間、プロトコルサポートの設定といった、ユーザ セッション時のユーザ機能についてきめ細かく制御します。また、TACACS+ 許可機能によって、ユーザが実行できるコマンドを制限することもできます。

- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+プロトコルは、スイッチと TACACS+デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

関連トピック

TACACS+ の前提条件 （2013 ページ）

TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1. 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これをユーザに表示します。ユーザがユーザ名を入力すると、スイッチはTACACS+ デーモンに接続してパスワード プロンプトを取得します。スイッチによってパスワード プロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

   TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。

   - ACCEPT：ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
   - REJECT：ユーザは認証されません。TACACS+デーモンに応じて、ユーザはアクセスを拒否されるか、ログイン シーケンスを再試行するように求められます。
   - ERROR：デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
   - CONTINUE：ユーザは、さらに認証情報の入力を求められます。

   認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛ての属性の形式でデータが含まれています。

   - Telnet、セキュア シェル（SSH）、rlogin、または特権 EXEC サービス
   - 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

関連トピック

TACACS+ の前提条件 （2013 ページ）

方式リスト

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティプロトコルを1つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

関連トピック

TACACS+ を設定する方法 （2019 ページ）
TACACS+ の前提条件 （2013 ページ）

TACACS+ 設定オプション

認証用に1つのサーバを使用することも、また、既存のサーバ ホストをグループ化するために AAA サーバ グループを使用するように設定することもできます。サーバをグループ化して設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバ グループは、グローバル サーバ ホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストが含まれています。

関連トピック

TACACS+ サーバ ホストの指定および認証キーの設定 （2020 ページ）

TACACS+ ログイン認証

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する1つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

関連トピック

TACACS+ ログイン認証の設定 （2021 ページ）
TACACS+ の前提条件 （2013 ページ）

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロ

ファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

関連トピック

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定 （2024 ページ）
TACACS+ の前提条件 （2013 ページ）

TACACS+ アカウンティング

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

関連トピック

TACACS+ アカウンティングの起動 （2026 ページ）

TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

（注） TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

TACACS+ を設定する方法

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。

関連トピック

方式リスト （2018 ページ）
TACACS+ の前提条件 （2013 ページ）

TACACS+ サーバ ホストの指定および認証キーの設定

TACACS+ サーバ ホストを特定し、認証キーを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**tacacs-server host** *hostname* 例： `Device(config)# tacacs-server host yourserver`	TACACS+ サーバを維持する IP ホストを特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 *hostname* には、ホストの名前または IP アドレスを指定します。
ステップ 4	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 5	**aaa group server tacacs+** *group-name* 例： `Device(config)# aaa group server tacacs+ your_server_group`	（任意）グループ名で AAA サーバグループを定義します。 このコマンドによって、Deviceをサーバ グループ サブコンフィギュレーション モードにします。
ステップ 6	**server** *ip-address* 例： `Device(config)# server 10.1.2.3`	（任意）特定の TACACS+ サーバを定義済みサーバ グループに関連付けます。AAA サーバ グループの TACACS+ サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 3 で定義済みのものでなければなりません。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

TACACS+ 設定オプション （2018 ページ）

TACACS+ ログイン認証の設定

TACACS+ ログイン認証を設定するには、次の手順を実行します。

始める前に

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。

（注） AAA 方式を使用して HTTP アクセスに対しのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しのセキュリティは確保しません。

ip http authentication コマンドの詳細については、『*Cisco IOS Security Command Reference, Release 12.4*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Device(config)# aaa authentication login default tacacs+ local`	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • *enable*：イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ **enable** *password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。

	コマンドまたはアクション	目的
		• *group tacacs+*：TACACS+ 認証を使用します。この認証方式を使用するには、あらかじめ TACACS+ サーバを設定しておく必要があります。詳細については、TACACS+ サーバ ホストの指定および認証キーの設定（2020 ページ）を参照してください。 • *line*：回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • *local*：ローカルユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • *local-case*：大文字と小文字が区別されるローカルユーザ名データベースを認証に使用します。**username** *name***password** グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 • *none*：ログインに認証を使用しません。
ステップ 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Device(config)# line 2 4`	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 6	**login authentication** {**default** | *list-name*} 例：	1 つの回線または複数回線に認証リストを適用します。

	コマンドまたはアクション	目的
	`Device(config-line)# login authentication default`	• **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 7	**end** 例： `Device(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

TACACS+ ログイン認証 （2018 ページ）
TACACS+ の前提条件 （2013 ページ）

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

aaa authorization グローバル コンフィギュレーション コマンドと **tacacs+** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization network tacacs+** 例： `Device(config)# aaa authorization network tacacs+`	ネットワーク関連のすべてのサービス要求に対してユーザ TACACS+ 認可を行うことを設定します。
ステップ 4	**aaa authorization exec tacacs+** 例： `Device(config)# aaa authorization exec tacacs+`	ユーザの特権 EXEC アクセスに対してユーザ TACACS+ 認可を行うことを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

関連トピック

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可 （2018 ページ）
TACACS+ の前提条件 （2013 ページ）

TACACS+ アカウンティングの起動

TACACS+ アカウンティングを開始するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting network start-stop tacacs+** 例： `Device(config)# aaa accounting network start-stop tacacs+`	ネットワーク関連のすべてのサービス要求について、TACACS+アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting exec start-stop tacacs+** 例： `Device(config)# aaa accounting exec start-stop tacacs+`	TACACS+アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

関連トピック

TACACS+ アカウンティング （2019 ページ）

AAA サーバが到達不能な場合のルータとのセッションの確立

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

TACACS+ のモニタリング

表 *125 : TACACS+* 情報を表示するためのコマンド

コマンド	目的
show tacacs	TACACS+ サーバの統計情報を表示します。

第 96 章

MACsec の暗号化

- 機能情報の確認 （2029 ページ）
- MACsec 暗号化について （2029 ページ）
- MKA および MACsec の設定 （2038 ページ）
- PSK を使用した MACsec MKA の設定 （2043 ページ）
- EAP-TLS を使用した MACsec MKA の理解 （2045 ページ）
- EAP-TLS を使用した MACsec MKA の設定 （2045 ページ）
- Cisco TrustSecMACsec に関する情報 （2064 ページ）
- Cisco TrustSec MACsec の設定 （2066 ページ）
- 設定例 （2068 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

MACsec 暗号化について

この章では、Cisco Catalyst 3850 および 3650 スイッチで Media Access Control Security（MACsec）暗号化を設定する方法について説明します。

MACsec は 2 台の MACsec 対応デバイス間のパケットの認証と暗号化の IEEE 802.1AE 規格です。これらの Catalyst スイッチは、スイッチとホスト デバイス間の暗号化に、ダウンリンク ポートでの MACsec Key Agreement（MKA）による 802.1AE 暗号化をサポートします。また、スイッチは、Cisco TrustSec ネットワーク デバイス アドミッション コントロール（NDAC）、

Security Association Protocol（SAP）および MKA ベースのキー交換プロトコルを使用して、スイッチ間（ネットワーク間デバイス）セキュリティのMACsec暗号化をサポートします。リンク層セキュリティはスイッチ間のパケット認証とスイッチ間のMACsec暗号化の両方を含みます（暗号化は任意です）。

（注） MACsec は NPE ライセンスまたは LAN Base サービス イメージではサポートされません。

表 *126 :* スイッチ ポートの *MACsec* サポート

インターフェイス	Connections	MACsec のサポート
ダウンリンク ポート	スイッチからホストへ	MACsec MKA の暗号化
アップリンク ポート	スイッチからスイッチへ	MACsec MKA の暗号化 Cisco TrustSec NDAC MACsec

Cisco TrustSec と Cisco SAP はスイッチ間のリンクにのみ使用され、PC や IP フォンなどのエンドホストに接続されたスイッチ ポートではサポートされません。MKA は、スイッチからホストへのリンク（ダウンリンク）とスイッチ間リンク（アップリンク）でサポートされます。ホスト側のリンクは、IEEE 802.1x の有無にかかわらず異種デバイスを扱うために、一般に柔軟な認証順序を使用し、オプションで MKA ベースの MACsec 暗号化を使用できます。Cisco NDAC および SAP は、コンパクトなスイッチがワイヤリング クローゼットの外側にセキュリティを拡張するために使用する、ネットワーク エッジ アクセス トポロジ（NEAT）と相互排他的です。

Media Access Control Security と MACsec Key Agreement

802.1AE で定義された MACsec では、暗号化キー入力のためにアウトオブバンド方式を使用することによって、有線ネットワーク上で MAC レイヤの暗号化を実現します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。MKA と MACsec は、802.1x 拡張認証プロトコル（EAP-TLS）または事前共有キー（PSK）フレームワークを使用した認証に成功した後に実装されます。

MACsec を使用するスイッチでは、MKA ピアに関連付けられたポリシーに応じて、MACsec フレームまたは非MACsecフレームを許可します。MACsecフレームは暗号化され、整合性チェック値（ICV）で保護されます。スイッチはMKAピアからフレームを受信すると、MKAによって提供されたセッション キーを使用してこれらのフレームを暗号化し、正しい ICV を計算します。スイッチはこの ICV をフレーム内の ICV と比較します。一致しない場合は、フレームが破棄されます。また、スイッチは現在のセッション キーを使用して、ICV を暗号化し、セキュアなポート（セキュアな MAC サービスを MKA ピアに提供するために使用されるアクセス ポイント）を介して送信されたフレームに追加します。

MKA プロトコルは、基礎となる MACsec プロトコルで使用される暗号キーを管理します。MKA の基本的な要件は 802.1x-REV で定義されています。MKA プロトコルでは 802.1x を拡張

し、相互認証の確認によってピアを検出し、MACsec 秘密キーを共有してピアで交換されるデータを保護できます。

EAP フレームワークでは、新しく定義された EAP-over-LAN（EAPOL）パケットとして MKA を実装します。EAP 認証では、データ交換で両方のパートナーで共有されるマスターセッション キー（MSK）を生成します。EAP セッション ID を入力すると、セキュアな接続アソシエーション キー名（CKN）が生成されます。スイッチは、アップリンクおよびダウンリンクの両方のオーセンティケータとして機能します。また、ダウンリンクのキー サーバとして機能します。これによってランダムなセキュア アソシエーション キー（SAK）が生成され、クライアントパートナーに送信されます。クライアントはキー サーバではなく、単一の MKA エンティティであるキー サーバとだけ対話できます。キーの派生と生成の後で、スイッチは定期的にトランスポートをパートナーに送信します。デフォルトの間隔は 2 秒間です。

EAPOL プロトコル データ ユニット（PDU）のパケット本体は、MACsec Key Agreement PDU（MKPDU）と呼ばれます。MKA セッションと参加者は、MKA ライフタイム（6 秒間）が経過しても参加者から MKPDU を受信していない場合に削除されます。たとえば、MKA ピアが接続を解除した場合、スイッチ上の参加者は MKA ピアから最後の MKPDU を受信した後、6 秒間が経過するまで MKA の動作を継続します。

MKA ポリシー

インターフェイスで MKA を有効にするには、定義された MKA ポリシーをインターフェイスに適用する必要があります。次のオプションを設定可能です。

- 16 ASCII 文字未満のポリシー名。
- 物理インターフェイスごとの 0 バイト、30 バイト、または 50 バイトの機密保持（暗号化）オフセット。

仮想ポート

仮想ポートは、1 つの物理ポート上の複数のセキュアな接続アソシエーションに使用します。各接続アソシエーション（ペア）は仮想ポートを表します。アップリンクでは、物理ポートごとに 1 つの仮想ポートのみを指定できます。ダウンリンクでは、物理ポートごとに最大 2 つの仮想ポートを指定でき、一方の仮想ポートはデータ VLAN の一部にできます。もう一方は音声 VLAN に対してパケットを外部的にタグ付けする必要があります。同じポートで同じ VLAN 内のセキュアなセッションとセキュアでないセッションを同時にホストすることはできません。この制限のため、802.1x マルチ認証モードはサポートされません。

この制限の例外は、マルチホスト モードで最初の MACsec サプリカントが正常に認証され、スイッチに接続されたハブに接続される場合です。ハブに接続された非 MACsec ホストでは、マルチホストモードであるため、認証なしでトラフィックを送信できます。最初にクライアントが成功した後、他のクライアントでは認証が必要ないため、マルチホストモードの使用は推奨しません。

仮想ポートは、接続アソシエーションの任意の ID を表し、MKA プロトコル外では意味を持ちません。仮想ポートは個々の論理ポート ID に対応します。仮想ポートの有効なポート ID は 0x0002 ～ 0xFFFF です。各仮想ポートは、16 ビットのポート ID に連結された物理インターフェイスの MAC アドレスに基づいて、一意のセキュア チャネル ID（SCI）を受け取ります。

MACsec およびスタッキング

MACsec を実行している Catalyst 3850 スイッチ スタック マスターは、MACsec をサポートしているメンバー スイッチ上のポートを示すコンフィギュレーション ファイルを維持します。スタック マスターは、次に示す機能を実行します。

- セキュアなチャネルとセキュアなアソシエーションの作成および削除を処理します。
- スタック メンバーにセキュアなアソシエーション サービス要求を送信します。
- ローカル ポートまたはリモート ポートからのパケット番号とリプレイ ウィンドウ情報を処理し、キー管理プロトコルを通知します。
- オプションがグローバルに設定された MACsec 初期化要求を、スタックに追加される新しいスイッチに送信します。
- ポート単位の設定をメンバー スイッチに送信します。

メンバー スイッチは、次の機能を実行します。

- スタック マスターからの MACsec 初期化要求を処理します。
- スタック マスターから送信された MACsec サービス要求を処理します。
- スタック マスターにローカル ポートに関する情報を送信します。

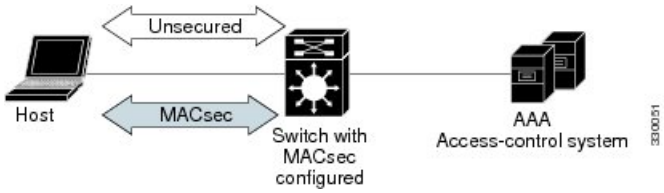
MACsec、MKA、および 802.1x ホスト モード

MACsec と MKA プロトコルは、802.1x シングルホスト モード、マルチホスト モード、またはマルチドメイン認証（MDA）モードで使用できます。マルチ認証モードはサポートされません。

シングルホスト モード

次の図に、MKA を使用して、MACsec で 1 つの EAP 認証済みセッションをセキュアにする方法を示します。

図 *105 :* セキュアなデータ セッションでのシングルホスト モードの *MACsec*

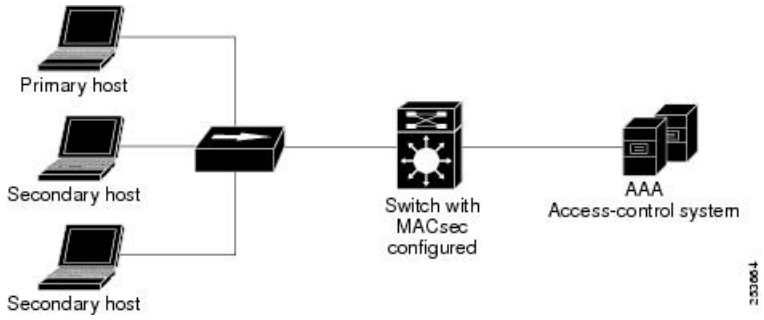


マルチ ホスト モード

標準の（802.1x REV ではない）802.1x マルチホスト モードでは、1 つの認証に基づいてポートが開いているか、閉じられています。1 人のユーザ（プライマリ セキュア クライアント サービスのクライアント ホスト）が認証される場合は、同じポートに接続されているホストに同じレベルのネットワーク アクセスが提供されます。セカンダリ ホストが MACsec サプリカントの場合、認証できず、トラフィック フローは発生しません。非 MACsec ホストであるセカンダリ ホストは、マルチホスト モードであるため、認証なしでネットワークにトラフィックを

送信できます。次の図に、標準のマルチホスト非セキュア モードにおける MACsec を示します。

図 *106*：マルチホスト モードの *MACsec*：非セキュア



（注） マルチホストモードは推奨されていません。これは最初にクライアントが成功した後、他のクライアントでは認証が必要ないことから、安全性が低いためです。

標準の（802.1x REV ではない）802.1x マルチドメイン モードでは、1 つの認証に基づいてポートが開いているか、閉じられています。プライマリ ユーザ（データ ドメインの PC）が認証されると、同じレベルのネットワーク アクセスが同じポートに接続されているドメインに提供されます。セカンダリ ユーザが MACsec サプリカントの場合、認証できず、トラフィック フローは発生しません。非 MACsec ホストであるセカンダリ ユーザ（音声ドメインの IP フォン）は、マルチドメイン モードであるため、認証なしでネットワークにトラフィックを送信できます。

MKA 統計情報

一部の MKA カウンタはグローバルに集約され、その他のカウンタはグローバルとセッション単位の両方で更新されます。また、MKA セッションのステータスに関する情報も取得できます。

次の例では、**show mka statistics** コマンドの出力を示します。

```
Switch# show mka sessions

Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=======================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server
Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN
=======================================================================================
Gi1/0/1        204c.9e85.ede4/002b p2               NO                YES
43             c800.8459.e764/002a 1                Secured
01000000000000000000000000000000000000000000000000000000000000000000

Switch#show mka sessions interface G1/0/1

Summary of All Currently Active MKA Sessions on Interface GigabitEthernet1/0/1...

=======================================================================================
```

```
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server
Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN
==========================================================================================
Gi1/0/1        204c.9e85.ede4/002b p2               NO                YES
43             c800.8459.e764/002a 1                Secured
0100000000000000000000000000000000000000000000000000000000000000


Switch#show mka sessions interface G1/0/1 de

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier...... 43
Interface Name........... GigabitEthernet1/0/1
Audit Session ID.........
CAK Name (CKN)........... 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)...... 89567
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)

MKA Policy Name.......... p2
Key Server Priority...... 2
Delay Protection......... NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------
  38046BA37D7DA77E06D006A9  89555       c800.8459.e764/002a   10

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------

Switch#show mka sessions de
```

```
Switch#show mka sessions detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier...... 43
Interface Name........... GigabitEthernet1/0/1
Audit Session ID.........
CAK Name (CKN)........... 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)...... 89572
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)

MKA Policy Name.......... p2
Key Server Priority...... 2
Delay Protection......... NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------
  38046BA37D7DA77E06D006A9  89560       c800.8459.e764/002a   10

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------

Switch#sh mka pol

MKA Policy Summary...

Policy            KS       Delay   Replay  Window Conf   Cipher          Interfaces
Name              Priority Protect Protect Size   Offset Suite(s)        Applied
=============================================================================================
*DEFAULT POLICY*  0        FALSE   TRUE    0      0      GCM-AES-128
```

```
p1                1        FALSE   TRUE    0      0      GCM-AES-128

p2                2        FALSE   TRUE    0      0      GCM-AES-128     Gi1/0/1


Switch#sh mka poli
Switch#sh mka policy p2
Switch#sh mka policy p2 ?
  detail    Detailed configuration/information for MKA Policy
  sessions  Summary of all active MKA Sessions with policy applied
  |         Output modifiers
  <cr>

Switch#sh mka policy p2 de

MKA Policy Configuration ("p2")
=======================
MKA Policy Name........ p2
Key Server Priority.... 2
Confidentiality Offset. 0
Cipher Suite(s)........ GCM-AES-128

Applied Interfaces...
  GigabitEthernet1/0/1

Switch#sh mka policy p2

MKA Policy Summary...

Policy            KS       Delay   Replay  Window Conf   Cipher          Interfaces
Name              Priority Protect Protect Size   Offset Suite(s)        Applied
==============================================================================================
p2                2        FALSE   TRUE    0      0      GCM-AES-128     Gi1/0/1


Switch#sh mka se?
sessions

Switch#sh mka ?
  default-policy  MKA Default Policy details
  keychains       MKA Pre-Shared-Key Key-Chains
  policy          MKA Policy configuration information
  presharedkeys   MKA Preshared Keys
  sessions        MKA Sessions summary
  statistics      Global MKA statistics
  summary         MKA Sessions summary & global statistics

Switch#sh mka statis
Switch#sh mka statistics ?
  interface  Statistics for a MKA Session on an interface
  local-sci  Statistics for a MKA Session identified by its Local Tx-SCI
  |          Output modifiers
  <cr>

Switch#sh mka statistics inter
Switch#show mka statistics interface G1/0/1

MKA Statistics for Session
==========================
Reauthentication Attempts.. 0

CA Statistics
   Pairwise CAKs Derived... 0
   Pairwise CAK Rekeys..... 0
```

```
   Group CAKs Generated.... 0
   Group CAKs Received..... 0

SA Statistics
   SAKs Generated.......... 1
   SAKs Rekeyed............ 0
   SAKs Received........... 0
   SAK Responses Received.. 1

MKPDU Statistics
   MKPDUs Validated & Rx... 89585
      "Distributed SAK".. 0
      "Distributed CAK".. 0
   MKPDUs Transmitted...... 89596
      "Distributed SAK".. 1
      "Distributed CAK".. 0


Switch#show mka ?
  default-policy  MKA Default Policy details
  keychains       MKA Pre-Shared-Key Key-Chains
  policy          MKA Policy configuration information
  presharedkeys   MKA Preshared Keys
  sessions        MKA Sessions summary
  statistics      Global MKA statistics
  summary         MKA Sessions summary & global statistics

Switch#show mka summ
Switch#show mka summary

Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

==========================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server
Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN
==========================================================================================
Gi1/0/1        204c.9e85.ede4/002b p2               NO                YES
43             c800.8459.e764/002a 1                Secured
01000000000000000000000000000000000000000000000000000000000000000000



MKA Global Statistics
======================
MKA Session Totals
   Secured.................... 1
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 0
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated............. 1
   SAKs Rekeyed............... 0
   SAKs Received.............. 0
   SAK Responses Received..... 1
```

```
MKPDU Statistics
   MKPDUs Validated & Rx...... 89589
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 89600
      "Distributed SAK"..... 1
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Session Failures
   Bring-up Failures................ 0
   Reauthentication Failures........ 0
   Duplicate Auth-Mgr Handle........ 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0
   SAK Cipher Mismatch.............. 0

CA Failures
   Group CAK Generation............. 0
   Group CAK Encryption/Wrap........ 0
   Group CAK Decryption/Unwrap...... 0
   Pairwise CAK Derivation.......... 0
   CKN Derivation................... 0
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability... 0
MACsec Failures
   Rx SC Creation................... 0
   Tx SC Creation................... 0
   Rx SA Installation............... 0
   Tx SA Installation............... 0

MKPDU Failures
   MKPDU Tx......................... 0
   MKPDU Rx Validation.............. 0
   MKPDU Rx Bad Peer MN............. 0
   MKPDU Rx Non-recent Peerlist MN.. 0

Switch#
```

MKA および MACsec の設定

MACsec MKA のデフォルト設定

MACsec はディセーブルです。MKA ポリシーは設定されていません。

MKA ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mka policy** *policy name*	MKA ポリシーを指定し、MKA ポリシー コンフィギュレーション モードを開始します。ポリシー名の長さは最大で 16 文字です。 （注） MKA ポリシー内のデフォルトの MACsec 暗号スイートは常に「GCM-AES-128」です。デバイスが「GCM-AES-128」および「GCM-AES-256」の両方の暗号方式をサポートしている場合は、ユーザ定義の MKA ポリシーを定義して使用し、必要に応じて、128 および 256 ビット両方の暗号を含めるか、または 256 ビットのみの暗号を含めることを強くお勧めします。
ステップ 3	**key-server** *priority*	MKA キー サーバ オプションを設定し、プライオリティを設定します（0 ～ 255 の間）。 （注） キー サーバ プライオリティの値を 255 に設定した場合、ピアはキー サーバになることはできません。
ステップ 4	**macsec-cipher-suite** *gcm-aes-128*	128 ビット暗号により SAK を取得するための暗号スイートを設定します。
ステップ 5	**confidentiality-offset** *Offset value*	各物理インターフェイスに機密性（暗号化）オフセットを設定します。

	コマンドまたはアクション	目的
		（注） オフセット値は、0、30、または50を指定できます。クライアントで Anyconnect を使用している場合は、オフセット 0 を使用することをお勧めします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mka policy**	入力内容を確認します。

例

次に、MKA ポリシーを設定する例を示します。

```
Switch(config)# mka policy mka_policy
Switch(config-mka-policy)# key-server priority 200
Switch(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Switch(config-mka-policy)# confidentiality-offset 30
Switch(config-mka-policy)# end
```

インターフェイスでの MACsec の設定

音声用に 1 つの MACsec セッションとデータ用に 1 つの MACsec セッションが存在するインターフェイスで MACsec を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch>enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Switch>configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	MACsec インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。インターフェイスは物理インターフェイスでなければなりません。

	コマンドまたはアクション	目的
ステップ 4	**switchport access vlan***vlan-id*	このポートのアクセス VLAN を設定します。
ステップ 5	**switchport mode access**	インターフェイスをアクセスポートとして設定します。
ステップ 6	**macsec**	インターフェイスで 802.1ae MACsec をイネーブルにします。macsec コマンドを使用すると、スイッチからホストへのリンク（ダウンリンク ポート）でのみ MKA MACsec が有効になります。
ステップ 7	**authentication event linksec fail action authorize vlan** *vlan-id*	（任意）認証の試行に失敗した後で、ポート上の制限付き VLAN を許可することによって、ユーザ証明書が認識されない認証リンク セキュリティの問題をスイッチが処理することを指定します。
ステップ 8	**authentication host-mode multi-domain**	ホストと音声デバイスの両方が、802.1x で許可されたポート上で認証されるように、ポート上の認証マネージャ モードを設定します。設定されていない場合、デフォルトのホストモードはシングルです。
ステップ 9	**authentication linksec policy must-secure**	LinkSec セキュリティ ポリシーを設定して、ピアを利用できる場合に、MACsec でセッションをセキュアにします。設定されていない場合、デフォルト値は *should secure* です。
ステップ 10	**authentication port-control auto**	ポート上で 802.1x 認証をイネーブルにします。スイッチとクライアント間の認証交換に基づいてポートが許可ステートまたは無許可ステートに変わります。
ステップ 11	**authentication periodic**	このポートの再認証を有効または無効にします。
ステップ 12	**authentication timer reauthenticate**	1 から 65535 までの値（秒）を入力します。サーバから再認証タイムアウト値を取得します。デフォルトの再認証時間は 3600 秒です。

	コマンドまたはアクション	目的
ステップ 13	**authentication violation protect**	新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続されたあとに新しいデバイスがそのポートに接続された場合に、予期しない着信 MAC アドレスを破棄するようポートを設定します。設定されていない場合、デフォルトではポートをシャット ダウンします。
ステップ 14	**mka policy** *policy name*	既存の MKA プロトコル ポリシーをインターフェイスに適用し、インターフェイス上で MKA をイネーブルにします。MKA ポリシーを設定しなかった場合（**mka policy** グローバル コンフィギュレーション コマンドを入力して）。
ステップ 15	**dot1x pae authenticator**	ポートを 802.1x ポート アクセス エンティティ（PAE）オーセンティケータとして設定します。
ステップ 16	**spanning-tree portfast**	関連するすべての VLAN 内の特定のインターフェイスで、スパニングツリー Port Fast をイネーブルにします。Port Fast機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。
ステップ 17	**end** 例： `Switch(config)#end`	特権 EXEC モードに戻ります。
ステップ 18	**show authentication session interface** *interface-id*	許可されたセッションのセキュリティ ステータスを確認します。
ステップ 19	**show authentication session interface** *interface-id* details	承認されたセッションのセキュリティ ステータスの詳細を確認します。
ステップ 20	**show macsec interface** *interface-id*	インターフェイスの MacSec ステータスを確認します。
ステップ 21	**show mka sessions**	確立された mka セッションを確認します。

	コマンドまたはアクション	目的
ステップ 22	**copy running-config startup-config** 例： `Switch#copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

PSK を使用した MACsec MKA の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**key chain** *key-chain-name* **macsec**	キー チェーンを設定して、キー チェーン コンフィギュレーション モードを開始します。
ステップ 3	**key** *hex-string*	キーチェーン内の各キーの固有識別子を設定し、キーチェーンのキー コンフィギュレーション モードを開始します。 （注） 128 ビット暗号の場合は、32 文字の 16 進数キー文字列を使用します。256 ビット暗号の場合は、64 文字の 16 進数キー文字列を使用します。
ステップ 4	**cryptographic-algorithm** *{gcm-aes-128 | gcm-aes-256}*	128 ビットまたは 256 ビット暗号による暗号化認証アルゴリズムを設定します。
ステップ 5	**key-string** *{ [0|6|7] pwd-string | pwd-string}*	キー文字列のパスワードを設定します。16 進数の文字のみを入力する必要があります。
ステップ 6	**lifetime local** [*start timestamp {hh::mm::ss | day | month | year}*] [**duration** *seconds* | *end timestamp {hh::mm::ss | day | month | year}*]	事前共有キーの有効期間を設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

例

次に例を示します。

```
Switch(config)# Key chain keychain1 macsec
Switch(config-key-chain)# key 1000
Switch(config-keychain-key)# cryptographic-algorithm gcm-aes-128
Switch(config-keychain-key)# key-string 12345678901234567890123456789012
Switch(config-keychain-key)# lifetime local 12:12:00 July 28 2016 12:19:00
July 28 2016
Switch(config-keychain-key)# end
```

PSK を使用した、インターフェイスでの MACsec MKA の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**mka policy** *policy-name*	MKA ポリシーを設定します。
ステップ 4	**mka pre-shared-key key-chain** *key-chain name*	MKA 事前共有キーのキーチェーン名を設定します。 （注） MKA 事前共有キーは、物理インターフェイスまたはサブインターフェイスで設定できますが、両方で設定することはできません。
ステップ 5	**macsec replay-protection window-size** *frame number*	リプレイ保護の MACsec ウィンドウ サイズを設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

例

次に例を示します。

```
Switch(config)# interface GigabitEthernet 0/0/0
Switch(config-if)# mka policy mka_policy
Switch(config-if)# mka pre-shared-key key-chain key-chain-name
```

```
Switch(config-if)# macsec replay-protection window-size 10
Switch(config-if)# end
```

EAP-TLS を使用した MACsec MKA の理解

Cisco IOS リリース 15.2(5)E 以降、MACsec MKA は、Cisco Catalyst 3850 および 3650 シリーズスイッチのスイッチ間リンクでサポートされています。

Extensible Authentication Protocol（EAP-TLS）による IEE 802.1X ポートベース認証を使用して、デバイスのアップリンク ポート間で MACsec MKA を設定できます。EAP-TLS は相互認証を許可し、MSK（マスターセッション キー）を取得します。そのキーから、MKA 操作用の接続アソシエーション キー（CAK）が取得されます。デバイスの証明書は、AAA サーバへの認証用に、EAP-TLS を使用して伝送されます。

EAP-TLS を使用した MACsec MKA の前提条件

- 認証局（CA）サーバがネットワークに設定されていることを確認します。
- CA 証明書を生成します。
- Cisco Identity Services Engine（ISE）リリース 2.0 が設定されていることを確認します。
- 両方の参加デバイス（CA サーバと Cisco Identity Services Engine（ISE））が Network Time Protocol（NTP）を使用して同期されていることを確認します。時間がすべてのデバイスで同期されていないと、証明書は検証されません。
- 802.1x 認証と AAA がデバイスに設定されていることを確認します。

EAP-TLS を使用した MACsec MKA の制限事項

- MKA は、ポート チャネルではサポートされていません。
- MKA は、高可用性とローカル認証ではサポートされていません。

EAP-TLS を使用した MACsec MKA の設定

ポイントツーポイント リンクで MKA による MACsec を設定するには、次のタスクを実行します。

- 証明書登録の設定
  - キー ペアの生成
  - SCEP 登録の設定
  - 証明書の手動設定

- 認証ポリシーの設定
- EAP-TLS プロファイルおよび IEEE 802.1x クレデンシャルの設定
- インターフェイスでの EAP-TLS を使用した MACsec MKA の設定

リモート認証

キー ペアの生成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**crypto key generate rsa label** *label name* **general-keys modulus** *size*	署名および暗号化用に RSA キー ペアを作成します。 label キーワードを使用すると、各キー ペアにラベルを割り当てることもできます。このラベルは、キー ペアを使用するトラストポイントによって参照されます。ラベルを割り当てなかった場合、キー ペアには <Default-RSA-Key> というラベルが自動的に付けられます。 追加のキーワードを使用しない場合、このコマンドは汎用 RSA キー ペアを 1 つ生成します。係数が指定されていない場合は、デフォルトのキー係数である 1024 が使用されます。その他の係数サイズを指定するには、modulus キーワードを使用します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show authentication session interface** *interface-id*	許可されたセッションのセキュリティ ステータスを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SCEP による登録の設定

Simple Certificate Enrollment Protocol（SCEP）は、HTTP を使用して認証局（CA）または登録局（RA）と通信する、シスコが開発した登録プロトコルです。SCEP は、要求および証明書の送受信用に最も一般的に使用される方式です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 3	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 4	**rsakeypair** *label*	証明書に関連付けるキーペアを指定します。 （注） **rsakeypair** 名は、信頼ポイント名と一致している必要があります。
ステップ 5	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 6	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 7	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。

	コマンドまたはアクション	目的
ステップ 8	**auto-enroll** *percent* **regenerate**	自動登録をイネーブルにします。これにより、クライアントは CA から自動的にロールオーバー証明書を要求できます。 自動登録がイネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。 デフォルトでは、デバイスのドメインネームシステム（DNS）名だけが証明書に含められます。 現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、percent 引数を使用します。 名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、regenerate キーワードを使用します。 ロールオーバー中のキーペアがエクスポート可能な場合、新しいキーペアもエクスポート可能です。次のコメントがトラストポイントコンフィギュレーションに表示され、キーペアがエクスポート可能かどうかが示されます。「! RSA key pair associated with trustpoint is exportable.」 新しいキーペアは、セキュリティ上の問題に対処するために生成することを推奨します。
ステップ 9	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 10	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 11	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。

登録の手動設定

CA が SCEP をサポートしない場合、またはルータと CA 間のネットワーク接続が不可能な場合。手動での証明書登録を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーションモードを開始します。
ステップ 3	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 4	**rsakeypair** *label*	証明書に関連付けるキーペアを指定します。
ステップ 5	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 6	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 7	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 8	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 9	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 10	**crypto pki enroll** *name*	証明書要求を生成し、証明書サーバにコピーおよびペーストするために要求を表示します。 プロンプトが表示されたら、登録情報を入力します。たとえば、証明書要求

	コマンドまたはアクション	目的
		にデバイスの FQDN および IP アドレスを含めるかどうかを指定します。 コンソール端末に対して証明書要求を表示するかについても選択できます。 必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。
ステップ 11	**crypto pki import** *name* **certificate**	許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。 デバイスは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場合、拡張子「-sign.crt」および「-encr.crt」が使用されます。 デバイスは、受信したファイルを解析して証明書を検証し、証明書をスイッチの内部証明書データベースに挿入します。 （注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキーペアのいずれも使用しません。
ステップ 12	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 13	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

802.1x 認証の有効化と AAA の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**dot1x system-auth-control**	デバイス上で 802.1X を有効にします。
ステップ 5	**radius server** *name*	RADIUS サーバの設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。
ステップ 6	**address** *ip-address* **auth-port** *port-number* **acct-port** *port-number*	RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。
ステップ 7	**automate-tester username** *username*	RADIUS サーバの自動テスト機能を有効にします。 このようにすると、デバイスは RADIUS サーバにテスト認証メッセージを定期的に送信し、サーバからの RADIUS 応答を待機します。成功メッセージは必須ではありません。認証失敗であっても、サーバが稼働していることを示しているため問題ありません。
ステップ 8	**key** *string*	デバイスと RADIUS サーバとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。
ステップ 9	**radius-server deadtime** 分	いくつかのサーバが使用不能になったときの RADIUS サーバの応答時間を短くし、使用不能になったサーバがすぐにスキップされるようにします。

	コマンドまたはアクション	目的
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**aaa group server radius** *group-name*	異なる RADIUS サーバホストを別々のリストと方式にグループ化し、サーバグループ コンフィギュレーション モードを開始します。
ステップ 12	**server** *name*	RADIUS サーバ名を割り当てます。
ステップ 13	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**aaa authentication dot1x default group** *group-name*	IEEE 802.1x 用にデフォルトの認証サーバ グループを設定します。
ステップ 15	**aaa authorization network default group** *group-name*	ネットワーク認証のデフォルト グループを設定します。

EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**eap profile** *profile-name*	EAP プロファイルを設定し、EAP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**method tls**	デバイスで EAP-TLS 方式を有効にします。
ステップ 5	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**dot1x credentials** *profile-name*	802.1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。
ステップ 8	**username** *username*	認証ユーザ ID を設定します。
ステップ 9	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

インターフェイスでの 802.1x MACsec MKA 設定の適用

EAP-TLS を使用して MACsec MKA をインターフェイスに適用するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	MACsec インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理インターフェイスでなければなりません。
ステップ 3	**macsec network-link**	インターフェイス上で MACsec をイネーブルにします。
ステップ 4	**authentication periodic**	このポートの再認証をイネーブルにします。
ステップ 5	**authentication timer reauthenticate interval**	再認証間隔を設定します。
ステップ 6	**access-session host-mode multi-domain**	ホストにインターフェイスへのアクセスを許可します。
ステップ 7	**access-session closed**	インターフェイスへの事前認証アクセスを防止します。
ステップ 8	**access-session port-control auto**	ポートの認可状態を設定します。
ステップ 9	**dot1x pae both**	ポートを 802.1X ポート アクセス エンティティ（PAE）のサプリカントおよ

	コマンドまたはアクション	目的
		びオーセンティケータとして設定します。
ステップ 10	**dot1x credentials profile**	802.1x クレデンシャル プロファイルをインターフェイスに割り当てます。
ステップ 11	**dot1x supplicant eap profile** *name*	EAP-TLS プロファイルをインターフェイスに割り当てます。
ステップ 12	**service-policy type control subscriber** *control-policy name*	インターフェイスに加入者制御ポリシーを適用します。
ステップ 13	**exit**	特権 EXEC モードに戻ります。
ステップ 14	**show macsec interface**	インターフェイスの MACsec の詳細を表示します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

ローカル認証

ローカル認証を使用した EAP クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa local authentication default authorization default**	デフォルトのローカル認証およびデフォルトのローカル認証方法を設定します。
ステップ 5	**aaa authentication dot1x default local**	IEEE 802.1x 用にデフォルトのローカルユーザ名認証リストを設定します。

	コマンドまたはアクション	目的
ステップ 6	**aaa authorization network default local**	ローカル ユーザの認可方式リストを設定します。
ステップ 7	**aaa authorization credential-download default local**	ローカル クレデンシャルの使用に関する認可方式リストを設定します。
ステップ 8	**exit**	特権 EXEC モードに戻ります。

ローカル EAP-TLS 認証と認証プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**dot1x credentials** *profile-name*	dot1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。
ステップ 5	**username** *name* **password** *password*	認証のユーザ ID およびパスワードを設定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**aaa attribute list** *list-name*	（任意）AAA 属性リスト定義を設定し、属性リスト コンフィギュレーション モードを開始します。
ステップ 8	**aaa attribute type linksec-policy must-secure**	（任意）AAA 属性タイプを指定します。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**username** *name* **aaa attribute list** *name*	（任意）ユーザ ID に AAA 属性リストを指定します。

	コマンドまたはアクション	目的
ステップ 11	**end**	特権 EXEC モードに戻ります。

SCEP による登録の設定

Simple Certificate Enrollment Protocol（SCEP）は、HTTP を使用して認証局（CA）または登録局（RA）と通信する、シスコが開発した登録プロトコルです。SCEP は、要求および証明書の送受信用に最も一般的に使用される方式です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーションモードを開始します。
ステップ 4	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 5	**rsakeypair** *label*	証明書に関連付けるキーペアを指定します。 （注） **rsakeypair** 名は、信頼ポイント名と一致している必要があります。
ステップ 6	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。

	コマンドまたはアクション	目的
ステップ 7	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 8	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 9	**auto-enroll** *percent* **regenerate**	自動登録をイネーブルにします。これにより、クライアントは CA から自動的にロールオーバー証明書を要求できます。 自動登録がイネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。 デフォルトでは、デバイスのドメインネームシステム（DNS）名だけが証明書に含められます。 現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、percent 引数を使用します。 名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、regenerate キーワードを使用します。 ロールオーバー中のキーペアがエクスポート可能な場合、新しいキーペアもエクスポート可能です。次のコメントがトラストポイントコンフィギュレーションに表示され、キーペアがエクスポート可能かどうかが示されます。「! RSA key pair associated with trustpoint is exportable.」 新しいキーペアは、セキュリティ上の問題に対処するために生成することを推奨します。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**exit**	グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 12	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。

登録の手動設定

CA が SCEP をサポートしない場合、またはルータと CA 間のネットワーク接続が不可能な場合。手動での証明書登録を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーションモードを開始します。
ステップ 4	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 5	**rsakeypair** *label*	証明書に関連付けるキーペアを指定します。
ステップ 6	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 7	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。

	コマンドまたはアクション	目的
ステップ 8	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法としてCRLを指定します。
ステップ 9	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**crypto pki enroll** *name*	証明書要求を生成し、証明書サーバにコピーおよびペーストするために要求を表示します。 プロンプトが表示されたら、登録情報を入力します。たとえば、証明書要求にデバイスの FQDN および IP アドレスを含めるかどうかを指定します。 コンソール端末に対して証明書要求を表示するかについても選択できます。 必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。
ステップ 12	**crypto pki import** *name* **certificate**	許可された証明書を取得するコンソール端末で、TFTPによって証明書をインポートします。 デバイスは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場合、拡張子「-sign.crt」および「-encr.crt」が使用されます。 デバイスは、受信したファイルを解析して証明書を検証し、証明書をスイッチの内部証明書データベースに挿入します。

	コマンドまたはアクション	目的
		（注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキーペアのいずれも使用しません。
ステップ 13	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 14	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**eap profile** *profile-name*	EAP プロファイルを設定し、EAP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**method tls**	デバイスで EAP-TLS 方式を有効にします。
ステップ 5	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。

	コマンドまたはアクション	目的
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**dot1x credentials** *profile-name*	802.1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。
ステップ 8	**username** *username*	認証ユーザ ID を設定します。
ステップ 9	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

インターフェイスでの 802.1x MKA MACsec 設定の適用

EAP-TLS を使用して MKA MACsec をインターフェイスに適用するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	MACsec インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理インターフェイスでなければなりません。
ステップ 4	**macsec**	インターフェイス上で MACsec をイネーブルにします。
ステップ 5	**authentication periodic**	このポートの再認証をイネーブルにします。
ステップ 6	**authentication timer reauthenticate interval**	再認証間隔を設定します。

	コマンドまたはアクション	目的
ステップ 7	**access-session host-mode multi-domain**	ホストにインターフェイスへのアクセスを許可します。
ステップ 8	**access-session closed**	インターフェイスへの事前認証アクセスを防止します。
ステップ 9	**access-session port-control auto**	ポートの認可状態を設定します。
ステップ 10	**dot1x pae both**	ポートを 802.1X ポート アクセス エンティティ（PAE）のサプリカントおよびオーセンティケータとして設定します。
ステップ 11	**dot1x credentials profile**	802.1x クレデンシャル プロファイルをインターフェイスに割り当てます。
ステップ 12	**dot1x authenticator eap profile** *name*	EAP-TLS オーセンティケータ プロファイルをインターフェイスに割り当てます。
ステップ 13	**dot1x supplicant eap profile** *name*	EAP-TLS サプリカント プロファイルをインターフェイスに割り当てます。
ステップ 14	**service-policy type control subscriber** *control-policy name*	インターフェイスに加入者制御ポリシーを適用します。
ステップ 15	**exit**	特権 EXEC モードに戻ります。
ステップ 16	**show macsec interface**	インターフェイスの MACsec の詳細を表示します。
ステップ 17	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

EAP-TLS を使用した MACsec MKA の確認

EAP-TLS を使用して MACsec MKA の設定を確認するには、次の **show** コマンドを使用します。以下に、**show** コマンドの出力例を示します。

show mka sessions コマンドは、アクティブな MACsec Key Agreement（MKA）プロトコルのセッションの概要を表示します。

```
Device# show mka sessions

  Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0
```

```
==========================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server

Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN

==========================================================================================
Te0/1/3        74a2.e625.4413/0013 *DEFAULT POLICY* NO                YES

19             74a2.e625.4c22/0012 1                Secured
1000000000000000000000000000000000000000000000000000000000000000
```

show macsec status interface *interface-id* は、指定されたインターフェイスの MACsec ステータス情報を表示します。

```
Device# show macsec status interface te0/1/2

  Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256
  Cipher:                   GCM-AES-128
  Confidentiality Offset:   0
  Replay Window:            64
  Delay Protect Enable:     FALSE
  Access Control:           must-secure

Transmit SC:
  SCI:                      74A2E6254C220012
  Transmitting:             TRUE
Transmit SA:
  Next PN:                  412
  Delay Protect AN/nextPN:  99/0

Receive SC:
  SCI:                      74A2E62544130013
  Receiving:                TRUE
Receive SA:
  Next PN:                  64
  AN:                       0
  Delay Protect AN/LPN:     0/0
```

show access-session interface *interface-id***details** は、指定されたインターフェイスのアクセス セッションに関する詳細情報を表示します。

```
Device# show access-session interface te1/0/1 details

   Interface:  TenGigabitEthernet1/0/1
             IIF-ID:  0x17298FCD
         MAC Address:  f8a5.c592.13e4
        IPv6 Address:  Unknown
        IPv4 Address:  Unknown
           User-Name:  DOT1XCRED
              Status:  Authorized
              Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  000000000000000BB72E8AFA
      Acct Session ID:  Unknown
              Handle:  0xc3000001
       Current Policy:  MUSTS_1
```

```
Local Policies:
 Security Policy:  Must Secure
      Security Status:  Link Secured

Server Policies:


Method status list:
       Method           State
     dot1xSup           Authc Success
        dot1x           Authc Success
```

Cisco TrustSecMACsec に関する情報

次の表に、TrustSec がイネーブルになった Cisco スイッチで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability リリースによって、サポートされるスイッチの数および各スイッチでサポートされる TrustSec 機能の数は増加しています。

Cisco TrustSec の機能	説明
802.1AE タギング（MACSec）	IEEE 802.1AE に基づくワイヤレート ホップ単位レイヤ 2 暗号化のプロトコル。 MACSec 対応デバイス間において、パケットは送信デバイスからの出力で暗号化され、受信デバイスへの入力で復号化されます。デバイス内では平文です。 この機能は、TrustSec ハードウェア対応デバイス間だけで利用できます。 （注） この機能は 2960x ではサポートされていません。
エンドポイント アドミッション コントロール（EAC）	EAC は、TrustSec ドメインに接続しているエンドポイント ユーザまたはデバイスの認証プロセスです。通常、EAC はアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可に成功すると、ユーザまたはデバイスに対してセキュリティ グループ タグが割り当てられます。現在、EAC は 802.1X、MAC 認証バイパス（MAB）、および Web 認証プロキシ（WebAuth）とすることができます。

Cisco TrustSec の機能	説明
ネットワーク デバイス アドミッション コントロール（NDAC）	NDAC は、TrustSec ドメイン内の各ネットワーク デバイスがピア デバイスのクレデンシャルおよび信頼性を確認できる認証プロセスです。NDAC は、IEEE 802.1X ポート ベースの認証に基づく認証フレームワークを利用し、EAP 方式として EAP-FAST を使用します。NDAC プロセスの認証および許可に成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションとなります。 （注） この機能は 2960x ではサポートされていません。
セキュリティ アソシエーション プロトコル（SAP）	NDAC 認証のあと、セキュリティ アソシエーション プロトコル（SAP）は、その後の TrustSec ピア間の MACSec リンク暗号化のキーおよび暗号スイートについて、自動的にネゴシエーションを行います。SAP は IEEE 802.11i で定義されます。
セキュリティ グループ タグ（SGT）	SGT は、TrustSec ドメイン内の送信元のセキュリティ分類を示す 16 ビットの単一ラベルです。イーサネット フレームまたは IP パケットに追加されます。
SGT 交換プロトコル（SXP）	Security Group Tag Exchange Protocol（SXP）。SXP を使用すると、TrustSec にハードウェアで対応していないデバイスが Cisco Identity Services Engine（ISE）または Cisco Secure アクセス コントロール システム（ACS）から認証されたユーザとデバイスの SGT 属性を受信できます。デバイスは、次にセキュリティ グループ アクセス コントロール リスト（SGACL）強制のために、送信元トラフィックをタグ付けする TrustSec にハードウェアで対応しているデバイスに、sourceIP-to-SGT バインディングを転送できます。

リンクの両端で 802.1AE MACsec をサポートしている場合、SAP ネゴシエーションが実行されます。サプリカントとオーセンティケータの間で EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティパラメータの交換、およびキーの管理が実行されます。これらの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョンとライセンスおよびリンク ハードウェア サポートに応じて、SAP ネゴシエーションは次の動作モードの 1 つを使用できます。

- Galois Counter Mode（GCM）：認証と暗号化
- GCM authentication（GMAC）：GCM 認証、暗号化なし
- No Encapsulation：カプセル化なし（クリア テキスト）
- null：カプセル化、認証または暗号化なし

Cisco TrustSec MACsec の設定

手動モードでの Cisco TrustSec スイッチ間リンク セキュリティの設定

始める前に

インターフェイスの Cisco TrustSec を手動で設定する場合は、次のような使用上の注意事項、および制約事項を考慮してください。

- SAP パラメータが定義されていない場合、Cisco TrustSec カプセル化または暗号化は行われません。
- SAP 動作モードとして GCM を選択すると、シスコの MACsec 暗号化ソフトウェア ライセンスが必要です。必要なライセンスなしで GCM を選択した場合、インターフェイスはリンク ダウン状態になります。
- これらの保護レベルは、SAP の Pairwise Master Key（sap pmk）を設定する場合にサポートされます。
  - SAP が設定されていない：保護は行われません。
  - **sap mode-list gcm-encrypt gmac no-encap**：保護が望ましいが必須ではない。
  - **sap mode-list gcm-encrypt gmac**：機密性が推奨され、整合性が必須。保護はサプリカントの設定に応じてサプリカントによって選択されます。
  - **sap mode-list gmac**：整合性のみ。
  - **sap mode-list gcm-encrypt**：機密性が必須。
  - **sap mode-list gmac gcm-encrypt**：整合性が必須であり推奨される。機密性は任意。

別の Cisco TrustSec デバイスへのインターフェイスで Cisco TrustSec を手動で設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface tengigabitethernet 1/1/2`	（注） インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**cts manual** 例： `Switch(config-if)# cts manual`	Cisco TrustSec 手動コンフィギュレーション モードを開始します。
ステップ 4	**sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]] 例： `Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap`	（任意）SAP の Pairwise Master Key（PMK）と動作モードを設定します。Cisco TrustSec の手動モードでは、SAP はデフォルトでディセーブルになっています。 • *key*：文字数が偶数個で最大 32 文字の 16 進値。 SAP 動作モードのオプションは次のとおりです。 • **gcm-encrypt**：認証および暗号化 （注） ソフトウェア ライセンスが MACsec 暗号化をサポートする場合、MACsec の認証と暗号化にこのモードを選択します。 • **gmac**：認証、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化、認証または暗号化なし （注） インターフェイスでデータ リンク暗号化を使用できない場合は、デフォルトおよび唯一使用可能な SAP 動作モードは **no-encap** です。SGT はサポートされません。
ステップ 5	**no propagate sgt** 例：	ピアが SGT を処理できない場合、このコマンドの **no** 形式を使用します。**no propagate sgt** コマンドを使用すると、イ

	コマンドまたはアクション	目的
	`Switch(config-if-cts-manual)# no propagate sgt`	ンターフェイスからピアに SGT が送信されなくなります。
ステップ 6	**exit** 例： `Switch(config-if-cts-manual)# exit`	Cisco TrustSec 802.1x インターフェイス コンフィギュレーション モードを終了します。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show cts interface** [*interface-id* | **brief** | **summary**]	（任意）TrustSec 関連のインターフェイス特性を表示して、設定を確認します。

例

次に、インターフェイスにCisco TrustSec認証を手動モードで設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# end
```

設定例

インターフェイスでの MACsec の設定

音声用に 1 つの MACsec セッションとデータ用に 1 つの MACsec セッションが存在するインターフェイスで MACsec を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch>enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Switch>configure terminal`	
ステップ 3	**interface** *interface-id*	MACsec インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。インターフェイスは物理インターフェイスでなければなりません。
ステップ 4	**switchport access vlan***vlan-id*	このポートのアクセス VLAN を設定します。
ステップ 5	**switchport mode access**	インターフェイスをアクセスポートとして設定します。
ステップ 6	**macsec**	インターフェイスで 802.1ae MACsec をイネーブルにします。macsec コマンドを使用すると、スイッチからホストへのリンク（ダウンリンク ポート）でのみ MKA MACsec が有効になります。
ステップ 7	**authentication event linksec fail action authorize vlan** *vlan-id*	（任意）認証の試行に失敗した後で、ポート上の制限付き VLAN を許可することによって、ユーザ証明書が認識されない認証リンク セキュリティの問題をスイッチが処理することを指定します。
ステップ 8	**authentication host-mode multi-domain**	ホストと音声デバイスの両方が、802.1x で許可されたポート上で認証されるように、ポート上の認証マネージャ モードを設定します。設定されていない場合、デフォルトのホストモードはシングルです。
ステップ 9	**authentication linksec policy must-secure**	LinkSec セキュリティ ポリシーを設定して、ピアを利用できる場合に、MACsec でセッションをセキュアにします。設定されていない場合、デフォルト値は *should secure* です。
ステップ 10	**authentication port-control auto**	ポート上で 802.1x 認証をイネーブルにします。スイッチとクライアント間の認証交換に基づいてポートが許可ステートまたは無許可ステートに変わります。

	コマンドまたはアクション	目的
ステップ 11	**authentication periodic**	このポートの再認証を有効または無効にします。
ステップ 12	**authentication timer reauthenticate**	1 から 65535 までの値（秒）を入力します。サーバから再認証タイムアウト値を取得します。デフォルトの再認証時間は 3600 秒です。
ステップ 13	**authentication violation protect**	新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続されたあとに新しいデバイスがそのポートに接続された場合に、予期しない着信 MAC アドレスを破棄するようポートを設定します。設定されていない場合、デフォルトではポートをシャット ダウンします。
ステップ 14	**mka policy** *policy name*	既存の MKA プロトコル ポリシーをインターフェイスに適用し、インターフェイス上で MKA をイネーブルにします。MKA ポリシーを設定しなかった場合（**mka policy** グローバル コンフィギュレーション コマンドを入力して）。
ステップ 15	**dot1x pae authenticator**	ポートを 802.1x ポート アクセス エンティティ（PAE）オーセンティケータとして設定します。
ステップ 16	**spanning-tree portfast**	関連するすべての VLAN 内の特定のインターフェイスで、スパニングツリー Port Fast をイネーブルにします。Port Fast機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。
ステップ 17	**end** 例： `Switch(config)#end`	特権 EXEC モードに戻ります。
ステップ 18	**show authentication session interface** *interface-id*	許可されたセッションのセキュリティ ステータスを確認します。

	コマンドまたはアクション	目的
ステップ 19	**show authentication session interface** *interface-id* details	承認されたセッションのセキュリティステータスの詳細を確認します。
ステップ 20	**show macsec interface** *interface-id*	インターフェイスの MacSec ステータスを確認します。
ステップ 21	**show mka sessions**	確立された mka セッションを確認します。
ステップ 22	**copy running-config startup-config** 例： `Switch#copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

EAP-TLS を使用した MACsec MKA の設定例

例:：証明書の登録

```
Configure Crypto PKI Trustpoint:
  crypto pki trustpoint POLESTAR-IOS-CA
   enrollment terminal
   subject-name CN=ASR1000x1@polestar.com, C=IN, ST=KA, OU=ENG,O=Polestar
   revocation-check none
   rsakeypair mkaioscarsa
   storage nvram:
  !
Manual Installation of Root CA certificate:
 crypto pki authenticate POLESTAR-IOS-CA
```

例：802.1x 認証の有効化と AAA の設定

```
aaa new-model
dot1x system-auth-control
radius server ISE
 address ipv4 <ISE ipv4 address> auth-port 1645 acct-port 1646
 automate-tester username dummy
 key dummy123
 radius-server deadtime 2
!
aaa group server radius ISEGRP
 server name ISE
!
aaa authentication dot1x default group ISEGRP
aaa authorization network default group ISEGRP
```

例：EAP-TLS プロファイルと 802.1x クレデンシャルの設定

```
eap profile EAPTLS-PROF-IOSCA
 method tls
 pki-trustpoint POLESTAR-IOS-CA
!

dot1x credentials EAPTLSCRED-IOSCA
 username asr1000@polestar.company.com
 pki-trustpoint POLESTAR-IOS-CA
!
```

例：インターフェイスでの 802.1 X、PKI、および MACsec の設定の適用

```
interface TenGigabitEthernet0/1
 macsec network-link
 authentication periodic
 authentication timer reauthenticate <reauthentication interval>
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 dot1x pae both
 dot1x credentials EAPTLSCRED-IOSCA
 dot1x supplicant eap profile EAPTLS-PROF-IOSCA
 service-policy type control subscriber DOT1X_POLICY_RADIUS
```

Cisco TrustSec スイッチ間リンク セキュリティの設定例

次に、Cisco TrustSec スイッチ間のセキュリティのためにシードおよび非シード デバイスに必要な設定を示します。リンク セキュリティ用に AAA および RADIUS を設定する必要があります。この例では、ACS-1 から ACS-3 は任意のサーバ名、cts-radius は Cisco TrustSec サーバです。

シード デバイスの設定

```
Switch(config)#aaa new-model
Switch(config)#radius server ACS-1
Switch(config-radius-server)#address ipv4 10.5.120.12 auth-port 1812 acct-port
 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#radius server ACS-2
Switch(config-radius-server)#address ipv4 10.5.120.14 auth-port 1812 acct-port
 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#radius server ACS-3
Switch(config-radius-server)#address ipv4 10.5.120.15 auth-port 1812 acct-port
 1813
Switch(config-radius-server)#pac key cisco123
```

```
Switch(config-radius-server)#exit
Switch(config)#aaa group server radius cts-radius
Switch(config-sg-radius)#server name ACS-1
Switch(config-sg-radius)#server name ACS-2
Switch(config-sg-radius)#server name ACS-3
Switch(config-sg-radius)#exit
Switch(config)#aaa authentication login default none
Switch(config)#aaa authentication dot1x default group cts-radius
Switch(config)#aaa authorization network cts-radius group cts-radius
Switch(config)#aaa session-id common
Switch(config)#cts authorization list cts-radius
Switch(config)#dot1x system-auth-control

Switch(config)#interface gi1/1/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#cts dot1x
Switch(config-if-cts-dot1x)#sap mode-list gcm-encrypt gmac

Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit

Switch(config)#interface gi1/1/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#cts manual
Switch(config-if-cts-dot1x)#sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
 gmac
Switch(config-if-cts-dot1x)#no propagate sgt
Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit

Switch(config)#radius-server vsa send authentication
Switch(config)#end
Switch#cts credentials id cts-36 password trustsec123
```

非シード デバイス

```
Switch(config)#aaa new-model
Switch(config)#aaa session-id common
Switch(config)#dot1x system-auth-control

Switch(config)#interface gi1/1/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#shutdown
Switch(config-if)#cts dot1x
Switch(config-if-cts-dot1x)#sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit

Switch(config)#interface gi1/1/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#shutdown
Switch(config-if)#cts manual
Switch(config-if-cts-dot1x)#sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
 gmac
Switch(config-if-cts-dot1x)#no propagate sgt
```

```
Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit

Switch(config)#radius-server vsa send authentication
Switch(config)#end
Switch(config)#cts credentials id cts-72 password trustsec123
```

第 97 章

RADIUS の設定

- 機能情報の確認 （2075 ページ）
- RADIUS を設定するための前提条件 （2075 ページ）
- RADIUS の設定に関する制約事項 （2076 ページ）
- RADIUS に関する情報 （2077 ページ）
- RADIUS の設定方法 （2106 ページ）
- CoA 機能のモニタリング （2123 ページ）
- その他の参考資料 （2124 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

RADIUS を設定するための前提条件

ここでは、RADIUS による Device アクセスの制御の前提条件を示します。

General:

- この章のいずれかのコンフィギュレーション コマンドを使用するには、RADIUS および認証、許可、ならびにアカウンティング（AAA）をイネーブルにする必要があります。
- RADIUS は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。
- 最低限、RADIUS サーバ ソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS認証の方式リストを定義する必要があります。また、任意でRADIUS許可およびアカウンティングの方式リストを定義できます。
- Device 上でRADIUS機能の設定を行う前に、RADIUSサーバにアクセスし、サーバを設定する必要があります。
- RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーのRADIUSサーバ ソフトウェアが稼働しているマルチユーザ システムです。詳細については、RADIUSサーバのマニュアルを参照してください。
- Change-of-Authorization（CoA）インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。CoA を使用すると、セッションの識別と接続解除要求を実行できます。アップデートは、指定されたセッションにだけ作用します。
- スイッチ スタックと RADIUS サーバとの間に冗長接続を設定することを推奨します。これによって、接続済みのスタック メンバの 1 つがスイッチ スタックから削除された場合でも、RADIUS サーバにアクセスできます。

RADIUS 操作の場合：

- ユーザは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります（イネーブルに設定されている場合）。

関連トピック

RADIUS およびスイッチ アクセス （2077 ページ）
RADIUS の動作 （2078 ページ）

RADIUS の設定に関する制約事項

ここでは、RADIUS による Device アクセスの制御の制約事項について説明します。

General:

- セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。

RADIUS は次のネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は、AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

関連トピック

RADIUS の概要 （2077 ページ）

RADIUS に関する情報

RADIUS およびスイッチ アクセス

この項では、RADIUS をイネーブルにし、設定する方法について説明します。RADIUS を使用すると、アカウンティングの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます。

関連トピック

RADIUS を設定するための前提条件 （2075 ページ）
スイッチのローカル認証および許可の設定 （2141 ページ）
SSH サーバ、統合クライアント、およびサポートされているバージョン （2149 ページ）

RADIUS の概要

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。RADIUS クライアントは、サポート対象の Cisco ルータおよびスイッチ上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。

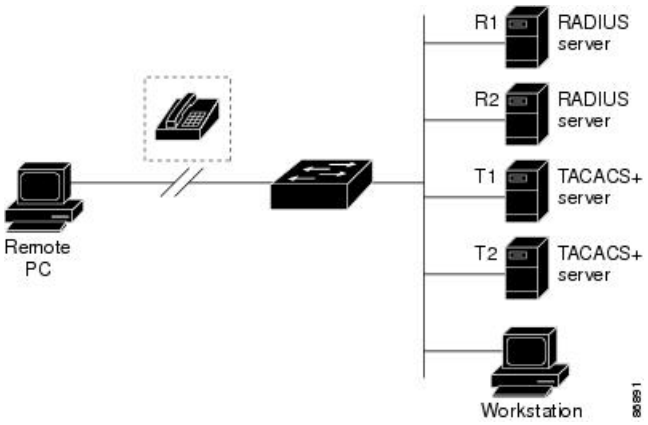
RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カード アクセス コントロール システムを使用するアク

セス環境。あるケースでは、RADIUS は Enigma のセキュリティ カードとともに使用してユーザを確認し、ネットワーク リソースのアクセスを許可します。

- すでに RADIUS を使用中のネットワーク。RADIUS クライアント装備のシスコ Deviceをネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。下の図 2「RADIUS サービスから TACACS+ サービスへの移行」を参照してください。
- ユーザが 1 つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1x などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、第 11 章「IEEE 802.1x ポートベース認証の設定」を参照してください。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

図 *107 : RADIUS* サービスから *TACACS+* サービスへの移行



関連トピック

RADIUS の設定に関する制約事項 （2076 ページ）

RADIUS の動作

RADIUS サーバによってアクセス コントロールされるDeviceに、ユーザがログインおよび認証を試みると、次のイベントが発生します。

1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由でRADIUSサーバに送信されます。

3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   - ACCEPT：ユーザが認証されたことを表します。
   - REJECT：ユーザの認証が失敗し、ユーザ名およびパスワードの再入力が要求されるか、またはアクセスが拒否されます。
   - CHALLENGE：ユーザに追加データを要求します。
   - CHALLENGE PASSWORD：ユーザは新しいパスワードを選択するように要求されます。

   ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

関連トピック

RADIUS を設定するための前提条件 （2075 ページ）

RADIUS 許可の変更

RADIUS 許可の変更（CoA）は、認証、認可、およびアカウンティング（AAA）セッションの属性を認証された後に変更するためのメカニズムを提供します。AAA でユーザ、またはユーザ グループのポリシーが変更された場合、管理者は、AAA サーバから Cisco Secure Access Control Server（ACS）などの RADIUS CoA パケットを送信し、認証を再初期化して新しいポリシーを適用することができます。このセクションでは、使用可能なプリミティブおよびそれらの CoA での使用方法を含む、RADIUS インターフェイスの概要について説明します。

- Change-of-Authorization 要求
- CoA 要求応答コード
- CoA 要求コマンド
- セッション再認証
- セッション強制終了のスタック構成ガイドライン

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。Catalyst は、RFC 5176 で規定された（通常はプッシュ モデルで使用される）RADIUS CoA 拡張機能をサポートし、外部の AAA またはポリシー サーバからのセッションを動的に再設定できるようにします。

は、次のセッション単位の CoA 要求をサポートしています。

- セッション再認証
- セッション終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了

この機能は、Cisco Secure Access Control Server (ACS) 5.1 に統合されています。

Catalyst で、RADIUS インターフェイスはデフォルトでイネーブルに設定されています。ただし、次の属性については、一部の基本的な設定が必要になります。

- セキュリティおよびパスワード：このガイドの「スイッチへの不正アクセスの防止」を参照してください。
- アカウンティング：このガイドの「スイッチベース認証の設定」の章の「RADIUS アカウンティングの起動」の項を参照してください。

Cisco IOS ソフトウェアは、RFC 5176 で定義されている RADIUS CoA の拡張をサポートします。この拡張は、一般に、外部 AAA またはポリシー サーバからのセッションのダイナミックな再構成を可能にするプッシュ モデルで使用されます。セッションの特定、セッションの終了、ホストの再認証、ポートのシャットダウン、およびポートバウンスでは、セッションごとの CoA 要求がサポートされます。このモデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgement（ACK）[CoA-ACK]
- CoA nonacknowledgement（NAK）[CoA-NAK]

要求は CoA クライアント（通常は AAA またはポリシー サーバ）から開始されて、リスナーとして動作するデバイスに転送されます。

次の表は、Identity-Based Networking Services でサポートされている RADIUS CoA コマンドとベンダー固有属性（VSA）を示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 *127 : Identity-Based Networking Services* でサポートされている *RADIUS CoA* コマンド

CoA コマンド	シスコの VSA
サービスのアクティブ化	Cisco:Avpair="subscriber:command=activate-service" Cisco:Avpair="subscriber:service-name=<*service-name*>" Cisco:Avpair="subscriber:precedence=<*precedence-number*>" Cisco:Avpair="subscriber:activation-mode=replace-all"
Deactivate service	Cisco:Avpair="subscriber:command=deactivate-service" Cisco:Avpair="subscriber:service-name=<*service-name*>"
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"

CoA コマンド	シスコの VSA
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Session query	Cisco:Avpair=“subscriber:command=session-query”
Session reauthenticate	Cisco:Avpair="subscriber:command=reauthenticate" Cisco:Avpair=“subscriber:reauthenticate-type=last” または Cisco:Avpair=“subscriber:reauthenticate-type=rerun”
Session terminate	これは、VSA を必要としない、標準の接続解除要求です。
Interface template	Cisco:AVpair="interface-template-name=<*interfacetemplate*>"

Change-of-Authorization 要求

Change of Authorization（CoA）要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。このモデルは、1 つの要求（CoA-Request）と 2 つの可能な応答コードで構成されています。

- CoA acknowledgment（ACK）[CoA-ACK]
- CoA non-acknowledgment（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から発信されて、リスナーとして動作するスイッチに送信されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してスイッチでサポートされています。

次の表に、この機能でサポートされている IETF 属性を示します。

表 *128*：サポートされている *IETF* 属性

Attribute Number	属性名
24	状態
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 *129 : Error-Cause* の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット（無視）
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求（プロキシ）
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチ セッションの選択がサポートされてない

CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。属性フィールドは、シスコのベンダー固有属性（VSA）を送信するために使用します。

関連トピック

CoA 要求コマンド （2084 ページ）

セッションの識別

特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id VSA（シスコの VSA）
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）
- 次のいずれかの IPv6 属性。
  - Framed-IPv6-Prefix（IETF 属性 #97）および Framed-Interface-Id（IETF 属性 #96）。ともに RFC 3162 に従った完全な IPv6 アドレスを作成する
  - Framed-IPv6-Address
- プレーン IP アドレス（IETF 属性 #8）

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、スイッチは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

複数のセッション ID 属性がメッセージ含まれる場合は、すべての属性がセッションと一致しなければなりません。そうでない場合は、スイッチが Disconnect - negative acknowledgement（NAK）または CoA -NAK と、「Invalid Attribute Value」エラー コードを返します。

RFC 5176 で定義されている CoA 要求コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                         Authenticator                         |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

属性フィールドは、シスコのベンダー固有属性（VSA）を送信するために使用します。

特定の適用ポリシーを対象とする CoA 要求の場合、上記のセッション ID 属性のいずれかがメッセージに含まれていると、デバイスはエラー コードが「Invalid Attribute Value」の CoA-NAK を返します。

関連トピック

CoA 接続解除要求 （2085 ページ）
CoA 要求：ホスト ポートのディセーブル化 （2086 ページ）
CoA 要求：バウンス ポート （2086 ページ）

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なり、個々の CoA コマンドで検討されます。

CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。CoA が成功したかを確認するには、**show** コマンドを使用します。

CoA 要求コマンド

表 *130 :* でサポートされる *CoA* コマンド

コマンド [8]	シスコの VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	これは、VSA を要求しない、標準の接続解除要求です。
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

[8] すべての CoA コマンドには、と CoA クライアント間のセッション識別情報が含まれている必要があります。

関連トピック

CoA 要求応答コード （2082 ページ）

セッション再認証

不明な ID またはポスチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファイル（たとえば、ゲスト VLAN）に関連付けられると、AAA サーバは通常、セッション再認証要求を生成します。再認証要求は、クレデンシャルが不明である場合にホストが適切な認証グループに配置されることを許可します。

セッション認証を開始するために、AAA サーバは *Cisco:Avpair="subscriber:command=reauthenticate"* の形式で Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。

現在のセッションステートは、メッセージに対するスイッチの応答を決定します。セッションが現在、IEEE 802.1x によって認証されている場合、スイッチは EAPOL（LAN 経由の拡張認証プロトコル）RequestId メッセージをサーバに送信することで応答します。

現在、セッションが MAC 認証バイパス（MAB）で認証されている場合は、スイッチはサーバにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

スイッチがコマンドを受信したときにセッション認証が実行中である場合は、スイッチはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションがまだ認証されてない、あるいはゲストVLAN、クリティカルVLAN、または同様のポリシーで認証されている場合は、再認証メッセージがアクセス コントロール方式を再開し、最初に試行されるように設定された方式で開始します。セッションの現在の許可は、再認証によって異なる認証結果になるまで維持されます。

スイッチ スタックでのセッションの再認証

スイッチ スタックでセッション再認証メッセージを受信すると、次の動作が発生します。

- 確認応答（ACK）を戻す前に、再認証の必要性がチェックされます。
- 適切なセッションで再認証が開始されます。
- 認証が成功または失敗のいずれかで完了すると、再認証をトリガーする信号がスタック メンバから削除されます。
- 認証の完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、再認証が開始されます。
- ACK の送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再転送コマンドが新しいコマンドとして扱われます。

セッションの終了

セッションを終了させる 3 種類の CoA 要求があります。CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。このコマンドを使用すると、指定されたホストのオーセンティケータ ステート マシンが再初期化されますが、そのホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA の設定で CoA 要求を使用します。このコマンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であり、そのホストに対してネットワーク アクセスをただちにブロックする必要があります。ポートへのネットワーク アクセスを復旧する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

プリンタなどのサプリカントを持たないデバイスが新しい IP アドレスを取得する必要がある場合（たとえば、VLAN 変更後）は、ポート バウンスでホスト ポート上のセッションを終了します（ポートを一時的にディセーブルした後、再びイネーブルにする）。

CoA 接続解除要求

このコマンドは標準の接続解除要求です。セッションが見つからない場合、スイッチは Disconnect-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。セッションがある場合は、スイッチはセッションを終了します。セッションが完全に削除された後、スイッチは接続解除 ACK を返します。

スイッチがクライアントに接続解除 ACK を返す前にスタンバイ スイッチにフェールオーバーする場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。再送信後もセッションが見つからない場合は、Disconnect-ACK と「Session Context Not Found」エラー コード属性が送信されます。

関連トピック

セッションの識別 （2083 ページ）

CoA 要求：ホスト ポートのディセーブル化

RADIUS サーバの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元するには、非 RADIUS メカニズムを使用して再びイネーブルにします。このコマンドは、次の新しいベンダー固有属性（VSA）が含まれている標準 CoA 要求メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチは CoA-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。このセッションがある場合は、スイッチはホスト ポートをディセーブルにし、CoA-ACK メッセージを返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

（注） 再送信コマンドの後に接続解除要求が失敗すると、（接続解除 ACK が送信されてない場合に）チェンジオーバー前にセッションが正常終了し、または元のコマンドが実行されてスタンバイ スイッチがアクティブになるまでの間に発生した他の方法（たとえば、リンク障害）によりセッションが終了することがあります。

関連トピック

セッションの識別 （2083 ページ）

CoA 要求：バウンス ポート

RADIUS サーバの CoA bounce port が RADIUS サーバから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチはCoA-NAKメッセージと「Session Context Not Found」エラー コード属性を返します。このセッションがある場合は、スイッチはホストポートを10秒間ディセーブルし、再びイネーブルにし（ポートバウンス）、CoA-ACK を返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブスイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブスイッチ上でその動作が再開されます。

関連トピック

セッションの識別 （2083 ページ）

セッション強制終了のスタック構成ガイドライン

スイッチ スタックでは、CoA 接続解除要求メッセージに必要な特別な処理はありません。

CoA 要求バウンス ポートのスタック構成 ガイドライン

bounce-port コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

スタック マスターで Auth Manager コマンド ハンドラが有効な **bounce-port** コマンドを受信すると、CoA-ACK メッセージを返す前に次の情報が確認されます。

- ポート バウンスの必要性
- ポート ID（ローカル セッション コンテキストで検出された場合）

スイッチで、ポート バウンスが開始されます（ポートが 10 秒間ディセーブルになり、再びイネーブルにされます）。

ポート バウンスが正常に実行された場合、ポート バウンスをトリガーした信号がスタンバイ スタック マスターから削除されます。

ポート バウンスの完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、ポート バウンスが開始されます。

CoA-ACK メッセージの送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再送信コマンドが新しいコマンドとして扱われます。

CoA 要求ディセーブル ポートのスタック構成 ガイドライン

disable-port コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

スタック マスターにある Auth Manager コマンド ハンドラで、有効な **disable-port** コマンドを受信した場合、CoA-ACK メッセージを返す前に次の情報が検証されます。

- ポート ディセーブルの必要性
- ポート ID（ローカル セッション コンテキストで検出された場合）

スイッチで、ポートをディセーブルする操作が試行されます。

ポートをディセーブルする操作が正常に実行された場合、ポートをディセーブルする操作をトリガーした信号がスタンバイ スタック マスターから削除されます。

ポートをディセーブルする操作の完了前にスタックマスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタックマスターの切り替え後、ポートがディセーブルにされます。

CoA-ACK メッセージの送信前にスタック マスターに障害が発生した場合、新たなスタックマスターでは、再送信コマンドが新しいコマンドとして扱われます。

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用してRADIUSを設定することはできません。RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

RADIUS サーバ ホスト

スイッチと RADIUS サーバの通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS ホストとして個々のポートを定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホストエントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホストエントリは、最初に設定したホストエントリのフェールオーバー バックアップとして動作します。この例では、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、スイッチは「%RADIUS-4-RADIUS_DEAD」メッセージを表示し、その後、同じデバイス上で 2 番めに設

定されたホスト エントリでアカウンティング サービスを試みます（RADIUS ホスト エントリは、設定した順序に従って試行されます）。

RADIUS サーバとスイッチは、共有するシークレット テキスト ストリングを使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバデーモンが稼働するホストと、そのホストがスイッチと共有するシークレット テキスト（キー）ストリングを指定する必要があります。

タイムアウト、再送信回数、および暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定することもできますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単位での設定を組み合わせることもできます。

関連トピック

RADIUS サーバ ホストの識別 （2106 ページ）
AAA サーバ グループの定義 （2111 ページ）
すべての RADIUS サーバの設定 （2116 ページ）
RADIUS ログイン認証の設定 （2108 ページ）

RADIUS ログイン認証

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外は、デフォルトの方式リストです。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

関連トピック

RADIUS ログイン認証の設定 （2108 ページ）

AAA Server Groups

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意の ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の異なる UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバ上の異なる 2 つのホストエントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じデバイス上でアカウンティング サービス用に設定されている 2 番めのホスト エントリを試行します。（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

関連トピック

AAA サーバ グループの定義 （2111 ページ）

AAA Authorization

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可をイネーブルにすると、スイッチは（ローカル ユーザ データベースまたはセキュリティ サーバ上に存在する）ユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

関連トピック

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定 （2113 ページ）

RADIUS アカウンティング

AAA アカウンティング機能は、ユーザが使用したサービスと、消費したネットワーク リソース量を追跡します。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で RADIUS セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。

関連トピック

RADIUS アカウンティングの起動 （2114 ページ）

ベンダー固有の RADIUS 属性

Internet Engineering Task Force（IETF）ドラフト規格に、ベンダー固有の属性（属性 26）を使用して、スイッチと RADIUS サーバ間でベンダー固有の情報を通信するための方式が定められています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、こ

の仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを1つサポートしています。シスコのベンダーIDは9であり、サポート対象のオプションはベンダータイプ1（名前は *cisco-avpair*）です。この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

protocol は、特定の認証タイプに使用するシスコのプロトコル属性の値です。 *attribute* および *value* は、シスコの TACACS+ 仕様で定義されている、該当の属性値（AV）ペアです。*sep* は、必須の属性の場合は =、任意指定の属性の場合は * です。TACACS+ 認証で使用できるすべての機能は、RADIUS でも使用できます。

たとえば、次の AV ペアにより、IP 認証中（PPP の IPCP アドレス割り当て中）には、シスコの「multiple named IP address pools」機能がアクティブになります。

```
cisco-avpair= ”ip:addr-pool=first“
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」はオプションになります。AV ペアはオプションにすることが可能である、ということに注意してください。

```
cisco-avpair= ”ip:addr-pool*first“
```

次に、ネットワーク アクセス サーバからユーザがログインしたらすぐに EXEC コマンドが実行されるようにする方法の例を示します。

```
cisco-avpair= ”shell:priv-lvl=15“
```

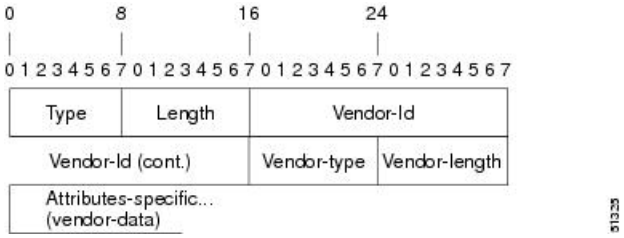
他のベンダーにも、それぞれ独自のベンダー ID、オプション、および関連する VSA があります。ベンダー ID および VSA の詳細については、RFC 2138『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

属性 26 には、次の 3 つの要素が含まれています。

- タイプ
- 長さ
- ストリング（またはデータ）
  - Vendor-Id
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

次の図は、属性 26 の「背後で」カプセル化される VSA のパケット形式を示します。

図 *108 :* 属性 *26* の背後でカプセル化される *VSA*



（注） VSA の形式はベンダーが指定します。Attribute-Specific フィールド（Vendor-Data とも呼ばれる）は、ベンダーによるその属性の定義によって異なります。

次の表に、「ベンダー固有 RADIUS IETF 属性テーブル」（次の 2 番目の表）で表示される重要なフィールドを示します。これは、サポート対象のベンダー固有 RADIUS 属性（IETF 属性 26）を表示します。

表 *131 :* ベンダー固有属性表のフィールドの説明

フィールド	説明
Number	次の表に示されるすべての属性は、IETF 属性 26 の拡張です。
Vendor-Specific Command Codes	特定のベンダーの識別に使用する定義されたコード。コード 9 は Cisco VSA、311 は Microsoft VSA、529 は Ascend VSA を定義します。
Sub-Type Number	属性 ID 番号。この番号は、属性 26 の背後でカプセル化される「2 番めのレイヤ」の ID 番号であること以外、IETF 属性の ID 番号に似ています。
Attribute	属性の ASCII ストリング名。
説明	属性の説明。

表 *132 :* ベンダー固有 *RADIUS IETF* 属性

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
MS-CHAP 属性				

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	311	1	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでしか使用されません。この属性は、PPP CHAP ID と同じです（RFC 2548）
26	311	11	MSCHAP-Challenge	ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャレンジが含まれます。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。（RFC 2548）
VPDN 属性				
26	9	1	l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウ サイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。
26	9	1	l2tp-drop-out-of-order	正しくない順序で受信したデータ パケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データ パケット上でシーケンス番号が送信されるわけではありません。

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	9	1	l2tp-hello-interval	hello キープアライブ インターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。
26	9	1	l2tp-hidden-avp	イネーブルにすると、L2TP 制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。
26	9	1	l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。
26	9	1	tunnel-tos-reflect	LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロードパケットの IP ヘッダーからトンネルパケットの IP ヘッダーにコピーします。
26	9	1	l2tp-tunnel-authen	この属性を設定すると、L2TP トンネル認証が実行されます。
26	9	1	l2tp-tunnel-password	L2TP トンネル認証および AVP 隠蔽に使用される共有秘密。

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	9	1	l2tp-udp-checksum	これは認可属性で、L2TP がデータ パケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」と「no」です。デフォルトは「no」です。
Store and Forward Fax 属性				
26	9	3	Fax-Account-Id-Origin	**mmoipaaareceive-id** コマンドまたは **mmoipaaasend-id** コマンドについて、アカウント ID の発信元がシステム管理者によって定義されたものとして示します。
26	9	4	Fax-Msg-Id=	Store and Forward Fax 機能によって割り当てられた一意のファクス メッセージ識別番号を示します。
26	9	5	Fax-Pages	このファクス セッション中に送信または受信したページ数を示します。このページ数には、カバー ページも含まれます。
26	9	6	Fax-Coverpage-Flag	カバー ページがこのファクス セッションのオフランプ ゲートウェイで生成されたかどうかを示します。true はカバー ページが生成されたことを示します。false はカバー ページが生成されなかったことを意味します。

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	9	7	Fax-Modem-Time	モデムがファクス データを送信した時間（x）、およびファクス セッションの合計時間（y）を秒単位で示します。これには、fax-mail および PSTN 時間が x/y の形式で含まれます。たとえば、10/15 は送信時間が 10 秒で、合計ファクス セッションが 15 秒であったことを示します。
26	9	8	Fax-Connect-Speed	この fax-mail が最初に送信または受信された時点のモデム速度を示します。有効値は、1200、4800、9600、および 14400 です。
26	9	9	Fax-Recipient-Count	このファクス送信の受信者数を示します。E メール サーバがセッション モードをサポートするまで、この数字は 1 にする必要があります。
26	9	10	Fax-Process-Abort-Flag	ファクス セッションが中断したこと、または正常に終了したことを示します。true はセッションが中断したことを示します。false はセッションが成功したことを示します。
26	9	11	Fax-Dsn-Address	DSN の送信先のアドレスを示します。

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	9	12	Fax-Dsn-Flag	DSN がイネーブルにされているかどうかを示します。true は DSN がイネーブルにされていることを示します。false は DSN がイネーブルにされていないことを示します。
26	9	13	Fax-Mdn-Address	MDN の送信先のアドレスを示します。
26	9	14	Fax-Mdn-Flag	メッセージ配信通知（MDN）がイネーブルにされているかどうかを示します。true は MDN がイネーブルにされていることを示します。false は MDN がイネーブルにされていないことを示します。
26	9	15	Fax-Auth-Status	このファクス セッションに対する認証が成功したかどうかを示します。このフィールドに対する有効値は、success、failed、bypassed、または unknown です。
26	9	16	Email-Server-Address	オンランプ fax-mail メッセージを処理する E メール サーバの IP アドレスを示します。
26	9	17	Email-Server-Ack-Flag	オンランプ ゲートウェイが fax-mail メッセージを受け入れる E メール サーバから肯定確認応答を受信したことを示します。

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	9	18	Gateway-Id	ファクス セッションを処理したゲートウェイの名前を示します。名前は、hostname.domain-name という形式で表示されます。
26	9	19	Call-Type	ファクスのアクティビティのタイプを、fax receive または fax send のどちらかで記述します。
26	9	20	Port-Used	この fax-mail の送受信いずれかに使用される Cisco AS5300 のスロット/ポート番号を示します。
26	9	21	Abort-Cause	ファクス セッションが中断した場合、中断の信号を送信したシステム コンポーネントを示します。中断する可能性のあるシステム コンポーネントには、FAP（Fax Application Process）、TIFF（TIFF リーダーまたは TIFF ライター）、fax-mail クライアント、fax-mail サーバ、ESMTP クライアント、ESMTP サーバなどがあります。
H323 属性				
26	9	23	Remote-Gateway-ID（h323-remote-address）	リモート ゲートウェイの IP アドレスを示します。
26	9	24	Connection-ID（h323-conf-id）	会議 ID を識別します。

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	9	25	Setup-Time（h323-setup-time）	以前、グリニッジ標準時（GMT）およびズール タイムと呼ばれていた協定世界時（UTC）でのこの接続のセットアップ時間を示します。
26	9	26	Call-Origin（h323-call-origin）	ゲートウェイに対するコールの発行元を示します。有効値は、originating および terminating です（回答）。
26	9	27	Call-Type（h323-call-type）	コールのレグ タイプを示します。有効値は、**telephony** および **VoIP** です。
26	9	28	Connect-Time（h323-connect-time）	このコール レッグの UTC での接続時間を示します。
26	9	29	Disconnect-Time（h323-disconnect-time）	このコール レッグが UTC で接続解除された時間を示します。
26	9	30	Disconnect-Cause（h323-disconnect-cause）	Q.931 仕様によって、接続がオフラインにされた理由を示します。
26	9	31	Voice-Quality（h323-voice-quality）	コールの音声品質に影響する Impairment Factor（ICPIF）を指定します。
26	9	33	Gateway-ID（h323-gw-id）	下位のゲートウェイの名前を示します。
大規模のダイヤルアウト属性				
26	9	1	callback-dialstring	コールバックに使用するダイヤリング文字列を定義します。

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	9	1	data-service	説明はありません。
26	9	1	dial-number	ダイヤルする番号を定義します。
26	9	1	force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。
26	9	1	map-class	ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップ クラスで設定される情報の参照を許可します。
26	9	1	send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	9	1	send-name	

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
				PPP 名前認証。PAP に適用する場合は、インターフェイス上で **ppppapsent-namepassword** コマンドを設定しないでください。PAP の場合、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAP の場合、「preauth:send-name」は、アウトバウンド認証だけでなく、インバウンド認証にも使用されます。CHAP インバウンドの場合、NAS は発信元のボックスへのチャレンジ パケットに、「preauth:send-name」で定義された名前を使用します。 （注） send-name 属性は時間の経過とともに変わっています。最初は、現在 send-name および remote-name 属性の両方で提供されている機能を実行していました。remote-name

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
				属性が追加されたため、send-name 属性は現在の動作に制限されています。
26	9	1	send-secret	PPP パスワード認証。ベンダー固有属性（VSA）の場合、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAP アウトバウンドの場合、「preauth:send-name」と「preauth:send-secret」の両方が応答パケットで使用されます。
26	9	1	remote-name	大規模のダイヤルアウトで使用するリモートホストの名前を提供します。ダイヤラは、大規模のダイヤルアウトのリモート名が認証された名前と一致することを確認し、偶発的なユーザ RADIUS 設定ミスから保護します（有効な電話番号にダイヤルしたが誤ったデバイスに接続されるなどのミスです）。
その他の属性				

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	9	2	Cisco-NAS-Port	NAS-Port アカウンティングに追加的なベンダー固有属性（VSA）を指定します。追加的な NAS-Port 情報を属性値ペア（AVPair）の形式で指定するには、**radius-servervsasend** グローバル コンフィギュレーション コマンドを使用します。 （注） この VSA は、通常アカウンティングで使用されますが認証（Access-Request）パケットで使用される場合もあります。
26	9	1	min-links	MLP に対するリンクの最小数を設定します。
26	9	1	proxyacl#<n>	ダウンロード可能なユーザ プロファイル（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。

番号	Vendor-Specific 企業コード	Sub-Type Number	属性	説明
26	9	1	spi	登録中にホーム エージェントがモバイル ノードの認証で必要とする認証情報を伝送します。この情報は、**ip mobile secure host <addr>** コンフィギュレーション コマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーション コマンドはそのまま含まれます。これにはセキュリティ パラメータ インデックス（SPI）、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。

関連トピック

ベンダー固有の RADIUS 属性を使用するデバイス設定 （2117 ページ）

ベンダー独自仕様の RADIUS サーバ通信

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバ間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS 属性セットを独自に機能拡張しているベンダーもあります。Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

前述したように、RADIUS（ベンダーの独自仕様によるものか、IETF ドラフトに準拠するものかを問わず）を設定するには、RADIUS サーバデーモンが稼働しているホストと、そのホストがスイッチと共有するシークレットテキストストリングを指定する必要があります。RADIUS ホストおよびシークレット テキスト ストリングを指定するには、**radius server** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

ベンダー独自の RADIUS サーバとの通信に関するデバイスの設定 （2119 ページ）

RADIUS の設定方法

RADIUS サーバ ホストの識別

これらの設定を Device と通信するすべての RADIUS サーバに適用するために使用する固有のグローバル コンフィギュレーション コマンドは、**radius-server timeout**、**radius-server retransmit**、**radius-server key** の 3 つです。

認証時用にAAAサーバグループを使用して既存のサーバホストをグループ化するようにDeviceを設定できます。詳細については、次の関連項目を参照してください。

RADIUSサーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、DeviceのIPアドレス、およびサーバとDeviceの双方で共有するキー ストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、次の手順を実行します。

始める前に

デバイス上にグローバルな機能とサーバ単位での機能（タイムアウト、再送信回数、およびキーコマンド）を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、およびキーに関するコマンドは、グローバルに設定したタイムアウト、再送信回数、およびキーに関するコマンドを上書きします。すべてのRADIUSサーバに対してこれらの値を設定する方法については、次の関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server** *server name* 例： `Device(config)# radius server rsim`	

	コマンドまたはアクション	目的
ステップ 4	**address** {**ipv4** | **ipv6**}*ip address*{ **auth-port** *port number* | **acct-port** *port number*} 例： `Device(config-radius-server)# address ipv4 124.2.2.12 auth-port 1612`	（任意）RADIUS サーバのパラメータを指定します。 **auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは1645 です。指定できる範囲は 0 ～ 65536 です。 **acct-port** *port-number* には、認証要求の UDP宛先ポートを指定します。デフォルトは 1646 です。
ステップ 5	**key** *string* 例： `Device(config-radius-server)# key rad123`	（任意）**key** *string* には、RADIUS サーバ上で動作する RADIUS デーモンと Deviceの間で使用する認証および暗号キーを指定します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキストストリングでなければなりません。キーは常に **radius server** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 6	**retransmit** *value* 例： `Device(config-radius-server)# retransmit 10`	（任意）サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ～ 100 です。この設定は、**radius-server retransmit** グローバル コンフィギュレーション コマンドによる設定を上書きします。
ステップ 7	**timeout** *seconds* 例： `Device(config-radius-server)# timeout 60`	（任意）Deviceが要求を再送信する前に RADIUS サーバからの応答を待機する時間間隔を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コン

	コマンドまたはアクション	目的
		フィギュレーションコマンドによる設定を上書きします。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

RADIUS サーバ ホスト （2088 ページ）
AAA サーバ グループの定義 （2111 ページ）
すべての RADIUS サーバの設定 （2116 ページ）

RADIUS ログイン認証の設定

RADIUS ログイン認証を設定するには、次の手順を実行します。

始める前に

AAA 方式を使用して HTTP アクセスに対しデバイスのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでデバイスを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しデバイスのセキュリティは確保しません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Device(config)# aaa authentication login default local`	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • *enable*：イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ **enable** *password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。

	コマンドまたはアクション	目的
		• *group radius*：RADIUS 認証を使用します。この認証方式を使用するには、あらかじめ RADIUS サーバを設定しておく必要があります。 • *line*：回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • *local*：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *name***password** グローバル コンフィギュレーション コマンドを使用します。 • *local-case*：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username** *password* グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 • *none*：ログインに認証を使用しません。
ステップ 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Device(config)# line 1 4`	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 6	**login authentication** {**default** | *list-name*} 例： `Device(config)# login authentication default`	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成

	コマンドまたはアクション	目的
		したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

RADIUS ログイン認証 （2089 ページ）
RADIUS サーバ ホスト （2088 ページ）

AAA サーバ グループの定義

定義したグループ サーバに特定のサーバを関連付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することも、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを特定することもできます。

AAA サーバ グループを定義するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server** *name* 例： `Device(config)# radius server ISE`	RADIUS サーバの設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。 デバイスは、IPv6 対応の RADIUS をサポートしています。
ステップ 4	**address** {**ipv4** | **ipv6**} {*ip-address* | *hostname*} **auth-port** *port-number***acct-port** *port-number* 例： `Device(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646`	RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。
ステップ 5	**end** *string* 例： `Device(config-radius-server)# key cisco123`	デバイスと RADIUS サーバとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。
ステップ 6	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例：	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

関連トピック

RADIUS サーバ ホストの識別 （2106 ページ）
RADIUS サーバ ホスト （2088 ページ）
AAA Server Groups （2089 ページ）

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

ユーザ特権アクセスおよびネットワーク サービスに関する RADIUS 許可を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization network radius** 例： `Device(config)# aaa authorization network radius`	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるように デバイス を設定します。

	コマンドまたはアクション	目的
ステップ 4	**aaa authorization exec radius** 例： `Device(config)# aaa authorization exec radius`	ユーザに特権 EXEC のアクセス権限がある場合、ユーザが RADIUS 許可を受けるように デバイス を設定します。 **exec** キーワードを指定すると、ユーザプロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

aaa authorization グローバル コンフィギュレーション コマンドと **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

関連トピック

AAA Authorization （2090 ページ）

RADIUS アカウンティングの起動

RADIUS アカウンティングを開始するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting network start-stop radius** 例： `Device(config)# aaa accounting network start-stop radius`	ネットワーク関連のあらゆるサービス要求に関して、RADIUS アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting exec start-stop radius** 例： `Device(config)# aaa accounting exec start-stop radius`	RADIUS アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。このコマンドは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

関連トピック

RADIUS アカウンティング （2090 ページ）

すべての RADIUS サーバの設定

すべての RADIUS サーバを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server key** *string*
	例：
	`Device(config)# radius-server key your_server_key`
	`Device(config)# key your_server_key`
		スイッチとすべての RADIUS サーバ間で共有されるシークレット テキスト ストリングを指定します。
		（注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。

ステップ 3	**radius-server retransmit** *retries* 例： `Device(config)# radius-server`	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ～ 1000 です。

	コマンドまたはアクション	目的
	`retransmit 5`	
ステップ 4	**radius-server timeout** *seconds* 例： `Device(config)# radius-server timeout 3`	スイッチが RADIUS 要求に対する応答を待って、要求を再送信するまでの時間（秒）を指定します。デフォルトは5秒です。指定できる範囲は 1 ～ 1000 です。
ステップ 5	**radius-server deadtime** 分 例： `Device(config)# radius-server deadtime 0`	RADIUS サーバが認証要求に応答していない場合、このコマンドはそのサーバに対する要求を停止する時刻を指定します。これにより、要求がタイムアウトするまで待たずとも、次に設定されているサーバを試行することができます。デフォルトは 0 です。指定できる範囲は 0 ～ 1440 分です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

RADIUS サーバ ホストの識別 （2106 ページ）
RADIUS サーバ ホスト （2088 ページ）

ベンダー固有の RADIUS 属性を使用するデバイス設定

ベンダー固有仕様の RADIUS 属性を使用するようにデバイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server vsa send** [**accounting** | **authentication**] 例： `Device(config)# radius-server vsa send accounting`	デバイスが VSA（RADIUS IETF 属性 26 で定義）を認識して使用できるようにします。 • （任意）認識されるベンダー固有属性の集合をアカウンティング属性だけに限定するには、**accounting** キーワードを使用します。 • （任意）認識されるベンダー固有属性の集合を認証属性だけに限定するには、**authentication** キーワードを使用します。 キーワードを指定せずにこのコマンドを入力すると、アカウンティングおよび認証のベンダー固有属性の両方が使用されます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例：	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

関連トピック

ベンダー固有の RADIUS 属性 （2090 ページ）

ベンダー独自の RADIUS サーバとの通信に関するデバイスの設定

ベンダー独自仕様の RADIUS サーバ通信を使用するようにデバイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server** *server name* 例： `Device(config)# radius server rsim`	RADIUS サーバを指定します。
ステップ 4	**address** { **ipv4** | **ipv6** }*ip address* 例： `Device(config-radius-server)# address ipv4 172.24.25.10`	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 5	**non-standard** 例： `Device(config-radius-server)# non-standard`	RADIUS サーバが RADIUS ベンダー独自の実装を使用していることを示します。

	コマンドまたはアクション	目的
ステップ 6	**key** *string* 例： `Device(config-radius-server)# key rad123`	デバイスとベンダー独自仕様の RADIUS サーバとの間で使用される共有秘密テキスト文字列を指定します。デバイスと RADIUS サーバはこのテキスト文字列を使用してパスワードを暗号化し、応答を交換します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ベンダー独自仕様の RADIUS サーバ通信 （2105 ページ）

デバイス 上での CoA の設定

CoA を デバイス で設定するには、次の手順を実行します。この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	デバイスを認証、許可、アカウンティング（AAA）サーバに設定し、外部ポリシーサーバとの相互作用を実行します。
ステップ 5	**client** {*ip-address* | *name*} [**vrf** *vrfname*] [**server-key** *string*]	ダイナミック許可ローカルサーバコンフィギュレーションモードを開始し、デバイスがCoAを受け取り、要求を取り外すRADIUSクライアントを指定します。
ステップ 6	**server-key** [**0** | **7**] *string* 例： `Device(config-sg-radius)# server-key your_server_key`	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 7	**port** *port-number* 例： `Device(config-sg-radius)# port 25`	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。
ステップ 8	**auth-type** {**any** | **all** | **session-key**} 例： `Device(config-sg-radius)# auth-type any`	デバイスが RADIUS クライアントに使用する許可のタイプを指定します。 クライアントは、許可用に設定されたすべての属性と一致していなければなりません。
ステップ 9	**ignore session-key**	（任意）セッションキーを無視するように デバイス を設定します。 **ignore** コマンドの詳細については、Cisco.com 上の『*Cisco IOS Intelligent*

	コマンドまたはアクション	目的
		Services Gateway Command Reference』を参照してください。
ステップ 10	**ignore server-key** 例： `Device(config-sg-radius)# ignore server-key`	（任意）サーバキーを無視するようにデバイス を設定します。 **ignore** コマンドの詳細については、Cisco.com 上の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。
ステップ 11	**authentication command bounce-port ignore** 例： `Device(config-sg-radius)# authentication command bounce-port ignore`	（任意）CoA 要求を無視して、セッションをホスティングするポートを一時的にディセーブルにするようにデバイスを設定します。ポートを一時的にディセーブルにする目的は、VLAN の変更が発生しても、その変更を検出するサプリカントがエンドポイント上にない場合に、ホストから DHCP 再ネゴシエーションを行わせることです。
ステップ 12	**authentication command disable-port ignore** 例： `Device(config-sg-radius)# authentication command disable-port ignore`	（任意）セッションをホスティングしているポートを管理上のシャットダウン状態にすることを要求する非標準コマンドを無視するようにデバイスを設定します。ポートをシャットダウンすると、セッションが終了します。 ポートを再びイネーブルにするには、標準の CLI または SNMP コマンドを使用します。
ステップ 13	**end** 例： `Device(config-sg-radius)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 15	**copy running-config startup-config** 例：	（任意）コンフィギュレーションファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

CoA 機能のモニタリング

表 *133 :* 特権 *EXEC* 表示コマンド

コマンド	目的
show aaa attributes protocol radius	RADIUS コマンドの AAA 属性を表示します。

表 *134 :* グローバル トラブルシューティング コマンド

コマンド	目的
debug radius	RADIUS のトラブルシューティングを行うための情報を表示します。
debug aaa coa	CoA 処理のトラブルシューティングを行うための情報を表示します。
debug aaa pod	POD パケットのトラブルシューティングを行うための情報を表示します。
debug aaa subsys	POD パケットのトラブルシューティングを行うための情報を表示します。
debug cmdhd [**detail** | **error** | **events**]	コマンド ヘッダーのトラブルシューティングを行うための情報を表示します。

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セッションアウェアなネットワーキングに対するアイデンティティコントロール ポリシーおよびアイデンティティサービステンプレートの設定。	『Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switch http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.ht
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	『Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Sw http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 98 章

RADIUS over DTLS の設定

- 機能情報の確認 （2127 ページ）
- RADIUS over DTLS の前提条件 （2127 ページ）
- RADIUS over DTLS に関する情報 （2128 ページ）
- RADIUS over DTLS を設定する方法 （2128 ページ）
- RADIUS over DTLS のモニタリング （2131 ページ）
- RADIUS over DTLS の設定例 （2132 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

RADIUS over DTLS の前提条件

RADIUS over DTLS の前提条件は次のとおりです。

- デバイスが Cisco IOS crypto K9 イメージを実行していること。
- crypto PKI がデバイス上に設定されていること。
- RADIUS over DTLS が Cisco ISE 2.2 以降でサポートされている。

RADIUS over DTLS に関する情報

DTLS は RADIUS 上の暗号化サービスを有効にして、セキュアなトンネル経由によるトランスポートを可能にします。RADIUS over DTLS は、クライアントとサーバの両方で実装されます。クライアント側は RADIUS の認証、承認、およびアカウンティング（AAA）を制御し、サーバ側は認可変更（CoA）を制御します。

次のパラメータを設定できます。

- クライアントごとの固有な idle_timeout、client trustpoint、および server trustpoint。
- グローバル CoA 固有の DTLS リスニング ポートとソース インターフェイスのリスト。

特定のサーバに対して DTLS を無効にするには、RADIUS サーバの構成モードで **no dtls** コマンドを使用します。

RADIUS over DTLS を設定する方法

DTLS サーバを設定する方法

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server** *radius-server-name* 例： `Device(config)# radius server R1`	RADIUS サーバ コンフィギュレーション モードを開始します。
ステップ 4	**dtls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries**	DTLS パラメータを設定します。次のパラメータを設定できます。 • **connectiontimeout** — DTLS 接続タイムアウト値を設定します。

	コマンドまたはアクション	目的

	number-of-connection-retries] [**trustpoint** [**client** | **server**]]
	例：
	`Device(config-radius-server)# dtls connectiontimeout 10`
	`Device(config-radius-server)# dtls idletimeout 5`
	`Device(config-radius-server)# dtls retries 15`
	`Device(config-radius-server)# dtls ip radius source-interface Ethernet 0/0`
	`Device(config-radius-server)# dtls ip vrf forwarding table-1`
	`Device(config-radius-server)# dtls port 10`
	`Device(config-radius-server)# dtls trustpoint`
		• **idletimeout** —
		DTLS アイドルタイムアウト値を設定します。
		• **ip** —
		IP 送信元パラメータを設定します。
		• **port** —
		DTLS ポート番号を設定します。
		• **retries** —
		DTLS 接続再試行の回数を設定します。
		• **trustpoint** —
		クライアントとサーバに DTLS トラストポイントを設定します。

ステップ 5	**end** 例： `Device(config-radius-server)# end`	特権 EXEC モードに戻ります。

DTLS CoA 用にダイナミック認証を設定する方法

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	ダイナミック許可ローカル サーバ コンフィギュレーション モードを開始し、デバイスが認可変更（CoA）を受け入れ、要求を取り外す RADIUS クライアントを指定します。デバイスを AAA

	コマンドまたはアクション	目的
		サーバとして設定し、外部ポリシーサーバとの連携を可能にする。
ステップ 4	**client {ip-addr | hostname}** [**dtls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-tp** *server-tp-name*] | **server-key** { **0** *string* | **6** *string* | **7** *string* | *string* } | **vrf** *vrf-id*] 例： `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 100 client-tp dtls_ise server-tp dtls_client`	AAA サーバ クライアントの IP アドレスまたはホスト名を設定します。次のオプションのパラメータを設定できます。 • **dtls** — クライアントのDTLSを有効にします。 • **client-tp** — クライアント トラストポイントを設定します。 • **idletimeout** — DTLSアイドルタイムアウト値を設定します。 • **server-tp** — サーバ トラストポイントを設定します。 • **server-key** — RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。 • **0** *string* — 暗号化されていないキーが続くことを示します。 • *string* — 非暗号化（クリア テキスト）共有キー。 • **6** *string* — 暗号キーが続くことを示します。 • *string* — 高度な暗号化方式[AES]による暗号化キー。 • **7** *string* — 非公開のキーが続くことを示します。

	コマンドまたはアクション	目的
		• *string* — 非公開の共有キー。 • *string* — 非暗号化（クリア テキスト）共有キー。 • **vrf** — クライアントの Virtual Routing and Forwarding（VRF）ID。
ステップ 5	**dtls** {**ip radius source-interface** *interface-name* | **port** *radius-dtls-server-port-number*} 例： `Device(config-locsvr-da-radius)# dtls ip radius source-interface GigabitEthernet 1/0/24`	RADIUS CoA サーバを設定します。次のパラメータを設定できます。 • **ip radius source-interface***interface-name* — RADIUS CoA サーバに発信元アドレスのインターフェイスを指定します。 • **port** *radius-dtls-server-port-number* — ローカルの DTLS RADIUS サーバがリッスンするポートを指定します。
ステップ 6	**end** 例： `Device(config-radius-server)# end`	特権 EXEC モードに戻ります。

RADIUS over DTLS のモニタリング

次のコマンドを使用して DTLS サーバの統計情報をモニタできます。

表 *135 : DTLS* サーバの統計情報をモニタするコマンド

コマンド	目的
show aaa servers	DTLS サーバに関連する情報を表示します。 以下の統計情報は、**show aaa servers** コマンドを使用して表示します。 • pkt_cnt_since_idle_tiemout • send_hs_start_cnt • hs_success_cnt • total_tx_pkt_cnt • total_rx_pkt_cnt • total_conn_reset_cnt • conn_reset_cnt_idle_timeout • conn_reset_cnt_no_resp • conn_reset_cnt_malformed_pkt • conn_reset_cnt_error_case
clear aaa counters servers radius{ *server id*|**all**}	RADIUS DTLS 固有の統計情報をクリアします。
debug radius dtls	RADIUS DTLS 固有のデバッグを有効にします。

RADIUS over DTLS の設定例

次に、DTLS 接続ごとの統計情報の出力例を示します。

```
Device# show aaa servers
DTLS: Packet count since last idletimeout 1,
Send handshake count 3,
Handshake Success 1,
Total Packets Transmitted 1,
Total Packets Received 1,
Total Connection Resets 2,
Connection Reset due to idle timeout 0,
Connection Reset due to No Response 2,
Connection Reset due to Malformed packet 0
```

第 99 章

Kerberos の設定

- 機能情報の確認 （2133 ページ）
- Kerberos によるスイッチ アクセスの制御の前提条件 （2133 ページ）
- Kerberos に関する情報 （2134 ページ）
- Kerberos を設定する方法 （2138 ページ）
- Kerberos 設定の監視 （2138 ページ）
- その他の参考資料 （2138 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Kerberos によるスイッチ アクセスの制御の前提条件

Kerberos によるスイッチ アクセスの制御の前提条件は、次のとおりです。

- リモート ユーザがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定し、ユーザとネットワーク サービスの両方に通信を行い、相互に認証させる必要があります。これを実現するには、互いの識別が必要です。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。また、KDC データベースにユーザ用のエントリも作成します。

- Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるスイッチを使用できます。

ホストおよびユーザのエントリを追加または作成する場合の注意事項は次のとおりです。

- Kerberos プリンシパル名はすべて小文字でなければなりません。
- Kerberos インスタンス名はすべて小文字でなければなりません。
- Kerberos レルム名はすべて大文字でなければなりません。

Kerberos に関する情報

ここでは、Kerberos の情報を提供します。

Kerberos とスイッチ アクセス

ここでは、Kerberosセキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。

（注） Kerberosの設定例では、信頼できるサードパーティを、Kerberosをサポートし、ネットワーク セキュリティ サーバとして設定され、Kerberosプロトコルを使用してユーザを認証するスイッチとすることができます。

Kerberos の概要

Kerberos はマサチューセッツ工科大学（MIT）が開発した秘密キーによるネットワーク認証プロトコルです。データ暗号規格（DES）という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberosは、信頼できるサードパーティという概念を使ってユーザとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティをキー発行局（KDC）と呼びます。

Kerberosは、ユーザが誰であるか、そのユーザが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC（つまり信頼できるKerberosサーバ）がユーザにチケットを発行します。これらのチケットには有効期限があり、ユーザ クレデンシャルのキャッシュに保存されます。Kerberosサーバは、ユーザ名やパスワードの代わりにチケットを使ってユーザとネットワーク サービスを認証します。

（注） Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるのであれば、どのスイッチも使用できます。

Kerberos のクレデンシャル発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザを 1 回認証すると、ユーザ クレデンシャルが有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、（UNIX サーバや PC などの）他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh

次の表に、一般的な Kerberos 関連用語とその定義を示します。

表 *136 : Kerberos* の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
許可	ユーザがネットワークやスイッチにおいてどのような権限を有しており、またどのような動作を実行できるかを、スイッチが識別する手段
クレデンシャル	認証チケット（TSG[9]、サービス クレデンシャルなど）を表す総称。Kerberos クレデンシャルで、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することにした場合、ユーザ名やパスワードを再入力する代わりにこれを使用できます。証明書の有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、*user@REALM* という形式です（たとえば、smith@EXAMPLE.COM）。Kerberos インスタンスのある Kerberos プリンシパルは、*user/instance@REALM* という形式です（たとえば、smith/admin@EXAMPLE.COM）。Kerberos インスタンスは、認証が成功した場合のユーザの承認レベルを指定するために使用できます。各ネットワーク サービスのサーバは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。 （注） Kerberos プリンシパル名およびインスタンス名はすべて小文字でなければなりません。 （注） Kerberos レルム名はすべて大文字でなければなりません。

用語	定義
KDC[10]	ネットワーク ホストで稼働する Kerberos サーバおよびデータベース プログラムで構成されるキー発行局
Kerberos 対応	Kerberos クレデンシャルのインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク サービスの ID を検証します。 （注） Kerberos レルム名はすべて大文字でなければなりません。
Kerberos サーバ	ネットワーク ホストで稼働しているデーモン。ユーザおよびネットワーク サービスはそれぞれ Kerberos サーバに ID を登録します。ネットワーク サービスは Kerberos サーバにクエリーを送信して、他のネットワーク サービスの認証を得ます。
KEYTAB[11]	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス クレデンシャルを暗号解除して認証します。Kerberos 5 よりも前のバージョンでは、KEYTAB は SRVTAB[12] と呼ばれます。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。 （注） Kerberos プリンシパル名はすべて小文字でなければなりません。
サービス クレデンシャル	ネットワーク サービスのクレデンシャル。KDC からクレデンシャルが発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。ユーザ TGT ともパスワードを共有します。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。SRVTAB は、Kerberos 5 以降のバージョンでは KEYTAB と呼ばれています。
TGT	身分証明書のことで、KDC が認証済みユーザに発行するクレデンシャル。TGT を受け取ったユーザは、KDC が示した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

9 チケット認可チケット
10 キー発行局
11 キー テーブル
12 サーバ テーブル

Kerberos の動作

Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてリモートユーザを認証できるデバイスを使用できます。Kerberos をカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモートユーザは、3 つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

リモート ユーザがデバイスを Kerberos サーバとして使用してネットワーク サービスで認証されるには、次の手順を実行する必要があります。

境界スイッチに対する認証の取得

ここでは、リモート ユーザが通過しなければならない最初のセキュリティ レイヤについて説明します。ユーザは、まず境界スイッチに対して認証を得なければなりません。リモートユーザが境界スイッチに対して認証を得る場合、次のプロセスが発生します。

1. ユーザが境界スイッチに対して、Kerberos 未対応の Telnet 接続を開始します。
2. ユーザ名とパスワードの入力を求めるプロンプトをスイッチが表示します。
3. スイッチが、このユーザの TGT を KDC に要求します。
4. KDC がユーザ ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使って TGT の暗号解除を試行します。
   - 暗号解除に成功した場合は、ユーザはスイッチに対して認証を得ます。
   - 暗号解除に成功しない場合は、ユーザ名とパスワードを再入力（Caps Lock または Num Lock のオン/オフに注意）するか、別のユーザ名とパスワードを入力してステップ 2 の手順を繰り返します。

Kerberos 未対応の Telnet セッションを開始し、境界スイッチの認証を得ているリモートユーザはファイアウォールの内側にいますが、ネットワーク サービスにアクセスするには、KDC から直接認証を得る必要があります。ユーザが KDC から認証を得なければならないのは、KDC が発行する TGT はスイッチに保存されており、ユーザがこのスイッチにログオンしないかぎり、追加の認証に使用できないからです。

KDC からの TGT の取得

ここでは、リモート ユーザが通過しなければならない 2 番めのセキュリティ レイヤについて説明します。ユーザは、ネットワーク サービスにアクセスするために、このレイヤで KDC の認証を得て、KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章にある「Obtaining a TGT from a KDC」を参照してください。

ネットワーク サービスに対する認証の取得

ここでは、リモート ユーザが通過しなければならない 3 番めのセキュリティ レイヤについて説明します。TGT を取得したユーザは、このレイヤで Kerberos レルム内のネットワーク サービスに対して認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章の「Authenticating to Network Services」を参照してください。

Kerberos を設定する方法

Kerberos 認証済みサーバ/クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

Kerberos 設定の監視

Kerberos 設定を表示するには、次のコマンドを使用します。

- **show running-config**
- **showkerberoscreds**：現在のユーザの認定証キャッシュに含まれる認定証を一覧表示します。
- **clearkerberoscreds**：転送済みの認定証を含め、現在のユーザの認定証キャッシュに含まれるすべての認定証を破棄します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Kerberos コマンド	『*Cisco IOS Security Command Reference*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 100 章

ローカル認証および許可の設定

- 機能情報の確認 （2141 ページ）
- ローカル認証および許可の設定方法 （2141 ページ）
- ローカル認証および許可のモニタリング （2144 ページ）
- その他の参考資料 （2144 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ローカル認証および許可の設定方法

スイッチのローカル認証および許可の設定

ローカル モードで AAA を実装するようにスイッチを設定すると、サーバがなくても動作するように AAA を設定できます。この場合、スイッチは認証および許可の処理を行います。この設定ではアカウンティング機能は使用できません。

（注） AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ローカル モードで AAA を実装するようにスイッチを設定して、サーバがなくても動作するように AAA を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa authentication login default local** 例： `Device(config)# aaa authentication login default local`	ローカルユーザ名データベースを使用するログイン認証を設定します。**default** キーワードにより、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ 5	**aaa authorization exec local** 例： `Device(config)# aaa authorization exec local`	ユーザの AAA 許可を設定し、ローカルデータベースを確認して、そのユーザに EXEC シェルの実行を許可します。

	コマンドまたはアクション	目的
ステップ 6	**aaa authorization network local** 例： `Device(config)# aaa authorization network local`	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。
ステップ 7	**username** *name* [**privilege** *level*] {**password** *encryption-type password*} 例： `Device(config)# username your_user_name privilege 1 password 7 secret567`	ローカルデータベースを入力し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 • *name* には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。 • （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type* には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 • *password* には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

SSH サーバ、統合クライアント、およびサポートされているバージョン （2149 ページ）
TACACS+ およびスイッチ アクセス （2015 ページ）
RADIUS およびスイッチ アクセス （2077 ページ）
SSH を実行するためのDeviceの設定 （2152 ページ）
SSH 設定時の注意事項 （2150 ページ）

ローカル認証および許可のモニタリング

ローカル認証および許可の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 101 章

セキュア シェル（SSH）の設定

（注） Cisco IOS XE Denali 16.3.1 以降では、セキュア シェル バージョン 1（SSHv1）が廃止されます。

- 機能情報の確認 （2147 ページ）
- セキュア シェルを設定するための前提条件 （2147 ページ）
- セキュア シェルの設定に関する制約事項 （2148 ページ）
- SSH に関する情報 （2149 ページ）
- SSH の設定方法 （2152 ページ）
- SSH の設定およびステータスのモニタリング （2156 ページ）
- その他の参考資料 （2156 ページ）
- SSH の機能情報 （2157 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

セキュア シェルを設定するための前提条件

セキュア シェル（SSH）用にスイッチを設定するための前提条件は、次のとおりです。

- SSH を動作させるには、スイッチに Rivest、Shamir、および Adleman（RSA）の公開キーと秘密キーのペアが必要です。これは SSH が必要なセキュア コピー プロトコル（SCP）も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。
- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。
- SCP はセキュリティについて SSH に依存します。
- SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。
- ユーザが SCP を使用するには適切な許可が必要です。
- 適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System（IFS）のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには **copy** コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。
- セキュア シェル（SSH）サーバは、IPsec（データ暗号規格（DES）または 3DES）の暗号化ソフトウェア イメージを必要とします。SSH クライアントは、IPsec（DES または 3DES）の暗号化ソフトウェア イメージが必要です。
- グローバル コンフィギュレーション モードで **hostname** および **ip domain-name** コマンドを使用して、デバイスのホスト名とホスト ドメインを設定します。

関連トピック

セキュア コピー プロトコル （2151 ページ）

セキュア シェルの設定に関する制約事項

セキュア シェル用に Device を設定するための制約事項は、次のとおりです。

- スイッチは、Rivest, Shamir, and Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、データ暗号規格（DES）（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアでのみサポートされます。DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。
- Device は、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES）暗号化アルゴリズムをサポートします。ただし、キーを暗号化する対称暗号化 AES はサポートされません。
- このソフトウェア リリースは、IP Security（IPSec）をサポートしていません。

- SCP を使用する場合、**copy** コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。
- ログイン バナーはセキュア シェル バージョン 1 ではサポートされません。セキュア シェル バージョン 2 ではサポートされています。
- リバース SSH の代替手段をコンソール アクセス用に設定する場合、-l キーワード、userid :{number} {ip-address} デリミタ、および引数が必須です。

関連トピック

セキュア コピー プロトコル （2151 ページ）

SSH に関する情報

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

SSH およびスイッチ アクセス

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

IPv6 の SSH 機能は IPv4 における機能と同じです。IPv6 の場合、SSH は IPv6 アドレスをサポートし、IPv6 トランスポート上において、リモート IPv6 ノードとのセキュリティ保護および暗号化された接続を有効化します。

SSH サーバ、統合クライアント、およびサポートされているバージョン

セキュア シェル（SSH）統合クライアント機能は、SSH プロトコル上で動作し、デバイスの認証および暗号化を実現するアプリケーションです。SSH クライアントによって、シスコ デバイスは別のシスコ デバイスなど SSH サーバを実行するデバイスに対して、セキュアで暗号化された接続を実行できます。この接続は、接続が暗号化される点を除いて Telnet のアウトバウンド接続と同様の機能を提供します。SSH クライアントは、認証および暗号化により、保護されていないネットワーク上でもセキュアな通信ができます。

SSH サーバおよび SSH 統合クライアントは、スイッチ上で実行されるアプリケーションです。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。SSH クライアントは、市販の一般的な SSH サーバと連動します。SSH クライアントは、Data Encryption Standard（DES）、3DES、およびパスワード認証の暗号をサポートします。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは、SSHv1 クライアントをサポートしています。

（注） SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

ユーザ認証は、デバイスに対する Telnet セッションの認証と同様に実行されます。SSH は、次のユーザ認証方式もサポートします。

- TACACS+
- RADIUS
- ローカル認証および許可

関連トピック

スイッチのローカル認証および許可の設定 （2141 ページ）
TACACS+ およびスイッチ アクセス （2015 ページ）
RADIUS およびスイッチ アクセス （2077 ページ）

SSH 設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できます（逆の場合も同様です）。
- スタック マスターで SSH サーバが実行されている場合で、スタック マスターに障害が発生した場合、新しいスタック マスターでは、前のスタック マスターによって生成された RSA キー ペアが使用されます。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力した後、CLI エラー メッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。詳細については、次の関連項目を参照してください。
- RSA キーのペアを生成する場合に、メッセージ「No host name specified」が表示されることがあります。このメッセージが表示された場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

関連トピック

SSH を実行するためのDeviceの設定 （2152 ページ）
スイッチのローカル認証および許可の設定 （2141 ページ）

セキュア コピー プロトコルの概要

Secure Copy Protocol（SCP）機能は、スイッチの設定やイメージ ファイルのコピーにセキュアな認証方式を提供します。SCP にはセキュア シェル（SSH）が必要です（Berkeley の r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルです）。

SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

また、SSH には AAA 認証が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。

（注） SCP を使用する場合、copy コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

セキュア コピー プロトコル

セキュア コピー プロトコル（SCP）機能は、デバイスの設定やスイッチ イメージ ファイルのコピーにセキュアな認証方式を提供します。SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol（RCP）と類似しています。また、SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、デバイスはユーザが正しい権限レベルを保有しているか確認する必要があります。セキュア コピー機能を設定するには、SCP の概念を理解する必要があります。

関連トピック

セキュア シェルを設定するための前提条件 （2147 ページ）
セキュア シェルの設定に関する制約事項 （2148 ページ）

SSH の設定方法

SSH を実行するためのDeviceの設定

SSH を実行するようにDeviceをセットアップするには、次の手順を実行してください。

始める前に

ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。この手順は必須です。詳細については、次の関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname** *hostname* 例： `Device(config)# hostname your_hostname`	Deviceのホスト名および IP ドメイン名を設定します。 （注） この手順を実行するのは、Deviceを SSH サーバとして設定する場合だけです。
ステップ 4	**ip domain-name** *domain_name* 例： `Device(config)# ip domain-name your_domain`	Deviceのホスト ドメインを設定します。
ステップ 5	**crypto key generate rsa** 例： `Device(config)# crypto key generate rsa`	Device上でローカルおよびリモート認証用にSSHサーバをイネーブルにし、RSA キー ペアを生成します。Deviceの RSA キー ペアを生成すると、SSH が自動的にイネーブルになります。

	コマンドまたはアクション	目的
		最小モジュラス サイズは、1024 ビットにすることを推奨します。 RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。 （注） この手順を実行するのは、Deviceを SSH サーバとして設定する場合だけです。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

SSH 設定時の注意事項 （2150 ページ）
スイッチのローカル認証および許可の設定 （2141 ページ）

SSH サーバの設定

SSH サーバを設定するには、次の手順を実行します。

（注） Device を SSH サーバとして設定する場合にのみ、この手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sshversion** [**1** | **2**] 例： `Device(config)# ip ssh version 1`	（任意）SSHv1 または SSHv2 を実行するようにDeviceを設定します。 • **1**：SSHv1 を実行するようにDeviceを設定します。 • **2**：SSHv2 を実行するようにDeviceを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、SSHサーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。
ステップ 4	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*} 例： `Device(config)# ip ssh timeout 90 authentication-retries 2`	SSH 制御パラメータを設定します。 • タイムアウト値は秒単位で指定します（デフォルト値は120秒）。指定できる範囲は0～120秒です。このパラメータは、SSHネゴシエーション フェーズに適用されます。接続が確立されると、DeviceはCLIベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク上の複数の CLI ベース セッション（セッション0～4）に対して、最大 5 つの暗号化同時 SSH 接続を使

	コマンドまたはアクション	目的
		用できます。実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントをサーバへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。

ステップ 5	次のいずれかまたは両方を使用します。
	• `line vty`*line_number*[*ending_line_number*]
	• **transport input ssh**
	例：
	`Device(config)# line vty 1 10`
	
	または
	`Device(config-line)# transport input ssh`
		（任意）仮想端末回線設定を設定します。
		• ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。*line_number* および *ending_line_number* には、回線のペアを指定します。指定できる範囲は 0 ～ 15 です。
		• 非 SSH Telnet によるDeviceへの接続を許可しない設定です。これにより、ルータは SSH 接続に限定されます。

ステップ 6	**end** 例： `Device(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SSH の設定およびステータスのモニタリング

次の表に、SSH サーバの設定およびステータスを示します。

表 *137 : SSH* サーバの設定およびステータスを表示するコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セッションアウェアなネットワーキングに対するアイデンティティコントロール ポリシーおよびアイデンティティサービステンプレートの設定。	『Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switch http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.ht
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	『Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Sw http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

SSH の機能情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

リリース	機能情報
Cisco IOS XE Denali 16.3.1	（注） Cisco IOS XE Denali 16.3.1 以降では、セキュア シェル バージョン 1（SSHv1）が廃止されます。

第 102 章

SSH 認証の X.509v3 証明書

• SSH 認証の X.509v3 証明書 （2159 ページ）

SSH 認証の X.509v3 証明書

SSH 認証の X.509v3 証明書機能はサーバ上で X.509v3 デジタル証明書を使用し、サーバ側で Secure Shell（SSH）ユーザ認証を使用します。

このモジュールでは、デジタル証明書用のサーバおよびユーザ証明書プロファイルを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

SSH 認証の X.509v3 証明書 の前提条件

- SSH 認証の X.509v3 証明書機能では、**ip ssh server authenticate user** コマンドの代わりに **ip ssh server algorithm authentication** コマンドが導入されます。**ip ssh server authenticate user** コマンドを使用すると、次の警告メッセージが表示されます。

```
Warning: SSH command accepted but this CLI will be deprecated soon. Please move to
new CLI "ip ssh server algorithm authentication". Please configure "default ip ssh
server authenticate user" to make CLI ineffective.
```

  - **ip ssh server authenticate user** コマンドの影響を受けないようにするには、**default ip ssh server authenticate user** コマンドを使用します。その後、IOS セキュア シェル

（SSH）サーバは **ip ssh server algorithm authentication** コマンドを使用して起動します。

SSH 認証の X.509v3 証明書 の制約事項

- SSH 認証の X.509v3 証明書 機能の実装は、IOS セキュア シェル（SSH）側にのみ適用できます。
- IOS SSH サーバは、IOS SSH サーバ側のサーバおよびユーザ認証について、x509v3-ssh-rsa アルゴリズム ベースの証明書のみをサポートします。

SSH 認証用の X.509v3 証明書に関する情報

デジタル証明書

認証の有効性は、公開署名キーとその署名者のアイデンティティとの関連の強さに依存します。X.509v3 形式（RFC5280）のデジタル証明書は、アイデンティティの管理を実行するために使用されます。信頼できるルート証明機関とその中間証明機関による署名の連鎖によって、指定の公開署名キーと指定のデジタル アイデンティティがバインドされます。

公開キー インフラストラクチャ（PKI）のトラストポイントは、デジタル証明書の管理に役立ちます。証明書とトラストポイントを関連付けることによって、証明書を追跡できます。トラストポイントには、認証局（CA）、さまざまなアイデンティティ パラメータ、およびデジタル証明書に関する情報が含まれています。複数のトラストポイントを作成して、異なる証明書に関連付けることができます。

X.509v3 を使用したサーバおよびユーザ認証

サーバ認証の場合、IOS セキュア シェル（SSH）が確認のためにそれ自体の証明書を SSH クライアントに送信します。このサーバ証明書は、サーバ証明書プロファイル（ssh-server-cert-profile-server コンフィギュレーション モード）で設定されたトラストポイントに関連付けられます。

ユーザ認証の場合、SSH クライアントが確認のためにユーザの証明書を IOS SSH サーバに送信します。SSH サーバは、サーバ証明書プロファイル（ssh-server-cert-profile-user コンフィギュレーション モード）で設定された公開キー インフラストラクチャ（PKI）トラストポイントを使用して、受信したユーザ証明書を確認します。

デフォルトでは、証明書ベースの認証が、IOS SSH サーバ端末でサーバおよびユーザに対して有効になっています。

SSH 認証用の X.509v3 証明書の設定方法

サーバ認証にデジタル証明書を使用するための IOS SSH サーバの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh server algorithm hostkey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]} 例： `Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa`	ホスト キー アルゴリズムの順序を定義します。セキュア シェル（SSH）クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。 （注） IOS SSH サーバには、1 つ以上の設定済みホスト キー アルゴリズムが必要です。 • ssh-rsa：公開キーベース認証 • x509v3-ssh-rsa：証明書ベース認証
ステップ 4	**ip ssh server certificate profile** 例： `Device(config)# ip ssh server certificate profile`	サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイル コンフィギュレーション モードを開始します。
ステップ 5	**server** 例： `Device(ssh-server-cert-profile)# server`	サーバ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユーザ コンフィギュレーション モードを開始します。
ステップ 6	**trustpoint sign** *PKI-trustpoint-name* 例：	公開キーインフラストラクチャ（PKI）トラストポイントをサーバ証明書プロファイルにアタッチします。SSH サー

	コマンドまたはアクション	目的
	`Device(ssh-server-cert-profile-server)# trustpoint sign trust1`	バは、この PKI トラストポイントに関連付けられた証明書をサーバ認証に使用します。
ステップ 7	**ocsp-response include** 例： `Device(ssh-server-cert-profile-server)# ocsp-response include`	（任意）Online Certificate Status Protocol（OCSP）の応答または OCSP ステープリングをサーバ証明書と一緒に送信します。 （注） デフォルトではこのコマンドの「no」形式が設定されており、OCSP応答はサーバ証明書と一緒には送信されません。
ステップ 8	**end** 例： `Device(ssh-server-cert-profile-server)# end`	SSH サーバ証明書プロファイルのサーバ コンフィギュレーション モードを終了し、特権EXECモードを開始します。

ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh server algorithm authentication {publickey | keyboard | password}** 例： `Device(config)# ip ssh server algorithm authentication publickey`	ユーザ認証アルゴリズムの順序を定義します。セキュア シェル（SSH）クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。 （注） IOS SSH サーバには、1 つ以上の設定済みユーザ認証アルゴリズムが必要です。

	コマンドまたはアクション	目的
		（注） ユーザ認証に証明書方式を使用するには、**publickey** キーワードを設定する必要があります。 （注） **ip ssh server algorithm authentication** コマンドは、**ip ssh server authenticate user** コマンドに置き換わります。
ステップ 4	**ip ssh server algorithm publickey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]} 例： `Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa`	公開キー アルゴリズムの順序を定義します。SSH クライアントによってユーザ認証に許可されるのは、設定済みのアルゴリズムのみです。 （注） IOS SSH クライアントには、1 つ以上の設定済み公開キー アルゴリズムが必要です。 • ssh-rsa：公開キーベース認証 • x509v3-ssh-rsa：証明書ベース認証
ステップ 5	**ip ssh server certificate profile** 例： `Device(config)# ip ssh server certificate profile`	サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイル コンフィギュレーション モードを開始します。
ステップ 6	**user** 例： `Device(ssh-server-cert-profile)# user`	ユーザ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユーザ コンフィギュレーション モードを開始します。
ステップ 7	**trustpoint verify** *PKI-trustpoint-name* 例： `Device(ssh-server-cert-profile-user)# trustpoint verify trust2`	受信したユーザ証明書の確認に使用される公開キー インフラストラクチャ（PKI）トラストポイントを設定します。 （注） 同じコマンドを複数回実行することで、複数のトラストポイントを設定します。最大 10 のトラストポイントを設定できます。

	コマンドまたはアクション	目的
ステップ 8	**ocsp-response required** 例： `Device(ssh-server-cert-profile-user)# ocsp-response required`	（任意）受信したユーザ証明書による Online Certificate Status Protocol（OCSP）の応答の有無を要求します。 （注） デフォルトではこのコマンドの「no」形式が設定されており、ユーザ証明書は OCSP 応答なしで受け入れられます。
ステップ 9	**end** 例： `Device(ssh-server-cert-profile-user)# end`	SSH サーバ証明書プロファイルのユーザ コンフィギュレーション モードを終了し、特権EXECモードを開始します。

デジタル証明書を使用したサーバおよびユーザ認証の設定の確認

手順

ステップ 1 enable

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show ip ssh

現在設定されている認証方式を表示します。証明書ベース認証の使用を確認するには、x509v3-ssh-rsa アルゴリズムが設定済みのホスト キー アルゴリズムであることを確認します。

例：

```
Device# show ip ssh

SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
```

SSH 認証用の X.509v3 証明書の設定例

例：サーバ認証にデジタル証明書を使用するための IOS SSH サーバの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# server
Device(ssh-server-cert-profile-server)# trustpoint sign trust1
Device(ssh-server-cert-profile-server)# exit
```

例：ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm authentication publickey
Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# user
Device(ssh-server-cert-profile-user)# trustpoint verify trust2
Device(ssh-server-cert-profile-user)# end
```

SSH 認証の X.509v3 証明書に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
SSH 認証	『セキュア シェル設定ガイド』の「セキュア シェル：ユーザ認証方式の設定」の章

関連項目	マニュアル タイトル
公開キー インフラストラクチャ（PKI）のトラストポイント	『*Public Key Infrastructure Configuration Guide*』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

SSH 認証の X.509v3 証明書 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *138 : SSH* 認証の *X.509v3* 証明書 の機能情報

機能名	リリース	機能情報
SSH 認証の X.509v3 証明書	Cisco IOS XE リリース 3.14S	SSH 認証の X.509v3 証明書機能はサーバ上で X.509v3 デジタル証明書を使用し、サーバ側で Secure Shell（SSH）ユーザ認証を使用します。 次のコマンドが導入または変更されました。**ip ssh server algorithm hostkey**、**ip ssh server algorithm authentication**、および **ip ssh server certificate profile**。

第 103 章

Secure Socket Layer HTTP の設定

- 機能情報の確認 （2169 ページ）
- Secure Sockets Layer（SSL）HTTP に関する情報 （2169 ページ）
- セキュア HTTP サーバおよびクライアントの設定方法 （2173 ページ）
- セキュア HTTP サーバおよびクライアントのステータスのモニタリング （2181 ページ）
- その他の参考資料 （2181 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Secure Sockets Layer（SSL）HTTP に関する情報

セキュア HTTP サーバおよびクライアントの概要

セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。シスコが実装するセキュア HTTP サーバおよび HTTP クライアントでは、アプリケーション層の暗号化に SSL バージョン 3.0 を使用します。HTTP over SSL は、HTTPS と省略されます（セキュアな接続の場合、URL が http://の代わりに https://で始まります）。

（注） SSL は 1999 年に Transport Layer Security（TLS）に発展しましたが、このような特定のコンテキストでまだ使用されています。

セキュア HTTP サーバ（スイッチ）の主な役割は、指定のポート（デフォルトの HTTPS ポートは 443）で HTTPS 要求を待ち受けて、HTTP 1.1 Web サーバへその要求を渡すことです。HTTP 1.1 サーバはその要求を処理して、セキュア HTTP サーバへ応答（呼び出す）します。セキュア HTTP サーバは HTTP 1.1 サーバの代わりに、元の要求に応えます。

セキュア HTTP クライアント（Web ブラウザ）の主な役割は、Cisco IOS アプリケーション要求に応答して、そのアプリケーションが要求した HTTPS User Agent サービスを実行し、応答を（そのアプリケーションに）返すことです。

（注） Cisco IOS XE Denali 16.3.1 以降では、HTTP サーバへの IPv6 ACL の接続に対するサポートが有効になっています。Cisco IOS XE Denali 16.3.1 より前は、IPv4 ACL のサポートのみがセキュアな HTTP サーバの設定に有効でした。 セキュアな HTTP サーバ用の設定 CLI を使用して、事前設定された IPv6 および IPv4 ACL を HTTP サーバに接続できます。

CA のトラストポイント

認証局（CA）は、要求を認可して参加するネットワーク デバイスに証明書を発行します。これらのサービスは、参加するデバイスに対する中央集中的なセキュリティ キーおよび証明書の管理を提供します。特定の CA サーバはトラストポイントと呼ばれます。

接続が実行されると、HTTPS サーバは、トラストポイントとなる特定の CA から得た X.509v3 の証明書を発行することで、セキュアな接続をクライアントに提供します。クライアント（通常、Web ブラウザ）は、その証明書の認証に必要な公開キーを保有しています。

セキュア HTTP 接続には、CA のトラストポイントを設定することを強く推奨します。HTTPS サーバを実行しているデバイスに CA のトラストポイントが設定されていないと、サーバは自身を認証して必要な RSA のキーのペアを生成します。自身で認証した（自己署名）証明書は適切なセキュリティではないので、接続するクライアントはその証明書が自己証明書であることを通知し、ユーザに接続の選択（確立または拒否）をさせる必要があります。この選択肢は内部ネットワーク トポロジ（テスト用など）に役立ちます。

CA のトラストポイントを設定していないと、セキュア HTTP 接続を有効にした場合、そのセキュア HTTP サーバ（またはクライアント）に対する一時的または永続的な自己署名証明書が自動的に生成されます。

- スイッチにホスト名とドメイン名が設定されてない場合、生成される自己署名証明書は一時的なものです。スイッチを再起動すると、この一時的な自己署名証明書は失われ、新たに自己署名証明書（一時的に）が割り当てられます。
- スイッチにホスト名とドメイン名が設定されている場合、生成される自己署名証明書は永続的なものです。この証明書は、スイッチを再起動しても、セキュア HTTP サーバを無効

にしても有効のままです。そのため、再度セキュア HTTP 接続を有効にしたときに使用できます。

（注） 認証局およびトラストポイントは、個々のデバイスで設定する必要があります。他のデバイスからコピーすると、それらはスイッチ上で無効になります。

新しい証明書を登録した場合、新しい設定の変更は、サーバが再起動するまで HTTPS サーバに適用されません。CLI を使用するか、または物理的な再起動によって、サーバを再起動できます。サーバを再起動すると、スイッチは新しい証明書の使用を開始します。

自己署名証明書が生成された場合、その情報は **show running-config** 特権 EXEC コマンドで出力できます。自己署名証明書を表示するコマンドの出力（show running-config コマンド）を例として一部示します。

```
Device# show running-config
Building configuration...

<output truncated>

crypto pki trustpoint TP-self-signed-3080755072
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3080755072
 revocation-check none
 rsakeypair TP-self-signed-3080755072
!
!
crypto ca certificate chain TP-self-signed-3080755072
 certificate self-signed 01
  3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109
  02161743 45322D33 3535302D 31332E73 756D6D30 342D3335 3530301E 170D3933
  30333031 30303030 35395A17 0D323030 31303130 30303030 305A3059 312F302D

<output truncated>
```

自己署名証明書は、セキュア HTTP サーバを無効にして、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで削除できます。その後、セキュア HTTP サーバを再度有効にすると、自己署名証明書が新たに生成されます。

（注） *TP self-signed* の後ろに表示されている値は、デバイスのシリアル番号によって異なります。

オプションのコマンド（**ip http secure-client-auth**）を使用すると、HTTPS サーバがクライアントからの X.509v3 証明書を要求します。クライアントの認証は、サーバ自身の認証よりも高いセキュリティを提供します。

認証局の詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Configuring Certification Authority Interoperability」の章を参照してください。

CipherSuite

CipherSuite は暗号化アルゴリズムおよびダイジェストアルゴリズムを指定して、SSL 接続に使用します。HTTPS サーバに接続すると、クライアントの Web ブラウザは、サポート対象の CipherSuite のリストを提供します。その後クライアントとサーバは、両方でサポートされている暗号化アルゴリズムで最適なものをリストから選択してネゴシエートします。たとえば、Netscape Communicator 4.76 は、米国のセキュリティ（RSA 公開キー暗号 MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC）をサポートしています。

最適な暗号化には、128 ビット暗号化をサポートするクライアントブラウザ（Microsoft Internet Explorer バージョン 5.5 以降または Netscape Communicator バージョン 4.76 以降など）が必要です。SSL_RSA_WITH_DES_CBC_SHA CipherSuite は、128 ビット暗号化を提供しないため、他の CipherSuite よりもセキュリティが低くなります。

CipherSuite は、よりセキュリティが高く、複雑になればなるほど、わずかですが処理時間が必要になります。次に、スイッチでサポートされる CipherSuite およびルータの処理負荷（速さ）による CipherSuite のランク（速い順）を定義します。

1. SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化に DES-CBC、およびメッセージダイジェストに SHA を使用した RSA のキー交換（RSA 公開キー暗号化）
2. SSL_RSA_WITH_NULL_SHA：メッセージの暗号化に NULL、およびメッセージ ダイジェストに SHA を使用したキー交換（SSL 3.0 専用）。
3. SSL_RSA_WITH_NULL_MD5：メッセージの暗号化に NULL、およびメッセージ ダイジェストに MD5 を使用したキー交換（SSL 3.0 専用）。
4. SSL_RSA_WITH_RC4_128_MD5：RC4 128 ビット暗号化、およびメッセージ ダイジェストに MD5 を使用した RSA のキー交換
5. SSL_RSA_WITH_RC4_128_SHA：RC4 128 ビット暗号化、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換
6. SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換（RSA 公開キー暗号化）
7. SSL_RSA_WITH_AES_128_CBC_SHA：AES 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。
8. SSL_RSA_WITH_AES_256_CBC_SHA：AES 256 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。
9. SSL_RSA_WITH_AES_128_CBC_SHA：AES 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。
10. SSL_RSA_WITH_AES_256_CBC_SHA：AES 256 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。

（注） Chromeの最新バージョンは4つの元の暗号スイートをサポートしません。そのため、Web GUIとゲスト ポータル両方へのアクセスが拒否されます。

（暗号化およびダイジェスト アルゴリズムをそれぞれ指定して組み合わせた）RSA は、SSL 接続においてキーの生成および認証の両方に使用されます。これは、CA のトラストポイントが設定されているかどうかにかかわりません。

SSL のデフォルト設定

標準の HTTP サーバはイネーブルに設定されています。

SSL はイネーブルに設定されています。

CA のトラストポイントは設定されていません。

自己署名証明書は生成されていません。

SSL の設定時の注意事項

SSL をスイッチ クラスタで使用すると、SSL セッションがクラスタ コマンダで終了します。クラスタ メンバのスイッチは標準の HTTP で動作させる必要があります。

CA のトラストポイントを設定する前に、システム クロックが設定されていることを確認してください。クロックが設定されていないと、不正な日付により証明書が拒否されます。

スイッチ スタック内のスタック マスターで、SSL セッションが強制終了されます。

セキュア HTTP サーバおよびクライアントの設定方法

CA のトラストポイントの設定

セキュア HTTP 接続には、CA のトラストポイントを正式に設定することを推奨します。CA のトラストポイントは、自己署名証明書より高いセキュリティがあります。

CA のトラストポイントを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**hostname** *hostname* 例： `Device(config)# hostname your_hostname`	スイッチのホスト名を指定します（以前ホスト名を設定していない場合のみ必須）。ホスト名はセキュリティキーと証明書に必要です。
ステップ 3	**ip domain-name** *domain-name* 例： `Device(config)# ip domain-name your_domain`	スイッチの IP ドメイン名を指定します（以前 IP ドメイン名を設定していない場合のみ必須）。IP ドメイン名はセキュリティキーと証明書に必要です。
ステップ 4	**crypto key generate rsa** 例： `Device(config)# crypto key generate rsa`	（任意）RSA キーペアを生成します。RSA キーのペアは、スイッチの証明書を入手する前に必要です。RSA キーのペアは自動的に生成されます。必要であれば、このコマンドを使用してキーを再生成できます。
ステップ 5	**crypto ca trustpoint** *name* 例： `Device(config)# crypto ca trustpoint your_trustpoint`	CA のトラストポイントにローカルの設定名を指定して、CA トラストポイントコンフィギュレーションモードを開始します。
ステップ 6	**enrollment url** *url* 例： `Device(ca-trustpoint)# enrollment url http://your_server:80`	スイッチによる証明書要求の送信先の URL を指定します。
ステップ 7	**enrollment http-proxy** *host-name port-number* 例： `Device(ca-trustpoint)# enrollment http-proxy your_host 49`	（任意）HTTP プロキシサーバを経由して CA から証明書を入手するようにスイッチを設定します。 • *host-name* には、CA を取得するために使用するプロキシサーバを指定します。 • *port-number* には、CA にアクセスするために使用するポート番号を指定します。

	コマンドまたはアクション	目的
ステップ 8	**crlquery** *url* 例： `Device(ca-trustpoint)# crl query ldap://your_host:49`	ピアの証明書が取り消されていないかを確認するために、証明書失効リスト（CRL）を要求するようにスイッチを設定します。
ステップ 9	**primary** *name* 例： `Device(ca-trustpoint)# primary your_trustpoint`	（任意）トラストポイントが CA 要求に対してプライマリ（デフォルト）トラストポイントとして使用されるように指定します。 • *name* には、設定したトラストポイントを指定します。
ステップ 10	**exit** 例： `Device(ca-trustpoint)# exit`	CA トラストポイントコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 11	**crypto ca authentication** *name* 例： `Device(config)# crypto ca authentication your_trustpoint`	CA の公開キーを取得して CA を認証します。ステップ 5 で使用した名前と同じものを使用します。
ステップ 12	**crypto ca enroll** *name* 例： `Device(config)# crypto ca enroll your_trustpoint`	指定した CA トラストポイントから証明書を取得します。このコマンドは、各 RSA キーのペアに対して 1 つの署名入りの証明書を要求します。
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

セキュア HTTP サーバの設定

セキュア HTTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

始める前に

証明に証明書の認証を使用する場合、前の手順を使用してスイッチの CA トラストポイントを設定してから、HTTP サーバを有効にする必要があります。CA のトラストポイントを設定し

ていない場合、セキュア HTTP サーバを最初に有効にした時点で、自己署名証明書が生成されます。サーバを設定した後、標準およびセキュア HTTP サーバ両方に適用するオプション（パス、適用するアクセス リスト、最大接続数、またはタイムアウト ポリシー）を設定できます。

Web ブラウザを使用してセキュア HTTP 接続を確認するには、https://*URL* を入力します（URL は IP アドレス、またはサーバ スイッチのホスト名）。デフォルト ポート以外のポートを設定している場合、URL の後ろにポート番号も指定する必要があります。次に例を示します。

（注） AES256_SHA2 はサポートされません。

```
https://209.165.129:1026
```

または

```
https://host.domain.com:1026
```

アクセス リスト（IPv4 ACL のみ）を指定するための従来の **ip http access-class** *access-list-number* コマンドは廃止予定です。引き続きこのコマンドを使用して、HTTP サーバへのアクセスを許可するアクセス リストを指定できます。2 つの新しいコマンドは、IPv4 および IPv6 ACL を指定するためのサポートを有効にするために導入されました。これらは、IPv4 ACL を指定するための **ip http access-class ipv4** *access-list-name* | *access-list-number* と、IPv6 ACL を指定するための **ip http access-class ipv6** *access-list-name* です。警告メッセージの受信を防ぐために、新しい CLI の使用をお勧めします。

アクセス リストを指定する際は、次の考慮事項があります。

- 存在しないアクセス リストを指定すると、設定は実行されますが、次の警告メッセージを受信します。

  ```
  ACL being attached does not exist, please configure it
  ```

- HTTP サーバにアクセス リストを指定するために **ip http access-class** コマンドを使用すると、次の警告メッセージが表示されます。

  ```
  This CLI will be deprecated soon, Please use new CLI ip http
  access-class ipv4/ipv6 <access-list-name>| <access-list-number>
  ```

- **ip http access-class ipv4** *access-list-name* | *access-list-number* または **ip http access-class ipv6** *access-list-name* を使用する場合、**ip http access-class** を使用してアクセス リストがすでに設定されていると、次の警告メッセージが表示されます。

  ```
  Removing ip http access-class <access-list-number>
  ```

ip http access-class *access-list-number* と **ip http access-class ipv4** *access-list-name* | *access-list-number* は同じ機能を共有します。コマンドを実行するごとに、その前のコマンドのコンフィギュレーションは上書きされます。2 つのコマンドの設定間の次の組み合わせによって、実行コンフィギュレーションへの影響が説明されます。

- **ip http access-class** *access-list-number* がすでに設定されている場合、**ip http access-class ipv4** *access-list-number* コマンドを使用して設定しようとすると、**ip http access-class**

access-list-number の設定が削除され、**ip http access-class ipv4** *access-list-number* の設定が実行コンフィギュレーションに追加されます。

- **ip http access-class** *access-list-number* がすでに設定されている場合、**ip http access-class ipv4** *access-list-name* コマンドを使用して設定しようとすると、**ip http access-class** *access-list-number* の設定が削除され、**ip http access-class ipv4** *access-list-name* の設定が実行コンフィギュレーションに追加されます。
- **ip http access-class ipv4** *access-list-number* がすでに設定されている場合、**ip http access-class** *access-list-name* を使用して設定しようとすると、**ip http access-class ipv4** *access-list-number* の設定がコンフィギュレーションから削除され、**ip http access-class** *access-list-name* の設定が実行コンフィギュレーションに追加されます。
- **ip http access-class ipv4** *access-list-name* がすでに設定されている場合、**ip http access-class** *access-list-number* を使用して設定しようとすると、**ip http access-class ipv4** *access-list-name* の設定がコンフィギュレーションから削除され、**ip http access-class** *access-list-number* の設定が実行コンフィギュレーションに追加されます。

手順

	コマンドまたはアクション	目的

ステップ 1	**show ip http server status**
	例：
	`Device# show ip http server status`
		（任意）HTTP サーバのステータスを表示して、セキュア HTTP サーバの機能がソフトウェアでサポートされているかどうかを判断します。出力で、次のラインのどちらかを確認してください。
		`HTTP secure server capability: Present`
		または
		`HTTP secure server capability: Not present`

ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http secure-server** 例： `Device(config)# ip http secure-server`	HTTPS サーバがディセーブルの場合、イネーブルにします。HTTPS サーバは、デフォルトでイネーブルに設定されています。

	コマンドまたはアクション	目的
ステップ 4	**ip http secure-port** *port-number* 例： `Device(config)# ip http secure-port 443`	（任意）HTTPS サーバに使用するポート番号を指定します。デフォルトのポート番号は 443 です。443 または 1025 ～ 65535 の範囲で指定できます。
ステップ 5	**ip http secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]} 例： `Device(config)# ip http secure-ciphersuite rc4-128-md5`	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これはデフォルトです。
ステップ 6	**ip http secure-client-auth** 例： `Device(config)# ip http secure-client-auth`	（任意）HTTP サーバを設定して、接続処理の間、認証のために、クライアントからの X.509v3 証明書を要求します。デフォルトでは、クライアントがサーバからの証明書を要求する設定になっていますが、サーバはクライアントを認証しないようになっています。
ステップ 7	**ip http secure-trustpoint** *name* 例： `Device(config)# ip http secure-trustpoint your_trustpoint`	X.509v3 セキュリティ証明書の取得およびクライアントの証明書接続の認証に使用する CA のトラストポイントを指定します。 （注） このコマンドの使用は、前の手順に従って CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。
ステップ 8	**ip http path** *path-name* 例： `Device(config)# ip http path /your_server:80`	（任意）HTML ファイルのベースとなる HTTP パスを設定します。パスは、ローカル システムにある HTTP サーバファイルの場所を指定します（通常、システムのフラッシュ メモリを指定します）。

	コマンドまたはアクション	目的
ステップ 9	**ip http access-class** *access-list-number* 例： `Device(config)# ip http access-class 2`	（任意）HTTP サーバへのアクセスの許可に使用するアクセス リストを指定します。
ステップ 10	**ip http access-class** { **ipv4** {*access-list-number* | *access-list-name*} | **ipv6** {*access-list-name*} } 例： `Device(config)# ip http access-class ipv4 4`	（任意）HTTP サーバへのアクセスの許可に使用するアクセス リストを指定します。
ステップ 11	**ip http max-connections** *value* 例： `Device(config)# ip http max-connections 4`	（任意）HTTP サーバへの同時最大接続数を指定します。値は10以上にすることを推奨します。これは、UI が想定どおりに機能するために必要な値です。
ステップ 12	**ip http timeout-policy idle** *seconds* **life** *seconds* **requests** *value* 例： `Device(config)# ip http timeout-policy idle 120 life 240 requests 1`	（任意）指定の状況下における、HTTP サーバへの接続最大時間を指定します。 • **idle**：データの受信がないか、応答データが送信できない場合の最大時間。指定できる範囲は 1 ～ 600 秒です。デフォルト値は180秒（3 分）です。 • **life**：接続を確立している最大時間。指定できる範囲は 1 ～ 86400 秒（24時間）です。デフォルト値は 180 秒です。 • **requests**：永続的な接続で処理される要求の最大数。最大値は 86400 です。デフォルトは 1 です。
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

セキュア HTTP クライアントの設定

セキュア HTTP クライアントを設定するには、特権 EXEC モードで次の手順を実行します。

始める前に

標準の HTTP クライアントおよびセキュア HTTP クライアントは常にイネーブルです。証明書の認証にはセキュア HTTP クライアントの証明書が必要です。次の手順では、前の手順で CA のトラストポイントをスイッチに設定していることを前提にしています。CA のトラストポイントが設定されておらず、リモートの HTTPS サーバがクライアントの認証を要求した場合、セキュア HTTP クライアントへの接続は失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip http client secure-trustpoint** *name* 例： `Device(config)# ip http client secure-trustpoint your_trustpoint`	（任意）リモートの HTTP サーバがクライアント認証を要求した場合に使用する、CA のトラストポイントを指定します。このコマンドの使用は、前の手順を使用して CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。クライアント認証が必要ない場合、またはプライマリのトラストポイントがすでに設定されている場合は、このコマンドは任意です。
ステップ 3	**ip http client secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]} 例： `Device(config)# ip http client secure-ciphersuite rc4-128-md5`	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これはデフォルトです。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

セキュア HTTP サーバおよびクライアントのステータスのモニタリング

SSL セキュア サーバおよびクライアントのステータスをモニタするには、次の表の特権 EXEC コマンドを使用します。

表 *139 : SSL* セキュア サーバおよびクライアントのステータスを表示するコマンド

コマンド	目的
show ip http client secure status	セキュア HTTP クライアントの設定を表示します。
show ip http server secure status	セキュア HTTP サーバの設定を表示します。
show running-config	セキュア HTTP 接続に対して生成された自己署名証明書を表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セッションアウェアなネットワーキングに対するアイデンティティコントロール ポリシーおよびアイデンティティサービステンプレートの設定。	『Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Sw http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-boo

関連項目	マニュアル タイトル
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	『Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Sw http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 104 章

IPv4 ACL の設定

- 機能情報の確認 （2185 ページ）
- IPv4 アクセス コントロール リストを設定するための前提条件 （2185 ページ）
- IPv4 アクセス コントロール リストの設定に関する制約事項 （2186 ページ）
- ACL によるネットワーク セキュリティに関する情報 （2187 ページ）
- ACL の設定方法 （2203 ページ）
- IPv4 ACL のモニタリング （2225 ページ）
- ACL の設定例 （2226 ページ）
- その他の参考資料 （2241 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IPv4アクセスコントロールリストを設定するための前提条件

ここでは、アクセス コントロール リスト（ACL）によるネットワーク セキュリティの設定の前提条件を示します。

- LAN ベース フィーチャ セットが実行しているスイッチでは、VLAN マップはサポートされません。

IPv4アクセスコントロールリストの設定に関する制約事項

一般的なネットワーク セキュリティ

次は、ACL によるネットワーク セキュリティの設定の制約事項です。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。インターフェイスのパケット フィルタおよびルート フィルタ用の ACL では、名前を使用できます。また、VLAN マップでも名前を指定できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- **appletalk** は、コマンドラインのヘルプ ストリングに表示されますが、**deny** および **permit** MAC アクセス リスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。
- ACL ワイルドカードは、ダウンストリーム クライアント ポリシーではサポートされていません。

IPv4 ACL ネットワーク インターフェイス

次の制限事項が、ネットワーク インターフェイスへの IPv4 ACL に適用されます。

- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2（ポート）ACL はVLANインターフェイスに適用された入力方向のレイヤ3ACL、またはVLANに適用された VLAN マップよりも優先します。
- レイヤ 3 インターフェイスに ACL が適用され、スイッチ上でルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。
- パケットをフィルタリングするために **preauth_ipv4_acl** ACL が設定されている場合、ACL は認証後に削除されます。
- レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。

（注） パケットがレイヤ3インターフェイスのアクセス グループによって拒否された場合、デフォルトでは、ルータはICMP到達不能メッセージを送信します。アクセスグループによって拒否されたこれらのパケットはハードウェアでドロップされず、スイッチの CPU にブリッジングされて、ICMP到達不能メッセージを生成します。ポート ACL はICMP到達不能メッセージを生成しません。ICMP 到達不能メッセージは、ルータ ACL で **no ip unreachables** インターフェイス コマンドを使用してディセーブルにできます。

レイヤ 2 インターフェイスの MAC ACL

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に留意してください。

- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

（注） **mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用される場合のみ有効です。このコマンドは、EtherChannel ポート チャネルでは使用できません。

IP アクセス リスト エントリ シーケンス番号

- この機能は、ダイナミック アクセス リスト、再帰アクセス リスト、またはファイアウォール アクセス リストをサポートしていません。

関連トピック

インターフェイスへの IPv4 ACL の適用 （2216 ページ）
IPv4 ACL のインターフェイスに関する注意事項 （2202 ページ）
名前付き MAC 拡張 ACL の作成 （2217 ページ）
レイヤ 2 インターフェイスへの MAC ACL の適用 （2219 ページ）

ACL によるネットワーク セキュリティに関する情報

この章では、アクセス コントロール リスト（ACL）を使用して、スイッチのネットワーク セキュリティを設定する方法について説明します。コマンドや表では、ACL をアクセス リストと呼ぶこともあります。

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACL はルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスまたは VLAN（仮想 LAN）でパケットを許可、または拒否します。ACL は、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。パケットがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。スイッチは、VLAN 内でブリッジングされるパケットを含めて、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ 3 スイッチにアクセス リストを設定します。ACL を設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラフィックの種類を決定したりできます。たとえば、電子メール トラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。ACL を着信トラフィック、発信トラフィック、またはその両方をブロックするように設定することもできます。

アクセス コントロール エントリ

ACL には、アクセス コントロール エントリ（ACE）の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

ACL でサポートされるタイプ

スイッチは、IP ACL とイーサネット（MAC）ACL をサポートしています。

- IP ACL は、TCP、ユーザ データグラム プロトコル（UDP）、インターネット グループ管理プロトコル（IGMP）、およびインターネット制御メッセージプロトコル（ICMP）などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

このスイッチは、Quality of Service（QoS）分類 ACL もサポートしています。

サポートされる ACL

スイッチでは、トラフィックをフィルタリングするために、次に示す 3 種類の ACL がサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。レイヤ 2 インターフェイスに適用できるのは IP アクセス リストを 1 つと MAC アドレス リストを 1 つだけです。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御し、レイヤ 3 インターフェイスで特定の方向（着信または発信）に適用されます。
- VLAN ACL または VLAN マップは、すべてのパケット（ブリッジド パケットおよびルーテッド パケット）のアクセスを制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。VLAN マップは、IPv4 のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されています。イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプロトコルがアクセス コントロールされます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケット（ルーテッド パケットまたはブリッジド パケット）が VLAN マップと照合されます。パケットは、スイッチ ポートを介して、または、ルーティングされたパケットの場合、ルーテッド ポートを介して、VLAN に入ることができます。

ACL 優先順位

VLAN マップ、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、入力トラフィックの場合のフィルタの優先順位は上からポート ACL、VLAN マップ、およびルータ ACL です。出力トラフィックの場合、フィルタの優先順位は、ルータ ACL、VLAN マップ、ポート ACL です。

次の例で、簡単な使用例を説明します。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- スイッチ仮想インターフェイス（SVI）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。他のポートで受信した着信のルーティン

グ IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

関連トピック

IPv4 アクセス コントロール リストの設定に関する制約事項 （2186 ページ）

ポート ACL

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL を使用できるのは、物理インターフェイスだけです。EtherChannel インターフェイスでは使用できません。ポート ACL は、アウトバウンドおよびインバウンド方向のインターフェイスに適用できます。次のアクセス リストがサポートされています。

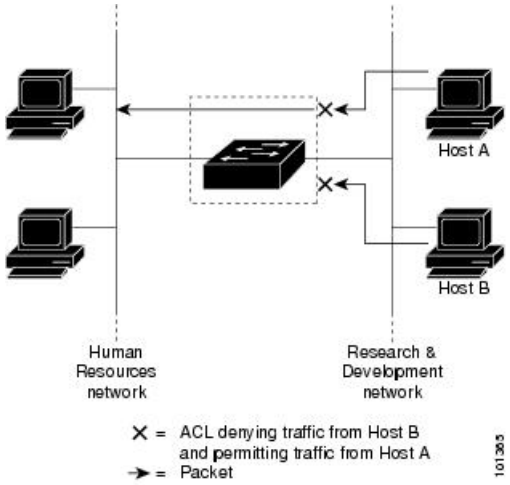
- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイス上の ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。

図 *109 : ACL* によるネットワーク内のトラフィックの制御

次に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマン リソース ネットワークにアクセスすることを許可しますが、ホスト B が

同一のネットワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2



インターフェイスだけに適用できます。

ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。

（注） レイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスであるスイッチ仮想インターフェイス（SVI）、物理層 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

スイッチは、IPv4 トラフィックの次のアクセス リストをサポートしています。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチはインターフェイスに設定されている機能に関連付けられている ACL が照合されます。 パケットがスイッチのインターフェイスに着信すると、その

インターフェイスに設定されているすべての着信機能に対応するACLが照合されます。パケットがルーティングされてからネクストホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACLを使用すると、ネットワーク全体またはネットワークの一部に対するアクセス コントロールが行えます。

VLAN マップ

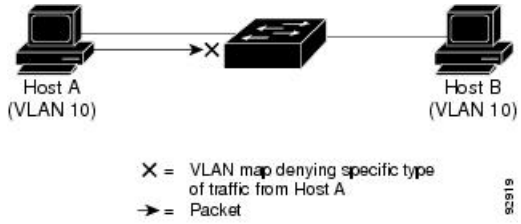
VLAN ACL または VLAN マップは、VLAN 内のネットワーク トラフィックを制御するために使用されます。スイッチまたはスイッチ スタックの VLAN 内でブリッジングされるすべてのパケットに VLAN マップを適用できます。VACL は、セキュリティ パケット フィルタリングおよび特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向（入力または出力）で定義されることはありません。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます（IP トラフィックは、MAC VACL マップではアクセス制御されません）。VLANマップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

VLANマップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

図 *110 : VLAN* マップによるトラフィックの制御

次に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用できます。



ACE およびフラグメント化されるトラフィックとフラグメント化されていないトラフィック

IPパケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

アクセス コントロール エントリ（ACE）には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化されたIPパケットのほとんどのフラグメントに標準的な方法では適用できません。

フラグメントにレイヤ4情報が含まれておらず、ACEが一部のレイヤ4情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ3情報（TCPやUDPなどのプロトコル タイプを含む）をチェックする許可ACEは、含まれていないレイヤ4情報の種類にかかわらず、フラグメントと一致すると見なされます。
- レイヤ4情報をチェックする拒否ACEは、フラグメントにレイヤ4情報が含まれていない限り、フラグメントと一致しません。

ACEおよびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例

次のコマンドで構成され、フラグメント化された3つのパケットに適用されるアクセス リスト102を例に取って説明します。

```
Device(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Device(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Device(config)# access-list 102 permit tcp any host 10.1.1.2
Device(config)# access-list 102 deny tcp any any
```

（注） 最初の2つのACEには宛先アドレスの後に *eq* キーワードがありますが、これは既知のTCP宛先ポート番号がそれぞれシンプル メール転送プロトコル（SMTP）およびTelnetと一致するかどうかをチェックすることを意味します。

- パケットAは、ホスト10.2.2.2のポート65000からホスト10.1.1.1のSMTPポートに送信されるTCPパケットです。このパケットがフラグメント化された場合、レイヤ4情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初のACE（permit）と一致します。残りのフラグメントも最初のACEと一致します。これは、それらのフラグメントにSMTPポート情報が含まれていなくても、最初のACEが適用されたときにレイヤ3情報だけをチェックするからです。この例の情報は、パケットがTCPであることと、宛先が10.1.1.1であることです。
- パケットBは、ホスト10.2.2.2のポート65001からホスト10.1.1.2のTelnetポートに送信されます。このパケットがフラグメント化された場合、レイヤ3情報とレイヤ4情報がすべて揃っているため、最初のフラグメントが2つめのACE（deny）と一致します。残りのフラグメントは、レイヤ4情報が含まれていないため、2つめのACEと一致しません。残りのフラグメントは3つめのACE（permit）と一致します。

  最初のフラグメントが拒否されたため、ホスト10.1.1.2は完全なパケットを再構成できず、その結果、パケットBは拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト10.1.1.2がパケットを再構成しようとするときにホストのリソースが消費されます。
- フラグメント化されたパケットCは、ホスト10.2.2.2のポート65001からホスト10.1.1.3のポートftpに送信されます。このパケットがフラグメント化された場合、最初のフラグ

メントが 4 つめの ACE（deny）と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

ACL とスイッチ スタック

スイッチ スタックの ACL サポートは、スタンドアロン スイッチと同じです。ACL の構成情報は、スタック内のすべてのスイッチに送信されます。アクティブ スイッチを含むスタック内のすべてのスイッチでは、情報が処理され、ハードウェアがプログラムされます。

アクティブ スイッチおよび ACL の機能

アクティブ スイッチにより、次の ACL 機能が実行されます。

- ACL 構成情報が処理され、情報がすべてのスタック メンバに送信されます。
- ACL 情報は、スタックに加入しているすべてのスイッチに配信されます。
- （たとえば、十分なハードウェア リソースがないなど）何らかの理由で、ソフトウェアによってパケットが送信される必要がある場合、ACL をパケットに適用後にのみ、アクティブ スイッチによってパケットが転送されます。
- そのハードウェアは、処理する ACL 情報でプログラムされます。

スタック メンバおよび ACL の機能

スタック メンバにより、次の ACL 機能が実行されます。

- スタック メンバでは、アクティブ スイッチから ACL 情報を受信し、ハードウェアがプログラムされます。
- スタンバイ スイッチとして設定されたスタック メンバがアクティブ スイッチが失敗したイベント内のアクティブ スイッチ機能を実行します。

アクティブ スイッチの障害および ACL

アクティブとスタンバイの両方のスイッチに ACL 情報があります。アクティブ スイッチに障害が発生すると、スタンバイが役割を引き継ぎます。新しいアクティブスイッチにより、すべてのスタック メンバーに ACL 情報が配信されます。

標準 IPv4 ACL および拡張 IPv4 ACL

ここでは、IP ACL について説明します。

ACL は、許可条件と拒否条件の順序付けられた集まりです。スイッチは、アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致する最初の条件が見つ

かった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、IPv4 について次の ACL（アクセス リスト）をサポートします。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることもできます。

IPv4 ACL スイッチでサポートされていない機能

このスイッチで IP v4ACL を設定する手順は、他の Cisco スイッチやルータで IP v4ACL を設定する手順と同じです。

以下の ACL 関連の機能はサポートされていません。

- 非 IP プロトコル ACL
- IP アカウンティング
- 再帰 ACL およびダイナミック ACL はサポートされていません。

アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。

次の一覧に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト（1 ～ 199 および 1300 ～ 2699）をサポートします。

表 *140*：アクセス リスト番号

アクセス リスト番号	タイプ	サポートあり
1 ～ 99	IP 標準アクセス リスト	Yes
100 ～ 199	IP 拡張アクセス リスト	Yes
200 ～ 299	プロトコルタイプコードアクセス リスト	なし
300 ～ 399	DECnet アクセス リスト	なし
400 ～ 499	XNS 標準アクセス リスト	なし
500 ～ 599	XNS 拡張アクセス リスト	なし
600 ～ 699	AppleTalk アクセス リスト	なし
700 ～ 799	48 ビット MAC アドレス アクセス リスト	なし

アクセス リスト番号	タイプ	サポートあり
800 ～ 899	IPX 標準アクセス リスト	なし
900 ～ 999	IPX 拡張アクセス リスト	なし
1000 ～ 1099	IPX SAP アクセス リスト	なし
1100 ～ 1199	拡張 48 ビット MAC サマリー アドレス アクセス リスト	なし
1200 ～ 1299	IPX サマリー アドレス アクセス リスト	なし
1300 ～ 1999	IP 標準アクセス リスト（拡張範囲）	Yes
2000 ～ 2699	IP 拡張アクセス リスト（拡張範囲）	Yes

番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

番号付き標準 IPv4 ACL

ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

スイッチは、**host** 一致条件があるエントリと *don't care* マスク 0.0.0.0 を含む一致条件があるエントリがリストの先頭に移動し、0 以外の *don't care* マスクを含むエントリよりも前に位置するように、標準アクセス リストの順序を書き換えます。そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号付き標準 IPv4 ACL を VLAN、端末回線、またはインターフェイスに適用できます。

番号付き拡張 IPv4 ACL

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコルタイプ情報を使用して制御のきめ細かさを高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

このスイッチは、ダイナミックまたはリフレクシブアクセスリストをサポートしていません。また、タイプ オブ サービス（ToS）の minimize-monetary-cost ビットに基づくフィルタリングもサポートしていません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

拡張 TCP、UDP、ICMP、IGMP、またはその他の IP ACL を定義できます。また、このスイッチはこれらの IP プロトコルをサポートします。

（注） ICMP エコー応答はフィルタリングできません。他の ICMP コードまたはタイプは、すべてフィルタリングできます。

これらの IP プロトコルがサポートされます。

- 認証ヘッダー プロトコル（**ahp**）
- 暗号ペイロード（**esp**）
- Enhanced Interior Gateway Routing Protocol（**eigrp**）
- 総称ルーティング カプセル化（**gre**）
- インターネット制御メッセージ プロトコル（**icmp**）
- インターネット グループ管理プロトコル（**igmp**）
- すべての内部プロトコル（**ip**）
- IP in IP トンネリング（**ipinip**）
- KA9Q NOS 互換 IP over IP トンネリング（**nos**）
- Open Shortest Path First ルーティング（**ospf**）
- ペイロード圧縮プロトコル（**pcp**）
- プロトコル独立型マルチキャスト（**pim**）
- 伝送制御プロトコル（**tcp**）
- ユーザ データグラム プロトコル（**udp**）

名前付き IPv4 ACL

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング（名前）を使用できます。名前付き ACL を使用すると、ルータ上で番号付きアクセス リストの場合より多くの IPv4 アクセス リストを設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付きアクセス リストで使用できるわけではありません。

（注） 標準ACLまたは拡張ACLに指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。標準IP ACLの名前は1 ～ 99です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定するときには、次の注意事項に留意してください。

- また、番号付き ACL も使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- VLAN マップには、標準 ACL または拡張 ACL（名前付きまたは番号付き）を使用できます。

ACL ロギング

標準IPアクセス リストによって許可または拒否されたパケットに関するログ メッセージが、スイッチのソフトウェアによって表示されます。つまり、ACLと一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、syslogメッセージを管理する logging console **logging console** コマンドで管理されます。

（注） ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可（*permit*）または拒否（*deny*）ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

（注） ロギング メッセージが多すぎて処理できない場合、または1秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作によって、ロギング パケットが多すぎてルータがクラッシュすることを回避します。そのため、課金ツールや、アクセス リストと一致する数の正確な情報源としてロギング設備をを使用しないでください。

ハードウェアおよびソフトウェアによる IP ACL の処理

ACL 処理はハードウェアで実行されます。ハードウェアで ACL の設定を保存する領域が不足すると、そのインターフェイス上のすべてのパケットがドロップします。

（注） スイッチまたはスタック メンバーのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受けるのは、スイッチに着信した該当 VLAN 内のトラフィックだけです。

ルータ ACL の場合は、次の場合にパケットが CPU に送信されることがあります。

- **log** キーワードを使用する。
- ICMP 到達不能メッセージを生成する。

show ip access-lists 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。スイッチド パケットおよびルーテッド パケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、 **show platform acl counters hardware** 特権 EXEC コマンドを使用します。

ルータ ACL の機能は、次のとおりです。

- 標準 ACL および拡張 ACL（入力および出力）の許可アクションや拒否アクションをハードウェアで制御し、アクセス コントロールのセキュリティを強化します。
- *ip unreachables* がディセーブルの場合、**log** を指定しないと、セキュリティ ACL の *deny* ステートメントと一致するフローがハードウェアによってドロップされます。許可ステートメントと一致するフローは、ハードウェアでスイッチングされます。
- ルータ ACL の ACE に **log** キーワードを追加すると、パケットのコピーが CPU に送信され、ロギングだけが行われます。ACE が許可ステートメントの場合も、パケットはハードウェアでスイッチングおよびルーティングされます。

VLAN マップの設定時の注意事項

VLAN マップは、VLAN 内でフィルタリングを制御する唯一の方法です。VLAN マップには方向の指定がありません。VLAN マップを使用して、特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。VLAN マップ内に該当パケット タイプ（IP または MAC）に対する match 句がある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットはドロップされます。該当パケット タイプに対する match コマンドがない場合、デフォルトでは、パケットが転送されます。

次は、VLAN マップ設定の注意事項です。

- インターフェイスでトラフィックを拒否するように設定された ACL がなく、VLAN マップが設定されていない場合、すべてのトラフィックが許可されます。

- 各 VLAN マップは一連のエントリで構成されます。VLAN マップのエントリの順序は重要です。スイッチに着信したパケットは、VLANマップの最初のエントリに対してテストされます。一致した場合は、VLANマップのその部分に指定されたアクションが実行されます。一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。
- 該当パケット タイプ（IP または MAC）に対する match 句が VLAN マップに 1 つまたは複数ある場合でも、パケットがそれらの match 句に一致しない場合、デフォルトではパケットがドロップされます。該当パケット タイプに対する match 句が VLAN マップ内にない場合、デフォルトではパケットが転送されます。
- VLAN マップのロギングはサポートされていません。
- レイヤ 2 インターフェイスに適用された IP アクセス リストまた MAC アクセス リストがスイッチにあって、ポートが属する VLAN に VLAN マップを適用する場合、ポート ACL が VLAN マップに優先します。
- ハードウェアに VLAN マップの設定を適用できない場合は、その VLAN 内のすべてのパケットがドロップします。

VLAN マップとルータ ACL

ブリッジングされたトラフィックおよびルーティングされたトラフィックの両方に対してアクセス コントロールを行うには、VLANマップを単独で使用するか、またはルータ ACL と VLAN マップを組み合わせて使用します。入力と出力両方のルーテッド VLAN インターフェイスでルータ ACL を定義したり、ブリッジングされたトラフィックのアクセスをコントロールする VLAN マップを定義したりできます。

パケット フローが ACL 内 VLAN マップの deny ステートメントと一致した場合、ルータ ACL の設定に関係なく、パケット フローは拒否されます。

（注） ルータ ACL を VLAN マップと組み合わせて使用し、ルータ ACL でのロギングを必要とするパケットが VLAN マップで拒否された場合、これらのパケットはロギングされません。

該当パケット タイプ（IP または MAC）に対する match 句が VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトではパケットがドロップされます。VLAN マップ内に match 句がなく、アクションが指定されていない場合、どの VLAN マップ エントリとも一致しないパケットは転送されます。

VLAN マップとルータ ACL の設定時の注意事項

ここに記載された注意事項は、ルータ ACL および VLAN マップを同じ VLAN 上で使用する必要がある設定に適用されます。ルータ ACL および VLAN マップを異なる VLAN に割り当てる設定には、これらの注意事項は適用されません。

ルータ ACL および VLAN マップを同じ VLAN に設定する必要がある場合は、ルータ ACL と VLAN マップの両方の設定に関し、ここで説明する注意事項に従ってください。

- VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつに限り設定できます。
- 可能な限り、すべてのエントリのアクションが同一で、末尾のデフォルトアクションだけが反対のタイプとなるように ACL を記述します。次のいずれかの形式を使用して、ACL を記述します。

  permit... permit... permit... deny ip any any

  または

  deny... deny... deny... permit ip any any
- ACL 内で複数のアクション（許可、拒否）を定義する場合は、それぞれのアクション タイプをまとめて、エントリ数を削減します。
- ACL 内にレイヤ 4 情報を指定しないでください。レイヤ 4 情報を追加すると、統合プロセスが複雑になります。ACL のフィルタリングが、full-flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）でなく、IP アドレス（送信元および宛先）に基づいて行われる場合に、最適な統合結果が得られます。可能な限り、IP アドレスには *don't care* ビットを使用してください。

  IP ACE とレイヤ 4 情報を含む TCP/UDP/ICMP ACE が両方とも ACL 内に存在し、full-flow モードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

ACL の時間範囲

time-range グローバル コンフィギュレーション コマンドを使用することによって、時刻および曜日に基づいて拡張 ACL を選択的に適用できます。まず、時間範囲の名前を定義し、その時間範囲内の時刻および日付または曜日を設定します。次に、ACL を適用してアクセス リストに制限を設定するときに時間範囲を入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間（指定期間内や指定曜日など）を定義できます。**time-range** キーワードおよび引数については、名前付きおよび番号付き拡張 ACL タスクの表を参照してください。

時間範囲を使用するいくつかの利点を次に示します。

- アプリケーションなどのリソース（IP アドレスとマスクのペア、およびポート番号で識別）へのユーザ アクセスをより厳密に許可または拒否できます。
- ログ メッセージを制御できます。ACL エントリを使用して特定の時刻に関してのみトラフィックをロギングできるため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセス リストを使用すると、CPU に負荷が生じます。これは、アクセス リストの新規設定を他の機能や、ハードウェア メモリにロードされた結合済みの設定とマージする

必要があるためです。そのため、複数のアクセスリストが短期間に連続して（互いに数分以内に）有効となるような設定とならないように注意する必要があります。

（注） 時間範囲は、スイッチのシステム クロックに基づきます。したがって、信頼できるクロックソースが必要です。ネットワーク タイム プロトコル（NTP）を使用してスイッチ クロックを同期させることを推奨します。

関連トピック

ACL の時間範囲の設定 （2213 ページ）

IPv4 ACL のインターフェイスに関する注意事項

ip access-group インターフェイス コンフィギュレーション コマンドをレイヤ 3 インターフェイス（SVI、レイヤ 3 EtherChannel、またはルーテッド ポート）に適用するには、そのインターフェイスに IP アドレスが設定されている必要があります。レイヤ 3 アクセス グループは、CPU のレイヤ 3 プロセスによってルーティングまたは受信されるパケットをフィルタリングします。このグループは、VLAN 内でブリッジングされるパケットに影響を与えません。

着信 ACL の場合、パケットの受信後スイッチはパケットを ACL と照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

発信 ACL の場合、パケットを受信し制御対象インターフェイスにルーティングしたあと、スイッチはパケットを ACL と照合します。ACL がパケットを許可した場合は、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスの ACL または発信インターフェイスの ACL のいずれであっても、常に入力インターフェイスから ICMP 到達不能メッセージが送信されます。ICMP 到達不能メッセージは通常、入力インターフェイス 1 つにつき、0.5 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

関連トピック

インターフェイスへの IPv4 ACL の適用 （2216 ページ）
IPv4 アクセス コントロール リストの設定に関する制約事項 （2186 ページ）

ACL の設定方法

IPv4 ACL の設定

このスイッチで IP ACL を使用する手順は次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。	
ステップ 2	その ACL をインターフェイスまたは端末回線に適用します。標準および拡張 IP ACL を VLAN マップに適用することもできます。	

番号付き標準 ACL の作成

番号付き標準 ACL を作成するには、次の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source source-wildcard* [**log**] 例： `Device(config)# access-list 2 deny your_host`	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。 *access-list-number* には、1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。

	コマンドまたはアクション	目的
		条件が一致した場合にアクセスを拒否する場合は **deny**、許可する場合は **permit** を指定します。 *source* には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • キーワード **any** は 0.0.0.0 255.255.255.255 という *source* および *source-wildcard* の省略形です。source-wildcard を入力する必要はありません。 • キーワード **host** は送信元および *source* 0.0.0.0 の *source-wildcard* の省略形です。 （任意）*source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 （任意）**log** を入力すると、エントリと一致するパケットの詳細を示すロギングメッセージがコンソールに送信されます。 **（注）** ロギングは、レイヤ 3 インターフェイスに割り当てられた ACL でだけサポートされます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN マップの設定 （2220 ページ）

番号付き拡張 ACL の作成

番号付き拡張 ACL を作成するには、次の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** tos] [**fragments**] [**log** [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `Device(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log`	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 *access-list-number* には、100 ～ 199 または 2000 ～ 2699 の 10 進数を指定します。 条件が一致した場合にパケットを拒否する場合は **deny**、許可する場合は **permit** を指定します。 *protocol* には、IP プロトコルの名前または番号を指定します。**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、または **udp**、あるいは IP プロトコル番号を表す 0 ~ 255 の範囲の整数を使用できます。一致条件としてインターネット プロトコル（ICMP、TCP、UDP など）を指定するには、キーワード **ip** を使用します。

	コマンドまたはアクション	目的
		（注） この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加の特定パラメータについては、次のステップを参照してください。 *source* には、パラメータの送信元であるネットワークまたはホストの番号を指定します。 *source-wildcard* は、ワイルドカードビットを送信元アドレスに適用します。 *destination* には、パラメータの宛先であるネットワークまたはホストの番号を指定します。 *destination-wildcard* は、ワイルドカードビットを宛先アドレスに適用します。 source、source-wildcard、destination、および destination-wildcard の値は、次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード **any**。 • 単一のホスト 0.0.0.0 を表すキーワード **host**。 その他のキーワードはオプションであり、次の意味を持ちます。 • **precedence**：パケットを 0 ～ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、**routine**（0）、**priority**（1）、**immediate**（2）、**flash**（3）、**flash-override**（4）、**critical**（5）、**internet**（6）、**network**（7）です。

	コマンドまたはアクション	目的
		• **fragments**：2 つ目以降のフラグメントをチェックする場合に入力します。 • **tos**：パケットを 0 ～ 15 の番号または名前で指定するサービス タイプ レベルと一致させる場合に入力します。指定できる値は、**normal**（0）、**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）です。 • **log**：エントリと一致するパケットに関するログ通知メッセージを作成し、コンソールに送信します。**log-input** を指定すると、ログ エントリに入力インターフェイスが追加されます。 • **time-range**：時間範囲の名前を指定します。 • **dscp**：パケットを 0 ～ 63 の番号で指定する DSCP 値と一致させる場合に入力します。また、指定できる値のリストを表示するには、疑問符（?）を使用します。 （注） **dscp** 値を入力した場合、**tos** または **precedence** は入力できません。**dscp** を入力しない場合は、**tos** と **precedence** 値の両方を入力できます。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log** [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] [*flag*] 例： `Device(config)# access-list 101 permit tcp any any eq 500`	拡張 TCP アクセス リストおよびアクセス条件を定義します。 次に示す例外を除き、拡張 IPv4 ACL に対して説明するパラメータと同じパラメータを使用します。 （任意）*operator* および *port* を入力すると、送信元ポート（*source source-wildcard* の後に入力した場合）または宛先ポート（*destination destination-wildcard* の後に入力した場

	コマンドまたはアクション	目的
		合）が比較されます。使用可能な演算子は、**eq**（等しい）、**gt**（より大きい）、**lt**（より小さい）、**neq**（等しくない）、**range**（包含範囲）などです。演算子にはポート番号を指定する必要があります（range の場合は 2 つのポート番号をスペースで区切って指定する必要があります）。 *port* には、10 進数（0 ～ 65535）のポート番号または TCP ポート名を入力します。TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。 他のオプションのキーワードの意味は次のとおりです。 • **established**：確立された接続と照合する場合に入力します。このキーワードは、**ack** または **rst** フラグでの照合と同じ機能を果たします。 • *flag*：指定された TCP ヘッダー ビットを基準にして照合します。入力できるフラグは、**ack**（確認応答）、**fin**（終了）、**psh**（プッシュ）、**rst**（リセット）、**syn**（同期）、または **urg**（緊急）です。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log** [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `Device(config)# access-list 101 permit udp any any eq 100`	（任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。 UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[operator [port]] ポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP では、**flag** および **established** キーワードは無効です。
ステップ 5	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*]	拡張 ICMP アクセス リストおよびアクセス条件を定義します。 ICMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほ

	コマンドまたはアクション	目的
	[**fragments**] [**log** [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `Device(config)# access-list 101 permit icmp any any 200`	とんど同じですが、ICMP メッセージタイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0～255 です。 • *icmp-code*：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。
ステップ 6	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log** [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `Device(config)# access-list 101 permit igmp any any 14`	（任意）拡張 IGMP アクセス リストおよびアクセス条件を定義します。 IGMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。 *igmp-type*：IGMP メッセージタイプと照合するには、0 ～ 15 の番号を入力するか、またはメッセージ名である **dvmrp**、**host-query**、**host-report**、**pim**、または **trace** を入力します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

VLAN マップの設定 （2220 ページ）

名前付き標準 ACL の作成

名前を使用して標準 ACL を作成するには、次の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list standard** *name* 例： `Device(config)# ip access-list standard 20`	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、1 ～ 99 の番号を使用できます。

ステップ 4	次のいずれかを使用します。
	• **deny** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]
	• **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]
	例：
	`Device(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255`
	または
	`Device(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0`
		アクセス リスト コンフィギュレーション モードで、パケットを転送するのかドロップするのかを決定する 1 つ以上の拒否条件または許可条件を指定します。
		• **host** *source*：送信元および送信元ワイルドカードの値である *source* 0.0.0.0。
		• **any**：送信元および送信元ワイルドカードの値である 0.0.0.0 255.255.255.255

ステップ 5	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-std-nacl)# end`	
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

名前付き拡張 ACL の作成

名前を使用して拡張 ACL を作成するには、次の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list extended** *name* 例： `Device(config)# ip access-list extended 150`	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、100 ～ 199 の番号を使用できます。
ステップ 4	{**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host** *source* | **any**} {*destination* [*destination-wildcard*] | host *destination* | **any**} [**precedence** *precedence*]	アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。**log** キーワードを使用し

	コマンドまたはアクション	目的
	[**tos** *tos*] [**established**] [**log**] [**time-range** *time-range-name*] 例： `Device(config-ext-nacl)# permit 0 any any`	て、違反を含む、アクセス リスト ロギング メッセージを取得します。 • **host** *source*：送信元および送信元ワイルドカードの値である *source* 0.0.0.0。 • **host** *destination*：接続先および接続先ワイルドカードの値である *destination* 0.0.0.0。 • **any**：source および source wildcard の値または destination および destination wildcard の値である 0.0.0.0 255.255.255.255
ステップ 5	**end** 例： `Device(config-ext-nacl)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、関連付けられた IP ホスト アドレス アクセス リストの指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に選択的に追加できません。ただし、**no permit** および **no deny** アクセス リスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

次のタスク

作成した名前付き ACL は、インターフェイスまたは VLAN に適用できます。

ACL の時間範囲の設定

ACL の時間範囲パラメータを設定するには、次の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device(config)# enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**time-range** *time-range-name* 例： `Device(config)# time-range workhours`	作成する時間範囲には意味のある名前（*workhours* など）を割り当て、時間範囲コンフィギュレーション モードを開始します。名前にスペースや疑問符を含めることはできません。また、文字から始める必要があります。

ステップ 4	次のいずれかを使用します。
	• **absolute** [**start** *time date*] [**end** *time date*]
	• **periodic** *day-of-the-week hh:mm to* [*day-of-the-week*] *hh:mm*
	• **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*
	例：
	`Device(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006`
	または
	`Device(config-time-range)# periodic`
		適用対象の機能がいつ動作可能になるかを指定します。
		• 時間範囲には、**absolute** ステートメントを 1 つだけ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。
		• 複数の **periodic** ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。
		設定例を参照してください。

	コマンドまたはアクション	目的
	`weekdays 8:00 to 12:00`	
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

複数の項目をそれぞれ異なる時間に有効にする場合は、上記の手順を繰り返してください。

関連トピック

ACL の時間範囲 （2201 ページ）

端末回線への IPv4 ACL の適用

番号付き ACL を使用して、1 つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

仮想端末回線と ACL に指定されたアドレス間の着信接続および発信接続を制限するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device(config)# enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** [**console** | **vty**] *line-number* 例： `Device(config)# line console 0`	設定する回線を指定し、インライン コンフィギュレーション モードを開始します。 • **console**：コンソール端末回線を指定します。コンソール ポートは DCE です。 • **vty**：リモート コンソール アクセス用の仮想端末を指定します。 *line-number* は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。指定できる範囲は0～16です。
ステップ 4	**access-class** *access-list-number* {**in** | **out**} 例： `Device(config-line)# access-class 10 in`	（デバイスへの）特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信接続および発信接続を制限します。
ステップ 5	**end** 例： `Device(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスへの IPv4 ACL の適用

ここでは、IPv4 ACL をネットワーク インターフェイスへ適用する方法について説明します。

インターフェイスへのアクセスを制御する管理には、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスには、レイヤ 2 インターフェイス（ポート ACL）またはレイヤ 3 インターフェイス（ルータ ACL）を指定できます。
ステップ 3	**ip access-group** {*access-list-number* | *name*} {**in** | **out**} 例： `Device(config-if)# ip access-group 2 in`	指定されたインターフェイスへのアクセスを制御します。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

関連トピック

IPv4 ACL のインターフェイスに関する注意事項 （2202 ページ）
IPv4 アクセス コントロール リストの設定に関する制約事項 （2186 ページ）

名前付き MAC 拡張 ACL の作成

VLAN またはレイヤ 2 インターフェイスで非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。その手順は、他の名前付き拡張 ACL を設定する場合と同様です。

名前付き MAC 拡張 ACL を作成するには、次の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mac access-list extended** *name* 例： `Device(config)# mac access-list extended mac1`	名前を使用して MAC 拡張アクセス リストを定義します。
ステップ 4	{**deny** | **permit**} {**any** | **host** *source MAC address* | *source MAC address mask*} {**any** | **host** *destination MAC address* | *destination MAC address mask*} [*type mask* | **lsap** *lsap mask* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp** | 0-*65535*] [**cos** *cos*]	拡張 MAC アクセス リスト コンフィギュレーション モードでは、すべての（**any**）送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定のホスト（**host**）送信元 MAC アドレス、およびすべての（any）宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに、**permit** または **deny** を指定します。

	コマンドまたはアクション	目的

	例：
	
	`Device(config-ext-macl)# deny any any decnet-iv`
	
	または
	
	`Device(config-ext-macl)# permit any any`
		（任意）次のオプションを入力することもできます。
		• *type mask*：Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号。10 進数、16 進数、または 8 進数で表記できます。一致検査の前に、任意で指定できる *don't care* ビットのマスクが EtherType に適用されます。
		• **lsap** *lsap mask*：IEEE 802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。任意で *don't care* ビットのマスクを指定できます。
		• **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**：非 IP プロトコル。
		• **cos** *cos*：プライオリティを設定する 0 ～ 7 の IEEE 802.1Q CoS 番号。

ステップ 5	**end** 例： `Device(config-ext-macl)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv4 アクセス コントロール リストの設定に関する制約事項 （2186 ページ）
VLAN マップの設定 （2220 ページ）

レイヤ 2 インターフェイスへの MAC ACL の適用

レイヤ 2 インターフェイスへのアクセスを制御するために MAC アクセス リストを適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。指定するインターフェイスは物理レイヤ2インターフェイス（ポート ACL）でなければなりません。
ステップ 4	**mac access-group** {*name*} {**in** | **out** } 例： `Device(config-if)# mac access-group mac1 in`	MAC アクセス リストを使用して、指定されたインターフェイスへのアクセスを制御します。 ポート ACL は発信および着信方向サポートされます。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show mac access-group** [**interface** *interface-id*] 例：	そのインターフェイスまたはすべてのレイヤ2インターフェイスに適用されている MAC アクセス リストを表示します。

	コマンドまたはアクション	目的
	`Device# show mac access-group interface gigabitethernet1/0/2`	
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチは、パケットを受信すると、着信 ACL とパケットを照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

関連トピック

IPv4 アクセス コントロール リストの設定に関する制約事項 （2186 ページ）

VLAN マップの設定

VLAN マップを作成して、1 つまたは複数の VLAN に適用するには、次のステップを実行します。

始める前に

VLAN に適用する標準 IPv4 ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan access-map** *name* [**number**] 例： `Device(config)# vlan access-map map_1 20`	VLAN マップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。 同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てら

	コマンドまたはアクション	目的
		れます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。 VLAN マップでは、特定の permit または deny キーワードを使用しません。VLANマップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致するという意味です。ACL 内の deny は、一致しないという意味です。 このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。
ステップ 2	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*] 例： `Device(config-access-map)# match ip address ip2`	1 つまたは複数の標準または拡張アクセス リストに対してパケットを照合します（IP またはMAC アドレスを使用）。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ照合されます。 （注） パケット タイプ（IP または MAC）に対する match 句が VLAN マップに設定されている場合で、そのマップ アクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。match 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。
ステップ 3	IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1 つ以上の ACL（標準または拡	マップ エントリに対するアクションを設定します。

	コマンドまたはアクション	目的

	張）とそのパケットを照合するには、次のコマンドのいずれかを入力します。
	• **action** { **forward**}
	`Device(config-access-map)# action forward`
	• **action** { **drop**}
	`Device(config-access-map)# action drop`	

ステップ 4	**vlan filter** *mapname* **vlan-list** *list* 例： `Device(config)# vlan filter map 1 vlan-list 20-22`	VLANマップを1つまたは複数のVLANに適用します。 listには単一のVLAN ID（22）、連続した範囲（10 ～ 22）、またはVLAN IDのストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。

関連トピック

番号付き標準 ACL の作成 （2203 ページ）
番号付き拡張 ACL の作成 （2205 ページ）
名前付き MAC 拡張 ACL の作成 （2217 ページ）
VLAN マップの作成 （2222 ページ）
VLAN への VLAN マップの適用 （2224 ページ）

VLAN マップの作成

各 VLAN マップは順番に並べられた一連のエントリで構成されます。VLAN マップ エントリを作成、追加、または削除するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**vlan access-map** *name* [**number**] 例： `Device(config)# vlan access-map map_1 20`	VLANマップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。 同じ名前のVLANマップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。 VLAN マップでは、特定の permit または deny キーワードを使用しません。VLANマップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致するという意味です。ACL 内の deny は、一致しないという意味です。 このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。
ステップ 3	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*] 例： `Device(config-access-map)# match ip address ip2`	1 つまたは複数の標準または拡張アクセス リストに対してパケットを照合します（IP またはMAC アドレスを使用）。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ照合されます。
ステップ 4	**action** {**drop** | **forward**} 例： `Device(config-access-map)# action forward`	（任意）マップ エントリに対するアクションを設定します。デフォルトは転送（forward）です。
ステップ 5	**end** 例： `Device(config-access-map)# end`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Device# show running-config`	アクセス リストの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN マップの設定 （2220 ページ）

VLAN への VLAN マップの適用

1 つの VLAN マップを 1 つまたは複数の VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan filter** *mapname***vlan-list** *list* 例： `Device(config)# vlan filter map 1 vlan-list 20-22`	VLANマップを1つまたは複数のVLANに適用します。 listには単一のVLAN ID（22）、連続した範囲（10 ～ 22）、または VLAN ID のストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN マップの設定 （2220 ページ）

IPv4 ACL のモニタリング

スイッチに設定されている ACL、およびインターフェイスと VLAN に適用された ACL を表示して IPv4 ACL をモニタできます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 またはレイヤ 3 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセス グループを表示できます。また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、次の表に記載された特権 EXEC コマンドを使用します。

表 *141*：アクセス リストおよびアクセス グループを表示するコマンド

コマンド	目的
show access-lists [*number* | *name*]	最新の IP および MAC アドレス アクセス リストの全体やその一部、または特定のアクセス リスト（番号付きまたは名前付き）の内容を表示します。
show ip access-lists [*number* | *name*]	最新の IP アクセス リスト全体、または特定の IP アクセス リスト（番号付きまたは名前付き）を表示します。

コマンド	目的
show ip interface *interface-id*	インターフェイスの詳細設定およびステータスを表示します。IP がイネーブルになっているインターフェイスに、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示されます。
show running-config [**interface** *interface-id*]	スイッチまたは指定されたインターフェイスのコンフィギュレーションファイルの内容（設定されたすべての MAC および IP アクセス リストや、どのアクセスグループがインターフェイスに適用されたかなど）を表示します。
show mac access-group [**interface** *interface-id*]	すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リスト を表示します。

ACL の設定例

例：ACL での時間範囲を使用

次の例に、*workhours*（営業時間）の時間範囲および会社の休日（2006 年 1 月 1 日）を設定し、設定を確認する例を示します。

```
Device# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に時間範囲名を入力します。次に、拡張アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての TCP トラフィックを許可します。

```
Device(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Device(config)# access-list 188 permit tcp any any time-range workhours
Device(config)# end
Device# show access-lists
Extended IP access list 188
   10 deny tcp any any time-range new_year_day_2006 (inactive)
   20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
Device(config)# ip access-list extended deny_access
Device(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Device(config-ext-nacl)# exit
Device(config)# ip access-list extended may_access
Device(config-ext-nacl)# permit tcp any any time-range workhours
Device(config-ext-nacl)# end
Device# show ip access-lists
Extended IP access list lpip_default
    10 permit ip any any
Extended IP access list deny_access
    10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
    10 permit tcp any any time-range workhours (inactive)
```

例：ACL へのコメントの挿入

remark キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント（注釈）を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、permit ステートメントまたは deny ステートメントの前後どちらにでも配置できます。コメントがどの permit ステートメントまたは deny ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する permit または deny ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list** *access-list number* **remark** *remark* グローバル コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
Device(config)# access-list 1 remark Permit only Jones workstation through
Device(config)# access-list 1 permit 171.69.2.88
Device(config)# access-list 1 remark Do not allow Smith through
Device(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリには、**remark** アクセス リスト コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

```
Device(config)# ip access-list extended telnetting
Device(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Device(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

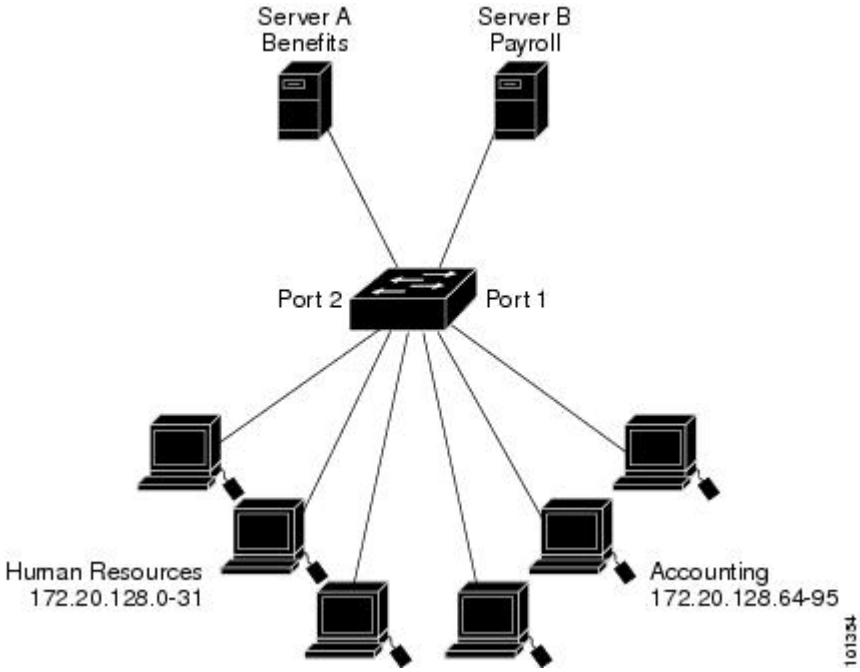
IPv4 ACL の設定例

ここでは、IPv4 ACL を設定および適用する例を示します。ACL のコンパイルに関する詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』および『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Adderssing and Services」の章にある「Configuring IP Services」の項を参照してください。

小規模ネットワークが構築されたオフィス用の ACL

図 *111* : ルータ *ACL* によるトラフィックの制御

次に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッドポート2に接続されたサーバAには、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。サーバAにはすべてのユーザがアクセスできますが、サーバBにアクセスできるユーザは制限されています。



ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバに着信するトラフィックをフィルタリングします。
- 拡張 ACL を作成し、サーバからポート 1 に着信するトラフィックをフィルタリングします。

例：小規模ネットワークが構築されたオフィスの ACL

次に、標準ACLを使用してポートからサーバBに着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ～ 172.20.128.95 から送信されるトラフィックだけを許

可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッド ポート 1 から送信されるトラフィックに適用されます。

```
Device(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Device(config)# end
Device# how access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 6 out
```

次に、拡張ACLを使用してサーバBからポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバ B）から経理部の宛先アドレス 172.20.128.64 ～ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。このACLは、ルーテッドポート1に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前に、プロトコル（IP）を入力する必要があります。

```
Device(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Device(config)# end
Device# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 106 in
```

例：番号付き ACL

次の例のネットワーク 36.0.0.0 は、2 番めのオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネット マスクは255.255.0.0 です。ネットワーク アドレス 36.0.0.0 の 3 番めおよび 4 番めのオクテットは、特定のホストを指定します。アクセス リスト 2 を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセス リストの最終行は、ネットワーク 36.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。この ACL は、ポートに着信するパケットに適用されます。

```
Device(config)# access-list 2 permit 36.48.0.3
Device(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Device(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# ip access-group 2 in
```

例：拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番めの行は、ホスト 128.88.1.2 の SMTP ポートへの着信 TCP 接続を許可します。3 番めの行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
```

```
Device(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Device(config)# access-list 102 permit icmp any any
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。ただし、IP ホストからは、専用メール ホストのメール（SMTP）ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。発信パケットのポート番号は予約されています。安全なネットワーク システムでは常にポート 25 でのメール接続が使用されているため、着信サービスと発信サービスを個別に制御できます。ACL は発信インターフェイスの入力 ACL および着信インターフェイスの出力 ACL として設定される必要があります。

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 102 in
```

次の例では、ネットワークはアドレスが 128.88.0.0 のクラス B ネットワークで、メール ホストのアドレスは 128.88.1.2 です。**established** キーワードは、確立された接続を表示する TCP 専用のキーワードです。TCP データグラムに ACK または RST ビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。スタック メンバー 1 のギガビット イーサネット インターフェイス 1 は、ルータをインターネットに接続するインターフェイスです。

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Device(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 102 in
```

例：名前付き ACL

名前付き標準 ACL および名前付き拡張 ACL の作成

次に、*Internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。*Internet_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
Device(config)# ip access-list standard Internet_filter
Device(config-ext-nacl)# permit 1.2.3.4
Device(config-ext-nacl)# exit
```

marketing_group ACL は、宛先アドレスとワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。ICMP トラフィッ

クを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ～ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
Device(config)# ip access-list extended marketing_group
Device(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Device(config-ext-nacl)# deny tcp any any
Device(config-ext-nacl)# permit icmp any any
Device(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Device(config-ext-nacl)# deny ip any any log
Device(config-ext-nacl)# exit
```

Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
Device(config)# interface gigabitethernet3/0/2
Device(config-if)# no switchport
Device(config-if)# ip address 2.0.5.1 255.255.255.0
Device(config-if)# ip access-group Internet_filter out
Device(config-if)# ip access-group marketing_group in
```

名前付き ACL からの個別 ACE の削除

次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```
Device(config)# ip access-list extended border-list
Device(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

例：IP ACL に適用される時間範囲

次に、月曜日から金曜日の午前 8 時 ～午後 6 時（18 時）の間、IP の HTTP トラフィックを拒否する例を示します。UDP トラフィックは、土曜日および日曜日の正午～午後 8 時（20 時）の間だけ許可されます。

```
Device(config)# time-range no-http
Device(config)# periodic weekdays 8:00 to 18:00
!
Device(config)# time-range udp-yes
Device(config)# periodic weekend 12:00 to 20:00
!
Device(config)# ip access-list extended strict
Device(config-ext-nacl)# deny tcp any any eq www time-range no-http
Device(config-ext-nacl)# permit udp any any time-range udp-yes
!
Device(config-ext-nacl)# exit
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# ip access-group strict in
```

例：コメント付き IP ACL エントリの設定

次に示す番号付き ACL の例では、Jones が所有するワークステーションにはアクセスを許可し、Smith が所有するワークステーションにはアクセスを許可しません。

```
Device(config)# access-list 1 remark Permit only Jones workstation through
Device(config)# access-list 1 permit 171.69.2.88
Device(config)# access-list 1 remark Do not allow Smith workstation through
Device(config)# access-list 1 deny 171.69.3.13
```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しません。

```
Device(config)# access-list 100 remark Do not allow Winter to browse the web
Device(config)# access-list 100 deny host 171.69.3.85 any eq www
Device(config)# access-list 100 remark Do not allow Smith to browse the web
Device(config)# access-list 100 deny host 171.69.3.13 any eq www
```

次に示す名前付き ACL の例では、Jones のサブネットにアクセスを許可しません。

```
Device(config)# ip access-list standard prevention
Device(config-std-nacl)# remark Do not allow Jones subnet through
Device(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次に示す名前付き ACL の例では、Jones のサブネットに発信 Telnet の使用を許可しません。

```
Device(config)# ip access-list extended telnetting
Device(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Device(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

例：ACL ロギング

ルータ ACL では、2 種類のロギングがサポートされています。**log** キーワードを指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。**log-input** キーワードを指定すると、ログ エントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセス リスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。**log** キーワードも指定されています。

```
Device(config)# ip access-list standard stan1
Device(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Device(config-std-nacl)# permit any log
Device(config-std-nacl)# exit
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group stan1 in
Device(config-if)# end
Device# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 37 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 37 messages logged
```

```
    File logging: disabled
    Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems

<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次に、名前付き拡張アクセス リスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```
Device(config)# ip access-list extended ext1
Device(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Device(config-ext-nacl)# deny udp any any log
Device(config-std-nacl)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip access-group ext1 in
```

次に、拡張 ACL のログの例を示します。

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
01:26:12:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1
packet
01:31:33:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8
packets
```

IP ACL のすべてのロギング エントリは %SEC-6-IPACCESSLOG で開始します。エントリの形式は、一致した ACL やアクセス エントリの種類に応じて若干異なります。

次に、**log-input** キーワードを指定した場合の出力メッセージの例を示します。

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400)
 ->
10.1.1.61 (0/0), 1 packet
```

log キーワードを指定した場合、同様のパケットに関するログ メッセージには入力インターフェイス情報が含まれません。

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0),
 1 packet
```

ACL および VLAN マップの設定例

例：パケットを拒否する ACL および VLAN マップの作成

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、*ip1* ACL（TCP パケット）に一致するすべてのパケットがドロップされます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する *ip1* ACL を作成します。VLAN マップには IP パケットに対する match 句が存在するため、デフォルトのアクションでは、どの match 句とも一致しない IP パケットがすべてドロップされます。

```
Device(config)# ip access-list extended ip1
Device(config-ext-nacl)# permit tcp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map_1 10
Device(config-access-map)# match ip address ip1
Device(config-access-map)# action drop
```

例：パケットを許可する ACL および VLAN マップの作成

次に、パケットを許可する VLAN マップを作成する例を示します。ACL *ip2* は UDP パケットを許可し、*ip2* ACL と一致するすべてのパケットが転送されます。このマップでは、これ以前のどの ACL とも一致しないすべての IP パケット（TCP でも UDP でもないパケット）がドロップされます。

```
Device(config)# ip access-list extended ip2
Device(config-ext-nacl)# permit udp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map_1 20
Device(config-access-map)# match ip address ip2
Device(config-access-map)# action forward
```

例：IP パケットのドロップおよび MAC パケットの転送のデフォルト アクション

次の例の VLAN マップでは、デフォルトで IP パケットがドロップされ、MAC パケットが転送されます。標準の ACL 101 および名前付き拡張アクセス リスト **igmp-match** および **tcp-match** をこのマップと組み合わせて使用すると、次のようになります。

- すべての UDP パケットが転送されます。
- すべての IGMP パケットがドロップされます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- すべての非 IP パケットが転送されます。

```
Device(config)# access-list 101 permit udp any any
Device(config)# ip access-list extended igmp-match
Device(config-ext-nacl)# permit igmp any any

Device(config)# action forward
```

```
Device(config-ext-nacl)# permit tcp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map drop-ip-default 10
Device(config-access-map)# match ip address 101
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan access-map drop-ip-default 20
Device(config-access-map)# match ip address igmp-match
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# vlan access-map drop-ip-default 30
Device(config-access-map)# match ip address tcp-match
Device(config-access-map)# action forward
```

例：MAC パケットのドロップおよび IP パケットの転送のデフォルト アクション

次の例の VLAN マップでは、デフォルトで MAC パケットがドロップされ、IP パケットが転送されます。MAC 拡張アクセス リスト **good-hosts** および **good-protocols** をこのマップと組み合わせて使用すると、次のようになります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- decnet-iv または vines-ip プロトコルを使用する MAC パケットが転送されます。
- その他のすべての非 IP パケットがドロップされます。
- すべての IP パケットが転送されます。

```
Device(config)# mac access-list extended good-hosts
Device(config-ext-macl)# permit host 000.0c00.0111 any
Device(config-ext-macl)# permit host 000.0c00.0211 any
Device(config-ext-nacl)# exit
Device(config)# action forward
Device(config-ext-macl)# mac access-list extended good-protocols
Device(config-ext-macl)# permit any any vines-ip
Device(config-ext-nacl)# exit
Device(config)# vlan access-map drop-mac-default 10
Device(config-access-map)# match mac address good-hosts
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan access-map drop-mac-default 20
Device(config-access-map)# match mac address good-protocols
Device(config-access-map)# action forward
```

例：すべてのパケットをドロップするデフォルト アクション

次の例の VLAN マップでは、デフォルトですべてのパケット（IP および非 IP）がドロップされます。例 2 および例 3 のアクセス リスト **tcp-match** および **good-hosts** をこのマップと組み合わせて使用すると、次のようになります。

- すべての TCP パケットが転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- その他のすべての MAC パケットがドロップされます。

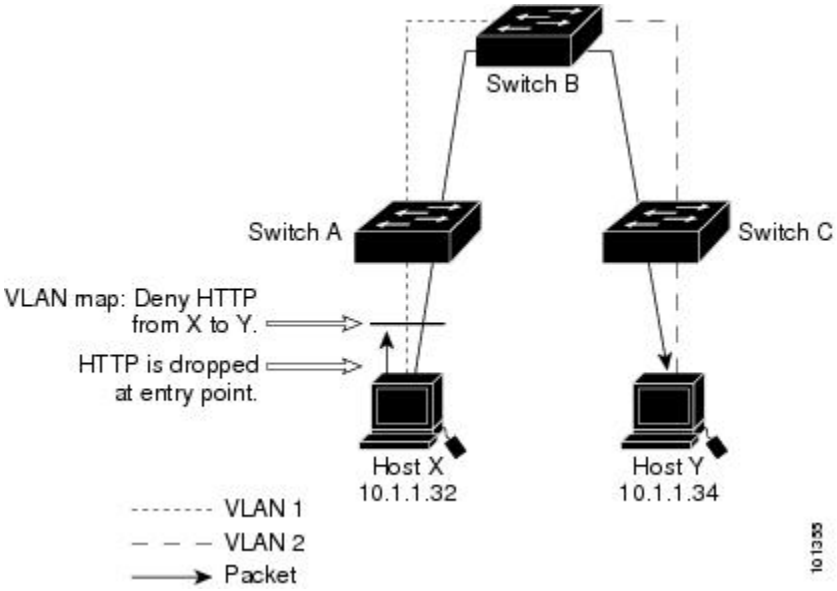
```
Device(config)# vlan access-map drop-all-default 10
Device(config-access-map)# match ip address tcp-match
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan access-map drop-all-default 20
Device(config-access-map)# match mac address good-hosts
Device(config-access-map)# action forward
```

ネットワークでの VLAN マップの使用方法の設定例

例：ワイヤリング クローゼットの設定

図 *112*：ワイヤリング クローゼットの設定

ワイヤリング クローゼット構成では、ルーティングがスイッチ上でイネーブルにされていない場合があります。ただし、この設定でも VLAN マップおよび QoS 分類 ACL はサポートされています。ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリング クローゼット スイッチ A およびスイッチ C に接続されていると想定します。ホスト X からホスト Y へのトラフィックは、ルーティングが有効に設定されたレイヤ 3 スイッチであるスイッチ B によって最終的にルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックのエントリ ポイントであるスイッチ A でアクセス コントロールできます。



HTTP トラフィックをホスト X からホスト Y へスイッチングしない場合は、ホスト X（IP アドレス 10.1.1.32）からホスト Y（IP アドレス 10.1.1.34）に向かうすべての HTTP トラフィックがスイッチ A でドロップされ、スイッチ B にブリッジングされないように、スイッチ A の VLAN マップを設定できます。

最初に、HTTP ポート上ですべての TCP トラフィックを許可（一致）する IP アクセス リスト *http* を定義します。

```
Device(config)# ip access-list extended http
```

```
Device(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Device(config-ext-nacl)# exit
```

次に、*http* アクセス リストと一致するトラフィックがドロップされ、その他のすべての IP トラフィックが転送されるように、VLAN アクセス マップ *map2* を作成します。

```
Device(config)# vlan access-map map2 10
Device(config-access-map)# match ip address http
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# ip access-list extended match_all
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map2 20
Device(config-access-map)# match ip address match_all
Device(config-access-map)# action forward
```

次に、VLAN アクセス マップ *map2* を VLAN 1 に適用します。

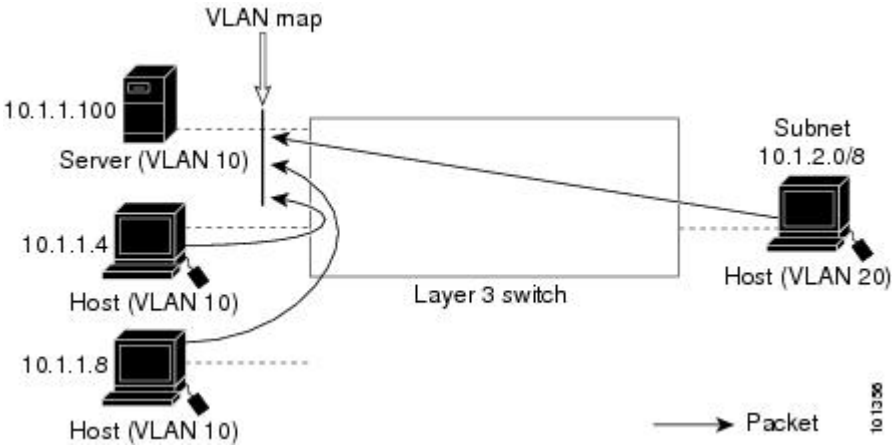
```
Device(config)# vlan filter map2 vlan 1
```

例：別の VLAN にあるサーバへのアクセスの制限

図 *113*：別の *VLAN* 上のサーバへのアクセスの制限

別の VLAN にあるサーバへのアクセスを制限できます。たとえば、VLAN 10 内のサーバ 10.1.1.100 では、次のホストへのアクセスを拒否する必要があります。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスを禁止します。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスを禁止します。



例：別の VLAN にあるサーバへのアクセスの拒否

次に、サブネット 10.1.2.0.8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 のアクセスを拒否し、その他の IP トラフィックを許可する VLAN マップ SERVER1-ACL を作成して、別の

VLAN内のサーバへのアクセスを拒否する例を示します。最後のステップでは、マップSERVER1を VLAN 10 に適用します。

正しいパケットと一致する IP ACL を定義します。

```
Device(config)# ip access-list extended SERVER1_ACL
Device(config-ext-nacl))# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Device(config-ext-nacl))# permit ip host 10.1.1.4 host 10.1.1.100
Device(config-ext-nacl))# permit ip host 10.1.1.8 host 10.1.1.100
Device(config-ext-nacl))# exit
```

SERVER1_ACL と一致する IP パケットをドロップして、この ACL と一致しない IP パケットを転送する ACL を使用して、VLAN マップを定義します。

```
Device(config)# vlan access-map SERVER1_MAP
Device(config-access-map)# match ip address SERVER1_ACL
Device(config-access-map)# action drop
Device(config)# vlan access-map SERVER1_MAP 20
Device(config-access-map)# action forward
Device(config-access-map)# exit
```

VLAN 10 に VLAN マップを適用します。

```
Device(config)# vlan filter SERVER1_MAP vlan-list 10
```

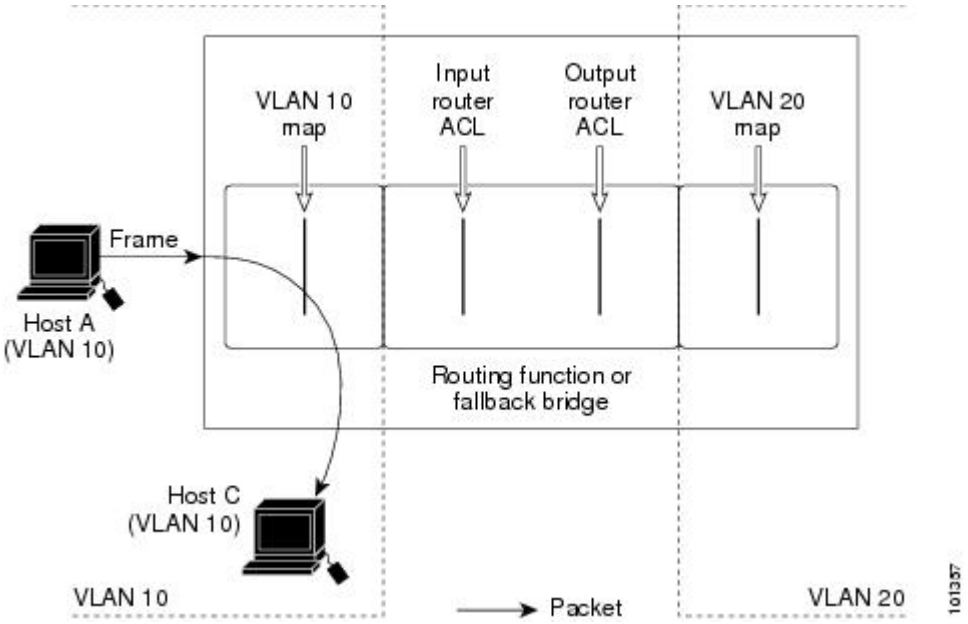
VLAN に適用されるルータ ACL と VLAN マップの設定例

ここでは、ルータ ACL および VLAN マップを VLAN に適用し、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットを処理する例を示します。次の図ではそれぞれの宛先に転送されるパケットを示します。パケットのパスが VLAN マップや ACL を示す線と交差するポイントで、パケットを転送せずにドロップする可能性もあります。

例：ACL およびスイッチド パケット

図 *114*：スイッチド パケットへの *ACL* の適用

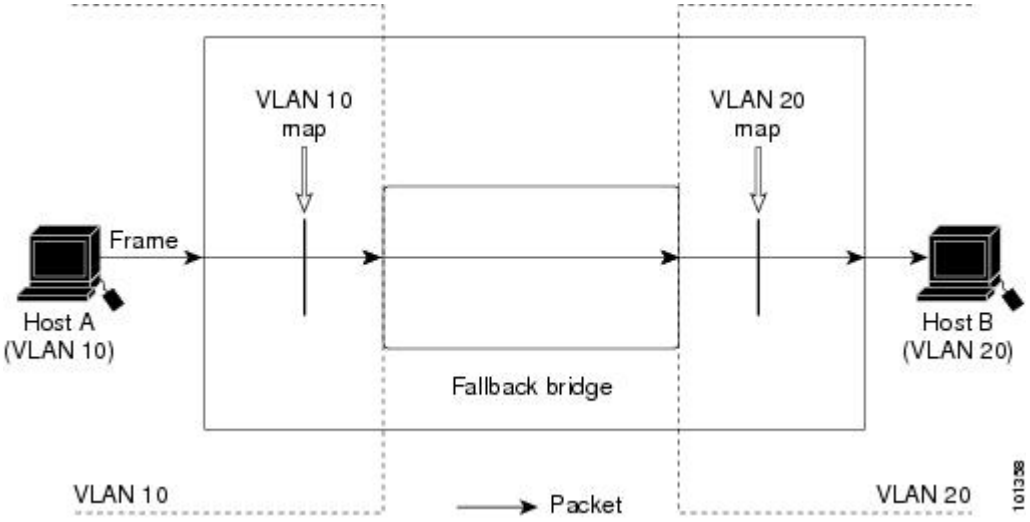
次の例に、VLAN内でスイッチングされるパケットにACLを適用する方法を示します。フォールバック ブリッジングによってルーティングまたは転送されず、VLAN 内でスイッチングされるパケットには、入力 VLAN の VLAN マップだけが適用されます。



例：ACL およびブリッジド パケット

図 *115*：ブリッジド パケットへの *ACL* の適用

次の例に、フォールバック ブリッジド パケットに ACL を適用する方法を示します。ブリッジド パケットの場合は、入力 VLAN にレイヤ 2 ACL だけが適用されます。また、非 IP および非 ARP パケットだけがフォールバック ブリッジド パケットとなります。

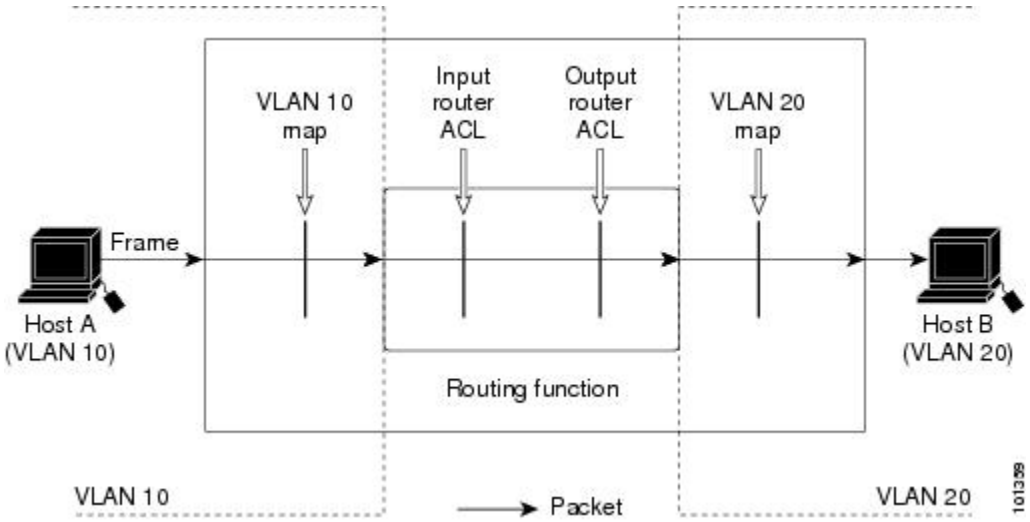


例：ACL およびルーテッド パケット

図 *116*：ルーテッド パケットへの *ACL* の適用

次の例に、ルーテッド パケットに ACL を適用する方法を示します。ACL は次の順番で適用されます。

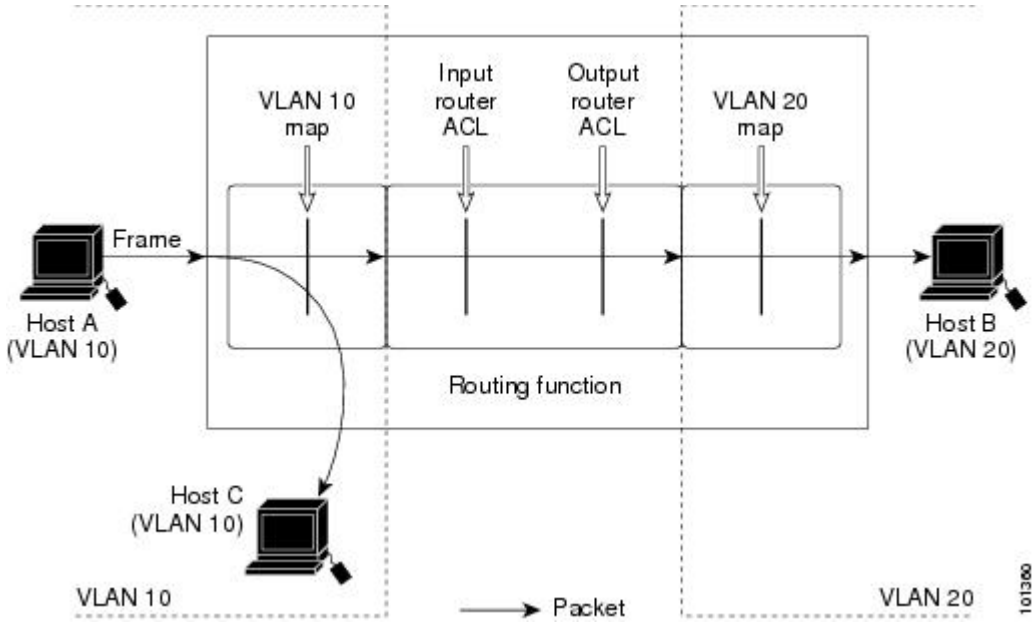
1. 入力 VLAN の VLAN マップ
2. 入力ルータ ACL
3. 出力ルータ ACL
4. 出力 VLAN の VLAN マップ



例：ACL およびマルチキャスト パケット

図 *117*：マルチキャスト パケットへの *ACL* の適用

次の例に、IPマルチキャスト用に複製されたパケットにACLを適用する方法を示します。ルーティングされるマルチキャストパケットには、2つの異なるフィルタが適用されます。1つは、宛先が入力VLAN内の他のポートである場合に使用され、もう1つは、宛先がパケットのルーティング先である別の VLAN 内にある場合に使用されます。パケットは複数の出力 VLAN にルーティングされる場合がありますが、この場合は宛先 VLAN ごとに異なるルータ出力 ACL およびVLANマップが適用されます。最終的に、パケットは一部の出力VLAN内で許可され、それ以外の VLAN で拒否されます。パケットのコピーが、許可された宛先に転送されます。ただし、入力 VLAN マップによってパケットがドロップされる場合、パケットのコピーは宛先に送信されません。



その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv4 アクセスコントロールリストのトピック	『Securing the Data Plane Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switch http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secdata-xe-3se-3850-libra

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 105 章

IPv6 ACL の設定

- 機能情報の確認 （2243 ページ）
- IPv6 ACL の概要 （2243 ページ）
- IPv6 ACL の制限 （2246 ページ）
- IPv6 ACL のデフォルト設定 （2247 ページ）
- IPv6 ACL の設定 （2247 ページ）
- インターフェイスへの IPv6 ACL の付加 （2252 ページ）
- VLAN マップの設定 （2254 ページ）
- VLAN への VLAN マップの適用 （2256 ページ）
- IPv6 ACL のモニタリング （2257 ページ）
- その他の参考資料 （2258 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IPv6 ACL の概要

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。また、スイッチで IP ベースおよび LAN ベース フィーチャ セットが稼働している場合、入力ルータ ACL を作成し、それを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

スイッチは、次の 3 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンド トラフィックまたはインバウンド トラフィックでサポートされます。IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。
- IPv6 ポート ACL は、インバウンドのレイヤ 2 インターフェイスでサポートされます。IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。
- VLAN ACL または VLAN マップは、VLAN 内のすべてのパケットのアクセスを制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。ACL VLAN マップは、L2 VLAN に適用されます。VLAN マップは、IPv6 のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されています。イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプロトコルがアクセス コントロールされます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケットが VLAN マップと照合されます。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

スイッチ スタックおよび IPv6 ACL

アクティブ スイッチは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバに配信します。

スタンバイ スイッチがアクティブ スイッチを引き継ぐと、ACL 設定がすべてのスタック メンバに配信されます。メンバ スイッチは、新しいスアクティブ スイッチによって配信された設定を同期し、不要なエントリを消去します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、アクティブ スイッチは変更内容をすべてのスタック メンバーに配信します。

ACL 優先順位

VLAN マップ、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、入力トラフィックの場合のフィルタの優先順位は上からポート ACL、VLAN マップ、およびルータ ACL です。出力トラフィックの場合、フィルタの優先順位は、ルータ ACL、VLAN マップ、ポート ACL です。

次の例で、簡単な使用例を説明します。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- スイッチ仮想インターフェイス（SVI）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、この

パケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。

- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。
- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

関連トピック

IPv4 アクセス コントロール リストの設定に関する制約事項 （2186 ページ）

VLAN マップ

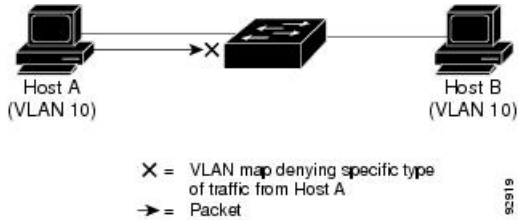
VLAN ACL または VLAN マップは、VLAN 内のネットワーク トラフィックを制御するために使用されます。スイッチまたはスイッチ スタックの VLAN 内でブリッジングされるすべてのパケットに VLAN マップを適用できます。VACL は、セキュリティ パケット フィルタリングおよび特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向（入力または出力）で定義されることはありません。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます（IP トラフィックは、MAC VACL マップではアクセス制御されません）。VLANマップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

VLANマップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

図 *118 : VLAN* マップによるトラフィックの制御

次に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用できます。



他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージ プロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。
- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリに空きがない場合、パケットはインターフェイスでドロップされ、アンロードのエラー メッセージが記録されます。

IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは再起 ACL（**reflect** キーワード）をサポートしません。

- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- レイヤ 2 EtherChannel に IPv6 ポート ACL を適用できません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポートまたはSVI）にACLを適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうか判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ（ACE）を追加しようとする場合、スイッチは現在インターフェイスに適用されている ACL に ACE が追加されるのを許可しません。

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム（IPv4 では **fragments** キーワード）がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。
- スイッチのハードウェア スペースがなくなった場合、ACL に関連付けられたパケットはインターフェイスでドロップされます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。
- スイッチは、プレフィックス長の最大範囲の IPv6 アドレス一致をサポートしません。

IPv6 ACL のデフォルト設定

デフォルトの IPv6 ACL 設定は次のとおりです。

```
Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**]{**ipv6 access-list** *list-name*| **client permit-control-packets**| **log-update threshold**| **role-based** *list-name*} 例： `Device(config)# ipv6 access-list example_acl_list`	IPv6 ACL 名を定義し、IPv6 アクセス リストコンフィギュレーションモードを開始します。
ステップ 4	[**no**]{**deny** | **permit**} protocol {*source-ipv6-prefix/|prefix-length*|**any threshold**| **host** *source-ipv6-address*} [operator [*port-number*]] { *destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]][**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、**udp**、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • *source-ipv6-prefix/prefix-length* または *destination-ipv6-prefix/ prefix-length* は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。

	コマンドまたはアクション	目的
		• **host** *source-ipv6-address* または *destination-ipv6-address* には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、**range**（包含範囲）があります。 *source-ipv6-prefix/prefix-length* 引数のあとの operator は、送信元ポートに一致する必要があります。*destination-ipv6- prefix/prefix-length* 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）**port-number** は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）**dscp** value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）**fragments** を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。

	コマンドまたはアクション	目的
		• （任意）**log** を指定すると、エントリと一致するパケットに関するログメッセージがコンソールに送信されます。**log-input** を指定すると、ログエントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 • （任意）**routing** を入力して、IPv6 パケットのルーティングを指定します。 • （任意）**sequence** *value* を入力して、アクセスリストステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4,294,967,295 です。 • （任意）**time-range** name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 5	{**deny** | **permit**} **tcp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [**operator** [**port-number**]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {**port** | protocol}] [**psh**] [**range** {**port** | protocol}] [**rst**] [**routing**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]	（任意）TCP アクセスリストおよびアクセス条件を定義します。 TCP の場合は **tcp** を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 • **ack**：確認応答（ACK）ビットセット • **established**：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • **fin**：終了ビットセット。送信元からのデータはそれ以上ありません。

	コマンドまたはアクション	目的
		• **neq** {*port* | protocol}：所定のポート番号上にないパケットだけを照合します。 • **psh**：プッシュ機能ビット セット • **range** {*port* | protocol}：ポート番号の範囲内のパケットだけを照合します。 • **rst**：リセット ビット セット • **syn**：同期ビット セット • **urg**：緊急ポインタ ビット セット
ステップ 6	{**deny** | **permit**} **udp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]] [**dscp** *value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**] [**sequence** *value*] [**time-range** *name*]]	（任意）UDP アクセス リストおよびアクセス条件を定義します。 ユーザデータグラムプロトコルの場合は、**udp** を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [*port*]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。
ステップ 7	{**deny** | **permit**} **icmp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]] [*icmp-type* [*icmp-code*] | icmp-message] [**dscp** *value*] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージプロトコルの場合は、**icmp** を入力します。ICMP パラメータはステップ 1 の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-code*：ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。

	コマンドまたはアクション	目的
		指定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、? キーを使用するか、またはこのリリースのコマンドリファレンスを参照してください。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ipv6 access-list**	アクセスリストの設定を確認します。
ステップ 10	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次のタスク

インターフェイスに IPv6 ACL をアタッチします。

インターフェイスへの IPv6 ACL の付加

レイヤ 3 インターフェイスで発信または着信トラフィックに、あるいはレイヤ 2 インターフェイスで着信トラフィックに ACL を適用できます。レイヤ 3 インターフェイスで着信トラフィックにだけ ACL を適用できます。

インターフェイスへのアクセスを制御するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	アクセス リストを適用するレイヤ 2 インターフェイス（ポート ACL 用）またはレイヤ 3 インターフェイス（ルータ ACL 用）を特定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no switchport**	ルータ ACL を適用する場合は、これによってインターフェイスがレイヤ2モード（デフォルト）からレイヤ3モードに変化します。
ステップ 5	**ipv6 address** *ipv6-address*	レイヤ3インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。
ステップ 6	**ipv6traffic-filter** *access-list-name* {**in** | **out**}	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例：	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

VLAN マップの設定

VLAN マップを作成して、1 つまたは複数の VLAN に適用するには、次のステップを実行します。

始める前に

VLAN に適用する IPv6 ACL を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan access-map** *name* [**number**] 例： `Device(config)# vlan access-map map_1 20`	VLANマップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。 同じ名前のVLANマップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。 VLAN マップでは、特定の permit または deny キーワードを使用しません。VLANマップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致する

	コマンドまたはアクション	目的
		という意味です。ACL 内の deny は、一致しないという意味です。 このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。
ステップ 4	**match** {**ip** | **ipv6** | **mac**} **address** {*name* | *number*} [*name* | *number*] 例： `Device(config-access-map)# match ipv6 address ip_net`	パケットを 1 つまたは複数のアクセス リストに対して照合します。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC アクセス リストに対してだけ照合されます。 （注） パケット タイプ（IP または MAC）に対する match 句が VLAN マップに設定されている場合で、そのマップ アクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。match 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。

ステップ 5	IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1 つ以上の ACL とそのパケットを照合するには、次のコマンドのいずれかを入力します。
	• **action** { **forward**}
	`Device(config-access-map)# action forward`
	• **action** { **drop**}
	`Device(config-access-map)# action drop`
		マップ エントリに対するアクションを設定します。

ステップ 6	**vlan filter** *mapname***vlan-list** *list* 例：	VLAN マップを 1 つまたは複数の VLAN に適用します。

	コマンドまたはアクション	目的
	`Device(config)# vlan filter map 1 vlan-list 20-22`	list には単一の VLAN ID（22）、連続した範囲（10 ～ 22）、または VLAN ID のストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。

VLAN への VLAN マップの適用

1 つの VLAN マップを 1 つまたは複数の VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan filter** *mapname***vlan-list** *list* 例： `Device(config)# vlan filter map 1 vlan-list 20-22`	VLAN マップを 1 つまたは複数の VLAN に適用します。 list には単一の VLAN ID（22）、連続した範囲（10 ～ 22）、または VLAN ID のストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例：	アクセス リストの設定を表示します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN マップの設定 （2220 ページ）

IPv6 ACL のモニタリング

次の表に示された 1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

コマンド	目的
show access-lists	スイッチに設定されたすべてのアクセス リストを表示します。
show ipv6 access-list [*access-list-name*]	設定済みのすべての IPv6 アクセス リストまたは名前で指定されたアクセス リストを表示します。
show vlan access-map[*map-name*]	VLAN アクセス マップ設定を表示します。
show vlan filter[**access-map***access-map*| **vlan***vlan-id*]	VACL と VLAN 間のマッピングを表示します。

次に、show access-lists 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Switch # show access-lists
Extended IP access list hello
    10 permit ip any any
IPv6 access list ipv6
    permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet (15 matches) sequence 20
    permit udp any any sequence 30
IPv6 access list outbound
    deny udp any any sequence 10
    deny tcp any any eq telnet sequence 20
```

次に、show vlan access-map 特権 EXEC コマンドの出力例を示します。出力には、VLAN アクセス マップ情報が表示されます。

```
Switch# show vlan access-map
Vlan access-map "m1"  10
  Match clauses:
    ipv6 address: ip2
  Action: drop
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 セキュリティ設定のトピック	『IPv6 Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』 http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/xe-3se/3850/ipv6-xe-3se-3850-library.html

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	『IPv6 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』 http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-xe-3se-3850-cr-book.html

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 106 章

DHCP の設定

- 機能情報の確認 （2261 ページ）
- DHCP に関する情報 （2261 ページ）
- DHCP 機能の設定方法 （2269 ページ）
- DHCP サーバ ポートベースのアドレス割り当ての設定 （2277 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

DHCP に関する情報

DHCP サーバ

DHCP サーバは、スイッチまたはルータ上の指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、それらのアドレスを管理します。DHCP サーバがそのデータベースから要求された設定パラメータを取得して DHCP クライアントに渡すことができない場合は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに要求を転送します。スイッチは、DHCP サーバとして機能できます。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送するレイヤ3デバイスです。リレーエージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは、DHCP メッセージを受け取ると、新しい DHCP メッセージを生成して、出力インターフェイス上で送信します。

DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと DHCP スヌーピング バインディング データベース（DHCP スヌーピング バインディング テーブルとも呼ばれる）の作成および管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。DHCP スヌーピングを使用することにより、エンドユーザに接続された信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。

（注） DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。

信頼できない DHCP メッセージとは、信頼できないインターフェイス経由で送信されたメッセージのことです。デフォルトでは、スイッチはすべてのインターフェイスを信頼できないものと見なします。そのため、スイッチはいくつかのインターフェイスを信頼して DHCP スヌーピングを使用するように設定する必要があります。サービス プロバイダー環境で DHCP スヌーピングを使用する場合は、カスタマーのスイッチなど、サービス プロバイダー ネットワーク内には存在しないデバイスから送信されたメッセージが信頼できないメッセージとなります。不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカルインターフェイスのインターフェイス情報が含まれています。このデータベースには、信頼できるインターフェイスに接続されたホストの情報はありません。

サービス プロバイダー ネットワークでは、信頼できるインターフェイスとして設定できるものの例として、同じネットワーク内のデバイスのポートに接続されたインターフェイスがあります。信頼できないインターフェイスには、ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスがあります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。アドレスが一致した場合（デフォルト）、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットをドロップします。

- DHCPOFFER パケット、DHCPACK パケット、DHCPNAK パケット、DHCPLEASEQUERY パケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスが一致しない。
- スイッチが DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バインディングデータベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP オプション 82 情報を挿入するエッジ スイッチに接続されているスイッチは、オプション 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットをドロップします。DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジ スイッチに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジ スイッチによって挿入されたオプション 82 情報を含むパケットを受け入れます。集約スイッチは、信頼できないスイッチインターフェイスを介して接続されたホストのバインディングを認識します。集約スイッチで、ダイナミック ARP インスペクションや IP ソース ガードなど、DHCP セキュリティ機能をイネーブルに設定することもできますが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない入力インターフェイスで受信します。集約スイッチ上のエッジスイッチとの接続ポートは、信頼できるインターフェイスとして設定する必要があります。

通常、ワイヤレス クライアントにパケットをブロードキャストするのは望ましくありません。したがって、DHCP スヌーピングは、宛先ブロードキャスト MAC アドレス（ffff.ffff.ffff）をサーバからワイヤレス クライアントに送信される DHCP パケットのユニキャスト MAC アドレスに置き換えます。ユニキャスト MAC アドレスは DHCP ペイロードの CHADDR フィールドから取得されます。この処理は、DHCP OFFER、DHCP ACK および DHCP NACK メッセージなどのクライアント パケットにサーバ用に適用されます。**ip dhcp snooping wireless bootp-broadcast enable** は、この動作を戻すために使用できます。ワイヤレス BOOTP ブロード

キャストがイネーブルの場合、サーバからのブロードキャスト DHCP パケットは、宛先 MAC アドレスを変更せずにワイヤレス クライアントに転送されます。

関連トピック

DHCP スヌーピングおよびオプション 82 を設定するための前提条件 （2274 ページ）

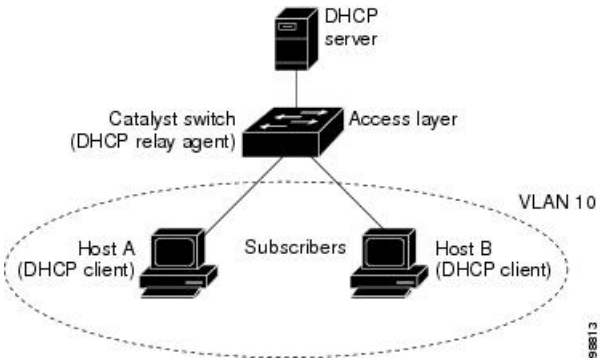
オプション 82 データ挿入

住宅地域にあるメトロポリタン イーサネット アクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチ ポートによっても識別されます。サブスクライバ LAN 上の複数のホストをアクセス スイッチの同じポートに接続できます。これらのホストは一意に識別されます。

（注） DHCP オプション 82 機能は、DHCP スヌーピングがグローバルに有効であり、オプション 82 を使用する加入者装置が割り当てられた VLAN で有効である場合に限りサポートされます。

次の図に、一元的な DHCP サーバがアクセス レイヤのスイッチに接続された加入者に IP アドレスを割り当てるメトロポリタン イーサネット ネットワークを示します。DHCP クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレー エージェント（Catalyst スイッチ）にヘルパー アドレスを設定することにより、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 *119*：メトロポリタン イーサネット ネットワークにおける *DHCP* リレー エージェント



スイッチで DHCP スヌーピング情報 オプション 82 を有効にすると、次のイベントがこの順序で発生します。

- ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。デフォルトでは、リモート ID サブオプションがスイッチの MAC アドレスで、回線 ID サブ

オプションはパケットを受信するポート ID（**vlan-mod-port**）です。リモート ID および回線 ID は設定できます。

- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するようなポリシーを実装したりできます。次に DHCP サーバは、DHCP 応答内にオプション 82 フィールドをエコーします。
- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、次のフィールドの値は変化しません（図「サブオプションのパケット形式」を参照）。

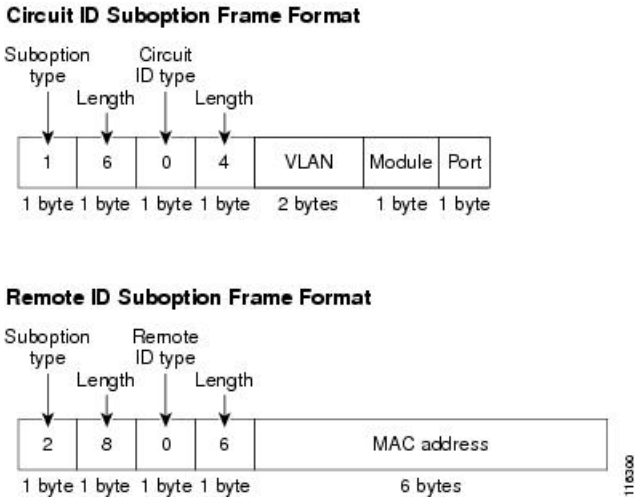
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号が 3 から始まります。たとえば、24 個の 10/100/1000 ポートおよび 4 つの Small Form-Factor Pluggable（SFP）モジュール スロットを搭載するスイッチでは、ポート 3 がギガビット イーサネット 1/0/1 ポート、ポート 4 がギガビット イーサネット 1/0/2 ポートとなり、以降同様に続きます。ポート 27 は SFP モジュール スロットのギガビット イーサネット 1/0/25 となり、以降同様に続きます。

図「サブオプションのパケット形式」に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。回線 ID サブオプションでは、モジュール番号は、スタックにあるスイッチ番号に対応します。

スイッチがこれらのパケット形式を使用するのは、DHCPスヌーピングをグローバルに有効にし、ip dhcp snooping information option グローバル コンフィギュレーション コマンドを入力した場合です。

図 *120*：サブオプションのパケット形式

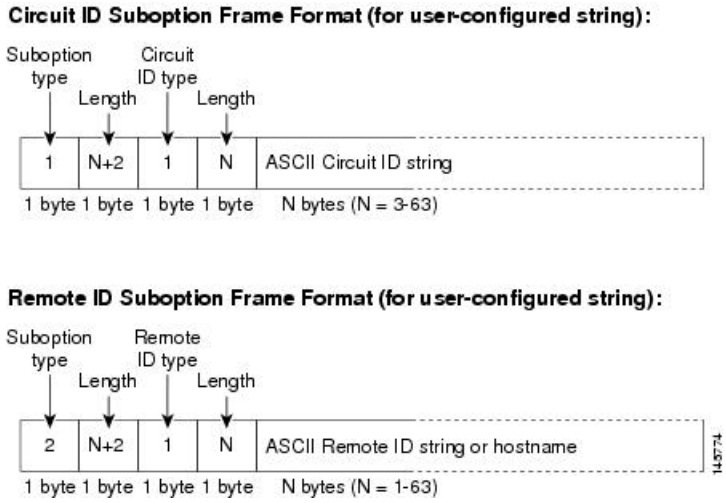


図「ユーザ設定のサブオプションのパケット形式」は、ユーザ設定のリモートIDサブオプション、および回線 ID サブオプションのパケット形式を示しています。スイッチでは、DHCP スヌーピングをグローバルに有効にし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力した場合に、これらのパケット形式が使用されます。

パケットでは、リモートIDおよび回線IDサブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

- 回線 ID サブオプション フィールド
  - 回線 ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
  - リモート ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。

図 *121 :* ユーザ設定のサブオプションのパケット形式



Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。これには IP アドレス、アドレス バインディング、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てること、または、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てることが可能です。手動および自動アドレス バインディングの詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章を参照してください。

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピング バインディング データベースに保存します。データベースには、64,000 のバインディングを含めることができます。

各データベース エントリ（バインディング）は、IP アドレス、それに関連付けられた MAC アドレス、リース期間（16 進形式）、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。データベース エージェントは、設定された場所のファイルにバインディングを保存します。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、まず 72 バイトのデータがあり、その後に 1 つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP インスペクションまたは IP ソース ガードがイネーブルにされ、DHCP スヌーピング バインディングデータベースがダイナミックバインディングされている場合、スイッチは接続を切断されます。このエージェントがディセーブルで、DHCPスヌーピングだけがイネーブルである場合、スイッチの接続は切断されませんが、DHCPスヌーピングはDHCPスプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディングデータベースを作成します。スイッチは、データベースに変更が加えられたときにはバインディング ファイルを更新します。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、ただちにデータベース内のエントリを更新します。スイッチはバインディング ファイル内のエントリも更新します。バインディング ファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイルが指定された時間内（書き込み遅延および中断タイムアウトの値によって設定される）に更新されない場合、更新は停止します。

バインディングが含まれるファイルの形式は次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の initial-checksum エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Gi1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 584a38f0
END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを DHCP スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スイッチがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している（スイッチはリース期間の終了時にバインディング エントリを削除しないことがある）。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- インターフェイスがルーテッド インターフェイスまたは DHCP スヌーピングにおける信頼できるインターフェイスである。

DHCP スヌーピングおよびスイッチ スタック

DHCP スヌーピングは、スタック マスターで管理されます。新しいスイッチがスタックに加入すると、スイッチでは、スタック マスターから DHCP スヌーピング設定を受信します。メンバがスタックから除外されると、スイッチに関連付けられているすべての DHCP スヌーピング アドレス バインディングがエージング アウトします。

すべてのスヌーピング統計情報は、スタック マスター上で生成されます。新しいスタック マスターが選出された場合、統計カウンタはリセットされます。

スタックのマージが発生し、スタック マスターではなくなった場合、スタック マスターにあったすべての DHCP スヌーピング バインディングが失われます。スタック パーティションでは、既存のスタック マスターに変更はなく、パーティション化スイッチに属しているバインディングは、エージング アウトします。パーティション化スイッチの新しいマスターでは、新たな着信 DHCP パケットの処理が開始されます。

DHCP 機能の設定方法

DHCP スヌーピングのデフォルト設定

表 *142 : DHCP* のデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要[13]
DHCP リレー エージェント	イネーブル[14]
DHCP パケット転送アドレス	未設定
リレー エージェント情報の確認	イネーブル（無効なメッセージは廃棄）。
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置換。

機能	デフォルト設定
DHCP スヌーピングをグローバルにイネーブル	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
パケットを信頼できない入力インターフェイスで受け取る DHCP スヌーピング オプション[15]	ディセーブル
DHCP スヌーピング レート制限	未設定
DHCP スヌーピング信頼状態	信頼できない
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピングの MAC アドレス検証	イネーブル
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブル、設定が必要。 （注） スイッチは、DHCP サーバとして設定されているデバイスからだけ、ネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブル、設定が必要。この機能は宛先が設定されている場合に限り有効。

[13] スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。
[14] スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。
[15] この機能は、スイッチがエッジスイッチによってオプション 82 情報が挿入されたパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

- スイッチ ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust interface** コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチ ポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。

- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報を表示したり、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報をクリアしたりできるようになりました。

DHCP サーバの設定

スイッチは、DHCP サーバとして機能できます。

スイッチを DHCP サーバとして設定するときの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の項の「Configuring DHCP」を参照してください。

DHCP サーバとスイッチ スタック

DHCP バインディング データベースは、スタック マスターで管理されます。新しいスタック マスターが割り当てられると、新しいマスターでは、TFTP サーバから保存されているバインディングデータベースがダウンロードされます。スイッチオーバーが発生した場合、アクティブな新しいスタック マスターは SSO 機能を使用して以前のアクティブ スタック マスターから同期されたデータベース ファイルを使用します。失われたバインディングに関連付けられていた IP アドレスは、解放されます。自動バックアップは、**ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*] グローバル コンフィギュレーション コマンドを使用して設定する必要があります。

DHCP リレー エージェントの設定

スイッチ上で DHCP リレー エージェントをイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service dhcp** 例：	スイッチ上で DHCP サーバおよび DHCP リレー エージェントをイネーブルにし

	コマンドまたはアクション	目的
	`Device(config)# service dhcp`	ます。デフォルトでは、この機能はイネーブルです。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

これらの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の項の「*Configuring DHCP*」の項を参照してください。

- リレー エージェント情報のチェック（検証）
- リレー エージェント転送ポリシーの設定

パケット転送アドレスの指定

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合、スイッチを **ip helper-address** *address* インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的なルールは、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。**ip helper-address** コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、どの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 1`	VLAN ID を入力してスイッチ仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 192.108.1.27 255.255.255.0`	インターフェイスに IP アドレスおよび IP サブネットを設定します。
ステップ 5	**ip helper-address** *address* 例： `Device(config-if)# ip helper-address 172.16.1.2`	DHCP パケット転送アドレスを指定します。 ヘルパー アドレスは特定の DHCP サーバ アドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 6	**end** 例： `Device(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	次のいずれかを使用します。 • **interface range** *port-range* • **interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス範囲コンフィギュレーションモードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport mode access** 例： `Device(config-if)# switchport mode access`	ポートの VLAN メンバーシップ モードを定義します。
ステップ 9	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 1`	ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。
ステップ 10	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

DHCP スヌーピングおよびオプション 82 を設定するための前提条件

DHCP スヌーピングおよびオプション 82 の前提条件は次のとおりです。

- DHCP スヌーピングは、スイッチ上でグローバルにイネーブルにする必要があります。

- スイッチ上でDHCPスヌーピングをグローバルにイネーブルにする前に、DHCPサーバやDHCPリレーエージェントとして機能するデバイスが設定され、イネーブルになっていることを確認してください。
- スイッチをDHCP要求に応答するようにする場合は、DHCPサーバとして設定する必要があります。
- スイッチでDHCPスヌーピング情報オプションを設定する前に、DHCPサーバとして機能するデバイスを設定してください。DHCPサーバが割り当てたり除外したりできるIPアドレスを指定するか、またはそれらのデバイスのDHCPオプションを設定する必要があります。
- DHCPスヌーピングを正しく機能させるためには、すべてのDHCPサーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。サービス プロバイダー ネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。
- DHCPスヌーピングでCisco IOS DHCPサーバ バインディング データベースを使用するには、Cisco IOS DHCPサーバ バインディング データベースを使用するようにスイッチを設定する必要があります。
- 信頼できない入力でパケットを受け入れるDHCPスヌーピング オプションを使用するには、スイッチがエッジ スイッチからオプション82情報を含むパケットを受信する集約スイッチである必要があります。
- 次の前提条件がDHCPスヌーピング バインディングデータベースの設定に適用されます。
  - DHCPスヌーピング用にスイッチを使用するには、DHCPスヌーピング バインディング データベースで宛先を設定する必要があります。
  - NVRAMとフラッシュ メモリは、いずれも記憶容量が限られているため、バインディング ファイルをTFTPサーバに保存することを推奨します。
  - ネットワーク ベースのURL（TFTPやFTPなど）については、スイッチがバインディングをそのURLのバインディング ファイルに初めて書き込む前に、設定されたURLに空のファイルを作成する必要があります。空のファイルをサーバ上に作成する必要があるかどうかについては、TFTPサーバのマニュアルを参照してください。TFTPサーバによっては、そのように設定できないことがあります。
  - データベースに正しいリース期間が記録されるように、ネットワーク タイム プロトコル（NTP）をイネーブルにし、設定することを推奨します。
  - NTPが設定されている場合、スイッチのシステム クロックがNTPと同期化されたときにだけ、スイッチがバインディングの変更内容をバインディングファイルに書き込みます。
- スイッチでDHCPリレー エージェントを設定する前に、DHCPサーバとして機能するデバイスを設定してください。DHCPサーバが割り当てたり除外したりできるIPアドレスを指定するか、デバイスのDHCPオプションを設定するか、またはDHCPデータベースエージェントをセットアップする必要があります。

- スイッチが DHCP パケットをリレーするようにする場合は、DHCP サーバの IP アドレスは DHCP クライアントのスイッチ仮想インターフェイス（SVI）に設定する必要があります。
- スイッチ ポートが DHCP サーバに接続されている場合は、ip dhcp snooping trust**ip dhcp snooping trust interface**インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチ ポートが DHCP クライアントに接続されている場合は、no ip dhcp snooping trust**no ip dhcp snooping trust**インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。

関連トピック

DHCP スヌーピング （2262 ページ）

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『Cisco IOS IP Configuration Guide, Release 12.4』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

DHCP スヌーピング情報のモニタリング

表 *143 : DHCP* 情報を表示するためのコマンド

show ip dhcp snooping	スイッチの DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングだけを表示します。このようなバインディングは、バインディング テーブルとも呼ばれます。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピングの統計情報を要約または詳細形式で表示します。
show ip source binding	動的および静的に設定されたバインディングを表示します。

（注） DHCP スヌーピングがイネーブルでインターフェイスがダウン ステートに変更された場合、静的に設定されたバインディングは削除されません。

DHCP サーバ ポートベースのアドレス割り当ての設定

DHCP サーバ ポートベースのアドレス割り当ての設定に関する情報

DHCP サーバ ポートベースのアドレス割り当ては、接続されたデバイス クライアントの ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポートで同じ IP アドレスを維持できるようにする機能です。

ネットワークに導入されたイーサネット スイッチは、直接接続されたデバイスに接続を提供します。工場の作業場など、一部の環境では、あるデバイスで不具合が発生した場合は、それと同時に、そのネットワークで代わりのデバイスが動作を開始しなければなりません。現在の DHCP 実装では、この代わりのデバイスに、DHCP が同じ IP アドレスを提供する保証はありません。コントロールやモニタリングなどを行うソフトウェアは、各デバイスに関連付けられた IP アドレスが一定であることを期待しています。デバイスを交換した場合、DHCP クライアントが変更された場合でも、アドレスの割り当ては一定のままでなければなりません。

DHCP サーバ ポートベースのアドレス割り当て機能が設定されている場合、この機能により、ある接続ポートで受信された DHCP メッセージでクライアント ID やクライアント ハードウェア アドレスが変更されたとしても、同じ接続ポートには常に同じ IP アドレスが提供されることが保証されます。DHCP プロトコルは、DHCP パケットのクライアント ID オプションにより、DHCP クライアントを識別します。クライアント ID オプションを含まないクライアントは、クライアント ハードウェア アドレスにより識別されます。この機能を設定すると、インターフェイスのポート名が、クライアント ID またはハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアント ID になります。

すべてのケースで、同じポートにイーサネット ケーブルを接続することにより、接続されたデバイスに、DHCP 経由で同じ IP アドレスが割り当てられます。

DHCP サーバ ポートベースのアドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけです。サードパーティ製のサーバではサポートされていません。

ポートベースのアドレス テーブルのデフォルト設定

デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。

ポートベースのアドレス割り当て設定時の注意事項

- デフォルトでは、DHCP サーバポートベースのアドレス割り当てはディセーブルにされています。
- DHCP プールから事前に設定された予約への割り当てを制限する（予約されていないアドレスはクライアントに提供されず、その他のクライアントはプールによるサービスを受けない）ために、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力することができます。

DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチ上で DHCP スヌーピング バインディング データベース エージェントをイネーブルにし、設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp snooping database** {**flash**[*number*]**:**/*filename* | **ftp:**//*user***:***password***@***host*/*filename* | **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** | **rcp:**//*user***@***host*/*filename*}| **tftp:**//*host*/*filename* 例： `Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2`	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイルの URL を指定します。 • **flash**[*number*]**:**/*filename* （任意）スタック マスターのスタック メンバ番号を指定するには、*number* パラメータを使用します。*number* の指定できる範囲は 1 ～ 9 です。 • **ftp:**//*user***:***password***@***host*/*filename*

	コマンドまたはアクション	目的
		• **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** • **rcp:**//*user*@*host*/*filename* • **tftp:**//*host*/*filename*
ステップ 4	**ip dhcp snooping database timeout** *seconds* 例： `Device(config)# ip dhcp snooping database timeout 300`	データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間（秒数）を指定します。 デフォルトは 300 秒です。指定できる範囲は 0 ～ 86400 です。無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。
ステップ 5	**ip dhcp snooping database write-delay** *seconds* 例： `Device(config)# ip dhcp snooping database write-delay 15`	バインディングデータベースが変更されてから転送を開始するまでの遅延時間を指定します。指定できる範囲は15 ～ 86400 秒です。デフォルトは 300 秒（5 分）です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id* **expiry** *seconds* 例： `Device# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000`	（任意）DHCP スヌーピング バインディングデータベースにバインディングエントリを追加します。*vlan-id* に指定できる範囲は 1 ～ 4904 です。*seconds* の範囲は 1 ～ 4294967295 です。 このコマンドは、追加するエントリごとに入力します。 このコマンドは、スイッチをテストまたはデバッグするときに使用します。
ステップ 8	**show ip dhcp snooping database** [**detail**] 例： `Device# show ip dhcp snooping database detail`	DHCP スヌーピング バインディングデータベースエージェントのステータスおよび統計情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルにイネーブル化し、インターフェイス上で加入者 ID を自動的に生成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp use subscriber-id client-id** 例： `Device(config)# ip dhcp use subscriber-id client-id`	すべての着信 DHCP メッセージで、加入者 ID がクライアント ID としてグローバルに使用されるように DHCP サーバを設定します。
ステップ 4	**ip dhcp subscriber-id interface-name** 例： `Device(config)# ip dhcp subscriber-id interface-name`	インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。 特定のインターフェイスで設定された加入者 ID は、このコマンドで優先されます。

	コマンドまたはアクション	目的
ステップ 5	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip dhcp server use subscriber-id client-id** 例： `Device(config-if)# ip dhcp server use subscriber-id client-id`	インターフェイス上ですべての着信 DHCP メッセージで、加入者 ID がクライアント ID として使用されるように DHCP サーバを設定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

スイッチ上での DHCP ポートベースのアドレス割り当てをイネーブルにした後で、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用して、IP アドレスの事前割り当てと、クライアントへの関連付けを行います。

DHCP サーバ ポートベースのアドレス割り当てのモニタリング

表 *144 : DHCP* ポートベースのアドレス割り当て情報を表示するためのコマンド

コマンド	目的
show interface *interface id*	特定のインターフェイスのステータスおよび設定を表示します。
show ip dhcp pool	DHCP アドレス プールを表示します。

コマンド	目的
show ip dhcp binding	Cisco IOS DHCP サーバのアドレス バインディングを表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
DHCP 設定情報および手順	『IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3S』 http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/dhcp-xe

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 107 章

IP ソース ガードの設定

IP ソース ガード（IPSG）は、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックを制限するセキュリティ機能で、DHCP スヌーピング バインディング データベースと手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングすることで実現されます。

この章は、次の内容で構成されています。

- 機能情報の確認 （2285 ページ）
- IP ソース ガードの概要 （2286 ページ）
- IP ソース ガードの設定方法 （2289 ページ）
- IP ソース ガードのモニタリング （2292 ページ）
- その他の参考資料 （2293 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IP ソース ガードの概要

IP ソース ガード

ネイバーの IP アドレスを使用する場合に、トラフィック攻撃を防ぐために IP ソース ガードを使用でき、そして信頼できないインターフェイスで DHCP スヌーピングがイネーブルの場合に、IP アドレスを使用しようとすると、IP ソース ガードをイネーブルにできます。

インターフェイス上で IPSG をイネーブルにすると、スイッチは、DHCP スヌーピングにより許可された DHCP パケットを除き、このインターフェイスで受信したすべての IP トラフィックをブロックします。

スイッチは IP アドレスをポートにバインドするためにハードウェアの発信元 IP 検索テーブルを使用します。IP および MAC のフィルタリングでは、送信元 IP 検索および送信元 MAC 検索が組み合わせが使用されます。送信元 IP アドレスを使用する IP トラフィックでは、バインディング テーブルが許可され、他のすべてのトラフィックは拒否されます。

IP ソース バインディング テーブルには、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング（スタティック IP 送信元バインディング）があります。このテーブルのエントリには IP アドレスと、関連 MAC アドレス、および関連 VLAN 番号があります。スイッチは、IP ソース ガードがイネーブルにされている場合だけ、IP ソース バインディング テーブルを使用します。

IPSG は、アクセス ポートおよびトランク ポートを含むレイヤ 2 ポートだけでサポートされます。送信元 IP アドレスと送信元 IP および MAC アドレス フィルタリングで IPSG を設定できます。

スタティック ホスト用 IP ソース ガード

（注） アップリンク ポート、またはトランク ポートで、スタティック ホスト用 IP ソース ガード（IPSG）を使用しないでください。

スタティック ホスト用 IPSG は、IPSG の機能を DHCP ではない、スタティックな環境に拡張するものです。これまでの IPSG は、DHCP スヌーピングにより作成されたエントリを使用して、スイッチに接続されたホストを検証していました。ホストから受信したトラフィックのうち、有効な DHCP を持たないものはすべてドロップされます。このセキュリティ機能によって、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックが制限されます。この機能は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソースバインディングに基づいてトラフィックをフィルタリングします。前バージョンの IPSG では、IPSG を動作させるために DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしで IPSG を動作させることができます。スタティック ホスト用 IPSG は、ポート ACL をインストールするために IP デバイス トラッキング

テーブルエントリに依存しています。このスイッチは、指定されたポートで有効なホストのリストを維持するために、ARP リクエスト、またはその他の IP パケットに基づいてスタティックエントリを作成します。また、指定されたポートにトラフィックを送信できるホストの数を指定することもできます。これはレイヤ 3 でのポート セキュリティと同じです。

スタティック ホスト用 IPSG はダイナミック ホストもサポートしています。ダイナミック ホストが、IP DHCP スヌーピング テーブルに存在する DHCP が割り当てられた IP アドレスを受信すると、IP デバイス トラッキング テーブルは同じエントリを学習します。スタック化環境では、マスターのフェールオーバーが発生すると、メンバ ポートに接続されたスタティック ホストの IP ソース ガード エントリは、そのまま残ります。**show ip device tracking all** 特権 EXEC コマンドを入力すると、IP デバイス トラッキング テーブルには、これらのエントリが ACTIVE であると表示されます。

（注） 複数のネットワーク インターフェイスを持つ IP ホストの一部は、ネットワーク インターフェイスに無効なパケットを注入することができます。この無効なパケットには、ソースアドレスとして、別のホスト ネットワーク インターフェイスの IP アドレス、または MAC アドレスが含まれます。この無効パケットは、スタティック ホスト用 IPSG がホストに接続され、無効な IP アドレス バインディングまたは MAC アドレス バインディングが学習されて、有効なバインディングが拒否される原因となります。ホストによる無効なパケットの注入を回避する方法については、対応するオペレーティング システムとネットワーク インターフェイスのベンダーにお問い合わせください。

最初、スタティック ホスト用 IPSG は ACL ベースのスヌーピング メカニズムを通じて、動的に IP バインディング、または MAC バインディングを学習します。IP バインディング、または MAC バインディングは、ARP パケット、および IP パケットにより、スタティック ホストから学習されます。これらはデバイス トラッキング データベースに保存されます。指定されたポートで動的に学習、または静的に設定された IP アドレスの数が最大値に達した場合、新しい IP アドレスを持つパケットはすべて、ハードウェアによりドロップされます。何らかの理由で移動された、またはなくなったホストを解決するために、スタティック ホスト用 IPSG は IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングをエージング アウトします。この機能は、DHCP スヌーピングとともに使用できます。複数バインディングは、DHCP ホストとスタティック ホストの両方に接続されたポートに確立されます。たとえば、バインディングは、デバイス トラッキング データベースと DHCP スヌーピング バインディング データベースの両方に保存されます。

IP ソース ガードの設定時の注意事項

- スタティック IP バインディングは、非ルーテッド ポートだけで設定できます。ルーテッド インターフェイスで **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを入力すると、次のエラー メッセージが表示されます。

```
Static IP source binding can only be configured on switch port.
```

- 送信元 IP フィルタリング機能を持つ IP ソース ガードがインターフェイスでイネーブルにされている場合、このインターフェイスのアクセス VLAN で、DHCP スヌーピングをイネーブルにしておく必要があります。
- 複数の VLAN を持つトランク インターフェイス上で IP ソース ガードをイネーブルにし、これらすべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。

（注） IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切にトラフィックをフィルタリングできない可能性があります。

- この機能は、802.1x ポートベースの認証がイネーブルにされている場合にイネーブルにできます。
- IP ソース ガード スマート ロギングを設定すると、指定されたアドレスや DHCP によって学習されたアドレス以外の送信元アドレスを持つパケットは拒否され、そのパケットの内容が NetFlow 収集装置に送信されます。この機能を設定する場合は、スマート ロギングがグローバルにイネーブルになっていることを確認してください。
- スイッチ スタックでは、IP ソース ガードがスタック メンバー インターフェイスに設定されていて、**noswitch** *stack-member-number***provision** グローバル コンフィギュレーション コマンドの入力によりそのスイッチの設定を削除した場合、インターフェイス スタティック バインディングはバインディング テーブルから削除されますが、実行コンフィギュレーションからは削除されません。**switch** *stack-member-number***provision** コマンドを入力することによって、スイッチを再度プロビジョニングした場合、バインディングは復元されます。

  実行コンフィギュレーションからバインディングを削除するには、**no switch provision** コマンドを入力する前に IP ソース ガードをディセーブルにする必要があります。インターフェイスがバインディング テーブルから削除される間にスイッチがリロードされると、設定も削除されます。

IP ソース ガードの設定方法

IP ソース ガードのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	**ip verify source**［**mac-check** ］ 例： `Device(config-if)# ip verify source`	送信元 IP アドレス フィルタリングによる IP ソース ガードを有効にします。 （任意）**mac-check**：送信元 IP アドレスによる IP ソース ガードおよび MAC アドレス フィルタリングをイネーブルにします。
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* 例： `Device(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4`	スタティック IP ソース バインディングを追加します。 スタティック バインディングごとにこのコマンドを入力します。

	コマンドまたはアクション	目的
	`interface gigabitethernet1/0/1`	
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定

スタティック ホスト用 IPSG を動作させるには、**ip device trackingmaximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルにイネーブルにしていない、または IP device tracking maximum をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**ip device tracking** 例： `Device(config)# ip device tracking`	IP ホスト テーブルをオンにし、IP デバイス トラッキングをグローバルに有効にします。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイスコンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access** 例： `Device(config-if)# switchport mode access`	アクセスとしてポートを設定します。
ステップ 6	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 10`	このポートに VLAN を設定します。
ステップ 7	**ip verify source**[**tracking**] [**mac-check**] 例： `Device(config-if)# ip verify source tracking mac-check`	送信元 IP アドレス フィルタリングによる IP ソース ガードを有効にします。 （任意）**tracking**：スタティック ホスト用 IP ソース ガードを有効にします。 （任意）**mac-check**：MAC アドレス フィルタリングを有効にします。 **ip verify source tracking mac-check** コマンドは、MAC アドレス フィルタリングのあるスタティック ホストに対して IP ソース ガードを有効にします。
ステップ 8	**ip device tracking maximum** *number* 例： `Device(config-if)# ip device tracking maximum 8`	そのポートで、IP デバイス トラッキングテーブルにより許可されるスタティック IP 数の上限を設定します。指定できる範囲は 1 ～ 10 です。最大値は 10 です。

	コマンドまたはアクション	目的
		（注） **ip device trackingmaximum** *limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

IP ソース ガードのモニタリング

表 *145 :* 特権 *EXEC* 表示コマンド

コマンド	目的
show ip verify source [**interface** *interface-id*]	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。
show ip device tracking { **all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *imac-address*}	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。

表 *146 :* インターフェイス コンフィギュレーション コマンド

コマンド	目的
ip verify source tracking	データ ソースを確認します。

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 108 章

ダイナミック ARP インスペクションの設定

- 機能情報の確認 （2296 ページ）
- ダイナミック ARP インスペクションの制約事項 （2296 ページ）
- ダイナミック ARP インスペクションの概要 （2297 ページ）
- ダイナミック ARP インスペクションのデフォルト設定 （2302 ページ）
- ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ （2302 ページ）
- 非 DHCP 環境での ARP ACL の設定 （2303 ページ）
- DHCP 環境でのダイナミック ARP インスペクションの設定 （2306 ページ）
- 着信 ARP パケットのレート制限 （2309 ページ）
- ダイナミック ARP インスペクション検証チェックの実行 （2311 ページ）
- DAI のモニタリング （2313 ページ）
- DAI の設定の確認 （2313 ページ）
- その他の参考資料 （2314 ページ）
- 機能情報の確認 （2315 ページ）
- ダイナミック ARP インスペクションの制約事項 （2315 ページ）
- ダイナミック ARP インスペクションの概要 （2317 ページ）
- ダイナミック ARP インスペクションのデフォルト設定 （2321 ページ）
- ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ （2322 ページ）
- 非 DHCP 環境での ARP ACL の設定 （2322 ページ）
- DHCP 環境でのダイナミック ARP インスペクションの設定 （2325 ページ）
- 着信 ARP パケットのレート制限 （2328 ページ）
- ダイナミック ARP インスペクション検証チェックの実行 （2330 ページ）
- DAI のモニタリング （2332 ページ）
- DAI の設定の確認 （2333 ページ）
- その他の参考資料 （2334 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ダイナミック ARP インスペクションの制約事項

ここでは、スイッチにダイナミック ARP インスペクションを設定するときの制約事項および注意事項を示します。

- ダイナミック ARP インスペクションは入力セキュリティ機能です。出力チェックはまったく行いません。
- ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションをサポートしていないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されるホストに対しては有効ではありません。中間者攻撃は単一のレイヤ2ブロードキャスト ドメインに制限されているため、チェックされないドメインと、ダイナミック ARP インスペクションによりチェックされるドメインは区別します。このアクションは、ダイナミック ARP インスペクションのためにイネーブルにされているドメインでホストの ARP キャッシュを保護します。
- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

  DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可または拒否を行います。
- ダイナミック ARP インスペクションは、アクセス ポート、トランク ポート、および EtherChannel ポートでサポートされます。

（注） RSPAN VLAN では、ダイナミック ARP インスペクションをイネーブルにしないでください。RSPAN VLAN でダイナミック ARP インスペクションをイネーブルにすると、ダイナミック ARP インスペクション パケットが RSPAN 宛先ポートに届かない可能性があります。

- 物理ポートを EtherChannel ポート チャネルに結合するには、この物理ポートとチャネル ポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポートチャネル内で中断状態のままとなります。ポート チャネルは、チャネルと結合された最初の物理ポートの信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態と一致する必要はありません。

  逆に、ポートチャネルで信頼状態を変更すると、スイッチは、チャネルを構成するすべての物理ポートで新しい信頼状態を設定します。

- レート制限は、スイッチ スタックの各スイッチで別々に算出されます。クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも高い可能性があることを意味します。たとえば、レート制限が 30 pps に設定された EtherChannel で、スイッチ 1 に 1 つのポート、およびスイッチ 2 に 1 つのポートがある場合、EtherChannel が errdisable にならずに、各ポートは 29 pps でパケットを受信できます。

- ポートチャネルの動作レートは、チャネル内のすべての物理ポートによる累積値です。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定すると、このチャネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャネル メンバーからの受信パケット レートの合計となります。EtherChannel ポートのレート制限は、各チャネル ポート メンバーが受信する ARP パケットのレートを確認してから設定してください。

  物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポートチャネルの設定に照合して検査されます。ポートチャネルのレート制限設定は、物理ポートの設定には依存しません。

  EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャネル（すべての物理ポートを含む）は errdisable ステートとなります。

- 着信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートの集約を反映し、複数のダイナミック ARP インスペクションがイネーブルにされた VLAN にわたってパケットを処理するために、トランク ポートのレートをより高く設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用して、レートを無制限に設定することもできます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。

- スイッチで、ダイナミック ARP インスペクションをイネーブルにすると、ARP トラフィックをポリシングするように設定されたポリサーの有効性は失われます。この結果、すべての ARP トラフィックは CPU に送信されます。

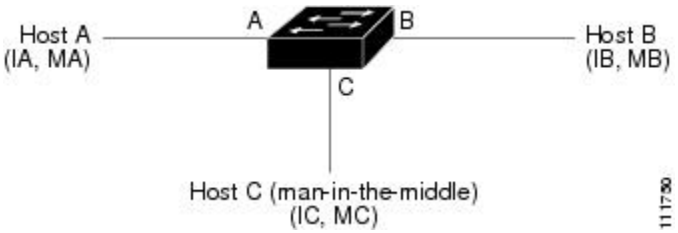
ダイナミック ARP インスペクションの概要

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B はホスト A に情報を送信する必要がありますが、ARP キャッシュにホスト A の MAC アドレスを持っていないとします。ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロー

ドキャスト ドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロードキャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。しかし、ARP は、ARP 要求が受信されなった場合でも、ホストからの余分な応答を許可するため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生することがあります。攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイヤ2ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。図 26-1 に、ARP キャッシュ ポイズニングの例を示します。

図 *122 : ARP* キャッシュ ポイズニング



ホスト A、B、および C は、インターフェイス A、B、および C 上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。カッコ内に示されているのは、これらの IP アドレス、および MAC アドレスです。たとえば、ホスト A が使用する IP アドレスは IA、MAC アドレスは MA です。ホスト A が IP レイヤにあるホスト B と通信する必要がある場合、ホスト A は IP アドレス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。スイッチとホスト B は、この ARP 要求を受信すると、IP アドレスが IA で、MAC アドレスが MA のホストに対する ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は、MAC アドレス MA にバインドされています。ホスト B が応答すると、スイッチ、およびホスト A は、IP アドレスが IB で、MAC アドレスが MB のホストに対するバインディングを ARP に読み込みます。

ホスト C は、IP アドレスが IA（または IB）で、MAC アドレスが MC のホストに対するバインディングを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングすることができます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は自身をホスト A からホスト B へのトラフィック ストリームに挿入します。従来の中間者攻撃です。

ダイナミック ARP インスペクションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。この機能により、ネットワークをある種の中間者攻撃から保護することができます。

ダイナミック ARP インスペクションにより、有効な ARP 要求と応答だけが確実にリレーされるようになります。スイッチが実行する機能は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

ダイナミック ARP インスペクションは、信頼できるデータベースである DHCP スヌーピング バインディング データベースに格納されている有効な IP/MAC アドレス バインディングに基づいて、ARP パケットの正当性を判断します。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピングにより構築されます。信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、このパケットを転送します。信頼できないインターフェイスでは、スイッチはこのパケットが有効である場合だけ、このパケットを転送します。

ip arp inspection vlan *vlan-range* グローバル コンフィギュレーション コマンドを使用して、VLAN ごとにダイナミック ARP インスペクションをイネーブルにすることができます。

非 DHCP 環境では、ダイナミック ARP インスペクションは、静的に設定された IP アドレスを持つホストに対するユーザ設定の ARP アクセス コントロール リスト（ACL）と照らし合わせて、ARP パケットの正当性を確認することができます。ARP ACL を定義するには、**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用します。

パケットの IP アドレスが無効である場合、または ARP パケットの本文にある MAC アドレスが、イーサネット ヘッダーで指定されたアドレスと一致しない場合、ARP パケットをドロップするようにダイナミック ARP インスペクションを設定することができます。このためには、**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} グローバル コンフィギュレーション コマンドを使用します。

インターフェイスの信頼状態とネットワーク セキュリティ

ダイナミック ARP インスペクションは、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイスに到着するパケットは、ダイナミック ARP インスペクションの確認検査をすべてバイパスし、信頼できないインターフェイスに到着するパケットには、ダイナミック ARP インスペクションの検証プロセスを受けます。

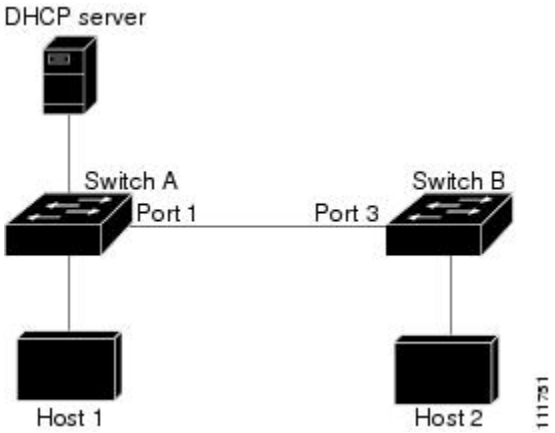
一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチ ポートすべてを信頼できるものに設定します。この構成では、指定されたスイッチからネットワークに入ってくる ARP パケットはすべて、セキュリティ チェックをバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、ip arp inspection trust インターフェイス コンフィギュレーション コマンドを使用します。

⚠

注意 信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

次の図では、スイッチ A とスイッチ B の両方が、ホスト 1 とホスト 2 を含む VLAN でダイナミック ARP インスペクションを実行しているとします。ホスト 1 とホスト 2 が、スイッチ A に接続している DHCP サーバから IP アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。したがって、スイッチ A とスイッチ B 間のインターフェイスが信頼できない場合は、ホスト 1 からの ARP パケットはスイッチ B ではドロップされ、ホスト 1 およびホスト 2 の間の接続は切断されます。

図 *123*：ダイナミック *ARP* インスペクションのために有効にされた *VLAN* 上の *ARP* パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティ ホールが生じます。スイッチ A でダイナミック ARP インスペクションが実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの間のリンクが信頼できるものとして設定されている場合はホスト 2）。この状況は、スイッチ B がダイナミック ARP インスペクションを実行している場合でも発生します。

ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションを実行しているスイッチに接続された（信頼できないインターフェイス上の）ホストが、そのネットワークにあるその他のホストの ARP キャッシュをポイズニングしていないことを保証します。しかし、ダイナミック ARP インスペクションにより、ネットワークの他の部分にあるホストが、ダイナミック ARP インスペクションを実行しているスイッチに接続されているホストのキャッシュをポイズニングできないようにすることはできません。

VLAN のスイッチの一部がダイナミック ARP インスペクションを実行し、残りのスイッチは実行していない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定します。ただし、非ダイナミック ARP インスペクションスイッチからパケットのバインディングを検証するには、ARP ACL を使用して、ダイナミック ARP インスペクションを実行するスイッチを設定します。このようなバインディングが判断できない場合は、レイヤ 3 で、ダイナミック ARP インスペクション スイッチを実行していないスイッチから、ダイナミック ARP インスペクションを実行しているスイッチを分離します。

（注） DHCP サーバとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。デフォルトでは、信頼できないインターフェイスのレートは 15 パケット/秒（pps）です。信頼できるインターフェイスはレート制限されません。この設定を変更するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。ユーザが介入するまで、ポートはこの状態を維持します。**errdisable recovery** グローバル コンフィギュレーション コマンドを使用すると、errdisable ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。

（注） EtherChannel のレート制限は、スタックにある各スイッチに個別に適用されます。たとえば、EtherChannel で 20 pps の制限が設定されている場合、EtherChannel にあるポートの各スイッチでは、最大 20 pps まで実行できます。スイッチが制限を超過した場合、EtherChannel 全体が errdisable ステートになります。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのは、ACL が **ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用して設定されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

廃棄パケットのロギング

スイッチがパケットをドロップすると、ログ バッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。各ログ エントリには、受信側の VLAN、ポート番号、送信元 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定します。記録されるパケットの種類を指定するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ARP インスペクションのデフォルト設定

機能	デフォルト設定
ダイナミック ARP インスペクション	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
着信 ARP パケットのレート制限	1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチドネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。 信頼できるすべてのインターフェイスでは、レート制限は行われません。 バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。
ログ バッファ	ダイナミック ARP インスペクションがイネーブル化されると、拒否またはドロップされた ARP パケットはすべてが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは 1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのは、ACL が ip arp inspection filter vlan グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

非 DHCP 環境での ARP ACL の設定

この手順は、図 2 に示すスイッチ B がダイナミック ARP インスペクション、または DHCP スヌーピングをサポートしていないときにダイナミック ARP インスペクションを設定する方法を示しています。

スイッチ A のポート 1 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、スイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが作り出されます。これを阻止するには、スイッチ A のポート 1 を信頼できないものとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない（スイッチ A で ACL 設定を適用することは不可能である）場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを使用してパケットをルートする必要があります。

スイッチ A で ARP ACL を設定するには、次の手順を実行します。この手順は、非 DHCP 環境では必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**arp access-list** *acl-name*	ARP ACL を定義し、ARP アクセス リスト コンフィギュレーション モードを開始します。デフォルトでは、ARP アクセス リストは定義されません。

	コマンドまたはアクション	目的
		（注） ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。
ステップ 4	**permit ip host** *sender-ip* **mac host** *sender-mac*	指定されたホスト（ホスト 2）からの ARP パケットを許可します。 • *sender-ip* には、ホスト 2 の IP アドレスを入力します。 • *sender-mac* には、ホスト 2 の MAC アドレスを入力します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]	VLAN に ARP ACL を適用します。デフォルトでは、定義済みの ARP ACL は、どのような VLAN にも適用されません。 • *arp-acl-name* には、ステップ 2 で作成した ACL の名前を指定します。 • *vlan-range* では、スイッチとホストが存在する VLAN を指定します。VLAN ID 番号により識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）**static** を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットは廃棄されます。DHCP バインディングは使用されません。 このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 句に一致しないパケットを許可する

	コマンドまたはアクション	目的
		か拒否するかは、DHCP バインディングによって決定されます。 IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセスリストで許可された場合だけに許可されます。
ステップ 7	**interface** *interface-id*	スイッチ B に接続されたスイッチ A のインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 8	**no ip arp inspection trust**	スイッチ B に接続されたスイッチ A のインターフェイスを untrusted として設定します。 デフォルトでは、すべてのインターフェイスは信頼できません。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカルキャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバルコンフィギュレーションコマンドで指定されたロギング設定に従ってログバッファに記録します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	次の show コマンドを使用します。 • **show arp access-list** acl-name • **show ip arp inspection vlan** *vlan-range* • **show ip arp inspection interfaces**	入力を確認します。
ステップ 11	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 12	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

DHCP 環境でのダイナミック ARP インスペクションの設定

始める前に

この手順では、2つのスイッチがダイナミック ARP インスペクションをサポートしているときに、この機能を設定する方法を示します。ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B にそれぞれ接続されています。スイッチは両方とも、ホストが配置されている VLAN 1 でダイナミック ARP インスペクションを実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。したがって、スイッチ A はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。

（注） 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

ダイナミック ARP インスペクションを設定するには、次の手順を実行します。この処理は、両方のスイッチで行う必要があります。この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**show cdp neighbors** 例： `Device(config-if)#show cdp neighbors`	スイッチ間の接続を確認します。
ステップ 3	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**ip arp inspection vlan** *vlan-range* 例： `Device(config)# ip arp inspection vlan 1`	VLAN 単位で、ダイナミック ARP インスペクションをイネーブルにします。デフォルトでは、すべての VLAN 上でダイナミック ARP インスペクションはディセーブルになっています。 vlan-range には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。両方のスイッチに同じ VLAN ID を指定します。
ステップ 5	**Interface***interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	他のスイッチに接続されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip arp inspection trust** 例： `Device(config-if)#ip arp inspection trust`	スイッチ間の接続を trusted に設定します。デフォルトでは、すべてのインターフェイスは信頼できません。 スイッチは、信頼できるインターフェイスにあるもう 1 つのスイッチから受信した ARP パケットは確認しません。この場合、パケットはそのまま転送されます。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先

	コマンドまたはアクション	目的
		にパケットを転送します。スイッチは、無効なパケットをドロップし、ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログバッファに記録します。
ステップ 7	**end** 例： `Device(config-if)#end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip arp inspection interfaces** 例：	インターフェイスでダイナミック ARP インスペクションの設定を検証します。
ステップ 9	**show ip arp inspection vlan** *vlan-range* 例： `Device(config-if)#show ip arp inspection vlan 1`	VLAN でダイナミック ARP インスペクションの設定を検証します。
ステップ 10	**show ip dhcp snooping binding** 例： `Device(config-if)#show ip dhcp snooping binding`	DHCP バインディングを確認します。
ステップ 11	**show ip arp inspection statistics vlan** *vlan-range* 例： `Device(config-if)#show ip arp inspection statistics vlan 1`	VLAN でダイナミック ARP インスペクションの統計情報を確認します。
ステップ 12	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

着信 ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。errordisable 回復をイネーブルにして、指定されたタイムアウト時間の後にポートがこのステートから自動的に抜け出すようにするまで、ポートはこのステートのままです。

（注） インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、レート制限をその信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

着信 ARP パケットのレートを制限するには、次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	レート制限されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip arp inspection limit {rate pps [burst interval seconds] | none}**	インターフェイス上の着信 ARP 要求および ARP 応答のレートを制限します。デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。バースト インターバルは 1 秒です。

	コマンドまたはアクション	目的
		キーワードの意味は次のとおりです。 • **rate***pps* には、1 秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ～ 2048 pps です。 • （任意）**burst interval***seconds* は、レートの高い ARP パケットの有無についてインターフェイスがモニタリングされる間隔（秒）を指定します。指定できる範囲は 1 ～ 15 です。 • **rate none** では、処理できる着信 ARP パケットのレートの上限を設定しません。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	次のコマンドを使用します。 • **errdisable detect cause arp-inspection** • **errdisable recovery cause arp-inspection** • **errdisable recovery interval** 間隔	（任意）ダイナミック ARP インスペクションの errdisable ステートからのエラー回復をイネーブルにし、ダイナミック ARP インスペクションの回復メカニズムで使用する変数を設定します。 デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。 **interval** *interval* では、errdisable ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。
ステップ 7	**exit**	特権 EXEC モードに戻ります。
ステップ 8	次の show コマンドを使用します。 • **show ip arp inspection interfaces** • **show errdisable recovery**	設定を確認します。
ステップ 9	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ダイナミック ARP インスペクション検証チェックの実行

ダイナミック ARP インスペクションは、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。宛先 MAC アドレス、送信側および宛先の IP アドレス、および送信元 MAC アドレスで追加検証を実行するように、スイッチを設定できます。

着信 ARP パケットで特定のチェックを実行するには、次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip arp inspection validate {[src-mac] [dst-mac] [ip]}**	着信 ARP パケットで特定の検査を実行します。デフォルトでは、検証は実行されません。 キーワードの意味は次のとおりです。 • **src-mac** では、イーサネット ヘッダーの送信元 MAC アドレスと ARP 本文の送信元 MAC アドレスが比較されます。この検査は、ARP 要求

	コマンドまたはアクション	目的
		および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **dst-mac** では、イーサネット ヘッダーの宛先 MAC アドレスと ARP 本文の宛先 MAC アドレスが比較されます。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **ip** では、ARP 本文から、無効な IP アドレスや予期しない IP アドレスがないかを確認します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。 少なくとも 1 つのキーワードを指定する必要があります。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが src および dst mac の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番めのコマンドによって src および dst mac の検証がディセーブルになります。
ステップ 4	**exit**	特権 EXEC モードに戻ります。
ステップ 5	**show ip arp inspection vlan** *vlan-range*	設定を確認します。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

DAI のモニタリング

DAI をモニタするには、次のコマンドを使用します。

コマンド	説明
clear ip arp inspection statistics	ダイナミック ARP インスペクション統計情報をクリアします。
show ip arp inspection statistics [**vlan** *vlan-range*]	指定の VLAN において、転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。
clear ip arp inspection log	ダイナミック ARP インスペクション ログ バッファをクリアします。
show ip arp inspection log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

show ip arp inspection statistics コマンドでは、スイッチは信頼されたダイナミック ARP インスペクション ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

DAI の設定の確認

DAI の設定を表示して確認するには、次のコマンドを使用します。

コマンド	説明
show arp access-list [*acl-name*]	ARP ACL についての詳細情報を表示します。
show ip arp inspection interfaces [interface-id]	指定されたインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。
show ip arp inspection vlan *vlan-range*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ダイナミック ARP インスペクションの制約事項

ここでは、スイッチにダイナミック ARP インスペクションを設定するときの制約事項および注意事項を示します。

- ダイナミック ARP インスペクションは入力セキュリティ機能です。出力チェックはまったく行いません。
- ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションをサポートしていないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されるホストに対しては有効ではありません。中間者攻撃は単一のレイヤ2ブロードキャスト ドメインに制限されているため、チェックされないドメインと、ダイナミック ARP インスペクションによりチェックされるドメインは区別します。このアクションは、ダイナミック ARP インスペクションのためにイネーブルにされているドメインでホストの ARP キャッシュを保護します。

- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

  DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可または拒否を行います。

- ダイナミック ARP インスペクションは、アクセス ポート、トランク ポート、および EtherChannel ポートでサポートされます。

  （注） RSPAN VLAN では、ダイナミック ARP インスペクションをイネーブルにしないでください。RSPAN VLAN でダイナミック ARP インスペクションをイネーブルにすると、ダイナミック ARP インスペクション パケットが RSPAN 宛先ポートに届かない可能性があります。

- 物理ポートを EtherChannel ポート チャネルに結合するには、この物理ポートとチャネル ポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポート チャネル内で中断状態のままとなります。ポート チャネルは、チャネルと結合された最初の物理ポートの信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態と一致する必要はありません。

  逆に、ポートチャネルで信頼状態を変更すると、スイッチは、チャネルを構成するすべての物理ポートで新しい信頼状態を設定します。

- レート制限は、スイッチ スタックの各スイッチで別々に算出されます。クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも高い可能性があることを意味します。たとえば、レート制限が 30 pps に設定された EtherChannel で、スイッチ 1 に 1 つのポート、およびスイッチ 2 に 1 つのポートがある場合、EtherChannel が errdisable にならずに、各ポートは 29 pps でパケットを受信できます。

- ポートチャネルの動作レートは、チャネル内のすべての物理ポートによる累積値です。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定すると、このチャネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャネル メンバーからの受信パケット レートの合計となります。EtherChannel ポートのレート制限は、各チャネル ポート メンバーが受信する ARP パケットのレートを確認してから設定してください。

  物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポートチャネルの設定に照合して検査されます。ポートチャネルのレート制限設定は、物理ポートの設定には依存しません。

  EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャネル（すべての物理ポートを含む）は errdisable ステートとなります。

- 着信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートの集約を反映し、複数のダイナミック ARP インスペクションがイネーブルにされた

VLAN にわたってパケットを処理するために、トランク ポートのレートをより高く設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用して、レートを無制限に設定することもできます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。

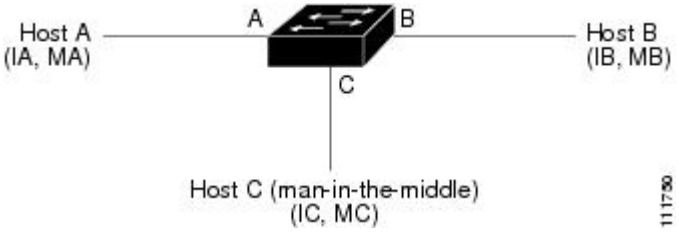
- スイッチで、ダイナミック ARP インスペクションをイネーブルにすると、ARP トラフィックをポリシングするように設定されたポリサーの有効性は失われます。この結果、すべての ARP トラフィックは CPU に送信されます。

ダイナミック ARP インスペクションの概要

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B はホスト A に情報を送信する必要がありますが、ARP キャッシュにホスト A の MAC アドレスを持っていないとします。ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャスト ドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロードキャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。しかし、ARP は、ARP 要求が受信されなった場合でも、ホストからの余分な応答を許可するため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生することがあります。攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイヤ 2 ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。図 26-1 に、ARP キャッシュ ポイズニングの例を示します。

図 *124 : ARP* キャッシュ ポイズニング



ホスト A、B、および C は、インターフェイス A、B、および C 上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。カッコ内に示されているのは、これらの IP アドレス、および MAC アドレスです。たとえば、ホスト A が使用する IP アドレスは IA、MAC アドレスは MA です。ホスト A が IP レイヤにあるホスト B と通信する必要がある場合、ホスト A は IP アドレス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。スイッチとホスト B は、この ARP 要求を受信すると、IP アドレスが IA で、MAC アドレスが MA のホストに対する ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は、MAC アドレス MA にバインドされています。ホスト

B が応答すると、スイッチ、およびホスト A は、IP アドレスが IB で、MAC アドレスが MB のホストに対するバインディングを ARP に読み込みます。

ホスト C は、IP アドレスが IA（または IB）で、MAC アドレスが MC のホストに対するバインディングを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングすることができます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は自身をホスト A からホスト B へのトラフィック ストリームに挿入します。従来の中間者攻撃です。

ダイナミック ARP インスペクションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。この機能により、ネットワークをある種の中間者攻撃から保護することができます。

ダイナミック ARP インスペクションにより、有効な ARP 要求と応答だけが確実にリレーされるようになります。スイッチが実行する機能は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

ダイナミック ARP インスペクションは、信頼できるデータベースである DHCP スヌーピング バインディング データベースに格納されている有効な IP/MAC アドレス バインディングに基づいて、ARP パケットの正当性を判断します。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピングにより構築されます。信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、このパケットを転送します。信頼できないインターフェイスでは、スイッチはこのパケットが有効である場合だけ、このパケットを転送します。

ip arp inspection vlan *vlan-range* グローバル コンフィギュレーション コマンドを使用して、VLAN ごとにダイナミック ARP インスペクションをイネーブルにすることができます。

非 DHCP 環境では、ダイナミック ARP インスペクションは、静的に設定された IP アドレスを持つホストに対するユーザ設定の ARP アクセス コントロール リスト（ACL）と照らし合わせて、ARP パケットの正当性を確認することができます。ARP ACL を定義するには、**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用します。

パケットの IP アドレスが無効である場合、または ARP パケットの本文にある MAC アドレスが、イーサネット ヘッダーで指定されたアドレスと一致しない場合、ARP パケットをドロップするようにダイナミック ARP インスペクションを設定することができます。このためには、**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} グローバル コンフィギュレーション コマンドを使用します。

インターフェイスの信頼状態とネットワーク セキュリティ

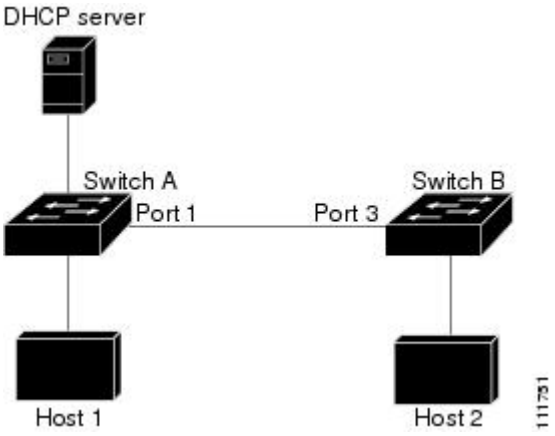
ダイナミック ARP インスペクションは、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイスに到着するパケットは、ダイナミック ARP インスペクションの確認検査をすべてバイパスし、信頼できないインターフェイスに到着するパケットには、ダイナミック ARP インスペクションの検証プロセスを受けます。

一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチポートすべてを信頼できるものに設定します。この構成では、指定されたスイッチからネットワークに入ってくるARPパケットはすべて、セキュリティ チェックをバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、ip arp inspection trust インターフェイス コンフィギュレーション コマンドを使用します。

注意 信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

次の図では、スイッチ A とスイッチ B の両方が、ホスト 1 とホスト 2 を含む VLAN でダイナミック ARP インスペクションを実行しているとします。ホスト 1 とホスト 2 が、スイッチ A に接続している DHCP サーバから IP アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。したがって、スイッチ A とスイッチ B 間のインターフェイスが信頼できない場合は、ホスト 1 からの ARP パケットはスイッチ B ではドロップされ、ホスト 1 およびホスト 2 の間の接続は切断されます。

図 *125*：ダイナミック *ARP* インスペクションのために有効にされた *VLAN* 上の *ARP* パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティ ホールが生じます。スイッチ A でダイナミック ARP インスペクションが実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの間のリンクが信頼できるものとして設定されている場合はホスト 2）。この状況は、スイッチ B がダイナミック ARP インスペクションを実行している場合でも発生します。

ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションを実行しているスイッチに接続された（信頼できないインターフェイス上の）ホストが、そのネットワークにあるその他のホストのARPキャッシュをポイズニングしていないことを保証します。しかし、ダイナミック ARP インスペクションにより、ネットワークの他の部分にあるホストが、ダイナミックARPインスペクションを実行しているスイッチに接続されているホストのキャッシュをポイズニングできないようにすることはできません。

VLAN のスイッチの一部がダイナミック ARP インスペクションを実行し、残りのスイッチは実行していない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定します。ただし、非ダイナミック ARP インスペクションスイッチからパケットのバインディングを検証するには、ARP ACL を使用して、ダイナミック ARP インスペクションを実行するスイッチを設定します。このようなバインディングが判断できない場合は、レイヤ 3 で、ダイナミック ARP インスペクション スイッチを実行していないスイッチから、ダイナミック ARP インスペクションを実行しているスイッチを分離します。

（注） DHCP サーバとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。デフォルトでは、信頼できないインターフェイスのレートは 15 パケット/秒（pps）です。信頼できるインターフェイスはレート制限されません。この設定を変更するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。ユーザが介入するまで、ポートはこの状態を維持します。**errdisable recovery** グローバル コンフィギュレーション コマンドを使用すると、errdisable ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。

（注） EtherChannel のレート制限は、スタックにある各スイッチに個別に適用されます。たとえば、EtherChannel で 20 pps の制限が設定されている場合、EtherChannel にあるポートの各スイッチでは、最大 20 pps まで実行できます。スイッチが制限を超過した場合、EtherChannel 全体が errdisable ステートになります。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのは、ACL が **ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用して設定されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

廃棄パケットのロギング

スイッチがパケットをドロップすると、ログ バッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。各ログエントリには、受信側の VLAN、ポート番号、送信元 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定します。記録されるパケットの種類を指定するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ARP インスペクションのデフォルト設定

機能	デフォルト設定
ダイナミック ARP インスペクション	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
着信 ARP パケットのレート制限	1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチドネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。 信頼できるすべてのインターフェイスでは、レート制限は行われません。 バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。

機能	デフォルト設定
ログ バッファ	ダイナミック ARP インスペクションがイネーブル化されると、拒否またはドロップされた ARP パケットはすべてが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは 1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのは、ACL が ip arp inspection filter vlan グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

非 DHCP 環境での ARP ACL の設定

この手順は、図 2 に示すスイッチ B がダイナミック ARP インスペクション、または DHCP スヌーピングをサポートしていないときにダイナミック ARP インスペクションを設定する方法を示しています。

スイッチ A のポート 1 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、スイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが作り出されます。これを阻止するには、スイッチ A のポート 1 を信頼できないものとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない（スイッチ A で ACL 設定を適用することは不可能である）場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを使用してパケットをルートする必要があります。

スイッチ A で ARP ACL を設定するには、次の手順を実行します。この手順は、非 DHCP 環境では必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**arp access-list** *acl-name*	ARP ACL を定義し、ARP アクセス リスト コンフィギュレーション モードを開始します。デフォルトでは、ARP アクセス リストは定義されません。 （注） ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。
ステップ 4	**permit ip host** *sender-ip* **mac host** *sender-mac*	指定されたホスト（ホスト 2）からの ARP パケットを許可します。 • *sender-ip* には、ホスト 2 の IP アドレスを入力します。 • *sender-mac* には、ホスト 2 の MAC アドレスを入力します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]	VLAN に ARP ACL を適用します。デフォルトでは、定義済みの ARP ACL は、どのような VLAN にも適用されません。 • *arp-acl-name* には、ステップ 2 で作成した ACL の名前を指定します。

	コマンドまたはアクション	目的
		• *vlan-range* では、スイッチとホストが存在する VLAN を指定します。VLAN ID 番号により識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）**static** を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットは廃棄されます。DHCP バインディングは使用されません。 このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。 IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセスリストで許可された場合だけに許可されます。
ステップ 7	**interface** *interface-id*	スイッチ B に接続されたスイッチ A のインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 8	**no ip arp inspection trust**	スイッチ B に接続されたスイッチ A のインターフェイスを untrusted として設定します。 デフォルトでは、すべてのインターフェイスは信頼できません。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC

	コマンドまたはアクション	目的
		アドレスとの有効なバインディングを持つことを確認してから、ローカルキャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバルコンフィギュレーションコマンドで指定されたロギング設定に従ってログバッファに記録します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	次の show コマンドを使用します。 • **show arp access-list** acl-name • **show ip arp inspection vlan** *vlan-range* • **show ip arp inspection interfaces**	入力を確認します。
ステップ 11	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

DHCP 環境でのダイナミック ARP インスペクションの設定

始める前に

この手順では、2つのスイッチがダイナミック ARPインスペクションをサポートしているときに、この機能を設定する方法を示します。ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B にそれぞれ接続されています。スイッチは両方とも、ホストが配置されている VLAN 1 でダイナミック ARP インスペクションを実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。したがって、スイッチ A はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。

（注） 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

ダイナミック ARP インスペクションを設定するには、次の手順を実行します。この処理は、両方のスイッチで行う必要があります。この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show cdp neighbors** 例： `Device(config-if)#show cdp neighbors`	スイッチ間の接続を確認します。
ステップ 3	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**ip arp inspection vlan** *vlan-range* 例： `Device(config)# ip arp inspection vlan 1`	VLAN 単位で、ダイナミック ARP インスペクションをイネーブルにします。デフォルトでは、すべての VLAN 上でダイナミック ARP インスペクションはディセーブルになっています。 vlan-range には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。両方のスイッチに同じ VLAN ID を指定します。
ステップ 5	**Interface***interface-id* 例：	他のスイッチに接続されるインターフェイスを指定して、インターフェイ

	コマンドまたはアクション	目的
	`Device(config)# interface gigabitethernet1/0/1`	スコンフィギュレーションモードを開始します。
ステップ 6	**ip arp inspection trust** 例： `Device(config-if)#ip arp inspection trust`	スイッチ間の接続を trusted に設定します。デフォルトでは、すべてのインターフェイスは信頼できません。 スイッチは、信頼できるインターフェイスにあるもう 1 つのスイッチから受信した ARP パケットは確認しません。この場合、パケットはそのまま転送されます。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカルキャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログバッファに記録します。
ステップ 7	**end** 例： `Device(config-if)#end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip arp inspection interfaces** 例：	インターフェイスでダイナミック ARP インスペクションの設定を検証します。
ステップ 9	**show ip arp inspection vlan** *vlan-range* 例： `Device(config-if)#show ip arp inspection vlan 1`	VLAN でダイナミック ARP インスペクションの設定を検証します。
ステップ 10	**show ip dhcp snooping binding** 例： `Device(config-if)#show ip dhcp snooping binding`	DHCP バインディングを確認します。

	コマンドまたはアクション	目的
ステップ 11	**show ip arp inspection statistics vlan** *vlan-range* 例： `Device(config-if)#show ip arp inspection statistics vlan 1`	VLAN でダイナミック ARP インスペクションの統計情報を確認します。
ステップ 12	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

着信 ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。errordisable 回復をイネーブルにして、指定されたタイムアウト時間の後にポートがこのステートから自動的に抜け出すようにするまで、ポートはこのステートのままです。

（注） インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、レート制限をその信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

着信 ARP パケットのレートを制限するには、次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	レート制限されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip arp inspection limit {rate pps [burst interval seconds] | none}**	インターフェイス上の着信 ARP 要求および ARP 応答のレートを制限します。デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。バースト インターバルは 1 秒です。 キーワードの意味は次のとおりです。 • **rate***pps* には、1 秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ～ 2048 pps です。 • （任意）**burst interval***seconds* は、レートの高い ARP パケットの有無についてインターフェイスがモニタリングされる間隔（秒）を指定します。指定できる範囲は 1 ～ 15 です。 • **rate none** では、処理できる着信 ARP パケットのレートの上限を設定しません。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	次のコマンドを使用します。 • **errdisable detect cause arp-inspection** • **errdisable recovery cause arp-inspection**	（任意）ダイナミック ARP インスペクションの errdisable ステートからのエラー回復をイネーブルにし、ダイナミック ARP インスペクションの回復メ

	コマンドまたはアクション	目的
	• **errdisable recovery interval** 間隔	カニズムで使用する変数を設定します。 デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。 **interval** *interval* では、errdisable ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。
ステップ 7	**exit**	特権 EXEC モードに戻ります。
ステップ 8	次の show コマンドを使用します。 • **show ip arp inspection interfaces** • **show errdisable recovery**	設定を確認します。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ダイナミック ARP インスペクション検証チェックの実行

ダイナミック ARP インスペクションは、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。宛先 MAC アドレス、送信側および宛先の IP アドレス、および送信元 MAC アドレスで追加検証を実行するように、スイッチを設定できます。

着信 ARP パケットで特定のチェックを実行するには、次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip arp inspection validate {[src-mac] [dst-mac] [ip]}**	着信 ARP パケットで特定の検査を実行します。デフォルトでは、検証は実行されません。 キーワードの意味は次のとおりです。 • **src-mac** では、イーサネット ヘッダーの送信元MACアドレスとARP本文の送信元MACアドレスが比較されます。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **dst-mac** では、イーサネット ヘッダーの宛先 MAC アドレスと ARP 本文の宛先MACアドレスが比較されます。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **ip** では、ARP 本文から、無効な IP アドレスや予期しない IP アドレスがないかを確認します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレ

	コマンドまたはアクション	目的
		スは ARP 応答内だけで検査されます。 少なくとも 1 つのキーワードを指定する必要があります。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが src および dst mac の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番めのコマンドによって src および dst mac の検証がディセーブルになります。
ステップ 4	**exit**	特権 EXEC モードに戻ります。
ステップ 5	**show ip arp inspection vlan** *vlan-range*	設定を確認します。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

DAI のモニタリング

DAI をモニタするには、次のコマンドを使用します。

コマンド	説明
clear ip arp inspection statistics	ダイナミック ARP インスペクション統計情報をクリアします。

コマンド	説明
show ip arp inspection statistics [**vlan** *vlan-range*]	指定のVLANにおいて、転送されたパケット、廃棄されたパケット、MAC検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。
clear ip arp inspection log	ダイナミック ARP インスペクション ログ バッファをクリアします。
show ip arp inspection log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

show ip arp inspection statistics コマンドでは、スイッチは信頼されたダイナミック ARP インスペクション ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

DAI の設定の確認

DAI の設定を表示して確認するには、次のコマンドを使用します。

コマンド	説明
show arp access-list [*acl-name*]	ARP ACL についての詳細情報を表示します。
show ip arp inspection interfaces [interface-id]	指定されたインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。
show ip arp inspection vlan *vlan-range*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 109 章

IEEE 802.1x ポートベースの認証の設定

この章では、IEEE 802.1x ポート ベース認証を設定する方法について説明します。IEEE 802.1x 認証は、不正なデバイス（クライアント）によるネットワーク アクセスを防止します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチまたはスイッチ スタックを意味します。

- 機能情報の確認 （2335 ページ）
- 802.1x ポートベース認証について （2335 ページ）
- 802.1x ポートベース認証の設定方法 （2375 ページ）
- 802.1x の統計情報およびステータスのモニタリング （2429 ページ）
- その他の参考資料 （2430 ページ）
- IPv4 アクセス コントロール リストに関する機能情報 （2431 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

802.1x ポートベース認証について

802.1x 規格では、一般の人がアクセス可能なポートから不正なクライアントが LAN に接続しないように規制する（適切に認証されている場合を除く）、クライアント/サーバ型のアクセス コントロールおよび認証プロトコルを定めています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN が提供するサービスを利用できるようにします。

（注） TACACS は、802.1x 認証ではサポートされていません。

802.1xアクセスコントロールでは、クライアントを認証するまでの間、そのクライアントが接続しているポート経由ではExtensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、およびスパニングツリー プロトコル（STP）トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

（注） RADIUS および AAA のデバッグのログを表示するには、**show platform software trace message smd** コマンドを使用します。詳細については、『*Command Reference Guide, Cisco IOS XE Denali 16.1.1*』の「Trace Commands」の項を参照してください。

ポートベース認証プロセス

IEEE 802.1X ポートベース認証を設定するには、認証、認可、およびアカウンティング（AAA）を有効にし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

AAA プロセスは認証から始まります。802.1x ポートベース認証がイネーブルであり、クライアントが 802.1x 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

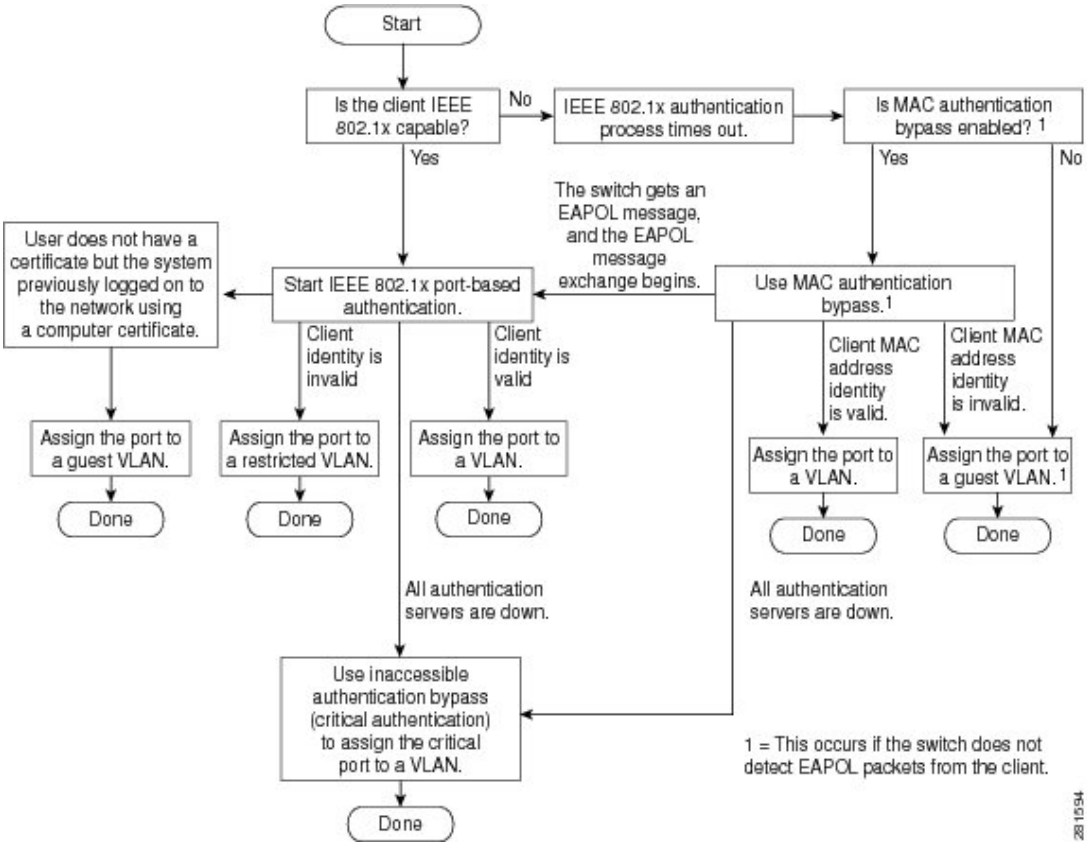
- クライアント ID が有効で 802.1x 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。

（注） アクセスできない認証バイパスは、クリティカル認証、または AAA 失敗ポリシーとも呼ばれます。

ポートで Multi Domain Authentication（MDA）が有効になっている場合、音声許可に該当する例外をいくつか伴ったフローを使用できます。

図 *126 :* 認証フローチャート

次の図は認証プロセスを示します。



次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

  スイッチ固有の値を使用するか、RADIUS サーバからの値に基づいて再認証タイマーを設定できます。

  RADIUS サーバを使用した 802.1x 認証の後で、スイッチは Session-Timeout RADIUS 属性（Attribute[27]）、および Termination-Action RADIUS 属性（Attribute[29]）に基づいてタイマーを使用します。

  Session-Timeout RADIUS 属性（Attribute[27]）には再認証が行われるまでの時間を指定します。

  Termination-Action RADIUS 属性（Attribute[29]）には、再認証中に行われるアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。アクションに *Initialize*（属性値は *DEFAULT*）を設定した場合、802.1x セッションは終了し、認証中、接続は失われます。アクションに *ReAuthenticate*（属性値は RADIUS-Request）を設定した場合、セッションは再認証による影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを入力します。

ポートベース認証の開始およびメッセージ交換

802.1x認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証を有効にすると、スイッチは、リンク ステートがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

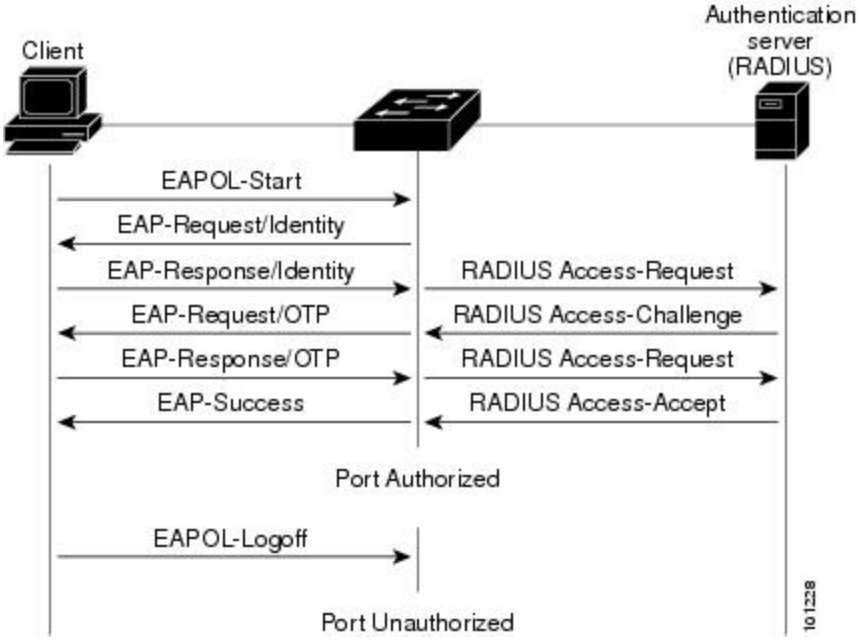
（注） ネットワーク アクセスデバイスで802.1x認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。

図 *127 :* メッセージ交換

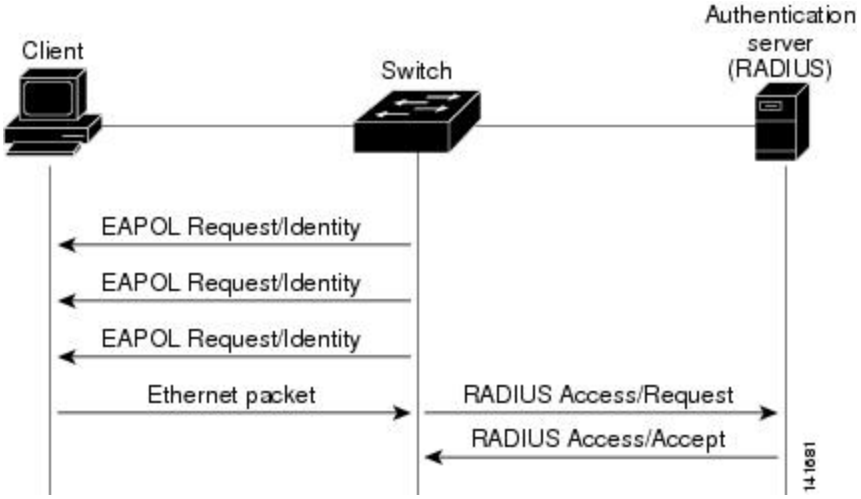
次の図に、クライアントが RADIUS サーバとの間で OTP（ワンタイム パスワード）認証方式を使用する際に行われるメッセージ交換を示します。



EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネットパケットを検出するとそのクライアントを認証できます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS Access/Request フレームにこの情報を保存します。サーバがスイッチに RADIUS Access/Accept フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネット パケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、802.1x 認証を開始します。

図 *128 : MAC* 認証バイパス中のメッセージ交換

次の図に、MAC 認証バイパス中のメッセージ交換を示します。



ポートベース認証の認証マネージャ

ポートベース認証方法

表 *147 : 802.1x* 機能

Authentication method	モード			
	シングル ホスト	マルチ ホスト	MDA	複数認証
802.1x	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL

Authentication method	モード			
	シングル ホスト	マルチ ホスト	MDA	複数認証
スタンドアロン Web 認証	プロキシ ACL、Filter-ID 属性、ダウンロード可能 ACL			
NAC レイヤ 2 IP 検証	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL
フォールバック方式としての Web 認証	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL

[16] Cisco IOS Release 12.2(50)SE 以降でサポートされています。
[17] 802.1x 認証をサポートしないクライアント用。

ユーザ単位 ACL および Filter-Id

（注） **any** は、ACL の発信元としてだけ設定できます。

（注） マルチホスト モードで設定された ACL では、ステートメントの発信元部分は *any* でなければなりません。（たとえば、**permit icmp** *any***host 10.10.1.1**）

定義された ACL の発信元ポートには **any** を指定する必要があります。指定しない場合、ACL は適用できず、認証は失敗します。シングル ホストは唯一例外的に後方互換性をサポートします。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。ホストに適用される ACL ポリシーは、別のホストのトラフィックには影響を与えません。マルチ ホスト ポートで認証されるホストが 1 つだけで、他のホストが認証なしでネットワーク アクセスを取得する場合、発信元アドレスに any を指定することで、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

ポートベース認証マネージャ CLI コマンド

認証マネージャ インターフェイス コンフィギュレーション コマンドは、802.1x、MAC 認証バイパスおよび Web 認証など、すべての認証方法を制御します。認証マネージャ コマンドは、接続ホストに適用される認証方法のプライオリティと順序を決定します。

認証マネージャ コマンドは、ホスト モード、違反モードおよび認証タイマーなど、一般的な認証機能を制御します。一般的な認証コマンドには、**authentication host-mode**、**authentication violation** および **authentication timer** インターフェイス コンフィギュレーション コマンドがあります。

802.1x 専用コマンドは、先頭に **dot1x** キーワードが付きます。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにします。ただし、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドは常にグローバルに 802.1x 認証をイネーブルまたはディセーブルにします。

（注） 802.1x 認証がグローバルにディセーブル化されても、Web 認証など他の認証方法はそのポートでイネーブルのままです。

authentication manager コマンドは従来の 802.1x コマンドと同様の機能を提供します。

認証マネージャが生成する冗長なシステム メッセージをフィルタリングすると、通常は、フィルタリングされた内容が認証の成功に結びつきます。802.1x 認証および MAB 認証の冗長なメッセージをフィルタリングすることもできます。認証方式ごとに異なるコマンドが用意されています。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの冗長なメッセージをフィルタリングします。
- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1x 認証の冗長なメッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC 認証バイパス（MAB）の冗長なメッセージをフィルタリングします。

表 *148 :* 認証マネージャ コマンドおよび以前の *802.1x* コマンド

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
authentication control-direction {**both** | **in**}	**dot1x control-direction** {**both** | **in**}	Wake-on-LAN（WoL）機能を使用して 802.1x 認証をイネーブルにし、ポート制御を単一方向または双方向に設定します。

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
authentication event	**dot1x auth-fail vlan** **dot1x critical (interface configuration)** **dot1x guest-vlan6**	ポート上で制限付き VLAN をイネーブルにします。 アクセス不能認証バイパス機能をイネーブルにします。 アクティブ VLAN を 802.1x ゲスト VLAN として指定します。
authentication fallback *fallback-profile*	**dot1x fallback** *fallback-profile*	802.1x 認証をサポートしていないクライアント用に、Web 認証をフォールバック方式として使用するようにポートを設定します。
authentication host-mode [multi-auth | multi-domain | multi-host | single-host]	**dot1x host-mode {single-host | multi-host | multi-domain}**	802.1x 許可ポートで単一のホスト（クライアント）または複数のホストの接続を許可します。
authentication order	**mab**	使用される認証方法の順序を柔軟に定義できるようにします。
authentication periodic	**dot1x reauthentication**	クライアントの定期的再認証をイネーブルにします。
authentication port-control {auto | force-authorized | force-un authorized}	**dot1x port-control {auto | force-authorized | force-unauthorized}**	ポートの許可ステートの手動制御をイネーブルにします。
authentication timer	**dot1x timeout**	802.1x タイマーを設定します。
authentication violation {protect | restrict | shutdown}	**dot1x violation-mode {shutdown | restrict | protect}**	新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続された後に新しいデバイスがそのポートに接続された場合に発生する違反モードを設定します。

許可ステートおよび無許可ステートのポート

802.1x 認証中に、スイッチのポート ステートによって、スイッチはネットワークへのクライアント アクセスを許可します。ポートは最初、無許可ステートです。このステートでは、音声 VLAN（仮想 LAN）ポートとして設定されていないポートは 802.1x 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは許可ステートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN ポートとして設定されている場合、VoIP トラフィックおよび 802.1x プロトコル パケットが許可された後クライアントが正常に認証されます。

（注） CDP バイパスはサポートされていないため、ポートが error-disabled ステートになる場合があります。

802.1x をサポートしていないクライアントが、無許可ステートの 802.1x ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x 対応のクライアントが、802.1x 標準が稼働していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

authentication port-control インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized**：802.1x 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized**：ポートが無許可ステートのままになり、クライアントからの認証の試みをすべて無視します。スイッチはポートを介してクライアントに認証サービスを提供できません。
- **auto**：802.1x 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、スイッチは要求を再送信します。所定の

回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

ポートのリンク ステートがアップからダウンに変更した場合、またはEAPOL-Logoffフレームを受信した場合に、ポートは無許可ステートに戻ります。

ポートベース認証とスイッチ スタック

スイッチが、スイッチ スタックに追加されるか、スイッチ スタックから削除される場合、RADIUS サーバとスタックとの間の IP 接続が正常な場合、802.1x 認証は影響を受けません。これは、スタック マスターがスイッチスタックから削除される場合も、適用されます。スタック マスターに障害が発生した場合、スタック メンバは、選択プロセスを使用することによって新しいスタック マスターになり、802.1x 認証プロセスは通常どおり続行されます。

サーバに接続されていたスイッチが削除されたか、そのスイッチに障害が発生したために、RADIUS サーバへの IP 接続が中断された場合、これらのイベントが発生します。

- すでに認証済みで、定期的な再認証がイネーブルではないポートは、認証ステートのままです。RADIUS サーバとの通信は、必要ではありません。
- すでに認証済みで、（**dot1x re-authentication** グローバル コンフィギュレーション コマンドを使用）定期的な再認証がイネーブルにされているポートは、再認証の発生時に、認証プロセスに失敗します。ポートは、再認証プロセス中に、非認証ステートに戻ります。RADIUS サーバとの通信が必要です。

  進行中の認証については、サーバ接続が行われていないため、認証はただちに失敗します。

障害が発生したスイッチが実行状態になり、スイッチスタックに再加入した場合、ブートアップの時刻と、認証の試行時までにRADIUSサーバへの接続が再確立されたかどうかによって、認証は失敗する場合と、失敗しない場合があります。

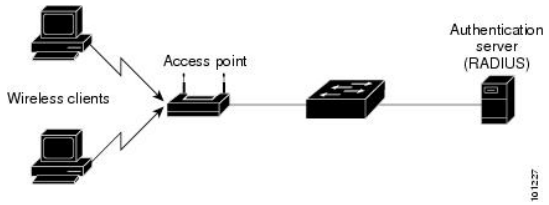
RADIUSサーバへの接続を失うことを避けるには、冗長接続を設定する必要があります。たとえば、スタック マスターへの冗長接続と、スタック メンバへの別の接続を設定できます。スタック マスターに障害が発生した場合でも、スイッチ スタックは、RADIUS サーバに接続されたままです。

802.1X のホスト モード

802.1x ポートは、シングル ホスト モードまたはマルチ ホスト モードで設定できます。シングル ホスト モードでは、802.1x 対応のスイッチ ポートに接続できるのはクライアント 1 つだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチホストモードでは、複数のホストを単一の802.1x対応ポートに接続できます。このモードでは、接続されたクライアントのうち1つが許可されれば、クライアントすべてのネットワークアクセスが許可されます。ポートが無許可ステートになると（再認証が失敗するか、またはEAPOL-Logoffメッセージを受信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

図 *129 :* マルチ ホスト モードの例



（注） すべてのホスト モードで、ポートベース認証が設定されている場合、ライン プロトコルは許可の前にアップのままです。

スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置とIP Phoneなどの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチ ポートに接続できます。

802.1x 複数認証モード

複数認証（multiauth）モードでは、データVLANで複数のクライアントを認証できます。各ホストは個別に認証されます。音声VLANが設定されている場合、このモードでは、VLANで1クライアントだけ認証できます（ポートが他の音声クライアントを検出すると、これらはポートから廃棄されますが、違反エラーは発生しません）。

ハブまたはアクセス ポイントが802.1x対応ポートに接続されている場合、接続されている各クライアントを認証する必要があります。802.1x以外のデバイスでは、MAC認証バイパスまたはWeb認証をホスト単位認証フォールバック メソッドとして使用し、単一のポートで異なる方法で異なるホストを認証できます。

複数認証ポートで認証できるデータ ホストの数には制限はありません。ただし、音声VLANが設定されている場合、許可される音声デバイスは1台だけです。ホスト制限がないため、定義された違反はトリガーされません。たとえば、別の音声デバイスが検出された場合、これは通知なしで廃棄され、違反はトリガーされません。音声VLANのMDA機能の場合、複数認証モードでは、認証サーバから受け取ったVSAに応じて、認証されたデバイスがデータまたは音声のいずれかのVLANに割り当てられます。

（注） ポートがマルチ認証モードの場合、ゲスト VLAN、および認証失敗 VLAN 機能はアクティブになりません。

次の条件で、RADIUS サーバから提供された VLAN をマルチ認証モードで割り当てることができます。

- ホストがポートで最初に許可されたホストであり、RADIUS サーバが VLAN 情報を提供している。
- 後続のホストが、動作 VLAN に一致する VLAN を使用して許可される。
- ホストは VLAN が割り当てられていないポートで許可され、後続のホストでは VLAN 割り当てが設定されていないか、VLAN 情報が動作 VLAN と一致している。
- ポートで最初に許可されたホストにはグループ VLAN が割り当てられ、後続のホストでは VLAN 割り当てが設定されていないか、グループ VLAN がポート上のグループ VLAN と一致している。後続のホストが、最初のホストと同じ VLAN グループの VLAN を使用する必要がある。VLAN リストが使用されている場合、すべてのホストは VLAN リストで指定された条件に従う。
- マルチ認証ポート上で、1 つの音声 VLAN 割り当てのみがサポートされている。
- VLAN がポート上のホストに割り当てられると、後続のホストは一致する VLAN 情報を持つ必要があり、この情報がなければポートへのアクセスを拒否される。
- ゲスト VLAN または認証失敗 VLAN をマルチ認証モードに設定できない。
- クリティカル認証 VLAN の動作が、マルチ認証モード用に変更されない。ホストが認証を試みたときにサーバに到達できない場合、許可されたすべてのホストは、設定された VLAN で再初期化される。

ユーザごとのマルチ認証 VLAN 割り当て

（注） この機能は、LAN base イメージを実行している Catalyst 2960X スイッチのみでサポートされています。

ユーザごとのマルチ認証 VLAN 割り当て機能を使用すると、単一の設定済みアクセス VLAN を持つポート上のクライアントに割り当てられた VLAN に基づいて複数の運用アクセス VLAN を作成することができます。データ ドメインに関連付けられたすべての VLAN に対するトラフィックが dot1q とタグ付けされていないアクセス ポートとして設定されているポートおよびこれらの VLAN は、ネイティブ VLAN として処理されます。

マルチ認証ポート 1 つあたりのホストの数は 8 ですが、さらに多くのホストが存在する場合があります。

（注） ユーザごとのマルチ認証 VLAN 割り当て機能は、音声ドメインではサポートされません。ポート上の音声ドメインのすべてのクライアントが同じ VLAN を使用する必要があります。

次のシナリオは、ユーザごとのマルチ認証 VLAN 割り当てに関連しています。

シナリオ 1

ハブがアクセス ポートに接続されている場合、およびポートがアクセス VLAN（V0）で設定されている場合。

ホスト（H1）は、ハブを介して VLAN（V1）に割り当てられます。ポートの運用 VLAN は V1 に変更されます。この動作は、単一ホスト ポートまたはマルチ ドメイン認証ポートで同様です。

2 番目のホスト（H2）が接続され、VLAN（V2）に割り当てられる場合、ポートには 2 つの運用 VLAN があります（V1 および V2）。H1 と H2 がタグなし入力トラフィックを送信すると、H1 トラフィックは VLAN（V1）に、H2 トラフィックは VLAN（V2）にマッピングされ、VLAN（V1）および VLAN（V2）のポートからの出トラフィックはすべてタグなしになります。

両方のホスト H1 と H2 がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN（V1）と VLAN（V2）がポートから削除され、設定された VLAN（V0）がポートに復元されます。

シナリオ 2

ハブがアクセス ポートに接続されている場合、およびポートがアクセス VLAN（V0）で設定されている場合。ホスト（H1）は、ハブを介して VLAN（V1）に割り当てられます。ポートの運用 VLAN は V1 に変更されます。

2 番目のホスト（H2）が接続され明示的な VLAN ポリシーなしで承認されると、H2 はポート上で復元される設定済み VLAN（V0）を使用することを予期されます。2 つの運用 VLAN、VLAN（V0）および VLAN（V1）からの出トラフィックはすべてタグなしになります。

ホスト（H2）がログアウトするか、またはセッションがなんらかの理由で削除されると、設定された VLAN（V0）がポートから削除され、VLAN（V1）がそのポートでの唯一の運用 VLAN になります。

シナリオ 3

ハブがオープン モードでアクセス ポートに接続されている場合、およびポートがアクセス VLAN（V0）で設定されている場合。

ホスト（H1）は、ハブを介して VLAN（V1）に割り当てられます。ポートの運用 VLAN は V1 に変更されます。2 番目のホスト（H2）が接続され無許可のままだと、オープン モードにより、運用 VLAN（V1）に引き続きアクセスできます。

ホスト H1 がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN（V1）はポートから削除され、ホスト（H2）は VLAN（V0）に割り当てられます。

（注） オープン モードと VLAN 割り当ての組み合わせは、ホスト（H2）に悪影響を与えます。そのホストは VLAN（V1）に対応するサブネット内に IP アドレスを含んでいるからです。

ユーザごとのマルチ認証 VLAN 割り当ての制限

ユーザごとのマルチ認証 VLAN 割り当て機能では、複数の VLAN からの出トラフィックは、ホストが自分宛てではないトラフィックを受信するポート上ではタグなしになります。これは、ブロードキャストおよびマルチキャスト トラフィックで問題になる可能性があります。

- **IPv4 ARP**：ホストは他のサブネットからの ARP パケットを受信します。これは、IP アドレス範囲が重複する異なる仮想ルーティングおよび転送（VRF）テーブルの 2 個のサブネットがポート上でアクティブな場合に問題となります。ホストの ARP キャッシュが無効なエントリを受け取る可能性があります。
- **IPv6 制御パケット**：IPv6 の導入環境では、ルータ アドバタイズメント（RA）は、その受信を想定されていないホストによって処理されます。ある VLAN からのホストが別の VLAN からの RA を受信すると、ホストはそれ自身に間違った IPv6 アドレスを割り当てます。このようなホストは、ネットワークにアクセスできません。

  回避策は、IPv6 ファースト ホップ セキュリティをイネーブルにして、ブロードキャスト ICMPv6 パケットがユニキャストに変換され、マルチ認証がイネーブルのポートから送信されるようにすることです。パケットは VLAN に属するマルチ認証ポートの各クライアント用に複製され、宛先 MAC が個々のクライアントに設定されます。1 つの VLAN を持つポートで、ICMPv6 パケットは正常にブロードキャストされます。
- **IP マルチキャスト**：送信先のマルチキャスト グループへのマルチキャスト トラフィックは、異なる VLAN 上のホストがそのマルチキャスト グループに参加している場合それらの VLAN 用に複製されます。異なる VLAN の 2 つのホストが（同じマルチ認証ポート上の）マルチキャスト グループに参加している場合、各マルチキャスト パケットのコピー 2 部がそのポートから送信されます。

MAC 移動

あるスイッチ ポートでMACアドレスが認証されると、そのアドレスは同じスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じ MAC アドレスを別の認証マネージャ対応ポートで検出すると、そのアドレスは許可されなくなります。

場合によっては、MAC アドレスを同じスイッチ上のポート間で移動する必要があります。たとえば、認証ホストとスイッチ ポート間に別のデバイス（ハブまたは IP Phone など）がある場合、ホストをデバイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC 移動をグローバルにイネーブルにできます。ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再認証されます。MAC 移動はすべてのホスト モードでサポートされます（認証ホストは、ポートでイネーブルにされているホスト モードに関係なく、スイッチの任意のポートに移動できます）。MAC アドレスがあるポートから別のポートに移動すると、スイッチは元のポートで認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。MAC 移動の機能は、音声およびデータ ホストの両方に適用されます。

（注） オープン認証モードでは、MACアドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

MAC 置換

MAC 置換機能は、ホストが、別のホストがすでに認証済みであるポートに接続しようとすると発生する違反に対処するように設定できます。

（注） 違反はマルチ認証モードでは発生しないため、マルチ認証モードのポートにこの機能は適用されません。マルチホストモードで認証が必要なのは最初のホストだけなので、この機能はこのモードのポートには適用されません。

replace キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、マルチドメイン モードのポートでの認証プロセスは、次のようになります。

- 既存の認証済みMACアドレスを使用するポートで新しいMACアドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータ ホストの MAC アドレスを、新しい MAC アドレスで置き換えます。
- 認証マネージャは、新しい MAC アドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MACアドレスはただちにMACアドレステーブルに追加されます。

802.1x アカウンティング

802.1x 標準では、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1xアカウンティングは、デフォルトでディセーブルです。802.1xアカウンティングをイネーブルにすると、次の処理を 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。
- 再認証が失敗します。

スイッチは802.1xアカウンティング情報を記録しません。その代わり、スイッチはこの情報をRADIUSサーバに送信します。RADIUSサーバは、アカウンティングメッセージを記録するように設定する必要があります。

802.1x アカウンティング属性値ペア

RADIUSサーバに送信された情報は、属性値（AV）ペアの形式で表示されます。これらのAVペアのデータは、各種アプリケーションによって使用されます（たとえば課金アプリケーションの場合、RADIUSパケットのAcct-Input-OctetsまたはAcct-Output-Octets属性の情報が必要です）。

AVペアは、802.1xアカウンティングが設定されているスイッチによって自動的に送信されます。次の種類のRADIUSアカウンティング パケットがスイッチによって送信されます。

- START：新規ユーザ セッションが始まると送信されます。
- INTERIM：既存のセッションが更新されると送信されます。
- STOP：セッションが終了すると送信されます。

（注） RADIUSおよびAAAのデバッグのログを表示するには、**show platform software trace message smd** コマンドを使用します。詳細については、『*Command Reference Guide, Cisco IOS XE Denali 16.1.1*』のセクション「Tracing Commands」を参照してください。

次の表に、AVペアおよびスイッチによって送信されるAVペアの条件を示します。

表 *149*：アカウンティング *AV* ペア

Attribute Number	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	送信	送信	送信
属性 [4]	NAS-IP-Address	送信	送信	送信
属性 [5]	NAS-Port	送信	送信	送信
属性 [8]	Framed-IP-Address	非送信	条件に応じて送信[18]	条件に応じて送信
属性 [30]	Called-Station-ID	送信	送信	送信
属性 [31]	Calling-Station-ID	送信	送信	送信
属性 [40]	Acct-Status-Type	送信	送信	送信
属性 [41]	Acct-Delay-Time	送信	送信	送信
属性 [42]	Acct-Input-Octets	非送信	送信	送信

Attribute Number	AV ペア名	START	INTERIM	STOP
属性 [43]	Acct-Output-Octets	非送信	送信	送信
Attribute[47]	Acct-Input-Packets	非送信	送信	送信
属性 [48]	Acct-Output-Packets	非送信	送信	送信
属性 [44]	Acct-Session-ID	送信	送信	送信
属性 [45]	Acct-Authentic	送信	送信	送信
属性 [46]	Acct-Session-Time	非送信	送信	送信
属性 [49]	Acct-Terminate-Cause	非送信	非送信	送信
属性 [61]	NAS-Port-Type	送信	送信	送信

[18] 有効な静的 IP アドレスが設定されているか、ホストに対する Dynamic Host Control Protocol（DHCP）バインディングが DHCP スヌーピング バインディング テーブルに存在している場合に、Framed-IP-Address の AV ペアが送信されます。

802.1x 準備状態チェック

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。802.1x 機能をサポートしていないデバイスでは、MAC 認証バイパスまたは Web 認証などの代替認証を使用します。

この機能が有用なのは、クライアントのサプリカントで NOTIFY EAP 通知パケットでのクエリーがサポートされている場合だけです。クライアントは、802.1x タイムアウト値内に応答しなければなりません。

関連トピック

802.1x 準備状態チェックの設定 （2380 ページ）

スイッチと RADIUS サーバ間の通信

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

関連トピック

スイッチと RADIUS サーバ間の通信の設定 （2388 ページ）

VLAN 割り当てを使用した 802.1x 認証

スイッチは、VLAN 割り当てを使用した 802.1x 認証をサポートしています。ポートの 802.1x 認証が成功すると、RADIUS サーバは VLAN 割り当てを送信し、スイッチ ポートを設定します。RADIUS サーバデータベースは、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに接続するクライアントのユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

音声デバイス認証は、Cisco IOS Release 12.2(37)SE のマルチドメイン ホスト モードでサポートされています。Cisco IOS Release 12.2(40)SE 以降、音声デバイスが許可されており、RADIUS サーバが許可された VLAN を返した場合、割り当てられた音声 VLAN 上でパケットを送受信するようにポート上の音声 VLAN が設定されます。音声 VLAN 割り当ては、マルチドメイン認証（MDA）対応のポートでのデータ VLAN 割り当てと同じように機能します。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 802.1x 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1x 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN とは、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべて、この VLAN に所属します。
- 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

  設定エラーには、ルーテッド ポートの VLAN、間違った VLAN ID、存在しないまたは内部（ルーテッド ポート）の VLAN ID、RSPAN VLAN、シャットダウンしている VLAN、あるいは一時停止している VLAN ID の指定などがあります。マルチドメイン ホスト ポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行（またはその逆）のために発生するものもあります。
- 802.1x 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。
- 802.1x ポートでマルチ ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN（RADIUS サーバにより指定）に配置されます。
- ポート セキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメイン ホ

ストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。

- あるデバイスでVLAN設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みのVLANと一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みのVLANが一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
- 音声デバイスが許可されて、ダウンロードされた音声VLANを使用している場合、音声VLAN設定を削除したり設定値をdot1pまたはuntaggedに修正したりすると、音声デバイスが未許可になり、マルチドメインホストモードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウンステートの場合、ポートは設定済みのアクセスVLANに配置されます。

802.1xポートが認証され、RADIUSサーバによって割り当てられたVLANに配置されると、そのポートのアクセスVLAN設定への変更は有効になりません。マルチドメインホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。

- あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済または割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
- 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウンステートの場合、ポートは設定済みのアクセスVLANに配置されます。

トランク ポート、ダイナミック ポート、または VLAN メンバーシップ ポリシー サーバ（VMPS）によるダイナミック アクセス ポート割り当ての場合、VLAN割り当て機能を使用した 802.1x 認証はサポートされません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x認証をイネーブルにします。（アクセスポートで802.1x認証を設定すると、VLAN割り当て機能は自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802

- [81] Tunnel-Private-Group-ID = VLAN 名または VLAN ID
- [83] Tunnel-Preference

属性 [64] は、値 *VLAN*（タイプ 13）でなければなりません。属性 [65] は、値*802*（タイプ 6）でなければなりません。属性 [81] は、IEEE 802.1x 認証ユーザに割り当てられた *VLAN* 名または *VLAN ID* を指定します。

ユーザ単位 ACL を使用した 802.1x 認証

ユーザ単位アクセス コントロール リスト（ACL）をイネーブルにして、異なるレベルのネットワーク アクセスおよびサービスを 802.1x 認証ユーザに提供できます。RADIUS サーバは、802.1x ポートに接続されるユーザを認証する場合、ユーザ ID に基づいて ACL 属性を受け取り、これらをスイッチに送信します。スイッチは、ユーザ セッションの期間中、その属性を 802.1x ポートに適用します。セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザ単位 ACL 設定が削除されます。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションには保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

ユーザは同一のスイッチ上で、ルータ ACL および入力ポート ACL を使用できます。ただし、ポートの ACL はルータ ACL より優先されます。入力ポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力ルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド パケットは、ルータ ACL によってフィルタリングされます。発信するルーテッド パケットには、ルータ ACL のフィルタが適用されます。コンフィギュレーションの矛盾を回避するには、RADIUS サーバに保存するユーザ プロファイルを慎重に計画しなければなりません。

RADIUS は、ベンダー固有属性などのユーザ単位属性をサポートします。ベンダー固有属性（VSA）は、オクテット ストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では inacl#<*n*> で、出力方向では outacl#<*n*> です。MAC ACL は、入力方向に限りサポートされます。VSA は入力方向に限りサポートされます。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザ単位コンフィギュレーションを定義します。RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。属性には、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す *.in* または *.out* が含まれています。RADIUS サーバが *.in* または *.out* 構文を許可しない場合、アクセス リストはデフォルトで発信 ACL に適用されます。スイッチでの Cisco IOS のアクセス リストに関するサポートが制限されているため、Filter-ID 属性は 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL および IP 拡張 ACL）に対してだけサポートされます。

ユーザ単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズにより制限されます。

ユーザ単位の ACL を設定するには、次の手順に従います。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- 802.1x ポートをシングル ホスト モードに設定します。

（注） ユーザ単位 ACL がサポートされるのはシングル ホスト モードだけです。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証

ACL およびリダイレクト URL は、ホストの 802.1x 認証または MAC 認証バイパス中に、RADIUS サーバからスイッチにダウンロードできます。また、Web 認証中に ACL をダウンロードすることもできます。

（注） ダウンロード可能な ACL は *dACL* とも呼ばれます。

複数のホストが認証され、それらのホストがシングル ホスト モード、MDA モード、またはマルチ認証モードである場合、スイッチは ACL の送信元アドレスをホスト IP アドレスに変更します。

ACL およびリダイレクト URL は、802.1x 対応のポートに接続されるすべてのデバイスに適用できます。

ACL が 802.1x 認証中にダウンロードされない場合、スイッチは、ポートのスタティック デフォルト ACL をホストに適用します。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、スイッチは ACL を認証ポリシーの一部として電話にだけ適用します。

（注） スタック構成がある dACL の制限は、ポートベースの dACL あたり 64 ACE です。スタック構成なしの制限は、利用可能な TCAM エントリの数になり、これはアクティブな他の ACL 機能によって異なります。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、ポート上にスタティック ACL がない場合、ダイナミックな認証デフォルト ACL が作成され、dACL がダウンロードされて適用される前にポリシーが実施されます。

（注） 認証デフォルト ACL は、実行コンフィギュレーションでは表示されません。

認証デフォルト ACL は、ポートで許可ポリシーを持つホストが 1 つ以上検出されると作成されます。認証デフォルト ACL は、最後の認証セッションが終了すると削除されます。認証デフォルト ACL は、**ip access-list extended auth-default-acl** グローバル コンフィギュレーション コマンドを使用して設定できます。

（注） 認証デフォルト ACL は、シングル ホスト モードの Cisco Discovery Protocol（CDP）バイパスをサポートしていません。CDP バイパスをサポートするには、インターフェイス上のスタティック ACL を設定する必要があります。

802.1x および MAB 認証方式では、オープンおよびクローズの 2 つの認証方式がサポートされます。クローズ認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL が作成されます。
- 認証デフォルト ACL は、ポリシーが実施されるまで DHCP トラフィックのみを許可します。
- 最初のホスト認証では、許可ポリシーは IP アドレスを挿入せずに適用されます。
- 別のホストが検出されると、最初のホストのポリシーがリフレッシュされ、最初のセッションと後続セッションのポリシーが IP アドレスを挿入して実施されます。

オープン認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL-OPEN が作成され、すべてのトラフィックが許可されます。
- セキュリティ違反を防ぐために、IP アドレスを挿入してポリシーが実施されます。
- Web 認証は、認証デフォルト ACL-OPEN に従います。

許可ポリシーのないホストへのアクセスを制御するために、ディレクティブを設定することができます。サポートされているディレクティブの値は、*open* と *default* です。*open* ディレクティブを設定すると、すべてのトラフィックが許可されます。*default* ディレクティブは、ポートから提供されるアクセスにトラフィックを従わせます。ディレクティブは、AAA サーバ上のユーザプロファイル、またはスイッチ上のいずれかで設定できます。AAA サーバ上でディレクティブを設定するには、**authz-directive =<open/default>** グローバル コマンドを使用します。スイッチ上でディレクティブを設定するには、**epm access-control open** グローバル コンフィギュレーション コマンドを使用します。

（注） ディレクティブのデフォルト値は *default* です。

設定された ACL なしでポート上の Web 認証にホストがフォールバックする場合は、次のようになります。

- ポートがオープン認証モードの場合、認証デフォルト ACL-OPEN が作成されます。
- ポートがクローズ認証モードの場合、認証デフォルト ACL が作成されます。

フォールバック ACL のアクセス コントロール エントリ（ACE）は、ユーザ単位のエントリに変換されます。設定されたフォールバック プロファイルにフォールバック ACL が含まれていない場合、ホストはポートに関連付けられた認証デフォルト ACL に従います。

（注） Web 認証でカスタム ロゴを使用し、それを外部サーバに格納する場合、認証の前にポートの ACL で外部サーバへのアクセスを許可する必要があります。外部サーバに適切なアクセスを提供するには、スタティック ポート ACL を設定するか、認証デフォルト ACL を変更する必要があります。

Cisco Secure ACS およびリダイレクト URL の属性と値のペア

スイッチはこれらの *cisco-av-pair* VSA を使用します。

- url-redirect は HTTP URL または HTTPS URL です。
- url-redirect-acl はスイッチ ACL 名または番号です。

スイッチは、CiscoSecure-defined-ACL 属性値ペアを使用して、エンドポイントからの HTTP または HTTPS リクエストを代行受信します。スイッチは、クライアント Web ブラウザを指定されたリダイレクト アドレスに転送します。Cisco Secure ACS 上の url-redirect AV ペアには、Web ブラウザがリダイレクトされる URL が格納されます。url-redirect-acl 属性値ペアには、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号が含まれます。

（注）
- ACL の permit ACE と一致するトラフィックがリダイレクトされます。
- url-redirect-acl の許可ルールに一致する ACE は、クライアントを url-redirect ページにリダイレクトします。拒否ルールが一致すると、クライアント トラフィックは許可されます。
- スイッチの URL リダイレクト ACL およびデフォルト ポート ACL を定義します。

リダイレクト URL が認証サーバのクライアントに設定される場合、接続されるクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

セキュリティ ACL/dACL とパント/リダイレクト ACL が一緒にセッションに適用されると、url-redirect-acl の優先度が高くなります。

リダイレクト ACL の使い方の詳細については、こちらのドキュメントを参照してください。

Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア

Cisco Secure ACS で、RADIUS cisco-av-pair ベンダー固有属性（VSA）を使用して、CiscoSecure-Defined-ACL 属性と値（AV）ペアを設定できます。このペアは、#ACL#-IP-name-number 属性を使って、Cisco Secure ACS でダウンロード可能な ACL の名前を指定します。

- *name* は ACL の名前です。
- *number* はバージョン番号（たとえば 3f783768）です。

ダウンロード可能な ACL が認証サーバのクライアントに設定される場合、接続されるクライアント スイッチ ポートのデフォルト ポート ACL も設定する必要があります。

デフォルト ACL がスイッチで設定されている場合、Cisco Secure ACS がホスト アクセス ポリシーをスイッチに送信すると、スイッチは、スイッチ ポートに接続されるホストからのトラフィックにこのポリシーを適用します。ポリシーが適用されない場合、デフォルト ACL が適用されます。Cisco Secure ACS がダウンロード可能な ACL をスイッチに送信する場合、この ACL は、スイッチ ポートに設定されているデフォルト ACL より優先されます。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信し、デフォルト ACL が設定されていない場合、許可失敗が宣言されます。

VLAN ID ベース MAC 認証

ダウンロード可能な VLAN ではなくスタティック VLAN ID に基づいてホストを認証する場合、VLAN ID ベース MAC 認証を使用できます。スタティック VLAN ポリシーがスイッチで設定されている場合、認証用の各ホストの MAC アドレスとともに、VLAN 情報が IAS（Microsoft）RADIUS サーバに送信されます。接続ポートに設定されている VLAN ID は MAC 認証に使用されます。VLAN ID ベース MAC 認証を IAS サーバで使用することで、ネットワークで一定数の VLAN を使用できます。

機能は、STP によってモニタおよび処理される VLAN の数も制限します。ネットワークは固定 VLAN として管理できます。

（注） この機能は Cisco ACS Server ではサポートされていません（ACS サーバは、新しいホストに送信される VLAN-ID を無視して、MAC アドレスに基づいた認証だけを行います）。

ゲスト VLAN を使用した 802.1x 認証

スイッチ上の各 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます（802.1x クライアントのダウンロードなど）。これらのクライアントは 802.1x 認証用にシステムをアップグレードできる場合がありますが、一部のホスト（Windows 98 システムなど）は IEEE 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチはEAPOLパケット履歴を保持します。EAPOLパケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが IEEE 802.1x 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

スイッチが 802.1x 対応の音声デバイスを許可しようとしたが、AAA サーバが使用できない場合、許可は失敗します。ただし、EAPOLパケットの検出はEAPOL履歴に保存されます。この音声デバイスは、AAA サーバが使用可能になると許可されます。ただし、他のデバイスによるゲスト VLAN へのアクセスは許可されなくなります。この状況を防ぐには、次のいずれかのコマンド シーケンスを使用します。

- **authentication event no-response action authorize vlan** *vlan-id* インターフェイス コンフィギュレーション コマンドを入力し、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。

（注） インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1x 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに 802.1x 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、単一のホスト、複数のホスト、複数認証、またはマルチドメイン モードにおける 802.1x ポートでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

スイッチは*MAC*認証バイパスをサポートします。MAC 認証バイパスが 802.1x ポートでイネーブルの場合、スイッチは、IEEE 802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。スイッチは、802.1x ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチ

はクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。

制限付き VLAN を使用した 802.1x 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチ スタックまたはスイッチの各 IEEE 802.1x ポートに対して制限付き VLAN（認証失敗 *VLAN* と呼ばれることもあります）を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1x 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効なクレデンシャルを持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。

（注） 両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチポートがスパニングツリーのブロッキング ステートから変わることができなくなります。制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。VLAN 内のポートは設定された間隔に従って再認証を試みます（デフォルトは 60 秒）。再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルにすることもできますが、ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しない限り、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の疑似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントによっては（Windows XP が稼働しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、すべてのホスト モードでの 802.1x ポート上、およびレイヤ 2 ポート上でサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

ダイナミック ARP インスペクション、DHCP スヌーピング、IP 送信元ガードなどの他のセキュリティ ポート機能は、制限付き VLAN に対して個別に設定できます。

アクセス不能認証バイパスを使用した 802.1x 認証

スイッチが設定された RADIUS サーバに到達できず、新しいホストを認証できない場合、アクセス不能認証バイパス機能を使用します。この機能は、クリティカル認証または *AAA* 失敗ポリシーとも呼ばれます。これらのホストをクリティカルポートに接続するようにスイッチを設定できます。

新しいホストがクリティカルポートに接続しようとすると、そのホストはユーザ指定のアクセス VLAN、クリティカル *VLAN* に移動されます。管理者はこれらのホストに制限付き認証を付与します。

スイッチは、クリティカルポートに接続されているホストを認証しようとする場合、設定されている RADIUS サーバのステータスをチェックします。利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワーク アクセスを許可して、ポートを認証ステートの特別なケースであるクリティカル認証ステートにします。

（注） クリティカル認証をインターフェイスで設定する場合は、クリティカル承認（クリティカル *vlan*）に使用する vlan をスイッチでアクティブにする必要があります。クリティカル *vlan* が非アクティブまたはダウンしていると、クリティカル認証セッションは非アクティブな vlan の有効化を試行し続け、繰り返し失敗します。これは大量のメモリ保持の原因となる可能性があります。

複数認証ポートのアクセス不能認証バイパスのサポート

ポートが任意のホスト モードで設定されていて、AAA サーバを使用できない場合、ポートはマルチホストモードに設定され、クリティカル VLAN に移動されます。マルチ認証（multiauth）ポートで、このアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan** *vlan-id* コマンドを使用します。新しいホストがクリティカル ポートに接続しようとすると、そのポートは再初期化され、接続されているすべてのホストがユーザ指定のアクセス VLAN に移動されます。

このコマンドは、すべてのホスト モードでサポートされます。

アクセス不能認証バイパスの認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカルポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカルポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイム アウトとなり、スイッチは次の認証試行の間にクリティカルポートをクリティカル認証ステートとします。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、クリティカル VLAN から移動するように、クリティカルポートを設定できます。このように設定した場合、クリティカル認証ステートのすべてのクリティカル ポートは自動的に再認証されます。

アクセス不能認証バイパス機能の相互作用

アクセス不能認証バイパスは、次の機能と相互に作用します。

- ゲスト VLAN：アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 8021.x ポートでイネーブルの場合、この機能は次のように相互に作用します。
  - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカルポートを RADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- 制限付き VLAN：ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- 802.1x アカウンティング：RADIUS サーバが使用できない場合、アカウンティングは影響を受けません。
- プライベート VLAN：プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。

- 音声VLAN：アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer（RSPAN）：アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

スイッチ スタックで、次の動作が発生します。

- キープアライブ パケットを送信することによって、スタック マスターにより、RADIUS サーバのステータスがチェックされます。RADIUS サーバのステータスが変更されると、スタック マスターからスタック メンバへ、情報が送信されます。クリティカル ポートの再認証時に、スタック メンバにより、RADIUS サーバのステータスがチェックされます。
- 新しいスタック マスターが選択されると、スイッチ スタックと RADIUS サーバとの間のリンクが変更される可能性があり、新しいスタックにより、キープアライブ パケットがただちに送信され、RADIUS サーバのステータスがアップデートされます。サーバのステータスが *dead* から *alive* に変化すると、スイッチはクリティカル認証ステートの状態にあるすべてのスイッチ ポートを再認証します。

メンバがスタックに追加されると、スタック マスターからメンバへサーバ ステータスが送信されます。

（注） スイッチ スタックは、LAN Base イメージを実行している Catalyst 2960-S スイッチだけでサポートされています。

802.1x クリティカル音声 VLAN

ポートに接続されている IP Phone がアクセス コントロール サーバ（ACS）によって認証される際、電話機は音声ドメインに参加します。ACS が到達不能である場合、スイッチはデバイスが音声デバイスなのかどうかを判断できません。サーバが使用できない場合、電話機は音声ネットワークにアクセスできないため、動作できません。

データ トラフィックの場合、アクセス不能認証バイパス（クリティカル認証）を設定し、サーバが使用できない場合にトラフィックがネイティブ VLAN を通過できるようにすることができます。RADIUS 認証サーバが使用できず（ダウンしていて）、アクセスできない認証バイパスがイネーブルの場合、スイッチは、クライアントにネットワークのアクセスを許可し、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN でポートをクリティカル認証ステートにします。設定された RADIUS サーバにスイッチが到達できず、新しいホストを認証できない場合、スイッチはこれらのホストをクリティカル ポートに接続します。クリティカル ポートに接続を試行している新しいホストは、ユーザ指定のアクセス VLAN（クリティカル VLAN）に移動され、制限付き認証を許可されます。

authentication event server dead action authorize voice インターフェイス コンフィギュレーション コマンドを使用して、クリティカル音声 VLAN 機能を設定できます。ACS が応答しない場合、ポートはクリティカル認証モードになります。ホストからのトラフィックが音声 VLAN

でタグ付けされると、接続デバイス（電話機）は、ポートに対して設定された音声 VLAN に配置されます。IP Phone は CDP（シスコ デバイス）や LLDP または DHCP を介して音声 VLAN ID を学習します。

switchport voice vlan *vlan-id* インターフェイス コンフィギュレーション コマンドを入力して、ポートの音声 VLAN を設定できます。

この機能は、マルチドメイン モードおよびマルチ認証ホスト モードでサポートされます。スイッチがシングルホスト モードまたはマルチホスト モードの場合にコマンドを入力できますが、デバイスがマルチドメインまたはマルチ認証ホストモードに変わらない限りコマンドは有効になりません。

802.1x ユーザ ディストリビューション

802.1x ユーザ ディストリビューションを設定すると、複数の異なる VLAN で同じグループ名のユーザのロード バランシングを行うことができます。

VLAN は、RADIUS サーバにより提供されるか、VLAN グループ名でスイッチ CLI を介して設定します。

- RADIUS サーバを設定して、ユーザの複数の VLAN 名を送信します。複数の VLAN 名は、ユーザへの応答の一部として送信できます。802.1x ユーザ ディストリビューションは、特定の VLAN のすべてのユーザを追跡し、許可されたユーザをユーザ数が最も少ない VLAN に移動することでロード バランシングを行います。
- RADIUS サーバを設定してユーザの VLAN グループ名を送信します。VLAN グループ名は、ユーザへの応答の一部として送信できます。スイッチ CLI を使用して設定した VLAN グループ名で、選択された VLAN グループ名を検索できます。VLAN グループ名が検出されると、この VLAN グループ名で対応する VLAN を検索して、ユーザ数が最も少ない VLAN が検出されます。ロード バランシングは、対応する許可済みユーザをその VLAN に移動することで行われます。

（注） RADIUS サーバは、VLAN-ID、VLAN 名または VLAN グループを任意に組み合わせて VLAN 情報を送信できます。

802.1x ユーザ ディストリビューションの設定時の注意事項

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされることを確認してください。
- 複数の VLAN を VLAN グループにマッピングできます。
- VLAN を追加または削除することで、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアする場合、VLAN の認証済みポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。

- アクティブ VLAN がグループにマッピングされても VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内で任意の VLAN の認証ステートであるポートまたはユーザはクリアされませんが、VLAN の VLAN グループへのマッピングはクリアされます。

音声 VLAN ポートを使用した IEEE 802.1x 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の 2 つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータ トラフィックを伝送する PVID。PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、IP Phone は IEEE 802.1x 認証とは独立して動作できます。

シングル ホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチ ホスト モードでは、サプリカントが PVID で認証された後、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチ ホスト モードがイネーブルの場合、サプリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで IEEE 802.1x 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

IEEE 802.1x 認証をスイッチ ポート上でイネーブルにすると、音声 VLAN でもあるアクセス ポート VLAN を設定できます。

IP 電話がシングル ホスト モードで 802.1x 対応のスイッチ ポートに接続されている場合、スイッチは認証を行わずに電話ネットワーク アクセスを承認します。ポートで Multidomain Authentication（MDA）を使用して、データ デバイスと IP フォンなどの音声デバイスの両方を認証することを推奨します。

（注） 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

ポート セキュリティを使用した IEEE 802.1x 認証

通常、IEEE 802.1x がイネーブルの場合に、ポート セキュリティをイネーブルにすることは推奨されません。IEEE 802.1x ではポート単位（IP テレフォニーに MDA が設定されている場合は VLAN 単位）で単一の MAC アドレスが適用されるため、ポート セキュリティは冗長であり、場合によっては期待される IEEE 802.1x の動作と干渉することがあります。

WoL 機能を使用した IEEE 802.1x 認証

IEEE 802.1x 認証の Wake-on-LAN（WoL）機能を使用すると、スイッチにマジック パケットと呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが IEEE 802.1x ポートを通じて接続され、ホストの電源がオフになると、IEEE 802.1x ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした IEEE 802.1x 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の IEEE 802.1x ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。

（注） PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

authentication control-direction in インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向に設定すると、そのポートはスパニングツリーフォワーディング ステートに変わります。ポートは、ホストにパケットを送信できますが、受信はできません。

authentication control-direction both インターフェイス コンフィギュレーション コマンドを使用してポートを双方向に設定すると、そのポートのアクセスが双方向で制御されます。ポートは、ホストとの間でパケットを送受信しません。

MAC 認証バイパスを使用した IEEE 802.1x 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレスに基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された IEEE 802.1x ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が IEEE 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可され

たクライアントMACアドレスのデータベースがあります。スイッチは、IEEE 802.1xポート上のクライアントを検出した後で、クライアントからのイーサネットパケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲストVLANが設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。このプロセスは、ほとんどのクライアントデバイスで動作します。ただし、代替のMACアドレス形式を使用しているクライアントでは動作しません。標準の形式とは異なる MAC アドレスを持つクライアントに対して MAB 認証をどのように実行するかや、RADIUSの設定のどこでユーザ名とパスワードが異なることが要求されるかを設定できます。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが802.1x対応サプリカントであることを確認し、（MAC 認証バイパス機能ではなく）802.1x 認証を使用してインターフェイスを認証します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでにMAC認証バイパスを使用してポートを許可し、IEEE 802.1xサプリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生するときに、Termination-Action RADIUS 属性値が DEFAULT であるために前のセッションが終了した場合、スイッチはポートに設定されている認証または再認証手法を使用します。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、IEEE 802.1x を使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てられた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS 属性（Attribute[27]）、および Termination-Action RADIUS 属性（Attribute[29]）に基づいて行われるときに、Termination-Action RADIUS 属性（Attribute[29]）のアクションが *Initialize*（属性値は *DEFAULT*）である場合、MAC 認証バイパス セッションは終了し、再認証の間の接続は失われます。MAC 認証バイパス機能が IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。これらの AV ペアの詳細については、RFC 3580『IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- IEEE 802.1x 認証：802.1x 認証がポートでイネーブルの場合にのみ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：IEEE 802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ
- 音声 VLAN

- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。
- Network Edge Access Topology（NEAT）：MAB と NEAT は相互に排他的です。インターフェイス上で NEAT がイネーブルの場合は、MAB をイネーブルにできません。また、インターフェイス上で MAB がイネーブルの場合は、NEAT をイネーブルにできません。

Cisco IOS Release 12.2(55)SE 以降では、冗長 MAB システム メッセージのフィルタリングをサポートします。

Network Admission Control レイヤ 2 IEEE 802.1x 検証

スイッチは、デバイスのネットワーク アクセスを許可する前にエンドポイント システムやクライアントのウイルス対策の状態またはポスチャを調べる Network Admission Control（NAC）レイヤ 2 IEEE 802.1x 検証をサポートしています。NAC レイヤ 2 IEEE 802.1x 検証を使用すると、以下の作業を実行できます。

- Session-Timeout RADIUS 属性（属性 [27]）と Termination-Action RADIUS 属性（属性 [29]）を認証サーバからダウンロードします。
- Session-Timeout RADIUS 属性（属性 [27]）の値として再認証試行間の秒数を指定し、RADIUS サーバからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS 属性（属性[29]）を使用してクライアントを再認証する際のアクションを設定します。値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- VLAN の番号や名前、または VLAN グループ名のリストを Tunnel Group Private ID（属性 [81]）の値として設定し、VLAN の番号や名前、または VLAN グループ名のプリファレンスを Tunnel Preference（属性 [83]）の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID（属性 [81]）属性がリストから選択されます。
- **show authentication** 特権 EXEC コマンドを使用して、クライアントのポスチャを表示する NAC ポスチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 IEEE 802.1x 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があることを除いて、IEEE 802.1x ポートベース認証と似ています。

柔軟な認証の順序設定

柔軟な認証の順序設定を使用して、ポートが新しいホストを認証するときに使用する方法の順序を設定できます。The IEEE 802.1X の柔軟な認証機能では、以下の 3 つの認証方法をサポートしています。

- dot1X：IEEE 802.1X 認証はレイヤ 2 の認証方式です。
- mab：MAC 認証バイパスはレイヤ 2 の認証方式です。

- webauth：Web 認証はレイヤ 3 の認証方式です。

この機能を使用すると、各ポートでどの認証方式を使用するかを制御できます。また、そのポートの方式についてフェールオーバー順も制御できます。たとえば、MAC 認証バイパスおよび 802.1x は、プライマリまたはセカンダリ認証方法として使用し、Web 認証は、これらの認証のいずれか、または両方が失敗した場合のフォールバック方法として使用できます。

The IEEE 802.1X の柔軟な認証機能では、以下のホスト モードをサポートしています。

- multi-auth：マルチ認証では、音声 VLAN に 1 つの認証、データ VLAN に複数の認証を使用できます。
- multi-domain：マルチドメイン認証では、音声 VLAN に 1 つ、データ VLAN に 1 つ、計 2 つの認証を使用できます。

関連トピック

柔軟な認証順序の設定 （2424 ページ）

Open1x 認証

Open1x 認証によって、デバイスが認証される前に、そのデバイスがポートにアクセスできるようになります。オープン認証が設定されている場合、新しいホストはポートに定義されているアクセス コントロール リスト（ACL）に基づいてトラフィックを渡します。ホストが認証されると、RADIUS サーバに設定されているポリシーがそのホストに適用されます。

オープン認証を次の状況で設定できます。

- シングル ホスト モードでのオープン認証：1 人のユーザだけが認証の前後にネットワークにアクセスできます。
- MDA モードでのオープン認証：音声ドメインの 1 人のユーザだけ、およびデータ ドメインの 1 人のユーザだけが許可されます。
- マルチ ホスト モードでのオープン認証：任意のホストがネットワークにアクセスできます。
- 複数認証モードでのオープン認証：MDA の場合と似ていますが、複数のホストを認証できます。

（注） オープン認証が設定されている場合は、他の認証制御よりも優先されます。これは、**authentication open** インターフェイス コンフィギュレーション コマンドを使用した場合、**authentication port-control** インターフェイス コンフィギュレーション コマンドに関係なく、ポートがホストにアクセス権を付与することを意味します。

関連トピック

Open1x の設定 （2425 ページ）

マルチドメイン認証

スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチ ポート上で認証できます。ポートはデータ ドメインと音声ドメインに分割されます。

（注） すべてのホスト モードで、ポートベース認証が設定されている場合、ライン プロトコルは許可の前にアップのままです。

MDA では、デバイス認証の順序が指定されません。ただし、最適な結果を得るには、MDA 対応のポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA のスイッチ ポートを設定する必要があります。
- ホスト モードがマルチドメインに設定されている場合、IP Phone の音声 VLAN を設定する必要があります。
- MDA 対応ポートでの音声 VLAN 割り当ては、Cisco IOS Release 12.2(40)SE 以降でサポートされています。
- 音声デバイスを認可するには、値を *device-traffic-class=voice* に設定した Cisco 属性値（AV）ペア属性を送信するように AAA サーバを設定する必要があります。この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応のポートのデータ デバイスだけに適用されます。許可に失敗した音声デバイスは、データ デバイスとして扱われます。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、errordisable になります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。他社製 IP Phone または音声デバイスはデータおよび音声 VLAN の両方に許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。音声デバイスが 音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポート セキュリティ MAC アドレス制限にカウントされません。
- MDA では、IEEE 802.1x 認証をサポートしていないデバイスへのスイッチ ポートの接続を許可するフォールバック メカニズムとして、MAC 認証バイパスを使用できます。

- データまたは音声デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスがデータ VLAN で検出された場合や、複数の音声デバイスが音声 VLAN で検出された場合、ポートは errdisable になります。
- ポートのホスト モードをシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変更すると、ポートでは許可されたデータ デバイスは許可されたままになります。ただし、ポートの音声 VLAN で許可されている Cisco IP Phone は自動的に削除されるので、そのポートでは再認証を行う必要があります。
- ゲスト VLAN や制限付き VLAN などのアクティブ フォールバック メカニズムは、ポートをシングル モードまたはマルチホスト モードからマルチドメイン モードに変更したあとでも設定されたままになります。
- ポートのホスト モードをマルチドメイン モードからシングル モードまたはマルチホスト モードに変更すると、許可されているすべてのデバイスがポートから削除されます。
- まずデータ ドメインを許可してゲスト VLAN に参加させる場合、IEEE 802.1x 非対応の音声デバイスは、音声 VLAN のパケットをタグ付けして、認証を開始する必要があります。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーを備えた、許可されたデバイスは、ポートの音声 VLAN とデータ VLAN の両方のトラフィックに影響を与えることがあります。このようなデバイスを使用する場合は、ポートでユーザ単位 ACL を適用するデバイスは 1 台だけにしてください。

Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ

Network Edge Access Topology（NEAT）機能は、ワイヤリング クローゼット（会議室など）外の領域まで識別を拡張します。これにより、任意のタイプのデバイスをポートで認証できます。

- 802.1x スイッチ サプリカント：802.1x サプリカント機能を使用することで、別のスイッチのサプリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼット外にあり、トランク ポートを介してアップストリーム スイッチに接続される場合に役に立ちます。802.1x スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチで認証します。サプリカント スイッチが認証に成功すると、オーセンティケータ スイッチでポート モードがアクセスからトランクに変更されます。サプリカント スイッチでは、CISP を有効にするときに手動でトランクを設定する必要があります。
- アクセス VLAN は、オーセンティケータ スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

デフォルトでは、BPDU ガードが有効にされたオーセンティケータ スイッチにサプリカントのスイッチを接続する場合、オーセンティケータのポートはサプリカント スイッチが認証する前にスパニングツリー プロトコル（STP）のブリッジ プロトコル データ ユニット（BPDU）を受信した場合、errdisable 状態になる可能性があります。Cisco IOS Release 15.0(1) SE 以降では、認証中にサプリカントのポートから送信されるトラフィックを制御できます。**dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証が完了する前にオーセンティケータ ポートがシャットダウンすることがないように、認証中に一時的にサプリカントのポートをブロックします。認証に失敗すると、サプリカントのポートが開きます。**no dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証期間中にサプリカント ポートが開きます。これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドによりオーセンティケータのスイッチ ポートで有効になっている場合、サプリカント スイッチで **dot1x supplicant controlled transient** コマンドを使用することを強く推奨します。

（注） **spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用して、グローバルにオーセンティケータ スイッチで BPDU ガードを有効にした場合、**dot1x supplicant controlled transient** コマンドを入力すると、BPDU の違反が避けられなくなります。

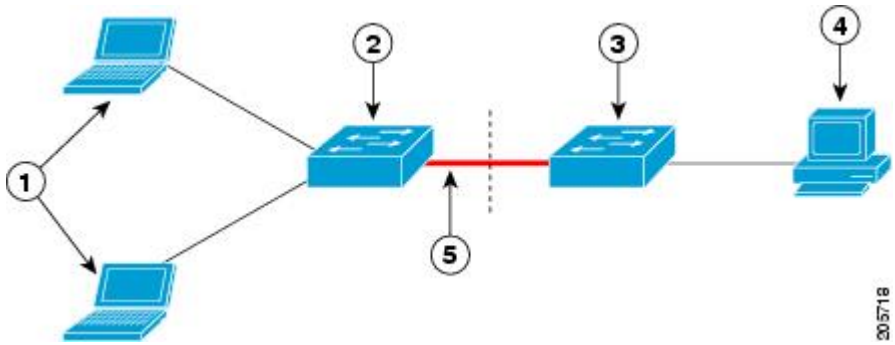
1 つ以上のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで MDA または multiauth モードをイネーブルにできます。マルチホスト モードはオーセンティケータ スイッチ インターフェイスではサポートされていません。

インターフェイスで有効になっているシングルホスト モードでオーセンティケータ スイッチをリブートすると、インターフェイスが認証前に err-disabled 状態に移行する場合があります。err-disabled 状態から回復するには、オーセンティケータ ポートをフラップしてインターフェイスを再度アクティブにし、認証を開始します。

すべてのホスト モードで機能するように **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを Network Edge Access Topology（NEAT）のサプリカント スイッチで使用します。

- ホスト許可：許可済み（サプリカントでスイッチに接続する）ホストからのトラフィックだけがネットワークで許可されます。これらのスイッチは、Client Information Signalling Protocol（CISP）を使用して、サプリカント スイッチに接続する MAC アドレスをオーセンティケータ スイッチに送信します。
- 自動有効化：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的に有効化します。これにより、サプリカント スイッチから着信する複数の VLAN のユーザ トラフィックが許可されます。ACS で cisco-av-pair を *device-traffic-class=switch* として設定します（この設定は *group* または *user* 設定で行うことができます）。

図 *130 : CISP* を使用したオーセンティケータまたはサプリカント スイッチ



1	ワークステーション（クライアント）	2	サプリカント スイッチ（ワイヤリング クローゼット外）
3	オーセンティケータ スイッチ	4	Access Control Server（ACS）
5	トランク ポート		

（注） **switchport nonegotiate** コマンドは、NEAT を使用したサプリカントおよびオーセンティケータ スイッチではサポートされません。このコマンドは、トポロジのサプリカント側で設定しないでください。オーセンティケータ サーバ側で設定した場合は、内部マクロによってポートからこのコマンドが自動的に削除されます。

音声認識 802.1x セキュリティ

（注） 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにするようにスイッチを設定します。以前のリリースでは、セキュリティ違反の原因であるデータ クライアントを認証しようとすると、ポート全体がシャットダウンし、接続が完全に切断されます。

この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

関連トピック

音声認識 802.1x セキュリティの設定 （2382 ページ）

コモン セッション ID

認証マネージャは、使用された認証方式が何であれ、クライアントの単一のセッションID（共通セッションID）を使用します。このIDは、表示コマンドやMIBなどのすべてのレポートに使用されます。セッション ID は、セッション単位のすべての Syslog メッセージに表示されます。

セッション ID には、次の情報が含まれます。

- ネットワーク アクセス デバイス（NAD）の IP アドレス
- 一意の 32 ビット整数（機械的に増加します）
- セッション開始タイム スタンプ（32 ビット整数）

次に、show authentication コマンドの出力に表示されたセッション ID の例を示します。この例では、セッション ID は 160000050000000B288508E5 です。

```
Device# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

次に、Syslog 出力にセッション ID が表示される例を示します。この例でも、セッション ID は 160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

セッションIDは、NAD、AAAサーバ、その他のレポート分析アプリケーションでクライアントを識別するために使用されます。ID は自動的に表示されます。設定は必要ありません。

802.1x ポートベース認証の設定方法

802.1x 認証のデフォルト設定

表 *150 : 802.1x* 認証のデフォルト設定

機能	デフォルト設定
スイッチの 802.1x イネーブル ステート	ディセーブル

機能	デフォルト設定
ポート単位の 802.1x イネーブル ステート	ディセーブル（force-authorized） ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • デフォルトのアカウンティング ポート • Key	• 指定なし • 1645 • 1646 • 指定なし
ホスト モード	シングル ホスト モード
制御方向	双方向制御
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
再認証回数	2回（ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数）
待機時間	60 秒（スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数）
再送信時間	30 秒（スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数）
最大再送信回数	2 回（スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数）
クライアント タイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間）

機能	デフォルト設定
認証サーバ タイムアウト時間	30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間） dot1x timeout server-timeout インターフェイス コンフィギュレーション コマンドを使用して、このタイムアウト時間を変更できます。
無活動タイムアウト	ディセーブル
ゲスト VLAN	指定なし
アクセス不能認証バイパス	ディセーブル
制限付き VLAN	指定なし
オーセンティケータ（スイッチ）モード	指定なし
MAC 認証バイパス	ディセーブル
音声認識セキュリティ	ディセーブル

802.1x 認証設定時の注意事項

802.1X 認証

802.1x 認証を設定する場合の注意事項は、次のとおりです。

- 802.1x 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当ててられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

  802.1x ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除された後、ポートは無許可になります。
- 802.1x プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポート タイプではサポートされません。
  - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブ

ルになりません。802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。

- EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x 認証をイネーブルにしようとすると、エラーメッセージが表示され、802.1x 認証はイネーブルになりません。
- スイッチド ポート アナライザ（SPAN）およびリモート SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートの 802.1x 認証をイネーブルにすることができます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1x 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは 802.1x 認証をイネーブルにすることができます。

- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x 認証をグローバルにイネーブルにする前に、802.1x 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- Cisco IOS Release 12.2(55)SE 以降のリリースでは、802.1x 認証に関連するシステム メッセージのフィルタリングがサポートされています。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、およびアクセス不能認証バイパス設定時の注意事項は、次のとおりです。

- 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。
- DHCP クライアントが接続されている 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1x 認証プロセスを再起動する設定を変更できます。802.1x 認証プロセスの設定を軽減します（**authentication timer inactivity** および **authentication timer reauthentication** インターフェイス コンフィギュレーション コマンド）。設定の減少量は、接続された 802.1x クライアントのタイプによって異なります。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
  - この機能はシングル ホスト モードおよびマルチホスト モードの 802.1x ポートでサポートされます。

- Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステートの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
- Windows XP クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。
- アクセス不能認証バイパス機能および制限 VLAN を 802.1x ポート上に設定できます。スイッチが制限付き VLAN 内でクリティカル ポートを再認証しようとし、すべての RADIUS サーバが利用不可能な場合、スイッチはポート ステートをクリティカル認証ステートに変更し、制限付き VLAN に残ります。
- CTS リンクがクリティカル認証モードである場合にマスターがリロードすると、SGT をデバイスに設定したポリシーは新しいマスターでは使用できません。これは、内部バインドが 3750-X スイッチ スタックのスタンバイ スイッチと同期しないためです。

- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。
- ワイヤレス ゲスト クライアントが固定クライアント VLAN の代わりに外部クライアント VLAN から IP を取得する際には、クライアントに新しい DHCP 要求を発行するために、WLAN 設定で **ip dhcp required** コマンドを使用する必要があります。これは、クライアントがアンカーで正しくない IP を取得することを防止します。
- Cisco WLC（外部の）のリロード後に、有線ゲスト クライアントが IP アドレスの取得に失敗した場合は、クライアントによって使用されているポートで shut/no shut を実行して再接続します。

MAC 認証バイパス

MAC 認証バイパス設定時の注意事項は次のとおりです。

- 特に明記していないかぎり、MAC 認証バイパスの注意事項は 802.1x 認証のものと同じです。
- ポートが MAC アドレスで許可された後に、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバ データベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。
- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を設定できます。指定できる範囲は 1 ～ 65535 秒です。

ポートあたりのデバイスの最大数

802.1x 対応のポートに接続できるデバイスの最大数です。

- シングル ホスト モードの場合、アクセス VLAN で接続できるデバイスは 1 台だけです。ポートが音声 VLAN でも設定されている場合、音声 VLAN を介して送受信できる Cisco IP Phone の数には制限はありません。
- マルチドメイン認証（MDA）モードの場合、アクセス VLAN で 1 台のデバイス、音声 VLAN で 1 台の IP Phone が許可されます。
- マルチホスト モードでは、1 つの 802.1x サプリカントだけがポートで許可されますが、非 802.1x ホストは数に制限なく、アクセス VLAN で許可されます。音声 VLAN で許可されるデバイスの数には制限はありません。

802.1x 準備状態チェックの設定

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。

802.1x 準備状態チェックは、802.1x で設定できるすべてのポートで使用できます。準備状態チェックは、**dot1x force-unauthorized** として設定されるポートでは使用できません。

802.1x 準備状態チェックをスイッチでイネーブルにする場合には、次の手順に従ってください。

始める前に

準備状態チェックをスイッチでイネーブルにする場合、次の注意事項に従ってください。

- 準備状態チェックは通常、802.1x がスイッチでイネーブルにされる前に使用されます。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用すると、スイッチ スタックのすべてのポートがテストされます。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x 対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。Syslog メッセージは生成されません。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x 対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。Syslog メッセージは生成されません。

- 準備状態チェックは、複数のホスト（たとえば、IP Phone に接続される PC）を扱うポートに送信できます。Syslog メッセージは、タイマー時間内に準備状態チェックに応答する各クライアントに生成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**dot1x test eapol-capable** [**interface** *interface-id*]
	例：
	`Device# dot1x test eapol-capable interface gigabitethernet1/0/13`
	`DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable`
		スイッチ上で 802.1x 準備状態チェックをイネーブルにします。
		（任意）*interface-id* では、IEEE 802.1x の準備状態をチェックするポートを指定します。
		（注） オプションの **interface** キーワードを省略した場合、スイッチのすべてのインターフェイスがテストされます。

ステップ 4	**dot1x test timeout** *timeout*	（任意）EAPOL 応答の待機に使用するタイムアウトを設定します。範囲は1～65535秒です。デフォルトは10秒です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

802.1x 準備状態チェック （2352 ページ）

音声認識 802.1x セキュリティの設定

（注） 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能をスイッチで使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにします。この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

スイッチで音声認識 802.1x 音声セキュリティを設定する場合、次の注意事項に従ってください。

- **errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力して、音声認識 802.1x セキュリティをイネーブルにします。音声認識 802.1x セキュリティをディセーブルにするには、このコマンドの **no** バージョンを入力します。このコマンドは、スイッチの 802.1x 設定ポートのすべてに適用されます。

  （注） **shutdown vlan** キーワードを指定しない場合、error-disabled ステートになったときにポート全体がシャットダウンされます。

- **errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して、error-disabled リカバリを設定すると、ポートは自動的に再びイネーブルにされます。error-disabled リカバリがポートで設定されていない場合、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。

- 個々の VLAN を再びイネーブルにするには、**clear errdisable interface** *interface-id* **vlan** [*vlan-list*] 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルにされます。

音声認識 802.1x セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**errdisable detect cause security-violation shutdown vlan**	セキュリティ違反エラーが発生したすべての VLAN をシャットダウンします。 （注） **shutdown vlan** キーワードを指定しない場合、すべてのポートが errdisable ステートになり、シャットダウンされます。
ステップ 3	**errdisable recovery cause security-violation**	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**clear errdisable interface***interface-id* **vlan** *[vlan-list]*	（任意）errordisableになっている個々の VLAN を再びイネーブルにします。 • interface-id の場合、個々の VLAN を再びイネーブルにするポートを指定します。 • （任意）vlan-list の場合、再びイネーブルにする VLAN のリストを指定します。vlan-list を指定しない場合は、すべての VLAN が再びイネーブルになります。
ステップ 5	次を入力します。 • **shutdown** • **no shutdown**	（任意）errordisable の VLAN を再びイネーブルにして、すべての errordisable 指示をクリアします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show errdisable detect**	入力内容を確認します。

例

次に、セキュリティ違反エラーが発生した任意の VLAN をシャットダウンするようにスイッチを設定する例を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次に、ポート ギガビット イーサネット 40/2 で errdisable ステートであったすべての VLAN を再度イネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet4/0/2
vlan
```

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

関連トピック

音声認識 802.1x セキュリティ （2374 ページ）

802.1x 違反モードの設定

次に示す状況で、シャットダウン、Syslogエラーを生成、または新しいデバイスからのパケットを廃棄するように 802.1x ポートを設定できます。

- デバイスが 802.1x 対応のポートに接続した
- ポートで認証されるデバイスの最大数に達した

スイッチ上にセキュリティ違反アクションを設定するには、特権EXECモードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1* 例： `Device(config)# aaa authentication dot1x default group radius`	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。

	コマンドまたはアクション	目的
		method1 には、**group radius** キーワードを入力して、認証用のすべてのRADIUSサーバ リストを使用できるようにします。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/4`	IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access** 例： `Device(config-if)# switchport mode access`	ポートをアクセスモードに設定します。
ステップ 6	**authentication violation** {**shutdown** | **restrict** | **protect** | **replace**} 例： `Device(config-if)# authentication violation restrict`	違反モードを設定します。キーワードの意味は次のとおりです。 • **shutdown**：エラーによってポートがディセーブルになります。 • **restrict**：Syslog エラーを生成します。 • **protect**：トラフィックをポートに送信するすべての新しいデバイスからパケットをドロップします。 • **replace**：現在のセッションを削除し、新しいホストで認証します。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

802.1X 認証の設定

ユーザ単位ACLまたはVLAN割り当てを可能にするには、AAA許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1x の AAA プロセスを示します。

始める前に

802.1x ポートベース認証を設定するには、認証、許可、アカウンティング（AAA）をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザがスイッチのポートに接続します。	
ステップ 2	認証が実行されます。	
ステップ 3	RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。	
ステップ 4	スイッチが開始メッセージをアカウンティング サーバに送信します。	
ステップ 5	必要に応じて、再認証が実行されます。	
ステップ 6	スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバに送信します。	
ステップ 7	ユーザがポートから切断します。	
ステップ 8	スイッチが停止メッセージをアカウンティング サーバに送信します。	

802.1x ポートベース認証の設定

802.1x ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**aaa authentication dot1x** {**default**} *method1* 例： `Device(config)# aaa authentication dot1x default group radius`	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。 （注） **group radius** キーワード以外にもコマンドラインのヘルプストリングに表示されますが、サポートされていません。
ステップ 4	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	スイッチで 802.1x 認証をグローバルに有効にします。
ステップ 5	**aaa authorization network** {**default**} **group radius** 例： `Device(config)# aaa authorization network default group radius`	（任意）ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。
ステップ 6	**radius server** *server name* 例： `Device(config)# radius server rsim address ipv4 124.2.2.12`	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 7	**key** *string* 例： `Device(config-radius-server)# key`	（任意）RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。

	コマンドまたはアクション	目的
	`rad123`	
ステップ 8	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	IEEE 802.1x 認証を有効にするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**switchport mode access** 例： `Device(config-if)# switchport mode access`	（任意）ステップ 6 および 7 で RADIUS サーバを設定した場合のみ、ポートをアクセス モードに設定します。
ステップ 10	**authentication port-control auto** 例： `Device(config-if)# authentication port-control auto`	ポートでの 802.1x 認証を有効にします。
ステップ 11	**dot1x pae authenticator** 例： `Device(config-if)# dot1x pae authenticator`	インターフェイスのポートアクセスエンティティを、オーセンティケータとしてのみ動作し、サプリカント用のメッセージは無視するように設定します。
ステップ 12	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

スイッチと RADIUS サーバ間の通信の設定

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

スイッチで RADIUS サーバのパラメータを設定するには、次の手順を実行します。この手順は必須です。

始める前に

認証、許可、およびアカウンティング（AAA）をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server** *server name* 例： `Device(config)# radius server rsim`	RADIUS サーバの名前を指定し、RADIUS サーバ コンフィギュレーション モードを開始します。
ステップ 4	**address** {**ipv4** | **ipv6**} *ip address* **auth-port** *port number* **acct-port** *port number* 例： `Device(config-radius-server)# address ipv4 124.2.2.12`	RADIUS サーバの IP アドレスを指定します。 **auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1645 です。指定できる範囲は 0 ～ 65536 です。 **acct-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1646 です。
ステップ 5	**key** *string* 例： `Device(config-radius-server)# key rad123`	Device と RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。

	コマンドまたはアクション	目的
		（注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に **radius server** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

スイッチと RADIUS サーバ間の通信 （2352 ページ）

ホスト モードの設定

authentication port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている IEEE 802.1x 許可ポート上で、複数のホスト（クライアント）を許可するには、特権EXECモードで次の手順を実行します。MDA を設定してイネーブルにするには、**multi-domain** キーワードを使用します。これにより、ホストデバイス、およびIP Phone（シスコ製または他社製）など音声デバイスの両方が同じスイッチ ポートで許可されます。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例：	複数ホストが間接的に接続されているポートを指定し、インターフェイス コ

	コマンドまたはアクション	目的
	`Device(config)# interface gigabitethernet2/0/1`	ンフィギュレーション モードを開始します。
ステップ 3	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] 例： `Device(config-if)# authentication host-mode multi-host`	単一の 802.1x 許可ポートで複数のホスト（クライアント）を許可することができます。 キーワードの意味は次のとおりです。 • **multi-auth**：音声 VLAN で 1 クライアント、データ VLAN で複数の認証クライアントを許可します。 （注） **multi-auth** キーワードを使用できるのは、**authentication host-mode** コマンドだけです。 • **multi-host**：シングル ホストの認証後に 802.1x 許可ポートで複数のホストの接続を許可します。 • **multi-domain**：ホスト デバイスと IP Phone（シスコ製または他社製）など音声デバイスの両方が、IEEE 802.1x 許可ポートで認証されるようにします。 （注） ホスト モードが **multi-domain** に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。 指定したインターフェイスで **authentication port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

定期的な再認証の設定

802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証を行う間隔（秒）を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication periodic** 例： `Device(config-if)# authentication periodic`	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。 （注） デフォルト値は3600秒です。再認証タイマーの値を変更するか、スイッチで RADIUS-provided セッション タイムアウトを使用するようにするには、**authentication timer reauthenticate** コマンドを入力します。
ステップ 4	**authentication timer** {{[**inactivity** | **reauthenticate** | **restart**]} {*value*}} 例： `Device(config-if)# authentication timer reauthenticate 180`	再認証の試行の間隔（秒）を設定します。 **authentication timer** キーワードの意味は次のとおりです。 • **inactivity**：クライアントからのアクティビティがなくなり無許可になるまでの間隔（秒単位） • **reauthenticate**：自動再認証試行が開始されるまでの時間（秒）

	コマンドまたはアクション	目的
		• **restart** *value*：無許可ポートの認証の試行が行われるまでの間隔（秒） このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。**authentication timer inactivity** インターフェイス コンフィギュレーション コマンドは、アイドル状態の期間を制御します。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、特権EXECモードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication timer inactivity** *seconds* 例： `Device(config-if)# authentication timer inactivity 30`	クライアントとの認証のやり取りに失敗した場合に、スイッチが待機状態のままでいる秒数を設定します。 指定できる範囲は1～65535秒です。デフォルトは60秒です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show authentication sessions interface** *interface-id* 例： `Device# show authentication sessions interface gigabitethernet2/0/1`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。スイッチがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、その後フレームを再送信します。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチがクライアントからの通知を待機する時間を変更するには、特権EXECモードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication timer reauthenticate** *seconds* 例： `Device(config-if)# authentication timer reauthenticate 60`	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 5 秒です。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show authentication sessions interface** *interface-id* 例： `Device# show authentication sessions interface gigabitethernet2/0/1`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチからクライアントへのフレーム再送信回数の設定

スイッチからクライアントへの再送信時間を変更できるだけでなく、（クライアントから応答が得られなかった場合に）スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチからクライアントへのフレーム再送信回数を設定するには、特権EXECモードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-req** *count* 例： `Device(config-if)# dot1x max-reauth-req 5`	スイッチが認証処理を再開するまでに、クライアントへEAP要求/アイデンティティ フレームを送信する回数を変更できます。指定できる範囲は1 ～ 10です。デフォルトは2です。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

再認証回数の設定

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： `Device(config-if)# switchport mode access`	RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**dot1x max-req** *count* 例： `Device(config-if)# dot1x max-req 4`	ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ～ 10 です。デフォルトは 2 です。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

MAC 移動のイネーブル化

MAC 移動を使用すると、認証されたホストをスイッチのポート間で移動できます。

スイッチで MAC 移動をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**authentication mac-move permit** 例： `Device(config)# authentication mac-move permit`	スイッチでMAC移動をイネーブルにします。デフォルトは deny です。 セッション認識型ネットワーク モードでは、デフォルト CLI は access-session mac-move deny です。セッション認識型ネットワークでMAC移動をイネーブルにするには、no access-session mac-move グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MAC 置換のイネーブル化

MAC 置換を使用すると、ホストはポート上の認証ホストを置換できます。

インターフェイス上で MAC 置換をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication violation** {**protect** | **replace** | **restrict** | **shutdown**} 例： `Device(config-if)# authentication violation replace`	インターフェイス上で MAC 置換をイネーブルにするには、**replace** キーワードを使用します。ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。 他のキーワードは、次のような機能があります。 • **protect**：ポートは、システム メッセージを生成せずに、予期しない MAC を使用するパケットをドロップします。 • **restrict**：違反パケットが CPU によってドロップされ、システムメッセージが生成されます。 • **shutdown**：ポートは、予期しない MAC アドレスを受信すると error disabled になります。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

802.1x アカウンティングの設定

802.1xアカウンティングを使用して、AAAシステムアカウンティングをイネーブルにすると、ロギングのためにシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバは、アクティブな 802.1x セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップ メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

（注） ロギングの開始、停止、仮のアップデート メッセージ、タイム スタンプなどのアカウンティング タスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになった後、802.1x アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`gigabitethernet1/0/3`	
ステップ 3	**aaa accounting dot1x default start-stop group radius** 例： `Device(config-if)# aaa accounting dot1x default start-stop group radius`	すべての RADIUS サーバのリストを使用して 802.1x アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting system default start-stop group radius** 例： `Device(config-if)# aaa accounting system default start-stop group radius`	（任意）システム アカウンティングをイネーブルにし（すべての RADIUS サーバのリストを使用）、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1x 対応でないクライアントはゲスト VLAN に配置されます。802.1x 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングル ホスト モードまたはマルチ ホスト モードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **switchport mode access** • **switchport mode private-vlan host** 例： `Device(config-if)# switchport mode private-vlan host`	• ポートをアクセス モードに設定します。 • レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication event no-response action authorize vlan** *vlan-id* 例： `Device(config-if)# authentication event no-response action authorize vlan 2`	アクティブ VLAN を 802.1x ゲスト VLANとして指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

制限付き VLAN の設定

スイッチ スタックまたはスイッチ上に制限付き VLAN を設定している場合、認証サーバが有効なユーザ名またはパスワードを受信できないと、IEEE 802.1x に準拠しているクライアントは制限付き VLAN に移されます。スイッチは、シングル ホスト モードでのみ制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **switchport mode access** • **switchport mode private-vlan host** 例： `Device(config-if)# switchport mode access`	• ポートをアクセス モードに設定します。 • レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** 例： `Device(config-if)# authentication port-control auto`	ポートでの 802.1x 認証をイネーブルにします。
ステップ 5	**authentication event fail action authorize vlan** *vlan-id* 例： `Device(config-if)# authentication event fail action authorize vlan 2`	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

制限付き VLAN の認証試行回数の設定

ユーザに制限付き VLAN を割り当てる前に、**authentication event retry** *retry count* インターフェイス コンフィギュレーション コマンドを使用して、認証試行回数を最大に設定できます。指定できる試行回数は 1 ～ 3 です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/3`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **switchport mode access** • **switchport mode private-vlan host** 例： または `Device(config-if)# switchport mode access`	• ポートをアクセス モードに設定します。 • レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** 例： `Device(config-if)# authentication port-control auto`	ポートでの 802.1x 認証をイネーブルにします。
ステップ 5	**authentication event fail action authorize vlan** *vlan-id* 例： `Device(config-if)# authentication event`	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN または音声 VLAN を除

	コマンドまたはアクション	目的
	`fail action authorize vlan 8`	き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。
ステップ 6	**authentication event retry** *retry count* 例： `Device(config-if)# authentication event retry 2`	ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は 1 ～ 3 秒です。デフォルトは 3 回に設定されています。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定

ポートにクリティカル音声 VLAN を設定し、アクセス不能認証バイパス機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	**radius-server dead-criteria** {**time** *seconds* } [**tries** *number*] 例： `Device(config)# radius-server dead-criteria time 20 tries 10`	RADIUS サーバが使用不可またはダウン（切断）と見なされる条件を設定します。 • **time**：1 ～ 120 秒。スイッチは、デフォルトの *seconds* 値を 10 ～ 60 の間で動的に決定します。

	コマンドまたはアクション	目的
		• **number**：1 ～ 100 の試行回数。スイッチは、デフォルトの **tries***number* を 10 ～ 100 の間で動的に決定します。
ステップ 4	**radius-serverdeadtime**分 例： `Device(config)# radius-server deadtime 60`	（任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分（24 時間）です。デフォルト値は 0 分です。
ステップ 5	**radius-server host ip-address** *address*[**acct-port** *udp-port*][**auth-port** *udp-port*] [**testusername** *name*[**idle-time** *time*] [**ignore-acct-port**][**ignore auth-port**]] [**key** *string*] 例： `Device(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username user1 idle-time 30 key abc1234`	（任意）次のキーワードを使用して RADIUS サーバ パラメータを設定します。 • **acct-port***udp-port*：RADIUS アカウンティング サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルトは 1646 です。 • **auth-port***udp-port*：RADIUS 認証サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルトは 1645 です。 （注） RADIUS アカウンティング サーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。 • **test username***name*：RADIUS サーバ ステータスの自動テストをイネーブルにして、使用するユーザ名を指定します。 • **idle-time** time：スイッチがテストパケットをサーバに送信した後の間隔を分数で設定します。範囲は 1 ～ 35791 分です。デフォルトは 60 分（1 時間）です。

	コマンドまたはアクション	目的
		• **ignore-acct-port**：RADIUS サーバアカウンティングポートのテストをディセーブルにします。 • **ignore-auth-port**：RADIUS サーバ認証ポートのテストをディセーブルにします。 • **key***string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号化キーに一致するテキストストリングでなければなりません。 （注） キーの先行スペースは無視されますが、途中および末尾のスペースは有効なので、キーは必ず **radius-server host** コマンド構文の最後の項目として設定してください。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 **radius-server key** {**0**string | **7***string* | *string*} グローバル コンフィギュレーション コマンドを使用しても認証および暗号キーを設定できます。
ステップ 6	**dot1x critical** {**eapol** | **recovery delay** *milliseconds*} 例： `Device(config)# dot1x critical eapol (config)# dot1x critical recovery delay 2000`	（任意）アクセス不能認証バイパスのパラメータを設定します。 • **eapol**：スイッチがクリティカルポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。

	コマンドまたはアクション	目的
		• **recovery delay***milliseconds*：使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカルポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルトは1000 ミリ秒です（ポートは毎秒再初期化できます）。
ステップ 7	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**authentication event server dead action** {**authorize** | **reinitialize**} **vlan** *vlan-id*] 例： `Device(config-if)# authentication event server dead action reinitialicze vlan 20`	これらのキーワードを使用して、RADIUS サーバが到達不能な場合にポートでホストを移動します。 • **authorize**：認証しようとする新しいホストをユーザ指定のクリティカル VLAN に移動します。 • **reinitialize**：ポートのすべての許可済みホストをユーザ指定のクリティカル VLAN に移動します。
ステップ 9	**switchport voice vlan** *vlan-id* 例： `Device(config-if)# switchport voice vlan`	ポートの音声 VLAN を指定します。音声 VLAN はステップ 6 で設定されたクリティカルデータ VLAN と同じにはできません。
ステップ 10	**authentication event server dead action authorize voice** 例： `Device(config-if)#  authentication event server dead action authorize voice`	RADIUS サーバが到達不能な場合、ポートのデータ トラフィックを音声 VLAN に移動するために、クリティカル音声 VLAN を設定します。
ステップ 11	**show authentication interface** *interface-id* 例：	（任意）設定を確認します。

	コマンドまたはアクション	目的
	`Device(config-if)# do show authentication interface gigabit 1/0/1`	
ステップ 12	**copy running-config startup-config** 例： `Device(config-if)# do copy running-config startup-config`	（任意）設定を確認します。

例

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server host** グローバル コンフィギュレーション コマンドを使用します。アクセス不能な認証バイパスをディセーブルにするには、**no authentication event server dead action** インターフェイス コンフィギュレーション コマンドを使用します。クリティカル音声 VLAN をディセーブルにするには、**authentication event server dead action authorize voice** インターフェイス コンフィギュレーション コマンドを使用します。

アクセス不能認証バイパスの設定例

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
Device(config)# radius-server dead-criteria time 30 tries 20
Device(config)# radius-server deadtime 60
Device(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username
user1 idle-time 30 key abc1234
Device(config)# dot1x critical eapol
Device(config)# dot1x critical recovery delay 2000
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# dot1x critical
Device(config-if)# dot1x critical recovery action reinitialize
Device(config-if)# dot1x critical vlan 20
Device(config-if)# end
```

WoL を使用した 802.1x 認証の設定

WoL を使用した 802.1x 認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/3`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication control-direction** {**both** | **in**} 例： `Device(config-if)# authentication control-direction both`	ポートで WoL を使用して 802.1x 認証をイネーブルにし、次のキーワードを使用してポートを双方向または単方向に設定します。 • **both**：ポートを双方向に設定します。ポートは、ホストにパケットを送受信できません。デフォルトでは、ポートは双方向です。 • **in**：ポートを単方向に設定します。ポートは、ホストにパケットを送信できますが、受信はできません。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show authentication sessions interface** *interface-id* 例： `Device# show authentication sessions interface gigabitethernet2/0/3`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication port-control auto** 例： `Device(config-if)# authentication port-control auto`	ポートでの 802.1x 認証をイネーブルにします。
ステップ 4	**mab** [**eap**] 例： `Device(config-if)# mab`	MAC 認証バイパスをイネーブルにします。 （任意）**eap** キーワードを使用して、スイッチが認可に EAP を使用するように設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

802.1x ユーザ ディストリビューションの設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan group** *vlan-group-name* **vlan-list** *vlan-list* 例： `Device(config)# vlan group eng-dept vlan-list 10`	VLAN グループを設定し、単一の VLAN または VLAN の範囲をそのグループにマッピングします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**no vlan group** *vlan-group-name* **vlan-list** *vlan-list* 例： `Device(config)# no vlan group eng-dept vlan-list 10`	VLAN グループ コンフィギュレーションまたは VLAN グループ コンフィギュレーションの要素をクリアします。

VLAN グループの設定例

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ コンフィギュレーションおよび指定 VLAN とのマッピングを確認する例を示します。

```
Device(config)# vlan group eng-dept vlan-list 10

Device(config)# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10

Device(config)# show dot1x vlan-group all
Group Name                      Vlans Mapped
```

```
-------------                    --------------
eng-dept                         10
hr-dept                          20
```

次に、VLAN を既存の VLAN グループに追加し、VLAN が追加されたことを確認する例を示します。

```
Device(config)# vlan group eng-dept vlan-list 30
Device(config)# show vlan group eng-dept
Group Name                       Vlans Mapped
-------------                    --------------
eng-dept                         10,30
```

次に、VLAN を VLAN グループから削除する例を示します。

```
Device# no vlan group eng-dept vlan-list 10
```

次に、すべての VLAN が VLAN グループからクリアされたときに、その VLAN グループもクリアされる例を示します。

```
Device(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

Device(config)# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループをクリアする方法を示します。

```
Device(config)# no vlan group end-dept vlan-list all
Device(config)# show vlan-group all
```

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

NAC レイヤ 2 802.1x 検証の設定

NAC レイヤ 2 802.1x 検証を設定できます。これは、RADIUS サーバを使用した 802.1x 認証とも呼ばれます。

NAC レイヤ 2 802.1x 検証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/3`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： `Device(config-if)# switchport mode access`	RADIUS サーバを設定した場合に限り、ポートをアクセスモードに設定します。
ステップ 4	**authentication event no-response action authorize vlan** *vlan-id* 例： `Device(config-if)# authentication event no-response action authorize vlan 8`	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。
ステップ 5	**authentication periodic** 例： `Device(config-if)# authentication periodic`	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。
ステップ 6	**authentication timer reauthenticate** 例： `Device(config-if)# authentication timer reauthenticate`	クライアントに対する再認証試行を設定します（1 時間に設定）。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show authentication sessions interface** *interface-id*	入力を確認します。

	コマンドまたはアクション	目的
	例： `Device# show authentication sessions interface gigabitethernet2/0/3`	
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

NEAT を使用したオーセンティケータ スイッチの設定

この機能を設定するには、ワイヤリング クローゼット外の 1 つのスイッチがサプリカントとして設定され、オーセンティケータ スイッチに接続されている必要があります。

（注） *cisco-av-pairs* は、ACS で *device-traffic-class=switch* として設定されている必要があります。これは、サプリカントが正常に認証された後でトランクとしてインターフェイスを設定します。

スイッチをオーセンティケータに設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable** 例： `Device(config)# cisp enable`	CISP をイネーブルにします。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**switchport mode access** 例： `Device(config-if)# switchport mode access`	ポート モードを **access** に設定します。
ステップ 5	**authentication port-control auto** 例： `Device(config-if)# authentication port-control auto`	ポート認証モードを auto に設定します。
ステップ 6	**dot1x pae authenticator** 例： `Device(config-if)# dot1x pae authenticator`	インターフェイスをポートアクセスエンティティ（PAE）オーセンティケータとして設定します。
ステップ 7	**spanning-tree portfast** 例： `Device(config-if)# spanning-tree portfast trunk`	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で Port Fast をイネーブルにします。
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet2/0/1`	設定を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

NEAT を使用したサプリカント スイッチの設定

スイッチをサプリカントに設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable** 例： `Device(config)# cisp enable`	CISP をイネーブルにします。
ステップ 3	**dot1x credentials** *profile* 例： `Device(config)# dot1x credentials test`	802.1x クレデンシャル プロファイルを作成します。これは、サプリカントとして設定されるポートに接続する必要があります。
ステップ 4	**username** *suppswitch* 例： `Device(config)# username suppswitch`	ユーザ名を作成します。
ステップ 5	**password** *password* 例： `Device(config)# password myswitch`	新しいユーザ名のパスワードを作成します。
ステップ 6	**dot1x supplicant force-multicast** 例： `Device(config)# dot1x supplicant force-multicast`	ユニキャストまたはマルチキャストパケットのいずれかを受信した場合にスイッチに強制的にマルチキャスト EAPOL だけを送信させます。 これにより、NEAT がすべてのホストモードでのサプリカントスイッチで機能できるようにもなります。

	コマンドまたはアクション	目的
ステップ 7	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport trunk encapsulation dot1q** 例： `Device(config-if)# switchport trunk encapsulation dot1q`	ポートをトランク モードに設定します。
ステップ 9	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	**dot1x pae supplicant** 例： `Device(config-if)# dot1x pae supplicant`	インターフェイスをポート アクセス エンティティ（PAE）サプリカントとして設定します。
ステップ 11	**dot1x credentials** *profile-name* 例： `Device(config-if)# dot1x credentials test`	802.1x クレデンシャル プロファイルをインターフェイスに対応付けます。
ステップ 12	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet1/0/1`	設定を確認します。

	コマンドまたはアクション	目的
ステップ 14	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。
ステップ 15	Auto Smartport マクロを使用した NEAT の設定	スイッチ VSA ではなく Auto Smartport ユーザ定義マクロを使用して、オーセンティケータ スイッチを設定することもできます。詳細については、このリリースに対応する『*Auto Smartports Configuration Guide*』を参照してください。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定

スイッチで 802.1x 認証を設定するほか、ACS を設定する必要があります。情報については、『*Configuration Guide for Cisco Secure ACS 4.2*』を参照してください。
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs_config.pdf

（注） スイッチにダウンロードする前に、ダウンロード可能な ACL を ACS で設定する必要があります。

ポートでの認証後、**show ip access-list** 特権 EXEC コマンドを使用して、ポートにダウンロードした ACL を表示できます。

ダウンロード可能な ACL の設定

これらのポリシーは、クライアントが認証され、クライアント IP アドレスが IP デバイス トラッキングテーブルに追加された後で有効になります。その後スイッチがダウンロード可能な ACL をポートに適用します。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**ip device tracking** 例： `Device(config)# ip device tracking`	IP デバイス トラッキング テーブルを設定します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa authorization network default local group radius** 例： `Device(config)# aaa authorization network default local group radius`	許可の方法をローカルに設定します。許可の方法を削除するには、**no aaa authorization network default local group radius** コマンドを使用します。
ステップ 5	**radius-server vsa send authentication** 例： `Device(config)# radius-server vsa send authentication`	RADIUS VSA 送信認証を設定します。
ステップ 6	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/4`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip access-group** *acl-id* **in** 例： `Device(config-if)# ip access-group default_acl in`	ポートの入力方向のデフォルト ACL を設定します。 （注） *acl-id* はアクセス リストの名前または番号です。
ステップ 8	**show running-config interface** *interface-id* 例： `Device(config-if)# show running-config`	設定を確認します。

	コマンドまたはアクション	目的
	`interface gigabitethernet2/0/4`	
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ダウンロード ポリシーの設定

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **{ deny | permit } { hostname | any | host } log** 例： `Device(config)# access-list 1 deny any log`	デフォルト ポート ACL を定義します。 access-list-number には、1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。 条件が一致した場合にアクセスを拒否する場合は **deny**、許可する場合は **permit** を指定します。 source は、次のようなパケットを送信するネットワークまたはホストの送信元アドレスです。 • **hostname**：ドット付き 10 進表記による 32 ビット長の値。 • **any**：source および source-wildcard の値 0.0.0.0 255.255.255.255 の省略形を意味するキーワード any。source-wildcard 値を入力する必要はありません。 • **host**：source および source-wildcard の値 source 0.0.0.0 の省略形を意味するキーワード host。

	コマンドまたはアクション	目的
		（任意）source-wildcard ビットを送信元アドレスに適用します。 （任意）ログを入力して、エントリと一致するパケットに関する情報ロギングメッセージをコンソールに送信します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/2`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip access-group** *acl-id* **in** 例： `Device(config-if)# ip access-group default_acl in`	ポートの入力方向のデフォルト ACL を設定します。 （注） acl-id はアクセス リストの名前または番号です。
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 7	**aaa authorization network default group radius** 例： `Device(config)# aaa authorization network default group radius`	許可の方法をローカルに設定します。許可の方法を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 8	**ip device tracking** 例： `Device(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。 IP デバイス トラッキング テーブルをディセーブルにするには、**no ip device tracking** グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 9	**ip device tracking probe [count | interval | use-svi]** 例： `Device(config)# ip device tracking probe count`	（任意）IP デバイストラッキングテーブルを設定します。 • **count** *count*：スイッチが ARP プローブを送信する回数を設定します。指定できる範囲は 1 ～ 5 です。デフォルトは 3 です。 • **interval** *interval*：スイッチが ARP プローブを再送信するまでに応答を待機する時間（秒単位）を設定します。範囲は 30 ～ 300 秒です。デフォルトは 30 秒です。 • **use-svi**：スイッチ仮想インターフェイス（SVI）IP アドレスを ARP プローブのソースとして使用します。
ステップ 10	**radius-server vsa send authentication** 例： `Device(config)# radius-server vsa send authentication`	ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。 （注） ダウンロード可能な ACL が機能する必要があります。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

VLAN ID ベース MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**mab request format attribute 32 vlan access-vlan** 例： `Device(config)# mab request format attribute 32 vlan access-vlan`	VLAN ID ベース MAC 認証をイネーブルにします。
ステップ 3	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

柔軟な認証順序の設定

下の手順で使用される例は、MAB が IEEE 802.1x 認証（dot1x）の前に試行されるように柔軟な認証の順序設定の順序を変更します。MAB は最初の認証方式として設定されているため、MAB に他のすべての認証方式よりも優先されます。

（注） これらの認証方式のデフォルトの順序とプライオリティを変更する前に、これらの変更による潜在的な結果を理解する必要があります。詳細について、http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/application_note_c27-573287_ps6638_Products_White_Paper.html を参照してください。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**switchport mode access** 例： `Device(config-if)# switchport mode access`	RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**authentication order [dot1x | mab] | {webauth}** 例： `Device(config-if)# authentication order mab dot1x`	（任意）ポート上で使用される認証方式の順序を設定します。
ステップ 5	**authentication priority [dot1x | mab] | {webauth}** 例： `Device(config-if)# authentication priority mab dot1x`	（任意）認証方式をポート プライオリティ リストに追加します。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

柔軟な認証の順序設定 （2369 ページ）

Open1x の設定

ポートの許可ステートの手動制御をイネーブルにするには、特権EXECモードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するポートを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 3	**switchport mode access** 例： `Device(config-if)# switchport mode access`	RADIUS サーバを設定した場合に限り、ポートをアクセスモードに設定します。
ステップ 4	**authentication control-direction** {**both** | **in**} 例： `Device(config-if)# authentication control-direction both`	（任意）ポート制御を単一方向モードまたは双方向モードに設定します。
ステップ 5	**authentication fallback** *name* 例： `Device(config-if)# authentication fallback profile1`	（任意）802.1x 認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。
ステップ 6	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] 例： `Device(config-if)# authentication host-mode multi-auth`	（任意）ポート上で認証マネージャモードを設定します。
ステップ 7	**authentication open** 例： `Device(config-if)# authentication open`	（任意）ポート上でオープンアクセスをイネーブルまたはディセーブルにします。
ステップ 8	**authentication order** [**dot1x** | **mab**] | {**webauth**} 例： `Device(config-if)# authentication`	（任意）ポート上で使用される認証方式の順序を設定します。

	コマンドまたはアクション	目的
	`order dot1x webauth`	
ステップ 9	**authentication periodic** 例： `Device(config-if)# authentication periodic`	（任意）ポート上で再認証をイネーブルまたはディセーブルにします。
ステップ 10	**authentication port-control {auto | force-authorized | force-un authorized}** 例： `Device(config-if)# authentication port-control auto`	（任意）ポートの許可ステートの手動制御をイネーブルにします。
ステップ 11	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

Open1x 認証 （2370 ページ）

ポート上での 802.1x 認証のディセーブル化

802.1x 認証をポートでディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで 802.1x 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： `Device(config-if)# switchport mode access`	（任意）RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**no dot1x pae authenticator** 例： `Device(config-if)# no dot1x pae authenticator`	ポートでの 802.1x 認証をディセーブルにします。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

802.1x 認証設定のデフォルト値へのリセット

802.1x認証設定をデフォルト値に戻すには、特権EXECモードで次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface`	インターフェイスコンフィギュレーション モードを開始し、設定するポートを指定します。

	コマンドまたはアクション	目的
	`gigabitethernet1/0/2`	
ステップ 3	**dot1x default** 例： `Device(config-if)# dot1x default`	設定可能な802.1xのパラメータをデフォルト値へ戻します。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

802.1x の統計情報およびステータスのモニタリング

表 *151*：特権 *EXEC* 表示コマンド

コマンド	目的
show dot1x all statistics	すべてのポートの 802.1x 統計情報を表示します。
show dot1x interface *interface-id* **statistics**	指定されたポートの 802.1x 統計情報を表示します。
show dot1x all [**count** | **details** | **statistics** | **summary**]	スイッチの 802.1x 管理ステータスおよび動作ステータスを表示します。
show dot1x interface *interface-id*	指定されたポートの 802.1x 管理ステータスおよび動作ステータスを表示します。

表 *152*：グローバル コンフィギュレーション コマンド

コマンド	目的
no dot1x logging verbose	冗長な802.1x認証メッセージをフィルタに掛けます（Cisco IOS Release 12.2(55) SE 以降）

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セッション アウェアなネットワーキングに対するアイデンティティ コントロール ポリシーおよびアイデンティティ サービス テンプレートの設定。	『Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switch http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.ht
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	『Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Sw http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv4 アクセス コントロール リストに関する機能情報

リリース	機能情報
Cisco IOS XE 3.2SE	IPv4 アクセス コントロール リストは、パケット フィルタリングを実行して、ネットワークを介して移動するパケットとその場所を制御します。このような制御によって、ネットワーク トラフィックを制限し、ユーザおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから外部に送信されるのを防ぐことで、セキュリティを実現します。この機能が導入されました。

リリース	機能情報
Cisco IOS 15.2(2)E	アクセス コントロール エントリの非隣接ポートに対する名前付き ACL のサポート機能を使用すると、1 つのアクセス コントロール エントリで非隣接ポートを指定できるため、複数のエントリが同じ送信元アドレス、宛先アドレス、およびプロトコルを持ち、ポートのみが異なる場合に、アクセス コントロール リストで必要なエントリ数を大幅に減らすことができます。
Cisco IOS 15.2(2)E	IP アクセス リスト エントリ シーケンス番号機能により、permit または deny ステートメントにシーケンス番号を適用したり、名前付き IP アクセス リストでそのようなステートメントを順序変更、追加、削除することができます。この機能により、IP アクセス リストを簡単に変更できるようになります。この機能が実装される前は、アクセス リストの最後にエントリを追加することしかできませんでした。そのため、末尾以外の任意の場所にステートメントを追加する必要があるときは、アクセス リスト全体を再設定する必要がありました。 次のコマンドが導入または変更されました。 **deny (IP)**、**ip access-list resequence deny (IP)**、**permit (IP)**

第 110 章

Web ベース認証の設定

この章では、Webベースの認証を設定する方法について説明します。この章の内容は、次のとおりです。

- 機能情報の確認 （2433 ページ）
- Web ベース認証の概要 （2433 ページ）
- Web ベース認証の設定方法 （2444 ページ）
- Web ベース認証ステータスの監視 （2457 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Web ベース認証の概要

IEEE 802.1x サプリカントが実行されていないホスト システムのエンド ユーザを認証するには、Web 認証プロキシと呼ばれる Web ベース認証機能を使用します。

（注） Web ベース認証は、レイヤ 2 およびレイヤ 3 インターフェイス上に設定できます。

HTTP セッションを開始すると、Web ベース認証は、ホストからの入力 HTTP パケットを代行受信し、ユーザに HTML ログイン ページを送信します。ユーザはクレデンシャルを入力しま

す。このクレデンシャルは、Webベース認証機能により、認証のために認証、許可、アカウンティング（AAA）サーバに送信されます。

認証が成功すると、Web ベース認証はログイン成功 HTML ページをホストに送信し、AAA サーバから返されたアクセス ポリシーを適用します。

認証に失敗した場合、Web ベース認証は、ログインの失敗を示す HTML ページをユーザに転送し、ログインを再試行するように、ユーザにプロンプトを表示します。最大試行回数を超過した場合、Web ベース認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザは待機期間中、ウォッチ リストに載せられます。

（注） 中央 Web 認証リダイレクト用の HTTPS トラフィック インターセプションはサポートされていません。

（注） グローバル パラメータ マップ（method-type、custom、redirect）は、すべてのクライアントおよび SSID で同じ Web 認証方式（consent、web consent、webauth など）を使用するときにのみ使用する必要があります。これにより、すべてのクライアントが同じ Web 認証方式になります。

要件により、1 つの SSID に consent、別の SSID に webauth を使用する場合、名前付きパラメータ マップを 2 つ使用する必要があります。1 番目のパラメータ マップには consent を設定し、2 番目のパラメータ マップには webauth を設定する必要があります。

（注） Webauth クライアントの認証試行時に受信する traceback には、パフォーマンスや行動への影響はありません。これは、ACL アプリケーションの EPM に FFM が返信したコンテキストがすでにキュー解除済み（タイマーの有効期限切れの可能性あり）で、セッションが「未承認」になった場合にまれに発生します。

デバイスのロール

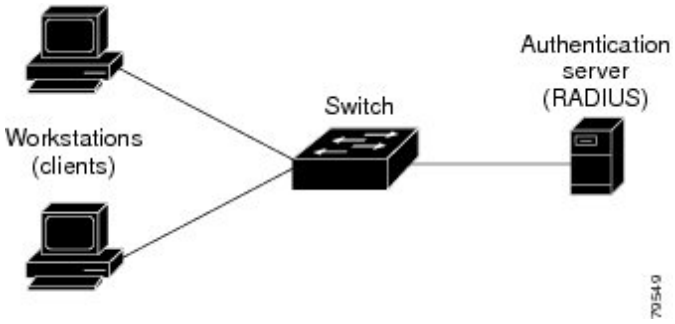
Web ベース認証では、ネットワーク上のデバイスに次のような固有の役割があります。

- クライアント：LAN およびサービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。このワークステーションでは、Java Script がイネーブルに設定された HTML ブラウザが実行されている必要があります。
- 認証サーバ：クライアントを認証します。認証サーバはクライアントの識別情報を確認し、そのクライアントが LAN およびスイッチのサービスへのアクセスを許可されたか、あるいはクライアントが拒否されたのかをスイッチに通知します。
- スイッチ：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として

動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。

図 *131 : Web* ベース認証デバイスの役割

次の図は、ネットワーク上でのこれらのデバイスの役割を示します。



ホストの検出

スイッチは、検出されたホストに関する情報を格納するために、IPデバイストラッキングテーブルを維持します。

（注） デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

レイヤ 2 インターフェイスでは、Web ベース認証は、これらのメカニズムを使用して、IP ホストを検出します。

- ARP ベースのトリガー：ARP リダイレクト ACL により、Web ベース認証は、スタティック IP アドレス、またはダイナミック IP アドレスを持つホストを検出できます。
- ダイナミック ARP インスペクション
- DHCP スヌーピング：スイッチがホストの DHCP バインディング エントリを作成するときに Web ベース認証が通知されます。

セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストをレビューします。

  ホスト IP が例外リストに含まれている場合、この例外リスト エントリからポリシーが適用され、セッションが確立されます。

- 認証バイパスをレビューします。

ホストIPが例外リストに含まれていない場合、Webベース認証は応答しないホスト（NRH）要求をサーバに送信します。

サーバの応答が access accepted であった場合、認証はこのホストにバイパスされます。セッションが確立されます。

- HTTP インターセプト ACL を設定します。

  NRH 要求に対するサーバの応答が access rejected であった場合、HTTP インターセプト ACLがアクティブ化され、セッションはホストからのHTTPトラフィックを待機します。

認証プロセス

Web ベース認証をイネーブルにすると、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTP トラフィックが代行受信され、認証が開始されます。スイッチは、ユーザにログインページを送信します。ユーザはユーザ名とパスワードを入力します。スイッチはこのエントリを認証サーバに送信します。
- 認証に成功した場合、スイッチは認証サーバからこのユーザのアクセスポリシーをダウンロードし、アクティブ化します。ログインの成功ページがユーザに送信されます
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザはログインを再試行します。失敗の回数が試行回数の最大値に達した場合、スイッチはログイン期限切れページを送信します。このホストはウォッチ リストに入れられます。ウォッチ リストのタイム アウト後、ユーザは認証プロセスを再試行することができます。
- 認証サーバがスイッチに応答せず、AAA 失敗ポリシーが設定されている場合、スイッチはホストに失敗アクセスポリシーを適用します。ログインの成功ページがユーザに送信されます
- ホストがレイヤ 2 インターフェイス上の ARP プローブに応答しなかった場合、またはホストがレイヤ 3 インターフェイスでアイドル タイムアウト内にトラフィックを送信しなかった場合、スイッチはクライアントを再認証します。
- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッションタイムアウトを適用します。

（注） Cisco IOS XE Denali 16.1.1 以降では、WLC での Web ベース認証のデフォルトのセッション タイムアウト値は 1800 秒です。Cisco IOS XE Denali 16.1.1 より前は、デフォルトのセッション タイムアウト値は無限の秒数でした。

- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信します。Termination-Action は、サーバからの応答に含まれます。

- Termination-Action がデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除されます。

ローカル Web 認証バナー

Web 認証を使用して、デフォルトのカスタマイズ済み Web ブラウザ バナーを作成して、スイッチにログインしたときに表示するようにできます。

このバナーは、ログインページと認証結果ポップアップページの両方に表示されます。デフォルトのバナー メッセージは次のとおりです。

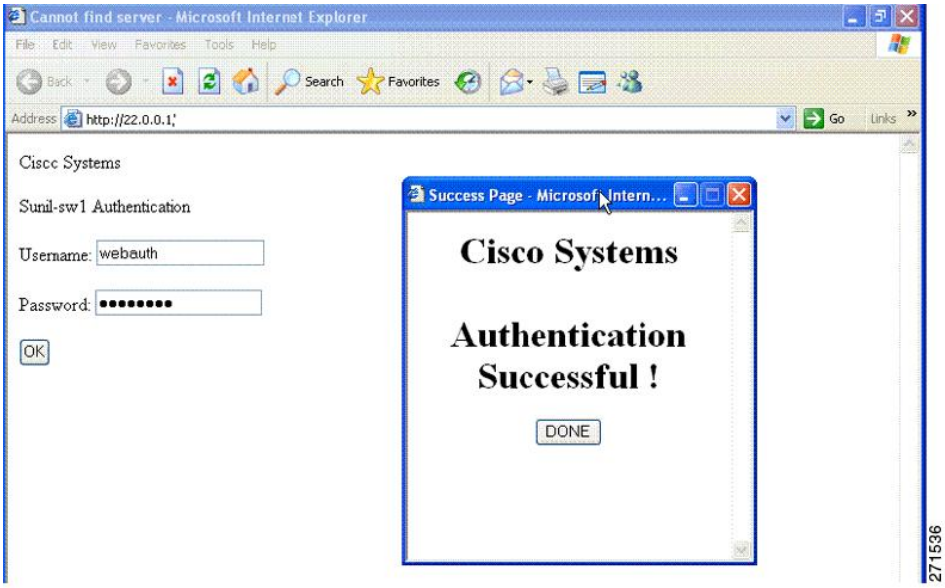
- 認証成功
- 認証失敗
- 認証期限切れ

ローカル ネットワーク認証バナーは、レガシーおよび新スタイル（セッション アウェア）の CLI で次のように設定できます。

- レガシー モード：ip admission auth-proxy-banner http グローバル コンフィギュレーション コマンドを使用します。
- 新スタイル モード：parameter-map type webauth global banner グローバル コンフィギュレーション コマンドを使用します。

ログイン ページには、デフォルトのバナー、*Cisco Systems*、および *Switch host-name Authentication* が表示されます。*Cisco Systems* は認証結果ポップアップ ページに表示されます。

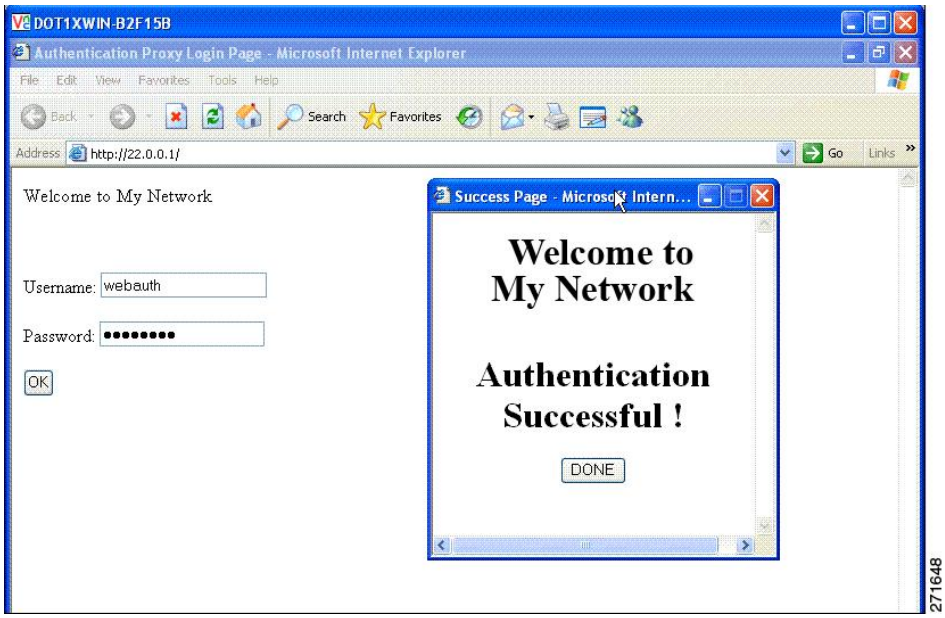
図 *132*：認証成功バナー



バナーは次のようにカスタマイズ可能です。

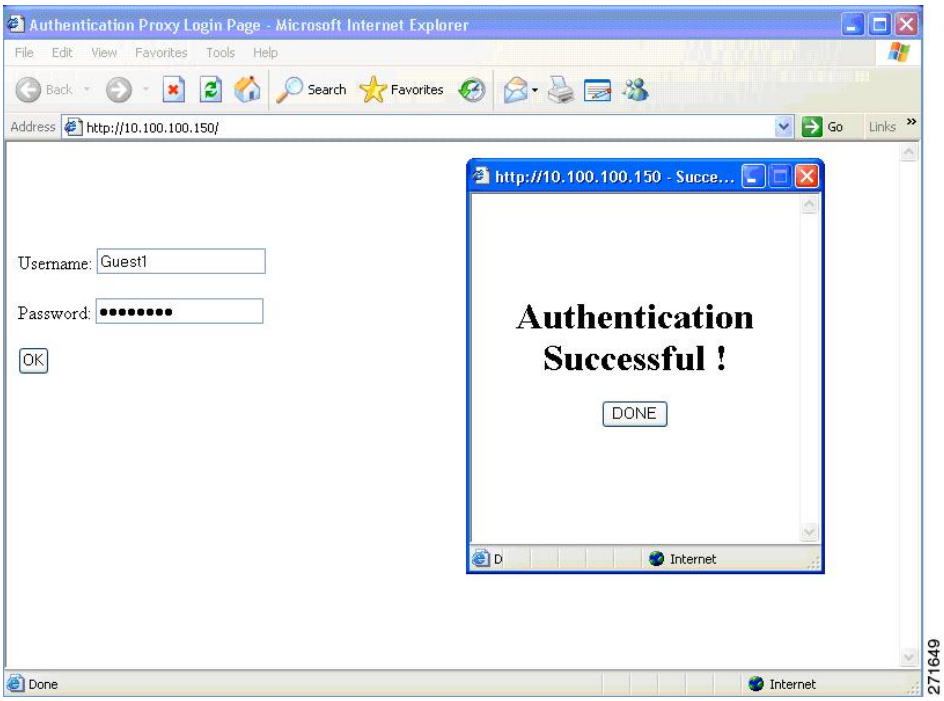
- スイッチ名、ルータ名、または会社名などのメッセージをバナーに追加する。
  - レガシー モード：**ip admission auth-proxy-banner http** *banner-text* グローバル コンフィギュレーション コマンドを使用します。
  - 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。
- ロゴまたはテキスト ファイルをバナーに追加する。
  - レガシー モード：**ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用します。
  - 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。

図 *133* : カスタマイズされた *Web* バナー



バナーが有効にされていない場合、Web認証ログイン画面にはユーザ名とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはバナーは表示されません。

図 *134*：バナーが表示されていないログイン画面



詳細については、セッション対応『*Session Aware Networking Configuration Guide*』、『*Cisco IOS XE Release 3SE (Catalyst 3850 Switches) Session Aware Networking Configuration Guide*』、『*Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』、および『*Web Authentication Enhancements - Customizing Authentication Proxy*』 Web ページを参照してください。

Web 認証カスタマイズ可能な Web ページ

Web ベース認証プロセスでは、スイッチ内部の HTTP サーバは、認証中のクライアントに配信される 4 種類の HTML ページをホストします。サーバはこれらのページを使用して、ユーザに次の 4 種類の認証プロセス ステートを通知します。

- ログイン：資格情報が要求されています。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：ログインの失敗回数が多すぎて、ログイン セッションが期限切れになりました。

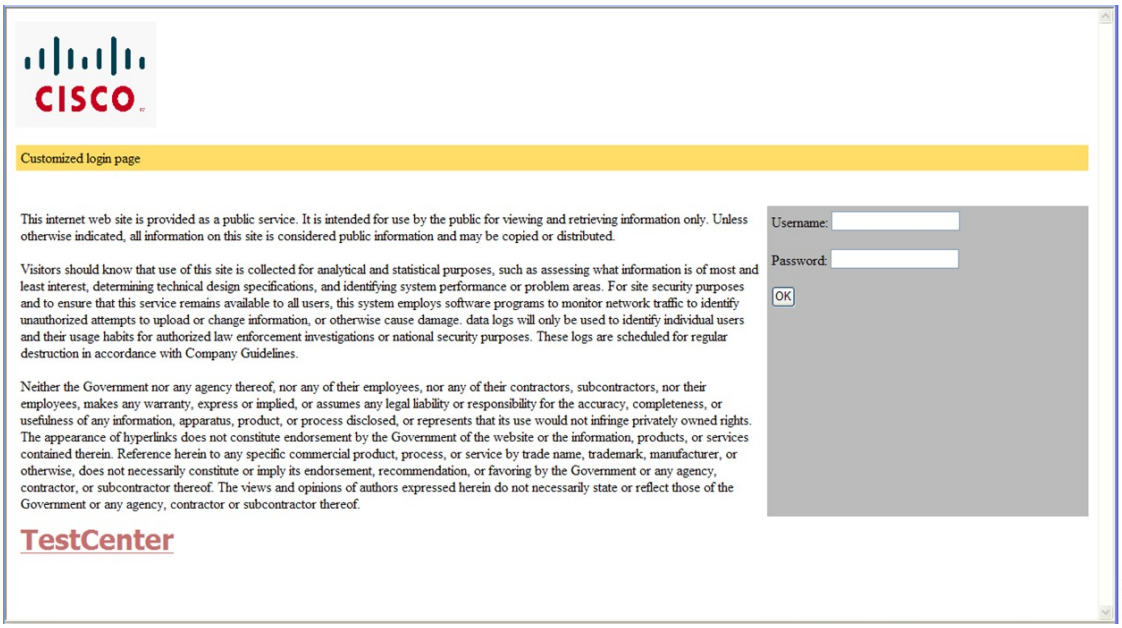
ガイドライン

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。

- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。
- バナー ページで、ログイン ページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。
- この URL 文字列は有効な URL（例：http://www.cisco.com）でなければなりません。不完全な URL は、Web ブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド（例：ページのタイムアウトを設定、暗号化されたパスワードの設定、同じページが 2 回送信されていないことの確認など）を記入する必要があります.
- 設定されたログイン フォームがイネーブルにされている場合、特定の URL にユーザをリダイレクトする CLI コマンドは使用できません。管理者は、Web ページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定の URL にユーザをリダイレクトする CLI コマンドを入力してから、Web ページを設定するコマンドを入力した場合、特定の URL にユーザをリダイレクトする CLI コマンドは効力を持ちません。
- 設定された Web ページは、スイッチのブート フラッシュ、またはフラッシュにコピーできます。
- スタック可能なスイッチでは、スタック マスターまたはスタック メンバーのフラッシュから設定済みのページにアクセスできます。
- ログイン ページを 1 つのフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、スタック マスター、またはメンバのフラッシュ）にすることができます。
- 4 ページすべてを設定する必要があります。
- Web ページを使ってバナー ページを設定した場合、このバナー ページには効果はありません。
- システム ディレクトリ（たとえば、flash、disk0、disk）に保存されていて、ログイン ページに表示する必要のあるロゴ ファイル（イメージ、フラッシュ、オーディオ、ビデオなど）すべてには、必ず、*web_auth_<filename>* の形式で名前をつけてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

デフォルトの内部 HTML ページの代わりに、自分の HTML ページを使用することができます。認証後のユーザのリダイレクト先で、内部成功ページの代わりとなる URL を指定することもできます。

図 *135 :* カスタマイズ可能な認証ページ



認証プロキシ Web ページの注意事項

カスタマイズされた認証プロキシ Web ページを設定する際には、次の注意事項に従ってください。

- カスタム Web ページ機能をイネーブルにするには、カスタム HTML ファイルを 4 個すべて指定します。指定したファイルの数が 4 個未満の場合、内部デフォルト HTML ページが使用されます。
- これら 4 個のカスタム HTML ファイルは、スイッチのフラッシュ メモリ内に存在しなければなりません。各 HTML ファイルの最大サイズは 8 KB です。
- カスタムページ上のイメージはすべて、アクセス可能はHTTPサーバ上に存在しなければなりません。インターセプト ACL は、管理ルール内で設定します。
- カスタム ページからの外部リンクはすべて、管理ルール内でのインターセプト ACL の設定を必要とします。
- 有効なDNSサーバにアクセスするには、外部リンクまたはイメージに必要な名前解決で、管理ルール内にインターセプト ACL を設定する必要があります。
- カスタムWebページ機能がイネーブルに設定されている場合、設定されたauth-proxy-bannerは使用されません。
- カスタム Web ページ機能がイネーブルに設定されている場合、ログインの成功に対するリダイレクション URL は使用できません。
- カスタム ファイルの指定を解除するには、このコマンドの **no** 形式を使用します。

カスタム ログイン ページはパブリック Web フォームであるため、このページについては、次の注意事項に従ってください。

- ログイン フォームは、ユーザによるユーザ名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

関連トピック

認証プロキシ Web ページのカスタマイズ （2452 ページ）

成功ログインに対するリダイレクト URL の注意事項

成功ログインに対するリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルに設定されている場合、リダイレクション URL 機能はディセーブルにされ、CLI では使用できません。リダイレクションは、カスタム ログイン成功ページで実行できます。
- リダイレクション URL 機能がイネーブルに設定されている場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの **no** 形式を使用します。
- Web ベースの認証クライアントが正常に認証された後にリダイレクション URL が必要な場合、URL 文字列は有効な URL（たとえば http://）で開始し、その後に URL 情報が続く必要があります。http:// を含まない URL が指定されると、正常に認証が行われても、そのリダイレクション URL によって Web ブラウザでページが見つからないまたは同様のエラーが生じる場合があります。

関連トピック

成功ログインに対するリダイレクション URL の指定 （2453 ページ）

その他の機能と Web ベース認証の相互作用

ポート セキュリティ

Web ベース認証とポート セキュリティは、同じポートに設定できます。Web ベース認証はポートを認証し、ポート セキュリティは、クライアントの MAC アドレスを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。この場合、このポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

関連トピック

ポート セキュリティのイネーブル化および設定 （2479 ページ）

LAN ポート IP

LAN ポート IP（LPIP）とレイヤ 2 Web ベース認証は、同じポートに設定できます。ホストは、まず Web ベース認証、次に LPIP ポスチャ検証を使用して認証されます。LPIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

Web ベース認証のアイドル時間が満了すると、NAC ポリシーは削除されます。ホストが認証され、ポスチャが再度検証されます。

Gateway IP

VLAN のいずれかのスイッチ ポートで Web ベース認証が設定されている場合、レイヤ 3 VLAN インターフェイス上にゲートウェイ IP（GWIP）を設定することはできません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェアで、両方の機能のホスト ポリシーが適用されます。GWIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

ACL

インターフェイスで VLAN ACL、または Cisco IOS ACL を設定した場合、ACL は、Web ベース認証のホスト ポリシーが適用された後だけ、ホスト トラフィックに適用されます。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの入力トラフィックについて、ポート ACL（PACL）をデフォルトのアクセス ポリシーとして設定することが、必須ではないですがより安全です。認証後、Web ベース認証のホスト ポリシーは、PACL に優先されます。ポートに設定された ACL がなくても、ポリシー ACL はセッションに適用されます。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN が VACL キャプチャ用に設定されているポートには Web ベース認証は設定できません。

コンテキストベース アクセス コントロール

コンテキストベース アクセス コントロール（CBAC）が、ポート VLAN のレイヤ 3 VLAN インターフェイスで設定されている場合、レイヤ 2 ポートで Web ベース認証は設定できません。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。Web ベース認証設定は、すべてのメンバ チャネルに適用されます。

Web ベース認証の設定方法

デフォルトの Web ベース認証の設定

次の表に、デフォルトの Web ベース認証の設定を示しています。

表 *153 :* デフォルトの *Web* ベース認証の設定

機能	デフォルト設定
AAA	無効
RADIUS サーバ • IP アドレス • UDP 認証ポート • Key	• 指定なし • 1645 • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

Web ベース認証の設定に関する注意事項と制約事項

- Web ベース認証は入力だけの機能です。
- Web ベース認証は、アクセス ポートだけで設定できます。Web ベース認証は、トランク ポート、EtherChannel メンバ ポート、またはダイナミック トランク ポートではサポートされていません。
- スタティックな ARP キャッシュが割り当てられているレイヤ 2 インターフェイス上のホストは認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能では検出されません。
- デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。
- スイッチ HTTP サーバを実行するには、IP アドレスを少なくとも 1 つ設定する必要があります。また、各ホスト IP アドレスに到達するようにルートを設定する必要もあります。HTTP サーバは、ホストに HTTP ログイン ページを送信します。
- 2 ホップ以上離れたところにあるホストでは、STP トポロジの変更により、ホスト トラフィックの到着するポートが変わってしまった場合、トラフィックが停止する可能性があ

ります。これは、レイヤ 2（STP）トポロジの変更後に、ARP および DHCP の更新が送信されていない場合に発生します。

- Web ベース認証は、ダウンロード可能なホスト ポリシーとして、VLAN 割り当てをサポートしていません。
- Web ベース認証はセッション認識型ポリシー モードで IPv6 をサポートします。IPv6 Web 認証には、スイッチで設定された少なくても 1 つの IPv6 アドレスおよびスイッチ ポートに設定設定された IPv6 スヌーピングが必要です。
- Web ベース認証および Network Edge Access Topology（NEAT）は、相互に排他的です。インターフェイス上で NEAT がイネーブルの場合、Web ベース認証を使用できず、インターフェイス上で Web ベース認証が実行されている場合は、NEAT を使用できません。
- Web ベース認証 NRH（応答しないホスト）は、音声デバイスではサポートされません。
- パスワード認証プロトコル（PAP）のみがコントローラの Web ベースの RADIUS 認証でサポートされます。チャレンジハンドシェイク認証プロトコル（CHAP）は、コントローラの Web ベースの RADIUS 認証でサポートされません。
- スイッチから RADIUS サーバへの通信の設定に使用される次の RADIUS セキュリティ サーバ設定を確認します。
  - ホスト名
  - ホスト IP アドレス
  - ホスト名と特定の UDP ポート番号
  - IP アドレスと特定の UDP ポート番号

  IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホストエントリは、最初に設定されたホストエントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って選択されます。
- RADIUS サーバ パラメータを設定する場合は、次の点に注意してください。
  - 別のコマンドラインに、**key** *string* を指定します。
  - **key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。
  - **key** *string* を指定する場合、キーの中間、および末尾にスペースを使用します。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。

- すべてのRADIUSサーバについて、タイムアウト、再送信回数、および暗号キー値をグローバルに設定するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、radius-server transmit、および radius-server key グローバル コンフィギュレーション コマンドを使用します。詳細については、『*Cisco IOS Security Configuration Guide*, Release 12.4』および『*Cisco IOS Security Command Reference*, Release 12.4』を参照してください。

（注） RADIUSサーバでは、スイッチのIPアドレス、サーバとスイッチで共有されるkey string、およびダウンロード可能なACL（DACL）などの設定を行う必要があります。詳細については、RADIUSサーバのマニュアルを参照してください。

認証ルールとインターフェイスの設定

この項での例は、レガシー スタイルの設定です。新しいスタイルの設定については、『*Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』を参照してください。

認証ルールおよびインターフェイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admissionname** *name***proxyhttp** 例： `Device(config)# ip admission name webauth1 proxy http`	Web ベース許可の認証ルールを設定します。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type slot/port* 例： `Device(config)# interface gigabitEthernet1/0/1`	インターフェイス コンフィギュレーション モードを開始し、Web ベース認証をイネーブルにする入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。 *type* には、fastethernet、gigabit ethernet、または tengigabitethernet を指定できます。
ステップ 5	**ip access-group** *name* 例： `Device(config-if)# ip access-group webauthag`	デフォルト ACL を適用します。
ステップ 6	**exit** 例： `Device(config-if)# exit`	コンフィギュレーション モードに戻ります。
ステップ 7	**ip device tracking** 例： `Device(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip admission status** 例： `Device# show ip admission status`	設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA 認証の設定

AAA 認証を設定するには、次の手順を実行します。

（注） dACL などの機能を使用する予定の場合は、AAA 認証にデフォルトのリストを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 機能をイネーブルにします。
ステップ 4	**aaa authentication login default group** {**tacacs+** | **radius**} 例： `Device(config)# aaa authentication login default group tacacs+`	ログイン時の認証方法のリストを定義します。
ステップ 5	**aaa authorization auth-proxy default group** {**tacacs+** | **radius**} 例： `Device(config)# aaa authorization auth-proxy default group tacacs+`	Web ベース許可の許可方式リストを作成します。
ステップ 6	**tacacs-server host** {*hostname* | *ip_address*} 例：	AAA サーバを指定します。

	コマンドまたはアクション	目的
	`Device(config)# tacacs-server host 10.1.1.1`	
ステップ 7	**tacacs-server key** {*key-data*} 例： `Device(config)# tacacs-server key`	スイッチと TACACS サーバとの間で使用される許可および暗号キーを設定します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

スイッチ/RADIUS サーバ間通信の設定

RADIUS サーバのパラメータを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**ip radius source-interface vlan** *vlan interface number* 例： `Device(config)# ip radius source-interface vlan 80`	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 4	**radius-server host** {*hostname* | *ip-address*} **test username** *username* 例： `Device(config)# radius-server host 172.120.39.46 test username user1`	リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **test username** *username* は、RADIUS サーバ接続の自動テストをイネーブルにするオプションです。指定された *username* は有効なユーザ名である必要はありません。 **key** オプションは、スイッチと RADIUS サーバの間で使用される認証と暗号キーを指定します。 複数の RADIUS サーバを使用するには、それぞれのサーバでこのコマンドを入力してください。
ステップ 5	**radius-server key** *string* 例： `Device(config)# radius-server key rad123`	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。
ステップ 6	**radius-server dead-criteria tries** *num-tries* 例： `Device(config)# radius-server dead-criteria tries 30`	RADIUS サーバに送信されたメッセージへの応答がない場合に、このサーバが非アクティブであると見なすまでの送信回数を指定します。指定できる *num-tries* の範囲は 1 ～ 100 です。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

HTTP サーバの設定

Web ベース認証を使用するには、Device で HTTP サーバをイネーブルにする必要があります。このサーバは HTTP または HTTPS のいずれかについてイネーブルにできます。

（注） Apple の疑似ブラウザは、**ip http secure-server** コマンドだけを設定すると開きません。 **ip http server** コマンドも設定する必要があります。

HTTP または HTTPS のいずれかでサーバを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http server** 例： `Device(config)# ip http server`	HTTP サーバをイネーブルにします。Web ベース認証機能は、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。
ステップ 4	**ip http secure-server** 例： `Device(config)# ip http secure-server`	HTTPS をイネーブルにします。 カスタム認証プロキシ Web ページを設定するか、成功ログインのリダイレクション URL を指定します。 （注） **ip http secure-server** コマンドを入力したときに、セキュア認証が確実に行われるようにするには、ユーザが HTTP 要求を送信した場合でも、ログインページは必ず HTTPS（セキュア HTTP）形式になるようにします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

認証プロキシ Web ページのカスタマイズ

Web ベースの認証中に、Deviceのデフォルト HTML ページではなく 4 種類の代わりの HTML ページがユーザに表示されるように、Web 認証を設定できます。

この機能のための同等のセッション認識型ネットワーク設定の例については、『*Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』マニュアルの「アイデンティティ制御ポリシーの設定」の章の「Web ベース認証のパラメータ マップの設定」の項を参照してください。

カスタム認証プロキシ Web ページの使用を指定するには、次の手順を実行してください。

始める前に

Deviceのフラッシュ メモリにカスタム HTML ファイルを保存します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admission proxy http login page file** *device:login-filename* 例： `Device(config)# ip admission proxy http login page file disk1:login.htm`	Deviceのメモリ ファイル システム内で、デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの場所を指定します。*device:* はフラッシュ メモリです。

	コマンドまたはアクション	目的
ステップ 4	**ip admission proxy http success page file** *device:success-filename* 例： `Device(config)# ip admission proxy http success page file disk1:success.htm`	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 5	**ip admission proxy http failure page file** *device:fail-filename* 例： `Device(config)# ip admission proxy http fail page file disk1:fail.htm`	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 6	**ip admission proxy http login expired page file** *device:expired-filename* 例： `Device(config)# ip admission proxy http login expired page file disk1:expired.htm`	デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

認証プロキシ Web ページの注意事項 （2441 ページ）

成功ログインに対するリダイレクション URL の指定

認証後に内部成功 HTML ページを効果的に置き換えユーザのリダイレクト先となる URL を指定するためには、次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admission proxy http success redirect** *url-string* 例： `Device(config)# ip admission proxy http success redirect www.example.com`	デフォルトのログイン成功ページの代わりにユーザをリダイレクトする URL を指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

成功ログインに対するリダイレクト URL の注意事項 （2442 ページ）

Web ベース認証パラメータの設定

クライアントが待機時間中にウォッチリストに掲載されるまで許容される失敗ログイン試行の最大回数を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip admission max-login-attempts** *number* 例： `Device(config)# ip admission max-login-attempts 10`	失敗ログイン試行の最大回数を設定します。指定できる範囲は 1 ～ 2147483647 回です。デフォルトは 5 分です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Web ベース認証ローカル バナーの設定

Web 認証が設定されているスイッチにローカル バナーを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip admission auth-proxy-banner http** [*banner-text* | *file-path*] 例： `Device(config)# ip admission auth-proxy-banner http C My Switch C`	ローカル バナーを有効にします。 （任意）*C banner-text C*（*C* は区切り文字）、またはバナーに表示されるファイル（たとえば、ロゴまたはテキストファイル）のファイル パスを入力して、カスタム バナーを作成します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Web ベース認証キャッシュ エントリの削除

Web ベース認証キャッシュ エントリを削除するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip auth-proxy cache** {* | *host ip address*} 例： `Device# clear ip auth-proxy cache`	Delete 認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除

	コマンドまたはアクション	目的
	`192.168.4.5`	するには、具体的な IP アドレスを入力します。
ステップ 3	**clear ip admission cache** {* | *host ip address*} 例： `Device# clear ip admission cache 192.168.4.5`	Delete 認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。

Web ベース認証ステータスの監視

すべてのインターフェイスまたは特定のポートに対する Web ベース認証設定を表示するには、このトピックのコマンドを使用します。

表 *154*：特権 *EXEC* 表示コマンド

コマンド	目的
show authentication sessions method webauth	FastEthernet、ギガビット イーサネット、または 10 ギガビット イーサネットのすべてのインターフェイスに対する Web ベースの認証設定を表示します。
show authentication sessions interface *type slot/port*[**details**]	FastEthernet、ギガビット イーサネット、または 10 ギガビット イーサネットの特定のインターフェイスに対する Web ベースの認証設定を表示します。 セッション認識型ネットワーク モードでは、**show access-session interface** コマンドを使用します。

第 111 章

ポート単位のトラフィック制御の設定

- ポートベースのトラフィック制御の概要 （2459 ページ）
- 機能情報の確認 （2460 ページ）
- ストーム制御に関する情報 （2460 ページ）
- ストーム制御の設定方法 （2462 ページ）
- 保護ポートに関する情報 （2467 ページ）
- 保護ポートの設定方法 （2468 ページ）
- 保護ポートの監視 （2470 ページ）
- ポート ブロッキングに関する情報 （2470 ページ）
- ポート ブロッキングの設定方法 （2470 ページ）
- ポート ブロッキングの監視 （2472 ページ）
- ポート セキュリティの前提条件 （2472 ページ）
- ポート セキュリティの制約事項 （2472 ページ）
- ポート セキュリティの概要 （2473 ページ）
- ポート セキュリティの設定方法 （2479 ページ）
- ポート セキュリティの設定例 （2503 ページ）

ポートベースのトラフィック制御の概要

ポート ベースのトラフィック制御は、特定トラフィック状態に応じてポート レベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。次のポートベースのトラフィック制御機能が、このガイドの記述対象の Cisco IOS リリースでサポートされます。

- Storm Control
- 保護ポート
- ポート ブロッキング
- ポート セキュリティ
- プロトコル ストーム プロテクション

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ストーム制御に関する情報

Storm Control

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム コントロール（またはトラフィック抑制）は、インターフェイスからスイッチング バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

トラフィック アクティビティの測定方法

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 秒単位で受信するビット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート

- 小さいフレームのトラフィック レートの秒単位のパケット数。この機能は、グローバルにイネーブルです。小さいフレームのしきい値は、各インターフェイスで設定されます。

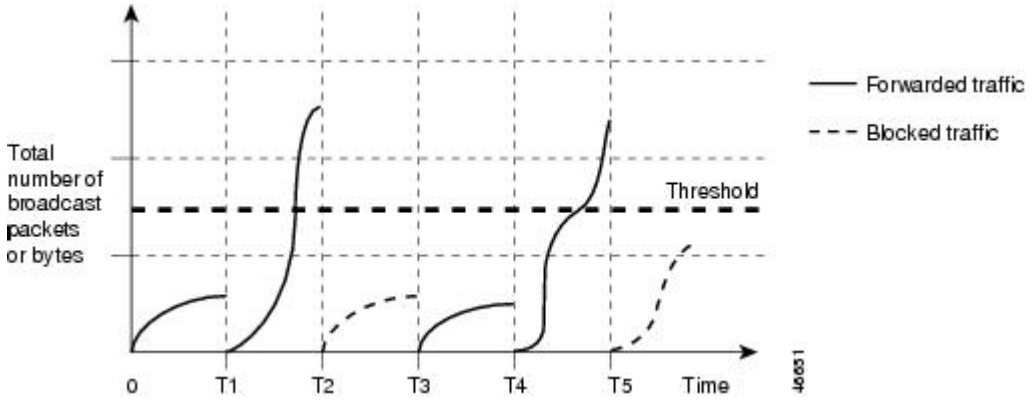
上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

（注） マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジプロトコルデータ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

トラフィック パターン

図 *136 :* ブロードキャスト ストーム制御の例

次の例は、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。



T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。したがって、T2 と T5 の後のインターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過できるパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート

上ではすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。

（注） パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御の設定方法

ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数 % の差異が生じる可能性があります。

（注） ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、次の手順を実行します。

始める前に

ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]} 例： `Device(config-if)# storm-control unicast level 87 65`	ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。 キーワードの意味は次のとおりです。 • *level* には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ～ 100.00 です。 • （任意）*level-low* には、下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第 2 位まで）。この値は上限抑制値より小さいか、または等しくなければなりません。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ～ 100.00 です。 しきい値に最大値（100%）を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。

	コマンドまたはアクション	目的
		• **bps** *bps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをビット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*bps-low* には、下限しきい値レベルをビット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ～ 10000000000.0 です。 • **pps** *pps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low* には、下限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は **0.0 ～** 10000000000.0 です。 BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号（k、m、gなど）を使用できます。
ステップ **5**	**storm-control action** {**shutdown** | **trap**} 例：	ストーム検出時に実行するアクションを指定します。デフォルトではトラフィッ

	コマンドまたはアクション	目的
	`Device(config-if)# storm-control action trap`	クにフィルタリングを実行し、トラップは送信しない設定です。 • ストーム中、ポートを error-disable の状態にするには、**shutdown** キーワードを選択します。 • ストームが検出された場合、SNMP（簡易ネットワーク管理プロトコル）トラップを生成するには、**trap** キーワードを選択します。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**] 例： `Device# show storm-control gigabitethernet1/0/1 unicast`	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御の設定が表示されます。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スモール フレーム到着レートの設定

67バイト未満の着信VLANタグ付きパケットは、小さいフレームと見なされます。このパケットはスイッチにより転送されますが、スイッチ ストーム制御カウンタを増加させません。

スイッチ上の小さいフレームの着信機能をグローバルにイネーブルにして、各インターフェイスのパケットの小さいフレームのしきい値を設定します。最小サイズよりも小さく、指定されたレート（しきい値）で着信するパケットは、ポートがディセーブルにされた後はドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**errdisable detect cause small-frame** 例： `Device(config)# errdisable detect cause small-frame`	スイッチ上の小さいフレームの着信レート機能をイネーブルにします。
ステップ 4	**errdisable recovery interval** 間隔 例： `Device(config)# errdisable recovery interval 60`	（任意）指定された errdisable ステートから回復する時間を指定します。
ステップ 5	**errdisable recovery cause small-frame** 例： `Device(config)# errdisable recovery cause small-frame`	（任意）小さいフレームの着信によりポートが errdisable になった後、そのポートを自動的に再イネーブルにするリカバリ時間を設定します。 ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。
ステップ 6	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 7	**small-frame violation-rate** *pps* 例： `Device(config-if)# small-frame violation rate 10000`	インターフェイスが着信パケットをドロップしてポートを errdisable にするようにしきい値レートを設定します。範囲は、1 ～ 10,000 パケット/秒（pps）です。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show interfaces** *interface-id* 例： `Device# show interfaces gigabitethernet1/0/2`	設定を確認します。
ステップ 10	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

保護ポートに関する情報

保護ポート

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ2トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャストトラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータ トラフィックは、レイヤ3デバイスを介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

スイッチ スタックは論理的には1つのスイッチを表しているため、レイヤ2トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチ スタックの保護ポート間では転送されません。

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

保護ポートのガイドライン

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

保護ポートの設定方法

保護ポートの設定

始める前に

保護ポートは事前定義されていません。これは設定する必要があるタスクです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport protected** 例： `Device(config-if)# switchport protected`	インターフェイスを保護ポートとして設定します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

保護ポートの監視

表 *155 :* 保護ポートの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

ポート ブロッキングに関する情報

ポート ブロッキング

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャスト トラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにします。

（注） マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

ポート ブロッキングの設定方法

インターフェイスでのフラッディング トラフィックのブロッキング

始める前に

インターフェイスは物理インターフェイスまたはEtherChannel グループのいずれも可能です。ポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport block multicast** 例： `Device(config-if)# switchport block multicast`	ポートからの未知のマルチキャストの転送をブロックします。 （注） 純粋なレイヤ 2 マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。
ステップ 5	**switchport block unicast** 例： `Device(config-if)# switchport block unicast`	ポートからの未知のユニキャストの転送をブロックします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces`	入力を確認します。

	コマンドまたはアクション	目的
	gigabitethernet1/0/1 switchport	
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ポート ブロッキングの監視

表 *156 :* ポート ブロッキングの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

ポート セキュリティの前提条件

（注） 最大値をインターフェイス上ですでに設定されているセキュアアドレスの数より小さい値に設定しようとすると、コマンドが拒否されます。

ポート セキュリティの制約事項

スイッチまたはスイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management（SDM）テンプレートによって決められます。この値は、使用可能な MAC

アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数を表します。

ポート セキュリティの概要

ポート セキュリティ

ポート セキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレス グループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュア ポートとしてポートを設定し、セキュア MAC アドレスが最大数に達した場合、ポートにアクセスを試みるステーションの MAC アドレスが識別されたセキュア MAC アドレスのいずれとも一致しないので、セキュリティ違反が発生します。また、あるセキュア ポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュア ポートにアクセスしようとしたときにも、違反のフラグが立てられます。

関連トピック

ポート セキュリティのイネーブル化および設定 （2479 ページ）
ポート セキュリティの設定例 （2503 ページ）

セキュア MAC アドレスのタイプ

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- スタティック セキュア MAC アドレス：**switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレス テーブルに保存されたのち、スイッチの実行コンフィギュレーションに追加されます。
- ダイナミック セキュア MAC アドレス：動的に設定されてアドレス テーブルにのみ保存され、スイッチの再起動時に削除されます。
- スティッキー セキュア MAC アドレス：動的に学習することも、手動で設定することもできます。アドレス テーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

スティッキ セキュア MAC アドレス

スティッキー ラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキー セキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインター

フェイスを設定できます。インターフェイスはスティッキ ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキー セキュア MAC アドレスに変換します。すべてのスティッキー セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキー セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション）に、自動的には反映されません。スティッキー セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキ セキュア アドレスを保存しない場合、アドレスは失われます。

スティッキ ラーニングがディセーブルの場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレス テーブルに追加されている状態で、アドレス テーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。

違反が発生した場合の対処に基づいて、次の 3 種類の違反モードのいずれかにインターフェイスを設定できます。

- protect（保護）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。

  （注） トランク ポートに protect 違反モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

- restrict（制限）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
- shutdown（シャットダウン）：ポート セキュリティ違反により、インターフェイスが error-disabled になり、ただちにシャットダウンされます。そのあと、ポートの LED が消

灯します。セキュア ポートが error-disabled ステートの場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこのステートを解除するか、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにできます。これは、デフォルトのモードです。

- shutdown vlan（VLAN シャットダウン）：VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。

次の表に、ポートセキュリティをインターフェイスに設定した場合の違反モードおよび対処について示します。

表 *157*：セキュリティ違反モードの処置

違反モード	トラフィックの転送 [19]	SNMP トラップの送信	Syslog メッセージの送信	エラー メッセージの表示 [20]	違反カウンタの増加	ポートのシャットダウン
protect	×	いいえ	いいえ	いいえ	いいえ	×
restrict	×	Yes	Yes	いいえ	Yes	×
シャットダウン	×	いいえ	いいえ	×	Yes	Yes
shutdown vlan	×	×	Yes	いいえ	Yes	× [21]

[19] 十分な数のセキュアMACアドレスを削除するまで未知の送信元アドレスを持つパケットがドロップされます。
[20] セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラー メッセージを返します。
[21] 違反が発生した VLAN のみシャットダウンします。

ポート セキュリティ エージング

ポート上のすべてのセキュア アドレスにエージング タイムを設定するには、ポート セキュリティ エージングを使用します。ポートごとに2つのタイプのエージングがサポートされています。

- absolute：指定されたエージング タイムの経過後に、ポート上のセキュア アドレスが削除されます。
- inactivity：指定されたエージング タイムの間、セキュア アドレスが非アクティブであった場合に限り、ポート上のセキュア アドレスが削除されます。

関連トピック

ポート セキュリティ エージングのイネーブル化および設定 （2485 ページ）

ポート セキュリティとスイッチ スタック

スタックに新規に加入したスイッチは、設定済みのセキュア アドレスを取得します。他のスタック メンバーから新しいスタック メンバーに、ダイナミック セキュア アドレスがすべてダウンロードされます。

スイッチ（アクティブ スイッチまたはスタック メンバのいずれか）がスタックから離れると、その他のスタック メンバに通知が行き、そのスイッチが設定または学習したセキュア MAC アドレスがセキュア MAC アドレス テーブルから削除されます。

デフォルトのポート セキュリティ設定

表 *158 :* デフォルトのポート セキュリティ設定

機能	デフォルト設定
ポート セキュリティ	ポート上でディセーブル
スティッキー アドレス ラーニング	ディセーブル
ポートあたりのセキュア MAC アドレスの最大数	1。
違反モード	shutdown。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。
ポート セキュリティ エージング	ディセーブルエージング タイムは 0 スタティック エージングはディセーブル タイプは absolute

ポート セキュリティの設定時の注意事項

- ポート セキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートをダイナミック アクセス ポートにすることはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。

- （注） 音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。

- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュア アドレスを設定する必要があります。

- トランク ポートがポートセキュリティで設定され、データ トラフィックのアクセス VLAN および音声トラフィックのアクセス VLAN に割り当てられている場合は、**switchport voice** および **switchport priority extend** インターフェイス コンフィギュレーション コマンドを入力しても効果はありません。

  接続装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレス、音声 VLAN の IP アドレスの順に要求すると、アクセス VLAN だけが IP アドレスに割り当てられます。

- インターフェイスの最大セキュアアドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。

- スイッチはスティッキセキュア MAC アドレスのポートセキュリティ エージングをサポートしていません。

次の表に、他のポートベース機能と互換性のあるポート セキュリティについてまとめます。

表 *159*：ポート セキュリティと他のポートベース機能との互換性

ポート タイプまたはポートの機能	ポート セキュリティとの互換性
DTP [22] ポート[23]	なし
トランク ポート	Yes
ダイナミックアクセス ポート[24]	なし
ルーテッド ポート	なし
SPAN 送信元ポート	Yes
SPAN 宛先ポート	No
EtherChannel	Yes
トンネリング ポート	Yes

ポート タイプまたはポートの機能	ポート セキュリティとの互換性
保護ポート	Yes
IEEE 802.1x ポート	Yes
音声 VLAN ポート[25]	Yes
IP ソース ガード	Yes
ダイナミック アドレス解決プロトコル（ARP）インスペクション	Yes
Flex Link	Yes

22 DTP = Dynamic Trunking Protocol

23 **switchport mode dynamic**インターフェイス コンフィギュレーション コマンドで設定されたポート。

24 **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドで設定される Vlan Query Protocol（VQP）ポート。

25 ポートに最大限可能なセキュアなアドレスを設定します（アクセスVLANで可能なセキュアなアドレスの最大数に 2 を加えた数）。

ポートベースのトラフィック制御の概要

ポート ベースのトラフィック制御は、特定トラフィック状態に応じてポート レベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。次のポートベースのトラフィック制御機能が、このガイドの記述対象のCisco IOS リリースでサポートされます。

- Storm Control
- 保護ポート
- ポート ブロッキング
- ポート セキュリティ
- プロトコル ストーム プロテクション

ポート セキュリティの設定方法

ポート セキュリティのイネーブル化および設定

始める前に

このタスクは、ポートにアクセスできるステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制約します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode** {**access** | **trunk**} 例： `Device(config-if)# switchport mode access`	インターフェイス スイッチポート モードを access または trunk に設定します。デフォルト モード（dynamic auto）のインターフェイスは、セキュア ポートとして設定できません。
ステップ 5	**switchport voice vlan** *vlan-id* 例： `Device(config-if)# switchport voice vlan 22`	ポート上で音声 VLAN をイネーブルにします。 vlan-id：音声トラフィックに使用する VLAN を指定します。

	コマンドまたはアクション	目的
ステップ 6	**switchport port-security** 例： `Device(config-if)# switchport port-security`	インターフェイス上でポートセキュリティをイネーブルにします。
ステップ 7	**switchport port-security [maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]] 例： `Device(config-if)# switchport port-security maximum 20`	（任意）インターフェイスの最大セキュアMACアドレス数を設定します。スイッチまたはスイッチスタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されているMACアドレスの最大数によって決まります。この値は、アクティブな SDM テンプレートによって決まります。この値は、使用可能なMACアドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュアMACアドレスで使用される MAC アドレスを含む）の総数を表します。 （任意）**vlan**：VLAN 当たりの最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-list*：トランク ポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、VLAN 単位の最大値を設定できます。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。 • **access**：アクセス ポート上で、アクセスVLANとしてVLANを指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。

	コマンドまたはアクション	目的
		（注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。
ステップ 8	**switchport port-security violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**} 例： `Device(config-if)# switchport port-security violation restrict`	（任意）違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。 • **protect**：ポート セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。 （注） トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。 • **restrict**：セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。セキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きま

	コマンドまたはアクション	目的
		す。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。 • **shutdown**：違反が発生すると、インターフェイスが error-disabled になり、ポートの LED が消灯します。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。 • **shutdown vlan**：VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。 （注） セキュア ポートが error-disabled ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力して、このステートから回復させることができます。手動で再びイネーブルにするには、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface vlan** 特権 EXEC コマンドを入力します。
ステップ 9	**switchport port-security [mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}] 例： `Device(config-if)# switchport`	（任意）インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定したセキュア MAC アドレスが最大数よ

	コマンドまたはアクション	目的
	`port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice`	り少ない場合、残りの MAC アドレスは動的に学習されます。 （注） このコマンドの入力後にスティッキー ラーニングをイネーブルにすると、動的に学習されたセキュアアドレスがスティッキー セキュア MAC アドレスに変換されて実行コンフィギュレーションに追加されます。 （任意）**vlan**：VLAN 当たりの最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。
ステップ 10	**switchport port-security mac-address sticky** 例：	（任意）インターフェイス上でスティッキ ラーニングをイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config-if)# switchport port-security mac-address sticky`	
ステップ 11	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}] 例： `Device(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice`	（任意）スティッキー セキュア MAC アドレスを入力し、必要な回数だけコマンドを繰り返します。設定したセキュア MAC アドレスの数が最大数より少ない場合、残りの MAC アドレスは動的に学習されてスティッキー セキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。 （注） このコマンドの入力前にスティッキー ラーニングをイネーブルにしないと、エラーメッセージが表示されてスティッキー セキュア MAC アドレスを入力できません。 （任意）**vlan**：VLAN 当たりの最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show port-security** 例： `Device# show port-security`	入力を確認します。
ステップ 14	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 15	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

ポート セキュリティ （2442 ページ）
ポート セキュリティ （2473 ページ）
ポート セキュリティの設定例 （2503 ページ）

ポート セキュリティ エージングのイネーブル化および設定

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュアポート上のデバイスを削除および追加し、なおかつポート上のセキュアアドレス数を制限できます。セキュアアドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}} 例： `Device(config-if)# switchport port-security aging time 120`	セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにします。またはエージング タイムやタイプを設定します。 （注） スイッチは、スティッキー セキュア アドレスのポート セキュリティ エージングをサポートしていません。 このポートに、スタティックに設定されたセキュア アドレスのエージングをイネーブルにする場合は、**static** を入力します。 *time* には、このポートのエージング タイムを指定します。有効な範囲は、0～1440 分です。 **type** には、次のキーワードのいずれか 1 つを選択します。 • **absolute**：（任意）エージング タイプを絶対エージングとして設定します。このポートのセキュア アドレスはすべて、指定した時間（分単位）が経過すると期限切れになり、セキュア アドレス リストから削除されます。 • **inactivity**：（任意）エージング タイプを非アクティブ エージングとして設定します。指定された time 期間中にセキュア送信元アドレスからのデータ トラフィックがない場

	コマンドまたはアクション	目的
		合に限り、このポートのセキュアアドレスが期限切れになります。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show port-security** [**interface** *interface-id*] [**address**] 例： `Device# show port-security interface gigabitethernet1/0/1`	入力を確認します。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ポート セキュリティ エージング （2475 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ストーム制御に関する情報

Storm Control

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム コントロール（またはトラフィック抑制）は、インターフェイスからスイッチングバスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

トラフィック アクティビティの測定方法

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 秒単位で受信するビット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 小さいフレームのトラフィック レートの秒単位のパケット数。この機能は、グローバルにイネーブルです。小さいフレームのしきい値は、各インターフェイスで設定されます。

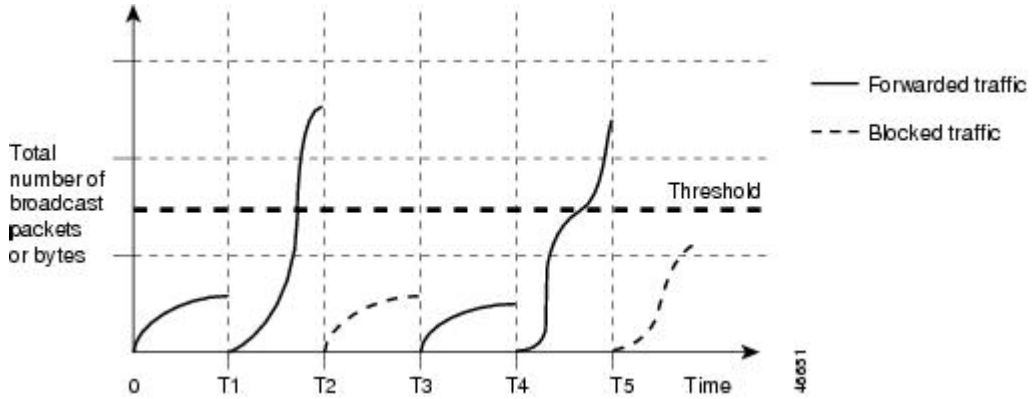
上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

（注） マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジプロトコルデータ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

トラフィック パターン

図 *137*: ブロードキャスト ストーム制御の例

次の例は、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。



T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。したがって、T2 と T5 の後のインターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過できるパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。

（注） パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御の設定方法

ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数 % の差異が生じる可能性があります。

（注） ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、次の手順を実行します。

始める前に

ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]} 例： `Device(config-if)# storm-control unicast level 87 65`	ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。 キーワードの意味は次のとおりです。 • *level* には、ブロードキャスト、マルチキャスト、またはユニキャスト

	コマンドまたはアクション	目的
		トラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ～ 100.00 です。 • （任意）*level-low* には、下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第 2 位まで）。この値は上限抑制値より小さいか、または等しくなければなりません。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ～ 100.00 です。 しきい値に最大値（100%）を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。 • **bps** *bps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをビット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*bps-low* には、下限しきい値レベルをビット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ～ 10000000000.0 です。

	コマンドまたはアクション	目的
		• **pps** *pps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low* には、下限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は **0.0 ～** 10000000000.0 です。 BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号（k、m、gなど）を使用できます。
ステップ **5**	**storm-control action** {**shutdown** | **trap**} 例： `Device(config-if)# storm-control action trap`	ストーム検出時に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。 • ストーム中、ポートを error-disable の状態にするには、**shutdown** キーワードを選択します。 • ストームが検出された場合、SNMP（簡易ネットワーク管理プロトコル）トラップを生成するには、**trap** キーワードを選択します。
ステップ **6**	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**] 例： `Device# show storm-control gigabitethernet1/0/1 unicast`	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御の設定が表示されます。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スモール フレーム到着レートの設定

67バイト未満の着信VLANタグ付きパケットは、小さいフレームと見なされます。このパケットはスイッチにより転送されますが、スイッチ ストーム制御カウンタを増加させません。

スイッチ上の小さいフレームの着信機能をグローバルにイネーブルにして、各インターフェイスのパケットの小さいフレームのしきい値を設定します。最小サイズよりも小さく、指定されたレート（しきい値）で着信するパケットは、ポートがディセーブルにされた後はドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**errdisable detect cause small-frame** 例： `Device(config)# errdisable detect cause small-frame`	スイッチ上の小さいフレームの着信レート機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**errdisable recovery interval** 間隔 例： `Device(config)# errdisable recovery interval 60`	（任意）指定された errdisable ステートから回復する時間を指定します。
ステップ 5	**errdisable recovery cause small-frame** 例： `Device(config)# errdisable recovery cause small-frame`	（任意）小さいフレームの着信によりポートが errdisable になった後、そのポートを自動的に再イネーブルにするリカバリ時間を設定します。 ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。
ステップ 6	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	インターフェイス コンフィギュレーションモードを開始し、設定するインターフェイスを指定します。
ステップ 7	**small-frame violation-rate** *pps* 例： `Device(config-if)# small-frame violation rate 10000`	インターフェイスが着信パケットをドロップしてポートを errdisable にするようにしきい値レートを設定します。範囲は、1 ～ 10,000 パケット/秒（pps）です。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show interfaces** *interface-id* 例： `Device# show interfaces gigabitethernet1/0/2`	設定を確認します。

	コマンドまたはアクション	目的
ステップ 10	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

保護ポートに関する情報

保護ポート

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ2トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータ トラフィックは、レイヤ3デバイスを介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

スイッチ スタックは論理的には1つのスイッチを表しているため、レイヤ2トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチスタックの保護ポート間では転送されません。

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

保護ポートのガイドライン

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

保護ポートの設定方法

保護ポートの設定

始める前に

保護ポートは事前定義されていません。これは設定する必要があるタスクです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport protected** 例：	インターフェイスを保護ポートとして設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# switchport protected`	
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

保護ポートの監視

表 *160 :* 保護ポートの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

次の作業

•

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

機能情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ポート ブロッキングに関する情報

ポート ブロッキング

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャスト トラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにします。

（注） マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

ポート ブロッキングの設定方法

インターフェイスでのフラッディング トラフィックのブロッキング

始める前に

インターフェイスは物理インターフェイスまたはEtherChannelグループのいずれも可能です。ポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport block multicast** 例： `Device(config-if)# switchport block multicast`	ポートからの未知のマルチキャストの転送をブロックします。 （注） 純粋なレイヤ 2 マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。
ステップ 5	**switchport block unicast** 例： `Device(config-if)# switchport block unicast`	ポートからの未知のユニキャストの転送をブロックします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ポート ブロッキングの監視

表 *161 :* ポート ブロッキングの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

次の作業

•

その他の参考資料

関連資料

関連項目	マニュアル タイトル

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

機能情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

ポート セキュリティの設定例

次に、ポート上でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する例を示します。違反モードはデフォルトです。スタティック セキュア MAC アドレスは設定せず、スティッキー ラーニングはイネーブルです。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 50
Device(config-if)# switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 上にスタティック セキュア MAC アドレスを設定する例を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 0000.0200.0004 vlan 3
```

次に、ポートのスティッキー ポート セキュリティをイネーブルにする例を示します。データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュア アドレスの総数を 20 に設定します（データ VLAN に 10、音声 VLAN に 10 を割り当てます）。

```
Device(config)# interface tengigabitethernet1/0/1
Device(config-if)# switchport access vlan 21
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan 22
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 20
Device(config-if)# switchport port-security violation restrict
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Device(config-if)# switchport port-security mac-address 0000.0000.0003
Device(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Device(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Device(config-if)# switchport port-security maximum 10 vlan access
Device(config-if)# switchport port-security maximum 10 vlan voice
```

関連トピック

ポート セキュリティ （2473 ページ）
ポート セキュリティのイネーブル化および設定 （2479 ページ）

第 112 章

IPv6 ファースト ホップ セキュリティの設定

- 機能情報の確認 （2505 ページ）
- IPv6 でのファースト ホップ セキュリティの前提条件 （2506 ページ）
- IPv6 でのファースト ホップ セキュリティの制約事項 （2506 ページ）
- IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）
- SISF ベースの IPv4 および IPv6 デバイス トラッキングに関する情報 （2510 ページ）
- SISF ベースの IP デバイス トラッキングおよびスヌーピング ポリシーを作成する方法 （2513 ページ）
- IPv6 スヌーピング ポリシーの設定方法 （2517 ページ）
- **IPv6 バインディング テーブルの内容を設定する方法** （2526 ページ）
- IPv6 ネイバー探索インスペクション ポリシーの設定方法 （2527 ページ）
- IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法 （2533 ページ）
- **IPv6 DHCP ガード ポリシーの設定方法** （2539 ページ）
- IPv6 ソース ガードの設定方法 （2544 ページ）
- IPv6 プレフィックス ガードの設定方法 （2547 ページ）
- IPv6 ファースト ホップ セキュリティの設定例 （2551 ページ）
- その他の参考資料 （2551 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

IPv6 でのファースト ホップ セキュリティの前提条件

- IPv6 がイネーブルになった必要な SDM テンプレートが設定されていること。
- IPv6 ネイバー探索機能についての知識が必要です。

IPv6 でのファースト ホップ セキュリティの制約事項

- 次の制限は、FHS ポリシーを EtherChannel インターフェイスに適用する場合に該当します（ポート チャネル）。
  - FHS ポリシーがアタッチされた物理ポートは EtherChannel グループに参加することができません。
  - FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。
- デフォルトでは、スヌーピング ポリシーにはセキュリティ レベルのガードがあります。そのようなスヌーピング ポリシーがアクセス スイッチに設定されると、ルータまたは DHCP サーバ/リレーに対応するアップリンク ポートが信頼できるポートとして設定されていても、IPv6（DHCPv6）サーバ パケットに対する外部 IPv6 ルータ アドバタイズメント(RA)または Dynamic Host Configuration Protocol はブロックされます。IPv6 RA または DHCPv6 サーバ メッセージを許可するには、次の手順を実行します。
  - IPv6 RA ガード ポリシー（RA の場合）または IPv6 DHCP ガード ポリシー（DHCP サーバ メッセージの場合）をアップリンク ポートに適用します。
  - 低いセキュリティ レベルでスヌーピング ポリシーを設定します（たとえば、glean や inspect など）。しかし、ファースト ホップ セキュリティ機能の利点が有効でないため、このようなスヌーピング ポリシーでは、低いセキュリティ レベルを設定することはお勧めしません。

IPv6 でのファースト ホップ セキュリティに関する情報

IPv6 のファーストホップ セキュリティ（FHS IPv6）は、ポリシーを物理インターフェイス、EtherChannel インターフェイス、または VLAN にアタッチできる一連の IPv6 セキュリティ機能です。IPv6 ソフトウェア ポリシー データベース サービスは、これらのポリシーを保存しアクセスします。ポリシーを設定または変更すると、ポリシー属性はソフトウェア ポリシーデータベースに保存または更新され、その後指定したとおりに適用されます。次の IPv6 ポリシーが現在サポートされています。

- IPv6 スヌーピング ポリシー：IPv6 スヌーピング ポリシーは、IPv6 内の FHS で使用できるほとんどの機能をイネーブルにできるコンテナ ポリシーとして機能します。

- IPv6 FHS バインディング テーブルの内容：スイッチに接続された IPv6 ネイバーのデータベース テーブルはネイバー探索（ND）プロトコル スヌーピングなどの情報ソースから作成されます。このデータベースまたはバインディング テーブルは、リンク層アドレス（LLA）、IPv4 または IPv6 アドレス、およびスプーフィングやリダイレクト攻撃を防止するためにネイバーのプレフィックス バインディングを検証するために、さまざまな IPv6 ガード機能（IPv6 ND インスペクションなど）によって使用されます。
- IPv6 ネイバー探索インスペクション：IPv6 ND インスペクションは、レイヤ 2 ネイバー テーブル内のステートレス自動設定アドレスのバインディングを学習し、保護します。IPv6 ND 検査は、信頼できるバインディング テーブル データベースを構築するためにネイバー探索メッセージを分析します。準拠していない IPv6 ネイバー探索メッセージはドロップされます。ND メッセージは、その IPv6 からメディア アクセス コントロール（MAC）へのマッピングが検証可能な場合に信頼できると見なされます。

  この機能によって、DAD、アドレス解決、ルータ ディスカバリ、ネイバー キャッシュに対する攻撃などの、ND メカニズムに固有の脆弱性のいくつかが軽減されます。

- IPv6 ルータ アドバタイズメント ガード：IPv6 ルータ アドバタイズメント（RA）ガード機能を使用すると、ネットワーク管理者は、ネットワーク スイッチ プラットフォームに到着した不要または不正な RA ガード メッセージをブロックまたは拒否できます。RA は、リンクで自身をアナウンスするためにルータによって使用されます。RA ガード機能は、これらの RA を分析して、未承認のルータによって送信された偽の RA をフィルタリングして除外します。ホスト モードでは、ポートではルータ アドバタイズメントとルータ リダイレクト メッセージはすべて許可されません。RA ガード機能は、レイヤ 2 デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。レイヤ 2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます。

- IPv6 DHCP ガード：IPv6 DHCP ガード機能は、承認されない DHCPv6 サーバおよびリレー エージェントからの返信およびアドバタイズメント メッセージをブロックします。IPv6 DHCP ガードは、偽造されたメッセージがバインディング テーブルに入るのを防ぎ、DHCPv6 サーバまたは DHCP リレーからデータを受信することが明示的に設定されていないポートで受信された DHCPv6 サーバ メッセージをブロックできます。この機能を使用するには、ポリシーを設定してインターフェイスまたは VLAN にアタッチします。DHCP ガード パケットをデバッグするには、**debug ipv6 snooping dhcp-guard** 特権 EXEC コマンドを使用します。

- IPv6 ソース ガード：IPv4 ソース ガードと同様、IPv6 ソース ガードは送信元アドレス スプーフィングを防ぐために、送信元アドレスまたはプレフィックスを検証します。

  ソース ガードでは、送信元または宛先アドレスに基づいてトラフィックを許可または拒否するようにハードウェアをプログラムします。ここでは、データ パケットのトラフィックのみを処理します。

  IPv6 ソース ガード機能は、ハードウェア TCAM テーブルにエントリを格納し、ホストが無効な IPv6 送信元アドレスでパケットを送信しないようにします。

  ソース ガード パケットをデバッグするには、debug ipv6 snooping source-guard 特権 EXEC コマンドを使用します。

（注） IPv6 ソース ガード機能およびプレフィックス ガード機能は、入力方向でのみサポートされています。つまり、出力方法ではサポートされていません。

次の制約事項が適用されます。

- FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。
- IPv6 ソース ガードがスイッチ ポートでイネーブルになっている場合は、そのスイッチ ポートが属するインターフェイスで NDP または DHCP スヌーピングをイネーブルにする必要があります。そうしないと、このポートからのすべてのデータ トラフィックがブロックされます。
- IPv6 ソース ガード ポリシーを VLAN に適用することはできません。インターフェイス レベルのみでサポートされています。
- IPv6 ソース ガードとプレフィックス ガードは同時に使用できません。ポリシーをインターフェイスに付加する際は、「アドレスを確認」するか「プレフィックスを確認」する必要はありますが、両方を確認する必要はありません。
- PVLAN と送信元/プレフィックス ガードは同時に適用できません。
- IPv6 送信元ガードとプレフィックス ガードは EtherChannel でサポートされています。

IPv6 送信元ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Source Guard」の章を参照してください。

- IPv6 プレフィックス ガード：IPv6 プレフィックス ガードは、IPv6 送信元ガード機能内で動作し、デバイスがトポロジに不正なアドレスから発信されたトラフィックを拒否できるようにします。IPv6 プレフィックス ガードは、IPv6 プレフィックスが DHCP プレフィックス委任を使用してデバイス（ホーム ゲートウェイなど）に委任される場合によく使用されています。この機能は、リンクに割り当てられたアドレスの範囲を検出し、この範囲に入っていないアドレスを発信元とするトラフィックをブロックします。

  IPv6 プレフィックス ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Prefix Guard」の章を参照してください。

- IPv6 宛先ガード：IPv6 宛先ガード機能は、IPv6 ネイバー探索で動作し、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決します。アドレス グリーニング機能に依存して、リンク上でアクティブなすべての宛先をバインディング テーブルに挿入してから、バインディング テーブルで宛先が見つからなかったときに実行される解決をブロックします。

（注） IPv6 宛先ガードは、設定された SVI のレイヤ2 VLANに適用することをお勧めします。

IPv6 宛先ガードに関する詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Destination Guard」の章を参照してください。

関連トピック

IPv6 スヌーピング ポリシーの設定方法 （2517 ページ）
IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法 （2523 ページ）
IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 （2524 ページ）
IPv6 スヌーピング ポリシーを全体的に VLAN にアタッチする方法 （2525 ページ）
IPv6 バインディング テーブルの内容を設定する方法 （2526 ページ）
IPv6 ネイバー探索インスペクション ポリシーの設定方法 （2527 ページ）
IPv6 ネイバー探索インスペクション ポリシーをインターフェイスにアタッチする方法 （2529 ページ）
IPv6 ネイバー探索インスペクション ポリシーを全体的に VLAN にアタッチする方法 （2532 ページ）
IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法 （2533 ページ）
IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法 （2536 ページ）
IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 （2537 ページ）
IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法 （2538 ページ）
IPv6 DHCP ガード ポリシーの設定方法 （2539 ページ）
IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法 （2541 ページ）
IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 （2542 ページ）
IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法 （2544 ページ）
IPv6 ソース ガードの設定方法 （2544 ページ）
IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法 （2546 ページ）
IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 （2546 ページ）
IPv6 プレフィックス ガードの設定方法 （2547 ページ）
IPv6 プレフィックス ガード ポリシーをインターフェイスにアタッチする方法 （2549 ページ）
IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 （2550 ページ）

SISF ベースの IPv4 および IPv6 デバイス トラッキングに関する情報

スイッチ統合セキュリティ機能ベース（SISF ベース）の IP デバイス トラッキングは、IP に依存しない CLI コマンドを使用して、IPv4 と IPv6 の両方で FHS が使用可能なスヌーピングおよびデバイス トラッキング機能を有効にするコンテナ ポリシーとして機能します。

既存のすべての IPv6 スヌーピング コマンド（Cisco IOS XE Denali 16.1.1 以前）は、IPv4 および IPv6 アドレス ファミリ両方に設定を適用できる SISF ベース device-tracking コマンドに対応します。

デバイスに存在するレガシー IP デバイス トラッキングおよび IPv6 スヌーピング設定では、新しい **device-tracking upgrade-cli** によって、既存の構成を新しい SISF ベースの device-tracking CLI コマンドに移行することができます。詳細については、IPDT および IPv6 スヌーピング コマンドの SISF ベースの Device-Tracking コマンドへの移行を参照してください。

SISF ベース デバイス トラッキング CLI への移行時の制限

- デバイスにレガシー IP デバイス トラッキング（IPDT）または IPv6 スヌーピング CLI 設定がない場合、以降すべての設定に対して新しい SISF ベース デバイス トラッキング CLI コマンドのみ使用できます。古い IP デバイス トラッキング CLI および Ipv6 スヌーピング CLI は使用できません。
- デバイスに IPv6 スヌーピングが設定されている場合は、以降の設定に引き続きレガシー IPv6 スヌーピング CLI を使用するか、または **device-tracking upgrade-cli** コマンドを使用して、IPv6 スヌーピング設定を新しい SISF ベース デバイス トラッキング CLI に移行できます。すべてのレガシー IPv6 スヌーピング コマンドが変換された後は、新しい device-tracking コマンドのみがデバイスで動作します。**device-tracking upgrade-cli** コマンドを使用していない場合は、レガシー IPv6 スヌーピング コマンドのみデバイスで使用できます。
- デバイスに IPDT が設定されている場合は、レガシー IPDT コマンドおよび IPv6 スヌーピング コマンドを引き続き使用できます。このオプションを使用すると、レガシー モードに制限されます。このモードでは、レガシー IPDT および IPv6 スヌーピング コマンドのみがデバイスで使用可能になります。しかし、既存の設定を新しい SISF ベースの device-tracking コマンドに移行することを推奨します。
- レガシー IPDT および IPv6 スヌーピング設定を新しい SISF ベースの device-tracking コマンドに移行するには、新しい **device-tracking upgrade-cli** コマンドを実行します。**device-tracking upgrade-cli** コマンドを実行した後は、新しい device-tracking コマンドのみがデバイスで使用でき、レガシー IPDT または IPv6 スヌーピング コマンドはサポートされません。
- 古い IPDT IPv6 スヌーピング CLI と新しい SISF ベース デバイス トラッキング CLI の両方を設定することはできません。
- 従来の設定を新しい SISF ベース デバイス トラッキング設定に移行するときに、**ip dhcp snooping vlan** コマンドがレガシー モードで有効であれば、WL-DEV-TRACK-DHCP と呼

ばれるデバイス トラッキング ポリシーが自動的に IPv4 および有効な IP デバイス トラッキングのある IPv6 クライアントの両方をトラックするため作成されます。**ip dhcp snooping vlan** が有効でない場合は、デバイス トラッキングに左右される他の機能をサポートするために、デバイス トラッキングをデバイスで有効にしてください。

IPDT および IPv6 スヌーピング コマンドの SISF ベースの Device-Tracking コマンドへの移行

device-tracking upgrade-cli コマンドを使用して、レガシー IP デバイス トラッキング（IPDT）と IPv6 スヌーピング CLI 設定を、新しい device-tracking CLI コマンドに移行しておくことをお勧めします。

設定シナリオと移行の結果

デバイスにあるレガシー設定に基づいて、**device-tracking upgrade-cli** コマンドは CLI を異なる方法でアップグレードします。既存の設定を移行する前に、次のシナリオ、および対応する移行情報を検討します。

IPDT 設定のみが存在する

デバイスに IP デバイス トラッキング（IPDT）設定のみがある場合は、**device-tracking upgrade-cli** コマンドを実行すると、内部で設定が解釈され、新しく作成されてインターフェイスで割り当てられる SISF ポリシーが使用されます。これにより、この SISF ポリシーを更新できます。

IPv6 スヌーピング設定のみが存在する

既存の IPv6 スヌーピング設定があるデバイスで、古い IPv6 スヌーピング コマンドを以降の設定に使用できます。次のオプションを使用できます。

- （推奨）**device-tracking upgrade-cli** コマンドを使用して、レガシー設定をすべて、新しい SISF ベースの device-tracking コマンドに移行する。すべてのレガシー コマンドが変換された後は、新しい device-tracking コマンドのみがデバイスで動作します。
- レガシー IPv6 スヌーピング コマンドを今後の設定に使用し、**device-tracking upgrade-cli** コマンドは実行しない。このオプションでは、デバイスで使用可能なのはレガシー IPv6 スヌーピング コマンドのみであり、新しい SISF ベースの device-tracking CLI コマンドは使用できません。

Default という名前のデバイス トラッキング ポリシーが、変換プロセスによって作成されます。このポリシーを他のインターフェイスに手動で割り当てることはできません。

IPDT と IPv6 スヌーピングの両方の設定が存在する

レガシー IPDT 設定と IPv6 スヌーピング設定の両方が存在するデバイスでは、**device-tracking upgrade-cli** コマンドを使用して、レガシー コマンドを新しい device-tracking CLI コマンドに変換します。ただし、インターフェイスに割り当てることができるスヌーピング ポリシーは 1 つだけであり、IPv6 スヌーピング ポリシー パラメータは IPDT 設定よりも優先される、ということに注意してください。

（注） 新しい SISF ベースのコマンドに移行しておらず、レガシー IPv6 スヌーピングや IPDT コマンドを使用し続けている場合、IPv4 デバイス トラッキング設定情報が IPv6 スヌーピング コマンドに表示される可能性があります。統合された機能では、IPv4 と IPv6 の両方の設定を扱うためです。これを回避するには、レガシー設定を移行して新しい device-tracking コマンドを使用するようお勧めします。

IPDT または IPv6 スヌーピング設定が存在しない

デバイスにレガシー IP デバイス トラッキング設定も IPv6 スヌーピング設定もない場合は、今後の設定に使用できるのは新しい SISF ベースの **device-tracking** コマンドのみです。レガシー IPDT コマンドと IPv6 スヌーピング コマンドは使用できません。

IPDT、IPv6 スヌーピング、およびデバイス トラッキング CLI の互換性

次の表に、新しい SISF ベースのデバイス トラッキング コマンドと、対応する IPDT および IPv6 スヌーピング コマンドを示します。

IP デバイス トラッキング（IPDT）	IPv6 スヌーピング	SISF ベースのデバイス トラッキング
ip device tracking probe count	サポート対象外	サポート対象外
ip device tracking probe delay	**ipv6 neighbor binding reachable-lifetime**	**device-tracking policy reachable-lifetime**
ip device tracking probe interval	**ipv6 snooping tracking retry-interval**	**device-tracking policy retry-interval**
ip device tracking probe use-svi	**ip device tracking probe auto-source override** として受け付け/解釈	**ip device tracking probe auto-source override** として受け付け/解釈
ip device tracking probe auto-source fallback	**device-tracking tracking auto-source fallback** *ip-address* {*ip-prefix* | *subnet-mask*} **override**	**device-tracking tracking auto-source fallback** *ip-address* {*ip-prefix* | *subnet-mask*} **override**
ip device tracking probe auto-source override	サポート対象外	サポート対象外
ip device tracking tracebuffer	サポート対象外	サポート対象外
ip device tracking maximum	**ipv6 snooping policy** *<name>* **limit**	**device-tracking snooping policy** *<name>* **limit**
ip device tracking probe count	サポート対象外	サポート対象外
ip device tracking probe interval	サポート対象外	サポート対象外
clear ip device tracking all	サポート対象外	サポート対象外

SISF ベースの IP デバイス トラッキングおよびスヌーピング ポリシーを作成する方法

デバイス トラッキング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **device-tracking policy** *policy-name* 例： `Device(config)# device-tracking policy example_policy`	デバイス トラッキング コンフィギュレーション モードを開始します。
ステップ 3	{[**device-role** {**node** | **switch**}] | [**limit address-count** *value*] | [**no**] | [**destination-glean**{**recovery**|**log-only**[**dhcp**]] | [**data-glean**{**recovery**|**log-only**{**dhcp** | **ndp**}] | **prefix-glean**] | [**security-level** {**glean** | **guard** | **inspect**}] | [**tracking** {**disable** [**stale-lifetime** [*seconds* | **infinite**] | **enable** [**reachable-lifetime** [*seconds* | **infinite**] }] | [**trusted-port**] } 例： Device **(config-device-tracking)# security-level inspect** 例： Device **(config-device-tracking)# trusted-port**	IPv4 と IPv6 の両方で次のオプションを有効にします。 • （任意）**device-role**{**node**] | **switch**}：ポートに接続されたデバイスのロールを指定します。デフォルトは **node** です。 • （任意）**limit address-count** *value*：ターゲットごとに許可されるアドレス数を制限します。 • （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。 • （任意）**destination-glean**{**recovery**| **log-only**}[**dhcp**]}：データ トラフィックの送信元アドレス グリーニングによるバインディング テーブルの回復をイネーブルにします。 • （任意）**data-glean**{**recovery**| **log-only**}[**dhcp** | **ndp**]}：送信元アドレスまたはデータ アドレスのグリーニングを使用したバインディング テーブルの回復をイネーブルにします。

	コマンドまたはアクション	目的
		• （任意）**security-level** {**glean**|**guard**|**inspect**}：この機能によって適用されるセキュリティのレベルを指定します。デフォルトは **guard** です。 **glean**：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。 **guard**：アドレスを収集し、メッセージを検査します。さらに、ルータ アドバタイズメント（RA）およびDHCP サーバメッセージを拒否します。これがデフォルトのオプションです。 **inspect**：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。 • （任意）**tracking** {**disable** | **enable**}：トラッキング オプションを指定します。 • （任意）**trusted-port**：信頼できるポートを設定します。該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。
ステップ 4	**end** 例： `Device(config-device-tracking)# exit`	設定モードを終了します。
ステップ 5	**show device-tracking policy** *policy-name* 例： `Device#show device-tracking policy example_policy`	デバイス トラッキング ポリシー設定を表示します。

	コマンドまたはアクション	目的

デバイス トラッキング ポリシーをインターフェイスにアタッチする方法

デバイス トラッキング ポリシーをインターフェイスにアタッチするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	[**no**] **device-trackingattach-policy** *policy name* 例： `Device(config-if)# device-tracking attach-policy example_policy`	デバイス トラッキング ポリシーをインターフェイスまたはそのインターフェイス上で指定された VLAN にアタッチします。 （注） SISF ベースのデバイス トラッキング ポリシーは、カスタム設定されている場合のみ無効にできます。DT-PROGRAMMATIC ポリシーは、DHCP スヌーピングの結果として適用されるため、削除することはできません。 SISF ベースのデバイス トラッキングを無効にするには、この設定例例：SISF ベースのデバイス トラッキングを無効にする方法にある手順に従ってください。

	コマンドまたはアクション	目的
ステップ 4	**show device-tracking policies** [**interface***interface*] 例： `Device#(config-if)# do show running-config`	指定されたインターフェイスの種類と番号に一致するポリシーを表示します。

デバイス トラッキング ポリシーを VLAN にアタッチする方法

複数のインターフェイスでデバイス トラッキング ポリシーを VLAN にアタッチするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 333`	デバイス トラッキング ポリシーをアタッチする VLAN を指定し、その VLAN インターフェイスのコンフィギュレーション モードを開始します。
ステップ 3	[**no**] **device-tracking** [**attach-policy** *policy_name*] 例： `Device(config-vlan-config)#device-tracking attach-policy example_policy`	すべてのスイッチインターフェイスで、デバイス トラッキング ポリシーを指定された VLAN にアタッチします。 （注） SISF ベースのデバイス トラッキング ポリシーは、カスタム設定されている場合のみ無効にできます。DT-PROGRAMMATIC ポリシーは、DHCP スヌーピングの結果として適用されるため、削除することはできません。 SISF ベースのデバイス トラッキングを無効にするには、この設定例例：SISF ベースのデバイス トラッキングを無効にする方法にある手順に従ってください。

	コマンドまたはアクション	目的
ステップ 4	**do show running-config** 例： `Device#(config-if)# do show running-config`	インターフェイスコンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

IPv6 スヌーピング ポリシーの設定方法

IPv6 スヌーピング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 snooping policy** *policy-name* 例： `Device(config)# ipv6 snooping policy example_policy`	スヌーピング ポリシーを作成し、IPv6 スヌーピング ポリシー コンフィギュレーション モードに移行します。
ステップ 3	{[**default**] | [**device-role** {**node** | **switch**}] | [**limit address-count** *value*] | [**no**] | [**protocol** {**dhcp** | **ndp**}] | [**security-level** {**glean** | **guard** | **inspect**}] | [**tracking** {**disable** [**stale-lifetime** [*seconds* | **infinite**] | **enable** [**reachable-lifetime** [*seconds* | **infinite**] }] | [**trusted-port**] } 例： Device **(config-ipv6-snooping)# security-level inspect** 例： Device **(config-ipv6-snooping)# trusted-port**	データ アドレス グリーニングをイネーブルにし、さまざまな条件に対してメッセージを検証し、メッセージのセキュリティ レベルを指定します。 • （任意）**default**：すべてをデフォルト オプションに設定します。 • （任意）**device-role**{**node**] | **switch**}：ポートに接続されたデバイスの役割を指定します。デフォルトは **node** です。 • （任意）**limit address-count** *value*：ターゲットごとに許可されるアドレス数を制限します。 • （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。 • （任意）**protocol**{**dhcp** | **ndp**}：分析のために、スヌーピング機能にどの

	コマンドまたはアクション	目的
		プロトコルをリダイレクトするかを指定します。デフォルトは、**dhcp** および **ndp** です。デフォルトを変更するには、**no protocol** コマンドを使用します。 • （任意）**security-level** {**glean**|**guard**|**inspect**}：この機能によって適用されるセキュリティのレベルを指定します。デフォルトは **guard** です。 **glean**：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。 **guard**：アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバ メッセージを拒否します。これがデフォルトのオプションです。 **inspect**：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。 • （任意）**tracking** {**disable** | **enable**}：デフォルトのトラッキング動作を上書きし、トラッキング オプションを指定します。 • （任意）**trusted-port**：信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。
ステップ 4	**end** 例：	コンフィギュレーション モードから特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-ipv6-snooping)# exit`	
ステップ 5	**show ipv6 snooping policy** *policy-name* 例： `Device#show ipv6 snooping policy example_policy`	スヌーピング ポリシー設定を表示します。

次のタスク

IPv6 スヌーピング ポリシーをインターフェイスまたは VLAN にアタッチします。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 ネイバー プロービングの設定方法

IPv6 ネイバー プロービングが機能するには、バインディング テーブルにデータを入力する必要があります。このタスクは、バインディング テーブル内のエントリのライフ サイクルで微調整を行うために実行します。

1 つの IPv6 クライアントは、随時に複数の IPv6 アドレスを持つことができます。**show ipv6 neighbor binding mac** *mac_address* コマンドを実行すると、これらのアドレスの状態は、そのクライアント MAC アドレスの IPv6 ネイバー バインディング テーブルで `REACHABLE` として表示されます。これらのアドレス上で 300 秒間コントロールアクティビティがない場合、アドレスは `STALE` 状態に移行し、それ以降はクライアントで使用できなくなります。

device-tracking tracking コマンドを使用して定期プローブ（デフォルトの間隔は 300 秒）をすべての IPv6 クライアントに送信し、クライアントの IPv6 アドレスがエージ アウトしておらず、`STALE` 状態に移行していないことを確かめます。これらのプローブは、送信元 IP アドレスがすべてゼロ、つまり、重複アドレス検出（DAD）プローブのスイッチから送信されます。DAD プローブに応答しないために 300 後にエージ アウトするクライアントがいくつか存在します。

（注） IPv6 ネイバー プロービングは、IP アドレスを取得するかまたは維持するのが難しいホストに関してネットワークの問題がある場合のみ、有効にしてください。特に、ホストが IP リースの更新をネゴシエーションしているときの時間枠内で DAD プローブがホストに発行されると、DAD チャレンジによりホストが IP アドレスを放棄することがあります。不必要に IPv6 ネイバー プロービングを有効にすると、予期しないホストの動作が生じる場合があります。

（注） Cisco IOS 15.2(5)E リリース以前の場合は、インターフェイス レベルで IPv6 スヌーピング ポリシーを削除し、VLAN レベルでポリシーをアタッチする必要があります。手順 8 と手順 9 を実行し、VLAN レベルで IPv6 スヌーピング ポリシーをアタッチします。

IPv6 ネイバー プロービングが VLAN で有効な場合は、トランク ポートを介する学習やホストを無効にするために、追加の設定を実行する必要があります。トランク ポートを介した学習を無効にするには、**trusted-port** および **device-role switch** でポリシーを設定する必要があります。この設定では、トランク ポートに接続されている他のアクセス スイッチに、それぞれが接続しているホストに対してファースト ホップ セキュリティを提供するポリシーを用意する必要があります。各スイッチはそれぞれのホストに対してセキュリティを提供する必要があります。手順 10 ～ 12 を実行し、これらの属性でポリシーを設定します。

以下の手順を実行し、IPv6 ネイバー プロービングを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**device-trackingtracking** 例： `Device(config)# device-tracking tracking`	IPv6 ネイバー プロービングを有効にします。 IPv6 ネイバー プロービングを無効にするには、このコマンドの **no** フォームを使用します。
ステップ 4	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 1810`	インターフェイス コンフィギュレーション モードを開始して、IP 情報が割り当てられている VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
ステップ 5	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
		（注） **ipv6 enable** を設定して VLAN に SVI を作成すると、結果として、SVI のリンク ローカル アドレスがプローブのソース アドレスとして使われます。このため、プロービングは DAD メッセージではなく、NS メッセージとして実行されます。この設定ではプローブ応答のレートが高くなります。一部のホストは DAD リクエストを無視することがあります。ただし、NS メッセージにはすべてのホストが応答します。
ステップ 6	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイスをイネーブルにします。 dot1x を IPv4 に対して有効にする場合、dot1x が有効になっているインターフェイス上のポリシーは自動的に設定され、トラッキングは特に IPv6 ネイバー プロービングに対して有効になります。この場合、グローバル設定レベルでトラッキング動作を変更しても、これらの自動的に設定されているポリシーのトラッキングには何の影響もありません。トラッキングはすべてのインターフェイスで常に有効になります。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 1815`	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 9	**ipv6 snooping** [**attach-policy** *policy_name*] 例：	すべてのスイッチおよびスタック インターフェイスで、IPv6 スヌーピング ポ

	コマンドまたはアクション	目的
	`Device(config-vlan-config)# ipv6 snooping attach-policy example_policy`	リシーを指定した VLAN にアタッチします。attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。デフォルトポリシーは、セキュリティ レベル guard、デバイス ロール node、プロトコル ndp および dhcp です。 （注） すべてのインターフェイスで同じユーザ定義のポリシーが設定されている場合、このポリシーを VLAN 上に設定して、インターフェイスから削除できます。インターフェイス上に設定されているポリシーが異なる場合、インターフェイスに設定されているポリシーは削除しないでください。上記のデフォルト ポリシーは VLAN レベルで適用してください。
ステップ 10	**ipv6 snooping policy** *policy_name* 例： `Device(config-vlan-config)# ipv6 snooping policy example_policy`	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始します。
ステップ 11	**trusted-port** 例： `Device(config-ipv6-snooping)# trusted-port`	信頼できるポートにするポートを設定します。
ステップ 12	**device-roleswitch** 例： `Device(config-ipv6-snooping)# device-role switch`	スイッチに接続されているデバイスの役割を設定します。
ステップ 13	**end** 例： `Device(config-ipv6-snooping)# end`	設定モードを終了します。

IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法

インターフェイスまたは VLAN に IPv6 ルータスヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	**switchport** 例： `Device(config-if)# switchport`	switchport モードを開始します。 （注） インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに switchport インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。switchport コンフィギュレーションモードではコマンドプロンプトは（config-if）# と表示されます。

	コマンドまたはアクション	目的

ステップ 4	**ipv6 snooping** [**attach-policy** *policy_name* [**vlan** {*vlan_id* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids*}] | **vlan** {*vlan_id* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	例：
	`Device(config-if)# ipv6 snooping`
	or
	`Device(config-if)# ipv6 snooping attach-policy example_policy`
	or
	`Device(config-if)# ipv6 snooping vlan 111,112`
	or
	`Device(config-if)# ipv6 snooping attach-policy example_policy vlan 111,112`
		インターフェイスまたはそのインターフェイス上の特定の VLAN にカスタム IPv6 スヌーピング ポリシーをアタッチします。デフォルトポリシーをインターフェイスにアタッチするには、**attach-policy** キーワードを指定せずに **ipv6 snooping** コマンドを使用します。デフォルト ポリシーをインターフェイス上の VLAN にアタッチするには、**ipv6 snooping vlan** コマンドを使用します。デフォルト ポリシーは、セキュリティ レベル **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。

ステップ 5	**do show running-config** 例： `Device#(config-if)# do show running-config`	インターフェイスコンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface range** *Interface_name* 例： `Device(config)# interface range Po11`	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには do show interfaces summary コマンドを使用します。

ステップ 3	**ipv6snooping** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	例：
	`Device(config-if-range)# ipv6 snooping attach-policy example_policy`
	or
	`Device(config-if-range)# ipv6 snooping attach-policy example_policy vlan 222,223,224`
	or
	`Device(config-if-range)#ipv6 snooping vlan 222, 223,224`
		IPv6 スヌーピング ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： `Device#(config-if-range)# do show running-config int po11`	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 スヌーピング ポリシーを全体的に VLAN にアタッチする方法

複数のインターフェイス上の VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 333`	VLANインターフェイスのコンフィギュレーションモードを開始し、IPv6スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6 snooping** [**attach-policy** *policy_name*] 例： `Device(config-vlan-config)#ipv6 snooping attach-policy example_policy`	すべてのスイッチおよびスタック インターフェイスで、IPv6 スヌーピング ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルトポリシーがアタッチされます。デフォルト ポリシーは、セキュリティ レベル **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。
ステップ 4	**do show running-config** 例： `Device#(config-if)# do show running-config`	インターフェイスコンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 バインディング テーブルの内容を設定する方法

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	[] [*vlan-id* {*ipv6-address* interface_type *stack/module/port hw_address* [[*seconds* | |] | [{ [default | disable] [[*seconds* | |] | [[[*seconds* | |] | [{*seconds*| [[*seconds* | |] }]**noipv6 neighbor bindingvlaninterfacereachable-lifetimevalue defaultinfinitetrackingreachable-lifetimevalue defaultinfiniteenablereachable-lifetimevalue defaultinfiniteretry-intervaldefaultreachable-lifetimevalue defaultinfinite** 例： `Device(config)# ipv6 neighbor binding`	バインディング テーブル データベースにスタティック エントリを追加します。
ステップ 3	[**no**] **ipv6 neighbor binding max-entries** *number* [**mac-limit** *number* | **port-limit** *number* [**mac-limit** *number*] | **vlan-limit** *number* [[**mac-limit** *number*] | [**port-limit** *number* [**mac-limit***number*]]]] 例： `Device(config)# ipv6 neighbor binding max-entries 30000`	バインディング テーブル キャッシュに挿入できるエントリの最大数を指定します。
ステップ 4	**ipv6 neighbor bindinglogging** 例： `Device(config)# ipv6 neighbor binding logging`	バインディング テーブル メイン イベントのロギングをイネーブルにします。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了して、ルータを特権EXEC モードにします。
ステップ 6	**show ipv6 neighbor binding** 例： `Device# show ipv6 neighbor binding`	バインディング テーブルの内容を表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 ネイバー探索インスペクション ポリシーの設定方法

特権 EXEC モードから、IPv6 ND インスペクション ポリシーを設定するには、次の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**]**ipv6 nd inspectionpolicy** *policy-name* 例： `Device(config)# ipv6 nd inspection policy example_policy`	ND インスペクション ポリシー名を指定し、ND インスペクション ポリシー コンフィギュレーションモードを開始します。
ステップ 3	**device-role** {**host** | **monitor** | **router** | **switch**} 例： `Device(config-nd-inspection)# device-role switch`	ポートに接続されているデバイスのロールを指定します。デフォルトは **host** です。
ステップ 4	**drop-unsecure** 例： `Device(config-nd-inspection)# drop-unsecure`	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
ステップ 5	**limit address-count** *value* 例： `Device(config-nd-inspection)# limit address-count 1000`	1 ～ 10,000 を入力します。
ステップ 6	**sec-level minimum** *value* 例： `Device(config-nd-inspection)# limit address-count 1000`	暗号化生成アドレス（CGA）オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
ステップ 7	**tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]} 例： `Device(config-nd-inspection)# tracking disable stale-lifetime infinite`	ポートでデフォルトのトラッキングポリシーを上書きします。
ステップ 8	**trusted-port** 例： `Device(config-nd-inspection)# trusted-port`	信頼できるポートにするポートを設定します。

	コマンドまたはアクション	目的
ステップ 9	**validate source-mac** 例： `Device(config-nd-inspection)# validate source-mac`	送信元 Media Access Control（MAC）アドレスをリンク層アドレスと照合します。
ステップ 10	**no {device-role | drop-unsecure | limit address-count | sec-level minimum | tracking | trusted-port | validate source-mac}** 例： `Device(config-nd-inspection)# no validate source-mac`	このコマンドの **no** 形式を使用してパラメータの現在の設定を削除します。
ステップ 11	**default {device-role | drop-unsecure | limit address-count | sec-level minimum | tracking | trusted-port | validate source-mac}** 例： `Device(config-nd-inspection)# default limit address-count`	設定をデフォルト値に戻します。
ステップ 12	**do show ipv6 nd inspection policy** *policy_name* 例： `Device(config-nd-inspection)# do show ipv6 nd inspection policy example_policy`	ND インスペクション コンフィギュレーション モードを終了しないで ND インスペクションの設定を確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 ネイバー探索インスペクション ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェース上の VLAN に IPv6 ND 検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** Interface_type *stack/module/port* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**ipv6 nd inspection** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	例：
	`Device(config-if)# ipv6 nd inspection attach-policy example_policy`
	or
	`Device(config-if)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
	or
	`Device(config-if)# ipv6 nd inspection vlan 222, 223,224`
		ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-config** 例： `Device#(config-if)# do show running-config`	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 ネイバー探索インスペクション ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ネイバー探索検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range** *Interface_name* 例： `Device(config)# interface Po11`	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには do show interfaces summary コマンドを使用します。

ステップ 3	**ipv6ndinspection** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	例：
	`Device(config-if-range)# ipv6 nd inspection attach-policy example_policy`
	or
	`Device(config-if-range)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
	or
	`Device(config-if-range)#ipv6 nd inspection vlan 222, 223,224`
		ND インスペクション ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： `Device#(config-if-range)# do show running-config int po11`	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6ネイバー探索インスペクションポリシーを全体的にVLANにアタッチする方法

複数のインターフェイス上の VLAN に IPv6 ND 探索ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 334`	VLANインターフェイスのコンフィギュレーションモードを開始し、IPv6スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6 nd inspection** [**attach-policy** *policy_name*] 例： `Device(config-vlan-config)#ipv6 nd inspection attach-policy example_policy`	すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルトポリシーがアタッチされます。 デフォルトのポリシーは、device-role **host**、no drop-unsecure、limit address-count disabled、sec-level minimum is disabled、tracking is disabled、no trusted-port、no validate source-mac です。
ステップ 4	**do show running-config** 例： `Device#(config-if)# do show running-config`	コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法

IPv6 ルータ アドバタイズメント ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**]**ipv6 nd raguardpolicy** *policy-name* 例： `Device(config)# ipv6 nd raguard policy example_policy`	RA ガード ポリシー名を指定し、RA ガードポリシー コンフィギュレーション モードを開始します。
ステップ 3	[**no**]**device-role** {**host** | **monitor** | **router** | **switch**} 例： `Device(config-nd-raguard)# device-role switch`	ポートに接続されているデバイスのロールを指定します。デフォルトは **host** です。
ステップ 4	[**no**]**hop-limit** {**maximum** | **minimum**} *value* 例： `Device(config-nd-raguard)# hop-limit maximum 33`	（1 ～ 255）最大および最小のホップ制限値の範囲。 ホップ制限値によるルータ アドバタイズメント メッセージのフィルタリングをイネーブルにします。不正 RA メッセージは低いホップ制限値（IPv4 の Time to Live と同じ）を持つ可能性があるため、ホストによって受け入れられると、ホストが不正 RA メッセージ ジェネレータを超えて宛先にトラフィックを生成することができなくなります。指定されていないホップ制限値を持つ RA メッセージはブロックされます。 設定されていない場合、このフィルタはディセーブルになります。 「**minimum**」を設定して、指定する値より低いホップ制限値を持つ RA メッ

	コマンドまたはアクション	目的
		セージをブロックします。 「**maximum**」を設定して、指定する値より高いホップ制限値を持つ RA メッセージをブロックします。
ステップ 5	[**no**]**managed-config-flag** {**off** | **on**} 例： `Device(config-nd-raguard)# managed-config-flag on`	管理アドレス設定（「M」フラグ）フィールドに基づいてルータアドバタイズメントメッセージのフィルタリングをイネーブルにします。「M」フィールドが 1 の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバを使用する場合があります。設定されていない場合、このフィルタはディセーブルになります。 **On**：「M」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。 **Off**：「M」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。
ステップ 6	[**no**]**match** {**ipv6 access-list** *list* | **ra prefix-list** *list*} 例： `Device(config-nd-raguard)# match ipv6 access-list example_list`	指定したプレフィックスリストまたはアクセス リストと照合します。
ステップ 7	[**no**]**other-config-flag** {**on** | **off**} 例： `Device(config-nd-raguard)# other-config-flag on`	その他の設定（「O」フラグ）フィールドに基づくルータアドバタイズメント メッセージのフィルタリングをイネーブルにします。「O」フィールドが 1 の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバを使用する場合があります。設定されていない場合、このフィルタはディセーブルになります。 **On**：「O」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。 **Off**：「O」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。

	コマンドまたはアクション	目的
ステップ 8	**[no]router-preference maximum {high | medium | low}** 例： `Device(config-nd-raguard)# router-preference maximum high`	「Router Preference」フラグを使用したルータ アドバタイズメントメッセージのフィルタリングをイネーブルにします。設定されていない場合、このフィルタはディセーブルになります。 • **high**：「Router Preference」が「high」、「medium」、または「low」に設定された RA メッセージを受け入れます。 • **medium**：「Router Preference」が「high」に設定された RA メッセージをブロックします。 • **low**：「Router Preference」が「medium」または「high」に設定された RA メッセージをブロックします。
ステップ 9	**[no]trusted-port** 例： `Device(config-nd-raguard)# trusted-port`	信頼できるポートとして設定すると、すべての接続デバイスが信頼され、より詳細なメッセージ検証は実行されません。
ステップ 10	**default {device-role | hop-limit {maximum | minimum} | managed-config-flag | match {ipv6 access-list | ra prefix-list } | other-config-flag | router-preference maximum| trusted-port}** 例： `Device(config-nd-raguard)# default hop-limit`	コマンドをデフォルト値に戻します。
ステップ 11	**do show ipv6 nd raguard policy** *policy_name* 例： `Device(config-nd-raguard)# do show ipv6 nd raguard policy example_policy`	（任意）：RA ガード ポリシー コンフィギュレーションモードを終了しないで ND ガード ポリシー設定を表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェース上の VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**ipv6 nd raguard** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	例：
	`Device(config-if)# ipv6 nd raguard attach-policy example_policy`
	or
	`Device(config-if)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	or
	`Device(config-if)# ipv6 nd raguard vlan 222, 223,224`
		ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-config** 例： `Device#(config-if)# do show running-config`	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6ルータアドバタイズメントガードポリシーをレイヤ2EtherChannelインターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ルータ アドバタイズメント ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range** *Interface_name* 例： `Device(config)# interface Po11`	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには do show interfaces summary コマンドを使用します。

ステップ 3	**ipv6ndraguard** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	例：
	`Device(config-if-range)# ipv6 nd raguard attach-policy example_policy`
	or
	`Device(config-if-range)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	or
	`Device(config-if-range)#ipv6 nd raguard vlan 222, 223,224`
		RA ガードポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-configinterface***portchannel_interface_name* 例：	コンフィギュレーション モードを終了しないで、ポリシーが特定のインター

	コマンドまたはアクション	目的
	`Device#(config-if-range)# do show running-config int po11`	フェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法

インターフェイスに関係なく VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 335`	VLANインターフェイスのコンフィギュレーション モードを開始し、IPv6 RA ガード ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6dhcp guard** [**attach-policy** *policy_name*] 例： `Device(config-vlan-config)#ipv6 nd raguard attach-policy example_policy`	すべてのスイッチおよびスタック インターフェイスで、IPv6 RA ガード ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	**do show running-config** 例： `Device#(config-if)# do show running-config`	コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 DHCP ガード ポリシーの設定方法

IPv6 DHCP（DHCPv6）ガード ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no]ipv6 dhcp guardpolicy** *policy-name* 例： `Device(config)# ipv6 dhcp guard policy example_policy`	DHCPv6 ガード ポリシー名を指定し、DHCPv6 ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**[no]device-role {client | server}** 例： `Device(config-dhcp-guard)# device-role server`	（任意）特定の役割のデバイスからのものではないポート上の DHCPv6 応答および DHCPv6 アドバタイズメントをフィルタします。デフォルトは **client** です。 • **client**：デフォルト値。アタッチされたデバイスがクライアントであることを指定します。サーバメッセージにはこのポートでドロップされます。 • **server**：適用されたデバイスが DHCPv6 サーバであることを指定します。このポートでは、サーバメッセージが許可されます。

ステップ 4	**[no] matchserveraccess-list** *ipv6-access-list-name*
	例：
	`;;Assume a preconfigured IPv6 Access List as follows:`
	`Device(config)# ipv6 access-list my_acls`
	`Device(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any`
	`;;configure DCHPv6 Guard to match approved access list.`
		（任意）。アドバタイズされた DHCPv6 サーバまたはリレー アドレスが認証されたサーバのアクセス リストからのものであることの確認をイネーブルにします（アクセス リストの宛先アドレスは「any」です）。設定されていない場合、このチェックは回避されます。空のアクセス リストは、permit all として処理されます。

	コマンドまたはアクション	目的
	`Device(config-dhcp-guard)# match server access-list my_acls`	

ステップ 5	**[no] matchreplyprefix-list** *ipv6-prefix-list-name*
	例：
	`;;Assume a preconfigured IPv6 prefix list as follows:`
	`Device(config)# ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128`
	`;; Configure DCHPv6 Guard to match prefix`
	`Device(config-dhcp-guard)# match reply prefix-list my_prefix`
		（任意）DHCPv6応答メッセージ内のアドバタイズされたプレフィクスが設定された承認プレフィクス リストからのものであることの確認をイネーブルにします。設定されていない場合、このチェックは回避されます。空のプレフィクスリストは、permit として処理されます。

ステップ 6	**[no]preference{ max** *limit* **| min** *limit* **}**
	例：
	`Device(config-dhcp-guard)# preference max 250`
	`Device(config-dhcp-guard)#preference min 150`
		device-role が **server** である場合に **max** および **min** を設定して、DHCPv6 サーバ アドバタイズメント値をサーバ優先度値に基づいてフィルタします。デフォルトではすべてのアドバタイズメントが許可されます。
		max *limit*：（0 ～ 255）（任意）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限未満であるかどうかの検証をイネーブルにします。デフォルトは255です。設定されていない場合、このチェックは回避されます。
		min *limit*：（0 ～ 255）（任意）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限を超過しているかどうかの検証をイネーブルにします。デフォルトは0です。設定されていない場合、このチェックは回避されます。

ステップ 7	**[no] trusted-port** 例： `Device(config-dhcp-guard)# trusted-port`	（任意）**trusted-port**：ポートを信頼モードに設定します。このポートでは、これ以上のポリシングは実行されません。 （注） 信頼できるポートを設定した場合、device-role オプションは使用できません。

	コマンドまたはアクション	目的
ステップ 8	**default** {**device-role** | **trusted-port**} 例： `Device(config-dhcp-guard)# default device-role`	（任意）**default**：コマンドをデフォルトに設定します。
ステップ 9	**do show ipv6 dhcp guard policy** *policy_name* 例： `Device(config-dhcp-guard)# do show ipv6 dhcp guard policy example_policy`	（任意）コンフィギュレーション サブモードを終了せずに IPv6 DHCP のガード ポリシーの設定を表示します。*policy_name* 変数を省略すると、すべての DHCPv6 ポリシーが表示されます。

DHCPv6 ガード設定の例

```
enable
configure terminal
ipv6 access-list acl1
 permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy pol1
 device-role server
 match server access-list acl1
 match reply prefix-list abc
 preference min 0
 preference max 255
 trusted-port
interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy pol1 vlan add 1
 vlan 1
  ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** Interface_type *stack/module/port* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**ipv6 dhcp guard** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	例：
	`Device(config-if)# ipv6 dhcp guard attach-policy example_policy`
	or
	`Device(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	or
	`Device(config-if)# ipv6 dhcp guard vlan 222, 223,224`
		DHCP ガード ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-config interface** Interface_type *stack/module/port* 例： `Device#(config-if)# do show running-config gig 1/1/4`	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 DHCP ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range** *Interface_name* 例： `Device(config)# interface Po11`	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには do show interfaces summary コマンドを使用します。

ステップ 3	**ipv6dhcpguard** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	例：
	`Device(config-if-range)# ipv6 dhcp guard attach-policy example_policy`
	or
	`Device(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	or
	`Device(config-if-range)#ipv6 dhcp guard vlan 222, 223,224`
		DHCP ガード ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： `Device#(config-if-range)# do show running-config int po11`	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法

複数のインターフェイス上の VLAN に IPv6 DHCP のガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 334`	VLANインターフェイスのコンフィギュレーションモードを開始し、IPv6スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6 dhcp guard** [**attach-policy** *policy_name*] 例： `Device(config-vlan-config)#ipv6 dhcp guard attach-policy example_policy`	すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルトポリシーがアタッチされます。デフォルト ポリシーは、device-role **client**、**no** trusted-port です。
ステップ 4	**do show running-config** 例： `Device#(config-if)# do show running-config`	コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 ソース ガードの設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**] **ipv6 source-guard policy** *policy_name* 例： `Device(config)# ipv6 source-guard policy example_policy`	IPv6 ソース ガード ポリシー名を指定し、IPv6 ソース ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	[**deny global-autoconf**] [**permit link-local**] [**default**{...}] [**exit**] [**no**{...}] 例： `Device(config-sisf-sourceguard)# deny global-autoconf`	（任意）IPv6 ソース ガード ポリシーを定義します。 • **deny global-autoconf**：自動設定されたグローバル アドレスからのデータ トラフィックを拒否します。これは、リンク上のすべてのグローバル アドレスが DHCP によって割り当てられている際に、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。 • **permit link-local**：リンクローカル アドレスから送信されたすべてのデータ トラフィックを許可します。 （注） ソース ガード ポリシーに基づく信頼できるオプションはサポートされません。
ステップ 5	**end** 例： `Device(config-sisf-sourceguard)# end`	IPv6 ソース ガード ポリシー コンフィギュレーション モードを終了します。
ステップ 6	**show ipv6 source-guard policy** *policy_name* 例： `Device# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

次のタスク

インターフェイスに IPv6 ソース ガード ポリシーを適用します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** Interface_type *stack/module/port* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 source-guard** [**attach-policy** <*policy_name*>] 例： `Device(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy** *policy_name* 例： `Device#(config-if)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel** *port-channel-number* 例： `Device (config)# interface Po4`	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。
ステップ 4	**ipv6 source-guard** [**attach-policy** <*policy_name*>] 例： `Device(config-if) # ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy** *policy_name* 例： `Device(config-if) #show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）
例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 （2551 ページ）

IPv6 プレフィックス ガードの設定方法

（注） プレフィックス ガードが適用されている場合にリンクローカル アドレスから送信されたルーティング プロトコル制御パケットを許可するには、ソースガード ポリシー コンフィギュレーション モードで permit link-local コマンドをイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**] **ipv6 source-guard policy** *source-guard-policy* 例： `Device (config)# ipv6 source-guard policy my_snooping_policy`	IPv6 ソースガード ポリシー名を定義して、スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	[**no**] **validate address** 例： `Device (config-sisf-sourceguard)# no validate address`	アドレス検証機能をディセーブルにし、IPv6 プレフィックス ガード機能を設定できるようにします。
ステップ 5	**validate prefix** 例： `Device (config-sisf-sourceguard)# validate prefix`	IPv6 ソース ガードをイネーブルにし、IPv6 プレフィックスガード動作を実行します。
ステップ 6	**exit** 例： `Device (config-sisf-sourceguard)# exit`	スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 source-guard policy** [*source-guard-policy*] 例： `Device # show ipv6 source-guard policy policy1`	IPv6 ソースガード ポリシー設定を表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6プレフィックスガードポリシーをインターフェイスにアタッチする方法

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** Interface_type *stack/module/port* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 source-guard attach-policy** *policy_name* 例： `Device(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy** *policy_name* 例： `Device(config-if)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）

IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel** *port-channel-number* 例： `Device (config)# interface Po4`	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。
ステップ 4	**ipv6 source-guard** [**attach-policy** <*policy_name*>] 例： `Device(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy** *policy_name* 例： `Device(config-if)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報 （2506 ページ）
例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 （2551 ページ）

IPv6 ファースト ホップ セキュリティの設定例

例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

次の例は、IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch(config-sisf-sourceguard) # validate address
switch(config-sisf-sourceguard)# exit
Switch(config)# interface Po4
Switch(config)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
Switch(config-if)# exit
switch(config)#
```

関連トピック

IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 （2546 ページ）

例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

次の例は、IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch (config-sisf-sourceguard)# no validate address
Switch((config-sisf-sourceguard)# validate prefix
Switch(config)# interface Po4
Switch(config-if)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
```

関連トピック

IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 （2550 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
『Implementing IPv6 Addressing and Basic Connectivity』	http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ipv6_addr_conn.html

関連項目	マニュアル タイトル
IPv6 ネットワーク管理とセキュリティのトピック	『IPv6 Configuration Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』 http://www.cisco.com/c/en/us/td/docs/ios-xe/ipv6/configuration/xe-3se/3850/ipv6-xe-3se-3850-book.html
IPv6 コマンド リファレンス	『IPv6 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』 http://www.cisco.com/c/en/us/td/docs/ios-xe/ipv6/command/xe-3se/3850/ipv6-xe-3se-3850-book.html

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 113 章

Cisco TrustSec の設定

- Cisco TrustSec の概要 （2553 ページ）
- 機能情報の確認 （2553 ページ）
- Cisco TrustSec の機能 （2554 ページ）
- Cisco TrustSec の機能情報 （2557 ページ）

Cisco TrustSec の概要

Cisco TrustSec は、ネットワーク内のユーザ、ホスト、およびネットワーク デバイスを強力に識別する機能に基づいた、シスコネットワークデバイスのセキュリティを改善します。TrustSec は、特定の役割についてデータ トラフィックを一意に分類することで、トポロジに依存しない、スケーラブルなアクセスコントロールを実現します。TrustSec は、認証されたピアおよびこれらのピアとの暗号化リンク間で信頼を確立することで、データの機密保持および整合性を保証します。

Cisco TrustSec の主要コンポーネントは、Cisco Identity Services Engine（ISE）です。スイッチ上で手動で設定することもできますが、Cisco ISE は TrustSec ID およびセキュリティ グループ ACL（SGACL）でスイッチをプロビジョニングできます。

機能情報の確認

スイッチ上で Cisco TrustSec を設定するには、次の URL にある『Cisco TrustSec Switch Configuration Guide』を参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec.html

Cisco TrustSec General Availability リリースのリリース ノートについては、次の URL を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

Catalyst 3850 および 3650 の制約事項と制限事項については、次の URL で入手できるノートを参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/appa_cat3k.html

概要、データ シート、プラットフォーム マトリクスごとの機能、およびケース スタディを含む Cisco TrustSec ソリューションの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/netsol/ns1051/index.html

Cisco TrustSec の機能

次の表に、TrustSec がイネーブルになった Cisco スイッチで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability リリースによって、サポートされるスイッチの数および各スイッチでサポートされる TrustSec 機能の数は増加しています。

Cisco TrustSec の機能	説明
802.1AE タギング（MACSec）	IEEE 802.1AE に基づくワイヤレート ホップ単位レイヤ 2 暗号化のプロトコル。 MACSec 対応デバイス間において、パケットは送信デバイスからの出力で暗号化され、受信デバイスへの入力で復号化されます。デバイス内では平文です。 この機能は、TrustSec ハードウェア対応デバイス間だけで利用できます。 （注） この機能は、Cisco IOS XE Denali 16.1.1の Catalyst 3850 および Catalyst 3650 スイッチではサポートされていません。 （注） この機能は 2960x ではサポートされていません。
エンドポイント アドミッション コントロール（EAC）	EAC は、TrustSec ドメインに接続しているエンドポイント ユーザまたはデバイスの認証プロセスです。通常、EAC はアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可に成功すると、ユーザまたはデバイスに対してセキュリティ グループ タグが割り当てられます。現在、EAC は 802.1X、MAC 認証バイパス（MAB）、および Web 認証プロキシ（WebAuth）とすることができます。

Cisco TrustSec の機能	説明
ネットワーク デバイス アドミッション コントロール（NDAC）	NDAC は、TrustSec ドメイン内の各ネットワーク デバイスがピア デバイスのクレデンシャルおよび信頼性を確認できる認証プロセスです。NDAC は、IEEE 802.1X ポート ベースの認証に基づく認証フレームワークを利用し、EAP 方式として EAP-FAST を使用します。NDAC プロセスの認証および許可に成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションとなります。 （注） この機能は 2960x ではサポートされていません。
セキュリティ グループ アクセス コントロール リスト（SGACL）	セキュリティ グループ アクセス コントロール リスト（SGACL）は、セキュリティ グループ タグをポリシーと関連付けます。ポリシーは、TrustSec ドメインから出力される SGT タグ付きトラフィックに対して適用されます。
Cisco TrustSec SGACL のハイ アベイラビリティ	Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）は、Cisco StackWise 技術をサポートしているスイッチでのハイ アベイラビリティ機能をサポートしています。Cisco StackWise 技術によってステートフルな冗長性が提供され、スイッチ スタックはアクセス制御エントリを強制し、処理できます。 この機能を有効にする Cisco TrustSec 固有の設定はありません。 この機能は、Cisco IOS XE Release Denali 16.2.1 以降で、Catalyst 3850 および 3650 シリーズ スイッチでのみサポートされます。

Cisco TrustSec の機能	説明
セキュリティ アソシエーション プロトコル（SAP）	NDAC 認証のあと、セキュリティ アソシエーション プロトコル（SAP）は、その後の TrustSec ピア間の MACSec リンク暗号化のキーおよび暗号スイートについて、自動的にネゴシエーションを行います。SAP は IEEE 802.11i で定義されます。 （注） この機能は、Cisco IOS XE Denali 16.1.1の Catalyst 3850 および Catalyst 3650 スイッチではサポートされていません。 （注） この機能は 2960x ではサポートされていません。
セキュリティ グループ タグ（SGT）	SGT は、TrustSec ドメイン内の送信元のセキュリティ分類を示す 16 ビットの単一ラベルです。イーサネット フレームまたは IP パケットに追加されます。
SGT Exchange Protocol（SXP）	Security Group Tag Exchange Protocol（SXP）。SXP を使用すると、TrustSec にハードウェアで対応していないデバイスが Cisco Identity Services Engine（ISE）または Cisco Secure アクセス コントロール システム（ACS）から認証されたユーザとデバイスの SGT 属性を受信できます。デバイスは、次にセキュリティ グループ アクセス コントロール リスト（SGACL）強制のために、送信元トラフィックをタグ付けする TrustSec にハードウェアで対応しているデバイスに、sourceIP-to-SGT バインディングを転送できます。

リンクの両端で 802.1AE MACsec をサポートしている場合、SAP ネゴシエーションが実行されます。サプリカントとオーセンティケータの間で EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティパラメータの交換、およびキーの管理が実行されます。これらの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョンとライセンスおよびリンク ハードウェア サポートに応じて、SAP ネゴシエーションは次の動作モードの 1 つを使用できます。

- Galois Counter Mode（GCM）：認証と暗号化
- GCM authentication（GMAC）：GCM 認証、暗号化なし
- No Encapsulation：カプセル化なし（クリア テキスト）
- null：カプセル化、認証または暗号化なし

Cisco TrustSec の機能情報

表 *162 : Cisco TrustSec* の機能情報

機能名	リリース	機能情報
• NDAC • SXPv1、SXPv2 • SGT • SGACL レイヤ 2 の適用 • SGT および VLAN から SGT へのマッピングのインターフェイス • サブネットと SGT のマッピング • レイヤ 3 ポート マッピング（PM） • レイヤ 3 アイデンティティ ポート マッピング（IPM） • セキュリティグループ名のダウンロード • SXP ループ検出 • ポリシーベースの CoA	Cisco IOS XE 3.3SE	これらの機能は、Catalyst 3850 および 3650 スイッチ、Cisco 5700 シリーズ Wireless LAN コントローラで追加されました。
SXPv1 および SXPv2	Cisco IOS XE 15.0(2)EX	SXP は Catalyst 2960-X スイッチで追加されています。
SXPv1 および SXPv2	Cisco IOS XE 15.0(2)EX1	SXP は Catalyst 2960-XR スイッチで追加されています。

第 114 章

コントロール プレーン ポリシングの設定

- 機能情報の確認 （2559 ページ）
- CoPP の制約事項 （2559 ページ）
- コントロール プレーン ポリシングに関する情報 （2560 ページ）
- CoPP の設定方法 （2564 ページ）
- CoPP の設定例 （2568 ページ）
- CoPP のモニタリング （2571 ページ）
- CoPP に関する追加情報 （2572 ページ）
- CoPP の機能履歴と情報 （2573 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

CoPP の制約事項

コントロール プレーン ポリシング（CoPP）の制約事項は、次のとおりです。

- 入力 CoPP だけがサポートされます。**system-cpp-policy** ポリシー マップは、入力方向でのみ、コントロール プレーン インターフェイスで使用可能です。
- コントロール プレーン インターフェイスにインストールできるのは、**system-cpp-policy** ポリシー マップのみです。

- **system-cpp-policy** ポリシー マップおよび 17 個のシステム定義のクラスは、変更または削除することはできません。
- **system-cpp-policy** ポリシー マップの下で許可されるのは、**police** アクションのみです。さらに、**police rate** は、パケット/秒単位（pps）でのみ設定できます。
- 1 つ以上の CPU キューがそれぞれのクラス マップの一部となります。複数の CPU キューが 1 つのクラスマップに属している場合、クラスマップのポリサー レートを変更すると、そのクラス マップに属しているすべての CPU キューに影響します。同様に、クラス マップを無効にすると、そのクラスマップに属するすべてのキューが無効になります。各クラス マップに属する CPU キューの詳細については、表 163 : CoPP のシステム定義された値（2562 ページ） を参照してください。

関連トピック

CPU キューの有効化またはポリサー レートの変更 （2564 ページ）
CPU キューの無効化 （2566 ページ）
すべての CPU キューに対するデフォルトのポリサー レートの設定 （2567 ページ）
ユーザ設定可能な CoPP の特徴 （2564 ページ）

コントロール プレーン ポリシングに関する情報

この章では、コントロール プレーン ポリシング（CoPP）が デバイス で機能する仕組みと、それを設定する方法について説明します。

CoPP の概要

CoPP 機能によって、不要なトラフィックまたは DoS トラフィックから CPU を保護し、コントロール プレーンおよび管理トラフィックを優先させることにより、デバイス のセキュリティが向上します。

デバイス は通常、3 つの操作プレーンにセグメント化され、それぞれに独自の目的があります。

- データ パケットを転送するための、データ プレーン。
- データを適切にルーティングするための、コントロール プレーン。
- ネットワーク要素を管理するための、管理プレーン。

CoPP を使用することで、大半の CPU 行きトラフィックを保護し、ルーティングの安定性と信頼性を確保し、パケットを確実に配信することができます。特に重要なのは、DoS 攻撃から CPU を保護するために CoPP を使用できることです。

CoPP は、モジュラ QoS コマンドライン インターフェイス（MQC）および CPU キューを使用して、これらの目的を達成します。さまざまなタイプのコントロール プレーン トラフィックが特定の条件に基づいてグループ化され、CPU キューに割り当てられます。ハードウェアに専用のポリサーを設定することで、これらの CPU キューを管理できます。たとえば、特定の CPU

キュー（トラフィック タイプ）のポリサー レートを変更したり、特定のタイプのトラフィックに対するポリサーを無効にしたりできます。

ポリサーはハードウェアに設定されていますが、CoPP は CPU のパフォーマンスやデータ プレーンのパフォーマンスには影響しません。しかし、CPU に着信するパケット数は制限されるため、CPU 負荷が制御されます。これは、ハードウェアからのパケットを待っているサービスが、より制御された着信パケットのレート（ユーザ設定可能なレート）を確認する可能性があることを意味します。

システム定義の CoPP の特徴

デバイス の初回の電源投入時は、システムによって次のタスクが自動的に実行されます。

- ポリシー マップ **system-cpp-policy** を検索します。このポリシー マップが検出されなかった場合は、ポリシーマップが作成され、コントロールプレーンにインストールされます。
- **system-cpp-policy** の下に 17 のクラス マップを作成します。

  次に デバイス の電源を入れたときに、すでに作成済みのポリシーとクラス マップがシステムによって検出されます。
- ポリシーがインストールされると、（32 のうち）16 の CPU キューがデフォルトで有効になり、それぞれデフォルトのレートが設定されます。デフォルトで有効になっている CPU キューとそのデフォルト レートを 表 163 : CoPP のシステム定義された値 （2562 ページ）に示します。

次の表に、デバイス をロードしたときにシステムが作成するクラス マップを示します。各クラス マップに対応するポリサーと、各クラス マップの下にグループ化された 1 つ以上の CPU キューを示します。クラス マップとポリサーには 1 対 1 のマッピングがあり、1 つ以上の CPU キューがクラス マップにマッピングします。

表 *163 : CoPP* のシステム定義された値

クラス マップ名	ポリサーインデックス（ポリサー No.）	CPU キュー（キュー No.）	CPU キューがデフォルトで有効になっているか	デフォルトのポリサーレート：1 秒あたりのパケット数（pps）
system-cpp-police-data	WK_CPP_POLICE_DA TA(0)	WK_CPU_Q_ICMP_GEN(3) WK_CPU_Q_BROADCAST(12)	Yes	200
system-cpp-police-l2-control	WK_CPP_POLICE_L2_ CONTROL(1)	WK_CPU_Q_L2_CONTROL(1)	いいえ	500
system-cpp-police-routing-control	WK_CPP_POLICE_ROUTING_CONTROL(2)	WK_CPU_Q_ROUTING_CONTROL(4)	Yes	500
system-cpp-police-control-low-priority	WK_CPP_POLICE_CO NTROL_LOW_PRI(3)	WK_CPU_Q_ICMP_REDIRECT(6) WK_CPU_Q_GENERAL_PUNT(25)	いいえ	500
system-cpp-police-wireless-priority1	WK_CPP_POLICE_WI RELESS_PRIO_1(4)	WK_CPU_Q_WIRELESS_PRIO_1(8)	いいえ	1000
system-cpp-police-wireless-priority2	WK_CPP_POLICE_WI RELESS_PRIO_2(5)	WK_CPU_Q_WIRELESS_PRIO_2(9)	いいえ	1000
system-cpp-police-wireless-priority3-4-5	WK_CPP_POLICE_WI RELESS_PRIO_3(6)	WK_CPU_Q_WIRELESS_PRIO_3(10) WK_CPU_Q_WIRELESS_PRIO_4(11) WK_CPU_Q_WIRELESS_PRIO_5(7)	いいえ	1000
system-cpp-police-punt-webauth	WK_CPP_POLICE_PU NT_WEBAUTH(7)	WK_CPU_Q_PUNT_WEBAUTH(22)	いいえ	1000
system-cpp-police-topology-control	WK_CPP_POLICE_TOPOLOGY_CONTROL(8)	WK_CPU_Q_TOPOLOGY_CONTROL(15)	いいえ	13000
system-cpp-police-multicast	WK_CPP_POLICE_MULTICAST(9)	WK_CPU_Q_TRANSIT_TRAFFIC(18) WK_CPU_Q_MCAST_DATA(30)	Yes	500

クラス マップ名	ポリサーインデックス（ポリサー No.）	CPU キュー（キュー No.）	CPU キューがデフォルトで有効になっているか	デフォルトのポリサーレート：1 秒あたりのパケット数（pps）
system-cpp-police-sys-data	WK_CPP_POLICE_SYS _DATA (10)	WK_CPU_Q_LEARNING_CACHE_OVFL(13) WK_CPU_Q_CRYPTO_CONTROL(23) WK_CPU_Q_EXCEPTION(24) WK_CPU_Q_EGR_EXCEPTION(28) WK_CPU_Q_NFL_SAMPLED_DATA(26) WK_CPU_Q_GOLD_PKT(31) WK_CPU_Q_RPF_FAILED(19)	Yes	100
system-cpp-police-dot1x-auth	WK_CPP_POLICE_DOT1X(11)	WK_CPU_Q_DOT1X_AUTH(0)	いいえ	1000
system-cpp-police-protocol-snooping	WK_CPP_POLICE_PR	WK_CPU_Q_PROTO_SNOOPING(16)	いいえ	500
system-cpp-police-sw-forward	WK_CPP_POLICE_SW_FWD (13)	WK_CPU_Q_SW_FORW ARDING_Q(14) WK_CPU_Q_SGT_CACHE_FULL(27) WK_CPU_Q_LOGGING(21)	Yes	1000
system-cpp-police-forus	WK_CPP_POLICE_FORUS(14)	WK_CPU_Q_FORUS_ADDR_RESOLUTION(5) WK_CPU_Q_FORUS_TRAFFIC(2)	いいえ	1000
system-cpp-police-multicast-end-station	WK_CPP_POLICE_MULTICAST_SNOOPING(15)	WK_CPU_Q_MCAST_END_STA TION_SERVICE(20)	Yes	2000
system-cpp-default	WK_CPP_POLICE_DEFAULT_POLICER	WK_CPU_Q_DHCP_SNOOPING WK_CPU_Q_SHOW_FORWARD	いいえ	1000

ユーザ設定可能な CoPP の特徴

次のタスクを実行して、コントロール プレーン トラフィックを管理できます。

- CPU キューを有効または無効にします。

  CPU キューを有効にするには、**system-cpp-policy** ポリシー マップ内で、対応するクラス マップの下にポリサー アクション（パケット/秒単位）を設定します。

  CPU キューを無効にするには、**system-cpp-policy** ポリシー マップ内で、対応するクラス マップの下のポリサー アクションを削除します。

- **system-cpp-policy** ポリシー マップ内で、対応するクラス マップの下にポリサー レート アクション（パケット/秒単位）を設定することで、ポリサー レートを変更します。

- グローバル コンフィギュレーション モードで **cpp system-default** コマンドを入力することによって、CPU キューをデフォルト値に設定します。

関連トピック

CPU キューの有効化またはポリサー レートの変更 （2564 ページ）
CPU キューの無効化 （2566 ページ）
すべての CPU キューに対するデフォルトのポリサー レートの設定 （2567 ページ）
CoPP の制約事項 （2559 ページ）
例：CPU キューの有効化または CPU キューのポリサー レートの変更 （2568 ページ）
例：CPU キューの無効化 （2569 ページ）
例：すべての CPU キューに対するデフォルトのポリサー レートの設定 （2570 ページ）

CoPP の設定方法

CPU キューの有効化またはポリサー レートの変更

CPU キューを有効にし、CPU キューのポリサー レートを変更する手順は、同じです。手順は次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**policy-map** *policy-map-name*
	例：
	`Device(config)# policy-map system-cpp-policy`
	`Device(config-pmap)#`
		ポリシー マップ コンフィギュレーション モードを開始します。

ステップ 4	**class** *class-name*
	例：
	`Device(config-pmap)# class system-cpp-police-protocol-snooping`
	`Device(config-pmap-c)#`
		クラス アクション コンフィギュレーション モードを開始します。有効にする CPU キューに対応するクラスの名前を入力します。参照先 表 163 : CoPP のシステム定義された値 （2562 ページ）

ステップ 5	**police rate** *rate* **pps** 例： `Device(config-pmap-c)# police rate 100 pps`	指定したトラフィック クラスに対し、1 秒間に処理される着信パケット数の上限を指定します。 （注） 指定するレートは、指定したクラス マップに属するすべての CPU キューに適用されます。
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config | begin system-cpp-policy** 例： `Device# show running-config | begin system-cpp-policy`	さまざまなトラフィック タイプに設定されたレートを表示します。

関連トピック

ユーザ設定可能な CoPP の特徴 （2564 ページ）
CoPP の制約事項 （2559 ページ）
例：CPU キューの有効化または CPU キューのポリサー レートの変更 （2568 ページ）
例：CPU キューの無効化 （2569 ページ）

例：すべての CPU キューに対するデフォルトのポリサー レートの設定 （2570 ページ）

CPU キューの無効化

CPU キューを無効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**policy-map** *policy-map-name*
	例：
	`Device(config)# policy-map system-cpp-policy`
	`Device(config-pmap)#`
		ポリシー マップ コンフィギュレーション モードを開始します。

ステップ 4	**class** *class-name*
	例：
	`Device(config-pmap)# class system-cpp-police-protocol-snooping`
	`Device(config-pmap-c)#`
		クラス アクション コンフィギュレーション モードを開始します。無効にする CPU キューに対応するクラスの名前を入力します。参照先 表 163 : CoPP のシステム定義された値 （2562 ページ）

ステップ 5	**no police rate** *rate* **pps** 例： `Device(config-pmap-c)# no police rate 100 pps`	指定したトラフィック クラスの着信パケットの処理を無効にします。 （注） これにより、指定したクラス マップに属するすべての CPU キューが無効になります。
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show running-config | begin system-cpp-policy** 例： `Device# show running-config | begin system-cpp-policy`	さまざまなトラフィック タイプに設定されたレートを表示します。

関連トピック

ユーザ設定可能な CoPP の特徴 （2564 ページ）
CoPP の制約事項 （2559 ページ）
例：CPU キューの有効化または CPU キューのポリサー レートの変更 （2568 ページ）
例：CPU キューの無効化 （2569 ページ）
例：すべての CPU キューに対するデフォルトのポリサー レートの設定 （2570 ページ）

すべての CPU キューに対するデフォルトのポリサー レートの設定

すべての CPU キューのポリサー レートをデフォルトのレートに設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**cpp system-default**
	例：
	`Device(config)# cpp system-default`
	`Defaulting CPP : Policer rate for all classes will be set to their defaults`
		すべてのクラスのポリサー レートをデフォルトのレートに設定します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show platform hardware fed switch** *switch-number* **qos que stat internal cpu policer** 例： `Device# show platform hardware fed switch 1 qos que stat internal cpu policer`	さまざまなトラフィック タイプに設定されたレートを表示します。

関連トピック

ユーザ設定可能な CoPP の特徴 （2564 ページ）
CoPP の制約事項 （2559 ページ）
例：CPU キューの有効化または CPU キューのポリサー レートの変更 （2568 ページ）
例：CPU キューの無効化 （2569 ページ）
例：すべての CPU キューに対するデフォルトのポリサー レートの設定 （2570 ページ）

CoPP の設定例

例：CPU キューの有効化または CPU キューのポリサー レートの変更

次の例に、CPU キューを有効にする方法、または CPU キューのポリサー レートを変更する方法を示します。ここでは、**class system-cpp-police-protocol-snooping** CPU キューが有効になり、ポリサー レートは **100 pps** です。

```
Device> enable
Device# configure terminal
Device(config)# policy-map system-cpp-policy
Device(config-pmap)# class system-cpp-police-protocol-snooping
Device(config-pmap-c)# police rate 100 pps
Device(config-pmap-c)# end


Device# show running-config | begin system-cpp-policy

policy-map system-cpp-policy
 class system-cpp-police-data
  police rate 200 pps
 class system-cpp-police-sys-data
  police rate 100 pps
```

```
 class system-cpp-police-sw-forward
  police rate 1000 pps
 class system-cpp-police-multicast
  police rate 500 pps
 class system-cpp-police-multicast-end-station
  police rate 2000 pps
 class system-cpp-police-punt-webauth
 class system-cpp-police-l2-control
 class system-cpp-police-routing-control
  police rate 500 pps
 class system-cpp-police-control-low-priority
 class system-cpp-police-wireless-priority1
 class system-cpp-police-wireless-priority2
 class system-cpp-police-wireless-priority3-4-5
 class system-cpp-police-topology-control
 class system-cpp-police-dot1x-auth
 class system-cpp-police-protocol-snooping
  police rate 100 pps
 class system-cpp-police-forus
 class system-cpp-default

<output truncated>
```

関連トピック

CPU キューの有効化またはポリサー レートの変更 （2564 ページ）
CPU キューの無効化 （2566 ページ）
すべての CPU キューに対するデフォルトのポリサー レートの設定 （2567 ページ）
ユーザ設定可能な CoPP の特徴 （2564 ページ）

例：CPU キューの無効化

次に、CPU キューをディセーブルにする例を示します。ここでは、**class system-cpp-police-protocol-snooping** CPU キューが無効になります。

```
Device> enable
Device# configure terminal
Device(config)# policy-map system-cpp-policy
Device(config-pmap)# class system-cpp-police-protocol-snooping
Device(config-pmap-c)# no police rate 100 pps
Device(config-pmap-c)# end


Device# show running-config | begin system-cpp-policy

policy-map system-cpp-policy
 class system-cpp-police-data
  police rate 200 pps
 class system-cpp-police-sys-data
  police rate 100 pps
 class system-cpp-police-sw-forward
  police rate 1000 pps
 class system-cpp-police-multicast
  police rate 500 pps
 class system-cpp-police-multicast-end-station
  police rate 2000 pps
 class system-cpp-police-punt-webauth
 class system-cpp-police-l2-control
 class system-cpp-police-routing-control
```

```
 police rate 500 pps
 class system-cpp-police-control-low-priority
 class system-cpp-police-wireless-priority1
 class system-cpp-police-wireless-priority2
 class system-cpp-police-wireless-priority3-4-5
 class system-cpp-police-topology-control
 class system-cpp-police-dot1x-auth
 class system-cpp-police-protocol-snooping
 class system-cpp-police-forus
 class system-cpp-default

<output truncated>
```

関連トピック

CPU キューの有効化またはポリサー レートの変更 （2564 ページ）
CPU キューの無効化 （2566 ページ）
すべての CPU キューに対するデフォルトのポリサー レートの設定 （2567 ページ）
ユーザ設定可能な CoPP の特徴 （2564 ページ）

例：すべてのCPUキューに対するデフォルトのポリサーレートの設定

次に、すべての CPU キューのポリサー レートをデフォルトに設定し、その後に設定を確認する方法の例を示します。ユーザ定義のポリシーは、システムのデフォルトポリシーの上に適用されます。つまり、ユーザ定義のクラスマップに一致する制御トラフィックは、ユーザ定義の CPP ポリサー クラスの下の集約ポリサーに従います。ユーザ定義のトラフィック クラスの統計情報は、バイト単位で報告されます。

```
Device> enable
Device# configure terminal
Device(config)# cpp system-default
Defaulting CPP : Policer rate for all classes will be set to their defaults
Device(config)# end

Deviceshow platform hardware fed switch 1 qos queue stats internal cpu policer

(default) (set)
QId PlcIdx  Queue Name                 Enabled   Rate     Rate      Drop
----------------------------------------------------------------------------
0    11     DOT1X Auth                   No      1000      1000        0
1    1      L2 Control                   No      500       400         0
2    14     Forus traffic                No      1000      1000        0
3    0      ICMP GEN                     Yes     200       200         0
4    2      Routing Control              Yes     1800      1800        0
5    14     Forus Address resolution     No      1000      1000        0
6    3      Punt Copy to ICMP Redirect   No      500       400         0
7    6      WLESS PRI-5                  No      1000      1000        0
8    4      WLESS PRI-1                  No      1000      1000        0
9    5      WLESS PRI-2                  No      1000      1000        0
10   6      WLESS PRI-3                  No      1000      1000        0
11   6      WLESS PRI-4                  No      1000      1000        0
12   0      BROADCAST                    Yes     200       200         0
13   10     Learning cache ovfl          Yes     100       200         0
14   13     Sw forwarding                Yes     1000      1000        0
15   8      Topology Control             No      13000     13000       0
16   12     Proto Snooping               No      500       400         0
17   16     DHCP Snooping                No      1000      1000        0
18   9      Transit Traffic              Yes     500       400         0
```

```
19   10     RPF Failed                    Yes     100       200         0
20   15     MCAST END STATION             Yes     2000      2000        0
21   13     LOGGING                       Yes     1000      1000        0
22   7      Punt Webauth                  No      1000      1000        0
23   10     Crypto Control                Yes     100       200         0
24   10     Exception                     Yes     100       200         0
25   3      General Punt                  No      500       400         0
26   10     NFL SAMPLED DATA              Yes     100       200         0
27   2      Low Latency                   Yes     1800      1800        0
28   10     EGR Exception                 Yes     100       200         0
29   16     Nif Mgr                       No      1000      1000        0
30   9      MCAST Data                    Yes     500       400         0
31   10     Gold Pkt                      Yes     100       200         0
```

関連トピック

CPU キューの有効化またはポリサー レートの変更 （2564 ページ）
CPU キューの無効化 （2566 ページ）
すべての CPU キューに対するデフォルトのポリサー レートの設定 （2567 ページ）
ユーザ設定可能な CoPP の特徴 （2564 ページ）

CoPP のモニタリング

CPU キューのトラフィック タイプやポリサー レート（ユーザが設定したレートやデフォルトのレート）などのポリサー設定を表示するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show platform hardware fed switch** *switch-number* **qos que stat internal cpu policer**	さまざまなトラフィック タイプに設定されたレートを表示します。

例

```
Device> enable
Device# show platform hardware fed switch 3 qos queue stats internal cpu policer
                                                (default)   (set)
QId PlcIdx  Queue Name                 Enabled   Rate      Rate       Drop
-----------------------------------------------------------------------------
0    11     DOT1X Auth                   No      1000      1000         0
1    1      L2 Control                   No      500       500          0
2    14     Forus traffic                No      1000      1000         0
3    0      ICMP GEN                     Yes     200       200          0
```

```
4    2      Routing Control             Yes     1800      1800        0
5    14     Forus Address resolution    No      1000      1000        0
6    3      ICMP Redirect               No      500       500         0
7    6      WLESS PRI-5                 No      1000      1000        0
8    4      WLESS PRI-1                 No      1000      1000        0
9    5      WLESS PRI-2                 No      1000      1000        0
10   6      WLESS PRI-3                 No      1000      1000        0
11   6      WLESS PRI-4                 No      1000      1000        0
12   0      BROADCAST                   Yes     200       200         0
13   10     Learning cache ovfl         Yes     100       100         0
14   13     Sw forwarding               Yes     1000      1000        0
15   8      Topology Control            No      13000     13000       0
16   12     Proto Snooping              No      500       500         0
17   16     DHCP Snooping               No      1000      1000        0
18   9      Transit Traffic             Yes     500       500         0
19   10     RPF Failed                  Yes     100       100         0
20   15     MCAST END STATION           Yes     2000      2000        0
21   13     LOGGING                     Yes     1000      1000        0
22   7      Punt Webauth                No      1000      1000        0
23   10     Crypto Control              Yes     100       100         0
24   10     Exception                   Yes     100       100         0
25   3      General Punt                No      500       500         0
26   10     NFL SAMPLED DATA            Yes     100       100         0
27   2      SGT Cache Full              Yes     1800      1800        0
28   10     EGR Exception               Yes     100       100         0
29   16     Show frwd                   No      1000      1000        0
30   9      MCAST Data                  Yes     500       500         0
31   10     Gold Pkt                    Yes     100       100         0
```

CoPP に関する追加情報

関連資料

関連項目	マニュアル タイトル
MQC QoS コマンド、および CoPP **show** コマンド	Command Reference, Cisco IOS XE Denali 16.1.x (Catalyst 3850 Switches)

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

CoPP の機能履歴と情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

機能名	リリース	機能情報
コントロール プレーン ポリシング（CoPP）または CPP	Cisco IOS XE 3.2SE、	この機能が導入されました。
CoPP の CLI コンフィギュレーション	Cisco IOS XE Denali 16.1.2	この機能はユーザ設定可能です。CPU キューの有効化および無効化、ポリサー レートの変更、およびポリサー レートのデフォルトへの設定を行うための CLI 設定オプション。

第 115 章

ワイヤレス ゲスト アクセスの設定

- 機能情報の確認 （2575 ページ）
- ゲスト アクセスの前提条件 （2575 ページ）
- ゲスト アクセスの制約事項 （2576 ページ）
- ワイヤレス ゲスト アクセスについて （2576 ページ）
- 高速安全ローミング （2576 ページ）
- ゲスト アクセスを設定する方法 （2577 ページ）
- ゲスト アクセスの設定例 （2591 ページ）
- ゲスト アクセスに関する追加情報 （2598 ページ）
- ゲスト アクセスの機能履歴と情報 （2599 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ゲスト アクセスの前提条件

- すべてのモビリティ ピアは、階層モビリティ アーキテクチャに対して設定されている必要があります。
- WLAN 上のゲスト コントローラ モビリティ アンカーの設定は、モビリティ エージェントおよびゲスト コントローラ上である必要があります。

- ゲスト アクセスは、3 ボックス ソリューションまたは 2 ボックス ソリューションが可能です。モビリティ トンネルのリンク ステータスは、以下の間で適用される必要があります。
  - モビリティ エージェント、モビリティ コントローラおよびゲスト コントローラ。

  または

  - モビリティ エージェント/モビリティ コントローラおよびゲスト コントローラ。

ゲスト アクセスの制約事項

ワイヤレス ゲスト アクセスについて

理想としては、ワイヤレス ゲスト ネットワークの実装で、企業の既存のワイヤレスおよび有線インフラストラクチャを最大限活用して、物理オーバーレイ ネットワークを構築する際のコストや複雑さを回避します。この場合は、次の要素と機能の追加が必要になります。

- 専用のゲスト WLAN/SSID：ゲストアクセスを必要とするあらゆる場所で、キャンパス ワイヤレス ネットワークを介して実装されます。ゲスト WLAN は、モビリティ アンカー（ゲスト コントローラ）が設定された WLAN で識別されます。
- ゲスト トラフィックのセグメンテーション：ゲストの移動場所を制限するために、キャンパス ネットワーク上のレイヤ 2 またはレイヤ 3 での実装テクニックを必要とします。
- アクセス コントロール：キャンパス ネットワーク内に組み込まれたアクセス コントロール機能の使用、または企業ネットワークからインターネットへのゲストアクセスを制御する外部プラットフォームの実装を伴います。
- ゲスト ユーザ資格情報の管理：スポンサーまたは Lobby 管理者がゲストの代わりに仮の資格情報を作成できるプロセス。この機能は、アクセス コントロール プラットフォーム内に常駐している場合と、AAA などの管理システムのコンポーネントになっている場合とがあります。

高速安全ローミング

高速セキュア ローミングは、Cisco Centralized Key Management（CCKM）、および 802.11i クライアントの Pairwise Master Key（PMK）情報をキャッシュすることで実現できます。Cisco Centralized Key Management（CCKM）はローミングの向上に役立ちます。クライアントのみがローミング プロセスを開始できますが、以下のような要因に影響されます。

- AP 間のオーバーラップ
- AP 間の距離
- チャネル、シグナル強度、および AP 上のロード
- データ レートと出力電力

高速ローミング クライアント（802.11i、[CCKM]）が新しいデバイスにローミングする場合は常に、クライアントは高速ローミング後にモビリティ「ハンドオフ」手順を実行します。また、モビリティ「ハンドオフ」手順後に学習した AAA 属性が再適用されます。

クライアントが 802.11i WPA2、CCKM、を使用している場合、高速セキュア ローミングの要件をすべて満たすために、ローミング中の完全な L2 認証を避ける必要があります。完全な L2 認証を避けるため、認証およびローミング クライアントのキーの継承に PMK キャッシュ（802.11i、 CCKM、）が使用されます。これには、モビリティ グループ内のモビリティ アンカー（MA）およびモビリティ コントローラ（MC）が同じ PMK キャッシュ値を持つことが必要です。

セッション タイムアウトは、PMK キャッシュの有効期限を定義します。クライアントが再認証に失敗した場合、または CLI から手動で削除された場合、PMK キャッシュも削除される場合があります。オリジナルのコントローラまたはスイッチの削除は、同じモビリティ グループ内の他のコントローラまたはスイッチにも影響します。

ゲスト アクセスを設定する方法

ロビー管理者アカウントの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**user-name** *user-name* 例： `Device (config)# user-name lobby`	ユーザ アカウントを作成します。
ステップ 3	**type lobby-admin** 例： `Device (config-user-name)# type lobby-admin`	ロビー管理者としてアカウント タイプを指定します。
ステップ 4	**password 0** *password* 例： `Device(config-user-name)# password 0 lobby`	ロビー管理者アカウントのパスワードを作成します。
ステップ 5	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device (config-user-name)# end`	
ステップ 6	**show running-config | section** *user-name* または **show running-config | section** 設定したロビー管理者のユーザ名 例： `Device # show running-config | section lobby`	設定の詳細を表示します。

例

ゲスト ユーザ アカウントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**user-name** *user-name* 例： `Device (config)# user-name guest`	Lobby Ambassador アカウントのユーザ名を作成します。
ステップ 3	**password** *unencrypted/hidden-password password* 例： `Device (config-user-name)# password 0 guest`	ユーザのパスワードを指定します。
ステップ 4	**type network-user description** *description* **guest-user lifetime year** *0-1* **month** *0-11* **day** *0-30* **hour** *0-23* **minute** *0-59* **second** *0-59* 例： `Device (config-user-name)# type network-user description guest guest-user lifetime year 1 month 10 day 3 hour 1 minute 5 second 30`	ユーザのタイプを指定します。
ステップ 5	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device (config-user-name)# end`	
ステップ 6	**show aaa local netuser all** 例： `Device # show aaa local netuser all`	設定の詳細を表示します。有効期間後に、ゲスト タイプとユーザ名は削除され、ゲスト ユーザ名と関連付けられるクライアントは認証解除されます。
ステップ 7	**show running-config | section***user-name* 例： `Device # show running-config | section guest`	設定の詳細を表示します。

例

モビリティ エージェント（MA）の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless mobility controller ip***mc-ipaddress* **public-ip** *mc-publicipaddress* 例： `Device (config) # wireless mobility controller ip27.0.0.1 public-ip 27.0.0.1`	MA が関連付けられるモビリティ コントローラを設定します。
ステップ 3	**wlan** *wlan-name wlan-id ssid* 例： `Device (config) # wlan mywlan 34 mywlan-ssid`	• *wlan-name* には、プロファイル名を入力します。範囲は 1 ～ 32 文字です。 • *wlan-id* には WLAN ID を入力します。範囲は 1 ～ 512 です。 • *ssid* では、この WLAN に対する Service Set Identifier（SSID）を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。

	コマンドまたはアクション	目的
ステップ 4	**client vlan id***vlan-group name/vlan-id* 例： `Device (config-wlan) # client vlan VLAN0136`	WLAN の VLAN ID またはグループを設定します。
ステップ 5	**no security wpa** 例： `Device (config-wlan) # no security wpa`	セキュリティ設定は GC で作成された WLAN で同じである必要があります。この例はオープン認証を対象としています。オープンおよび webauth などの他のセキュリティタイプに対して、適切なコマンドを提供する必要があります。
ステップ 6	**mobility anchor** *ipaddress* 例： `Device (config-wlan) # mobility anchor 9.3.32.2`	ゲストコントローラをモビリティアンカーとして設定します。
ステップ 7	**aaa-override** 例： `Device (config-wlan) # aaa-override`	（任意）AAA オーバーライドをイネーブルにします。AAA オーバーライドは、AAA 属性を優先する必要が生じたときのために、非オープン認証で要求されます。ゲストユーザを有効期限が切れた後に認証解除する必要があるか、AAA オーバーライド属性をユーザに与える必要がある場合にのみ必要です。
ステップ 8	**no shutdown** 例： `Device(config-wlan) # no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `Device (config) # end`	特権 EXEC モードに戻ります。
ステップ 10	**show wireless mobility summary** 例： `Device # show wireless mobility summary`	モビリティ コントローラの IP アドレス、およびモビリティ トンネルのステータスを確認します。
ステップ 11	**show wlan name** *wlan-name/id* 例： `Device # show wlan name mywlan`	モビリティアンカーの設定を表示します。

例

モビリティ コントローラの設定

モビリティ コントローラ モードは **wireless mobility controller** コマンドを使用してイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless mobility group member ip** *ip-address* **public-ip** *ip-address* **group** *group-name* 例： `Device (config) # wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test`	MC グループ内のすべてのピアを追加します。*ip-address* は、ゲスト コントローラの IP アドレスである必要があります。
ステップ 3	**wireless mobility controller peer-group** *peer-group-name* 例： `Device (config) # wireless mobility controller peer-group pg`	スイッチのピア グループを作成します。
ステップ 4	**wireless mobility controller peer-group** *peer-group-name* **member ip** *ipaddress* **public-ip** *ipaddress* 例： `Device (config) # wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip 9.7.136.10`	スイッチのピア グループに MA を追加します。
ステップ 5	**end** 例： `Device (config) # end`	特権 EXEC モードに戻ります。
ステップ 6	**show wireless mobility summary** 例： `Device # show wireless mobility summary`	設定の詳細を表示します。

例

Web 認証証明書の入手

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**crypto pki import** *trustpoint name* **pkcs12 tftp:** *passphrase* 例： `Device (config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco`	証明書をインポートします。
ステップ 3	**end** 例： `Device (config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show crypto pki** *trustpoints cert* 例： `Device # show crypto pki trustpoints cert`	設定の詳細を表示します。

例

Web 認証証明書の表示

手順

	コマンドまたはアクション	目的
ステップ 1	**show crypto ca certificate verb** 例： `Device # show crypto ca certificate verb`	現在の Web 認証証明書の詳細を表示します。

例

デフォルトの Web 認証ログイン ページの選択

AAA オーバーライド フラグは、ローカルまたはリモート AAA サーバを使用した Web 認証のために、WLAN でイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map type webauth** *parameter-map name* 例： `Device (config) # parameter-map type webauth test`	web-auth パラメータ マップを設定します。
ステップ 3	**wlan** *wlan-name* 例： `Device (config) # wlan wlan10`	wlan-name に、プロファイル名を入力します。範囲は 1 ～ 32 文字です。
ステップ 4	**shutdown** 例： `Device (config) # shutdown`	WLAN をディセーブルにします。
ステップ 5	**security web-auth** 例： `Controller (config-wlan) # security web-auth`	WLAN の Web 認証をイネーブルにします。
ステップ 6	**security web-auth authentication-list** *authentication list name* 例： `Controller (config-wlan) # security web-auth authentication-list test`	認証リスト名と Web 認証 WLAN のマップを可能にします。
ステップ 7	**security web-auth parameter-map** *parameter-map name* 例： `Device (config) # security web-auth parameter-map test`	パラメータ マップ名と Web 認証 WLAN のマップを可能にします。

	コマンドまたはアクション	目的
ステップ 8	**no shutdown** 例： `Device (config) # no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `Device (config) # end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config | section** *wlan-name* 例： `Device# show running-config | section mywlan`	設定の詳細を表示します。
ステップ 11	**show running-config | section parameter-map type webauth** *parameter-map* 例： `Device# show running-config | section parameter-map type webauth test`	設定の詳細を表示します。

例

外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択

AAA オーバーライド フラグは、ローカルまたはリモート AAA サーバを使用した Web 認証のために、WLAN でイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map type webauth global** 例： `Device (config) # parameter-map type webauth global`	グローバル webauth タイプ パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 3	**virtual-ip {ipv4 | ipv6}** *ip-address* 例： `Device (config-params-parameter-map) # virtual-ip ipv4 1.1.1.1`	仮想 IP アドレスを設定します。
ステップ 4	**parameter-map type webauth** *parameter-map name* 例： `Device (config-params-parameter-map) # parameter-map type webauth test`	webauth タイプ パラメータを設定します。
ステップ 5	**type {authbypass | consent | webauth | webconsent}** 例： `Device (config-params-parameter-map) # type webauth`	consent、passthru、webauth、または webconsent など WebAuth のサブタイプを設定します。
ステップ 6	**redirect [for-login|on-success|on-failure]** *URL* 例： `Device (config-params-parameter-map) # redirect for-login http://9.1.0.100/login.html`	ログイン ページ、成功ページおよび失敗ページのリダイレクト URL を設定します。
ステップ 7	**redirect portal {ipv4 | ipv6}** *ip-address* 例： `Device (config-params-parameter-map) # redirect portal ipv4 23.0.0.1`	外部ポータルの IPv4 アドレスを設定します。
ステップ 8	**end** 例： `Device (config-params-parameter-map) # end`	特権 EXEC モードに戻ります。
ステップ 9	show running-config | section parameter-map 例： `Device # show running-config | section parameter-map`	設定の詳細を表示します。

例

WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map type webauth** *parameter-map-name* 例： `Device (config) # parameter-map type webauth test`	webauth タイプ パラメータを設定します。
ステップ 3	**custom-page login device** *html-filename* 例： `Device (config-params-parameter-map)# custom-page login device flash:login.html`	Web 認証カスタマイズ ログイン ページに対するファイル名を指定できます。
ステップ 4	**custom-page login expired** *html-filename* 例： `Device (config-params-parameter-map)# custom-page login expired device flash:loginexpired.html`	Web 認証カスタマイズ ログイン期限切れページのファイル名を指定することを可能にします。
ステップ 5	**custom-page failure device** *html-filename* 例： `Device (config-params-parameter-map)# custom-page failure device device flash:loginfail.html`	Web認証カスタマイズログイン失敗ページに対するファイル名を指定できます。
ステップ 6	**custom-page success device** *html-filename* 例： `Device (config-params-parameter-map)# custom-page success device device flash:loginsuccess.html`	Web認証カスタマイズログイン成功ページに対するファイル名を指定できます。
ステップ 7	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device (config-params-parameter-map)# end`	
ステップ 8	**show running-config | section parameter-map type webauth** *parameter-map* 例： `Device (config) # show running-config | section parameter-map type webauth test`	設定の詳細を表示します。

例

AAA-Override の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan-name* 例： `Device (config) # wlan ramban`	*wlan-name* にはプロファイル名を入力します。範囲は 1 ～ 32 文字です。
ステップ 3	**aaa-override** 例： `Device (config-wlan) # aaa-override`	WLAN の AAA オーバーライドをイネーブルにします。
ステップ 4	**end** 例： `Device (config-wlan) # end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config | section** *wlan-name* 例： `Device # show running-config | section ramban`	設定の詳細を表示します。

例

クライアントの負荷分散の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan-name* 例： `Device (config)# wlan ramban`	*wlan-name* にはプロファイル名を入力します。
ステップ 3	**shutdown** 例： `Device (config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 4	**mobility anchor** *ip-address1* 例： `Device (config-wlan) # mobility anchor 9.7.136.15`	ゲスト コントローラをモビリティ アンカーとして設定します。
ステップ 5	**mobility anchor** *ip-address2* 例： `Device (config-wlan) # mobility anchor 9.7.136.16`	ゲスト コントローラをモビリティ アンカーとして設定します。
ステップ 6	**no shutdown wlan** 例： `Device (config-wlan) # no shutdown wlan`	WLAN をイネーブルにします。
ステップ 7	**end** 例： `Device (config-wlan) # end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config | section** *wlan-name* 例： `Device # show running-config | section ramban`	設定の詳細を表示します。

例

事前認証 ACL の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan-name* 例： `Device (config)# wlan ramban`	*wlan-name* にはプロファイル名を入力します。
ステップ 3	**shutdown** 例： `Device (config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 4	**ip access-group web** *preauthrule* 例： `Device (config-wlan)# ip access-group web preauthrule`	認証前に適用する必要のある ACL を設定します。
ステップ 5	**no shutdown** 例： `Device (config)# no shutdown`	WLAN をイネーブルにします。
ステップ 6	**end** 例： `Device (config-wlan)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show wlan name** *wlan-name* 例： `Device# show wlan name ramban`	設定の詳細を表示します。

例

IOS ACL 定義の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip access-list extended** *access-list number* 例： `Device (config) # ip access-list extended 102`	拡張 IP アクセス リストを設定します。
ステップ 3	**permit udp any eq** *port number* **any** 例： `Device (config-ext-nacl) # permit udp any eq 8080 any`	宛先ホストを設定します。
ステップ 4	**end** 例： `Device (config-wlan) # end`	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** *ACL 番号* 例： `Device # show access-lists 102`	設定の詳細を表示します。

例

Webpassthrough の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**parameter-map type webauth** *parameter-map name* 例： `Device (config) # parameter-map type webauth webparalocal`	webauth タイプ パラメータを設定します。
ステップ 3	**type consent** 例： `Device (config-params-parameter-map) # type consent`	WebAuth タイプを同意として設定します。
ステップ 4	**end** 例： `Device (config-params-parameter-map) # end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config | section parameter-map type webauth** *parameter-map* 例： `Device (config) # show running-config | section parameter-map type webauth test`	設定の詳細を表示します。

例

ゲスト アクセスの設定例

例：Lobby Ambassador アカウントの作成

次の例は、Lobby Ambassador アカウントを設定する方法を示しています。

```
Device# configure terminal
Device(config)# user-name lobby
Device(config)# type lobby-admin
Device(config)# password 0 lobby
Device(config)# end
Device#  show running-config | section lobby
    user-name lobby
    creation-time 1351118727
    password 0 lobby
    type lobby-admin
```

例：Web 認証証明書の入手

次の例は、Web 認証証明書を取得する方法を示しています。

```
Device# configure terminal
Device(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco
Device(config)# end
Device# show crypto pki trustpoints cert
 Trustpoint cert:
    Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
          Serial Number (hex): 00
    Certificate configured.
Device# show  crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    Name: ldapserver
    e=rkannajr@cisco.com
    cn=ldapserver
    ou=WNBU
    o=Cisco
    st=California
    c=US
  Validity Date:
    start date: 07:35:23 UTC Jan 31 2012
    end   date: 07:35:23 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12
  Storage: nvram:rkannajrcisc#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
```

```
    o=Cisco
    l=SanJose
    st=California
    c=US
  Validity Date:
    start date: 07:27:56 UTC Jan 31 2012
    end   date: 07:27:56 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12 ldap
  Storage: nvram:rkannajrcisc#0CA.cer
```

例：Web 認証証明書の表示

次の例は、Web 認証証明書を表示する方法を示しています。

```
Device# show crypto ca certificate verb
     Certificate
     Status: Available
     Version: 3
     Certificate Serial Number (hex): 2A9636AC00000000858B
     Certificate Usage: General Purpose
     Issuer:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
    Subject:
    Name: WS-C3780-6DS-S-2037064C0E80
    Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
    cn=WS-C3780-6DS-S-2037064C0E80
    serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
    CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/cmca.crl
    Validity Date:
    start date: 15:43:22 UTC Aug 21 2011
    end   date: 15:53:22 UTC Aug 21 2021
    Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
    Signature Algorithm: SHA1 with RSA Encryption
    Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
    Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
    X509v3 extensions:
    X509v3 Key Usage: F0000000
      Digital Signature
      Non Repudiation
      Key Encipherment
      Data Encipherment
    X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
    X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
    Authority Info Access:
    Associated Trustpoints: CISCO_IDEVID_SUDI
    Key Label: CISCO_IDEVID_SUDI
```

例：ゲスト ユーザ アカウントの設定

次の例は、ゲスト ユーザ アカウントを設定する方法を示しています。

```
Device# configure terminal
Device(config)# user-name guest
```

```
Device(config-user-name)# password 0 guest
Device(config-user-name)# type network-user description guest guest-user lifetime year
1 month 10 day 3 hour 1 minute 5 second 30
Device(config-user-name)# end
Device# show aaa local netuser all
User-Name           : guest
Type                : guest
Password            : guest
Is_passwd_encrypted : No
Descriptio          : guest
Attribute-List      : Not-Configured
First-Login-Time    : Not-Logged-In
Num-Login           : 0
Lifetime            : 1 years 10 months 3 days 1 hours 5 mins 30 secs
Start-Time          : 20:47:37 chennai Dec 21 2012
```

例：モビリティ コントローラの設定

次の例は、モビリティ コントローラを設定する方法を示しています。

```
Device# configure terminal
Device(config)# wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test
Device(config)# wireless mobility controller peer-group pg
Device(config)# wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip
 9.7.136.10
Device(config)# end
Device# show wireless mobility summary

Mobility Controller Summary:

Mobility Role                                   : Mobility Controller
Mobility Protocol Port                          : 16666
Mobility Group Name                             : default
Mobility Oracle                                 : Enabled
DTLS Mode                                       : Enabled

Mobility Keepalive Interval                     : 10
Mobility Keepalive Count                        : 3
Mobility Control Message DSCP Value             : 7
Mobility Domain Member Count                    : 3

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

IP              Public IP       Group Name      Multicast IP    Link Status
-------------------------------------------------------------------------------
9.9.9.2         -               default         0.0.0.0         UP   : UP
12.12.11.11     12.13.12.12     rasagna-grp                     DOWN : DOWN
27.0.0.1        23.0.0.1        test                            DOWN : DOWN

Switch Peer Group Name          : spg1
Switch Peer Group Member Count  : 0
Bridge Domain ID                : 0
Multicast IP Address            : 0.0.0.0

Switch Peer Group Name          : pg
Switch Peer Group Member Count  : 1
Bridge Domain ID                : 0
Multicast IP Address            : 0.0.0.0
```

```
IP               Public IP            Link Status
-----------------------------------------------------
9.7.136.10       9.7.136.10           DOWN : DOWN
```

例：デフォルトの Web 認証ログイン ページの選択

次の例は、デフォルトの Web 認証ログイン ページを選択する方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their
CPL control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly
 advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
Device(config)# wlan wlan50
Device(config-wlan)# shutdown
Device(config-wlan)# security web-auth authentication-list test
Device(config-wlan)# security web-auth parameter-map test
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show running-config | section wlan50
wlan wlan50 50 wlan50
 security wpa akm cckm
 security wpa wpa1
 security wpa wpa1 ciphers aes
 security wpa wpa1 ciphers tkip
 security web-auth authentication-list test
 security web-auth parameter-map test
 session-timeout 1800
 no shutdown

Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
 type webauth
```

例：外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択

次の例は、外部 Web サーバからカスタマイズされた Web 認証ログイン ページを選択する方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
Device(config-params-parameter-map)# parameter-map type webauth test
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
Device(config-params-parameter-map)# redirect portal ipv4 23.0.0.1
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
```

```
redirect portal ipv4 23.0.0.1
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

例：WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て

次の例は、WLAN ごとのログイン割り当て、ログイン失敗、およびログアウト ページを割り当てる方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type webauth test
Device(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
Device(config-params-parameter-map)# custom-page login expired device
flash:loginexpire.html
Device(config-params-parameter-map)# custom-page failure device flash:loginfail.html
Device(config-params-parameter-map)# custom-page success device flash:loginsucess.html
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 23.0.0.1
 custom-page login device flash:loginsantosh.html
 custom-page success device flash:loginsucess.html
 custom-page failure device flash:loginfail.html
 custom-page login expired device flash:loginexpire.html
```

例：AAA-Override の設定

次の例は、AAA-Override を設定する例を示しています。

```
Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# aaa-override
Device(config-wlan)# end
Device# show running-config | section fff
 wlan fff 44 fff
 aaa-override
 shutdown
```

例：クライアントの負荷分散の設定

次の例は、クライアントの負荷分散を設定する方法を示しています。

```
Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# mobility anchor 9.7.136.15
Device(config-wlan)# mobility anchor 9.7.136.16
Device(config-wlan)# no shutdown wlan
Device(config-wlan)# end
```

```
Device# show running-config | section fff
wlan fff 44 fff
 aaa-override
 shutdown
```

例：事前認証 ACL の設定

次の例は、事前認証 ACL を設定する方法を示しています。

```
Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# ip access-group web preauthrule
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show wlan name fff
```

例：IOS ACL 定義の設定

次に、IOS ACL 定義を設定する例を示します。

```
Device# configure terminal
Device(config)# ip access-list extended 102
Device(config-ext-nacl)# permit udp any eq 8080 any
Device(config-ext-nacl)# end
Device# show access-lists 102
 Extended IP access list 102
    10 permit udp any eq 8080 any
```

例：Webpassthrough の設定

次の例は、Webpassthrough を設定する方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type webauth webparalocal
Device(config-params-parameter-map)# type consent
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 23.0.0.1
```

ゲスト アクセスに関する追加情報

関連資料

関連項目	マニュアル タイトル
モビリティ CLI コマンド	『*Mobility Command Reference, Cisco IOS XE 3SE (Cisco WLC 5700 Series)*』
モビリティ設定	『*Mobility Configuration Guide, Cisco IOS XE 3SE (Cisco WLC 5700 Series)*』
セキュリティ CLI コマンド	『*Security Command Reference, Cisco IOS Release 3SE (Cisco WLC 5700 Series)*』
Catalyst 5700 シリーズ ワイヤレス コントローラの Web ベースの認証	『*Security Configuration Guide, Cisco IOS Release 3SE (Cisco WLC 5700 Series)*』
有線ゲスト アクセス設定およびコマンド	*Identity Based Networking Services*

標準および RFC

標準/RFC	Title
なし	-

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ゲスト アクセスの機能履歴と情報

リリース	機能情報
Cisco IOS XE Release 3.2SE	この機能が導入されました。

第 116 章

不正なデバイスの管理

- 機能情報の確認 （2601 ページ）
- 不正なデバイスについて （2602 ページ）
- 不正検出の設定方法 （2607 ページ）
- 不正検出のモニタリング （2609 ページ）
- 例：不正検出の設定 （2609 ページ）
- 不正検出に関する追加情報 （2610 ページ）
- 不正検出設定の機能履歴と情報 （2611 ページ）
- 機能情報の確認 （2611 ページ）
- 不正なデバイスについて （2611 ページ）
- 不正検出の設定方法 （2617 ページ）
- 不正検出のモニタリング （2619 ページ）
- 例：不正検出の設定 （2619 ページ）
- 不正検出に関する追加情報 （2620 ページ）
- 不正検出設定の機能履歴と情報 （2621 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

不正なデバイスについて

不正なアクセスポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセスポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連のクリア ツー センド（CTS）フレームを送信できるようになります。アクセスポイントになりすまして、特定のクライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。無線 LAN サービス プロバイダーは、空間からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、認可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正アクセスポイントは、企業のファイアウォールの内側にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、セキュリティで保護されていないアクセスポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

次に、不正なデバイスの管理に関する注意事項を示します。

- 許可とアソシエーションの検出後、ただちに阻止フレームが送信されます。強化された不正阻止アルゴリズムを使用すると、アドホック クライアントをより効果的に阻止することができます。
- ローカル モード アクセス ポイントは、関連付けられたクライアントに対応するように設計されています。これらのアクセス ポイントは比較的短時間でオフチャネル スキャンを実行します（各チャネル約 50 ミリ秒）。高度な不正検出を実行するには、監視モードのアクセス ポイントを使用する必要があります。あるいは、スキャン間隔を 180 秒から 120 または60秒などに短縮して、無線がオフチャネルになる頻度を増やします。これにより、不正が検出される可能性は増加します。ただしこの場合も、アクセスポイントが各チャネルに費やす時間は約 50 ミリ秒です。
- 家庭の環境で展開されるアクセスポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。
- クライアントカードの実装により、アドホックの抑制の効果が低下することがあります。
- 不正なアクセス ポイントの分類および報告は、不正の状態と、不正なアクセス ポイントの状態を自動的に移行できるようにする、ユーザ定義の分類規則に従って行うことができます。
- 各コントローラは、不正アクセスポイントの封じ込めを無線チャンネルごとに3台（監視モード アクセス ポイントの場合、無線チャネルごとに 6 台）に制限します。

- Rogue Location Discovery Protocol（RLDP）は、オープン認証に設定されている不正なアクセス ポイントを検出します。
- RLDP はブロードキャスト Basic Service Set Identifier（BSSID）を使用する不正なアクセス ポイント（つまり Service Set Identifier をビーコンでブロードキャストするアクセス ポイント）を検出します。
- RLDP は、同じネットワークにある不正なアクセス ポイントのみを検出します。ネットワークのアクセス リストによって不正なアクセス ポイントからコントローラへの RLDP のトラフィックの送信が阻止されている場合は、RLDP は機能しません。
- RLDP は 5 GHz の動的周波数選択（DFS）チャネルでは機能しません。ただし RLDP は、管理対象のアクセス ポイントが DFS チャネルの監視モードである場合には機能します。
- メッシュ AP で RLDP が有効にされていて、その AP が RLDP タスクを実行すると、そのメッシュ AP のアソシエーションはコントローラから解除されます。回避策は、メッシュ AP で RLDP を無効にすることです。
- RLDP が監視モードではない AP で有効になっている場合、RLDP の処理中にクライアント接続の中断が発生します。
- 不正を手動で阻止すると、不正なエントリは期限切れになった後でも保持されます。
- 不正を自動、ルール、AwIPS などの他の防御方法で阻止すると、不正なエントリは期限切れになると削除されます。
- コントローラは、不正なクライアントの検証を AAA サーバに一度だけ要求します。その結果、不正なクライアント検証が最初の試行で失敗すると、不正なクライアントは今後脅威として検出されなくなります。これを回避するには、[**Validate Rogue Clients Against AAA**] を有効にする前に、認証サーバに有効なクライアント エントリを追加します。
- 7.4 以前のリリースでは、ルールによってすでに分類された不正は再分類されませんでした。7.5 リリースでは、不正ルールの優先順位に基づいて不正を再分類できるようにこの動作が強化されました。優先順位は、コントローラが受信する不正レポートを使用して決定されます。
- WLAN、LAN、11a 無線および 11bg 無線の不正な AP の MAC アドレスは、不正 BSSID の +/- 1 の差異で設定されているので、不正検出 AP は、5Mhz チャネルの不正な有線 AP の関連付けおよび阻止に失敗します。8.0 リリースでは、MAC アドレスの範囲を広げることによって、この動作が強化されました。不正検出 AP は有線 ARP MAC と不正 BSSID を +/- 3 の差異で関連付けます。
- オープン認証を使用する不正アクセス ポイントはネットワーク上で検出できます。NAT 有線または不正有線検出は、WLC（RLDP と不正検出 AP の両方）ではサポートされません。非隣接 MAC アドレスは、RLDP ではなく AP の不正検出モードでサポートされます。
- ハイ アベイラビリティのシナリオでは、不正検出セキュリティ レベルを高か重要に設定すると、スタンバイ Cisco WLC の不正タイマーは、不正検出保留の安定時間の 300 秒が過ぎないと開始しません。したがって、スタンバイ Cisco WLC のアクティブ設定が反映されるのは、300 秒が過ぎてからです。

（注） 不正AP、不正クライアント、または一時的な封じ込めの設定は、リロード時に破棄されます。リロード後にすべての不正を再設定する必要があります。

（注） 不正クライアントのトラップを制御するための独立したコマンドはありません。ただし、不正クライアントのトラップは、不正 AP でも使用する **config trapflags rogueap {enable | disable}** コマンドで有効、無効を切り替えることができます。GUI 設定でも、[Management] -> [SNMP] -> [TrapControl] -> [Security] -> [Rogue AP] で AP フラグを使用して、不正クライアントを制御してください。

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol（RLDP）は、不正 AP で認証が設定されていない（オープン認証）場合に使用される積極的なアプローチです。このモードは、デフォルトで無効になっており、不正チャネルに移動して、クライアントとして不正に接続するようにアクティブ AP に指示します。この間に、アクティブ AP は、接続されたすべてのクライアントに認証解除メッセージを送信してから、無線インターフェイスをシャットダウンします。次に、クライアントとして不正 AP にアソシエートします。その後で、AP は、不正 AP から IP アドレスの取得を試み、ローカル AP と不正接続情報を含む User Datagram Protocol（UDP）パケット（ポート 6352）を不正 AP を介してコントローラに転送します。コントローラがこのパケットを受信すると、不正 AP が RLDP 機能を使用して有線ネットワークで検出されたことをネットワーク管理者に通知するためのアラームが設定されます。

RLDP の不正 AP の検出精度は 100% です。オープン AP と NAT AP を検出します。

（注） Lightweight AP が不正 AP とアソシエートして DHCP アドレスを受信するかどうかを確認するには、**debug dot11 rldp enable** コマンドを使用します。このコマンドは、Lightweight AP からコントローラに送信された UDP パケットも表示します。

ここで、Lightweight AP から送信される UDP （宛先ポート 6352）パケットのサンプルを示します。0020 0a 01 01 0d 0a 01 .....(.*.....0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00 .....x.....0040 00 00 00 00 00 00 00 00 00 00

最初の 5 バイトのデータには、不正 AP によってローカル モード AP に割り当てられた DHCP アドレスが含まれています。次の 5 バイトはコントローラの IP アドレスで、その後に不正 AP MAC アドレスを表す 6 バイトが続きます。その後に、18 バイトの 0 が続きます。

ここで、RLDP の動作手順を示します。

1. 信号強度値を使用して不正に最も近い統合 AP を特定します。
2. その後で、この AP が WLAN クライアントとして不正に接続します。3 回のアソシエーションを試みて、成功しない場合はタイムアウトします。

3. アソシエーションが成功すると、AP が DHCP を使用して IP アドレスを取得します。
4. IP アドレスが取得されたら、AP（WLAN クライアントとして機能している）は、コントローラの IP アドレスのそれぞれに UDP パケットを送信します。
5. コントローラがクライアントから RLDP パケットの 1 つでも受信すると、その不正が重大度が critical の on-wire としてマークされます。

（注） コントローラのネットワークと不正デバイスが設置されたネットワークの間にフィルタリングルールが設定されている場合は、RLDP パケットがコントローラに到達できません。

RLDP の注意事項：

- RLDP は、認証と暗号化が無効になっている SSID をブロードキャストするオープン不正 AP でのみ動作します。
- RLDP では、クライアントとして機能しているマネージド AP が不正ネットワーク上で DHCP を介して IP アドレスを取得できる必要があります。
- 手動 RLDP を使用して、不正上で RLDP トレースを複数回試すことができます。
- RLDP プロセス中は、AP がクライアントにサービスを提供できません。これがローカルモード AP のパフォーマンスと接続に悪影響を及ぼします。この問題を回避するために、RLDP はモニタ モード AP に対してのみ選択的に有効にできます。
- RLDP は、5GHz DFS チャネルで動作する不正 AP への接続は試行しません。

（注） RLDP は、シスコの Atonomous 不正アクセス ポイントではサポートされていません。これらのアクセス ポイントは、RLDP クライアントによって送信された DHCP 検出要求をドロップします。また不正なアクセス ポイント チャネルが動的周波数選択（DFS）を必要とする場合、RLDP はサポートされません。自動 RLDP 試行で不正（ノイズの多い RF 環境などが原因）が検出されなかった場合は、コントローラが再試行しません。ただし、不正デバイス上で RLDP を手動で開始できます。

不正なデバイスの検出

コントローラは、近くにあるすべてのアクセス ポイントを継続的に監視し、不正なアクセス ポイントとクライアントに関する情報を自動的に検出および収集します。コントローラは不正なアクセス ポイントを検出すると、Rogue Location Discovery Protocol（RLDP）を使用し、不正検出モードのアクセス ポイントが接続されて、不正がネットワークに接続されているかどうかを特定します。

コントローラは、オープン認証および設定された不正デバイスで RLDP を開始します。RLDP が Flexconnect またはローカル モードのアクセス ポイントを使用すると、クライアントはその時点で接続を解除されます。RLDP のサイクルが終了すると、クライアントはアクセスポイン

トに再接続します。不正なアクセスポイントが検出された時点で（自動設定）、RLDPのプロセスが開始されます。

すべてのアクセス ポイント、または監視（リッスン専用）モードに設定されたアクセス ポイントでのみRLDPを使用するようにコントローラを設定できます。後者のオプションでは、混雑した無線周波数（RF）空間での自動不正アクセス ポイント検出が実現され、不要な干渉を生じさせたり、正規のデータ アクセス ポイント機能に影響を与えずにモニタリングを実行できます。すべてのアクセスポイントでRLDPを使用するようにコントローラを設定した場合、モニタ アクセス ポイントとローカル（データ）アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 動作に対してモニタ アクセス ポイントを選択します。ネットワーク上に不正があるとRLDPが判断した場合、検出された不正を手動または自動で阻止することを選択できます。

RLDPは、オープン認証に設定されている不正なアクセスポイントの存在をネットワーク上で一度だけ（デフォルト設定の再試行回数）検出します。再試行は **config rogue ap rldp retries** コマンドで設定できます。

3 種類の方法でコントローラから RLDP を開始またはトリガーできます。

1. コントローラの CLI から RLDP 開始コマンドを手動で入力します。RLDP を開始するための同等の GUI オプションはサポートされていません。

   config rogue ap rldp initiate *mac-address*

2. コントローラの CLI から RLDP をスケジュールします。RLDP をスケジュールするための同等の GUI オプションはサポートされていません。

   config rogue ap rldp schedule

3. 自動 RLDP。コントローラの CLI または GUI から自動 RLDP を設定できますが、次の注意事項を考慮してください。

   - 不正検出のセキュリティ レベルが custom に設定されている場合にのみ、自動 RLDP オプションを設定できます。
   - 自動 RLDP および RLDP のスケジュールを同時に有効にすることはできません。

不正なアクセス ポイントは、自動または手動で Contained 状態に変更されます。コントローラは、不正の阻止に最も効果的なアクセス ポイントを選択し、そのアクセス ポイントに情報を提供します。アクセスポイントは、無線あたりの不正阻止数のリストを保存します。自動阻止の場合は、監視モードのアクセス ポイントだけを使用するようにコントローラを設定できます。阻止動作は次の 2 つの方法で開始されます。

- コンテナ アクセス ポイントが定期的に不正阻止のリストを確認し、ユニキャスト阻止フレームを送信します。不正なアクセスポイントの阻止の場合、フレームは不正なクライアントがアソシエートされている場合にのみ送信されます。
- 阻止された不正アクティビティが検出されると、阻止フレームが送信されます。

個々の不正阻止には、一連のユニキャスト アソシエーション解除フレームおよび認証解除フレームの送信が含まれます。

Cisco Prime Infrastructure のインタラクションと不正検出

Cisco Prime Infrastructure ではルール ベースの分類がサポートされ、コントローラで設定された分類ルールが使用されます。コントローラは、次のイベント後に Cisco Prime Infrastructure にトラップを送信します。

- 不明なアクセス ポイントが Friendly 状態に初めて移行すると、コントローラは、不正の状態が Alert の場合にのみ Cisco Prime Infrastructure にトラップを送信します。不正の状態が Internal または External であると、トラップは送信されません。
- タイムアウトの経過後に不正なエントリが削除されると、Malicious（Alert、Threat）または Unclassified（Alert）に分類された不正なアクセス ポイントに関して、コントローラから Cisco Prime Infrastructure にトラップが送信されます。コントローラでは、不正の状態が Contained、Contained Pending、Internal、および External である不正なエントリは削除されません。

不正検出の設定方法

不正検出の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless wpsroguedetectionmin-rssi** *rssi in dBm* 例： `Device(config)# wireless wps rogue detection min-rssi 100`	不正に必要な最小 RSSI 値を指定します。これは、AP が不正を検出し、デバイスで不正エントリが作成されるために必要な値です。 rssi in dBm パラメータの有効範囲は –128 ～ –70 dBm で、デフォルト値は –128 dBm です。

	コマンドまたはアクション	目的
		（注） この機能は、すべてのAPモードに適用できます。RSSI値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、APが不正を検出する最小RSSI値を指定することで、このオプションを使用して不正をフィルタリングすることができます。
ステップ 3	**wireless wpsroguedetectionmin-transient-time** *time in seconds* 例： `Device(config)# wireless wps rogue detection min-transient-time`	不正が初めてスキャンされた後、AP で不正スキャンを連続的に実行する間隔を入力します。 time in sec パラメータの有効範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。 （注） この機能は、モニタ モードの AP のみに適用されます。 一時的な間隔値を使用して、APが不正をスキャンする間隔を制御できます。APでは、それぞれの一時的間隔値に基づいて、不正のフィルタリングも実行できます。 この機能には次の利点があります。 • APからコントローラへの不正レポートが短くなる • 一時的な不正エントリをコントローラで回避できる • 一時的な不正への不要なメモリ割り当てを回避できる
ステップ 4	**wireless wpsrogueclient** {**aaa** | **mse**} 例： `Device(config)# wireless wps rogue client aaa`	不正なクライアントが有効なクライアントかどうかを検証するために、AAAサーバまたはローカル データベース、または MSE を設定します。

	コマンドまたはアクション	目的
	`Device(config)# wireless wps rogue client mse`	
ステップ 5	**wireless wpsrogue apvalid-clientauto-contain** 例： `Device(config)# wireless wps rogue ap valid-client auto-contain`	信頼できるクライアントが関連付けられる不正なアクセス ポイントを自動的に阻止するように指定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

不正検出のモニタリング

この項では、不正検出の新しいコマンドについて説明します。

次のコマンドは、上で不正検出をモニタするために使用できます。

表 *164*：不正検出モニタリングのコマンド

コマンド	目的
show wireless wps rogue ap summary	によって検出されたすべての不正アクセスポイントのリストを表示します。
show wireless wps rogue client detailed *client-mac*	特定の不正クライアントの詳細情報を表示します。
show wireless wps rogue client summary	で検出されたすべての不正なクライアントのリストを表示します。
show nmsp capability	NMSP 機能を表示します。

例：不正検出の設定

この例は、検出された不正 AP が存在する必要がある最小 RSSI を、で作成されたエントリを持つように設定する方法を示しています。

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-rssi -100
Device(config)# end
Device# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

次に、分類インターバルを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-transient-time 500
Device(config)# end
Device# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

次に、不正なクライアントが有効なクライアントかどうかを検証するために MSE を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue client mse
Device(config)# end
Device# show wireless wps rogue client summary
```

次に、信頼できるクライアントが関連付けられる不正なアクセスポイントを自動的に阻止する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue ap valid-client auto-contain
Device(config)# end
Device# show wireless wps rogue ap summary
Device# show nmsp capability
```

不正検出に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

不正検出設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。
Cisco IOS XE 3E	MSE に対する不正な検証。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

不正なデバイスについて

不正なアクセス ポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセス ポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連のクリア ツー センド（CTS）フレームを送信できるようになります。アクセス ポイントになりすまして、特定のク

ライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。無線 LAN サービス プロバイダーは、空間からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、認可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正アクセスポイントは、企業のファイアウォールの内側にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、セキュリティで保護されていないアクセスポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

次に、不正なデバイスの管理に関する注意事項を示します。

- 許可とアソシエーションの検出後、ただちに阻止フレームが送信されます。強化された不正阻止アルゴリズムを使用すると、アドホック クライアントをより効果的に阻止することができます。
- ローカル モード アクセス ポイントは、関連付けられたクライアントに対応するように設計されています。これらのアクセス ポイントは比較的短時間でオフチャネル スキャンを実行します（各チャネル約 50 ミリ秒）。高度な不正検出を実行するには、監視モードのアクセス ポイントを使用する必要があります。あるいは、スキャン間隔を 180 秒から 120 または60秒などに短縮して、無線がオフチャネルになる頻度を増やします。これにより、不正が検出される可能性は増加します。ただしこの場合も、アクセスポイントが各チャネルに費やす時間は約 50 ミリ秒です。
- 家庭の環境で展開されるアクセスポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。
- クライアントカードの実装により、アドホックの抑制の効果が低下することがあります。
- 不正なアクセス ポイントの分類および報告は、不正の状態と、不正なアクセス ポイントの状態を自動的に移行できるようにする、ユーザ定義の分類規則に従って行うことができます。
- 各コントローラは、不正アクセスポイントの封じ込めを無線チャンネルごとに3台（監視モード アクセス ポイントの場合、無線チャネルごとに 6 台）に制限します。
- Rogue Location Discovery Protocol（RLDP）は、オープン認証に設定されている不正なアクセス ポイントを検出します。
- RLDP はブロードキャスト Basic Service Set Identifier（BSSID）を使用する不正なアクセスポイント（つまり Service Set Identifier をビーコンでブロードキャストするアクセス ポイント）を検出します。

- RLDP は、同じネットワークにある不正なアクセス ポイントのみを検出します。ネットワークのアクセス リストによって不正なアクセス ポイントからコントローラへの RLDP のトラフィックの送信が阻止されている場合は、RLDP は機能しません。
- RLDP は 5 GHz の動的周波数選択（DFS）チャネルでは機能しません。ただし RLDP は、管理対象のアクセス ポイントが DFS チャネルの監視モードである場合には機能します。
- メッシュ AP で RLDP が有効にされていて、その AP が RLDP タスクを実行すると、そのメッシュ AP のアソシエーションはコントローラから解除されます。回避策は、メッシュ AP で RLDP を無効にすることです。
- RLDP が監視モードではない AP で有効になっている場合、RLDP の処理中にクライアント接続の中断が発生します。
- 不正を手動で阻止すると、不正なエントリは期限切れになった後でも保持されます。
- 不正を自動、ルール、AwIPS などの他の防御方法で阻止すると、不正なエントリは期限切れになると削除されます。
- コントローラは、不正なクライアントの検証を AAA サーバに一度だけ要求します。その結果、不正なクライアント検証が最初の試行で失敗すると、不正なクライアントは今後脅威として検出されなくなります。これを回避するには、[**Validate Rogue Clients Against AAA**] を有効にする前に、認証サーバに有効なクライアント エントリを追加します。
- 7.4 以前のリリースでは、ルールによってすでに分類された不正は再分類されませんでした。7.5 リリースでは、不正ルールの優先順位に基づいて不正を再分類できるようにこの動作が強化されました。優先順位は、コントローラが受信する不正レポートを使用して決定されます。
- WLAN、LAN、11a 無線および 11bg 無線の不正な AP の MAC アドレスは、不正 BSSID の +/- 1 の差異で設定されているので、不正検出 AP は、5Mhz チャネルの不正な有線 AP の関連付けおよび阻止に失敗します。8.0 リリースでは、MAC アドレスの範囲を広げることによって、この動作が強化されました。不正検出 AP は有線 ARP MAC と不正 BSSID を +/- 3 の差異で関連付けます。
- オープン認証を使用する不正アクセス ポイントはネットワーク上で検出できます。NAT 有線または不正有線検出は、WLC（RLDP と不正検出 AP の両方）ではサポートされません。非隣接 MAC アドレスは、RLDP ではなく AP の不正検出モードでサポートされます。
- ハイ アベイラビリティのシナリオでは、不正検出セキュリティ レベルを高か重要に設定すると、スタンバイ Cisco WLC の不正タイマーは、不正検出保留の安定時間の 300 秒が過ぎないと開始しません。したがって、スタンバイ Cisco WLC のアクティブ設定が反映されるのは、300 秒が過ぎてからです。

（注） 不正 AP、不正クライアント、または一時的な封じ込めの設定は、リロード時に破棄されます。リロード後にすべての不正を再設定する必要があります。

（注） 不正クライアントのトラップを制御するための独立したコマンドはありません。ただし、不正クライアントのトラップは、不正 AP でも使用する **config trapflags rogueap {enable | disable}** コマンドで有効、無効を切り替えることができます。GUI 設定でも、[Management] -> [SNMP] -> [TrapControl] -> [Security] -> [Rogue AP] で AP フラグを使用して、不正クライアントを制御してください。

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol（RLDP）は、不正 AP で認証が設定されていない（オープン認証）場合に使用される積極的なアプローチです。このモードは、デフォルトで無効になっており、不正チャネルに移動して、クライアントとして不正に接続するようにアクティブ AP に指示します。この間に、アクティブ AP は、接続されたすべてのクライアントに認証解除メッセージを送信してから、無線インターフェイスをシャットダウンします。次に、クライアントとして不正 AP にアソシエートします。その後で、AP は、不正 AP から IP アドレスの取得を試み、ローカル AP と不正接続情報を含む User Datagram Protocol（UDP）パケット（ポート 6352）を不正 AP を介してコントローラに転送します。コントローラがこのパケットを受信すると、不正 AP が RLDP 機能を使用して有線ネットワークで検出されたことをネットワーク管理者に通知するためのアラームが設定されます。

RLDP の不正 AP の検出精度は 100% です。オープン AP と NAT AP を検出します。

（注） Lightweight AP が不正 AP とアソシエートして DHCP アドレスを受信するかどうかを確認するには、**debug dot11 rldp enable** コマンドを使用します。このコマンドは、Lightweight AP からコントローラに送信された UDP パケットも表示します。

ここで、Lightweight AP から送信される UDP （宛先ポート 6352）パケットのサンプルを示します。0020 0a 01 01 0d 0a 01 .....(.*.....0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00 .....x.....0040 00 00 00 00 00 00 00 00 00 00 00

最初の 5 バイトのデータには、不正 AP によってローカル モード AP に割り当てられた DHCP アドレスが含まれています。次の 5 バイトはコントローラの IP アドレスで、その後に不正 AP MAC アドレスを表す 6 バイトが続きます。その後に、18 バイトの 0 が続きます。

ここで、RLDP の動作手順を示します。

1. 信号強度値を使用して不正に最も近い統合 AP を特定します。
2. その後で、この AP が WLAN クライアントとして不正に接続します。3 回のアソシエーションを試みて、成功しない場合はタイムアウトします。
3. アソシエーションが成功すると、AP が DHCP を使用して IP アドレスを取得します。
4. IP アドレスが取得されたら、AP（WLAN クライアントとして機能している）は、コントローラの IP アドレスのそれぞれに UDP パケットを送信します。

5. コントローラがクライアントから RLDP パケットの 1 つでも受信すると、その不正が重大度が critical の on-wire としてマークされます。

（注） コントローラのネットワークと不正デバイスが設置されたネットワークの間にフィルタリングルールが設定されている場合は、RLDP パケットがコントローラに到達できません。

RLDP の注意事項：

- RLDP は、認証と暗号化が無効になっている SSID をブロードキャストするオープン不正 AP でのみ動作します。
- RLDP では、クライアントとして機能しているマネージド AP が不正ネットワーク上で DHCP を介して IP アドレスを取得できる必要があります。
- 手動 RLDP を使用して、不正上で RLDP トレースを複数回試すことができます。
- RLDP プロセス中は、AP がクライアントにサービスを提供できません。これがローカルモード AP のパフォーマンスと接続に悪影響を及ぼします。この問題を回避するために、RLDP はモニタ モード AP に対してのみ選択的に有効にできます。
- RLDP は、5GHz DFS チャネルで動作する不正 AP への接続は試行しません。

（注） RLDPは、シスコのAtonomous不正アクセス ポイントではサポートされていません。これらのアクセス ポイントは、RLDPクライアントによって送信されたDHCP検出要求をドロップします。また不正なアクセスポイントチャネルが動的周波数選択（DFS）を必要とする場合、RLDPはサポートされません。自動 RLDP 試行で不正（ノイズの多い RF 環境などが原因）が検出されなかった場合は、コントローラが再試行しません。ただし、不正デバイス上でRLDPを手動で開始できます。

不正なデバイスの検出

コントローラは、近くにあるすべてのアクセス ポイントを継続的に監視し、不正なアクセスポイントとクライアントに関する情報を自動的に検出および収集します。コントローラは不正なアクセス ポイントを検出すると、Rogue Location Discovery Protocol（RLDP）を使用し、不正検出モードのアクセスポイントが接続されて、不正がネットワークに接続されているかどうかを特定します。

コントローラは、オープン認証および設定された不正デバイスで RLDP を開始します。RLDP が Flexconnect またはローカル モードのアクセス ポイントを使用すると、クライアントはその時点で接続を解除されます。RLDPのサイクルが終了すると、クライアントはアクセスポイントに再接続します。不正なアクセスポイントが検出された時点で（自動設定）、RLDPのプロセスが開始されます。

すべてのアクセス ポイント、または監視（リッスン専用）モードに設定されたアクセス ポイントでのみRLDPを使用するようにコントローラを設定できます。後者のオプションでは、混

雑した無線周波数（RF）空間での自動不正アクセス ポイント検出が実現され、不要な干渉を生じさせたり、正規のデータ アクセス ポイント機能に影響を与えずにモニタリングを実行できます。すべてのアクセスポイントでRLDPを使用するようにコントローラを設定した場合、モニタ アクセス ポイントとローカル（データ）アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 動作に対してモニタ アクセス ポイントを選択します。ネットワーク上に不正があるとRLDPが判断した場合、検出された不正を手動または自動で阻止することを選択できます。

RLDPは、オープン認証に設定されている不正なアクセスポイントの存在をネットワーク上で一度だけ（デフォルト設定の再試行回数）検出します。再試行は **config rogue ap rldp retries** コマンドで設定できます。

3 種類の方法でコントローラから RLDP を開始またはトリガーできます。

1. コントローラの CLI から RLDP 開始コマンドを手動で入力します。RLDP を開始するための同等の GUI オプションはサポートされていません。

   config rogue ap rldp initiate *mac-address*

2. コントローラの CLI から RLDP をスケジュールします。RLDP をスケジュールするための同等の GUI オプションはサポートされていません。

   config rogue ap rldp schedule

3. 自動 RLDP。コントローラの CLI または GUI から自動 RLDP を設定できますが、次の注意事項を考慮してください。

   - 不正検出のセキュリティ レベルが custom に設定されている場合にのみ、自動 RLDP オプションを設定できます。
   - 自動 RLDP および RLDP のスケジュールを同時に有効にすることはできません。

不正なアクセス ポイントは、自動または手動で Contained 状態に変更されます。コントローラは、不正の阻止に最も効果的なアクセス ポイントを選択し、そのアクセス ポイントに情報を提供します。アクセスポイントは、無線あたりの不正阻止数のリストを保存します。自動阻止の場合は、監視モードのアクセス ポイントだけを使用するようにコントローラを設定できます。阻止動作は次の 2 つの方法で開始されます。

- コンテナ アクセス ポイントが定期的に不正阻止のリストを確認し、ユニキャスト阻止フレームを送信します。不正なアクセスポイントの阻止の場合、フレームは不正なクライアントがアソシエートされている場合にのみ送信されます。
- 阻止された不正アクティビティが検出されると、阻止フレームが送信されます。

個々の不正阻止には、一連のユニキャスト アソシエーション解除フレームおよび認証解除フレームの送信が含まれます。

Cisco Prime Infrastructure のインタラクションと不正検出

Cisco Prime Infrastructure ではルール ベースの分類がサポートされ、コントローラで設定された分類ルールが使用されます。コントローラは、次のイベント後に Cisco Prime Infrastructure にトラップを送信します。

- 不明なアクセス ポイントがFriendly状態に初めて移行すると、コントローラは、不正の状態が Alert の場合にのみ Cisco Prime Infrastructure にトラップを送信します。不正の状態が Internal または External であると、トラップは送信されません。
- タイムアウトの経過後に不正なエントリが削除されると、Malicious（Alert、Threat）または Unclassified（Alert）に分類された不正なアクセス ポイントに関して、コントローラから Cisco Prime Infrastructure にトラップが送信されます。コントローラでは、不正の状態が Contained、Contained Pending、Internal、および External である不正なエントリは削除されません。

不正検出の設定方法

不正検出の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless wpsroguedetectionmin-rssi** *rssi in dBm* 例： `Device(config)# wireless wps rogue detection min-rssi 100`	不正に必要な最小 RSSI 値を指定します。これは、AP が不正を検出し、デバイスで不正エントリが作成されるために必要な値です。 rssi in dBm パラメータの有効範囲は –128 ～ –70 dBm で、デフォルト値は –128 dBm です。 （注） この機能は、すべての AP モードに適用できます。RSSI 値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、AP が不正を検出する最小 RSSI 値を指定することで、このオプションを使用して不正をフィルタリングすることができます。

	コマンドまたはアクション	目的
ステップ 3	**wireless wpsroguedetectionmin-transient-time** *time in seconds* 例： `Device(config)# wireless wps rogue detection min-transient-time`	不正が初めてスキャンされた後、AP で不正スキャンを連続的に実行する間隔を入力します。 time in sec パラメータの有効範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。 （注） この機能は、モニタ モードの AP のみに適用されます。 一時的な間隔値を使用して、AP が不正をスキャンする間隔を制御できます。AP では、それぞれの一時的間隔値に基づいて、不正のフィルタリングも実行できます。 この機能には次の利点があります。 • AP からコントローラへの不正レポートが短くなる • 一時的な不正エントリをコントローラで回避できる • 一時的な不正への不要なメモリ割り当てを回避できる

ステップ 4	**wireless wpsrogueclient** {**aaa** | **mse**}
	例：
	`Device(config)# wireless wps rogue client aaa`
	`Device(config)# wireless wps rogue client mse`
		不正なクライアントが有効なクライアントかどうかを検証するために、AAA サーバまたはローカル データベース、または MSE を設定します。

ステップ 5	**wireless wpsrogue apvalid-clientauto-contain** 例： `Device(config)# wireless wps rogue ap valid-client auto-contain`	信頼できるクライアントが関連付けられる不正なアクセス ポイントを自動的に阻止するように指定します。
ステップ 6	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config)# end`	ンフィギュレーション モードを終了できます。

不正検出のモニタリング

この項では、不正検出の新しいコマンドについて説明します。

次のコマンドは、上で不正検出をモニタするために使用できます。

表 *165 :* 不正検出モニタリングのコマンド

コマンド	目的
show wireless wps rogue ap summary	によって検出されたすべての不正アクセスポイントのリストを表示します。
show wireless wps rogue client detailed *client-mac*	特定の不正クライアントの詳細情報を表示します。
show wireless wps rogue client summary	で検出されたすべての不正なクライアントのリストを表示します。
show nmsp capability	NMSP 機能を表示します。

例：不正検出の設定

この例は、検出された不正 AP が存在する必要がある最小 RSSI を、で作成されたエントリを持つように設定する方法を示しています。

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-rssi -100
Device(config)# end
Device# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

次に、分類インターバルを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-transient-time 500
Device(config)# end
Device# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

次に、不正なクライアントが有効なクライアントかどうかを検証するために MSE を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue client mse
```

```
Device(config)# end
Device# show wireless wps rogue client summary
```

次に、信頼できるクライアントが関連付けられる不正なアクセスポイントを自動的に阻止する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue ap valid-client auto-contain
Device(config)# end
Device# show wireless wps rogue ap summary
Device# show nmsp capability
```

不正検出に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

不正検出設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。
Cisco IOS XE 3E	MSE に対する不正な検証。

第 117 章

不正なアクセス ポイントの分類

- 機能情報の確認 （2623 ページ）
- 不正なアクセス ポイントの分類について （2623 ページ）
- 不正なアクセス ポイントの分類の制限 （2626 ページ）
- 不正なアクセス ポイントの分類方法 （2628 ページ）
- 例：不正なアクセス ポイントの分類 （2631 ページ）
- 不正なアクセス ポイントの分類に関する追加情報 （2631 ページ）
- 不正なアクセス ポイントの分類の機能履歴および情報 （2632 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

不正なアクセス ポイントの分類について

コントローラ ソフトウェアでは、不正なアクセス ポイントを Friendly、Malicious、または Unclassified に分類して表示するルールを作成できます。

デフォルトでは、いずれの分類ルールも有効になっていません。したがって、すべての未知（管理対象外）のアクセス ポイントは Unclassified に分類されます。ルールを作成し、その条件を設定して、ルールを有効にすると、未分類のアクセスポイントは分類し直されます。ルールを変更するたびに、Alert 状態にあるすべてのアクセス ポイント（Friendly、Malicious、および Unclassified）にそのルールが適用されます。

不正またはアドホック不正を手動で未分類および Alert 状態に移動すると、その不正はデフォルト状態に移動されることになります。不正ルールは、未分類および Alert 状態に手動で移動されたすべての不正に適用されます。

（注） ルールベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。

（注） 1 台のコントローラにつき最大 64 の不正分類ルールを設定できます。

コントローラは、管理対象のアクセスポイントの 1 つから不正レポートを受信すると、次のように応答します。

1. コントローラは未知（管理対象外）のアクセス ポイントが危険性のない MAC アドレスのリストに含まれているか確認します。そのリストに含まれている場合、コントローラはそのアクセス ポイントを Friendly として分類します。
2. 未知（管理対象外）のアクセス ポイントが危険性のない MAC アドレスのリストに含まれていない場合、コントローラは、不正状態の分類ルール適用処理を開始します。
3. 不正なアクセス ポイントが Malicious、Alert または Friendly、Internal または External にすでに分類されている場合は、コントローラはそのアクセスポイントを自動的に分類しません。不正なアクセスポイントがそれ以外に分類されており、Alert 状態にある場合に限り、コントローラはそのアクセス ポイントを自動的に分類し直します。
4. コントローラは、優先度の一番高いルールを適用します。不正なアクセスポイントがルールで指定された条件に一致すると、コントローラはそのアクセスポイントをルールに設定された分類タイプに基づいて分類します。
5. 不正なアクセスポイントが設定されたルールのいずれにも一致しないと、コントローラはそのアクセス ポイントを Unclassified に分類します。
6. コントローラは、すべての不正なアクセスポイントに対して上記の手順を繰り返します。
7. 不正なアクセスポイントが社内ネットワーク上にあると RLDP で判断されると、ルールが設定されていない場合でも、コントローラは不正の状態を Threat とマークし、そのアクセス ポイントを自動的に Malicious に分類します。その後、不正なアクセス ポイントに対して手動で封じ込め処理を行うことができますが（不正を自動的に封じ込めるよう RLDP が設定されていない限り）、その場合は不正の状態が Contained に変更されます。不正なアクセス ポイントがネットワーク上にないと、コントローラによって不正の状態が Alert とマークされ、そのアクセスポイントを手動で封じ込め処理を行うことができるようになります。
8. 必要に応じて、各アクセスポイントを本来とは異なる分類タイプや不正の状態に手動で変更することも可能です。

表 *166*：分類マッピング

ルール ベースの分類タイプ	不正の状態
Friendly	• Internal：不明なアクセスポイントがネットワーク内に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、Internal に設定します。たとえば、ラボ ネットワーク内のアクセス ポイントなどです。 • External：不明なアクセスポイントがネットワーク外に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、External に設定します。たとえば、近隣のコーヒー ショップに属するアクセス ポイントなどです。 • Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。
Malicious	• Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • Threat：未知（管理対象外）のアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。 • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。 • Contained Pending：不明なアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。
未分類	• Pending：最初の検出で、不明なアクセス ポイントは 3 分間 Pending 状態に置かれます。この間に、管理対象のアクセスポイントでは、不明なアクセス ポイントがネイバー アクセス ポイントであるかどうかが判定されます。 • Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。 • Contained Pending：不明なアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。

分類および不正アクセス ポイントのステータスは以下のように設定されています。

- Known から Friendly、Internal
- Acknowledged から Friendly、External
- Contained から Malicious、Contained

前述のように、コントローラでは、ユーザ定義のルールに基づいて未知（管理対象外）のアクセスポイントの分類タイプと不正の状態が自動的に変更されます。もしくは、未知（管理対象外）のアクセスポイントを本来とは異なる分類タイプと不正の状態に手動で変更することができます。

表 *167 :* 設定可能な分類タイプ/不正の状態の推移

遷移元	目的
Friendly（Internal、External、Alert）	Malicious（Alert）
Friendly（Internal、External、Alert）	Unclassified（Alert）
Friendly（Alert）	Friendly（Internal、External）
Malicious（Alert、Threat）	Friendly（Internal、External）
Malicious（Contained、Contained Pending）	Malicious（Alert）
Unclassified（Alert、Threat）	Friendly（Internal、External）
Unclassified（Contained、Contained Pending）	Unclassified（Alert）
Unclassified（Alert）	Malicious（Alert）

不正の状態が Contained の場合、不正なアクセス ポイントの分類タイプを変更する前に、そのアクセス ポイントが封じ込められないようにする必要があります。不正なアクセス ポイントを Malicious から Unclassified に変更する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

不正なアクセス ポイントの分類の制限

この機能には、次のルールが適用されます。

- カスタム タイプの不正の分類は、不正ルールに関連付けられています。このため、不正を手動で Custom として分類することはできません。カスタム クラスの変更は不正ルールを使用する場合にのみ行えます。
- 不正分類の変更に対して、ルールによって30分ごとに阻止用のトラップが送信されます。カスタム分類の場合、最初のトラップはカスタム分類よりも前に存在していたため、そのトラップに重大度スコアは含まれません。不正が分類されると、30分後に生成される後続のトラップから重大度スコアが取得されます。

- 不正ルールは、優先順位に従って、コントローラ内の新しい着信不正レポートごとに適用されます。
- 不正がより高い優先度ルールを満たし、分類されると、同じレポートの優先順位リスト内で下位に下がることはありません。
- 以前に分類された不正は、次の制限に従って、新しい不正レポートが作成されるたびに、再分類されます。
  - ルールによって Friendly に分類され、状態が ALERT に設定されている不正は、新しい不正レポートを受け取ると再分類が開始されます。
  - 不正が管理者によって Friendly に手動で分類されると、状態は INTERNAL になり、次に続く不正レポートで再分類されません。
  - 不正が Malicious に分類されると、その状態に関係なく、後続の不正レポートで再分類されません。
- 一部の属性が新しい不正レポートで欠落している場合、複数の不正ルールによって、Friendly から Malicious に不正の状態が遷移する可能性があります。
- どの不正ルールによっても、Maliciousから他の分類に不正の状態が遷移することはありません。
- 不正 AP が Friendly に分類される場合、その不正 AP は近くに存在し、既知の AP であり、追跡する必要はないことを意味します。したがって、すべての不正 AP は Friendly な不正 AP に関連付けられている場合、削除されるか追跡されません。
- サービス セット識別子（SSID）が不正ルールの一部として定義され、show wireless wps rogue rule detailed**show wireless wps rogue rule detailed** コマンドを使用して不正ルールの詳細が表示されている場合、Cisco IOS XE リリース 3.7E 以前のリリースと Cisco IOS XE Denali 16.1.1 以降のリリースでは出力が異なります。

  次に、Cisco IOS XE リリース 3.6E 以前のリリースで **show wireless wps rogue rule detailed** コマンドを実行した場合の出力例を示します。

```
Switch# show wireless wps rogue rule detailed test

Priority                                    : 1
Rule Name                                   : wpstest
State                                       : Disabled
Type                                        : Pending
Match Operation                             : Any
Hit Count                                   : 0
Total Conditions                            : 1
Condition :
  type                                      : Ssid
  SSID Count                                : 2
  SSID 1                                    : ssid1
  SSID 2                                    : ssid2
```

  次に、Cisco IOS XE Denali 16.1.1 以降のリリースで **show wireless wps rogue rule detailed** コマンドを実行した場合の出力例を示します。

```
Switch# show wireless wps rogue rule detailed test

Priority                                    : 1
Rule Name                                   : wpstest
State                                       : Disabled
Type                                        : Pending
Match Operation                             : Any
Hit Count                                   : 0
Total Conditions                            : 1
Condition :
  type                                      : Ssid
  SSID Count                                : 2
  SSID                                      : ssid1
  SSID                                      : ssid2
```

不正なアクセス ポイントの分類方法

不正分類ルールの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**wireless wps rogue rule** *rule-name* **priority** *priority*
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)#`
		ルールを作成またはイネーブルにします。ルールを作成する場合、ルールのプライオリティを入力する必要があります。
		（注） ルールを作成した後、ルールを編集する場合、ディセーブルになった不正ルールに対してのみプライオリティを変更できます。有効にされた不正ルールのプライオリティは変更できません。編集時の不正ルールのプライオリティ変更は任意です。

ステップ 3	**classify** {**friendly** | **malicious**}
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# classify friendly`
		ルールを分類します。

	コマンドまたはアクション	目的

ステップ 4	**condition** {**client-count** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**}
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# condition client-count 5`
		不正アクセスポイントが満たす必要のあるルールに以下の条件を追加することを指定します。
		• **client-count**：不正アクセスポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正なアクセスポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセスポイントはMaliciousに分類されます。このオプションを選択する場合は、*condition_value* パラメータに、不正なアクセスポイントにアソシエートされたクライアントの最小数を入力します。有効な値の範囲は1～10（両端の値を含む）で、デフォルト値は0です。
		• **duration**：不正アクセスポイントが最小期間で検出される必要があります。このオプションを選択する場合は、*condition_value* パラメータに最小検出期間の値を入力します。有効な値の範囲は0～3600秒（両端の値を含む）で、デフォルト値は0秒です。
		• **encryption**：アドバタイズされたWLANで暗号化が無効になっている必要があります。
		• **infrastructure**：SSIDがコントローラで認識される必要があります。
		• **rssi**：不正アクセスポイントには、最小のRSSI値が必要です。たとえば、不正なアクセスポイントが設定値より大きいRSSIを持つ場合、そのアクセスポイントはMaliciousに分類されます。このオプションを選択する場合は、*condition_value* パラメータに最小RSSI値を入力します。有効な値の範囲は-95～-50

	コマンドまたはアクション	目的
		dBm（両端の値を含む）で、デフォルト値は 0 dBm です。 • **ssid**：不正なアクセス ポイントには、特定の SSID が必要です。コントローラによって管理されない SSID を追加する必要があります。このオプションを選択する場合は、*condition_value* パラメータに SSID を入力します。SSID はユーザ設定の SSID リストに追加されます。

ステップ 5	**match** {**all** | **any**}
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# match all`
		検出された不正なアクセスポイントがルールに一致していると見なされ、そのルールの分類タイプが適用されるためには、ルールで定義されているすべての条件を満たす必要があるか、一部の条件を満たす必要があるかを指定します。

ステップ 6	**default**
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# default`
		コマンドをデフォルトに設定するように指定します。

ステップ 7	**exit**
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# exit`
	`Device(config)#`
		サブモードの終了を指定します。

ステップ 8	**shutdown**
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# shutdown`
		特定の不正ルールをディセーブルにすることを指定します。たとえば、ルール **rule_3** はディセーブルです。

ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

	コマンドまたはアクション	目的
ステップ 10	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 11	**wireless wps rogue ruleshutdown** 例： `Device(config)# wireless wps rogue rule shutdown`	すべての不正ルールをディセーブルにすることを指定します。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

例：不正なアクセス ポイントの分類

次の例は、不正アクセスポイントをFriendlyとして組織および表示できるルールを作成する方法を示しています。

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# classify friendly
Device(config-rule)# end
```

この例は、不正アクセス ポイントが満たす必要のある条件を適用する方法を示しています。

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition client-count 5
Device(config-rule)# condition duration 1000
Device(config-rule)# end
```

不正なアクセス ポイントの分類に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

不正なアクセス ポイントの分類の機能履歴および情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 118 章

wIPS の設定

- 機能情報の確認 （2633 ページ）
- wIPS について （2633 ページ）
- アクセス ポイントで wIPS を設定する方法 （2641 ページ）
- wIPS 情報のモニタリング （2641 ページ）
- 例：wIPS の設定 （2642 ページ）
- wIPS の設定に関する追加情報 （2642 ページ）
- wIPS 設定実行の機能履歴 （2643 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

wIPS について

Cisco 適応型ワイヤレス侵入防御システム（wIPS）は、無線の脅威の検出およびパフォーマンス管理のための高度な手法を使用します。この手法では、ネットワーク トラフィック分析、ネットワーク デバイス/トポロジに関する情報、シグニチャベースの技法、および異常検出を組み合わせることにより、非常に正確で全面的な無線の脅威防御を実現できます。インフラストラクチャに完全に統合されたソリューションを採用して、有線ネットワークと無線ネットワークの両方で無線トラフィックを継続的に監視し、ネットワークインテリジェンスを使用してさまざまなソースからの攻撃を分析することにより、損害または漏洩が発生する前に、攻撃を正確に特定し事前に防止することができます。

シスコの適合型 wIPS は、Cisco 3300 シリーズ Mobility Services Engine（MSE）の一部です。MSE は、Cisco Aironet AP を継続的に監視して、収集された情報を一元処理します。シスコの適応型 wIPS の機能と、Cisco MSE への Cisco Prime Infrastructure の統合により、wIPS は wIPS ポリシーとアラームを設定、監視して、脅威をレポートします。

（注） お使いの wIPS が Cisco WLC、アクセス ポイント、Cisco MSE で構成されている場合、これら 3 つのエンティティはすべて UTC タイム ゾーンに設定してください。

シスコの適応型 wIPS は Cisco WLC には設定されていません。代わりに、プロファイル設定が Cisco Prime Infrastructure から wIPS サービスに転送され、wIPS サービスによってそのプロファイルが Cisco WLC に転送されます。このプロファイルは、Cisco WLC のフラッシュ メモリに保存され、Cisco WLC に参加するときに AP に送信されます。アクセス ポイントのアソシエーションを解除して、別の Cisco WLC に参加するとき、そのアクセス ポイントは新しい Cisco WLC から新しい wIPS プロファイルを受信します。

wIPS 機能のサブセットを備えたローカル モードの AP を、拡張ローカル モード アクセス ポイント、または ELM AP と呼びます。アクセス ポイントが次のいずれかのモードであれば、その AP を wIPS モードで動作するように設定できます。

- Monitor
- ローカル

通常のローカル モードまたは の AP は、wIPS 機能のサブセットで拡張します。この機能を使用すると、独立したオーバーレイ ネットワークがなくても、AP を展開して保護機能を提供できます。

wIPS ELM の、オフチャネル アラーム検出機能は限定的です。AP は定期的にオフチャネルになり、動作していないチャネルを短時間監視し、そのチャネルで攻撃を検出した場合はアラームをトリガーします。ただし、オフチャネルのアラーム検出はベストエフォートであり、攻撃を検出してアラームをトリガーするには時間がかかることがあります。そのため ELM AP が断続的にアラームを検出しては（確認できないため）クリアする、という場合があります。上記のいずれかのモードの AP は、ポリシー プロファイルに基づくアラームを Cisco WLC 経由で定期的に wIPS サービスに送信できます。wIPS サービスはアラームを格納および処理して、SNMP トラップを生成します。Cisco Prime Infrastructure は自身の IP アドレスをトラップの宛先として設定し、SNMP トラップを Cisco MSE から受信します。

次の表に SNMP トラップ制御とそれに対応するトラップを示します。トラップ制御が有効な場合、そのトラップ制御のトラップはすべて有効です。

（注） Cisco WLC が SNMP トラップの送信に使用するのは SNMPv2 のみです。

表 *168 : SNMP* トラップ制御と対応トラップ

タブ名	トラップ コントロール	Trap
General	Link (Port) Up/Down	linkUp、linkDown
	Spanning Tree	newRoot、topologyChange、stpInstanceNewRootTrap、stpInstanceTopologyChangeTrap
	Config Save	bsnDot11EssCreated、bsnDot11EssDeleted、bsnConfigSaved、ciscoLwappScheduledResetNotif、ciscoLwappClearResetNotif、ciscoLwappResetFailedNotif、ciscoLwappSysInvalidXmlConfig
AP	AP Register	bsnAPDisassociated、bsnAPAssociated
	AP Interface Up/Down	bsnAPIfUp、bsnAPIfDown
Client Traps	802.11 アソシエーション	bsnDot11StationAssociate
	802.11 ディスアソシエーション	bsnDot11StationDisassociate
	802.11 認証解除	bsnDot11StationDeauthenticate
	802.11 認証失敗	bsnDot11StationAuthenticateFail
	802.11 アソシエーション失敗	bsnDot11StationAssociateFail
	Exclusion	bsnDot11StationBlacklisted
	NAC Alert	cldcClientWlanProfileName、cldcClientIPAddress、cldcApMacAddress、cldcClientQuarantineVLAN、cldcClientAccessVLAN

タブ名	トラップ コントロール	Trap
Security Traps	User Authentication	bsnTooManyUnsuccessLoginAttempts、cLWAGuestUserLoggedIn、cLWAGuestUserLoggedOut
	RADIUS Servers Not Responding	bsnRADIUSServerNotResponding、ciscoLwappAAARadiusReqTimedOut
	WEP Decrypt Error	bsnWepKeyDecryptError
	Rogue AP	bsnAdhocRogueAutoContained、bsnRogueApAutoContained、bsnTrustedApHasInvalidEncryption、bsnMaxRogueCountExceeded、bsnMaxRogueCountClear、bsnApMaxRogueCountExceeded、bsnApMaxRogueCountClear、bsnTrustedApHasInvalidRadioPolicy、bsnTrustedApHasInvalidSsid、bsnTrustedApIsMissing
	SNMP Authentication	agentSnmpAuthenticationTrapFlag
	Multiple Users	multipleUsersTrap
自動 RF プロファイル トラップ	Load Profile	bsnAPLoadProfileFailed
	Noise Profile	bsnAPNoiseProfileFailed
	Interference Profile	bsnAPInterferenceProfileFailed
	Coverage Profile	bsnAPCoverageProfileFailed
自動 RF 更新トラップ	channel update	bsnAPCurrentChannelChanged
	Tx Power Update	bsnAPCurrentTxPowerChanged

タブ名	トラップ コントロール	Trap
Mesh Traps	Child Excluded Parent	ciscoLwappMeshChildExcludedParent
	Parent Change	ciscoLwappMeshParentChange
	Authfailure Mesh	ciscoLwappMeshAuthorizationFailure
	Child Moved	ciscoLwappMeshChildMoved
	Excessive Parent Change	ciscoLwappMeshExcessiveParentChange
	Excessive Children	ciscoLwappMeshExcessiveChildren
	Poor SNR	ciscoLwappMeshAbateSNR、ciscoLwappMeshOnsetSNR
	Console Login	ciscoLwappMeshConsoleLogin
	Excessive Association	ciscoLwappMeshExcessiveAssociation
	Default Bridge Group Name	ciscoLwappMeshDefaultBridgeGroupName

次に、「*SNMP* トラップ制御と対応トラップ」の表に記載されているトラップについて説明します。

- 一般トラップ
  - [SNMP Authentication]：SNMPv2 エンティティが、適切に認証されていないプロトコル メッセージを受信しました。

    （注） SNMP V3 モードで設定されているユーザが正しくないパスワードで Cisco WLC にアクセスを試みると、認証は失敗し、エラー メッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。

  - [Link (Port) Up/Down]：リンクのステータスは、アップまたはダウンから変更されます。
  - [Link (Port) Up/Down]：リンクのステータスは、アップまたはダウンから変更されます。
  - [Multiple Users]：2 人のユーザが同じ ID でログインしました。
  - [Rogue AP]：不正アクセス ポイントが検出されるたびに、このトラップが MAC アドレスとともに送信されます。また、以前に検出された不正アクセス ポイントが存在しなくなっている場合にこのトラップが送信されます。
  - [Config Save]：Cisco WLC 設定が変更されると送信される通知。
- Cisco AP トラップ

- [AP Register]：アクセス ポイントが Cisco WLC とアソシエートまたはディスアソシエートすると送信される通知。
- [AP Interface Up/Down]：アクセス ポイント インターフェイス（802.11X）の状態がアップまたはダウンになると送信される通知です。

- クライアント関連トラップ
  - [802.11 Association]：クライアントがアソシエーション フレームを送信すると送信されるアソシエーション通知。
  - [802.11 Disassociation]：クライアントがディスアソシエーション フレームを送信すると送信されるディスアソシエーション通知。
  - [802.11 Deauthentication]：クライアントが認証解除フレームを送信すると送信される認証解除通知。
  - [802.11 Failed Authentication]：クライアントが成功以外のステータス コードの認証フレームを送信すると送信される認証エラー通知。
  - [802.11 Failed Association]：クライアントが成功以外のステータス コードのアソシエーション フレームを送信すると送信されるアソシエーション エラー通知。
  - [Exclusion]：クライアントが除外リストに掲載（blacklisted）されている場合に送信されるアソシエーション失敗通知。
  - [Authentication]：クライアントが正常に認証されると送信される認証通知。
  - [Max Clients Limit Reached]：[Threshold] フィールドに定義されている最大数のクライアントが Cisco WLC とアソシエートされた場合に送信される通知。
  - [NAC Alert]：クライアントが SNMP NAC 対応 WLAN に join する場合に送信されるアラート。

    この通知は、NAC 対応 SSID 上のクライアントがその存在に関する情報を NAC アプライアンスに通知するために Layer2 認証を完了したときに生成されます。cldcClientWlanProfileName は、802.11 ワイヤレス クライアントが接続されている WLAN のプロファイル名を表します。cldcClientIPAddress は、クライアントの一意の IP アドレスを表します。cldcApMacAddress は、クライアントがアソシエートされている AP の MAC アドレスを表します。cldcClientQuarantineVLAN は、クライアントの隔離 VLAN を表します。cldcClientAccessVLAN は、クライアントのアクセス VLAN を表します。
  - [Association with Stats]：クライアントが Cisco WLC とアソシエートするときや、ローミングするときに、データ統計とともに送信されるアソシエーション通知。データの統計情報には、送受信されたバイトとパケットが含まれます。
  - [Disassociation with Stats]：クライアントが Cisco WLC からディスアソシエートするときに、データ統計とともに送信されるディスアソシエーション通知。データの統計情報には、送受信されたパケットとバイト、SSID、セッション ID が含まれます。

（注） 新しいリリースからリリース 7.4 にダウングレードする場合、リリース 7.4 のサポート対象外のトラップ（たとえば、NAC Alert トラップ）をダウングレード前に有効にしておくと、すべてのトラップが無効になります。ダウングレードが終了したら、ダウングレード前に有効であったすべてのトラップを有効にする必要があります。他のすべてのトラップが無効にならないように、ダウングレードする前に新しいトラップを無効にすることをお勧めします。

- Security Traps
  - [User Auth Failure]：このトラップは、クライアントの RADIUS 認証の失敗が発生したことを通知します。
  - [RADIUS Server No Response]：このトラップは、RADIUS クライアントが送信した認証要求に応答する RADIUS サーバがないことを示します。
  - [WEP Decrypt Error]：Cisco WLC が WEP 復号化エラーを検出すると送信される通知です。
  - [Rogue AP]：不正アクセス ポイントが検出されるたびに、このトラップが MAC アドレスとともに送信されます。また、以前に検出された不正アクセスポイントが存在しなくなっている場合にこのトラップが送信されます。
  - [SNMP Authentication]：SNMPv2 エンティティが、適切に認証されていないプロトコル メッセージを受信しました。

（注） SNMP V3 モードで設定されているユーザが正しくないパスワードで Cisco WLC にアクセスを試みると、認証が失敗し、エラーメッセージが表示されます。ただし、認証エラーの場合、トラップログは生成されません。

  - [Multiple Users]：2 人のユーザが同じ ID でログインしました。
- SNMP Authentication
  - [Load Profile]：[Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Noise Profile]：[Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Interference Profie]：[Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Coverage Profile]：[Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- 自動 RF プロファイル トラップ

- [Load Profile]：[Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Noise Profile]：[Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Interference Profie]：[Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Coverage Profile]：[Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。

- 自動 RF 更新トラップ
  - [Channel Update]：アクセス ポイントの動的チャネル アルゴリズムが更新されると送信される通知。
  - [Tx Power Update]：アクセス ポイントの動的送信電力アルゴリズムが更新されると送信される通知。
- Mesh Traps
  - [Child Excluded Parent]：親メッシュ ノードを介して、Cisco WLC に対するアソシエーションの失敗数が定義された回数に達すると送信される通知。
  - 子メッシュ ノード数が検出応答タイムアウトのしきい値制限を超えると送信される通知。子メッシュ ノードが、定義された間隔で除外された親メッシュ ノードのアソシエーションを試行することはありません。子メッシュ ノードは、ネットワークに参加するときに、除外された親 MAC アドレスを記憶しており、それを Cisco WLC に通知します。
  - [Parent Change]：子メッシュ ノードがその親を変更すると、通知がエージェントによって送信されます。子メッシュ ノードは以前の親を記憶し、ネットワークに再度参加するときに、親の変更について Cisco WLC に通知します。
  - [Child Moved]：親メッシュ ノードが子メッシュ ノードとの接続を失うと送信される通知。
  - [Excessive Parent Change]：子メッシュ ノードが親を頻繁に変更すると送信される通知です。各メッシュ ノードは一定期間の親の変更回数のカウントを保持します。これが定義されたしきい値を超えると、子メッシュ ノードが Cisco WLC に通知します。
  - [Excessive Children]：RAP や MAP で子の数が超過すると送信される通知。
  - [Poor SNR]：子メッシュ ノードが、バックホール リンクでより低い SNR を検出すると送信される通知です。他のトラップの場合、子メッシュ ノードが、「clMeshSNRThresholdAbate」によって定義されるオブジェクトより高い SNR をバックホール リンクで検出すると、通知をクリアするための通知が送信されます。
  - [Console Login]：MAP コンソールでログインが成功するか、3 回の試行の後に失敗するとエージェントが通知を送信します。
  - [Default Bridge Group Name]：デフォルトのブリッジ グループ名で MAP メッシュ ノードがその親に参加すると送信される通知。

（注） 上記以外のトラップにトラップ制御機能はありません。これらのトラップは、頻繁に生成されないので、トラップ制御は必要ありません。Cisco WLC で生成されるその他のトラップをオフにすることはできません。

（注） 上記のすべてのケースで、Cisco WLC は純粋に転送デバイスとして機能します。

アクセス ポイントで wIPS を設定する方法

アクセス ポイントでの wIPS の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**apname** *name* **mode** *submode wips* 例： `Device# ap name ap1 mode local wips`	ローカルまたはモニタ モードに対してアクセス ポイントを設定し、wIPS にサブモードを設定します。
ステップ 2	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 3	**showwirelesswpswipssummary** 例： `Device# show wireless wps wips summary`	アクセス ポイントで wIPS 設定を表示します。
ステップ 4	**showwirelesswpswipsstatistics** 例： `Device# show wireless wps wips statistics`	wIPS 設定の現在のステートを表示します。

wIPS 情報のモニタリング

このセクションは、wIPS の新しいコマンドについて説明します。

以下のコマンドは、アクセス ポイント上で設定された wIPS をモニタするために使用できます。

表 *169 : wIPS* コマンドのモニタリング

コマンド	目的
show wireless wps wips summary	アクセス ポイントでwIPS設定を表示します。
show wireless wps wips statistics	wIPS 設定の現在のステートを表示します。

例：wIPS の設定

次に、AP1 上で wIPS を設定する例を示します。

```
Device# ap name ap1 mode local submode wips
Device# end
Device# show wireless wps wips summary
```

wIPS の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
wIPS コマンド	『*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

wIPS 設定実行の機能履歴

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 119 章

侵入検知システムの設定

- 機能情報の確認 （2645 ページ）
- 侵入検知システムについて （2645 ページ）
- 侵入検知システムを設定する方法 （2646 ページ）
- 侵入検知システムのモニタリング （2647 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

侵入検知システムについて

シスコ侵入検知システム/侵入防御システム（CIDS/IPS）は、特定のクライアントに関わる攻撃がレイヤ 3 ～ レイヤ 7 で検出されたとき、これらのクライアントによるワイヤレス ネットワークへのアクセスをブロックするようデバイスに指示します。このシステムは、ワーム、スパイウェア/アドウェア、ネットワーク ウイルス、およびアプリケーションの不正使用などの脅威の検出、分類、阻止を支援することにより、強力なネットワーク保護を提供します。潜在的な攻撃を検出するには 2 つの方法があります。

- IDS センサー
- IDS シグニチャ

IDS センサーは、ネットワーク内のさまざまなタイプの IP レベルの攻撃を検出するように設定できます。センサーで攻撃が特定されたら、違反クライアントを回避（shun）するようデバイ

スに警告することができます。新規IDSセンサーが追加される場合、回避するクライアントのリストを取得するために デバイス がセンサにクエリを発行できるように、IDS センサーを デバイス と登録する必要があります。

IDSセンサーは、疑わしいクライアントを検出すると、デバイスにこのクライアントを回避するよう警告します。回避エントリは、同じモビリティ グループ内のすべての デバイス に配信されます。回避すべきクライアントが現在、このモビリティ グループ内の デバイス に join している場合、アンカー デバイス はこのクライアントを動的除外リストに追加し、外部 デバイス はクライアントを切り離します。次回、このクライアントがデバイスに接続を試みた場合、アンカー デバイス はハンドオフを拒否し、外部 デバイス にクライアントを除外することを通知します。

侵入検知システムを設定する方法

IDS センサーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless wps cids-sensor** *index* [**ip-address** *ip-addr* **username** *username* **password** *password_type* *password*] 例： `Device(config)# wireless wps cids-sensor 2 231.1.1.1 admin pwd123`	内部インデックス番号を保持する IDS センサーを設定します。index パラメータは、コントローラで IDS センサーが検索される順序を決定します。コントローラでは最大 5 つの IDS センサーをサポートします。 • **ip-address**：（任意）IDS に IP アドレスを提供します。 • **username**：（任意）IDS のユーザ名を設定します。 • **password**：（任意）対応するユーザ名のパスワードを設定します。
ステップ 3	**wireless wps cids-sensor** *index* 例： `Device(config)# wireless wps cids-sensor 1`	IDS コンフィギュレーション サブモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	[**default exit fingerprint interval no port shutdown**] 例： `Device(config-cids-index)# default`	さまざまな IDS パラメータを設定します。 • **default**：（任意）コマンドをデフォルトに設定します。 • **exit**：（任意）サブモードを終了します。 • **fingerprint**：（任意）センサーの TLS フィンガープリントを設定します。 • **interval**：（任意）センサーのクエリ間隔を設定します。範囲は 10 ～ 3600 秒です。 • **no**：（任意）コマンドを解除するか、デフォルトを設定します。 • **port**：（任意）センサーのポート番号を設定します。 • **shutdown**：（任意）侵入検知センサーをシャット ダウンします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

侵入検知システムのモニタリング

表 *170*：ワイヤレス マルチキャストをモニタリングするためのコマンド

コマンド	説明
show wireless wps cids-sensor *index*	指摘されたインデックス値で IDS センサーの IDS 設定を表示します。
show wireless wps cids-sensor summary	すべての設定された IDS のリストを、インデックス、IP アドレス、ポート番号、インターバル値、ステータスおよびクエリなどの対応する値とともに表示します。
show wireless wps shun-list	IDS 回避リストを表示します。

第 XVIII 部

スタック マネージャおよびハイ アベイラビリティ

- スイッチ スタックの管理 （2651 ページ）
- Cisco NSF with SSO の設定 （2689 ページ）
- StackWise Virtual の設定 （2705 ページ）
- ワイヤレス ハイ アベイラビリティの設定 （2723 ページ）

第 120 章

スイッチ スタックの管理

- 機能情報の確認 （2651 ページ）
- スイッチ スタックの前提条件 （2651 ページ）
- スイッチ スタックの制約事項 （2652 ページ）
- スイッチ スタックに関する情報 （2652 ページ）
- スイッチ スタックの設定方法 （2669 ページ）
- スイッチ スタックのトラブルシューティング （2676 ページ）
- デバイス スタックのモニタリング （2678 ページ）
- スイッチ スタックの設定例 （2679 ページ）
- スイッチ スタックに関する追加情報 （2687 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

スイッチ スタックの前提条件

スイッチ スタック内のすべてのスイッチがアクティブ スイッチと同じライセンス レベルを実行している必要があります。ライセンス レベルについては、『*System Management Configuration Guide (Catalyst 3850 Switches)*』を参照してください。

スイッチ スタック内のすべてのスイッチが互換性のあるソフトウェア バージョンを実行している必要があります。

スイッチ スタックの制約事項

スイッチ スタック設定の制約事項を以下に示します。

- LAN Base ライセンス レベルを実行しているスイッチ スタックは、レイヤ 3 機能をサポートしません。
- スイッチ スタックは、StackWise-480 ポート経由で接続された最大 9 つのスタック対応スイッチで構成できます。
- スイッチ スタックに Catalyst 3850 スイッチと Catalyst 3650 スイッチを組み合わせて含めることはできません。
- スイッチ スタックには、異なるライセンス レベルの組み合わせを含めることはできません。

（注） 混合スタック設定では、一部の機能に対するサポートが制限されます。特定の機能の詳細については、関連するCatalyst 3850コンフィギュレーション ガイドを参照してください。

スイッチ スタックに関する情報

スイッチ スタックの概要

スイッチ スタックは、StackWise-480 ポート経由で接続された最大 9 つのスタック対応スイッチで構成できます。スタック メンバーは1つの統合システムとして連携します。レイヤ2プロトコルとレイヤ 3 プロトコルが、スイッチ スタック全体を単一のエンティティとしてネットワークに提示します。

スイッチ スタックには、必ず 1 個のアクティブ スイッチおよび 1 個のスタンバイ スイッチがあります。アクティブ スイッチが使用不可能になった場合、スタンバイ スイッチがアクティブ スイッチの役割を担い、スタックは継続して動作します。

アクティブ スイッチがスイッチ スタックの動作を制御し、スタック全体の単一管理点になります。アクティブ スイッチから、以下を設定します。

- すべてのスタック メンバーに適用されるシステム レベル（グローバル）の機能
- スタック メンバーごとのインターフェイス レベルの機能

アクティブ スイッチには、スイッチ スタックの保存済みの実行コンフィギュレーション ファイルが格納されています。コンフィギュレーション ファイルには、スイッチ スタックのシステム レベルの設定と、スタック メンバーごとのインターフェイス レベルの設定が含まれます。

各スタック メンバーは、バックアップ目的で、これらのファイルの現在のコピーを保持します。

スイッチ スタックは、StackWise-480 ポート経由で接続された最大 9 つのスタック対応スイッチで構成できます。スタック内のスイッチは、同種であり、かつライセンス レベルが同じであることが必要です。

スイッチ スタックでサポートされる機能

アクティブ スイッチ上でサポートされるシステムレベルの機能は、スイッチ スタック全体でサポートされます。

暗号化機能

アクティブ スイッチが暗号化ユニバーサル ソフトウェア イメージ（暗号化対応）を実行している場合は、スイッチ スタック上で暗号化機能を使用できます。

StackWise-480

スタック メンバーは、StackWise-480 テクノロジーを使用して、1 つの統合システムとして連携します。レイヤ 2 プロトコルとレイヤ 3 プロトコルは、スイッチ スタック全体をネットワーク内の単一のエンティティとしてサポートします。

（注） LAN Base イメージを実行しているスイッチ スタックは、レイヤ 3 機能をサポートしません。

StackWise-480 は、480 Gbps のスタック帯域幅で、ステートフル スイッチオーバー（SSO）を使用してスタック内に復元力を提供します。スタックは、メンバー スイッチが選出したアクティブ スイッチによって管理される単一のスイッチングユニットとして動作します。アクティブ スイッチによって、スタック内のスタンバイ スイッチが自動的に選出されます。アクティブ スイッチは、すべてのスイッチング、ルーティング、およびワイヤレスに関する情報を作成して更新し、この情報を継続的にスタンバイ スイッチと同期します。アクティブ スイッチで障害が発生した場合、スタンバイ スイッチがアクティブ スイッチの役割を担い、スタックは継続して動作します。アクセス ポイントは、アクティブ スイッチに直接接続されていなければ、アクティブからスタンバイへのスイッチオーバー中に切断されることはありません。この場合、アクセス ポイントは電源がオフになって、リブートします。動作中のスタックは、サービスを中断せずに、新しいメンバーを追加したり、既存のメンバーを削除することができます。

高速スタック コンバージェンス

フル リング スタック内の単一リンクが動作しなくなると、パケットの転送が中断して、スタックがハーフ リングに移行します。Catalyst 3850では、このトラフィックの中断（またはスタック コンバージェンス時間）が数ミリ秒続きます。

StackPower

StackPower を使用すれば、スタック内の電源をスタック内のすべてのスイッチに共通のリソースとして共有することができます。StackPower は、スイッチに実装された個別の電源を統合し

て 1 つの電源プールを構成し、必要とされる場所に電力を供給します。StackPower ケーブルを使用して、最大 4 つのスイッチを StackPower スタック内で設定できます。

StackPower の詳細については、 *Interface and Hardware Component Configuration Guide*（*Catalyst 3850 Switches*） を参照してください。

スイッチ スタックのメンバーシップ

スタンドアロン デバイスは、アクティブ スイッチとしても動作するスタック メンバーを 1 つだけ持つデバイス スタックです。スタンドアロンデバイスを別のデバイスと接続して、2 つのスタック メンバーで構成され、一方がアクティブ スイッチであるスイッチ スタックを構築できます。スタンドアロン デバイスを既存のデバイス スタックに接続して、スタック メンバーシップを増やすこともできます。

すべてのスタック メンバーで hello メッセージが送受信されます。

- スタック メンバーが応答しない場合は、そのメンバーがスタックから削除されます。
- スタンバイ デバイスが応答しない場合は、新しいスタンバイ デバイスが選択されます。
- アクティブ デバイスが応答しない場合は、スタンバイ デバイスがアクティブ デバイスになります。

加えて、アクティブ スイッチとスタンバイ デバイス間でキープアライブ メッセージが送受信されます。

- スタンバイ デバイスが応答しない場合は、新しいスタンバイ デバイスが選択されます。
- アクティブ デバイスが応答しない場合は、スタンバイ デバイスがアクティブ デバイスになります。

スイッチ スタック メンバーシップの変更

スタック メンバを同一のモデルと交換した場合、新たなスイッチ（プロビジョニングされるスイッチとも呼びます）は交換されたスイッチと同じメンバ番号を使用すると、交換されたスイッチとまったく同じ設定で機能します。

アクティブ スイッチを削除したり、電源の入ったスタンドアロン スイッチまたはスイッチ スタックを追加したりしないかぎり、メンバーシップの変更中も、スイッチスタックの動作は間断なく継続されます。

- 電源の入ったスイッチの追加（マージ）により、すべてのスイッチはリロードし、その中から新しいアクティブ スイッチを選定します。新しく選定されたアクティブ スイッチは、その役割と設定を保持します。他のすべてのスイッチは、個別のスタック メンバー番号を保持し、新しく選択されたアクティブ スイッチのスタック設定を使用します。
- 電源が入った状態のスタック メンバを取り外すと、スイッチ スタックが、それぞれ同じ設定を持つ 2 つ以上のスイッチ スタックに分割（パーティション化）されます。これにより、以下の現象が発生する可能性があります。

- ネットワーク内での IP アドレスの競合。スイッチ スタックを分離されたままにしておきたい場合は、新しく作成されたスイッチ スタックの IP アドレス（複数の場合あり）を変更してください。
- スタック内の 2 つのメンバー間の MAC アドレスの競合。**stack-mac update force** コマンドを使用すると、この競合を解消できます。

新しく作成されたスイッチ スタックにアクティブ スイッチまたはスタンバイ スイッチがない場合、スイッチ スタックはリロードし、新しいアクティブ スイッチを選定します。

（注） スイッチ スタックに追加または削除するスイッチの電源がオフであることを確認します。

スタック メンバーを追加または削除したら、スイッチ スタックがすべての帯域幅（480 Gbps）で動作していることを確認します。スタック モード LED が点灯するまで、スタック メンバの Mode ボタンを押します。スタック内のすべてのスイッチでは、右側の最後の 2 つのポート LED がグリーンに点灯します。スイッチ モデルに応じて、右側の最後の 2 つのポートは 10 ギガビット イーサネット ポートまたは Small Form-Factor Pluggable（SFP）モジュール ポート（10/100/1000 ポート）になります。スイッチの一方または両方の LED がグリーンでない場合、スタックは全帯域幅で稼働していません。

スタックを分割しないで、電源が入ったスタック メンバを取り外す場合、次の手順を実行します。

- 新規に作成されたスイッチ スタックのスイッチの電源をオフにします。
- それをそのスタック ポートを介して元のスイッチ スタックに再接続します。
- スイッチの電源を入れます。

スイッチ スタックに影響するケーブル配線と電源の考慮事項については、*Catalyst 3850* スイッチハードウェア インストレーションガイド を参照してください。

スタック メンバー番号

スタック メンバー番号（1 ～ 9）は、デバイス スタック内の各メンバーを識別します。また、メンバー番号によって、スタック メンバーが使用するインターフェイス レベルの設定が決定します。**show switch** EXEC コマンドを使用すると、スタック メンバー番号を表示できます。

新しい初期設定状態の デバイス（デバイス スタックに参加していないスイッチまたはスタック メンバー番号が手動で割り当てられていないスイッチ）は、デフォルト スタック メンバー番号 1 で出荷されます。そのスイッチがデバイス スタックに参加すると、そのデフォルト スタック メンバー番号がスタック内で使用可能な最小メンバー番号に変更されます。

同じデバイス スタック内のスタック メンバーが同じスタック メンバー番号を持つことはできません。スタンドアロン デバイスを含むすべてのスタック メンバーは、番号が手動で変更されるまで、または、その番号がスタック内の他のメンバーによってすでに使用されていないかぎり、独自のメンバー番号を保持します。

- **switch** *current-stack-member-number***renumber** *new-stack-member-number* EXEC コマンドを使用して手動でスタック メンバー番号を変更した場合は、その番号がスタック内の他のメンバーに未割り当てなときにだけ、スタック メンバーのリセット後（または、**reload slot** *stack-member-number* 特権 EXEC コマンドの使用後）に新番号が有効となります。スタック メンバー番号を変更するもう 1 つの方法は、デバイス_NUMBER 環境変数を変更することです。

  番号がスタック内の他のメンバーによって使用されている場合は、デバイスがスタック内で使用可能な最小番号を選択します。

  手動でスタック メンバーの番号を変更し、新たなメンバー番号にインターフェイス レベルの設定が関連付けられていない場合は、スタック メンバーをデフォルト設定にリセットします。

  割り当てられた デバイス 上では、**switch** *current-stack-member-number***renumber** *new-stack-member-number* EXEC コマンドを使用できません。使用すると、コマンドは拒否されます。

- スタック メンバーを別のデバイス スタックに移動した場合、そのスタック メンバーは、自分の番号がスタック内の他のメンバーによって使用されていない場合にだけ、その番号を保持します。その番号が使用されている場合は、デバイスがスタック内で使用可能な最小番号を選択します。

- デバイス スタックをマージした場合は、新しいアクティブ スイッチ のデバイス スタックに参加しているデバイスがスタック内で使用可能な最小番号を選択します。

ハードウェア インストレーション ガイドに記載されているように、デバイス ポート LED をスタック モードで使用すれば、各スタック メンバーのスタック メンバー番号を目視で確認できます。

デフォルト モードでは、スタック マスターのスタック LED だけが緑色に点滅します。ただし、[MODE] ボタンを **[Stack]** オプションまでスクロールすると、すべてのスタック メンバのスタック LED が緑色に点灯します。

[MODE] ボタンが [Stack] オプションまでスクロールすると、各スタック メンバのスイッチ番号が、そのスイッチの最初の 5 つのポートの LED で表示されます。スイッチ番号は、すべてのスタック メンバで、バイナリ形式で表示されます。スイッチでは、オレンジ色の LED は値 0、緑の LED は値 1 を示します。

スイッチ番号 5（バイナリ 00101）の例：

スイッチ番号 5 のスタック メンバについては、最初の 5 つの LED が以下の色の組み合わせで点灯します。

- ポート 1：オレンジ
- ポート 2：オレンジ
- ポート 3：緑
- ポート 4：オレンジ

- ポート 5：緑

同様に、スイッチ番号に基づき、すべてのスタック メンバーで、最初の 5 つの LED がオレンジ色か緑色に点灯します。

（注）

- 水平スタック ポートを相手側の通常のネットワーク ポートに接続した場合、相手側から受信した SDP パケットがないと、スタック ポートの送受信は 30 秒以内に無効になります。
- スタック ポートはダウンしませんが、送受信だけ無効になります。次に示すログ メッセージがコンソールに表示されます。ピア側のネットワーク ポートがスタック ポートに変換されると、このスタック ポートの送受信が有効になります。

```
%STACKMGR-4-HSTACK_LINK_CONFIG: Verify peer stack port setting for
hstack StackPort-1 switch 5 (hostname-switchnumber)
```

スタック メンバーのプライオリティ値

スタック メンバのプライオリティ値が高いほど、アクティブ スイッチ として選択され、自分のスタック メンバ番号を保持できる可能性が高くなります。プライオリティ値は 1 ～ 15 の範囲で指定できます。デフォルトのプライオリティ値は 1 です。**show switch** EXEC コマンドを使用すると、スタック メンバーのプライオリティ値を表示できます。

（注）アクティブ スイッチにするデバイスには、最大プライオリティ値を割り当てることをお勧めします。これにより、再選択が実施されたときにそのデバイスがアクティブ スイッチとして再選択されることが保証されます。

スタック メンバーのプライオリティ値を変更するには、**switch** *stack-member-number* **priority** *new priority-value* EXEC コマンドを使用します。詳細については、「スタック メンバー プライオリティ値の設定」のセクションを参照してください。

新しいプライオリティ値はすぐに有効となりますが、現在の アクティブ スイッチ には影響しません。新たなプライオリティ値は、現在の アクティブ スイッチ またはスイッチ スタックのリセット時に、どのスタック メンバが新たな アクティブ スイッチ として選択されるかを決定する場合に影響を及ぼします。

スイッチ スタック ブリッジ ID と MAC アドレス

スイッチ スタックは、そのブリッジ *ID* によって、または、レイヤ 3 デバイスとして動作している場合はそのルータ MAC アドレスによって、ネットワーク内で識別されます。ブリッジ ID とルータ MAC アドレスは、アクティブ スイッチの MAC アドレスによって決定されます。

アクティブ スイッチが変わった場合は、新しいアクティブ スイッチの MAC アドレスによって、新しいブリッジ ID とルータ MAC アドレスが決定されます。

スイッチ スタック全体がリロードした場合は、スイッチ スタックがアクティブ スイッチの MAC アドレスを使用します。

スイッチ スタック上の永続的 MAC アドレス

永続的 MAC アドレス機能を使用すれば、スタック MAC アドレスが変更されるまでの時間遅延を設定できます。この期間に、前のアクティブ スイッチがスタックに再参加すると、スイッチが現在はスタック メンバーで、アクティブ スイッチではない場合でも、スタックはその MAC アドレスをスタック MAC アドレスとして使用し続けます。この期間に前のアクティブ スイッチがスタックに再参加しなかった場合は、スイッチ スタックが新しいアクティブ スイッチの MAC アドレスをスタック MAC アドレスとして取得します。デフォルトでは、新しいアクティブ スイッチが引き継ぐ場合でも、スタック MAC アドレスは最初のアクティブ スイッチの MAC アドレスになります。

永続的 MAC アドレス機能を使用すれば、スタック MAC アドレスが新しいスタック マスターの MAC アドレスに変更されるまでの時間遅延を設定できます。この機能がイネーブルになっている場合は、スタック MAC アドレスが約 4 分後に変更されます。この期間に、前のスタック マスターがスタックに再参加すると、スイッチが現在はスタック メンバーで、スタック マスターではない場合でも、スタックはその MAC アドレスをスタック MAC アドレスとして使用し続けます。前のスタック マスターがこの期間にスタックに復帰しない場合、スイッチ スタックは新しいスタック マスターの MAC アドレスをスタック MAC アドレスとして取得します。

また、スタック MAC アドレスが新しいアクティブ スイッチ MAC アドレスに変更されないように、スタック MAC の永続性を設定することもできます。

アクティブ スイッチとスタンバイ スイッチの選択と再選択

すべてのスタック メンバは、アクティブ スイッチまたはスタンバイ スイッチにすることができます。アクティブ スイッチが使用できなくなった場合、スタンバイ スイッチがアクティブ スイッチになります。

アクティブ スイッチは、次のイベントのいずれかが発生しないかぎり、役割を維持します。

- スイッチ スタックがリセットされた。
- アクティブ スイッチがスイッチ スタックから削除された。
- アクティブ スイッチがリセットされたか、電源が切れた。
- アクティブ スイッチに障害が発生した。
- 電源の入ったスタンドアロン スイッチまたはスイッチ スタックが追加され、スイッチ スタック メンバーシップが増えた。

すべてのスタック メンバは、スタック マスターになる資格を持っています。スタック マスターが使用不能になると、残りのメンバの中から新しいスタック マスターが選択されます。

アクティブ スイッチ は、次にリストした順番で、いずれかのファクタに基づいて選択または再選択されます。

1. 現在 アクティブ スイッチ であるスイッチ。
2. 最高のスタック メンバ プライオリティ値を持つスイッチ

（注） アクティブ スイッチ にしたいスイッチには、最高のプライオリティ値を割り当てることを推奨します。これにより、再選択が発生したときにそのスイッチを アクティブ スイッチ として選択させられます。

3. 起動時間が最短のスイッチ。機能イメージライセンス間の起動時間の差によってアクティブ スイッチが決まります。たとえば、IP Services ライセンス レベルが稼働しているスイッチが、IP Base ライセンス レベルが稼働しているスイッチより高いプライオリティを持っている場合でも、起動に 120 秒長くかかった場合は、IP Base ライセンス レベルが稼働しているスイッチの方がアクティブ スイッチになります。この問題を回避するには、IP Base ライセンス レベルを稼働させるスイッチをアップグレードして、他方のスイッチとライセンス機能セットとソフトウェア イメージを同じにするか、またはアクティブ スイッチを手動で起動し、最低 8 秒間待機してから、IP Base ライセンス レベルを実行する新しいメンバー スイッチを起動します。
4. コンフィギュレーション ファイルを保持するスイッチ
5. MAC アドレスが最小のスイッチ

（注） 新しいスタンバイ スイッチを選択または再選択する場合の要素は、アクティブ スイッチの選択または再選択の場合と同様で、アクティブ スイッチを除くすべての参加スイッチに適用されます。

選択後、新しいアクティブ スイッチは数秒後に使用可能になります。その間、スイッチ スタックはメモリ内の転送テーブルを使用してネットワークの中断を最小限に抑えます。新たなアクティブ スイッチが選択され、リセットされている間、他の使用可能なスタック メンバーの物理インターフェイスには何も影響はありません。

以前のアクティブ スイッチが使用可能になっても、アクティブ スイッチとしての役割を継続することはありません。

スイッチ スタック全体の電源を入れるかリセットした場合、一部のスタック メンバがアクティブ スイッチ選択に参加しない場合があります。同じ 2 分の間に電源が投入されたスタック メンバは、アクティブ スイッチの選択に参加し、アクティブ スイッチとして選択される可能性があります。120 秒間経過後に電源が投入されたスタック メンバは、この初回の選択には参加しないで、スタック メンバになります。アクティブ スイッチの選択に影響する電源の注意事項については、スイッチのハードウェア インストレーション ガイドを参照してください。

ハードウェア インストレーション ガイドに記載されているとおり、スイッチの ACTV LED を使用して、そのスイッチがアクティブ スイッチかどうかを確認できます。

スタック マスターは、次のイベントのいずれかが発生しないかぎり、役割を維持します。

- スイッチ スタックがリセットされた。*
- スタック マスターがスイッチ スタックから削除された。
- スタック マスターがリセットされたか、電源が切れた。
- スタック マスターに障害が発生した。
- 電源の入ったスタンドアロン スイッチまたはスイッチ スタックが追加され、スイッチ スタック メンバーシップが増えた。*

アスタリスク（*）が付いているイベントでは、示されている要素に基づいて現在のスタック マスターが再選択される場合があります。

スイッチ スタック全体に電源を入れるかリセットすると、一部のスタック メンバーがスタック マスター選択に参加しない場合があります。同じ 20 秒の間に電源が投入されたスタック メンバーは、スタック マスターの選択に参加し、スタック マスターとして選択される可能性があります。20 秒間経過後に電源が投入されたスタック メンバーは、この初回の選択には参加しないで、スタック メンバーになります。再選択には、すべてのスタック メンバが参加します。スタック マスターの選択に影響を与える電源投入に関する考慮事項については、ハードウェア インストレーション ガイドの「Switch Installation」の章を参照してください。

数秒後、新たなスタック マスターが使用可能になります。その間、スイッチ スタックはメモリ内の転送テーブルを使用してネットワークの中断を最小限に抑えます。新たなスタック マスターが選択され、リセットされている間、他の使用可能なスタック メンバーの物理インターフェイスには何も影響はありません。

新たなスタック マスターが選択され、以前のスタック マスターが使用可能になっても、以前のスタック マスターはスタック マスターとしての役割は再開しません。

スイッチ スタックのコンフィギュレーション ファイル

アクティブ スイッチは、スイッチ スタックの保存された実行コンフィギュレーション ファイルを保持します。スタンバイ スイッチは、自動的に、同期された実行コンフィギュレーション ファイルを受け取ります。スタック メンバーは、実行コンフィギュレーション ファイルがスタートアップ コンフィギュレーション ファイルに保存された時点で同期されたコピーを受け取ります。アクティブ スイッチが使用できなくなると、スタンバイ スイッチが現行の実行コンフィギュレーションを引き継ぎます。

アクティブ スイッチは、スイッチ スタックの保存された実行コンフィギュレーション ファイルを保持します。すべてのスタック メンバーは、定期的に、アクティブ スイッチからコンフィギュレーション ファイルの同期されたコピーを受け取ります。アクティブ スイッチが使用できなくなると、アクティブ スイッチの役割を担うスタック メンバーが最新のコンフィギュレーション ファイルを保持します。

コンフィギュレーション ファイルには、次の設定情報が格納されています。

- すべてのスタック メンバーに適用される IP 設定、STP 設定、VLAN 設定、SNMP 設定などのシステム レベル（グローバル）のコンフィギュレーション設定
- スタック メンバーのインターフェイス固有のコンフィギュレーション設定：各スタック メンバーに固有

（注） 実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存せずにアクティブ スイッチを交換した場合は、アクティブ スイッチのインターフェイス固有の設定が保存されます。

スイッチ スタックに参加している新しい初期設定のままの デバイスは、そのスイッチ スタックのシステム レベルの設定を使用します。デバイスが電源をオンにする前に別のスイッチ スタックに移動された場合、そのデバイスは保存されたコンフィギュレーション ファイルを失って、新しいスイッチスタックのシステム レベルの設定を使用します。デバイスが新しいスイッチスタックに参加する前にスタンドアロンデバイスとして電源をオンにされた場合は、スタックがリロードされます。スタックがリロードすると、新しいデバイスがアクティブ スイッチになって、そのコンフィグレーションを保持し、他のスタック メンバーのコンフィギュレーション ファイルを上書きする可能性があります。

各スタック メンバーのインターフェイス固有のコンフィギュレーションには、スタック メンバー番号が関連付けられます。スタック メンバーは、番号が手動で変更された場合、または同じスイッチスタック内の他のメンバーによってすでに使用されている場合以外は、自分の番号を保持します。スタック メンバーの番号を変更した場合は、そのスタック メンバーのリセット後に新しい番号が有効になります。

- そのメンバー番号に対応するインターフェイス固有のコンフィギュレーションが存在しない場合は、スタック メンバーはデフォルトのインターフェイス固有のコンフィギュレーションを使用します。
- そのメンバー番号に対応するインターフェイス固有のコンフィギュレーションが存在する場合は、スタック メンバーはそのメンバー番号に関連付けられたインターフェイス固有のコンフィギュレーションを使用します。

故障したメンバーを同一のモデルに交換すると、交換後のメンバーが、自動的に、故障したデバイスと同じインターフェイス固有のコンフィギュレーションを使用します。インターフェイス設定を再設定する必要はありません。交換後のデバイス（プロビジョニングされたデバイスとも呼ばれる）には、故障したデバイスと同じスタック メンバー番号を割り当てる必要があります。

スタンドアロン デバイスのコンフィギュレーションの場合と同様に、スタック コンフィギュレーションをバックアップして復元します。

スタック メンバーを割り当てるためのオフライン設定

オフライン設定機能を使用すると、新しいスイッチがスイッチ スタックに参加する前に、スイッチに割り当て（設定を割り当て）できます。現在スタックに属していないスイッチに関連

付けられたスタック メンバー番号、スイッチ タイプ、およびインターフェイスを設定できます。スイッチ スタックで作成した設定を割り当てられた設定と呼びます。スイッチ スタックに追加され、この設定を受信するスイッチを割り当てられたスイッチと呼びます。

switch *stack-member-number* **provision** *type* グローバル コンフィギュレーション コマンドにより、手動で設定を作成しプロビジョニングします。*stack-member-number* は、スタックに追加する前に、プロビジョニングされたスイッチ上で変更する必要があり、スイッチスタック上の新しいスイッチ用に作成したスタック メンバー番号と一致する必要があります。割り当てられた設定内のスイッチ タイプは新しく追加したスイッチのスイッチ タイプと一致する必要があります。スイッチスタックにスイッチを追加する場合に、割り当てられた設定が存在しないときは、割り当てられる設定が自動的に作成されます。

プロビジョニングされたスイッチに関連付けられているインターフェイスを設定すると、スイッチスタックがその設定を受け入れ、実行コンフィギュレーションにその情報が表示されます。ただし、スイッチがアクティブでないため、インターフェイス上の設定が機能しないうえ、割り当てられたスイッチに関連付けられたインターフェイスが特定の機能の表示には現れません。たとえば、プロビジョニングされたスイッチに関連付けられている VLAN 設定情報は、スイッチ スタック上の **show vlan** ユーザ EXEC コマンド出力に表示されません。

スイッチスタックは、割り当てられたスイッチがスタックに属するかどうかに関係なく、実行コンフィギュレーションに割り当てられた設定を保持します。**copy running-config startup-config** 特権 EXEC コマンドを入力すると、プロビジョニングされた設定をスタートアップ コンフィギュレーション ファイルに保存できます。スタートアップ コンフィギュレーション ファイルでは、割り当てられたスイッチがスタックに属するかどうかに関係なく、スイッチスタックは保存した情報をリロードして使用できます。

割り当てられたスイッチのスイッチ スタックへの追加による影響

プロビジョニングされたデバイスをスイッチスタックに追加すると、スタックはプロビジョニングされた設定かデフォルト設定のどちらかを適用します。下の表に、スイッチスタックが、プロビジョニングされた設定とプロビジョニングされたスイッチを比較するときに発生するイベントを示します。

表 *171 :* プロビジョニングされた設定とプロビジョニングされたスイッチの比較結果

シナリオ		結果
スタック メンバー番号とデバイス タイプが一致する場合。	**1.** プロビジョニングされたスイッチのスタック メンバ番号と、スタックのプロビジョニングされた設定のスタック メンバ番号が一致する場合、かつ **2.** プロビジョニングされたスイッチのデバイスタイプと、スタック上でプロビジョニングされた設定内のデバイス タイプが一致する場合。	スイッチスタックは、プロビジョニングされた設定をプロビジョニングされたスイッチに適用し、スタックに追加します。
スタック メンバー番号は一致するが、デバイス タイプが一致しない場合。	**1.** プロビジョニングされたスイッチのスタック メンバ番号と、スタックのプロビジョニングされた設定のスタック メンバ番号が一致する場合、ただし **2.** プロビジョニングされたスイッチのデバイスタイプと、スタック上でプロビジョニングされた設定内のデバイス タイプが一致しない場合。	スイッチスタックは、デフォルト設定をプロビジョニングされたスイッチに適用し、スタックに追加します。 プロビジョニングされた設定は、新しい情報を反映するために変更されます。
プロビジョニングされた設定でスタック メンバ番号が検出されない		スイッチスタックは、デフォルト設定をプロビジョニングされたスイッチに適用し、スタックに追加します。 プロビジョニングされた設定は、新しい情報を反映するために変更されます。
プロビジョニングされたスイッチのスタック メンバ番号が、プロビジョニングされた設定で検出されない		スイッチスタックは、デフォルト設定をプロビジョニングされたスイッチに適用し、スタックに追加します。

プロビジョニングされた設定で指定されたタイプとは異なるプロビジョニングされたスイッチを、電源が切られたスイッチ スタックに追加して電力を供給すると、スイッチ スタックがス

タートアップ コンフィギュレーション ファイル内の（現在は不正な）**switch** *stack-member-number***provision** *type* グローバル コンフィギュレーション コマンドを拒否します。ただし、スタックの初期化中は、スタートアップ コンフィギュレーション ファイルのデフォルトでないインターフェイス コンフィギュレーション情報が、（間違ったタイプの可能性がある）割り当てられたインターフェイス向けに実行されます。実際のデバイスタイプと前にプロビジョニングされたスイッチタイプの違いによって、拒否されるコマンドと、受け入れられるコマンドがあります。

（注） スイッチスタックに新しいデバイスのプロビジョニングされた設定が含まれていない場合は、デバイスがデフォルトのインターフェイス設定でスタックに参加します。その後で、スイッチスタックが、新しいデバイスと一致する **switch** *stack-member-number***provision** *type* グローバル コンフィギュレーション コマンドで、その実行コンフィギュレーションに追加されます。設定情報については、「スイッチスタックへの新しいメンバーのプロビジョニング」のセクションを参照してください。

スイッチ スタックの割り当てられたスイッチの交換による影響

スイッチスタック内の割り当てられたスイッチに障害が発生し、スタックから削除して別のデバイスと交換すると、スタックが割り当てられた設定またはデフォルト設定をそのスイッチに適用します。スイッチスタックが割り当てられた設定と割り当てられたスイッチを比較するときに発生するイベントは、割り当てられたスイッチをスタックに追加するときに発生するものと同じです。

割り当てられたスイッチのスイッチ スタックからの削除による影響

割り当てられたスイッチをスイッチ スタックから削除すると、削除されたスタック メンバーに関連付けられた設定は、割り当てられた情報として実行コンフィギュレーション内に残ります。設定を完全に削除するには、**no switch** *stack-member-number* **provision** グローバル コンフィギュレーション コマンドを使用します。

互換性のないソフトウェアを実行しているスイッチのアップグレード

自動アップグレード機能と自動アドバイス機能を使用すれば、スイッチスタックと互換性のないソフトウェア パッケージがインストールされたスイッチを互換性のあるバージョンのソフトウェアにアップグレードしてスイッチ スタックに参加できるようにすることができます。

自動アップグレード

自動アップグレード機能の目的は、スイッチを互換性のあるソフトウェア イメージにアップグレードしてスイッチ スタックに参加できるようにすることです。

新しいスイッチがスイッチ スタックに参加しようとすると、各スタック メンバーがそれ自体と新しいスイッチの互換性チェックを実行します。各スタック メンバーは、アクティブ スイッチに互換性チェックの結果を送信し、その結果に基づいてスイッチがスイッチスタックに参加

できるかどうかが判断されます。新しいスイッチ上のソフトウェアがスイッチスタックと互換性がない場合は、新しいスイッチがバージョン不一致（VM）モードに入ります。

既存のスイッチ スタックで自動アップグレード機能がイネーブルになっている場合は、アクティブ スイッチ が、自動的に、互換性のあるスタック メンバー上で実行されているものと同じソフトウェアイメージで新しいスイッチをアップグレードします。自動アップグレードは、一致しないソフトウェアが検出された数分後に起動します。

自動アップグレードはデフォルトでディセーブルになっています。

自動アップグレードには自動コピー プロセスと自動抽出プロセスが含まれます。

- 自動コピーは、スタック メンバー上で実行しているソフトウェアイメージを新しいスイッチに自動的にコピーして、そのスイッチをアップグレードします。また、自動コピーは、自動アップグレードがイネーブルになっている場合、新しいスイッチ上に十分なフラッシュ メモリが存在する場合、およびスイッチ スタック上で実行しているソフトウェア イメージが新しいスイッチに適合する場合に実行されます。

  （注） VM モードのスイッチでは、すべてのリリース済みのソフトウェアが稼働するとは限りません。たとえば、新しいスイッチハードウェアは以前のバージョンのソフトウェアでは認識されません。

- 自動抽出（auto-extract）は、自動アップグレードプロセスがスタック内で新しいスイッチにコピーする適切なソフトウェアを見つけられなかった場合に実行されます。この場合、自動抽出プロセスは、スイッチスタックまたは新しいスイッチをアップグレードするために必要なbinファイルを、スタック内のすべてのスイッチで検索します。binファイルは、スイッチ スタックまたは新しいスイッチ内の任意のフラッシュ ファイル システムに配置できます。スタック メンバー上で新しいスイッチに適したbinファイルが見つかった場合は、このプロセスがファイルを抽出して自動的に新しいスイッチをアップグレードします。

自動アップグレード機能は、バンドル モードで使用することはできません。スイッチ スタックは、インストール済みモードで実行する必要があります。スイッチスタックがバンドルモードになっている場合は、**software expand** 特権 EXEC コマンドを使用してインストール済みモードに変更します。

自動アップグレードをイネーブルにするには、新しいスイッチ上で **software auto-upgrade enable** グローバル コンフィギュレーション コマンドを使用します。自動アップグレードのステータスをチェックするには、**show running-config** 特権 EXEC コマンドを使用して表示された *Auto upgrade* 行を確認します。

新しいスイッチを特定のソフトウェア バンドルでアップグレードするように自動アップグレードを設定するには、**software auto-upgrade source url** グローバル コンフィギュレーション コマンドを使用します。ソフトウェア バンドルが無効になっている場合は、新しいスイッチは、互換性のあるスタック メンバー上で実行しているものと同じソフトウェア イメージでアップグレードされます。

自動アップグレードプロセスが完了すると、新しいスイッチがリロードして、完全に機能するメンバーとしてスタックに参加します。リロード時に両方のスタック ケーブルが接続されていれば、スイッチ スタックが2つのリング上で動作するため、ネットワークのダウンタイムが発生しません。

互換性のないソフトウェアを実行しているスイッチのアップグレードの詳細については、『*Cisco IOS File System, Configuration Files, and Bundle Files Appendix, Cisco IOS XE Release 3SE*（*Catalyst 3850 Switches*）』を参照してください。

自動アドバイス

自動アドバイス機能は次の場合に起動されます。

- 自動アップグレード機能がディセーブルになっている。
- 新しいスイッチがバンドルモードで、スタックがインストール済みモードになっている。自動アドバイスは、新しいスイッチをインストール済みモードに変更するための **software auto-upgrade** 特権 EXEC コマンドの使用に関する syslog メッセージを表示します。
- スタックがバンドルモードになっている。自動アドバイスは、新しいスイッチがスタックに参加できるようにするためのバンドル モードでの起動に関する syslog メッセージを表示します。
- 新しいスイッチが互換性のないソフトウェアを実行しているために、自動アップグレードの試みが失敗した。スイッチ スタックが新しいスイッチとの互換性チェックを実行した後に、自動アドバイスが、新しいスイッチが自動アップグレードできるかどうかに関する syslog メッセージを表示します。

自動アドバイスはディセーブルにできません。また、スイッチ スタック ソフトウェアと、バージョン不一致（VM）モードのスイッチのソフトウェアに同じライセンス レベルが含まれていない場合は提案を表示しません。

自動アドバイス（auto-advise）は、自動アップグレード プロセスが新しいスイッチにコピーする適切なスタック メンバー ソフトウェアを見つけられない場合に実行されます。このプロセスにより、スイッチ スタックまたは新しいスイッチを手動でアップグレードするために必要なコマンド（**archive copy-sw** または **archive download-sw** 特権 EXEC コマンド）とイメージ名（tar ファイル名）が表示されます。推奨されているイメージは、実行中のスイッチ スタック イメージまたはスイッチ スタック（新しいスイッチを含む）内のフラッシュ ファイル システム上の tar ファイルです。スタックのフラッシュ ファイル システムで適切なイメージが見つからない場合、自動アドバイス プロセスによって、スイッチ スタックに新規ソフトウェアをインストールするように伝えられます。自動アドバイスはディセーブルにできません。また、そのステータスを確認するコマンドはありません。

自動アドバイス メッセージの例

自動アップグレードがディセーブルになっており、互換性のないスイッチが参加しようとしている：例

この自動アドバイスのサンプル出力は、自動アップグレード機能がディセーブルになっており、互換性のないスイッチ1がスイッチ スタックに参加しようとした場合に表示されるシステム メッセージを示しています。

```
*Oct 18 08:36:19.379: %INSTALLER-6-AUTO_ADVISE_SW_INITIATED: 2 installer:  Auto advise
initiated for switch 1
*Oct 18 08:36:19.380: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  Searching stack for
software to upgrade switch 1
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  Switch 1 with incompatible
 software has been
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  added to the stack. The
 software running on
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  all stack members was
scanned and it has been
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  determined that the
'software auto-upgrade'
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  command can be used to
 install compatible
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  software on switch 1.
```

自動アップグレードがディセーブルになっており、新しいスイッチがバンドルモードで動作している：例

この自動アドバイスのサンプル出力は、自動アップグレードがディセーブルになっており、バンドルモードで動作しているスイッチがインストール済みモードで動作しているスタックに参加しようとした場合に表示されるシステム メッセージを示しています。

```
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW_INITIATED: 2 installer:  Auto advise
initiated for switch 1
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  Switch 1 running bundled
 software has been added
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  to the stack that is
running installed software.
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  The 'software
auto-upgrade' command can be used to
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  convert switch 1 to the
 installed running mode by
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  installing its running
 software.
```

スイッチ スタックの管理接続

スイッチ スタックおよびスタック メンバ インターフェイスは、アクティブ スイッチを経由して管理します。CLI、SNMP、およびサポートされているネットワーク管理アプリケーション（CiscoWorks など）を使用できます。個別の デバイス ごとにスタック メンバーを管理することはできません。

（注） SNMP を使用して、サポートされる MIB によって定義されるスタック全体のネットワーク機能を管理します。スイッチは、スタックのメンバーシップや選択などのスタック構成固有の機能を管理するための MIB をサポートしません。

IP アドレスによるスイッチ スタックへの接続

スイッチ スタックは、単一 IP アドレスを介して管理されます。IP アドレスは、システムレベル設定であり、アクティブ スイッチやその他のスタック メンバー固有ではありません。スタックからアクティブ スイッチまたはその他のスタック メンバーを削除しても IP 接続があれば、そのまま同じ IP アドレスを使用してスタックを管理できます。

（注） スイッチ スタックからスタック メンバーを削除した場合、各スタック メンバーは自身の IP アドレスを保持します。したがって、ネットワーク内で同じ IP アドレスを持つ 2 つのデバイスが競合するのを避けるため、スイッチ スタックから削除したデバイスの IP アドレスを変更しておきます。

スイッチ スタック設定の関連情報については、「スイッチ スタックのコンフィギュレーション ファイル」のセクションを参照してください。

コンソール ポートまたはイーサネット管理ポートによるスイッチ スタックへの接続

アクティブ スイッチに接続するには、次のいずれかの方法を使用します。

- 1 つまたは複数のスタック メンバーのコンソール ポートを経由して、端末または PC をアクティブ スイッチに接続できます。
- 1 つまたは複数の スタック メンバーのイーサネット管理ポートを経由して、PC をアクティブ スイッチに接続できます。イーサネット管理ポート経由でスイッチ スタックに接続する方法については、「イーサネット管理ポートの使用」のセクションを参照してください。

1 つまたは複数のスタック メンバのコンソール ポートを経由して、ターミナルまたは PC をスタック マスターに接続することで、アクティブ スイッチに接続できます。

アクティブ スイッチに複数の CLI セッションを使用する場合は注意が必要です。1 つのセッションで入力したコマンドは、別のセッションには表示されません。そのため、コマンドを入力したセッションを識別できなくなることがあります。

スイッチ スタックを管理する場合は、1 つの CLI セッションだけを使用することを推奨します。

スイッチ スタックの設定方法

永続的 MAC アドレス機能のイネーブル化

（注） この機能を設定するためにコマンドを入力すると、設定の結果を記述した警告メッセージが表示されます。この機能は慎重に使用してください。古い アクティブ スイッチ の MAC アドレスを同じドメイン内で使用すると、トラフィックが失われることがあります。

永続 MAC アドレスをイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**stack-mac persistent timer** [**0** | *time-value*] 例： `Device(config)# stack-mac persistent timer 7`	スタック マスターが変更された後、スタック MAC アドレスが新しいアクティブ スイッチの MAC アドレスに変更されるまでの遅延時間をイネーブルにします。この間に以前のアクティブ スイッチがスタックに再加入した場合、スタックはその MAC アドレスをスタック MAC アドレスとして使用します。 時間は 0 ～ 60 分の範囲で指定できます。 • 約 4 分というデフォルトの遅延を設定するには、値を指定しないでコマンドを入力します。必ず値を入力することを推奨します。

	コマンドまたはアクション	目的
		値を指定しないでコマンドを入力すると、実行コンフィギュレーションファイルには、遅延時間は明示タイマー値4分として書き込まれます。 • 現在のアクティブ スイッチの MAC アドレスを無期限に使用し続けるには、**0** を入力します。 スタック MAC アドレスを現在のアクティブ スイッチの MAC アドレスにただちに変更するための **no stack-mac persistent timer** コマンドを入力するまで、前のアクティブ スイッチのスタック MAC アドレスが使用されます。 • スタック MAC アドレスが新しいアクティブ スイッチの MAC アドレスに変更されるまでの時間を設定するには、*time-value* に 1 ～ 60 分の範囲内の値を入力します。 設定された時間が過ぎるまで、または **no stack-mac persistent timer** コマンドを入力するまで、以前のアクティブ スイッチのスタック MAC アドレスが使用されます。 （注） 新しいアクティブ スイッチが引き継いだ後、時間切れになる前に **no stack-mac persistent timer** コマンドを入力した場合、スイッチ スタックは現在のアクティブ スイッチ MAC アドレスに移行します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例：	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

次のタスク

永続的 MAC アドレス機能をディセーブルにするには、**no stack-mac persistent timer** グローバル コンフィギュレーション コマンドを使用します。

スタック メンバー番号の割り当て

この任意の作業は、アクティブ スイッチ からのみ使用できます。

メンバー番号をスタック メンバーに割り当てるには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**switch** *current-stack-member-number* **renumber** *new-stack-member-number* 例： `Device# switch 3 renumber 4`	スタック メンバの現在のスタック メンバ番号と新たなスタック メンバ番号を指定します。指定できる範囲は1～9です。 スタック メンバの現在のスタック メンバ番号と新たなメンバ番号を指定します。指定できる範囲は 1 ～ 2 です。 **show switch** ユーザ EXEC コマンドを使用すると、現在のスタック メンバ番号を表示できます。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 5	**reload slot** *stack-member-number* 例： `Device# reload slot 4`	スタック メンバをリセットします。
ステップ 6	**show switch** 例： `showDevice`	スタック メンバ番号を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スタック メンバー プライオリティ値の設定

この任意の作業は、アクティブ スイッチ からのみ使用できます。

プライオリティ値をスタック メンバーに割り当てるには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**switch** *stack-member-number***priority** *new-priority-number* 例： `Device# switch 3 priority 2`	スタック メンバのスタック メンバ番号と、新しいプライオリティを指定します。スタック メンバ番号の有効範囲は 1 ～ 9 です。プライオリティ値の範囲は 1 ～ 15 です。 **show switch** ユーザ EXEC コマンドを使用して、現在のプライオリティ値を表示できます。 新しいプライオリティ値はすぐに有効となりますが、現在の アクティブ スイッ

	コマンドまたはアクション	目的
		チ には影響しません。新たなプライオリティ値は、現在の アクティブ スイッチ またはスイッチ スタックのリセット時に、どのスタック メンバが新たな アクティブ スイッチ として選択されるかを決定する場合に影響を及ぼします。
ステップ 3	**show switch** *stack-member-number* 例： `Device# show switch`	スタック メンバー プライオリティ値を確認します。
ステップ 4	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ スタックへの新しいメンバーのプロビジョニング

この任意の作業は、アクティブ スイッチ からのみ使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**show switch** 例： `Device# show switch`	スイッチ スタックに関する要約情報を表示します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**switch** *stack-member-number* **provision** *type* 例： `Device(config)# switch 3 provision WS-xxxx`	事前に設定されたスイッチのスタック メンバー番号を指定します。デフォルトでは、スイッチはプロビジョニングされません。 *Stack-member-number* の範囲は 1 ～ 9 です。スイッチ スタック内でまだ使用されていないスタック メンバー番号を指

	コマンドまたはアクション	目的
		定します。ステップ 1 を参照してください。 *Type* には、コマンドライン ヘルプ ストリングに示されたサポート対象のスイッチのモデル番号を入力します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

プロビジョニングされたスイッチ情報の削除

開始する前に、スタックから割り当てられたスイッチを削除する必要があります。この任意の作業は、アクティブ スイッチ からのみ使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no switch** *stack-member-number* **provision** 例： `Device(config)# no switch 3 provision`	指定されたメンバーの割り当て情報を削除します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config** 例：	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

例

次のように設定されたスタック内の割り当てられたスイッチを削除する場合：

- スタックは 4 つのメンバーを持つ
- スタック メンバー 1 がアクティブ スイッチである
- スタック メンバー 3 が割り当てられたスイッチである

さらに、割り当てられた情報を削除し、エラー メッセージを受信しないようにするには、スタック メンバー 3 の電源を切り、スタック メンバー 3 とそれが接続されているスイッチとの間の StackWise-480 スタック ケーブルを抜き、そのケーブルを別のメンバー間に再接続して、**no switch** *stack-member-number* **provision** グローバル コンフィギュレーション コマンドを入力します。

スイッチ スタック内の非互換スイッチの表示

手順

	コマンドまたはアクション	目的
ステップ 1	**show switch** **例：** `Device# show switch`	スイッチ スタック内の非互換スイッチを表示します（[Current State] が [V-Mismatch] で表示されます）。[V-Mismatch] 状態は、非互換ソフトウェアのスイッチを示します。アクティブ スイッチ と同じライセンス レベルで実行されていないスイッチには、[Lic-Mismatch] と出力表示されます ライセンス レベルの管理については、『*System Management Configuration Guide (Catalyst 3850 Switches)*』を参照してください。

スイッチ スタックでの互換性のないスイッチのアップグレード

手順

	コマンドまたはアクション	目的
ステップ 1	**software auto-upgrade** 例： `Device# software auto-upgrade`	スイッチ スタック内の互換性のないスイッチをアップグレードします。または、バンドル モードのスイッチをインストール済みモードに変更します。
ステップ 2	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ スタックのトラブルシューティング

スタック ポートの一時的なディセーブル化

スタック ポートでフラッピングが発生し、スタック リングが不安定になっている場合に、そのポートをディセーブルにするには、**switch** *stack-member-number* **stack port** *port-number* **disable** 特権 EXEC コマンドを入力します。ポートを再びイネーブルにするには、**switch** *stack-member-number* **stack port** *port-number* **enable** コマンドを入力します。

（注） **switch** *stack-member-number* **stack port** *port-number* **disable** コマンドの使用には注意が必要です。スタック ポートをディセーブルにすると、スタックは半分の帯域幅で稼働します。

スタック ポートを通じてすべてのメンバーが接続されており、準備完了状態であれば、スタックはフルリング状態です。

次の現象が発生すると、スタックが部分リング状態になります。

- すべてのメンバがスタック ポートを通じて接続されたが、一部が ready ステートではない。
- スタック ポートを通じて接続されていないメンバーがある。

手順

	コマンドまたはアクション	目的
ステップ 1	**switch** *stack-member-number* **stack port** *port-number* **disable** 例： `Device# switch 2 stack port 1 disable`	指定されたポートをディセーブルにします。
ステップ 2	**switch** *stack-member-number* **stack port** *port-number* **enable** 例： `Device# switch 2 stack port 1 enable`	スタック ポートを再びイネーブルにします。

スタックがフルリング状態のときにスタック ポートをディセーブルにしようとする場合は、1 つのスタック ポートしかディセーブルにすることができません。次のメッセージが表示されます。

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

スタックが部分リング状態のときにスタック ポートをディセーブルにしようとしても、そのポートをディセーブルにすることができません。次のメッセージが表示されます。

```
Disabling stack port not allowed with current stack configuration.
```

他のメンバーの起動中のスタック ポートの再イネーブル化

スイッチ 1 のポート 1 がスイッチ 4 のポート 2 に接続されています。ポート 1 でフラッピングが発生した場合は、**switch 1 stack port 1 disable** 特権 EXEC コマンドを使用してポート 1 をディセーブルにすることができます。スイッチ 1 のポート 1 がディセーブルになっており、スイッチ 1 の電源がまだオンになっている状態でスタック ポートを再びイネーブルにするには、次の手順を実行します。

手順

ステップ 1 スイッチ 1 のポート 1 とスイッチ 4 のポート 2 の間のスタック ケーブルを取り外します。

ステップ 2 スタックからスイッチ 4 を取り外します。

ステップ 3 スイッチを追加してスイッチ 4 を交換し、スイッチ番号 4 を割り当てます。

ステップ 4 スイッチ 1 のポート 1 とスイッチ 4（交換後のスイッチ）のポート 2 の間のケーブルを再接続します。

ステップ 5 スイッチ間のリンクを再びイネーブルにします。**switch 1 stack port 1 enable** 特権 EXEC コマンドを入力して、スイッチ 1 のポート 1 をイネーブルにします。

ステップ 6 スイッチ 4 の電源を入れます。

⚠

注意 スイッチ 1 のポート 1 をイネーブルにする前にスイッチ 4 の電源を入れると、スイッチのいずれかがリロードされる場合があります。

最初にスイッチ 4 の電源を入れると、リンクを起動するために **switch 1 stack port 1 enable** および **switch 4 stack port 2 enable** 特権 EXEC コマンドを入力する必要がある場合があります。

デバイス スタックのモニタリング

表 *172 :* スタック情報を表示するコマンド

コマンド	説明
show switch	割り当てられたスイッチやバージョン不一致モードのスイッチのステータスなど、スタックに関するサマリー情報を表示します。
show switch *stack-member-number*	特定のメンバーに関する情報を表示します。
show switch detail	スタックに関する詳細情報を表示します。
show switch neighbors	スタック ネイバーを表示します。
show switch stack-ports [**summary**]	スタックのポート情報を表示します。スタックのケーブル長、スタックのリンク ステータス、およびループバック ステータスを表示するには、**summary** キーワードを使用します。
show redundancy	冗長システムと現在のプロセッサ情報を表示します。冗長システムの情報にはシステム稼働時間、スタンバイ失敗、スイッチオーバー理由、ハードウェア、設定冗長モードおよび動作冗長モードが含まれます。表示される現在のプロセッサ情報にはアクティブ位置、ソフトウェアの状態、現在の状態での稼働時間などが含まれます。
show redundancy state	アクティブおよびスタンバイ デバイスの冗長状態をすべて表示します。

スイッチ スタックの設定例

スイッチ スタックの設定のシナリオ

これらのスイッチ スタック設定シナリオのほとんどが、少なくとも 2 つのデバイスが StackWise-480 スタック ポート経由で接続されていることを前提とします。

表 *173 :* 設定シナリオ

シナリオ		結果
既存のアクティブ スイッチによって明確に決定されるアクティブ スイッチ選択	StackWise-480 スタック ポート経由で 2 つの電源の入ったスイッチ スタックを接続します。	2 つのアクティブ スイッチのうち 1 つだけが新しいアクティブ スイッチになります。
スタック メンバーのプライオリティ値によって明確に決定されるアクティブ スイッチ選択	**1.** StackWise-480 スタック ポート経由で 2 つのスイッチを接続します。 **2.** **switch** *stack-member-number* **priority** *new-priority-number* EXEC コマンドを使用して、一方のスタック メンバにより高いメンバ プライオリティ値を設定します。 **3.** 両方のスタック メンバーを同時に再起動します。	より高いプライオリティ値を持つスタック メンバーがアクティブ スイッチに選択されます。
コンフィギュレーション ファイルによって明確に決定されるアクティブ スイッチ選択	両方のスタック メンバーが同じプライオリティ値を持つものと仮定します。 **1.** 一方つのスタック メンバーがデフォルトのコンフィギュレーションを持ち、他方のスタック メンバーが保存済み（デフォルトでない）のコンフィギュレーション ファイルを持つことを確認します。 **2.** 両方のスタック メンバーを同時に再起動します。	保存済みのコンフィギュレーション ファイルを持つスタック メンバーがアクティブ スイッチに選択されます。

シナリオ		結果
MAC アドレスによって明確に決定されるアクティブ スイッチ選択	両方のスタック メンバーが同じプライオリティ値、コンフィギュレーション ファイル、ライセンス レベルを持っていると仮定して、両方のスタック メンバーを同時に再起動します。	MAC アドレスが小さい方のスタック メンバーがアクティブ スイッチに選択されます。
スタック メンバー番号の競合	一方のスタック メンバーが他方のスタック メンバーより高いプライオリティ値を持つものと仮定します。 **1.** 両方のスタック メンバーが同じスタック メンバー番号を持つように確認します。必要に応じて、**switch** *current-stack-member-number* **renumber** *new-stack-member-number* EXEC コマンドを使用します。 **2.** 両方のスタック メンバーを同時に再起動します。	より高いプライオリティ値を持つスタック メンバーが、自分のスタック メンバー番号を保持します。もう一方のスタック メンバーは、新たなスタック メンバー番号を持ちます。
スタック メンバーの追加	**1.** 新しいスイッチの電源を切ります。 **2.** StackWise-480 スタック ポート経由で、新しいスイッチを電源の入ったスイッチ スタックに接続します。 **3.** 新しいスイッチの電源を入れます。	アクティブ スイッチが保持されます。新たなスイッチがスイッチ スタックに追加されます。
アクティブ スイッチの障害	アクティブ スイッチを取り外します（または電源をオフにします）。	スタンバイ スイッチが新しいアクティブ スイッチになります。スタック内の他のすべてのスタック メンバーは、スタック メンバーのままで、再起動はされません。

シナリオ		結果
9 台を超えるスタック メンバーの追加	**1.** StackWise-480 スタック ポート経由で、10 台のデバイスを接続します。 **2.** すべてのデバイスの電源をオンにします。	2 台のデバイスがアクティブ スイッチになります。1 台のアクティブ スイッチが 9 台のスタック メンバーで構成されます。その他のアクティブ スイッチはスタンドアロン デバイスとして残ります。 アクティブ スイッチのデバイスとそれぞれのアクティブ スイッチに属しているデバイスを識別するには、デバイス上の Mode ボタンとポート LED を使用します。

永続的 MAC アドレス機能のイネーブル化：例

次に、永続的 MAC アドレス機能に 7 分の遅延時間を設定し、設定を確認する例を示します。

```
Device(config)# stack-mac persistent timer 7
  WARNING: The stack continues to use the base MAC of the old Master
  WARNING: as the stack MAC after a master switchover until the MAC
  WARNING: persistency timer expires. During this time the Network
  WARNING: Administrators must make sure that the old stack-mac does
  WARNING: not appear elsewhere in this network domain. If it does,
  WARNING: user traffic may be blackholed.
  Device(config)# end
  Device# show switch
  Switch/Stack Mac Address : 0016.4727.a900
  Mac persistency wait time: 7 mins
                                             H/W   Current
  Switch#  Role   Mac Address     Priority Version  State
  -----------------------------------------------------------
  *1       Active 0016.4727.a900     1      P2B     Ready
```

スイッチ スタックへの新しいメンバーの割り当て：例

次に、スタック メンバー番号 2 が設定されたスイッチをスイッチ スタックに割り当てる例を示します。 **show running-config** コマンドの出力は、プロビジョニングされたスイッチに関連付けられたインターフェイスを示します。

```
Device(config)# switch 2 provision switch_PID
  Device(config)# end
  Device# show running-config | include switch 2
  !
  interface GigabitEthernet2/0/1
  !
  interface GigabitEthernet2/0/2
  !
```

```
interface GigabitEthernet2/0/3
<output truncated>
```

show switch stack-ports summary コマンドの出力：例

スタック メンバ 2 のポート 1 だけがディセーブルです。

```
Device# show switch stack-ports summary
  Device#/   Stack    Neighbor    Cable     Link    Link    Sync       #          In
   Port#      Port                Length     OK    Active    OK     Changes    Loopback
              Status                                                To LinkOK
  --------   ------   --------   --------   ----   ------   ----   ---------   --------
    1/1      OK          3       50 cm      Yes     Yes     Yes        1         No
    1/2      Down       None     3 m        Yes     No      Yes        1         No
    2/1      Down       None     3 m        Yes     No      Yes        1         No
    2/2      OK          3       50 cm      Yes     Yes     Yes        1         No
    3/1      OK          2       50 cm      Yes     Yes     Yes        1         No
    3/2      OK          1       50 cm      Yes     Yes     Yes        1         No
```

表 *174 : show switch stack-ports summary* コマンドの出力

フィールド	説明
Switch#/Port#	メンバー番号と、そのスタック ポート番号
Stack Port Status	スタック ポートのステータス。 • Absent：スタック ポートにケーブルが検出されません。 • Down：ケーブルは検出されましたが、接続されたネイバーがアップになっていないか、スタック ポートがディセーブルになっています。 • OK：ケーブルが検出され、接続済みのネイバーが起動しています。
Neighbor	スタック ケーブルの接続先の、アクティブなメンバーのスイッチの数。
Cable Length	有効な長さは 50 cm、1 m、または 3 m です。 スイッチがケーブルの長さを検出できない場合は、値は *no cable* になります。ケーブルが接続されていないか、リンクが信頼できない可能性があります。

フィールド	説明
Link OK	スタック ケーブルが接続され機能しているかどうか。相手側には、接続されたネイバーが存在する場合も、そうでない場合もあります。 リンク パートナーは、ネイバー スイッチ上のスタック ポートのことです。 • No：このポートに接続されているスタック ケーブルがないか、スタック ケーブルが機能していません。 • Yes：このポートには正常に機能するスタック ケーブルが接続されています。
Link Active	スタック ケーブル相手側にネイバーが接続されているかどうか。 • No：相手側にネイバーが検出されません。ポートは、このリンクからトラフィックを送信できません。 • Yes：相手側にネイバーが検出されました。ポートは、このリンクからトラフィックを送信できます。
Sync OK	リンク パートナーが、スタック ポートに有効なプロトコル メッセージを送信するかどうか。 • No：リンク パートナーからスタック ポートに有効なプロトコル メッセージが送信されません。 • Yes：リンクの相手側は、ポートに有効なプロトコル メッセージを送信します。
# Changes to LinkOK	リンクの相対的安定性。 短期間で多数の変更が行われた場合は、リンクのフラップが発生することがあります。
In Loopback	スタック ケーブルがメンバのスタック ポートに接続されているかどうか。 • No：メンバーの 1 つ以上のスタック ポートに、スタック ケーブルが接続されています。 • Yes：メンバーのどのスタック ポートにも、スタック ケーブルが接続されていません。

ソフトウェア ループバック：例

メンバーが 3 つのスタックでは、スタック ケーブルですべてのメンバーが接続されます。

```
Device# show switch stack-ports summary
  Device#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync   #Changes   In
            Status            Length    OK    Active  OK     To LinkOK  Loopback
```

```
  --------  ------  --------  --------  ----  ------  ----  ---------   --------
    1/1     OK         3      50 cm     Yes    Yes    Yes        1        No
    1/2     OK         2      3 m       Yes    Yes    Yes        1        No
    2/1     OK         1      3 m       Yes    Yes    Yes        1        No
    2/2     OK         3      50 cm     Yes    Yes    Yes        1        No
    3/1     OK         2      50 cm     Yes    Yes    Yes        1        No
    3/2     OK         1      50 cm     Yes    Yes    Yes        1        No
```

スイッチ 1 のポート 1 からスタック ケーブルを切断すると、次のメッセージが表示されます。

```
01:09:55: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 3 has changed to state DOWN

  01:09:56: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 1 has changed to state
DOWN

  Device# show switch stack-ports summary
  Device#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback

  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1     Absent    None    No cable  No     No     No         1        No
    1/2     OK         2      3 m       Yes    Yes    Yes        1        No
    2/1     OK         1      3 m       Yes    Yes    Yes        1        No
    2/2     OK         3      50 cm     Yes    Yes    Yes        1        No
    3/1     OK         2      50 cm     Yes    Yes    Yes        1        No
    3/2     Down      None    50 cm     No     No     No         1        No
```

スイッチ 1 のポート 2 からスタック ケーブルを切断すると、スタックが分割されます。

スイッチ 2 とスイッチ 3 がスタック ケーブルで接続された 2 メンバー スタックのメンバーになります。

```
Device# show sw stack-ports summary
  Device#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    2/1     Down      None    3 m       No     No     No         1        No
    2/2     OK         3      50 cm     Yes    Yes    Yes        1        No
    3/1     OK         2      50 cm     Yes    Yes    Yes        1        No
    3/2     Down      None    50 cm     No     No     No         1        No
```

スイッチ 1 はスタンドアロン スイッチです。

```
Device# show switch stack-ports summary
  Device#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1     Absent    None    No cable  No     No     No         1        Yes
    1/2     Absent    None    No cable  No     No     No         1        Yes
```

スタック ケーブルが接続されたソフトウェア ループバック：例

- スイッチ 1 のポート 1 のポート ステータスが *Down* で、ケーブルが接続されています。

スイッチ 1 のポート 2 のポート ステータスが *Absent* で、ケーブルが接続されていません。

```
Device# show switch stack-ports summary
  Device#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1     Down      None    50 Cm      No     No     No       1          No
    1/2     Absent    None    No cable   No     No     No       1          No
```

- 物理ループバックでは、ケーブルはスタック ポートとスイッチの両方に接続されています。この設定を使用して、次のテストを行えます。
  - 正常に稼働しているスイッチのケーブル
  - 正常なケーブルを使用したスタック ポート

```
Device# show switch stack-ports summary
  Device#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    2/1       OK       2      50 cm     Yes    Yes    Yes       1         No
    2/2       OK       2      50 cm     Yes    Yes    Yes       1         No
```

ポート ステータスを見ると、次のことがわかります。

- スイッチ 2 はスタンドアロン スイッチである。
- ポートはトラフィックを送受信できる。

スタック ケーブルが接続されていないソフトウェア ループバック：例

```
Device# show switch stack-ports summary
  Device#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1     Absent    None    No cable   No     No     No       1         Yes
    1/2     Absent    None    No cable   No     No     No       1         Yes
```

切断されたスタック ケーブルの特定：例

すべてのスタック メンバーは、スタック ケーブルで接続されます。スイッチ 1 のポート 2 と、スイッチ 2 のポート 1 が接続されます。

次に、メンバーのポート ステータスを示します。

```
Device# show switch stack-ports summary
  Device#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
```

```
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     OK         2      50 cm     Yes    Yes    Yes        0        No
  1/2     OK         2      50 cm     Yes    Yes    Yes        0        No
  2/1     OK         1      50 cm     Yes    Yes    Yes        0        No
  2/2     OK         1      50 cm     Yes    Yes    Yes        0        No
```

スイッチ 1 のポート 2 からケーブルを切断すると、次のメッセージが表示されます。

```
%STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 2 has changed to state DOWN

  %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 1 has changed to state DOWN
```

ポート ステータスは以下の通りです。

```
  Device# show switch stack-ports summary
  Device#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1       OK       2      50 cm     Yes    Yes    Yes        1        No
    1/2     Absent    None    No cable   No     No     No        2        No
    2/1      Down     None    50 cm      No     No     No        2        No
    2/2       OK       1      50 cm     Yes    Yes    Yes        1        No
```

ケーブルの片方だけが、スタック ポート（スイッチ 2 のポート 1）に接続されます。

- スイッチ 1 のポート 2 の *Stack Port Status* 値は *Absent* で、スイッチ 2 のポート 1 の値は *Down* です。
- *Cable Length* 値は *No cable* です。

問題の診断

- スイッチ 1 のポート 2 のケーブル接続を確認します。
- スイッチ 1 のポート 2 が次の状態であれば、ポートまたはケーブルに問題があります。
  - *In Loopback* 値が *Yes* である。

  または

  - *Link OK*、*Link Active*、または *Sync OK* 値が *No* である。

スタック ポート間の不安定な接続の修正：例

すべてのメンバーは、スタック ケーブルで接続されます。スイッチ 1 のポート 2 と、スイッチ 2 のポート 1 が接続されます。

ポート ステータスは次のとおりです。

```
Device# show switch stack-ports summary
  Device#
```

```
Sw#/Port#  Port     Neighbor  Cable     Link  Link    Sync  #Changes   In
           Status             Length    OK    Active  OK    To LinkOK  Loopback
 --------  ------   --------  --------  ----  ------  ----  ---------  --------
   1/1       OK        2      50 cm     Yes    Yes    Yes       1          No
   1/2      Down      None    50 cm      No     No     No       2          No
   2/1      Down      None    50 cm      No     No     No       2          No
   2/2       OK        1      50 cm     Yes    Yes    Yes       1          No
```

問題の診断

- Stack Port Status の値が *Down* になっています。
- Link OK、Link Active、および Sync OK の値が *No* になっています。
- Cable Length の値が *50 cm* になっています。スイッチがケーブルを検出し、正しく識別しています。

スイッチ 1 のポート 2 と、スイッチ 2 のポート 1 との接続は、少なくとも 1 つのコネクタ ピンで不安定になっています。

スイッチ スタックに関する追加情報

関連資料

関連項目	マニュアル タイトル
スイッチ スタックのケーブル配線と電源供給。	*Catalyst 3850* スイッチハードウェア インストレーションガイド http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960cx_3650cx/hardware/installation/guide/b_2960cx-3560cx_hig.html
SGACL ハイ アベイラビリティ	『*Cisco TrustSec Switch Configuration Guide*』の「Cisco TrustSec SGACL High Availability」モジュール

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびライセンスされたフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 121 章

Cisco NSF with SSO の設定

- 機能情報の確認 （2689 ページ）
- NSF with SSO の前提条件 （2689 ページ）
- NSF with SSO の制約事項 （2690 ページ）
- NSF with SSO に関する情報 （2690 ページ）
- Cisco NSF with SSO の設定方法 （2697 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

NSF with SSO の前提条件

NSF with SSO の前提条件と考慮事項を次に示します。

- ルーティング プロトコルの使用には IP Services ライセンス レベルが必要です。ルーティング用 EIGRP スタブおよび OSPF は、IP Base ライセンス レベルでサポートされます。
- NSF の BGP サポートでは、ネイバー ネットワーキング デバイスが NSF 認識である必要があります。つまり、デバイスにはグレースフル リスタート機能があり、セッション確立中にOPENメッセージ内でこの機能をアドバタイズする必要があります。NSF 対応ルータが特定の BGP ネイバーにグレースフル リスタート機能がないことを検出すると、NSF 対応セッションをそのネイバーと確立しません。グレースフル リスタート機能のある他のすべてのネイバーは、この NSF 対応ネットワーキング デバイスと NSF 対応セッションを継続します。

- OSPF NSF では、すべてのネイバー ネットワーキング デバイスが NSF を認識する必要があります。NSF 対応ルータが特定のネットワーク セグメントで NSF 非認識ネイバーを検出すると、そのセグメントで NSF 機能をディセーブルにします。NSF 対応または NSF 認識ルータで完全に構成された他のネットワーク セグメントに対しては、継続して NSF 機能を提供します。

NSF with SSO の制約事項

NSF with SSO の制約事項を次に示します。

- NSF 機能は、IPv4 ルーティング プロトコルに対してのみサポートされます。NSF 機能は、IPv6 ルーティング プロトコルに対してはサポートされません。
- IP マルチキャスト ルーティングは SSO を認識しないため、NSF はサポートされません。
- NSF は、IOS-XE ソフトウェアが LAN Base モードで動作している場合は、サポートされません。
- NSF が動作するには、SSO をデバイス上に設定する必要があります。
- NSF/SSO は、IP バージョン 4 トラフィックおよびプロトコルのみをサポートします。IPv6 トラフィックはサポートしていません。
- グレースフル リスタート機能をサポートするためには、すべてのレイヤ 3 のネイバー デバイスが NSF Helper または NSF 対応である必要があります。
- IETF の場合、すべてのネイバー デバイスで NSF 認識ソフトウェア イメージが実行されている必要があります。

NSF with SSO に関する情報

NSF with SSO の概要

スイッチでは、アクティブ スイッチが使用できなくなった場合にスタンバイ スイッチが処理を引き継ぐようにすることで、障害耐性をサポートします。Cisco Nonstop Forwarding（NSF）は、ステートフル スイッチオーバー（SSO）と連動して、ネットワークを使用できない時間を最小限に抑えます。

NSF には次の利点があります。

- ネットワークのアベイラビリティの向上：NSF は、ユーザのセッション情報がスイッチオーバー後も維持されるように、ネットワーク トラフィックとアプリケーションのステート情報を転送し続けます。

- ネットワーク全体の安定性：ネットワークの安定性は、ネットワーク内でルータに障害が発生し、ルーティング テーブルが失われたときに作成されるルート フラップの数を減らすことで改善できます。
- 隣接ルータはリンク フラップを検出しません。インターフェイスはスイッチオーバーの間アップ状態のままなので、隣接ルータはリンク フラップを検出しません（リンクがダウンして、アップに戻ることはありません）。
- ルーティング フラップの回避：SSO がスイッチオーバー時にネットワーク トラフィックを転送し続けるので、ルーティング フラップが回避されます。
- スイッチオーバーの前に確立したユーザ セッションを維持します。

アクティブ スイッチとスタンバイ スイッチ間でキープアライブ メッセージが送受信されます。

- スタンバイ スイッチが応答しない場合は、新しいスタンバイ スイッチが選択されます。
- アクティブ スイッチが応答しない場合は、スタンバイ スイッチがアクティブ スイッチになります。

加えて、すべてのスタック メンバーで hello メッセージが送受信されます。

- スタック メンバーが応答しない場合は、そのメンバーがスタックから削除されます。
- スタンバイ スイッチが応答しない場合は、新しいスタンバイ スイッチが選択されます。
- アクティブ スイッチが応答しない場合は、スタンバイ スイッチがアクティブ スイッチになります。

SSO の動作

スタンバイ スイッチは、SSO モードで稼働する場合、完全に初期化されたステートで起動し、アクティブ スイッチの固定コンフィギュレーションおよび実行コンフィギュレーションと同期化します。そのあと、スタンバイ スーパーバイザ エンジンは、次のプロトコルのステートを維持し、ステートフル スイッチオーバーをサポートする機能に関するハードウェアおよびソフトウェア ステートの変更すべてを同期化して維持します。そのため、冗長アクティブ スイッチ構成内のレイヤ 2 セッションへの割り込みは最小限になります。

アクティブ スイッチに障害が発生した場合、スタンバイ スイッチがアクティブ スイッチになります。この新しいアクティブ スイッチは既存のレイヤ 2 スイッチング情報を使用して、トラフィック転送を続けます。ルーティング テーブルが新しいアクティブ スイッチに追加されるまで、レイヤ 3 の転送は延期されます。

（注） IOS-XE ソフトウェアが LAN Base ライセンス レベルで動作している場合は、SSO レイヤ 2 のみがサポートされます。

次の機能のステートは、アクティブ スイッチとスタンバイ スイッチの間で保存されます。

- 802.3

- 802.3u
- 802.3x（フロー制御）
- 802.3ab（GE）
- 802.3z（CWDM を含めたギガビット イーサネット）
- 802.3ad（LACP）
- 802.1p（レイヤ 2 QoS）
- 802.1q
- 802.1X（認証）
- 802.1D（スパニングツリー プロトコル）
- 802.3af（インライン パワー）
- PAgP
- VTP
- ダイナミック ARP インスペクション
- DHCP
- DHCP スヌーピング
- IP ソース ガード
- IGMP スヌーピング（バージョン 1 および 2）
- DTP（802.1Q および ISL）
- MST
- PVST+
- Rapid PVST
- PortFast/UplinkFast/BackboneFast
- BPDU ガードおよびフィルタリング
- 音声 VLAN
- ポート セキュリティ
- ユニキャスト MAC フィルタリング
- ACL（VACL、PACL、RACLS）
- QoS（DBL）
- マルチキャスト ストーム制御/ブロードキャストストーム制御

SSO は、次の機能と互換性があります。ただし、次の機能のプロトコル データベースはスタンバイ スイッチとアクティブ スイッチの間で同期されません。

- レイヤ 2 プロトコル トンネリング（L2PT）を備えた 802.1Q トンネリング
- ベビー ジャイアント
- ジャンボ フレーム サポート
- CDP
- フラッディング ブロック
- UDLD
- SPAN/RSPAN
- NetFlow

スイッチ上のすべてのレイヤ3プロトコルは、SSO がイネーブルにされている場合、スタンバイ スイッチで学習されます。

NSF の動作

Cisco IOS ノンストップ フォワーディング（NSF）は常にステートフル スイッチオーバー（SSO）とともに実行され、レイヤ3トラフィックの冗長性を確保します。NSF は、ルーティングについては BGP、OSPF、EIGRP ルーティング プロトコルでサポートされ、転送についてはシスコ エクスプレス フォワーディング（CEF）でサポートされています。ルーティング プロトコルでは NSF 機能および認識機能が拡張されました。これは、プロトコルを稼働するルータがスイッチオーバーを検出でき、ネットワーク トラフィックを転送し続け、ピア デバイスからのルート情報を回復するのに必要なアクションを実行できることを意味します。

ルーティングプロトコルがルーティング情報ベース（RIB）テーブルを再作成している間、それぞれのプロトコルは、CEF に依存してスイッチオーバー中にパケットの転送を続行します。ルーティング プロトコルが収束したあと、CEF は FIB テーブルを更新し、失効したルート エントリを削除します。次に、CEF は新しい FIB 情報でハードウェアを更新します。

アクティブ スイッチが BGP（**graceful-restart** コマンドを使用）、OSPF、または EIGRP ルーティング プロトコル用に設定されている場合、ルーティング更新は、アクティブ スイッチが選択されている間、自動的に送信されます。

スイッチは、IP Services ライセンス レベルでは BGP、OSPF および EIGRP プロトコルについて NSF 認識および NSF 機能をサポートし、IP Base ライセンス レベルでは EIGRP スタブについて NSF 認識をサポートします。

NSF は 2 つの主要な要素で構成されています。

- NSF 認識

  ネットワーキング デバイスが NSF 互換ソフトウェアを実行している場合、このデバイスは NSF 認識です。アクティブ スイッチ選択が発生していても NSF ルータがまだパケットを転送可能なことを隣接ルータ デバイスが検出する機能を NSF 認識といいます。レイヤ

3 ルーティング プロトコル（BGP、OSPF、EIGRP）に対する Cisco IOS 拡張機能は、CEF ルーティングテーブルが時間切れにならないように、またはNSFルータがルートをドロップしないように、ルート フラッピングを防ぐよう設計されています。NSF認識ルータは、ルーティング プロトコル情報をネイバー NSF ルータに送信します。NSF 認識は、EIGRP スタブ、EIGRP、OSPF プロトコルに対してはデフォルトでイネーブルになります。NSF 認識は BGP に対してデフォルトではディセーブルに設定されています。

- NSF 機能

  NSF をサポートするようにデバイスを設定した場合にデバイスは NSF 対応になります。NSF 認識ネイバーまたは NSF 対応ネイバーからルーティング情報を再構築します。NSF は SSO と連動して IP パケットを転送し続けることにより、アクティブ スイッチ選択のあとのレイヤ 3 ネットワークを利用できない時間を最小限にします。レイヤ 3 ルーティング プロトコル（BGP、OSPFv2、EIGRP）の再コンバージェンスは、ユーザが意識する必要がなく、バックグラウンドで自動的に実行されます。ルーティング プロトコルはネイバー デバイスから情報を回復し、シスコ エクスプレス フォワーディング（CEF）テーブルを再構築します。

（注） NSF は IPv6 をサポートしておらず、サポートしているのは IPv4 ユニキャストだけです。

Cisco Express Forwarding; シスコ エクスプレス フォワーディング

Cisco IOS ノンストップ フォワーディング（NSF）の重要な要素は、パケット転送です。シスコ製のネットワーキング デバイスでは、パケット転送はシスコ エクスプレス フォワーディング（CEF）によって実行されます。CEF は FIB を維持し、スイッチオーバー時に最新だった FIB 情報を使用して、スイッチオーバー中のパケットの転送を続行します。この機能により、スイッチオーバー中のトラフィックの中断を短くします。

通常の NSF 操作中に、アクティブなスーパバイザ スイッチ上の CEF は、現在の FIB と隣接データベースを、スタンバイ スイッチ上の FIB と隣接データベースと同期させます。スイッチオーバー時に、スタンバイ スイッチは最初 FIB と、アクティブ スイッチでカレントだったもののミラー イメージである隣接データベースを備えています。CEF はスタンバイ スイッチ上の転送エンジンに、アクティブ スイッチの CEF によって送信される変更を維持します。転送エンジンは、インターフェイスおよびデータ パスが使用可能になりしだい、スイッチオーバー後も転送を継続できます。

ルーティング プロトコルがプレフィックス単位で RIB を再び読み込み始めるため、CEF に対してプレフィックス単位のアップデートが行われます。CEFはこれを使用してFIBと隣接データベースを更新します。既存エントリと新規エントリには、最新であることを示す新しいバージョン（「エポック」）番号が付けられます。転送エンジンでは、コンバージェンス中に転送情報が更新されます。RIBが収束すると、スイッチが信号通知を行います。ソフトウェアは、現在のスイッチオーバー エポックよりも前のエポックを持った FIB および隣接エントリをす

べて削除します。これで FIB は最新のルーティング プロトコル転送情報を表示するようになります。

BGP の動作

NSF 対応ルータは BGP ピアで BGP セッションを開始し、OPEN メッセージをピアへ送信します。メッセージに含まれるものは、NSF 対応デバイスに「グレースフル」リスタート機能があるステートメントです。グレースフル リスタートは、BGP ルーティング ピアがスイッチオーバーのあとにルーティング フラップが発生するのを防ぐメカニズムです。BGP ピアがこの機能を受信した場合、メッセージを送信するデバイスが NSF 対応であることを認識しています。NSF 対応ルータ ピアおよび BGP ピアは両方ともセッションの確立時に、OPEN メッセージ内でグレースフル リスタート機能を交換する必要があります。両方のピアがグレースフル リスタート機能を示すステートメントを交換しない場合、このセッションでグレースフル リスタートは行われません。

BGP セッションがアクティブ スイッチのスイッチオーバー中に中断された場合、NSF 認識 BGP ピアが NSF 対応ルータに関連するルートすべてを失効としてマーキングしますが、一定期間の転送先を決定するためにこれらのルートを使用し続けます。この機能は、新しいアクティブ スイッチが BGP ピアでルーティング情報のコンバージェンスを待っている間に、パケットが失われないようにします。

アクティブ スイッチのスイッチオーバーが発生した後、NSF 対応ルータは BGP ピアとのセッションを再確立します。新しいセッションの確立時に、NSF 対応ルータが再起動したことを識別する新しいグレースフル リスタート メッセージを送信します。

この時点で、ルーティング情報は 2 つの BGP ピアの間で交換されます。交換が完了すると、NSF 対応デバイスはルーティング情報を使用して新しい転送情報を持った RIB および FIB で更新されます。NSF 認識デバイスはネットワーク情報を使用して、失効ルートを BGP テーブルから削除します。その後 BGP プロトコルが完全に収束されます。

BGP ピアがグレースフル リスタート機能をサポートしていない場合、OPEN メッセージ内のグレースフル リスタート機能は無視されますが、NSF 対応デバイスとの BGP セッションは確立します。この機能により、NSF 非認識（つまり NSF 機能のない）BGP ピアとの相互運用が可能になりますが、NSF 非認識 BGP ピアとの BGP セッションではグレースフル リスタートは使用できません。

（注） NSF の BGP サポートでは、ネイバー ネットワーキング デバイスが NSF 認識である必要があります。つまり、デバイスにはグレースフル リスタート機能があり、セッション確立中に OPEN メッセージ内でこの機能をアドバタイズする必要があります。NSF 対応ルータが特定の BGP ネイバーにグレースフル リスタート機能がないことを検出すると、NSF 対応セッションをそのネイバーと確立しません。グレースフル リスタート機能のある他のすべてのネイバーは、この NSF 対応ネットワーキング デバイスと NSF 対応セッションを継続します。

OSPF の動作

OSPF NSF 対応ルータがアクティブ スイッチのスイッチオーバーを実行する場合、ルータは OSPF ネイバーとリンク ステートデータベースを再同期化するため、次の作業を行う必要があります。

- ネイバー関係をリセットしないで、ネットワーク上で利用できる OSPF ネイバーを再学習します。
- ネットワークのリンク ステート データベース内容を再取得します。

NSF 対応ルータは、アクティブ スイッチのスイッチオーバーの後できるだけ迅速に、ネイバー NSF 認識デバイスに OSPF NSF 信号を送信します。ネイバー ネットワーキング デバイスは、このルータとのネイバー関係をリセットしてはならないインジケータとしてこの信号を認識します。NSF 対応ルータがネットワーク上の他のルータから信号を受信すると、ネイバー リストの再構築を始めます。

ネイバー関係が再構築されると、NSF 対応ルータはすべての NSF 認識ネイバーとデータベースの再同期化を始めます。この時点でルーティング情報は OSPF ネイバーの間で交換されます。交換が完了すると、NSF 対応デバイスはルーティング情報を使用して、失効ルートを削除し、RIB を更新して、新しい転送情報で FIB を更新します。その後、OSPF プロトコルは完全に収束されます。

（注） OSPF NSF では、すべてのネイバー ネットワーキング デバイスが NSF を認識する必要があります。NSF 対応ルータが特定のネットワーク セグメントで NSF 非認識ネイバーを検出すると、そのセグメントで NSF 機能をディセーブルにします。NSF 対応または NSF 認識ルータで完全に構成された他のネットワーク セグメントに対しては、継続して NSF 機能を提供します。

EIGRP の動作

EIGRP NSF 対応ルータが NSF 再起動後に最初に再起動したときには、ネイバーはなくトポロジテーブルは空です。ルータはインターフェイスを確立してネイバーを再取得し、トポロジとルーティングテーブルを再構築する必要があるときに、スタンバイ（今はアクティブ）スイッチから通知を受けます。再起動ルータおよびピアは、再起動ルータへのデータ トラフィック転送を中断することなく、次の作業を実行する必要があります。EIGRP ピア ルータは再起動ルータから学習したルートを維持し、NSF 再起動プロセスを介してトラフィックを転送し続けます。

ネイバーによって隣接関係がリセットされないように、再起動するルータは再起動を示すために EIGRP パケット ヘッダーの新しい再起動（RS）ビットを使用します。RS ビットは、NSF 再起動中に hello パケットと初期 INIT アップデート パケットに設定されます。Hello パケットの RS ビットを使用すると、ネイバーにすばやく NSF 再起動を通知できます。RS ビットを参照しない場合、ネイバーは INIT アップデートの受信、または Hello ホールド タイマーの期限切れによってリセットされた隣接関係を検出します。RS ビットを使用しない場合、ネイバーは、リセットされた隣接関係を NSF または通常の起動方法を使用して処理する必要があるかどうか認識できません。

helloパケットまたはINITパケットを受信することでネイバーが再起動の知らせを受信すると、ピア リスト内で再起動したピアを見つけ、再起動しているルータとの隣接関係を維持します。ネイバーはトポロジーテーブルを、最初のアップデートパケットに設定されたRSビットのある再起動ルータに送信します。このパケットはNSF認識であり、再起動ルータに役立つことを示しています。ネイバーはNSF再起動ネイバーでない場合、Helloパケットに RS ビットを設定しません。

（注） ルータが NSF を認識できていても、コールド スタートで起動されたために NSF 再起動ネイバーを支援しない場合もあります。

1 つ以上のピア ルータが NSF 認識の場合、再起動ルータはアップデートを受信してからデータベースを再構築します。再起動ルータは Routing Information Base（RIB）に通知できるように収束したかどうかを認識する必要があります。各 NSF 認識ルータは、End of Table（EOT）内容を表示するために、最新アップデート パケットの EOT マーカーを送信する必要があります。再起動ルータは EOT マーカーを受信すると、収束したことを認識します。再起動ルータはアップデートの送信を開始できます。

NSF 認識ピアは、再起動ルータから EOT 表示を受信したときに再起動ルータが収束した時間を認識します。その後ピアはトポロジーテーブルをスキャンして、送信元として再起動されたネイバーを持ったルートを検索します。ピアはルート タイムスタンプと再起動イベント タイムスタンプを比較し、ルートがまだ利用できるかどうかを判断します。ピアはアクティブになり、再起動したルータを介して利用できなくなったルート用に代替パスを検索します。

再起動ルータがすべての EOT 表示をネイバーから受信した場合、または NSF 収束タイマーが満了した場合、EIGRP は RIB にコンバージェンスを通知します。EIGRP は RIB コンバージェンス信号を待ってから、トポロジー テーブルを待機中の NSF 認識ピアすべてにフラッディングします。

Cisco NSF with SSO の設定方法

SSO の設定

あらゆるサポート対象プロトコルを持った NSF を使用するには、SSO を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**mode sso** 例： `Device(config-red)# mode sso`	SSO を設定します。このコマンドにより、スタンバイ スイッチが再起動され、SSO モードで機能を開始します。
ステップ 3	**end** 例： `Device(config-red)# end`	EXEC モードに戻ります。
ステップ 4	**show running-config** 例： `Device# show running-config`	SSO がイネーブルになっていることを確認します。
ステップ 5	**show redundancy states** 例： `Device# show redundancy states`	動作中の冗長モードを表示します。

SSO の設定例

次に、SSO 対応としてシステムを設定し、冗長ステートを表示する例を示します。

```
Device(config)# redundancy
  Device(config)# mode sso
  Device(config)# end
  Device# show redundancy states
  my state = 13 -ACTIVE
  peer state = 8 -STANDBY HOT
  Mode = Duplex
  Unit = Primary
  Unit ID = 5
  Redundancy Mode (Operational) = sso
  Redundancy Mode (Configured) = sso
  Split Mode = Disabled
  Manual Swact = Enabled
  Communications = Up
  client count = 29
  client_notification_TMR = 30000 milliseconds
  keep_alive TMR = 9000 milliseconds
  keep_alive count = 1
  keep_alive threshold = 18
  RF debug mask = 0x0
```

CEF NSF の確認

CEF NSF を確認するには、**show cef state** 特権 EXEX コマンドを使用します。

```
Device# show cef state
CEF Status:
RP instance
```

```
common CEF enabled
IPv4 CEF Status:
CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
universal per-destination load sharing algorithm, id DEA83012
IPv6 CEF Status:
CEF disabled/not running
dCEF disabled/not running
universal per-destination load sharing algorithm, id DEA83012
RRP state:
I am standby RRP: no
RF Peer Presence: yes
RF PeerComm reached: yes
RF Progression blocked: never
Redundancy mode: rpr(1)
CEF NSF sync: disabled/not running
CEF ISSU Status:
FIBHWIDB broker
No slots are ISSU capable.
FIBIDB broker
No slots are ISSU capable.
FIBHWIDB Subblock broker
No slots are ISSU capable.
FIBIDB Subblock broker
No slots are ISSU capable.
Adjacency update
No slots are ISSU capable.
IPv4 table broker
No slots are ISSU capable.
CEF push
No slots are ISSU capable.
```

NSF の BGP の設定

BGP NSF に参加しているピア デバイスすべてに BGP グレースフル リスタートを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp as-number** 例： `Device(config)# router bgp 300`	BGP ルーティング プロセスをイネーブルにして、スイッチをスイッチコンフィギュレーション モードにします。
ステップ 3	**bgp graceful-restart** 例： `Device(config)# bgp graceful-restart`	BGP グレースフル リスタート機能をイネーブルにし、BGP NSF を開始します。BGP セッションが確立されたあとでこのコマンドを入力した場合、BGP ネイバーと交換する機能のセッションを再開

	コマンドまたはアクション	目的
		する必要があります。再起動スイッチとすべてのピアでこのコマンドを入力します。

BGP NSF の確認

BGP の NSF を確認するには、BGP のグレースフル リスタートが SSO 対応ネットワーキング デバイスとネイバーデバイスに設定されているかどうかを確認する必要があります。確認する手順は、次のとおりです。

手順

ステップ 1 **show running-config** コマンドを入力して、「bgp graceful-restart」が SSO 対応スイッチの BGP 設定に表示されていることを確認します。

例：

```
Device# show running-config
.
.
.
router bgp 120
.
.
.
bgp graceful-restart
neighbor 192.0.2.0 remote-as 300
.
.
.
```

ステップ 2 各 BGP ネイバーでステップ 1 を繰り返します。

ステップ 3 SSO デバイスおよびネイバー デバイスで、グレースフル リスタート機能がアドバタイズおよび受信されたことを示していることを確認し、グレースフル リスタート機能を備えたアドレス ファミリであることを確認します。アドレス ファミリが表示されていない場合、BGP NSF も発生しません。

例：

```
Device# show ip bgp neighbors
BGP neighbor is 192.0.2.3, remote AS 1, internal link
BGP version 4, remote router ID 192.0.2.4
BGP state = Established, up for 00:02:38
Last read 00:00:38, last write 00:00:35, hold time is 180, keepalive interval is 60
seconds
Neighbor capabilities:
Route refresh: advertised and received(new)
Address family IPv4 Unicast: advertised and received
Message statistics:
InQ depth is 0
OutQ depth is 0
Sent Rcvd
Opens: 1 1
```

```
Notifications: 0 0
Updates: 0 0
Keepalives: 4 4
Route Refresh: 0 0
Total: 5 5
Default minimum time between advertisement runs is 0 seconds
.............................................................
(Remaining output deleted)
```

OSPF NSF の設定

OSPF NSF に参加しているすべてのピア デバイスは OSPF NSF を認識できるようにする必要があります。NSF ソフトウェア イメージをデバイスにインストールすれば自動的に認識するようになります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *processID* 例： `Device(config)# router ospf processID`	OSPF ルーティング プロセスをイネーブルにして、スイッチをルータ コンフィギュレーション モードにします。
ステップ 3	**nsf** 例： `Device(config)# nsf`	OSPF 用に NSF 動作をイネーブルにします。

OSPF NSF の確認

手順

ステップ 1 show running-config コマンドを入力して、「nsf」が SSO 対応デバイスの OSPF 設定に表示されていることを確認します。

例：

```
Device(config)#show running-config
route ospf 120
log-adjacency-changes
nsf
network 192.0.2.0 192.0.2.255 area 0
network 192.0.2.1 192.0.2.255 area 1
```

```
network 192.0.2.2 192.0.2.255 area 2
.
.
.
```

ステップ 2 **show ip ospf** コマンドを入力して、デバイス上で NSF がイネーブルであることを確認します。

例：

```
Device show ip ospf
Routing Process "ospf 1" with ID 192.0.2.1
Start time: 00:02:07.532, Time elapsed: 00:39:05.052
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
transit capable is 0
External flood list length 0
IETF Non-Stop Forwarding enabled
restart-interval limit: 120 sec
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
Number of interfaces in this area is 3 (1 loopback)
Area has no authentication
SPF algorithm last executed 00:08:53.760 ago
SPF algorithm executed 2 times
Area ranges are
Number of LSA 3. Checksum Sum 0x025BE0
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

EIGRP NSF の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *as-number* 例： `Device(config)# router eigrp as-number`	EIGRP ルーティング プロセスをイネーブルにして、スイッチをルータ コンフィギュレーション モードにします。
ステップ 3	**nsf** 例： `Device(config-router)# nsf`	EIGRP NSF をイネーブルにします。 「再起動」スイッチとすべてのピアでこのコマンドを入力します。

EIGRP NSF の確認

手順

ステップ 1 **running-config command** コマンドを入力して、「nsf」が SSO 対応デバイスの EIGRP 設定に表示されていることを確認します。

例：

```
Device show running-config
..
.
router eigrp 100
auto-summary
nsf
..
.
```

ステップ 2 **show ip protocols** コマンドを入力して、デバイス上で NSF がイネーブルであることを確認します。

例：

```
Device show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.0.2.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 1
Routing for Networks:
Routing on Interfaces Configured Explicitly (Area 0):
Loopback0
GigabitEthernet5/3
TenGigabitEthernet3/1
Routing Information Sources:
Gateway Distance Last Update
192.0.2.1 110 00:01:02
Distance: (default is 110)
Routing Protocol is "bgp 601"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
IGP synchronization is disabled
Automatic route summarization is disabled
Neighbor(s):
Address FiltIn FiltOut DistIn DistOut Weight RouteMap
192.0.2.0
Maximum path: 1
Routing Information Sources:
Gateway Distance Last Update
192.0.2.0 20 00:01:03
Distance: external 20 internal 200 local 200
```

第 122 章

StackWise Virtual の設定

- 機能情報の確認 （2705 ページ）
- Cisco StackWise Virtual の制約事項 （2705 ページ）
- Cisco StackWise Virtual の前提条件 （2706 ページ）
- Cisco StackWise Virtual について （2706 ページ）
- Cisco StackWise Virtual 冗長性 （2709 ページ）
- マルチシャーシ EtherChannel （2710 ページ）
- Cisco StackWise Virtual のパケット処理 （2712 ページ）
- デュアル アクティブ検出 （2716 ページ）
- Cisco StackWise Virtual の実装 （2717 ページ）
- Cisco StackWise Virtual の設定方法 （2718 ページ）
- Cisco StackWise Virtual の設定の確認 （2720 ページ）
- Cisco StackWise Virtual の機能情報 （2721 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Cisco StackWise Virtual の制約事項

- Cisco IOS XE Denali 16.3.3 では、サポートされている Cisco StackWise Virtual リンクの最大数は 4 です。

- Cisco StackWise Virtual は Cisco Catalyst 3850 シリーズ スイッチの WS-C3850-48XS-S、WS-C3850-48XS-E、WS-C3850-48XS-F-S、WS-C3850-48XS-F-E モデルでのみサポートされます。
- デュアル アクティブと StackWise Virtual リンクの設定は動的に実行され、デバイスは設定後に再起動されます。
- Cisco StackWise Virtual は、IP Services および IP Base ライセンスでサポートされます。ライセンスは 2 台の Cisco StackWise Virtual メンバー スイッチ間で一致している必要があります。ライセンスの移行では、両方の Cisco StackWise Virtual メンバー スイッチを再起動してライセンスを有効にする必要があります。

Cisco StackWise Virtual の前提条件

- Cisco StackWise Virtual ソリューションのすべてのスイッチは同じレベルのライセンスを実行している必要があります。推奨されるライセンスのレベルは IP Base または IP Services です。
- Cisco StackWise Virtual のすべてのスイッチは互換性のあるソフトウェアのバージョンを実行している必要があります。

Cisco StackWise Virtual について

StackWise Virtual の概要

Cisco StackWise Virtual は、2 台の Cisco Catalyst 3850 シリーズ スイッチを 1 つの仮想スイッチにペアリングするネットワーク システム仮想化技術です。Cisco StackWise Virtual ソリューションの Cisco Catalyst 3850 シリーズ スイッチは、コントロール プレーンと管理プレーンを 1 つにすることで業務効率を簡素化するほか、フォワーディング プレーンの分散によりシステムの帯域幅を拡大し、推奨されるネットワーク設計を使うことで弾力性のあるネットワークの構築を支援します。Cisco StackWise Virtual により、2台の Catalyst 3850 シリーズ スイッチは 40-G または10-G イーサーネット接続を使用して 1 台の論理的な仮想スイッチとして動作できます。

（注） Cisco IOS XE Denali 16.3.3 では、Cisco StackWise Virtual は Cisco Catalyst 3850 シリーズ スイッチの WS-C3850-48XS-S、WS-C3850-48XS-E、WS-C3850-48XS-F-S、WS-C3850-48XS-F-E モデルでのみサポートされます。これらはこの章で参照されているモデルです。

Cisco StackWise Virtual トポロジ

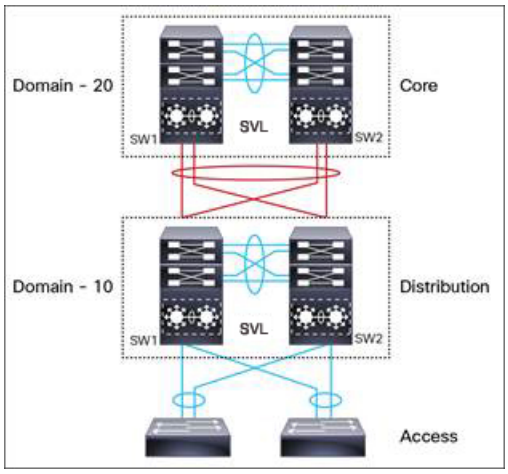
一般的なネットワーク設計は、コア、ディストリビューション、アクセス レイヤで構成されています。Cisco Catalyst 3850 シリーズ スイッチのデフォルト モードはスタンドアロンです。2 台の冗長スイッチをディストリビューション レイヤに展開する場合は、次のネットワークの課題が生じます。

- アクセス レイヤ間で VLAN ID を再使用する場合、ネットワークの全体的なパフォーマンスに影響するスパニング ツリー ループが生じる。
- スパニング ツリー プロトコル ループ、ルートおよびブリッジ プロトコル データ ユニット管理に対してレイヤ 2 ネットワークを保護するには、スパニング ツリー プロトコルと設定が必要。
- IP ゲートウェイの機能を仮想化するために、First Hop Redundancy Protocol などの追加のプロトコルが必要。これは、各 VLAN の STP ルートのプライオリティに対して整合性を確保する必要がある。
- Protocol Independent Multicast 代表ルータ（PIM DR）設定を最適化し、VLAN 上にマルチキャスト転送トポロジを選択的に構築する必要がある。
- スタンドアロンのディストリビューション レイヤ システムは、プロトコル駆動型のリモート障害検出を提供するため、コンバージェンス時間が遅くなる。FHRP と PIM のタイマーを最適化し、迅速な障害の検出と回復プロセスに対応する必要がある。

アグリゲーション レイヤとコラプスト アグリゲーション レイヤおよびコア レイヤには、Cisco StackWise Virtual モデルが推奨されます。Cisco StackWise 技術では、イーサネット ネットワーク上に拡張する場合、従来のバック スタック ケーブルの長さが制限にならないため柔軟性が得られます。スタックは冗長 40-G または 10-G ファイバ リンク上に形成でき、ディストリビューションまたはアグリゲーション スイッチを長距離にわたって展開できます。

STP では、ディストリビューション スイッチに接続されているポートの 1 つをアクセス スイッチ上でブロックし続けます。注意してください。この結果、アクティブ リンクに障害が発生すると STP コンバージェンスを引き起こし、ネットワークにはトラフィックの損失、フラッディング、トランジェント ループの可能性といった問題が生じます。一方、複数のスイッチが論理的に 1 つのスイッチにマージされている場合、ディストリビューション スイッチによりすべてのアクセス スイッチで EtherChannel バンドルを形成できるため、EtherChannel 内にリンク障害が生じても、EtherChannel 内の少なくとも 1 つのメンバーがアクティブであれば影響はありません。

図 *138 : Cisco StackWise Virtual* を使用した一般的なネットワーク設計



複数の物理スイッチの1つの論理スイッチへの仮想化は、コントロールと管理プレーンの観点のみに基づきます。コントロール プレーンが共通のため、ピア スイッチに対する 1 つの論理エンティティのように見える場合があります。スイッチのデータ プレーンは分散されます。各スイッチは、他のメンバーを使用せずにローカルのインターフェイス上で転送できる能力を備えています。ただし、スイッチに到着するパケットを異なるメンバーのポートから転送する必要がある場合は、入力スイッチで入力処理が実行された後にパケットの転送コンテキストが宛先スイッチに渡されます。出力処理は出力スイッチでのみ実行されます。これにより、宛先ポートがローカル スイッチにあるかリモート スイッチにあるかに関係なく、データ プレーンの動作はスイッチ全体で均一になります。ただし、共通のコントロールプレーンにより、各転送エンティティのデータ プレーン エントリはすべてのスイッチで同等になります。

また、Cisco StackWise Virtual をアクティブにするスイッチ、コントロール プレーンのスタンバイにするスイッチを選択する選定メカニズムもあります。アクティブ スイッチは、すべての管理、ブリッジング プロトコル、ルーティング プロトコル、およびソフトウェア データ パスを担います。これらは、Cisco StackWise Virtual アクティブ スイッチのアクティブ スーパーバイザで集中管理されます。

Cisco StackWise Virtual メンバー スイッチは、Virtual Communication Manager（VCM）と呼ばれる仮想ソフトウェア モジュールを使用して StackWise Virtual リンク上で互いに通信します。

Cisco StackWise Virtual ソリューションのコンポーネントは次の通りです。

- スタック メンバー
- StackWise Virtual リンク：10-Gb または 40-Gb イーサーネット接続

StackWise Virtual リンクは、イーサネット上でスイッチを接続するリンクです。通常、Cisco StackWise Virtual は複数の 10-G または 40-G の物理リンクで構成されています。スイッチング ユニット間のすべてのコントロール トラフィックとデータ トラフィックの伝送を行います。物理ポートは、StackWise Virtual リンクとして設定できます。スイッチの電源を入れてハードウェアが初期化されると、コントロール プレーンの初期化の前に、設定されている StackWise Virtual リンクを探します。

Cisco StackWise Virtual Header（SVH）は 64 バイトのオーバーヘッド フレームで、Cisco StackWise Virtual ドメインの 2 つのスタック メンバー間で各 SVL を通過するコントロール、データ、管理プレーンのすべてのトラフィックに追加されます。SVH カプセル化トラフィックは OSI レイヤ 2 で動作し、Cisco StackWise Virtual が有効なスイッチでのみ認識および処理できます。SVL インターフェイスはブリッジング不可で、L2 または L3 ネットワーク上でルーティング不可のトラフィックを許可します。

Cisco StackWise Virtual 冗長性

Cisco StackWise Virtual は、アクティブ スイッチとスタンバイ スイッチ間でステートフル スイッチオーバー（SSO）を行います。以下に示す方法では、Cisco StackWise Virtual の冗長モデルがスタンドアロン モードの冗長モデルと異なります。

- Cisco StackWise Virtual アクティブ スイッチとスタンバイ スイッチは別々のスイッチでホストされ、StackWise Virtual リンクを使用して情報を交換します。
- アクティブ スイッチは、Cisco StackWise Virtual の両方のスイッチを制御します。アクティブ スイッチは、レイヤ 2 およびレイヤ 3 の制御プロトコルを実行し、両方のスイッチのスイッチング モジュールを管理します。
- Cisco StackWise Virtual アクティブ スイッチとスタンバイ スイッチは、データ トラフィックの転送を実行します。

（注） Cisco StackWise Virtual アクティブ スイッチに障害が生じた場合、スタンバイ スイッチはスイッチオーバーを開始し、Cisco StackWise Virtual アクティブ スイッチの役割を引き受けます。

SSO 冗長性

StackWise Virtual システムでは、次の要件を満たしている場合に、SSO 冗長性が機能します。

- ソフトウェア アップグレード中である場合を除き、両方のスイッチが同じソフトウェア バージョンを実行していること。
- 2 台のスイッチで、StackWise Virtual リンク関連の設定が一致していること。
- ノンストップ フォワーディング（NSF）設定が SSO ピアリングの構築に依存していないこと。
- ライセンスの種類が、両方のスイッチ モデルで同じであること。
- 両方のスイッチ モデルが同じ StackWise Virtual ドメインにあること。

SSO 冗長性により、StackWise Virtual スタンバイ スイッチは、StackWise Virtual アクティブ スイッチに障害が発生した場合に常に制御を引き受けられるようになっています。設定情報、転送情報、ステート情報は、起動時や StackWise Virtual アクティブスイッチの設定が変更された

ときに、Stackwise Virtual アクティブ スイッチから冗長スイッチへ同期するようになっています。スイッチオーバー発生時のトラフィックの中断は最小限に抑えられます。

StackWise Virtual が SSO 冗長性の要件を満たしていない場合、ピア スイッチとの関係は確立できません。StackWise Virtual は、StackWise Virtual アクティブ スイッチとスタンバイ スイッチ間でステートフル スイッチオーバー（SSO）を実行します。StackWise Virtual は初期化中に各スイッチの役割を判断します。

StackWise Virtual スタンバイ スイッチの CPU はホット スタンバイ状態で実行されます。StackWise Virtual は、StackWise Virtual リンクを使用して StackWise Virtual アクティブ スイッチから StackWise Virtual スタンバイ スイッチに設定データを同期します。また、ハイ アベイラビリティをサポートしているプロトコルと機能により、StackWise Virtual スタンバイ スイッチに対してイベントやステート情報が同期されます。

ノンストップ フォワーディング

SSO 冗長モードを使用しているシステムにノンストップ フォワーディング（NSF）技術を実装すると、ネットワークの中断がキャンパスユーザとアプリケーションに対して透過的になります。高可用性は、コントロール プレーン処理スタックメンバー スイッチがリセットされる場合でも提供されます。下層のレイヤ 3 の障害時には、NSF 対応プロトコルがグレースフルネットワーク トポロジ再同期を実行します。冗長スタックメンバー スイッチにプリセットされている転送情報はそのまま残るため、このスイッチがネットワーク内でデータ転送を続行します。このサービス可用性により、平均修復時間（MTTR）は大幅に短縮され、平均故障間隔（MTBF）は拡大するため、高いレベルのネットワーク可用性が実現します。

マルチシャーシ EtherChannel

マルチシャーシ EtherChannel（MEC）は、速度やデュプレックスなどの共通の特性を持つ物理ポートがバンドルされた EtherChannel です。それらは、各 Cisco StackWise Virtual システム全体に分散されます。Cisco StackWise Virtual MEC は、EtherChannel をサポートしているネットワーク要素（ホスト、サーバ、ルータ、スイッチなど）に接続できます。Cisco StackWise Virtual は、レイヤ 2 またはレイヤ 3 モードで展開されている最大 128 の MEC をサポートします。

Cisco StackWise Virtual システムで、MEC は追加機能を備えた EtherChannel です。つまり、Cisco StackWise Virtual は、Cisco Catalyst 3850 stackWise-480 のバック スタックのように、各スイッチのポート全体でロードバランシングを行います。たとえば、トラフィックが Cisco StackWise Virtual アクティブ スイッチに入る場合、Cisco StackWise Virtual は Cisco StackWise Virtual アクティブ スイッチのパケットから生成されたハッシュに基づいて MEC リンクを選択します。

各 MEC はオプションで、Cisco PAgP、IEEE LACP、または Static ON モードのいずれかをサポートするように設定できます。Cisco PAgP または LACP を使用する EtherChannel と互換性のあるネイバーの実装が推奨されます。Cisco Wireless LAN Controller（WLC）など、リモート接続のネイバーがこのリンクバンドル プロトコルをサポートしていない場合は、Static ON モードを展開できます。これらのプロトコルは、Cisco StackWise Virtual アクティブ スイッチ上でのみ動作します。

MEC は、Cisco StackWise Virtual アクティブ スイッチと Cisco StackWise Virtual スタンバイ スイッチ間に任意の比率で分散させることができる 8 個までの物理リンクをサポートできます。MEC ポートは、両方のスイッチで均等に分散させることをお勧めします。

MEC ハッシュのサポート

（注） ローカル ハッシュは、Cisco IOS XE Denali 16.3.3 ではサポートされていません。

パケットを受信すると必ず、そのフローについて計算されたハッシュ値に基づいて宛先ポートが選択されます。宛先ポートは、MEC のポートがローカル チャネルで利用できる場合でも、リモート スイッチで選択できます。このため、MEC メンバー ポートの 1 つ以上のポートがローカル スイッチにある場合でも、ユニキャスト トラフィックが StackWise Virtual リンク上を移動することがあります。同様に、マルチキャスト トラフィックも、StackWise Virtual リンクを介して送信されます。

MEC 障害シナリオ

MEC では、各スイッチへのリンクを少なくとも 1 つは持つように構成することを推奨します。この構成により、スイッチに障害が発生した場合でも、データ トラフィックの代替パスを常に確保できます。

次のセクションでは、発生する可能性のある問題と結果の影響について説明します。

単一 MEC リンクの障害

MEC 内のリンクに障害が発生した（そして MEC 内の別のリンクは動作している）場合、通常のポートと同様に、MEC は動作しているリンク間でロード バランシングを再調整します。

Cisco StackWise Virtual アクティブ スイッチへのすべての MEC リンクの障害

Cisco StackWise Virtual アクティブ スイッチへのすべてのリンクに障害が発生した場合、MEC が Cisco StackWise Virtual スタンバイ スイッチへの動作可能なリンクを持つ通常の EtherChannel になります。

Cisco StackWise Virtual アクティブ スイッチで終了するデータ トラフィックは、Cisco StackWise Virtual スタンバイ スイッチまで StackWise Virtual リンクを介して MEC に到達します。制御プロトコルは、Cisco StackWise Virtual アクティブ スイッチで動作を続行します。プロトコル メッセージは、StackWise Virtual リンクを介して MEC に到達します。

すべての MEC リンクの障害

MEC 内のすべてのリンクに障害が発生した場合、EtherChannel の論理インターフェイスは Unavailable に設定されます。レイヤ 2 制御プロトコルは、通常の EtherChannel のリンク ダウン イベントと同様の修正措置を実行します。

隣接スイッチでは、ルーティングプロトコルとスパニングツリープロトコル（STP）により、通常の EtherChannel と同様の修正措置が実行されます。

Cisco StackWise Virtual スタンバイ スイッチの障害

Cisco StackWise Virtual スタンバイ スイッチに障害が発生した場合、MEC が、Cisco StackWise Virtual アクティブ スイッチで動作可能なリンクを持つ通常の EtherChannel として機能します。接続されているピア スイッチにより、リンクの障害が検出され、StackwWise Virtual アクティブ スイッチへのリンクだけを使用するようにロード バランシング アルゴリズムが調整されます。

Cisco StackWise Virtual アクティブ スイッチの障害

Cisco StackWise Virtual アクティブ スイッチに障害が発生すると、ステートフル スイッチオーバー（SSO）が実行されます。スイッチオーバーの完了後、MEC は新しい Cisco StackWise Virtual アクティブ スイッチで動作可能になります。接続されているピア スイッチにより、（障害となったスイッチへの）リンクの障害が検出され、新しい Cisco StackWise Virtual アクティブ スイッチへのリンクだけを使用するようにロード バランシング アルゴリズムが調整されます。

Cisco StackWise Virtual のパケット処理

Cisco StackWise Virtual では、Cisco StackWise Virtual アクティブ スイッチがレイヤ 2 およびレイヤ 3 のプロトコルと機能を実行し、両方のスイッチ上のポートを管理します。

Cisco StackWise Virtual は、StackWise Virtual リンクを使用してピア スイッチ間でシステムおよびプロトコル情報を通信し、2 台のスイッチ間でデータ トラフィックを伝送します。

ここでは、Cisco StackWise Virtual でのパケット処理について説明します。

StackWise Virtual リンク上のトラフィック

StackWise Virtual リンクでは、2 台のスイッチ間のデータ トラフィックとインバンド制御トラフィックが送信されます。StackWise Virtual リンクを介して転送されるすべてのフレームは、特殊な StackWise Virtual ヘッダー（SVH）でカプセル化されます。SVH は、制御トラフィックとデータ トラフィックで 64 バイトのオーバーヘッドを追加し、これによりピア スイッチでパケットを転送するための情報を Cisco StackWise Virtual に渡します。

StackWise Virtual リンクは、2 台のスイッチ間で制御メッセージを転送します。メッセージには、Cisco StackWise Virtual アクティブ スイッチが処理し、Cisco StackWise Virtual スタンバイ スイッチのインターフェイスが受信または送信するプロトコルメッセージが含まれます。制御トラフィックには、Cisco StackWise Virtual アクティブ スイッチと Cisco StackWise Virtual スタンバイ スイッチ上のスイッチング モジュール間のモジュール プログラミングも含まれます。

Cisco StackWise Virtual は、以下の状況下で、StackWise Virtual リンクを介してデータ トラフィックを送信します。

- VLAN 上でレイヤ 2 トラフィックのフラッディングが発生しているとき（デュアル ホーム リンクの場合でも）
- Cisco StackWise Virtual アクティブ スイッチ上のソフトウェアでパケットが処理されるが、入力インターフェイスは Cisco StackWise Virtual スタンバイ スイッチ上にあるとき
- 次のように、パケットの宛先がピア スイッチ上にあるとき
  - 既知の宛先インターフェイスがピア スイッチ上にある VLAN 内のトラフィック
  - マルチキャスト グループおよびマルチキャスト レシーバのために複製されたトラフィックがピア スイッチ上にある場合
  - 既知のユニキャスト宛先 MAC アドレスがピア スイッチ上にある場合
  - パケットが、ピア スイッチ上のポートを宛先とする MAC 通知フレームである場合

また、StackWise Virtual リンクは、NetFlow エクスポート データや SNMP データなどのシステム データを Cisco StackWise Virtual スタンバイ スイッチから Cisco StackWise Virtual アクティブ スイッチに転送します。

StackWise Virtual リンク上のトラフィックは、EtherChannel で利用できるのと同じグローバル ハッシュ アルゴリズム（デフォルトのアルゴリズムは送信元/宛先 IP）に基づいてロード バランシングされます。

Layer 2 Protocols

Cisco StackWise Virtual アクティブ スイッチは、両方のスイッチでレイヤ 2 プロトコル（STP や VTP など）を実行してスイッチング モジュールを管理します。Cisco StackWise Virtual スタンバイ スイッチのスイッチング モジュールで送受信するプロトコル メッセージは、StackWise Virtual リンクを通過して Cisco StackWise Virtual アクティブ スイッチに到達する必要があります。

Cisco StackWise Virtual のすべてのレイヤ 2 プロトコルは、スタンドアロン モードで同じように動作します。ここでは、Cisco StackWise Virtual の一部のプロトコルについて、動作の違いを説明します。

スパニングツリー プロトコル

Cisco StackWise Virtual アクティブ スイッチは STP を実行します。Cisco StackWise Virtual スタンバイ スイッチは、StackWise Virtual リンクを介して、STP BPDU を Stackwise Virtual アクティブ スイッチにリダイレクトします。

通常、STP ブリッジ ID はスイッチの MAC アドレスから導出されます。スイッチオーバー後もブリッジ ID が変わらないように、Cisco StackWise Virtual は元のスイッチの MAC アドレスを STP ブリッジ ID として使い続けます。

EtherChannel 制御プロトコル

Link Aggregation Control Protocol（LACP）パケットとポート集約プロトコル（PAgP）パケットには、デバイス ID が組み込まれます。Cisco StackWise Virtual は、両方のスイッチに共通のデバイス ID を定義します。3 つのモードがすべてサポートされている場合でも、Multi EtherChannels ではモード ON ではなく PAgP または LACP のいずれかを使用します。

（注） デュアル アクティブ シナリオ検出をサポートするため、新しい PAgP 拡張が定義されています。

スイッチド ポート アナライザ

StackWise Virtual リンク ポートではスイッチ ポート アナライザ（SPAN）はサポートされません。SVL ポートを SPAN 送信元または SPAN 宛先にすることはできません。Cisco StackWise Virtual は、非 SVL インターフェイスに対してすべての SPAN 機能をサポートします。Cisco StackWise Virtual で利用可能な SPAN セッションの数は、スタンドアロン モードで動作する単一のスイッチのものと同じです。

プライベート VLAN

Stackwise Virtual 上のプライベート VLAN は、スタンドアロン モードの場合と同じように動作します。唯一の例外は、独立トランク ポートのネイティブ VLAN を明示的に設定する必要があることです。

STP、EtherChannel 制御プロトコル、SPAN、およびプライベート VLAN 以外に、Dynamic Trunking Protocol（DTP）、Cisco Discovery Protocol（CDP）、VLAN Trunk Protocol（VTP）、Unidirectional Link Detection Protocol（UDLD）は、SVL 接続上で実行される追加のレイヤ 2 コントロール プレーン プロトコルです。

Layer 3 Protocols

Cisco StackWise Virtual アクティブ スイッチは、StackWise Virtual で使用するレイヤ 3 プロトコルと機能を実行します。すべてのレイヤ 3 プロトコル パケットは、Cisco StackWise Virtual アクティブ スイッチに送信されて処理されます。両方のメンバー スイッチは、それぞれのインターフェイスで入力トラフィックのハードウェア転送を行います。ソフトウェア転送が必要な場合、パケットは Cisco StackWise Virtual アクティブ スイッチに送信されて処理されます。

Cisco StackWise Virtual アクティブ スイッチが割り当てた同じルータ MAC アドレスが、両方の Cisco StackWise Virtual メンバー スイッチのすべてのレイヤ 3 インターフェイスに使用されます。スイッチオーバー後も、元のルータ MAC アドレスが使用されます。ルータ MAC アドレスは設定可能であり、仮想 MAC（ドメイン ID から取得）、シャーシ MAC（スイッチオーバー後も保持される）、ユーザ設定の MAC アドレスの 3 種類のオプションから選択できます。Cisco StackWise Virtual は、デフォルトで仮想 MAC アドレスを使用します。

次のセクションでは、Cisco StackWise Virtual のレイヤ 3 プロトコルについて説明します。

IPv4

Cisco StackWise Virtual アクティブ スイッチの CPU は、IPv4 ルーティング プロトコルを実行し、必要なソフトウェア転送を行います。Cisco StackWise Virtual スタンバイ スイッチで受信したすべてのルーティング プロトコル パケットは、StackWise Virtual リンク経由で Cisco StackWise Virtual アクティブ スイッチにリダイレクトされます。Cisco StackWise Virtual アクティブ スイッチは、いずれかの Cisco StackWise Virtual メンバー スイッチのポートで送信するすべてのルーティング プロトコル パケットを生成します。

ハードウェア転送は、Cisco StackWise Virtual の両方のメンバー間で分配されます。Cisco StackWise Virtual アクティブ スイッチの CPU は、Cisco StackWise Virtual スタンバイ スイッチに転送情報ベース（FIB）のアップデートを送信し、その結果すべてのルートおよび隣接関係がハードウェアにインストールされます。

ローカル隣接（ローカル ポートから到達可能）に送信されるパケットは、入力スイッチでローカルに転送されます。リモート隣接（リモート ポートから到達可能）に送信されるパケットは、StackWise Virtual を通過する必要があります。

Cisco StackWise Virtual アクティブ スイッチの CPU は、すべてのソフトウェア転送と機能の処理を実行します（フラグメンテーションやパケット存続時間超過機能など）。スイッチオーバーが発生すると、新しい Cisco StackWise Virtual アクティブ スイッチが最新の Cisco Express Forwarding 情報やその他の転送情報を取得するまで、ソフトウェア転送は中断します。

仮想スイッチ モードで Non-Stop Forwarding（NSF）をサポートするための要件は、スタンドアロン冗長動作モードと同じです。

ルーティング ピアの観点からは、マルチシャーシ EtherChannel（MEC）はスイッチオーバー中も動作可能です（故障したスイッチへのリンクがダウンしているだけで、ルーティングの隣接部分は有効）。

Cisco StackWise Virtual は、転送情報ベースのエントリにあるすべてのパスについて、それがローカルでもリモートでも、レイヤ 3 でロード バランシングを実行します。

IPv6

Cisco StackWise Virtual は、スタンドアロン システムに存在するため、IPv6 のユニキャストとマルチキャストをサポートします。

IPv4 マルチキャスト

IPv4 マルチキャスト プロトコルは Cisco StackWise Virtual アクティブ スイッチで実行されます。Cisco StackWise Virtual スタンバイ スイッチで受信する Internet Group Management Protocol（IGMP）と Protocol Independent Multicast（PIM）プロトコル パケットは、StackWise Virtual リンク経由で StackWise Virtual アクティブ スイッチに送信されます。StackWise Virtual アクティブ スイッチは、いずれかの Cisco StackWise Virtual メンバーのポートで送信する IGM および PIM プロトコル パケットを生成します。

Cisco StackWise Virtual アクティブ スイッチは、マルチキャスト転送情報ベース（MFIB）の状態を Cisco StackWise Virtual スタンバイ スイッチに同期します。両方のメンバー スイッチ上で、すべてのマルチキャスト ルートが、ローカル発信インターフェイス用にのみプログラムさ

れているレプリケーション拡張テーブル（RET）エントリと共にハードウェアにロードされます。両方のメンバー スイッチがハードウェア転送を行うことができます。

（注） スイッチオーバーによってマルチキャストルートが変更されるのを避けるために、マルチキャスト トラフィックを伝送するすべてのリンクは Equal Cost Multipath（ECMP）ではなく MEC として設定することを推奨します。

StackWise Virtual リンクを通過するパケットのために、すべてのレイヤ 3 マルチキャストの複製が出力スイッチで行われます。出力スイッチに複数のレシーバがある場合、1 パケットだけが複製され、StackWise Virtual に転送されてから、すべてのローカル出力ポートに複製されます。

ソフトウェア機能

ソフトウェア機能は、Cisco StackWise Virtual アクティブ スイッチでのみ実行されます。ソフトウェア処理が必要な Cisco StackWise Virtual スタンバイ スイッチへの着信パケットは、StackWise Virtual リンク経由で Cisco StackWise Virtual アクティブ スイッチに送信されます。

デュアル アクティブ検出

元の Cisco StackWise Virtual アクティブ スイッチが稼動したままの場合、両方のスイッチが Cisco StackWise Virtual アクティブ スイッチになります。この状況を、デュアル アクティブ シナリオと呼びます。このシナリオでは、両方のスイッチで同じ IP アドレス、SSH キー、および STP ブリッジ ID が使用されるため、ネットワークの安定性に悪影響を及ぼすことがあります。Cisco StackWise Virtual はデュアル アクティブ シナリオを検出し、リカバリ アクションを実行します。デュアルアクティブ検出リンクは、これを軽減するために使用される専用リンクです。

StackWise Virtual リンクに障害が生じた場合、Cisco StackWise Virtual スタンバイ スイッチは、Cisco StackWise Virtual アクティブ スイッチの状態を判断できません。遅延なくスイッチオーバーを確実に実行するために、Cisco StackWise Virtual スタンバイ スイッチは Cisco StackWise Virtual アクティブ スイッチに障害が発生したものと想定し、スイッチオーバーを開始して Cisco StackWise Virtual のアクティブ ロールを引き継ぎます。

デュアル アクティブ検出リンク

（注） Cisco IOS XE Denali 16.3.3 では、fast hello デュアル アクティブ検出方式のみサポートされています。

dual-active fast hello パケット検出方式を使用するには、2 台の Cisco StackWise Virtual スイッチ間に直接イーサネット接続をプロビジョニングする必要があります。最大4つのリンクをこの目的に使用できます。

2 台のスイッチは、スイッチ ステートに関する情報が記述された特殊な dual-active hello メッセージを定期的に交換します。すべての Stackwise Virtual リンクが失敗してデュアル アクティブ シナリオが生じると、各スイッチは、ピアのメッセージからデュアル アクティブ シナリオが生じていることを認識します。これにより、リカバリ アクション（2717ページ）セクションで説明するようにリカバリ アクションが開始されます。タイマーの期限が満了するまでに、予想していた dual-active fast hello メッセージをピアから受信しなかった場合、スイッチはリンクがデュアル アクティブ検出を実行できる状態にないと見なします。

リカバリ アクション

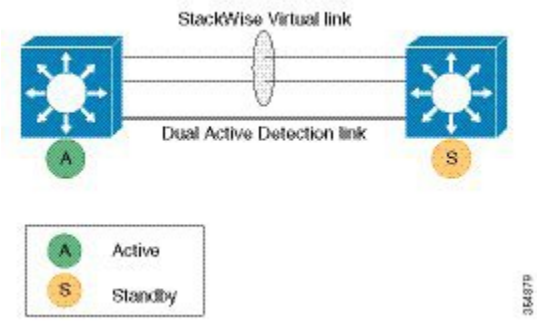
Cisco StackWise Virtual アクティブ スイッチは、デュアル アクティブ状態を検出すると、StackWise Virtual リンク以外のすべてのインターフェイスをシャットダウンし、ネットワークから自身を削除します。スイッチは、StackWise Virtual リンクが回復するまで、リカバリ モードで待機します。StackWise Virtual リンクの障害を物理的に修復し、リカバリ スイッチを手動でリロードしてスタンバイ スイッチにしてください。

Cisco StackWise Virtual の実装

Cisco StackWise Virtual の 2 ノード ソリューションは、通常、アグリゲーション レイヤに展開します。2 台の Cisco Catalyst 3850XS シリーズ スイッチを StackWise Virtual リンク（SVL）を介して接続します。

Cisco StackWise Virtual は、2 台のスイッチを多数のポートを備えた 1 つの論理スイッチへと結合し、シングル ポイント管理を行えるようにします。メンバー スイッチの 1 台がコントロールと管理のプレーンのマスターになり、もう一方のスイッチはスタンバイになります。複数の物理スイッチの1つの論理スイッチへの仮想化は、コントロールと管理の観点のみに基づきます。コントロール プレーンが共通のため、ピア スイッチに対する 1 つの論理エンティティのように見える場合があります。スイッチのデータ プレーンは集約されており、各スイッチの転送コンテキストは、スイッチ間でトラフィックが転送されるときに、さらに処理するために他のメンバー スイッチに渡されます。ただし、共通のコントロール プレーンにより、各転送エンティティのデータ プレーン エントリはすべてのスイッチで同等になります。

図 *139 : 2* ノード ソリューション



どのスイッチで Cisco StackWise Virtual をアクティブにし、どのスイッチをコントロール プレーンのスタンバイにするかを決定する選定メカニズムを使用できます。アクティブ スイッチは、管理、ブリッジング プロトコル、ルーティング プロトコル、およびソフトウェア データ パスを担います。これらは、Cisco StackWise Virtual アクティブ スイッチのアクティブなスイッチ スーパーバイザで集中管理されます。

Cisco StackWise Virtual の設定方法

Cisco StackWise Virtual 設定の構成

StackWise Virtual を有効にするには、次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**stackwise-virtual** 例： `Device(config)# stackwise-virtual`	Cisco StackWise Virtual を有効にして、StackWise Virtual サブモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**domain** *id* 例： `Device(config-stackwise-virtual)# domain 2`	（任意）Cisco StackWise Virtual ドメイン ID を指定します。 ドメイン ID の範囲は 1 ～ 255 です。デフォルト値は 1 です。

次のタスク

Cisco StackWise Virtual を有効にして必要なインターフェイスを Cisco StackWise Virtual リンクに設定してから、**show stackwise-virtual** コマンドを使用して設定情報を確認します。確認後、設定を保存してスイッチを再起動し、スタックを形成します。

Cisco StackWise Virtual リンクの設定

（注） Cisco StackWise Virtual リンクは、10-G インターフェイスの 45 ～ 48 のポート値とすべての 40-G インターフェイスでサポートされます。

StackWise Virtual リンク ポートとして 10 ギガビット イーサネット ポートを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface TenGigabitEthernet** *<interface>* 例： `Device(config)#interface TenGigabitEthernet1/0/2`	10-G イーサネット インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**stackwise-virtual link** *link value* 例：	インターフェイスと設定した StackWise Virtual リンクを関連付けます。

	コマンドまたはアクション	目的
	`Device(config-if)#stackwise-virtual link 1`	

StackWise Virtual デュアル アクティブ検出リンクの設定

StackWise デュアル アクティブ検出リンクとして 10 ギガビット イーサネット ポートを構成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface TenGigabitEthernet** *<interface>* 例： `Device(config)#interface TenGigabitEthernet1/0/2`	10-G インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**stackwise-virtual dual-active-detection** 例： `Device(config-if)#stackwise-virtual dual-active-detection`	インターフェイスを StackWise Virtual デュアル アクティブ検出に関連付けます。 （注） このコマンドは、設定後はデバイス上に表示されませんが、機能し続けます。

Cisco StackWise Virtual の設定の確認

StackWise Virtual の設定を確認するには、次の **show** コマンドを使用します。

show stackwise-virtual switch *number <1-2>*	スタック内の特定のスイッチの情報を表示します。
show stackwise-virtual link	StackWise Virtual リンク情報を表示します。

show stackwise-virtual bandwidth	Cisco StackWise Virtual で利用できる帯域幅を表示します。
show stackwise-virtual neighbors	Cisco StackWise Virtual のネイバーを表示します。
show stackwise-virtual dual-active-detection	StackWise Virtual デュアルアクティブ検出情報を表示します。

Cisco StackWise Virtual の機能情報

リリース	変更内容
Cisco IOS XE Denali 16.3.3	この機能が導入されました。

第 123 章

ワイヤレス ハイ アベイラビリティの設定

- 機能情報の確認 （2723 ページ）
- ハイ アベイラビリティについて （2723 ページ）
- 冗長性に関する情報 （2724 ページ）
- アクセス ポイントのステートフル スイッチオーバーについて （2726 ページ）
- グレースフル スイッチオーバーの開始 （2727 ページ）
- ハイ アベイラビリティ用の EtherChannel の設定 （2727 ページ）
- LACP の設定 （2728 ページ）
- ハイ アベイラビリティのトラブルシューティング （2729 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、http://www.cisco.com/go/cfn にアクセスします。Cisco.com のアカウントは必要ありません。

ハイ アベイラビリティについて

ハイ アベイラビリティ機能は、デバイスがスタック ケーブルで接続され、Cisco StackWise-480 テクノロジーがイネーブルの場合、デフォルトでイネーブルになります。これをディセーブルにはできません。ただし、コマンドライン インターフェイスを使用して手動のグレースフル スイッチオーバーを開始して、でイネーブルのハイ アベイラビリティ機能を使用することができます。

Cisco ワイヤレス LAN コントローラでは、ハイ アベイラビリティは冗長性とともに実現されます。

Cisco ワイヤレス LAN コントローラでは、冗長性は 2 通りの方法（n+1 と AP SSO 冗長性）で実現されます。

アクティブ コントローラとスタンバイ コントローラ間でキープアライブ メッセージが送受信されます。

- スタンバイ コントローラが応答しない場合は、新しいスタンバイ コントローラが選択されます。
- アクティブ コントローラが応答しない場合は、スタンバイ コントローラがアクティブ コントローラになります。

加えて、すべてのスタック メンバーで hello メッセージが送受信されます。

- スタック メンバーが応答しない場合は、そのメンバーがスタックから削除されます。
- スタンバイ コントローラが応答しない場合は、新しいスタンバイ コントローラが選択されます。
- アクティブ コントローラが応答しない場合は、スタンバイ コントローラがアクティブ コントローラになります。

冗長性に関する情報

N+1 冗長性の場合、アクセス ポイントは、第 1、第 2、および第 3 コントローラで設定されます。1 台のコントローラで管理されるアクセス ポイント数が原因で第 1 コントローラに障害が発生した場合、アクセス ポイントは第 2 コントローラにフェール オーバーします。AP SSO 冗長性の場合、第 1 コントローラが使用できない場合、アクセス ポイントはそのコントローラを再検出し、第 2 コントローラで CAPWAP トンネルを再確立します。ただし、コントローラに再度参加させるには、すべてのクライアントを切断して、再認証を実行する必要があります。

選択したアクセス ポイントおよび選択したコントローラ用の第 1、第 2、および第 3 コントローラを設定できます。

理想的なハイ アベイラビリティ展開では、第 1 および第 2 コントローラに接続されたアクセス ポイントを持つことができ、1 台のコントローラは、アクセス ポイントへ接続せずに維持できます。このように、アクセス ポイントを持たないコントローラは障害発生時に引き継ぐことができ、アクティブなコントローラのサービスを再開できます。

アクセス ポイントの冗長性の設定

選択したアクセス ポイントの第 1、第 2、または第 3 コントローラを設定するには、この項に説明されているコマンドを使用する必要があります。

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	conf t **例：** `Controller # conf t`	端末を設定します。
ステップ 2	ap capwap backup primary **例：** `Controller # ap capwap backup primary WLAN-Controller-A`	選択したアクセス ポイントの第 1 コントローラを設定します。
ステップ 3	**ap capwap backup secondary** **例：** `Controller # ap capwap backup secondary WLAN-Controller-B`	選択したアクセス ポイントの第 2 コントローラを設定します。
ステップ 4	ap capwap backup tertiary **例：** `Controller # ap capwap backup tertiary WLAN-Controller-C`	選択したアクセス ポイントの第 3 コントローラを設定します。

次のタスク

選択したアクセス ポイントの第 1、第 2、および第 3 コントローラの設定が完了したら、**show ap name** *AP-NAME* コマンドを使用して設定を確認する必要があります。**show ap name** *AP-NAME* コマンドの詳細については、『Lightweight Access Point Configuration Guide for Cisco Wireless LAN Controller』を参照してください。

-

ハートビート メッセージの設定

ハートビート メッセージを使用して、コントローラの障害検出時間を短縮することができます。障害が発生すると、コントローラがハートビートタイマーを待機した後にアクティブからホットスタンバイへのスイッチオーバーが発生します。コントローラがハートビート時間内に動作しない場合は、スタンバイがアクティブ コントローラとして引き継ぎます。理想的には、アクセス ポイントが指定されたタイムアウト値以内に 3 つのハートビート メッセージを生成し、コントローラがタイムアウト値以内に応答しない場合、スタンバイ コントローラがアクティブ コントローラを引き継ぎます。ネットワークに応じてタイムアウト値を指定できます。理想的には、スイッチオーバーの実行時に混乱が生じるためタイマー値は高くない値にします。この項では、コントローラの障害検出時間を短縮するために、タイムアウト値を使用してコントローラとアクセス ポイント間のハートビート間隔を設定する方法について説明します。

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	conf t 例： `controller # conf t`	端末を設定します。
ステップ 2	ap capwap timers heartbeat-timeout 例： `controller #  ap capwap timers heartbeat-timeout`	コントローラとアクセス ポイント間のハートビート間隔を設定します。タイムアウト値の範囲は 1 ～ 30 です。

アクセスポイントのステートフルスイッチオーバーについて

アクセス ポイント ステートフル スイッチオーバー（AP SSO）とは、すべてのアクセス ポイントがステートフルにスイッチオーバーし、ユーザセッション情報がスイッチオーバー中も維持され、アクセス ポイントがネットワーク内でセッションを失うことなく動作継続することで、ネットワークの可用性が高まることを意味します。スタックのアクティブ は、IP 機能やルーティング情報交換を含め、すべてのネットワーク機能を実行するよう装備されます。は、1000 アクセス ポイントと 12000 クライアントをサポートします。

ただし、スイッチオーバー発生時に FlexConnect モードでローカルにスイッチされるクライアントを除き、すべてのクライアントが認証解除され新しいアクティブに再度関連付けられる必要があります。

スタック内で冗長ペアが形成されると、ハイアベイラビリティが実現します。これには、アクティブからスタンバイへのスイッチオーバーの間もアクセスポイントが接続された状態を維持することが含まれます。

（注） デバイスが冗長ペアを形成した後は、 スタック内で AP SSO をディセーブルにできません。

（注） スイッチオーバーの後、新しいスタンバイがスタック構成時にリロードされた場合は、一括同期できないことが理由です。これは正常にスタック構成をするための2回目の試行で、リロード後に見られます。これは、コマンド *exception dump device second flash* を実行すると発生します。このコマンドは、クラッシュ情報ディレクトリがフルの場合に、クラッシュファイルをフラッシュにダンプするために使用されます。クラッシュが発生し、クラッシュ情報に領域が残されていない場合には、fullcore または crash ファイルをフラッシュに保存します。

グレースフル スイッチオーバーの開始

手動スイッチオーバーを実行し、で有効なハイ アベイラビリティ機能を使用するには、**redundancy force-switchover** コマンドを実行します。このコマンドは、アクティブからスタンバイ へのグレースフル スイッチオーバーを開始します。

```
Device# redundancy force-switchover
System configuration has been modified. Save ? [yes/no] : yes
Building configuration …
Preparing for switchover …
Compressed configuration from 14977 bytes to 6592 bytes[OK]This will reload the active
unit and force switchover to standby[confirm] : y
```

ハイ アベイラビリティ用の EtherChannel の設定

LAG または EtherChannel は、スタンバイ装置とアクティブ装置の両方の既存のポートすべてを単一の論理ポートにバンドルし、60 Gbps の集約帯域幅を実現します。EtherChannel の作成は、障害に対する保護を可能にします。作成された Etherchannel または LAG は、アクセス ポイントのハイ アベイラビリティを確保するための冗長リンクに使用されます。

EtherChannel の設定と EtherChannel モードの詳細については、『Layer 2 (Link Aggregation) Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)』を参照してください。

手順

ステップ 1 スタック ケーブルを使用して、電力がダウン状態の 2 台のデバイスを接続します。

ステップ 2 両方のデバイスに同時に電源投入して起動するか、1 台のに電源投入して起動します。

デバイスが正常起動し、ハイ アベイラビリティ ペアを形成します。

ステップ 3 装置で EtherChannel または LAG を設定します。

ステップ 4 設定した EtherChannel のステータスを表示するには、**show etherchannel summary** コマンドを使用します。

設定が完了すると、指定されたすべてのポートは単一のチャネルにバンドルされ、**show etherchannel summary** コマンドの出力に表示されます。

ステップ 5 **show ap uptime** コマンドを実行して、接続されたアクセス ポイントを確認します。

LACP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *number* 例： `Device(config)# interface Port-channel Po2`	ポートチャネル インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**lacp max-bundle** *number* 例： `Device(config-if)# lacp max-bundle 6`	ポートチャネルで許可される、アクティブなバンドルされた LACP ポートの最大数を定義します。値の範囲は 1 ～ 8 です。
ステップ 4	**lacp port-priority** *number* 例： `Device(config-if)# lacp port-priority 4`	LACP を使用するポートに設定するポート プライオリティを指定します。値の範囲は 0 ～ 65535 です。
ステップ 5	**switchport backup interface** *po2* 例： `Device(config-if)# switchport backup interface Po2`	バックアップ インターフェイスとしてインターフェイスを指定します。
ステップ 6	**end**	インターフェイスとコンフィギュレーション モードを終了します。
ステップ 7	**show etherchannel summary** 例： `Device# show etherchannel summary`	EtherChannel プロパティの概要を表示します。
ステップ 8	**show interfaces switchport backup** 例： `Device# show interfaces switchport backup`	バックアップ EtherChannel のプロパティの概要を表示します。

ハイ アベイラビリティのトラブルシューティング

スタンバイ コンソールへのアクセス

スタック内のアクティブ のコンソールにのみアクセスできます。スタンバイ にアクセスするには、次のコマンドを使用します。

始める前に

シスコ サポートの管理下でのみこの機能を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service internal** 例： `Device(config)# service internal`	Cisco IOS デバッグ コマンドをイネーブルにします。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 4	**main-cpu** 例： `Device(config)# main-cpu`	冗長メイン コンフィギュレーション サブモードを開始します。
ステップ 5	**standby console enable** 例： `Device(config)# standby console enable`	スタンバイ コンソールをイネーブルにします。
ステップ 6	**exit** 例： `Device(config)# exit`	コンフィギュレーション モードを終了します。

スイッチオーバー前

スイッチオーバーはに障害が発生した場合に発生します。ただし、手動スイッチオーバーの実行時は、次のコマンドを実行して正常なスイッチオーバーを開始することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**show redundancy states** 例： `Device# show redundancy states`	アクティブおよびスタンバイ デバイスのハイ アベイラビリティ ロールを表示します。
ステップ 2	**show switch detail** 例： `Device# show switch detail`	スタックの物理特性を表示します。スタックの物理状態が「Ready」または「Port」かどうか確認します。
ステップ 3	**show platform ses states** 例： `Device# show platform ses states`	スタック マネージャのシーケンスを表示します。
ステップ 4	**show ap summary** 例： `Device# show ap summary`	アクティブおよびスタンバイ デバイスのすべてのアクセス ポイントを表示します。
ステップ 5	**show capwap detail** 例： `Device# show capwap detail`	アクティブおよびスタンバイ デバイスの CAPWAP トンネルの詳細を表示します。
ステップ 6	**show dtls database-brief** 例： `Device# show dtls database-brief`	アクティブおよびスタンバイ デバイスの DTLS の詳細を表示します。
ステップ 7	**show power inline** 例： `Device# show power inline`	イーサネットの電源状態を表示します。 （注） フェールオーバーが発生時した場合、正常なスイッチオーバーのために、SSO では、スタンバイ コントローラはスタンバイホット状態、冗長ポートはターミナル状態である必要があります。

スイッチオーバー後

ここでは、アクティブからスタンバイ へのスイッチオーバーが実行されるのを保障するため、ユーザが実行する必要のある手順を定義します。スタンバイ からアクティブへのスイッチオーバー成功後、アクティブへ接続されたすべてのアクセス ポイントはスタンバイ（その後アクティブ）に再参加する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**show ap uptime** 例： `Device# show ap uptime`	スイッチオーバー後のアクセス ポイントのアップタイムが十分に大きいかどうかを確認します。
ステップ 2	**show wireless summary** 例： `Device# show wireless summary`	アクティブ に接続されているクライアントを表示します。
ステップ 3	**show wcdb database all** 例： `Device# show wcdb database all`	クライアントがアップタイムに達したかを表示します。
ステップ 4	**show power inline** 例： `Device# show power inline`	Power over Ethernet の電源状態を表示します。

デバイス スタックのモニタリング

表 *175*：スタック情報を表示するコマンド

コマンド	説明
show switch	割り当てられたスイッチやバージョン不一致モードのスイッチのステータスなど、スタックに関するサマリー情報を表示します。
show switch *stack-member-number*	特定のメンバーに関する情報を表示します。
show switch detail	スタックに関する詳細情報を表示します。
show switch neighbors	スタック ネイバーを表示します。
show switch stack-ports [**summary**]	スタックのポート情報を表示します。スタックのケーブル長、スタックのリンク ステータス、およびループバック ステータスを表示するには、**summary** キーワードを使用します。

コマンド	説明
show redundancy	冗長システムと現在のプロセッサ情報を表示します。冗長システムの情報にはシステム稼働時間、スタンバイ失敗、スイッチオーバー理由、ハードウェア、設定冗長モードおよび動作冗長モードが含まれます。表示される現在のプロセッサ情報にはアクティブ位置、ソフトウェアの状態、現在の状態での稼働時間などが含まれます。
show redundancy state	アクティブおよびスタンバイ デバイスの冗長状態をすべて表示します。

LACP の設定：例

次に、LACP を設定して LACP バンドルの作成と状態を確認する例を示します。

```
Device(config)# !
interface TenGigabitEthernet1/0/1
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/2
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/3
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/4
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/5
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/6
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/1
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/2
 switchport mode trunk
```

```
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/3
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/4
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/5
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/6
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface Vlan1
 no ip address
 ip igmp version 1
 shutdown
!

Device#  show etherchannel summary

  Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Te1/0/1(P)  Te1/0/2(P)  Te1/0/3(P)
                                 Te1/0/4(H)  Te1/0/5(H)  Te1/0/6(H)
                                 Te2/0/1(P)  Te2/0/2(P)  Te2/0/3(P)
                                 Te2/0/4(H)  Te2/0/5(H)  Te2/0/6(H)
```

次に、スイッチのバックアップ インターフェイス ペアの例を示します。

```
Device# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------------
```

```
Port-channel1             Port-channel2             Active Standby/Backup Up
```

次に、に設定された EtherChannel の概要の例を示します。

```
Device# show ethernet summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Te1/0/1(P)  Te1/0/2(P)  Te1/0/3(P)
                                 Te1/0/4(P)  Te1/0/5(P)  Te1/0/6(P)
2      Po2(SU)         LACP      Te2/0/1(P)  Te2/0/2(P)  Te2/0/3(P)
                                 Te2/0/4(P)  Te2/0/5(P)  Te2/0/6(P)
```

第 XIX 部

システム管理

- スイッチの管理 （2737 ページ）
- ブート整合性の可視性 （2775 ページ）
- デバイスのセットアップ設定の実行 （2781 ページ）
- 自律ネットワーキングの設定 （2823 ページ）
- Right-To-Use ライセンスの設定 （2833 ページ）
- 管理者のユーザ名とパスワードの設定 （2851 ページ）
- 802.11 パラメータおよび帯域選択の設定 （2857 ページ）
- アグレッシブ ロード バランシングの設定 （2877 ページ）
- クライアント ローミングの設定 （2883 ページ）
- 有線ネットワークでの Application Visibility and Control の設定 （2899 ページ）
- ワイヤレス ネットワークでの Application Visibility and Control の設定 （2925 ページ）
- ロケーションの設定 （2953 ページ）
- 音声パラメータとビデオ パラメータの設定 （2963 ページ）
- RFID タグ追跡の設定 （2987 ページ）
- ロケーションの設定 （2991 ページ）
- Cisco Hyperlocation （3001 ページ）
- フロー制御のモニタリング （3011 ページ）
- SDM テンプレートの設定 （3015 ページ）
- システム メッセージ ログの設定 （3023 ページ）
- オンライン診断の設定 （3039 ページ）
- コンフィギュレーション ファイルの管理 （3051 ページ）

• コンフィギュレーションの置換とロールバック （3093 ページ）
• フラッシュ ファイル システムの操作 （3111 ページ）
• スイッチ ソフトウェアのアップグレード （3125 ページ）
• 条件付きデバッグとラジオアクティブ トレース （3127 ページ）
• ソフトウェア設定のトラブルシューティング （3135 ページ）

第 124 章

スイッチの管理

- 機能情報の確認 （2737 ページ）
- デバイスの管理に関する情報 （2737 ページ）
- デバイスを管理する方法 （2746 ページ）
- デバイスのモニタリングおよび保守の管理 （2767 ページ）
- デバイス管理の設定例 （2768 ページ）
- デバイス管理に関する追加情報 （2771 ページ）
- デバイス管理に関する追加情報 （2772 ページ）
- デバイス管理の機能履歴と情報 （2774 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

デバイスの管理に関する情報

システム日時の管理

デバイスのシステム日時は自動設定方式（RTC および NTP）または手動設定方式を使用して管理できます。

（注） ここで使用するコマンドの構文および使用方法の詳細については、*Cisco.com* で、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

システム クロック

時刻サービスの基本となるのはシステム クロックです。このクロックはシステムがスタートアップした瞬間から稼働し、日時を常時トラッキングします。

システム クロックは、次のソースにより設定できます。

- NTP
- 手動設定

システム クロックは、次のサービスに時刻を提供します。

- ユーザの **show** コマンド
- ログおよびデバッグ メッセージ

システム クロックは、グリニッジ標準時（GMT）とも呼ばれる協定世界時（UTC）に基づいて内部的に時刻を追跡します。ローカルのタイムゾーンおよび夏時間に関する情報を設定することにより、時刻がローカルのタイム ゾーンに応じて正確に表示されるようにできます。

システムクロックは、時刻に信頼性があるかどうか（つまり、信頼できると見なされるタイムソースによって時刻が設定されているか）を常時トラッキングします。信頼性のない場合は、時刻は表示目的でのみ使用され、再配信されません。

ネットワーク タイム プロトコル

NTPは、ネットワーク上のデバイス間の時刻の同期化を目的に設計されています。NTPはユーザ データグラム プロトコル（UDP）で稼働し、UDP は IP 上で稼働します。NTP は RFC 1305 で規定されています。

NTP ネットワークは通常、タイム サーバに接続されたラジオ クロックやアトミック クロックなど、正規の時刻源から時刻を取得します。NTPは、ネットワークにこの時刻を分配します。NTP はきわめて効率的で、1 分間に 1 パケットを使用するだけで、2 台のデバイスを 1 ミリ秒以内に同期化できます。

NTP では、信頼できるタイム ソースから各マシンが何 NTP ホップ隔たっているかを表すために、ストラタムという概念が使用されます。ストラタム 1 タイム サーバには、ラジオ クロックまたは原子時計が直接接続されており、ストラタム 2 タイム サーバは、NTP を使用してストラタム 1 タイム サーバから時刻を取得します（以降のストラタムも同様です）。NTP が稼働するデバイスは、タイム ソースとして、NTP を使用して通信するストラタム番号が最小のデバイスを自動的に選択します。この方法によって、NTP時刻配信の自動編成型ツリーが効率的に構築されます。

NTPでは、同期化されていないデバイスと同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

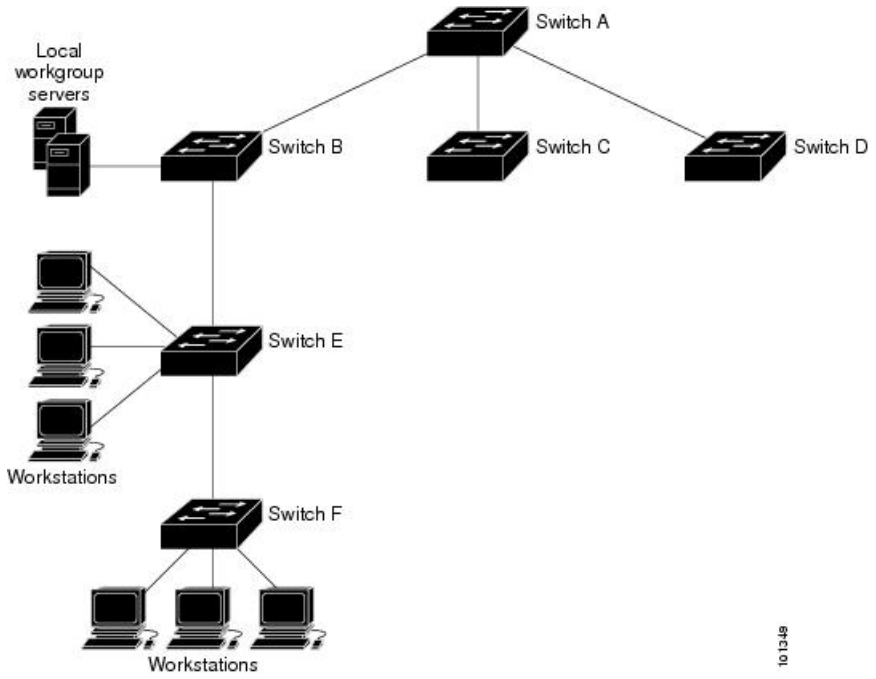
NTPが稼働するデバイス間の通信（アソシエーション）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するようにNTPを設定できます。各デバイスを、単にブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られます。

デバイス上で維持される時刻は、重要なリソースです。NTPのセキュリティ機能を使用して、不正確な時刻が誤って、あるいは意図的に設定されることがないようにしてください。その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

シスコによる NTP の実装では、ストラタム 1 サービスをサポートしていないため、ラジオ クロックまたは原子時計に接続できません。ネットワークの時刻サービスは、IPインターネット上のパブリック NTP サーバから取得することを推奨します。

次の図に NTP を使用した一般的なネットワークの例を示します。デバイス A は、NTP サーバ モードで設定した**デバイス** B、C、D の NTP マスターです。スイッチ B、C、D とデバイス A の間にはサーバ アソシエーションが設定されています。デバイス E はアップストリームおよびダウンストリーム デバイス、デバイス B およびデバイス F それぞれの NTP ピアとして設定されます。

図 *140 :* 一般的な *NTP* ネットワークの構成



ネットワークがインターネットから切り離されている場合、シスコの NTP によって、実際には、他の方法で時刻を学習しているにもかかわらず、デバイスが NTP を使用して同期化しているように動作を設定できます。他のデバイスは、NTP によりこのデバイスと同期化されます。

複数のタイム ソースがある場合は、NTP は常に、より信頼性があると見なされます。NTP の時刻は、他の方法による時刻に優先します。

自社のホスト システムに NTP ソフトウェアを組み込んでいるメーカーが数社あり、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホスト システムも時間が同期化されます。

NTP ストラタム

NTP では、信頼できるタイム ソースから各マシンが何 NTP ホップ隔たっているかを表すために、ストラタムという概念が使用されます。ストラタム 1 タイム サーバには、ラジオ クロックまたは原子時計が直接接続されており、ストラタム 2 タイム サーバは、NTP を使用してストラタム 1 タイム サーバから時刻を取得します（以降のストラタムも同様です）。NTP が稼働するデバイスは、タイム ソースとして、NTP を使用して通信するストラタム番号が最小のデバイスを自動的に選択します。この方法によって、NTP時刻配信の自動編成型ツリーが効率的に構築されます。

NTP では、同期化されていないデバイスと同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

NTP アソシエーション

NTPが稼働するデバイス間の通信（アソシエーション）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するようにNTPを設定できます。各デバイスを、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られます。

NTP セキュリティ

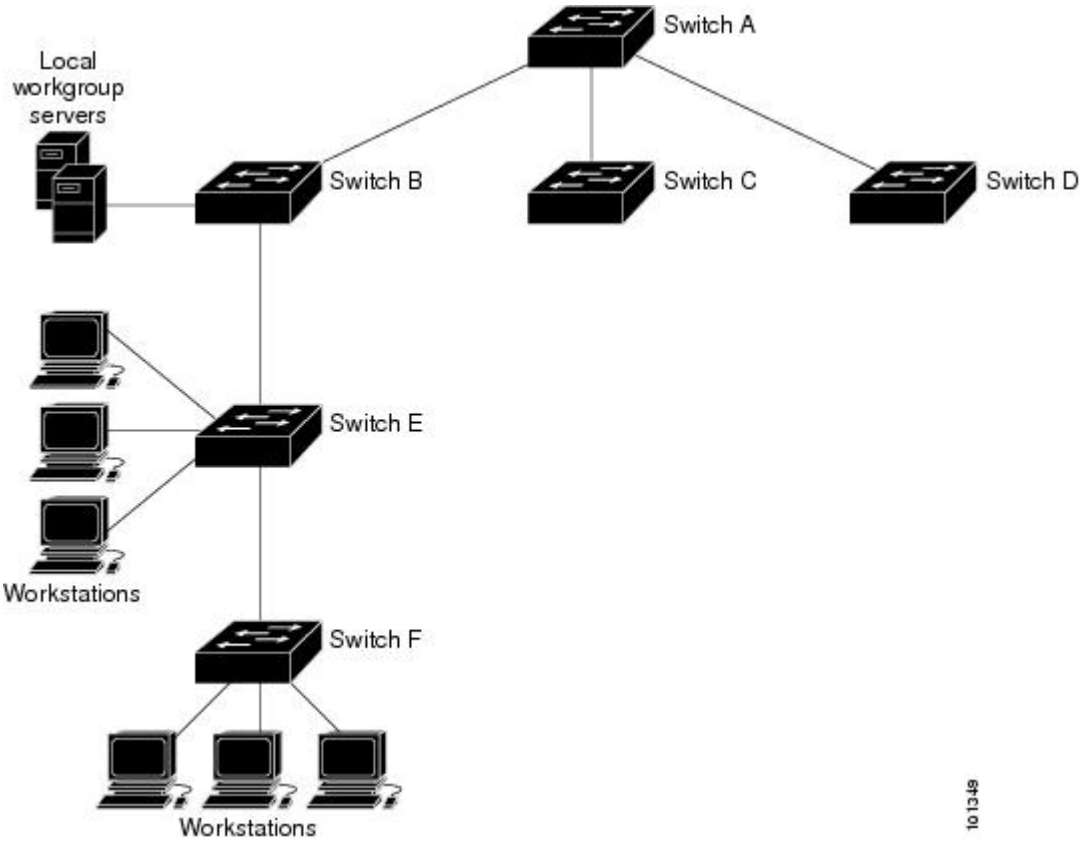
デバイス上で維持される時刻は、重要なリソースです。NTPのセキュリティ機能を使用して、不正確な時刻が誤って、あるいは意図的に設定されることがないようにしてください。その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

NTP の実装

NTP の実装では、ストラタム 1 サービスがサポートされないため、ラジオ クロックまたは原子時計に接続できません。ネットワークの時刻サービスは、IPインターネット上のパブリック NTP サーバから取得することを推奨します。

図 *141*：一般的な *NTP* ネットワークの構成

次の図はNTPを使用した一般的なネットワークの例を示します。スイッチAは、スイッチB、C、D が NTP サーバ モードに設定されている（スイッチ A との間にサーバ アソシエーションが設定されている）場合のNTPマスターです。スイッチEは、アップストリーム スイッチ（スイッチ B）とダウンストリーム スイッチ（スイッチ F）の NTP ピアとして設定されます。



ネットワークがインターネットから切り離されている場合、NTPによって、実際には、他の方法で時刻を取得している場合でも、NTPを使用した同期化と同様にデバイスの動作を設定できます。他のデバイスは、NTP によりこのデバイスと同期化されます。

複数のタイム ソースがある場合は、NTP は常に、より信頼性があると見なされます。NTP の時刻は、他の方法による時刻に優先します。

自社のホスト システムに NTP ソフトウェアを組み込んでいるメーカーが数社あり、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホスト システムも時間が同期化されます。

NTP バージョン 4

デバイスには、NTP バージョン 4 が実装されています。NTPv4 は NTP バージョン 3 の拡張版です。NTPv4 は IPv4 と IPv6 の両方をサポートし、NTPv3 との下位互換性があります。

NTPv4 は次の互換性を提供します。

- IPv6 のサポート。
- NTPv3 よりさらに向上したセキュリティ。NTPv4 プロトコルは、公開キー暗号化および標準 X509 認証に基づくセキュリティ フレームワークを提供します。
- ネットワークに対する時間分布ヒエラルキーの自動計算。特定のマルチキャスト グループを使用して、NTPv4 は、最も低い帯域幅コストで最高の時間精度を達成するサーバのヒエラルキーを自動的に設定します。この機能では、サイトローカル IPv6 マルチキャスト アドレスが活用されます。

NTPv4 の設定の詳細については、『*Cisco IOS IPv6 Configuration Guide, Release 12.4T*』の「*Implementing NTPv4 in IPv6*」の章を参照してください。

システム名およびシステム プロンプト

デバイスを識別するシステム名を設定します。デフォルトでは、システム名およびシステム プロンプトは デバイス です。

システム プロンプトを設定していない場合は、システム名の最初の 20 文字がシステム プロンプトとして使用されます。大なり記号（>）が付加されます。システム名が変更されると、プロンプトは更新されます。

ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*, *Release 12.4*』および『*Cisco IOS IP Command Reference*, *Volume 2 of 3: Routing Protocols*, *Release 12.4*』を参照してください。

スタックのシステム名およびシステム プロンプト

アクティブ スイッチを介してスタック メンバにアクセスする場合は、**session** *stack-member-number* 特権 EXEC コマンドを使用する必要があります。スタック メンバ番号の有効範囲は 1 ～ 4 です。このコマンドを使用すると、スタック メンバの番号がシステム プロンプトの末尾に追加されます。たとえば、Switch-2# はスタック メンバ 2 の特権 EXEC モードのプロンプトであり、スイッチ スタックのシステム プロンプトは Switch です。

デフォルトのシステム名とプロンプトの設定

デフォルトのスイッチのシステム名およびプロンプトは *Switch* です。

DNS

DNS プロトコルは、ドメイン ネーム システム（DNS）を制御します。DNS とは分散型データベースであり、ホスト名を IP アドレスにマッピングできます。デバイスに DNS を設定すると、**ping**、**telnet**、**connect** などのすべての IP コマンドおよび関連する Telnet サポート操作で IP アドレスの代わりにホスト名を使用できます。

IP によって定義される階層型の命名方式では、デバイスを場所またはドメインで特定できます。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。たとえば、シスコは、IP で *com* というドメイン名に分類される商業組織なので、ドメイン名は *cisco.com*

となります。このドメイン内の特定のデバイス、たとえばファイル転送プロトコル（FTP）システムは、*ftp.cisco.com* で表されます。

IP ではドメイン名をトラッキングするために、ドメイン ネーム サーバという概念が定義されています。ドメイン ネーム サーバの役割は、名前から IP アドレスへのマッピングをキャッシュ（またはデータベース）に保存することです。ドメイン名を IP アドレスにマッピングするには、まず、ホスト名を明示し、ネットワーク上に存在するネーム サーバを指定し、DNS をイネーブルにします。

DNS のデフォルト設定値

表 *176 : DNS* のデフォルト設定値

機能	デフォルト設定
DNS イネーブル ステート	イネーブル
DNS デフォルト ドメイン名	未設定
DNS サーバ	ネーム サーバのアドレスが未設定

ログイン バナー

Message-of-The-Day（MoTD）バナーおよびログイン バナーを作成できます。MOTD バナーはログイン時に、接続されたすべての端末に表示されます。すべてのネットワーク ユーザに影響するメッセージ（差し迫ったシステム シャットダウンの通知など）を送信する場合に便利です。

ログイン バナーも接続されたすべての端末に表示されます。表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

（注） ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*』を参照してください。

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

MAC Address Table

MAC アドレス テーブルには、デバイスがポート間のトラフィック転送に使用するアドレス情報が含まれています。このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応しています。アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

- ダイナミック アドレス：デバイスが取得し、使用されなくなった時点で期限切れとなる送信元の MAC アドレス
- スタティック アドレス：手動で入力され、期限切れにならず、デバイスのリセット時にも消去されないユニキャスト アドレス

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN（仮想 LAN）ID、アドレスに対応付けられたポート番号、およびタイプ（スタティックまたはダイナミック）のリストです。

（注） ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

MAC アドレス テーブルの作成

すべてのポートでサポートされる複数の MAC アドレスを使用して、他のネットワーク デバイスにデバイス上のすべてのポートを接続できます。デバイスは、各ポートで受信するパケットの送信元アドレスを取得し、アドレステーブルにアドレスとそれに関連付けられたポート番号を追加することによって、動的なアドレス指定を行います。ネットワークでデバイスの追加または削除が行われると、デバイスによってアドレステーブルが更新され、新しいダイナミック アドレスが追加され、使用されていないアドレスは期限切れになります。

エージング インターバルは、グローバルに設定されています。ただし、デバイスは VLAN ごとにアドレス テーブルを維持し、STP によって VLAN 単位で有効期間を短縮できます。

デバイスは、受信したパケットの宛先アドレスに基づいて、任意の組み合わせのポート間でパケットを送信します。デバイスは、MAC アドレス テーブルを使用することによって、宛先アドレスに関連付けられたポートに限定してパケットを転送します。宛先アドレスがパケットを送信したポート上にある場合は、パケットはフィルタリング処理され、転送されません。デバイスは、常にストア アンド フォワード方式を使用します。このため、完全なパケットをいったん保存してエラーがないか検査してから転送します。

MAC アドレスおよび VLAN

すべてのアドレスは VLAN と関連付けされます。1 つのアドレスを複数の VLAN に対応付け、それぞれで異なる宛先を設定できます。たとえば、ユニキャスト アドレスを VLAN 1 のポート 1 および VLAN 5 のポート 9、10、1 に転送するといったことが可能です。

VLAN ごとに、独自の論理アドレス テーブルが維持されます。ある VLAN で認識されているアドレスが別の VLAN で認識されるには、別の VLAN 内のポートによって学習されるか、または別の VLAN 内のポートにスタティックに対応付けられる必要があります。

MAC アドレスおよびデバイスのスタック

すべてのスタック メンバにある MAC アドレス テーブルでは、同期が取られます。いかなる時点でも、各スタック メンバには、各 VLAN のアドレス テーブルの同じコピーがあります。アドレスがエージング アウトすると、アドレスは、すべてのスタック メンバにあるアドレス

テーブルから削除されます。デバイスがスイッチ スタックに参加すると、そのデバイスでは、他のスタック メンバでラーニングされた各 VLAN のアドレスを受信します。スタック メンバがスイッチ スタックに残っているときには、残りのスタック メンバは、エージング アウトするか、前のスタック メンバによってラーニングされたすべてのアドレスが削除されます。

MAC アドレス テーブルのデフォルト設定

次の表に、MAC アドレス テーブルのデフォルト設定を示します。

表 *177 : MAC* アドレスのデフォルト設定

機能	デフォルト設定
エージング タイム	300 秒
ダイナミック アドレス	自動学習
スタティック アドレス	未設定

ARP テーブルの管理

デバイスと通信するには（イーサネット上のデバイスなど）、ソフトウェアは最初にそのデバイスの 48 ビット MAC アドレスまたはローカル データ リンク アドレスを学習する必要があります。IP アドレスからローカル データ リンク アドレスを学習するプロセスを、アドレス解決といいます。

アドレス解決プロトコル（ARP）は、ホスト IP アドレスを、該当するメディアまたは MAC アドレスおよび VLAN ID に対応付けます。IP アドレスを使用して、ARP は対応する MAC アドレスを見つけます。MAC アドレスが見つかると、IP と MAC アドレスとの対応を ARP キャッシュに格納し、すばやく検索できるようにします。その後、IP データグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化および ARP 要求/応答については、サブネットワーク アクセス プロトコル（SNAP）で規定されています。IP インターフェイスでは、標準的なイーサネット形式の ARP カプセル化（**arpa** キーワードで表される）がデフォルトでイネーブルに設定されています。

手動でテーブルに追加された ARP エントリは期限切れにならないので、手動で削除する必要があります。

CLI（コマンドライン インターフェイス）の手順については、*Cisco.com* で Cisco IOS Release 12.4 のマニュアルを参照してください。

デバイスを管理する方法

手動による日付と時刻の設定

正確なシステム時刻は再開と再起動により保持されますが、日付と時刻はシステムが再開してから手動で設定できます。

手動設定は必要な場合にのみ使用することを推奨します。デバイスが同期できる外部ソースがある場合は、システム クロックを手動で設定する必要はありません。

（注） アクティブ スイッチに障害が発生し、別のスタック メンバがアクティブ スイッチの役割を引き継ぐ前に手動でシステムクロックを設定している場合は、この設定を再設定する必要があります。

システム クロックの設定

ネットワーク上に、NTP サーバなどの時刻サービスを提供する外部ソースがある場合、手動でシステム クロックを設定する必要はありません。

システム クロックを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかを使用します。 • **clock set** *hh:mm:ss day month year* • **clock set** *hh:mm:ss month day year* 例： `Device# clock set 13:32:00 23 March 2013`	次のいずれかの書式を使ってシステム クロックを手動で設定します。 • *hh:mm:ss*：時間（24 時間形式）、分、秒を指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • *day*：月の日で日付を指定します。 • *month*：月を名前で指定します。 • *year*：年を指定します（略式表記で指定しないでください）。

タイム ゾーンの設定

タイム ゾーンを手動で設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**clock timezone** *zone hours-offset* [*minutes-offset*] 例： `Device(config)# clock timezone AST -3 30`	時間帯を設定します。 内部時間は、協定世界時（UTC）で維持されるため、このコマンドは表示専用で、時刻を手動で設定するときだけに使用されます。 • *zone*：標準時が適用されているときに表示されるタイム ゾーンの名前を入力します。デフォルトは UTC です。 • *hours-offset*：UTC からのオフセット時間数を入力します。 • （任意）*minutes-offset*：UTC からのオフセット分数を入力します。ローカル タイム ゾーンが UTC と 1 時間の差の割合である場合に指定できます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

夏時間の設定

毎年特定の日に夏時間が開始および終了する地域に夏時間を設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**clock summer-time** *zone date month year hh:mm date month year hh:mm* [*offset*]]**date** 例： `Device(config)# clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00`	毎年指定された日に開始および終了する夏時間を設定します。
ステップ 4	**clock summer-time** *zone***recurring** [*week day month hh:mm week day month hh:mm* [*offset*]] 例： `Device(config)# clock summer-time`	毎年指定された日に開始および終了する夏時間を設定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。

	コマンドまたはアクション	目的
	PDT recurring 10 March 2013 2:00 3 November 2013 2:00	終了時間は夏時間を基準にしています。夏時間はデフォルトでディセーブルに設定されています。パラメータなしで **clock summer-time** *zone***recurring** を指定すると、夏時間のルールはデフォルトにより米国のルールになります。 開始月が終了月より後の場合は、システムでは南半球にいると見なされます。 • *zone*：夏時間が有効な場合に表示される時間帯名（PDT など）を指定します。 •（任意）*week*：月の週（1 ～ 4、**first**、または **last**）を指定します。 •（任意）*day*：曜日（Sunday、Monday など）を指定します。 •（任意）*month*：月（January、February など）を指定します。 •（任意）*hh:mm*：時および分単位で時間（24時間形式）を指定します。 •（任意）*offset*：夏時間中に追加する分数を指定します。デフォルトは 60 です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ユーザの居住地域の夏時間が定期的なパターンに従わない（次の夏時間のイベントの正確な日時を設定する）場合は、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**clock summer-time** *zone* **date**[*month date year hh:mm month date year hh:mm* [*offset*]]or**clock summer-time** *zone* **date** [*date month year hh:mm date month year hh:mm* [*offset*]]	最初の日付で夏時間開始の日付を、2番めの日付で終了の日付を設定します。 夏時間はデフォルトでディセーブルに設定されています。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前（たとえば PDT）を入力します。 • （任意）*week* には、月の何週目かを指定します（1 ～ 5、または last）。 • （任意）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh:mm* には、時刻を時間（24時間形式）と分で指定します。 • （任意）*offset* には、夏時間の間、追加する分数を指定します。デフォルトは 60 です。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

システム名の設定

システム名を手動で設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname** *name* 例： `Device(config)# hostname remote-users`	システム名を設定します。システム名を設定すると、システム プロンプトとしても使用されます。 デフォルト設定はDeviceです。 名前は ARPANET ホスト名のルールに従う必要があります。このルールではホスト名は文字で始まり、文字または数字で終わり、その間には文字、数字、また

	コマンドまたはアクション	目的
		はハイフンしか使用できません。名前には 63 文字まで使用できます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

DNS の設定

デバイスの IP アドレスをホスト名として使用する場合、この IP アドレスが使用されるため、DNS クエリは発生しません。ピリオド（.）なしでホスト名を設定すると、ピリオドと、それに続くデフォルトのドメイン名がホスト名に追加され、その後で DNS クエリーが行われ、名前を IP アドレスにマッピングします。デフォルトのドメイン名は、グローバル コンフィギュレーション コマンド **ip domain-name** で設定される値です。ホスト名にピリオド（.）がある場合は、Cisco IOS ソフトウェアは、ホスト名にデフォルトのドメイン名を追加せずに IP アドレスを検索します。

DNS を使用するようにスイッチを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**ip domain-name** *name* 例： `Device(config)# ip domain-name Cisco.com`	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 ブート時にはドメイン名は設定されていませんが、デバイスの設定が BOOTP または Dynamic Host Configuration Protocol（DHCP）サーバから行われている場合、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（この情報がサーバに設定されている場合）。
ステップ 4	**ip name-server** *server-address1* [*server-address2 ... server-address6*] 例： `Device(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300`	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバ アドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。デバイスは、最初にプライマリ サーバへ DNS クエリを送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 5	**ip domain-lookup** [**nsap** | **source-interface** *interface*] 例： `Device(config)# ip domain-lookup`	（任意） デバイス上で、DNS に基づくホスト名からアドレスへの変換をイネーブルにします。この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Message-of-the-Day ログイン バナーの設定

デバイスにログインしたときに画面に表示される 1 行以上のメッセージ バナーを作成できます。

MOTD ログイン バナーを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**banner motd** *c message c*
	例：
	`Device(config)# banner motd #`
	`This is a secure site. Only`
		MoTD を指定します。
		c：ポンド記号（#）など、目的のデリミタを入力して **Return** キーを押します。区切り文字はバナー テキストの始まり

	コマンドまたはアクション	目的

	`authorized users are allowed.`
	`For access, contact technical support.`
	`#`
		と終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。
		message：255 文字までのバナー メッセージを入力します。メッセージ内には区切り文字を使用できません。

ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ログイン バナーの設定

接続されたすべての端末でログインバナーが表示されるように設定できます。バナーが表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

ログイン バナーを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	

ステップ 3	**banner login** *c message c*
	例：
	`Device(config)# banner login $`
	`Access for authorized users only.`
	`Please enter your username and password.`
	`$`
		ログイン メッセージを指定します。
		c：ポンド記号（#）など、目的のデリミタを入力して Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。
		message：255 文字までのログイン メッセージを入力します。メッセージ内には区切り文字を使用できません。

ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MAC アドレス テーブルの管理

アドレス エージング タイムの変更

ダイナミック アドレス テーブルのエージング タイムを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mac address-table aging-time** [*0* | *10-1000000*] [**routed-mac** | **vlan** *vlan-id*] 例： `Device(config)# mac address-table aging-time 500 vlan 2`	ダイナミック エントリが使用または更新された後、MAC アドレス テーブル内に保持される時間を設定します。 指定できる範囲は 10 ～ 1000000 秒です。デフォルトは 300 です。0 を入力して期限切れをディセーブルにすることもできます。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。 *vlan-id*：有効な ID は 1 ～ 4094 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MAC アドレス変更通知トラップの設定

NMS ホストに MAC アドレス変更通知トラップを送信するようにスイッチを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server host** *host-addr community-string notification-type* { **informs** | **traps** } {**version** {**1** | **2c** | **3**}} {**vrf** *vrf instance name*} 例： `Device(config)# snmp-server host 172.20.10.10 traps private mac-notification`	トラップ メッセージの受信側を指定します。 • *host-addr*：NMS の名前またはアドレスを指定します。 • **traps**（デフォルト）：ホストに SNMP トラップを送信します。 • **informs**：ホストに SNMP インフォームを送信します。 • **version**：サポートする SNMP バージョンを指定します。informs にはバージョン 1（デフォルト）を使用できません。 • *community-string*：通知処理で送信する文字列を指定します。**snmp-server host** コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type*：**mac-notification** キーワードを使用します。 • **vrf** *vrf instance name*：このホストの VPN ルーティング/転送インスタンスを指定します。

	コマンドまたはアクション	目的
ステップ 4	**snmp-server enable traps mac-notification change** 例： `Device(config)# snmp-server enable traps mac-notification change`	デバイスが MAC アドレス変更通知トラップを送信できるようにします。
ステップ 5	**mac address-table notification change** 例： `Device(config)# mac address-table notification change`	MACアドレス変更通知機能をイネーブルにします。

ステップ 6	**mac address-table notification change** [**interval** *value*] [**history-size** *value*]
	例：
	`Device(config)# mac address-table notification change interval 123`
	`Device(config)#mac address-table notification change history-size 100`
		トラップ インターバル タイムと履歴テーブルのサイズを入力します。
		• （任意）**interval** *value*：NMS に生成されるトラップの各セット間の通知トラップ インターバルを秒単位で指定します。指定できる範囲は 0 ～ 2147483647 秒です。デフォルトは 1 秒です。
		• （任意）**history-size** *value*：MAC 通知履歴テーブルの最大エントリ数を指定します。指定できる範囲は 0 ～ 500 です。デフォルトは 1 です。

ステップ 7	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。
ステップ 8	**snmp trap mac-notification change** {**added** | **removed**} 例： `Device(config-if)# snmp trap mac-notification change added`	インターフェイス上で MAC アドレス変更通知トラップをイネーブルにします。 • MACアドレスがインターフェイスに追加された（**added**）場合にトラップをイネーブルにします。 • MACアドレスがインターフェイスから削除された（**removed**）場合

	コマンドまたはアクション	目的
		に MAC 通知トラップをイネーブルにします。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

MAC アドレス移動通知トラップの設定

MAC移動通知を設定する場合は、MACアドレスが、同じVLAN内のあるポートから別のポートに移動すると常に、SNMP 通知が生成されてネットワーク管理システムに送信されます。

NMSホストにMACアドレス移動通知トラップを送信するようにデバイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type* 例： `Device(config)# snmp-server host 172.20.10.10 traps private mac-notification`	トラップ メッセージの受信側を指定します。 • *host-addr*：NMS の名前またはアドレスを指定します。 • **traps**（デフォルト）：ホストに SNMP トラップを送信します。 • **informs**：ホストに SNMP インフォームを送信します。 • **version**：サポートする SNMP バージョンを指定します。informs にはバージョン 1（デフォルト）を使用できません。 • *community-string*：通知処理で送信する文字列を指定します。**snmp-server host** コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type*：**mac-notification** キーワードを使用します。
ステップ 4	**snmp-server enable traps mac-notification move** 例： `Device(config)# snmp-server enable traps mac-notification move`	デバイスが NMS に MAC アドレス移動通知トラップを送信できるようにします。
ステップ 5	**mac address-table notification mac-move** 例： `Device(config)# mac address-table notification mac-move`	MAC アドレス移動通知機能をイネーブルにします。
ステップ 6	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

スイッチによる MAC アドレス移動通知トラップの送信をディセーブルにするには、**no snmp-server enable traps mac-notification move** グローバル コンフィギュレーション コマンドを使用します。MAC アドレス変更通知機能をディセーブルにするには、**no mac address-table notification mac-move** グローバル コンフィギュレーション コマンドを使用します。

設定を確認するには、**show mac address-table notification mac-move** 特権 EXEC コマンドを入力します。

MAC しきい値通知トラップの設定

MAC しきい値通知を設定する場合は、MAC アドレス テーブルのしきい値の制限値に達するか、その値を超えると、SNMP 通知が生成されてネットワーク管理システムに送信されます。

NMS ホストに MAC アドレス テーブルしきい値通知トラップを送信するようにスイッチを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**snmp-server host** *host-addr* {**traps** |**informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type* 例： `Device(config)# snmp-server host 172.20.10.10 traps private mac-notification`	トラップ メッセージの受信側を指定します。 • *host-addr*：NMS の名前またはアドレスを指定します。 • **traps**（デフォルト）：ホストに SNMP トラップを送信します。 • **informs**：ホストに SNMP インフォームを送信します。 • **version**：サポートする SNMP バージョンを指定します。informs にはバージョン 1（デフォルト）を使用できません。 • *community-string*：通知処理で送信する文字列を指定します。**snmp-server host** コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type*：**mac-notification** キーワードを使用します。
ステップ 4	**snmp-server enable traps mac-notification threshold** 例： `Device(config)# snmp-server enable traps mac-notification threshold`	NMS への MAC しきい値通知トラップをイネーブルにします。
ステップ 5	**mac address-table notification threshold** 例： `Device(config)# mac address-table notification threshold`	MAC アドレスしきい値通知機能をイネーブルにします。

	コマンドまたはアクション	目的

ステップ 6	**mac address-table notification threshold** [**limit** *percentage*] | [**interval** *time*]
	例：
	`Device(config)# mac address-table notification threshold interval 123`
	`Device(config)# mac address-table notification threshold limit 78`
		MAC アドレスしきい値使用状況モニタリングのしきい値を入力します。
		• （任意）**limit** *percentage*：MAC アドレス テーブルの使用率を指定します。有効値は 1 ～ 100 % です。デフォルト値は 50% です。
		• （任意）**interval** *time*：通知の間隔を指定します。有効値は120秒以上です。デフォルトは 120 秒です。

ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スタティック アドレス エントリの追加および削除

スタティック アドレスを追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* 例： `Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1`	MAC アドレス テーブルにスタティック アドレスを追加します。 • *mac-addr*：アドレス テーブルに追加する宛先 MAC ユニキャスト アドレスを指定します。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。 • *vlan-id*：指定された MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4094 です。 • *interface-id*：受信パケットが転送されるインターフェイスを指定します。有効なインターフェイスは、物理ポートまたはポート チャネルです。スタティック マルチキャスト アドレスの場合、複数のインターフェイス ID を入力できます。スタティック ユニキャスト アドレスの場合、インターフェイスは同時に 1 つしか入力できません。ただし、同じ MAC アドレスおよび VLAN ID を指定すると、コマンドを複数回入力できます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例：	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

ユニキャスト MAC アドレス フィルタリングの設定

デバイスが送信元または宛先ユニキャスト スタティック アドレスをドロップするよう設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mac address-table static** *mac-addr***vlan** *vlan-id***drop** 例： `Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop`	ユニキャストMACアドレスフィルタリングをイネーブルにし、デバイスが指定した送信元または宛先ユニキャスト スタティック アドレスを持つパケットをドロップするように設定します。 • *mac-addr*：送信元または宛先ユニキャスト MAC アドレス（48 ビット）を指定します。このMACアドレスを持つパケットはドロップされます。 • *vlan-id*：指定された MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4094 です。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

デバイスのモニタリングおよび保守の管理

コマンド	目的
clear mac address-table dynamic	すべてのダイナミックエントリを削除します。
clear mac address-table dynamic address *mac-address*	特定の MAC アドレスを削除します。
clear mac address-table dynamic interface *interface-id*	指定された物理ポートまたはポート チャネル上のすべてのアドレスを削除します。
clear mac address-table dynamic vlan *vlan-id*	指定された VLAN 上のすべてのアドレスを削除します。
show clock [*detail*]	時刻と日付の設定を表示します。
show ip igmp snooping groups	すべての VLAN または指定された VLAN に対するレイヤ 2 マルチキャスト エントリを表示します。
show mac address-table address *mac-address*	指定された MAC アドレスの MAC アドレステーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。

コマンド	目的
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface *interface-name*	指定されたインターフェイスのMACアドレステーブル情報を表示します。
show mac address-table move update	MACアドレステーブル移動更新情報を表示します。
show mac address-table multicast	マルチキャストのMACアドレスのリストを表示します。
show mac address-table notification {change | mac-move | threshold}	MAC通知パラメータおよび履歴テーブルを表示します。
show mac address-table secure	セキュア MAC アドレスを表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan *vlan-id*	指定された VLAN の MAC アドレス テーブル情報を表示します。

デバイス管理の設定例

例：システム クロックの設定

次の例は、システム クロックを手動で設定する方法を示しています。

```
Device# clock set 13:32:00 23 July 2013
```

例：サマー タイムの設定

次に、サマータイムが 3 月 10 日の 02:00 に開始し、11 月 3 日の 02:00 に終了する場合の設定を例として示します。

```
Device(config)# clock summer-time PDT recurring PST date
10 March 2013 2:00 3 November 2013 2:00
```

次に、サマータイムの開始日と終了日を設定する例を示します。

```
Device(config)#clock summer-time PST date
20 March 2013 2:00 20 November 2013 2:00
```

例：MOTD バナーの設定

次の例は、開始および終了デリミタにポンド記号（#）を使用して、MOTD バナーを設定する方法を示しています。

```
Device(config)# banner motd #

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

#

Device(config)#
```

次に、前の設定により表示されたバナーの例を示します。

```
Unix> telnet 192.0.2.15

Trying 192.0.2.15...

Connected to 192.0.2.15.

Escape character is '^]'.

This is a secure site. Only authorized users are allowed.

For access, contact technical support.

User Access Verification

Password:
```

例：ログイン バナーの設定

次の例は、開始および終了デリミタにドル記号（$）を使用して、にログイン バナーを設定する方法を示しています。

```
Device(config)# banner login $

Access for authorized users only. Please enter your username and password.

$

Device(config)#
```

例：MAC アドレス変更通知トラップの設定

次に、NMS として 172.20.10.10 を指定し、NMS への MAC アドレス通知トラップの送信をイネーブルにし、MAC アドレス変更通知機能をイネーブルにし、インターバル タイムを 123 秒

に設定し、履歴サイズを 100 エントリに設定し、特定のポートで MAC アドレスが追加された場合のトラップをイネーブルにする例を示します。

```
Device(config)# snmp-server host 172.20.10.10 traps private mac-notification
Device(config)# snmp-server enable traps mac-notification change
Device(config)# mac address-table notification change
Device(config)# mac address-table notification change interval 123
Device(config)# mac address-table notification change history-size 100
Device(config)# interface gigabitethernet1/2/1
Device(config-if)# snmp trap mac-notification change added
```

例：MAC しきい値通知トラップの設定

次に、NMS として 172.20.10.10 を指定し、MAC アドレスしきい値通知機能をイネーブルにし、インターバル タイムを 123 秒に設定し、制限を 78% に設定する例を示します。

```
Device(config)# snmp-server host 172.20.10.10 traps private mac-notification
Device(config)# snmp-server enable traps mac-notification threshold
Device(config)# mac address-table notification threshold
Device(config)# mac address-table notification threshold interval 123
Device(config)# mac address-table notification threshold limit 78
```

例：MAC アドレス テーブルへのスタティック アドレスの追加

次の例では、MAC アドレス テーブルにスタティック アドレス c2f3.220a.12f4 を追加する方法を示します。VLAN 4 でこの MAC アドレスを宛先アドレスとして持つパケットを受信すると、パケットは指定されたポートに転送されます。

```
Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet1/1/1
```

例：ユニキャスト MAC アドレス フィルタリングの設定

次に、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つドロップパケットを設定する例を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

```
Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

デバイス管理に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference (Catalyst 3850 Switches)*』
ネットワーク管理の設定	『*Network Management Configuration Guide (Catalyst 3850 Switches)*』
レイヤ 2 の設定	『*Layer 2/3 Configuration Guide (Catalyst 3850 Switches)*』
VLAN コンフィギュレーション	『*VLAN Configuration Guide (Catalyst 3850 Switches)*』
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*）
プラットフォームに依存しない設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*） *IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*）

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

デバイス管理に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference (Catalyst 3650 Switches)*
ネットワーク管理の設定	*Network Management Configuration Guide (Catalyst 3650 Switches)*
レイヤ 2 の設定	*Layer 2/3 Configuration Guide (Catalyst 3650 Switches)*
VLAN コンフィギュレーション	*VLAN Configuration Guide (Catalyst 3650 Switches)*

関連項目	マニュアル タイトル
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S（Catalyst 3650 Switches）*
プラットフォームに依存しない設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S（Catalyst 3650 Switches）* *IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S（Catalyst 3650 Switches）*

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

デバイス管理の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 125 章

ブート整合性の可視性

- 機能情報の確認 （2775 ページ）
- ブート整合性の可視性について （2775 ページ）
- ソフトウェア イメージとハードウェアの確認 （2776 ページ）
- プラットフォーム ID とソフトウェア整合性の確認 （2776 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ブート整合性の可視性について

ブート整合性の可視性によって、シスコのプラットフォーム ID とソフトウェアの整合性情報が可視化され、実用可能になります。プラットフォーム ID は、プラットフォームの製造元でインストールされた ID を示しています。ソフトウェアの整合性ではブート整合性の測定値が明らかになり、それを使用してプラットフォームが信頼できるコードを起動しているかどうかを評価できます。

ブート プロセス中に、ソフトウェアはブート ローダ アクティビティの各ステージのチェックサム レコードを作成します。

このレコードを取得して、シスコ認定レコードと比較し、ソフトウェアイメージが正規かどうかを確認できます。チェックサム値が一致していない場合は、シスコによって認定されていない、または未承認パーティによって改ざんされているソフトウェアイメージを実行している可能性があります。

ソフトウェア イメージとハードウェアの確認

このタスクでは、スイッチの起動時に作成されたチェックサム レコードを取得する方法について説明します。特権 EXEC モードで次のコマンドを入力します。

（注） 次のコマンドを実行した後で、メッセージ **% Please Try After Few Seconds** が CLI に表示されることがあります。これはCLIの障害を示すものではありませんが、必要な出力を取得するために必要な基盤となるインフラストラクチャの設定を示します。数分間待機して、コマンドを再度試すことをお勧めします。

メッセージ **% Error retrieving SUDI certificate** および **% Error retrieving integrity data** は、実際の CLI 障害を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show platform sudi certificate** ［**sign** ［**nonce** *nonce*］］ 例： `Device# show platform sudi certificate sign nonce 123`	特定の SUDI のチェックサム レコードを表示します。 • （オプション）**sign**：署名を示します • （オプション）**nonce**：ナンス値を入力します
ステップ 2	**show platform integrity** ［**sign** ［**nonce** *nonce*］］ 例： `Device# show platform integrity sign nonce 123`	ブート段階のチェックサム レコードを表示します。 • （オプション）**sign**：署名を示します • （オプション）**nonce**：ナンス値を入力します

プラットフォーム ID とソフトウェア整合性の確認

プラットフォーム ID の確認

次に、PEM形式でセキュアな固有デバイス識別子（SUDI）チェーンを表示する例を示します。最初の証明書はCisco Root CA 2048 で、2 番目はシスコの下位 CA（ACT2 SUDI

CA）です。どちらの証明書も、https://www.cisco.com/security/pki/ で公開されているものと一致しているかを確認できます。3 番目は SUDI 証明書です。

```
Device#show platform sudi certificate sign nonce 123

-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIEAJT3DDANBgkqhkiG9w0BAQsFADAnMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMB4XDTE1MTExNDA5MzMzN1oXDTI1
MTExNDA5MzMzN1owczEsMCoGA1UEBRMjUElEOldTLUMzNjUwLTEyWDQ4VVEgU046
RkRPMTk0NkJHMDUxDjAMBgNVBAoTBUNpc2NvMRgwFgYDVQQLEw9BQ1QtMiBMaXRl
IFNVREkxGTAXBgNVBAMTEFdTLUMzNjUwLTEyWDQ4VVEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC6SARWyImWrRV/x7XQogAE+02WmzKki+4arMVBvl9o
GgvJfkoJDdaHOROSUkEE3qXtd8N3lfKy3TZ+jtHD85m2aGz6+IRx/e/lLsQzi6dl
WIB+N94pgecFBONPR9wJriox1IGD3B43b0hMLkmro4R5Zrs8XFkDo9k1tBU7F2O7
GEzb/WkO5NLexznef2Niglx9fCDL0HC27BbsR5+03p8jhG0+mvrp8M9du1HKiGin
ZIV4XgTMp1/k/TVaIepEGZuWM3hxdUZjkNGG1c1m+oB8vLX3UlSL76sDBBoiaprD
rjXBgBIozyFW8tTjh50jMDG84hKD5s31ifOe4KpqEcnVAgMBAAGjbzBtMA4GA1Ud
DwEB/wQEAwIF4DAMBgNVHRMBAf8EAjAAME0GA1UdEQRGMESgQgYJKwYBBAEJFQID
```

```
oDUTM0NoaXBJRD1VWUpOTlZJMENBUkhVM1Z1SUVSbFl5QXlPQ0F4TXpvek5Ub3lN
U0EwS0NnPTANBgkqhkiG9w0BAQsFAAOCAQEADjtM8vdlf+p1WKSKX1C1qQ4aEnD5
p8T5e4iTer7Y1fbCrHIEEm3mnip+568j299z0H8V7PDp1ljuLHyMFTC+945F9RfA
eAuVWVb5A9dnGL8MssBJe2lVSnZwrWkT1EIdxLYrTiPAQHtll6CN77S4u/f71oYE
tzPE5AGfyGw7ro1MEPVGffaQmYUDAwKFNBH1uI7c2S1qlwk4WWZ6xxci+lhaQnIG
pWzapaiAYL1XrcBz4KwFc1ZZpQT6hHw24jzYaYimvCo+/kSKuA9xNdtSu18ycox0
zKnXQ17s6aChMMt7Y8Nh4iz9BDejoOF6/b3sM0wRi+2/4j+6/GhcMRs0Og==
-----END CERTIFICATE-----

Signature version: 1
Signature:
405C770D802B73947EDBF8DD0D2C8180F10D4B3EF9699444514219C579D2ED52F7D5
83E0F4408133FC4E9F549B2EB1C21725F7CB1C79F98271E47E780E703E674723880F
B52D4963E1D1FB9787B38E28B8E696570A180B7A2F1311B1F174EAA79F55DB4765DF
67386126D899E07EDF6C26E0A81272EAA114437DD03F26992937082756AE1F1BFAFB
BFACD6BE9CF9C84C961FACE9FA0FEE64D85AE4FA0086969D0702C536ABDB8FBFDC47
C14C17D02FEBF4F7F5BB24D2932FA876F56B4C07816270AA0B4195C53D975C85AEAE
3A74F2DBF293F52423ECB7B8539667080A9C57DA3E4B08B2B2CA623B2CBAF7080A0A
EB09B222E5B756970A3AA27E0F1D17C8A243
```

オプションの RSA 2048 署名は、3 つの証明書、署名のバージョンおよびユーザにより提供されるナンスに対するものです

```
RSA PKCS#1v1.5 Sign {<Nonce (UINT64)> || <Signature Version (UINT32)> || <Cisco Root CA
 2048 cert (DER)> ||
<Cisco subordinate CA (DER)> || <SUDI certificate (DER)> }
```

シスコの管理ソリューションには、上記の出力を解釈する機能が装備されています。しかし、OpenSSL コマンドを使用した簡単なスクリプトを使用してプラットフォームの ID を表示して署名を確認することもでき、それによってシスコの一意のデバイス ID を確保できます。

```
[linux-host:~]openssl x509 -in sudicert.pem -subject -noout
subject= /serialNumber=PID:WS-C3650-12X48UQ SN:FDO1946BG05/O=Cisco/OU=ACT-2 Lite
SUDI/CN=WS-C3650-12X48UQ
```

ソフトウェア整合性の確認

次に、ブート段階のチェックサム レコードを表示する例を示します。ハッシュ測定値は、連続してブートされたソフトウェアの 3 つの段階それぞれについて表示されます。これらのハッシュをシスコが提供する基準値と比較できます。出力に署名するオプションを使用すると、出力は正規であり改ざんされていないことを保証する機能が検証ツールに付与されます。リプレイ攻撃から保護するために、ナンスを提供できます。

```
Device #show platform integrity sign nonce 456

Platform: WS-C3650-12X48UQ
Boot Loader Version: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.16, engineering
 software (D)
Boot Loader Hash: DB5A686E9F4CE358481DE3AF8B9C762F0A604E3B4764DF2A351F176E3D7
D3C60EB85C02906BD8CF28228C0DFC2AA8960CAFE6675D696E4ABA0CD687C0609E7E2
Boot 0 Version: F01062R15.0508d68fa2015-09-15
Boot 0 Hash: 6EF15CD54D3C66A8B644194A67B7ED57044C8C2E0EECB69736A7FFEC1F6D0EAD
OS Version: 2016-10-18_10.57_mundru
OS Hash: 4C85AECC88DAA49D940BBF65B1F17269F55C8D98DEFB4140F981923AA961140293E1
3B3E6E68CE3F8ED7F596CD858ACDD4BEF6538F59C1E243C351353026E6CD
PCR0: 90214167AAF35C06B2AC97292596E5669EAB72578FCDAD0B91746683BAA7B2B0
PCR8: FC2CE1BAC397F97008936DF372A2218BB16A798222B8FF55A7B6AEDA8018EDF5
Signature version: 1
```

```
Signature:
632A724F1AB6ADE134F6B0E8724D2052B3157F45B47E547763EE224A848E807CD737600587FF68
2526A8FE354A116CC9EDEBD9C659B9927336542EE4295084368327D01BD22AB4849BB3C007B6EB
B67708685FD6BC85DD045431E19A389FEB358894D4FBCF7C0FC960AC9133B61099DFD507F316C1
BF82F7F98687C7E7E8F99355DC1A95BD511B0B8DCB0CA909828F9EFBDF18847930392A8E3D072D
F3D90536880BAE9B7D7CF0E301D3F5AF16E7517FC2700E2F75911B836D6559A18E15B4CF452555
91656DF22DFF73392F777AEB796BCF9AC046C581ADEF19CA48A98F620BB58A79B32DA8B3BFB1CF
8399468A096E2F0C54B8B3ECD15EE3FE2C5ABDB5A029
```

オプションの RSA 2048 署名は SUDI 秘密キーで生成され、SUDI 証明書に含まれている SUDI 公開キーで確認できます。PCR 値全体の署名、署名のバージョンおよびユーザにより提供されるナンスが表示されます。

```
RSA PKCS# 1 v1.5 Sign { <Nonce (UINT64)> || <Signature Version (UINT32)> || <PCR0 (32
bytes)> || <PCR8 (32 bytes)> }
```

シスコの管理ソリューションには、上記の出力を解釈する機能が装備されており、結果を公開されているシスコの値と比較し、署名を確認します。

第 126 章

デバイスのセットアップ設定の実行

- 機能情報の確認 （2781 ページ）
- デバイスセットアップ設定の実行に関する情報 （2781 ページ）
- デバイスセットアップ設定の実行方法 （2797 ページ）
- デバイスのセットアップ設定のモニタリング （2813 ページ）
- デバイス のセットアップを実行する場合の設定例 （2817 ページ）
- デバイスのセットアップの実行に関する追加情報 （2819 ページ）
- WCM サブパッケージのインストール （2820 ページ）
- デバイスセットアップ設定の機能履歴と情報 （2822 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

デバイスセットアップ設定の実行に関する情報

IP アドレスの割り当ておよびDHCP 自動設定を含む初期デバイス設定タスクを実行する前に、このモジュールのセクションを確認します。

デバイスブート プロセス

デバイスを起動するには、ハードウェア インストレーション ガイドの手順にしたがって、デバイスを設置して電源をオンにし、デバイスの初期設定（IP アドレス、サブネット マスク、デフォルト ゲートウェイ、シークレット、Telnet パスワードなど）を行う必要があります。

通常の起動プロセスにはブートローダ ソフトウェアの動作が含まれ、以下のアクティビティが実行されます。

- 下位レベルの CPU 初期化を行います。CPU レジスタを初期化することにより、物理メモリがマッピングされる場所、容量、速度などを制御します。
- CPU サブシステムの電源投入時セルフ テスト（POST）を実行し、システム DRAM をテストします。
- システム ボード上のファイル システムを初期化します。
- デフォルトのオペレーティング システム ソフトウェア イメージをメモリにロードし、デバイスを起動します。

ブート ローダにより、オペレーティング システムがロードされる前に、ファイル システムにアクセスすることができます。ブート ローダの使用目的は通常、オペレーティング システムのロード、展開、および起動に限定されます。オペレーティング システムが CPU を制御できるようになると、ブートローダは、次にシステムがリセットされるか電源が投入されるまでは非アクティブになります。

また、オペレーティング システムが使用不可能になるほどの重大な障害が発生した場合は、ブートローダはシステムにトラップドアからアクセスします。トラップドア メカニズムによりシステムへのアクセスを十分に行うことで、必要に応じて、XMODEM プロトコルを使用してオペレーティングシステムのソフトウェアイメージを再インストールし、失われたパスワードを回復し、最終的にオペレーティング システムを再起動できます。

デバイス情報を割り当てるには、PC または端末をコンソール ポートに接続するか、PC をイーサネット管理ポートに接続して、PC または端末エミュレーション ソフトウェアのボーレートおよびキャラクタ フォーマットをデバイスのコンソール ポートの設定と一致させておく必要があります。

- デフォルトのボーレートは 9600 です。
- デフォルトのデータ ビットは 8 です。

（注） データ ビット オプションを 8 に設定した場合、パリティ オプションは「なし」に設定します。

- デフォルトのストップ ビットは 2（マイナー）です。
- デフォルトのパリティ設定は「なし」です。

ソフトウェア インストーラ機能

次のスイッチでソフトウェア インストーラ機能がサポートされます。

- スタンドアロン スイッチ、スイッチ スタック、またはスタック内のスイッチのサブセットでのソフトウェア バンドルのインストール。デフォルトでは、スイッチ スタックが設定されている場合、すべてのスイッチでインストールが行われます。
- スイッチのスタックでは、すべてのスイッチをインストールモードすることが推奨されます。
- 以前にインストールしたパッケージ セットへのソフトウェア ロールバック。
- 有効なインストール済みパッケージがブート フラッシュに存在しない場合の緊急インストール。
- 互換性のないソフトウェアを持つスイッチ スタックに参加しているスイッチの自動アップグレード。
- スイッチ スタック内の別のスイッチにパッケージをインストールするための供給元として 1 台のスイッチのパッケージを使用してのインストール。

（注） ソフトウェア インストールおよびロールバックは、インストール モードのみで実行しているときに行う必要があります。**software expand** EXEC コマンドを使用すると、ブートのバンドル モードをインストール モードに変換できます。

ソフトウェアのブート モード

デバイスでは、ソフトウェア パッケージを起動するための次の 2 種類のモードがサポートされています。

- インストール モード
- バンドル モード

関連トピック

例 : インストール モードでのソフトウェアブートアップ ディスプレイ （2814 ページ）
例 : 緊急インストール （2816 ページ）

インストール モードでのブート

以下のフラッシュ内のソフトウェア パッケージのプロビジョニング ファイルを起動して、インストール モードでデバイスを起動できます:

デバイス: **boot flash:packages.conf**

プロビジョニング ファイルには、起動、マウント、実行するソフトウェア パッケージのリストが含まれます。インストールされている各パッケージの ISO ファイル システムは、フラッシュからルート ファイル システムに直接マウントされます。

（注） インストール モードで起動するために使用するパッケージとプロビジョニング ファイルは、フラッシュに保存する必要があります。usbflash0 または tftp: からインストール モードで起動することはサポートされていません。

関連トピック

例 : インストール モードでのソフトウェアブートアップ ディスプレイ （2814 ページ）
例 : 緊急インストール （2816 ページ）

バンドル モードでのブート

バンドル（.bin）ファイルを使用して、デバイス をバンドル モードでブートできます :

```
switch:  boot flash:cat3850-universalk9.SSA.03.08.83.EMD.150-8.83.EMD.bin
```

バンドルに含まれるプロビジョニング ファイルは、どのパッケージを起動、マウント、および実行するかを判断するために使用されます。パッケージはバンドルから取得され、RAM にコピーされます。各パッケージの ISO ファイル システムは、ルート ファイル システムにマウントされます。

インストール モードでの起動とは異なり、バンドル モードでの起動では、バンドルのサイズに対応するサイズの追加メモリが使用されます。

インストール モードでの起動とは異なり、バンドル モードでの起動は複数のメディアから利用できます :

- flash:
- usbflash0:
- tftp:

（注） バンドル モードでの起動では、自動インストールおよびスマート インストール機能はサポートされません。

（注） バンドル モードでの起動では、AP イメージのプレダウンロード機能はサポートされません。プレダウンロード機能の詳細については、Cisco WLC 5700 シリーズの「*Preloading an Image to Access Points*（アクセス ポイントへのイメージのダウンロード）」の章を参照してください。

関連トピック

例 : インストール モードでのソフトウェアブートアップ ディスプレイ （2814 ページ）

例：緊急インストール （2816 ページ）

スイッチ スタックのブート モード

スタック内のすべてのスイッチは、インストール モードまたはブート モードで実行している必要があります。混合モードのスタックはサポートされません。新しいスイッチが、別のブート モードのスタックに参加する場合、新しいスイッチは、V 不一致状態となります。

混合モードのスイッチ スタックが同時に起動する場合、アクティブ スイッチを除くすべてのスイッチは、V 不一致状態となります。ブート モードが自動アップグレードをサポートしない場合、スイッチ スタック メンバはアクティブ スイッチと同じブート モードで再起動する必要があります。

スタックがインストール モードで実行されている場合、スイッチ スタックに参加しようとしている新しいスイッチを自動的にアップグレードするために、自動アップグレード機能が使用できます。

自動アップグレード機能により新しいスイッチのブート モードがインストール モードに変更されます。スタックがバンドル モードでのブートで実行されている場合、自動アップグレード機能は使用できなくなります。スイッチ スタックに参加できるように、バンドル モードを使用して新しいスイッチを起動する必要があります。

次の例では、ブート モードがアクティブ スイッチと互換性がない場合に、スイッチ スタックに参加しようとするスイッチの状態を示します。

```
Device# show switch

Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch#   Role   Mac Address    Priority Version   State
-----------------------------------------------------------
 1       Member 6400 f125.1a00   1        0        V-Mismatch
*2       Active 6400.f125.1100   1        V01      Ready
Device
```

デバイス 情報の割り当て

IP 情報を割り当てるには、デバイスのセットアップ プログラムを使用する方法、Dynamic Host Configuration Protocol（DHCP）サーバを使用する方法、または手動で実行する方法があります。

特定の IP 情報の設定が必要な場合、デバイスのセットアップ プログラムを使用してください。このプログラムを使用すると、ホスト名とイネーブル シークレット パスワードを設定することもできます。

また、任意で、Telnet パスワードを割り当てたり（リモート管理中のセキュリティ確保のため）、スイッチをクラスタのコマンドまたはメンバスイッチとして、あるいはスタンドアロンスイッチとして設定したりできます。

サーバの設定後は DHCP サーバを使用して、IP 情報の集中管理と自動割り当てを行います。

（注） DHCP を使用している場合は、デバイスが動的に割り当てられた IP アドレスを受信してコンフィギュレーション ファイルを読み込むまでは、セットアップ プログラムからの質問に応答しないでください。

デバイスの設定手順を熟知している経験豊富なユーザの場合は、デバイスを手動で設定してください。それ以外のユーザは、「ブート プロセス」で説明したセットアップ プログラムを使用してください。

デフォルトのスイッチ情報

表 *178 :* デフォルトのスイッチ情報

機能	デフォルト設定
IP アドレスおよびサブネット マスク	IP アドレスまたはサブネット マスクは定義されていません。
デフォルト ゲートウェイ	デフォルト ゲートウェイは定義されていません。
イネーブル シークレット パスワード	パスワードは定義されていません。
Hostname	出荷時に割り当てられるデフォルトのホスト名は、デバイス です。
Telnet パスワード	パスワードは定義されていません。
クラスタ コマンド スイッチ機能	ディセーブル
クラスタ名	クラスタ名は定義されません。

DHCP ベースの自動設定の概要

DHCP は、インターネットホストおよびインターネットワーキングデバイスに設定情報を提供します。このプロトコルには、2 つのコンポーネントがあります。1 つは DHCP サーバからデバイスにコンフィギュレーション パラメータを提供するコンポーネント、もう 1 つはデバイスにネットワーク アドレスを割り当てるコンポーネントです。DHCP はクライアント/サーバ モデルに基づいています。指定された DHCP サーバが、動的に設定されるデバイスに対して、

ネットワーク アドレスを割り当て、コンフィギュレーション パラメータを提供します。デバイスは、DHCP クライアントおよび DHCP サーバとして機能できます。

DHCP ベースの自動設定では、デバイス（DHCP クライアント）は起動時に、IP アドレス情報およびコンフィギュレーション ファイルを使用して自動的に設定されます。

DHCP ベースの自動設定を使用すると、デバイス上で DHCP クライアント側の設定を行う必要はありません。ただし、DHCP サーバで、IP アドレスに関連した各種リース オプションを設定する必要があります。

DHCP を使用してネットワーク上のコンフィギュレーション ファイルの場所をリレーする場合は、TFTP サーバおよびドメイン ネーム システム（DNS）サーバの設定が必要になることがあります。

（注） スイッチ スタックと DHCP、DNS、TFTP サーバとの間では冗長接続を確立することを推奨します。接続されているスタック メンバーがスイッチ スタックから削除された場合でも、これらのサーバがアクセス可能なまま維持されるように保証するうえで役立ちます。

デバイスの DHCP サーバは、スイッチと同じ LAN 上に配置することも、そのデバイスとは別の LAN 上に配置することもできます。DHCP サーバが異なる LAN 上で動作している場合、デバイスと DHCP サーバ間に、DHCP のリレー デバイスを設定する必要があります。リレー デバイスは、直接接続されている 2 つの LAN 間でブロードキャスト トラフィックを転送します。ルータはブロードキャスト パケットを転送しませんが、受信したパケットの宛先 IP アドレスに基づいてパケットを転送します。

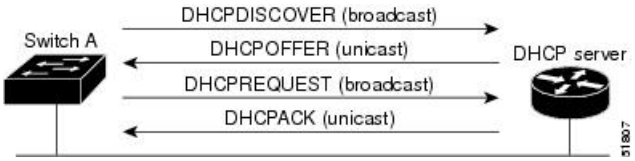
DHCP ベースの自動設定は、デバイスの BOOTP クライアント機能に代わるものです。

DHCP クライアントの要求プロセス

デバイスを起動したときに、デバイスにコンフィギュレーションファイルがない場合、DHCP クライアントが呼び出され、DHCP クライアントが DHCP サーバに設定情報を要求します。コンフィギュレーション ファイルが存在し、その設定に特定のルーテッド インターフェイスの **ip address dhcp** インターフェイス コンフィギュレーション コマンドが含まれる場合、DHCP クライアントが呼び出され、DHCP クライアントがインターフェイスに IP アドレス情報を要求します。

次は、DHCP クライアントと DHCP サーバの間で交換される一連のメッセージです。

図 *142 : DHCP* クライアント/サーバ間のメッセージ交換



クライアントであるデバイス A は、DHCP サーバの場所を特定するために、DHCPDISCOVER メッセージをブロードキャストします。DHCP サーバは、DHCPOFFER ユニキャスト メッセージによって、使用可能なコンフィギュレーション パラメータ（IP アドレス、サブネット マス

ク、ゲートウェイ IP アドレス、DNS IP アドレス、IP アドレス用のリースなど）をクライアントに提示します。

DHCPREQUEST ブロードキャスト メッセージでは、クライアントは、提示された設定情報に対して、DHCP サーバに正式な要求を戻します。この正式な要求はブロードキャストされるため、クライアントから DHCPDISCOVER ブロードキャスト メッセージを受信した他のすべての DHCP サーバは、クライアントに提示した IP アドレスを再利用できます。

DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに戻すことで、IP アドレスがクライアントに割り当てられたことを確認します。このメッセージによって、クライアントとサーバはバウンドされ、クライアントはサーバから受信した設定情報を使用します。デバイスの受信する情報量は、DHCP サーバの設定方法によって異なります。

DHCPOFFER ユニキャスト メッセージによって送信されたコンフィギュレーション パラメータが無効である（コンフィギュレーション エラーがある）場合、クライアントは DHCP サーバに、DHCPDECLINE ブロードキャスト メッセージを戻します。

DHCP サーバはクライアントに、提示されたコンフィギュレーション パラメータが割り当てられていない、パラメータのネゴシエーション中にエラーが発生した、または DHCPOFFER メッセージに対するクライアントの応答が遅れている（DHCP サーバがパラメータを別のクライアントに割り当てた）という意味の DHCPNAK 拒否ブロードキャスト メッセージを送信します。

DHCP クライアントは、複数の DHCP サーバまたは BOOTP サーバから提示を受け取り、そのうちの任意の 1 つを受け入れることができますが、通常は最初に受け取った提示を受け入れます。DHCP サーバから提示された IP アドレスが必ずしもクライアントに割り当てられるわけではありません。ただし、サーバは通常、クライアントが正式にアドレスを要求するまではアドレスを確保しておきます。デバイスが BOOTP サーバからの応答を受け入れ、自身を設定する場合、デバイスはデバイス コンフィギュレーション ファイルを取得するために、TFTP 要求をユニキャストするのではなくブロードキャストします。

DHCP ホスト名オプションにより、デバイスのグループはホスト名および標準コンフィギュレーションを集中管理型 DHCP サーバから取得できます。クライアント（デバイス）は DCHPDISCOVER メッセージ内に、DHCP サーバからのホスト名および他のコンフィギュレーション パラメータの要求に使用される Option 12 フィールドを加えます。すべてのクライアントのコンフィギュレーション ファイルは、DHCP から取得したホスト名を除き、まったく同じです。

クライアントにデフォルトのホスト名がある場合（**hostname** *name* グローバル コンフィギュレーション コマンドを設定していないか、**no hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を削除していない場合）は、**ip address dhcp** インターフェイス コンフィギュレーション コマンドを入力すると、DHCP のホスト名オプションがパケットに含まれません。この場合、インターフェイスの IP アドレスを取得中にクライアントが DHCP との相互作用で DHCP ホスト名オプションを受信した場合、クライアントは DHCP ホスト名オプションを受け入れて、システムに設定済みのホスト名があることを示すフラグが設定されます。

DHCP ベースの自動設定およびイメージ アップデート

DHCPイメージアップグレード機能を使用すると、ネットワーク内の1つ以上のデバイスに新しいイメージ ファイルおよび新しいコンフィギュレーション ファイルをダウンロードするようにDHCPサーバを設定できます。ネットワーク内のすべてのスイッチでのイメージおよびコンフィギュレーションの同時アップグレードによって、ネットワークに加えられたそれぞれの新しいデバイスが、同じイメージとコンフィギュレーションを確実に受信するようになります。

DHCP イメージ アップグレードには、自動設定およびイメージ アップデートの 2 つのタイプがあります。

DHCP ベースの自動設定の制約事項

- ネットワーク内に割り当てられた IP アドレスがなく、1 つ以上のレイヤ 3 インターフェイスが起動してない場合は、設定プロセスが保存されたDHCPベースの自動設定は停止します。
- タイムアウトを設定しない限り、設定機能を備えている DHCP ベースの自動設定は IP アドレスのダウンロードを無期限に繰り返します。
- コンフィギュレーションファイルをダウンロードできないか破損している場合は、自動インストールプロセスが停止します。
- TFTP からダウンロードされたコンフィギュレーション ファイルは、実行コンフィギュレーション内の既存コンフィギュレーションとマージされますが、**write memory** または **copy running-configuration startup-configuration** 特権 EXEC コマンドを入力しない限り、NVRAMに保存されません。ダウンロードされたコンフィギュレーションがスタートアップ コンフィギュレーションに保存された場合、後続のシステム再起動中にこの機能はトリガーされません。

DHCP 自動設定

DHCP 自動設定は、コンフィギュレーション ファイルを DHCP サーバからネットワーク内の1つ以上のデバイスにダウンロードします。ダウンロードされたコンフィギュレーションファイルは、デバイスの実行コンフィギュレーションファイルになります。このファイルは、デバイスがリロードされるまで、フラッシュ メモリに保存されたブートアップ コンフィギュレーションを上書きしません。

DHCP 自動イメージ アップデート

DHCP自動設定とともにDHCP自動イメージアップグレードを使用すると、コンフィギュレーションおよび新しいイメージをネットワーク内の 1 つ以上のデバイスにダウンロードできます。新しいコンフィギュレーションおよび新しいイメージをダウンロードしている1つのデバイススイッチ（または複数のデバイス）は、ブランク（つまり、出荷時のデフォルト設定がロードされている状態）にできます。

コンフィギュレーションをすでに持っているスイッチに新しいコンフィギュレーションをダウンロードすると、ダウンロードされたコンフィギュレーションは、スイッチに保存されているコンフィギュレーション ファイルに追加されます（どの既存のコンフィギュレーション ファイルも、ダウンロードされたファイルに上書きされません）。

デバイスの DHCP 自動イメージ アップデートをイネーブルにするには、イメージ ファイルおよびコンフィギュレーションファイルがあるTFTPサーバを、正しいオプション67（コンフィギュレーション ファイル名）、オプション 66（DHCP サーバ ホスト名）、オプション 150（TFTP サーバ アドレス）、およびオプション 125（Cisco IOS イメージ ファイルの説明）の設定で設定する必要があります。

デバイスをネットワークに設置すると、自動イメージアップデート機能が開始します。ダウンロードされたコンフィギュレーションファイルはデバイスの実行コンフィギュレーションに保存され、新しいイメージがダウンロードされてデバイスにインストールされます。デバイスを再起動すると、このコンフィギュレーションがデバイスのコンフィギュレーションに保存されます。

DHCP サーバ設定時の注意事項

デバイスを DHCP サーバとして設定する場合、次の注意事項に従ってください。

- DHCPサーバには、デバイスのハードウェア アドレスによって各デバイスと結び付けられている予約済みのリースを設定する必要があります。
- デバイスに IP アドレス情報を受信させるには、DHCP サーバに次のリース オプションを設定する必要があります。
  - クライアントの IP アドレス（必須）
  - クライアントのサブネット マスク（必須）
  - DNS サーバの IP アドレス（任意）
  - ルータの IP アドレス（デバイスで使用するデフォルト ゲートウェイ アドレス）（必須）
- デバイスにTFTPサーバからコンフィギュレーションファイルを受信させる場合は、DHCPサーバに次のリース オプションを設定する必要があります。
  - TFTP サーバ名（必須）
  - ブートファイル名（クライアントが必要とするコンフィギュレーションファイル名）（推奨）
  - ホスト名（任意）
- DHCPサーバの設定によっては、デバイスはIPアドレス情報またはコンフィギュレーション ファイル、あるいはその両方を受信できます。
- 前述のリースオプションを設定しなかった場合、DHCPサーバは、設定されたパラメータのみを使用してクライアントの要求に応答します。IP アドレスおよびサブネット マスク

が応答に含まれていないと、デバイスは設定されません。ルータの IP アドレスまたは TFTP サーバ名が見つからなかった場合、デバイスは TFTP 要求をユニキャストしないでブロードキャストする場合があります。その他のリース オプションは、使用できなくても自動設定には影響しません。

- デバイスは DHCP サーバとして動作可能です。デフォルトでは、Cisco IOS DHCP サーバおよび DHCP リレー エージェント機能はデバイス上でイネーブルにされていますが、設定されていません。（これらの機能は動作しません）

TFTP サーバの目的

DHCP サーバの設定に基づいて、デバイスは TFTP サーバから 1 つまたは複数のコンフィギュレーション ファイルをダウンロードしようとします。TFTP サーバへの IP 接続に必要なすべてのオプションについてデバイスに応答するよう DHCP を設定している場合で、なおかつ、TFTP サーバ名、アドレス、およびコンフィギュレーション ファイル名を指定して DHCP サーバを設定している場合、デバイスは指定された TFTP サーバから指定されたコンフィギュレーション ファイルをダウンロードしようとします。

コンフィギュレーション ファイル名、および TFTP サーバを指定しなかった場合、またはコンフィギュレーション ファイルをダウンロードできなかった場合は、デバイスはファイル名と TFTP サーバアドレスをさまざまに組み合わせてコンフィギュレーション ファイルをダウンロードしようとします。ファイルには、特定のコンフィギュレーション ファイル名（存在する場合）と次のファイルが指定されています。network-config、cisconet.cfg、*hostname*.config、または *hostname*.cfg です。この場合、*hostname* はデバイスの現在のホスト名です。使用される TFTP サーバアドレスには、（存在する場合）指定された TFTP サーバのアドレス、およびブロードキャスト アドレス（255.255.255.255）が含まれています。

デバイスが正常にコンフィギュレーション ファイルをダウンロードするには、TFTP サーバのベース ディレクトリに 1 つまたは複数のコンフィギュレーション ファイルが含まれていなければなりません。含めることのできるファイルは、次のとおりです。

- DHCP 応答で指定されているコンフィギュレーション ファイル（実際のデバイス コンフィギュレーション ファイル）。
- network-confg または cisconet.cfg ファイル（デフォルトのコンフィギュレーション ファイル）
- router-confg または ciscortr.cfg ファイル（これらのファイルには、すべてのデバイスに共通のコマンドが含まれています。通常、DHCP および TFTP サーバが適切に設定されていれば、これらのファイルはアクセスされません）

DHCP サーバ リース データベースに TFTP サーバ名を指定する場合は、DNS サーバのデータベースに TFTP サーバ名と IP アドレスのマッピングを設定することも必要です。

使用する TFTP サーバが、デバイスとは異なる LAN 上にある場合、またはデバイスがブロードキャスト アドレスを使用してアクセスした場合（前述のすべての必須情報が DHCP サーバの応答に含まれていない場合に発生）は、リレーを設定して TFTP サーバに TFTP パケットを転送する必要があります。適切な解決方法は、必要なすべての情報を使用して DHCP サーバを設定することです。

DNS サーバの目的

DHCP サーバは、DNS サーバを使用して TFTP サーバ名を IP アドレスに変換します。DNS サーバ上で、TFTP サーバ名から IP アドレスへのマッピングを設定する必要があります。TFTP サーバには、デバイスのコンフィギュレーション ファイルが存在します。

DHCP の応答時に IP アドレスを取得する DHCP サーバのリース データベースに、DNS サーバの IP アドレスを設定できます。リース データベースには、DNS サーバの IP アドレスを 2 つまで入力できます。

DNS サーバは、デバイスと同じ LAN 上に配置することも、別の LAN 上に配置することもできます。DNS サーバが別の LAN 上に存在する場合、デバイスはルータを介して DNS サーバにアクセスできなければなりません。

コンフィギュレーション ファイルの入手方法

IP アドレスおよびコンフィギュレーション ファイル名が DHCP で専用のリースとして取得できるかどうかに応じて、デバイスは次の方法で設定情報を入手します。

- IP アドレスおよびコンフィギュレーション ファイル名が、デバイス用に予約され、DHCP 応答（1 ファイル読み込み方式）で提供されている場合

  デバイスは DHCP サーバから、IP アドレス、サブネット マスク、TFTP サーバ アドレス、およびコンフィギュレーション ファイル名を受信します。デバイスは、TFTP サーバにユニキャスト メッセージを送信し、指定されたコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、ブートアップ プロセスを完了します。

- デバイスの IP アドレスおよびコンフィギュレーション ファイル名が予約されているが、DHCP 応答に TFTP サーバ アドレスが含まれていない場合（1 ファイル読み込み方式）。

  デバイスは DHCP サーバから、IP アドレス、サブネット マスク、およびコンフィギュレーション ファイル名を受信します。デバイスは、TFTP サーバにブロードキャスト メッセージを送信し、指定されたコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、ブートアップ プロセスを完了します。

- IP アドレスだけがデバイス用に予約され、DHCP 応答で提供されており、コンフィギュレーション ファイル名は提供されない場合（2 ファイル読み込み方式）

  デバイス は DHCP サーバから、IP アドレス、サブネット マスク、および TFTP サーバ アドレスを受信します。デバイスは、TFTP サーバにユニキャストメッセージを送信し、network-confg または cisconet.cfg のデフォルト コンフィギュレーション ファイルを取得します（network-confg ファイルが読み込めない場合、デバイスは cisconet.cfg ファイルを読み込みます）。

  デフォルト コンフィギュレーション ファイルには、デバイスのホスト名から IP アドレスへのマッピングが含まれています。デバイスは、ファイルの情報をホストテーブルに書き込み、ホスト名を入手します。ファイルにホスト名がない場合、デバイスは DHCP 応答で指定されたホスト名を使用します。DHCP 応答でホスト名が指定されていない場合、デバイスはデフォルトのスイッチをホスト名として使用します。

デフォルトのコンフィギュレーション ファイルまたは DHCP 応答からホスト名を入手した後、デバイスはホスト名と同じ名前のコンフィギュレーション ファイル（network-confg または cisconet.cfg のどちらが先に読み込まれたかに応じて、*hostname*-confg または *hostname*.cfg）を TFTP サーバから読み込みます。cisconet.cfg ファイルが読み込まれている場合は、ホストのファイル名は 8 文字に切り捨てられます。

network-confg、cisconet.cfg、またはホスト名と同じ名前のファイルを読み込むことができない場合、デバイスは router-confg ファイルを読み込みます。router-confg ファイルを読み込むことができない場合、デバイスは ciscortr.cfg ファイルを読み込みます。

（注） DHCP 応答から TFTP サーバを入手できなかった場合、ユニキャスト伝送によるコンフィギュレーション ファイルの読み込みにすべて失敗した場合、または TFTP サーバ名を IP アドレスに変換できない場合には、デバイスは TFTP サーバ要求をブロードキャストします。

環境変数の制御方法

通常動作デバイスでは、9600 bps に設定されているコンソール接続のみを通じてブート ローダ モードを開始します。電源コードを再接続中にデバイス電源コードを取り外し、[Mode] ボタンを押します。すべてのオレンジのシステム LED が点灯したままになったら、[Mode] ボタンを放してもかまいません。ブートローダの デバイス プロンプトが表示されます。

デバイスのブート ローダ ソフトウェアは不揮発性の環境変数をサポートするため、これらの環境変数を使用して、ブートローダまたはシステムで稼働する他のソフトウェアの動作を制御できます。ブートローダの環境変数は、UNIX または DOS システムで設定できる環境変数と類似しています。

値を持つ環境変数は、フラッシュ ファイル システムの外にあるフラッシュ メモリに保存されます。

ファイルの各行には、環境変数名と等号に続いて、その変数の値が指定されます。変数が存在しない場合は、変数の値はありません。値がヌルストリングと表示された場合は、変数に値が設定されています。ヌル ストリング（たとえば " "）が設定されている変数は、値が設定された変数です。多くの環境変数は事前に定義されており、デフォルト値が設定されています。

環境変数の設定を変更するには、ブートローダにアクセスするか、Cisco IOS コマンドを使用します。通常の環境では、環境変数の設定を変更する必要はありません。

一般的な環境変数

この表では、最も一般的な環境変数の機能について説明します。

表 *179 :* 一般的な環境変数

変数	ブートローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
BOOT	**set BOOT** *filesystem*:/ *file-url* ... 自動起動時にロードして実行を試みる、セミコロンで区切られた実行可能ファイルのリスト。	**boot system** {*filesystem*: /*file-url* ...| **switch** {*number* | **all**}} 次の起動時にロードする Cisco IOS イメージと、イメージがロードされるスタック メンバーを指定します。このコマンドは、BOOT 環境変数の設定を変更します。 パッケージプロビジョニング ファイルは、*packages.conf* ファイルとも呼ばれ、起動時にどのソフトウェア パッケージをアクティブ化するかを判断するために、システムが使用するものです。 • インストール モードで起動する場合、アクティブ化するパッケージを指定するために、**boot** コマンドで指定されたパッケージプロビジョニング ファイルが使用されます。例：**boot flash:packages.conf**。 • バンドル モードで起動する場合、起動したバンドルに含まれているパッケージのプロビジョニング ファイルがバンドルに含まれているパッケージのアクティブ化に使用されます。例：**boot flash:image.bin**。

変数	ブートローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
MANUAL_BOOT	**set MANUAL_BOOT yes** スイッチの起動を自動で行うか手動で行うかを決定します。 有効な値は 1、yes、0、および no です。no または 0 に設定されている場合、ブートローダはシステムを自動的に起動しようとします。それ以外の値に設定されている場合は、ブートローダ モードから手動でスイッチを起動する必要があります。	**boot manual** 次回の起動時にスイッチを手動で起動できるようにします。MANUAL_BOOT 環境変数の設定が変更されます。 次回のシステム再起動時には、スイッチはブートローダ モードになります。システムを起動するには、**boot flash:** *filesystem***:/** *file-url* ブート ローダ コマンドを使用してブート可能なイメージの名前を指定します。
CONFIG_FILE	**set CONFIG_FILE flash:/** *file-url* Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を変更します。	**boot config-file flash:/** *file-url* Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。このコマンドによって、CONFIG_FILE 環境変数が変更されます。
SWITCH_NUMBER	**set SWITCH_NUMBER** *stack-member-number* スタック メンバのメンバ番号を変更します。	**switch** *current-stack-member-number* **renumber** *new-stack-member-number* スタック メンバのメンバ番号を変更します。
SWITCH_PRIORITY	**set SWITCH_PRIORITY** *stack-member-number* スタック メンバのプライオリティ値を変更します。	**switch** *stack-member-number***priority** *priority-number* スタック メンバのプライオリティ値を変更します。
BAUD	**set BAUD** *baud-rate*	**line console 0** **speed** *speed-value* ボー レートを設定します。
ENABLE_BREAK	**set ENABLE_BREAK yes/no**	**boot enable-break switch yes/no** 自動起動時の break をイネーブルにします。**break** コマンドの入力に与えられた時間は 5 秒です。

TFTP の環境変数

イーサネット管理ポートを通してスイッチに PC を接続していると、TFTP でブートローダに対してコンフィギュレーションファイルのアップロードまたはダウンロードができます。このテーブルの環境変数が設定されていることを確認します。

表 *180 : TFTP* の環境変数

変数	説明
MAC_ADDR	スイッチの MAC アドレスを指定します。 （注） 変数は変更しないことを推奨します。 ただし、ブートローダを稼働した後に変数を変更した場合、またはこの変数が保存されている値と異なる場合は、TFTP を使用する前にこのコマンドを入力します。
IP_ADDR	スイッチの関連付けられた IP サブネットに IP アドレスおよびサブネット マスクを指定します。
DEFAULT_ROUTER	デフォルト ゲートウェイに IP アドレスおよびサブネット マスクを指定します。

ソフトウェア イメージのリロードのスケジューリング

デバイス上でソフトウェアイメージのリロードを後で（深夜や週末など、デバイスをあまり使用しないときに）行うよう、スケジュールを設定できます。または（ネットワーク内のすべてのデバイスでソフトウェアのアップグレードを実行する場合などに）ネットワーク全体でリロードを同時に行うことができます。

（注） リロードのスケジュールは、約 24 日以内に設定する必要があります。

リロード オプションには以下のものがあります。

- 指定した分数、または時間および分数が経過したときに、ソフトウェアがリロードされます。リロードは、約 24 時間以内に実行する必要があります。最大 255 文字で、リロードの理由を指定できます。
- ソフトウェアのリロードが（24時間制で）指定された時間に有効になります。月日を指定すると、指定された日時にリロードが行われるようにスケジュールが設定されます。月日を指定しなかった場合、リロードは当日の指定時刻に行われます（指定時刻が現時刻より後の場合）。または翌日の指定時刻に行われます（指定時刻が現在時刻よりも前の場合）。00:00 を指定すると、深夜 0 時のリロードが設定されます。

reload コマンドはシステムを停止させます。手動で起動することが設定されていない限り、システムは自動的に再起動します。

手動で起動するようにデバイスが設定されている場合、仮想端末からリロードを実行しないでください。これは、デバイスがブート ローダ モードになることでリモート ユーザが制御を失う、ということを防止するための制約です。

コンフィギュレーションファイルを変更すると、リロードの前にコンフィギュレーションを保存するように指示するプロンプトがデバイスにより表示されます。保存操作時に、CONFIG_FILE 環境変数がすでに存在しないスタートアップ コンフィギュレーション ファイルを示していた場合、保存を続行するかどうかという問い合わせがシステムから出されます。その状況のまま続けると、リロード時にセットアップ モードが開始されます。

スケジュールがすでに設定されたリロードを取り消すには、**reload cancel** 特権 EXEC コマンドを使用します。

デバイスセットアップ設定の実行方法

DHCP を使用してデバイスに新しいイメージおよび新しいコンフィギュレーションをダウンロードするには、少なくとも 2 つのデバイス を設定する必要があります。1 つ目のデバイスは DHCP サーバおよび TFTP サーバと同じように機能し、2 つ目のデバイス（クライアント）は新しいコンフィギュレーション ファイル、または新しいコンフィギュレーション ファイルおよび新しいイメージ ファイルをダウンロードするように設定されています。

DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定

このタスクでは、新しいデバイス。の自動設定をサポートできるように、ネットワーク内の既存のデバイスで TFTP や DHCP 設定の DHCP 自動設定を行う方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool** *poolname* 例： `Device(config)# ip dhcp pool pool`	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**boot** *filename* 例： `Device(dhcp-config)# boot config-boot.text`	ブートイメージとして使用されるコンフィギュレーションファイルの名前を指定します。
ステップ 4	**network** *network-number mask prefix-length* 例： `Device(dhcp-config)# network 10.10.10.0 255.255.255.0`	DHCP アドレス プールのサブネットネットワーク番号およびマスクを指定します。 （注） プレフィックス長は、アドレスプレフィックスを構成するビット数を指定します。プレフィックスは、クライアントのネットワークマスクを指定する二者択一の方法です。プレフィックス長は、スラッシュ（/）で開始する必要があります。
ステップ 5	**default-router** *address* 例： `Device(dhcp-config)# default-router 10.10.10.1`	DHCP クライアントのデフォルト ルータの IPアドレスを指定します。
ステップ 6	**option 150** *address* 例： `Device(dhcp-config)# option 150 10.10.10.1`	TFTP サーバの IP アドレスを指定します。
ステップ 7	**exit** 例： `Device(dhcp-config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**tftp-server flash**:*filename.text* 例： `Device(config)# tftp-server flash:config-boot.text`	TFTP サーバ上のコンフィギュレーション ファイルを指定します。

	コマンドまたはアクション	目的
ステップ 9	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/4`	コンフィギュレーションファイルを受信するクライアントのアドレスを指定します。
ステップ 10	**no switchport** 例： `Device(config-if)# no switchport`	インターフェイスをレイヤ 3 モードにします。
ステップ 11	**ip address** *address mask* 例： `Device(config-if)# ip address 10.10.10.1 255.255.255.0`	IP アドレスとインターフェイスのマスクを指定します。
ステップ 12	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

例：DHCP サーバとしてのデバイスの設定 （2817 ページ）

DHCP 自動イメージ アップデート（コンフィギュレーション ファイルおよびイメージ）の設定

このタスクでは、新しいスイッチのインストールをサポートするように既存のデバイスでTFTPおよび DHCP を設定する DHCP 自動設定について説明します。

始める前に

最初にデバイスにアップロードするテキスト ファイル（たとえば、autoinstall_dhcp）を作成します。テキスト ファイルに、ダウンロードするイメージの名前を指定します（たとえば、c3750e-ipservices-mz.122-44.3.SE.tarc3750x-ipservices-mz.122-53.3.SE2.tar）。このイメージは、bin ファイルでなく、tar ファイルである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool** *poolname* 例： `Device(config)# ip dhcp pool pool1`	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**boot** *filename* 例： `Device(dhcp-config)# boot config-boot.text`	ブートイメージとして使用されるファイルの名前を指定します。
ステップ 4	**network** *network-number mask prefix-length* 例： `Device(dhcp-config)# network 10.10.10.0 255.255.255.0`	DHCP アドレス プールのサブネット ネットワーク番号およびマスクを指定します。 （注） プレフィックス長は、アドレスプレフィックスを構成するビット数を指定します。プレフィックスは、クライアントのネットワーク マスクを指定する二者択一の方法です。プレフィックス長は、スラッシュ（/）で開始する必要があります。
ステップ 5	**default-router** *address* 例： `Device(dhcp-config)# default-router 10.10.10.1`	DHCP クライアントのデフォルト ルータの IPアドレスを指定します。
ステップ 6	**option 150** *address* 例： `Device(dhcp-config)# option 150 10.10.10.1`	TFTP サーバの IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 7	**option 125** *hex* 例： `Device(dhcp-config)# option 125 hex 0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370`	イメージファイルのパスを記述したテキストファイルのパスを指定します。
ステップ 8	**copy tftp flash** *filename.txt* 例： `Device(config)# copy tftp flash image.bin`	デバイスに、テキストファイルをアップロードします。
ステップ 9	**copy tftp flash** *imagename.bin* 例： `Device(config)# copy tftp flash image.bin`	デバイスに、新しいイメージの tar ファイルをアップロードします。
ステップ 10	**exit** 例： `Device(dhcp-config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**tftp-server flash:** *config.text* 例： `Device(config)# tftp-server flash:config-boot.text`	TFTP サーバ上の Cisco IOS コンフィギュレーション ファイルを指定します。
ステップ 12	**tftp-server flash:** *imagename.bin* 例： `Device(config)# tftp-server flash:image.bin`	TFTP サーバ上のイメージ名を指定します。
ステップ 13	**tftp-server flash:** *filename.txt* 例： `Device(config)# tftp-server flash:boot-config.text`	ダウンロードするイメージファイルの名前を記述したテキストファイルを指定します。

	コマンドまたはアクション	目的
ステップ 14	**interface** *interface-id* 例： `Device(config)# interface gigabitEthernet1/0/4`	コンフィギュレーションファイルを受信するクライアントのアドレスを指定します。
ステップ 15	**no switchport** 例： `Device(config-if)# no switchport`	インターフェイスをレイヤ 3 モードにします。
ステップ 16	**ip address** *address mask* 例： `Device(config-if)# ip address 10.10.10.1 255.255.255.0`	IP アドレスとインターフェイスのマスクを指定します。
ステップ 17	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 18	**copyrunning-configstartup-config** 例： `Device(config-if)# end`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

例：DHCP 自動イメージ アップデートの設定 （2818 ページ）

DHCP サーバからファイルをダウンロードするクライアントの設定

（注） レイヤ3インターフェイスだけを設定してイネーブルにする必要があります。保存されているコンフィギュレーションのDHCPベースの自動設定にIPアドレスを割り当てないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot host dhcp** 例： `Device(conf)# boot host dhcp`	保存されているコンフィギュレーションで自動設定をイネーブルにします。
ステップ 3	**boot host retry timeout** *timeout-value* 例： `Device(conf)# boot host retry timeout 300`	（任意）システムがコンフィギュレーション ファイルをダウンロードしようとする時間を設定します。 （注） タイムアウトを設定しないと、システムは無期限にDHCP サーバから IP アドレスを取得しようとします。
ステップ 4	**banner config-save ^C** *warning-message*^C 例： `Device(conf)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause You to No longer Automatically Download Configuration Files at Reboot^C`	（任意）コンフィギュレーション ファイルを NVRAM に保存しようとするときに表示される警告メッセージを作成します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show boot** 例： `Device# show boot`	設定を確認します。

関連トピック

例：DHCP サーバから設定をダウンロードするためのデバイスの設定 （2818 ページ）

複数の SVI への IP 情報の手動割り当て

このタスクでは、複数のスイッチ仮想インターフェイス（SVI）に IP 情報を手動で割り当てる方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 99`	インターフェイスコンフィギュレーション モードを開始して、IP 情報が割り当てられている VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
ステップ 3	**ip address** *ip-address subnet-mask* 例： `Device(config-vlan)# ip address 10.10.10.2 255.255.255.0`	IP アドレスとサブネット マスクを入力します。
ステップ 4	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip default-gateway** *ip-address* 例： `Device(config)# ip default-gateway 10.10.10.1`	デバイスに直接接続しているネクストホップのルータ インターフェイスの IP アドレスを入力します。このスイッチにはデフォルト ゲートウェイが設定されています。デフォルトゲートウェイは、デバイススイッチから宛先 IP アドレスを取得していない IP パケットを受信します。 デフォルト ゲートウェイが設定されると、デバイスは、ホストが接続する必要のあるリモート ネットワークに接続できます。

	コマンドまたはアクション	目的
		（注） IP でルーティングするようにデバイスを設定した場合、デフォルト ゲートウェイの設定は不要です。 （注） デフォルトゲートウェイの構成に基づいて、デバイスの CAPWAP は中継を行い、ルーティングされたアクセス ポイントとデバイスの接続をサポートします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces vlan** *vlan-id* 例： `Device# show interfaces vlan 99`	設定された IP アドレスを確認します。
ステップ 8	**show ip redirects** 例： `Device# show ip redirects`	設定されたデフォルト ゲートウェイを確認します。

デバイスのスタートアップ コンフィギュレーションの変更

システム コンフィギュレーションを読み書きするためのファイル名の指定

Cisco IOS ソフトウェアは、デフォルトで config.text ファイルを使用して、システム コンフィギュレーションの不揮発性コピーを読み書きします。別のファイル名を指定することもできます。次回の起動時には、その名前のファイルが読み込まれます。

始める前に

このタスクではスタンドアロンの デバイス を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot flash**:*/file-url* 例： `Device(config)# boot flash:config.text`	次回の起動時に読み込むコンフィギュレーション ファイルを指定します。 *file-url*：パス（ディレクトリ）およびコンフィギュレーション ファイル名。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show boot** 例： `Device# show boot`	入力を確認します。 **boot** グローバル コンフィギュレーション コマンドによって、CONFIG_FILE 環境変数の設定が変更されます。
ステップ 5	**copyrunning-configstartup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチの手動による起動

スイッチはデフォルトで自動的に起動しますが、手動で起動するように設定することもできます。

始める前に

このタスクのスタンドアロン スイッチを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot manual** 例： `Device(config)# boot manual`	次回の起動時に、スイッチを手動で起動できるようにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show boot** 例： `Device# show boot`	入力を確認します。 **boot manual** グローバル コンフィギュレーション コマンドによって、MANUAL_BOOT 環境変数の設定が変更されます。 次回、システムを再起動したときには、スイッチはブートローダ モードになり、ブートローダ モードであることが *switch:* プロンプトによって示されます。システムを起動するには、**boot** *filesystem:/file-url* ブート ローダ コマンドを使用します。 • *filesystem*：システム ボードのフラッシュ デバイスに flash: を使用します。 デバイス: **boot flash:** • *file-url*：パス（ディレクトリ）および起動可能なイメージの名前を指定します。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。

	コマンドまたはアクション	目的
ステップ 5	**copyrunning-configstartup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Deviceをインストール モードで起動する場合

手順

	コマンドまたはアクション	目的
ステップ 1	**cp** *source_file_path destination_file_path* 例： `Device# copy tftp://10.0.0.6/cat3k_caa-universalk9.SSA.03.12.02.EXP.150-12.02.EXP.150-12.02.EXP.bin flash:`	（任意）FTP または TFTP サーバから、bin ファイル（`image.bin`）をフラッシュまたは USB フラッシュにコピーします。

ステップ 2	**software expand file** *source_file_path*
	例：
	TFTP からの bin ファイルの解凍：
	`Switch# software expand file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to flash:`
	`Preparing expand operation ...`
	`[1]: Downloading file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to active switch 1`
	`[1]: Finished downloading file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to active switch 1`
	`[1]: Copying software from active switch 1 to switch 2`
	`[1]: Finished copying software to switch 2`
	`[1 2]: Expanding bundle cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin`
	`[1 2]: Copying package files`
	`[1 2]: Package files copied`
	`[1 2]: Finished expanding bundle cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin`
	
	`18 -rw- 74387812 Dec 7 2012 05:55:43 +00:00 cat3k_caa-base.SSA.03.09.37.EXP.pkg`
	`19 -rw- 2738868 Dec 7 2012 05:55:44 +00:00 cat3k_caa-drivers.SSA.03.09.37.EXP.pkg`
	
	`20 -rw- 32465772 Dec 7 2012`
		フラッシュ、FTP、TFTP、HTTP、または HTTPS サーバに保存された bin ファイルを、起動したデバイスに解凍します。
		（注） `packages.conf` ファイルが拡張されたファイル内に含まれていることを確認します。

	コマンドまたはアクション	目的
	05:55:44 +00:00 cat3k_caa-infra.SSA.03.09.37.EXP.pkg 21 -rw- 30389036 Dec 7 2012 05:55:44 +00:00 cat3k_caa-iosd-universalk9.SSA.150-9.37.EXP.pkg 22 -rw- 18342624 Dec 7 2012 05:55:44 +00:00 cat3k_caa-platform.SSA.03.09.37.EXP.pkg 23 -rw- 63374028 Dec 7 2012 05:55:44 +00:00 cat3k_caa-wcm.SSA.10.0.10.14.pkg 17 -rw- 1239 Dec 7 2012 05:56:29 +00:00 packages.conf	
ステップ 3	**reload** 例： Device: **reload**	デバイスをリロードします。 （注） packages.confデバイスファイルを使用して手動または自動で起動できます。手動で起動した場合、ステップ 4 に進むことができます。それ以外の場合、デバイスは自動的に起動します。
ステップ 4	**boot flash:packages.conf** 例： switch: **boot flash:packages.conf**	packages.conf ファイルでデバイスをブートします。
ステップ 5	**show version** 例： switch# **show version** Switch Ports Model SW Version SW Image Mode ------ ----- ----- ---------- ---------- ---- 1 6 WS-C3850-6DS-S 03.09.26.EXP ct3850-ipservicesk9 INSTALL	デバイスが**インストール** モードであることを確認します。

Deviceをバンドル モードで起動する場合

デバイスを起動するには、いくつかの方法があります。1 つは、TFTP サーバから bin ファイルをコピーしてデバイスを起動する方法です。または、**boot flash:<image.bin>** コマンドか、**boot usbflash0:<image.bin>** コマンドを使用して、デバイスをフラッシュまたは USB フラッシュから直接起動することもできます。

以下の手順は、バンドルモードで TFTP サーバからデバイスを起動する方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	**cp** *source_file_path destination_file_path* 例： `Device# copy tftp://10.0.0.6/cat3k_caa-universalk9.SPA.03.12.02.EZP.15-12.02.EZP.15-12.02.EZP.bin flash:`	（任意）FTP または TFTP サーバから、bin ファイル（`image.bin`）をフラッシュまたは USB フラッシュにコピーします。
ステップ 2	**switch:BOOT=<source path of .bin file>** 例： `Device: switch:BOOT=tftp://10.0.0.2/cat3k_caa-universalk9.SPA.03.09.37.EZP.15-9.37.EZP.bin`	ブート パラメータを設定します。
ステップ 3	**boot** 例： `switch: boot`	デバイスをブートします。

ステップ 4	**show version**
	例：
	`switch# show version`
	`Switch Ports Model SW Version SW Image Mode`
	`------ ----- ----- ---------- ---------- ----`
	`1 6 WS-C3850-6DS-S 03.09.40.EXP ct3850-ipservicesk9 BUNDLE`
		デバイスが**バンドル** モードであることを確認します。

スイッチ スタックで特定のソフトウェア イメージを起動する場合

スイッチはデフォルトで、BOOT 環境変数の情報を使用して、システムを自動的に起動しようとします。この変数が設定されていない場合、スイッチは、フラッシュ ファイル システム全体に再帰的に縦型検索し、最初の実行可能イメージをロードして実行しようとします。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。起動する具体的なイメージを指定することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**boot system switch** {*number* | **all**} 例： `Switch(config)# boot system switch 2 flash:cat3850-universalk9.SSA.03.08.83.EMD.150-8.83.EMD.bin`	（任意）スタックのスイッチについては、次回起動時にシステム イメージをロードするスイッチ メンバを指定します。 • スタック メンバを指定するには、*number* を使用します（1 つのスタック メンバのみを指定）。 • すべてのスタック メンバを指定するには、**all** を使用します。 Catalyst 3750-X スタック マスターまたはスタック メンバーを開始する場合、他の Catalyst 3750-X スタック メンバーにスイッチ イメージを指定できます。 Catalyst 3750-E スタック マスターまたはスタック メンバーを開始する場合、他の Catalyst 3750-E スタック メンバーにスイッチ イメージを指定できます。 Catalyst 3750 スイッチを指定する場合、Catalyst 3750 スタック メンバーでこのコマンドを入力します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show boot system** 例： `Device# show boot system`	入力を確認します。 **boot system** グローバル コマンドは、BOOT 環境変数の設定を変更します。 次回の起動時に、スイッチは BOOT 環境変数の情報を使用して、システムを自動的に起動しようとします。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ソフトウェア イメージのリロードのスケジュール設定

このタスクでは、ソフトウェアイメージを後でリロードするようにデバイスを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**copy running-config startup-config** 例： `copy running-config startup-config`	**reload** コマンドを使用する前に、デバイスの設定情報をスタートアップ コンフィギュレーションに保存します。

ステップ 3	**reload in** [*hh*:]*mm* [*text*]
	例：
	`Device(config)# reload in 12`
	`System configuration has been modified. Save? [yes/no]: y`
		指定した分数、または時間および分数が経過したときに、ソフトウェアがリロードされるようにスケジュールを設定します。リロードは、約 24 日以内に実行する必要があります。最大 255 文字で、リロードの理由を指定できます。

ステップ 4	**reload slot** [*stack-member-number*]
	例：
	`Device(config)# reload slot 6`
	`Proceed with reload? [confirm] y`
		スイッチ スタックのソフトウェアのリロードをスケジューリングします。

ステップ 5	**reload at** *hh*: *mm* [*month day* | *day month*] [*text*] 例：	リロードを実行する時間を、時間数と分数で指定します。

	コマンドまたはアクション	目的
	`Device(config)# reload at 14:00`	（注） デバイスのシステム クロックが（ネットワーク タイム プロトコル（NTP）、ハードウェア カレンダー、または手動で）設定されている場合にのみ、**at** キーワードを使用します。時刻は、デバイスに設定されたタイム ゾーンに基づきます。リロードが複数のデバイスで同時に行われるようにスケジューリングするには、各デバイスの時間が NTP と同期している必要があります。
ステップ 6	**reload cancel** 例： `Device(config)# reload cancel`	以前にスケジューリングされたリロードをキャンセルします。
ステップ 7	**show reload** 例： **show reload**	以前デバイスにスケジューリングされたリロードに関する情報、またはリロードがスケジューリングされているかを表示します。

デバイスのセットアップ設定のモニタリング

例：デバイス実行コンフィギュレーションの確認

```
Device# show running-config
Building configuration...

Current configuration: 1363 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Stack1
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxE0
!
.
<output truncated>
.
```

```
interface gigabitethernet6/0/2
mvr type source

<output truncated>

...!
interface VLAN1
 ip address 172.20.137.50 255.255.255.0
 no ip directed-broadcast
!
ip default-gateway 172.20.137.1 !
!
snmp-server community private RW
snmp-server community public RO
snmp-server community private@es0 RW
snmp-server community public@es0 RO
snmp-server chassis-id 0x12
!
end
```

例：インストール モードでのソフトウェアブートアップ ディスプレイ

この例では、インストール モードでのソフトウェア ブートアップの表示を示します。

```
switch: boot flash:packages.conf

Getting rest of image
Reading full image into memory....done
Reading full base package into memory...: done = 74596432
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042f354
Kernel Size : 0x318412/3245074
Initramfs Address : 0x60747768
Initramfs Size : 0xdc08e8/14420200
Compression Format: .mzip

Bootable image at @ ram:0x6042f354
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@boot_system:
 377
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

All packages are Digitally Signed
Starting System Services
Nov 7 09:57:05 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_START: Switch 2
is starting stack discovery
##########################################################################################
Nov 7 09:59:07 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_DONE: Switch 2 has
 finished stack discovery
Nov 7 09:59:07 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-SWITCH_ADDED: Switch 2
 has been added to the stack
Nov 7 09:59:14 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-ACTIVE_ELECTED: Switch
 2 has been elected ACTIVE

Restricted Rights Legend
```

```
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706



Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),

Version 03.09.12.EMD EARLY DEPLOYMENT ENGINEERING NOVA_WEEKLY BUILD, synced to
DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 04-Nov-12 22:53 by gereddy
License level to iosd is ipservices
```

この例では、バンドル モードでのソフトウェア ブートアップの表示を示します。

```
switch: boot flash:cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin


Reading full image into
memory.....................................................................done
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042ff38
Kernel Size : 0x318412/3245074
Initramfs Address : 0x6074834c
Initramfs Size : 0xdc08e8/14420200
Compression Format: .mzip

Bootable image at @ ram:0x6042ff38
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "flash:cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin" uncompressed and
installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

All packages are Digitally Signed
Starting System Services
Nov 7 09:45:49 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_START: Switch 2
is starting stack discovery
##########################################################################################################
Nov 7 09:47:50 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_DONE: Switch 2 has
 finished stack discovery
Nov 7 09:47:50 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-SWITCH_ADDED: Switch 2
 has been added to the stack
Nov 7 09:47:58 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-ACTIVE_ELECTED: Switch
 2 has been elected ACTIVE

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
```

```
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706



Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
 Version 03.09.12.EMD
EARLY DEPLOYMENT ENGINEERING NOVA_WEEKLY BUILD, synced to
DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 04-Nov-12 22:53 by gereddy
License level to iosd is ipservices
```

関連トピック

ソフトウェアのブート モード （2783 ページ）
インストール モードでのブート （2783 ページ）
バンドル モードでのブート （2784 ページ）

例：緊急インストール

以下に、**emergency-install** boot コマンドが開始された場合の出力サンプルの例を示します。

```
switch: emergency-install
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin


The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin)...
Reading full image into memory.....................done
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)



Initiating Emergency Installation of bundle
tftp://172.19.211.47/cstohs/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin
```

```
Downloading bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Validating bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Installing bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Verifying bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Package cat3k_caa-base.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-drivers.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-infra.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SSA.150-9.12.EMD.pkg is Digitally Signed
Package cat3k_caa-platform.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-wcm.SSA.03.09.12.EMD.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.



Booting...(use DDR clock 667 MHz)Initializing and Testing RAM +++@@@@####...++@@++@@++@@++@
```

関連トピック

ソフトウェアのブート モード （2783 ページ）
インストール モードでのブート （2783 ページ）
バンドル モードでのブート （2784 ページ）

デバイス のセットアップを実行する場合の設定例

例：DHCP サーバとしてのデバイスの設定

```
Device# configure terminal
Device(config)# ip dhcp pool pool1
Device(dhcp-config)# network 10.10.10.0 255.255.255.0
Device(dhcp-config)# boot config-boot.text
Device(dhcp-config)# default-router 10.10.10.1
Device(dhcp-config)# option 150 10.10.10.1
Device(dhcp-config)# exit
Device(config)# tftp-server flash:config-boot.text
Device(config)# interface gigabitethernet1/0/4
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.10.1 255.255.255.0
Device(config-if)# end
```

関連トピック

DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定 （2797 ページ）

例：DHCP 自動イメージ アップデートの設定

```
Device# configure terminal
Device(config)# ip dhcp pool pool1
Device(dhcp-config)# network 10.10.10.0 255.255.255.0
Device(dhcp-config)# boot config-boot.text
Device(dhcp-config)# default-router 10.10.10.1
Device(dhcp-config)# option 150 10.10.10.1
Device(dhcp-config)# option 125 hex
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370
Device(dhcp-config)# exit
Device(config)# tftp-server flash:config-boot.text
Device(config)# tftp-server flash:image_name
Device(config)# tftp-server flash:boot-config.text
Device(config)# tftp-server flash: autoinstall_dhcp
Device(config)# interface gigabitethernet1/0/4
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.10.1 255.255.255.0
Device(config-if)# end
```

関連トピック

DHCP 自動イメージ アップデート（コンフィギュレーション ファイルおよびイメージ）の設定 （2799 ページ）

例：DHCP サーバから設定をダウンロードするためのデバイスの設定

次に、VLAN 99 上のレイヤ 3 SVI インターフェイスを使用し、保存されているコンフィギュレーションで DHCP ベースの自動設定をイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# boot host dhcp
Device(config)# boot host retry timeout 300
Device(config)# banner config-save ^C Caution - Saving Configuration File to NVRAM May
Cause You to No longer Automatically Download Configuration Files at Reboot^C
Device(config)# vlan 99
Device(config-vlan)# interface vlan 99
Device(config-if)# no shutdown
Device(config-if)# end
Device# show boot
BOOT path-list:
Config file:          flash:/config.text
Private Config file:  flash:/private-config.text
Enable Break:         no
Manual Boot:          no
HELPER path-list:
NVRAM/Config file
      buffer size:    32768
Timeout for Config
          Download:    300 seconds
Config Download
       via DHCP:       enabled (next boot: enabled)
Device#
```

関連トピック

DHCP サーバからファイルをダウンロードするクライアントの設定 （2802 ページ）

例：ソフトウェア イメージのリロードのスケジューリング

次に、当日の午後 7 時 30 分に、ソフトウェアをデバイスにリロードする例を示します。

```
Device# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 2013 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

次に、未来の日時を指定して、ソフトウェアをデバイスにリロードする例を示します。

```
Device# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 2013 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```

デバイスのセットアップの実行に関する追加情報

関連資料

関連項目	マニュアル タイトル
デバイス セットアップ コマンド ブート ローダ コマンド	『*System Management Command Reference (Catalyst 3850 Switches)*』
プレダウンロード機能	*System Management Configuration Guide*（*Cisco WLC 5700 Series*）
IOS XE DHCP 設定	*IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*）
ハードウェアの設置	*Catalyst 3850* スイッチハードウェア インストレーションガイド
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*）

関連項目	マニュアル タイトル
プラットフォームに依存しない設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S（Catalyst 3850 Switches）*

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

WCM サブパッケージのインストール

このドキュメントでは、Cisco Catalyst 3850 および 3650 シリーズ スイッチでのワイヤレス コントロールモジュール（WCM）サブパッケージをインストールする手順について説明します。

WCM モジュールおよび AP イメージから成る WCM サブパッケージは、機能をアップグレードし、新しい AP をサポートし、既知の問題を解決します。これはイメージの WCM の部分だ

けをアップグレードするので、イメージ全体のアップグレードは不要で、それによるネットワーク ダウンタイムはありません。たとえば、WCMが、イメージのバージョンの不一致により、新しい AP をネットワークに接続させることができなかった場合は、イメージの WCM の部分だけをアップグレードして、新しい AP のサポートを追加します。WCM がアップグレードされると、ネットワーク内のすべての AP は、新しいイメージに自動的にアップグレードされます。

利点

- WCM のバグを修正
- 新しい AP をサポート
- WCM で使用可能な機能を更新

前提条件

- コントローラは、インストール モードで起動する必要があります。
- WCM サブパッケージは、インストーラがサポートする送信元で使用可能である必要があります。たとえば、フラッシュ、TFTP、USB などです。

[Restrictions（機能制限）]

- WCMサブパッケージは、イメージ16.1の以前のマイナー バージョンにのみインストールできます（たとえば、16.01.YY の WCM パッケージ（cat3k_caa-wcm.16.01.YY.SS A.pkg）をインストールできるのは、16.01.01 ～ 16.01.YY のスーパー パッケージ（cat3k_caa-universalk9.16.01.[01-to-YY].SSA.bin）です）。
- アップグレードしたら、スイッチを再起動する必要があります。

WCM サブパッケージのインストール

手順

ステップ 1 コントローラの WCM パッケージをアップグレードします。

request platform software package install switch all file flash: wcm_sub_package.pkg auto-copy

ステップ 2 （任意）APイメージをダウンロードしてインストールします。この手順では、APを新しいイメージで事前にダウンロードおよびプログラミングすることで、ネットワークのダウンタイムを減少させます。そうしないと、コントローラがリロードしたとき、コントローラと AP 間のバージョンに不一致が発生し、その AP は新しい AP イメージを使用して自身のアップグレードを開始するため、ネットワークのダウンタイムがさらに長くなる可能性があります。

（注） ダウンロードおよびインストール後に、CLI が AP に達したことを確認するために 30 秒間待機します。

a) 接続されているすべての AP に新しいイメージをプッシュします。
ap image predownload

b) ダウンロードの経過表示をモニタします。
show ap image

c) すべての AP のブート変数を新しいイメージを指すように指定します。
ap image swap

d) AP をリセットします。
ap image reset

ステップ 3 コントローラをリロードします。リロード後、新しい WCM パッケージのコントローラがリロードし、新しい AP イメージの AP がリロードすると、アップグレードしたコントローラに接続を開始します。
reload

デバイスセットアップ設定の機能履歴と情報

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 127 章

自律ネットワーキングの設定

- 自律型ネットワーキング （2823 ページ）

自律型ネットワーキング

自律型ネットワーキングでは、自己管理のコンセプトを導入し、ネットワーク デバイスをインテリジェントに機能させることにより、ネットワーク オペレータのネットワーク管理を簡素化します。

自律型ネットワーキングの前提条件

- 自律型ネットワーキング インフラストラクチャ機能は、イーサネット ポートと IPv6 アドレスのみをサポートしています。
- 隣接関係検出（AD）メッセージを交換するために、すべてのインターフェイスがデフォルトで稼働状態になります（デバイス内にスタートアップ コンフィギュレーションがない場合）。
- 自律型コントロール プレーンは、Autonomic Networking Infrastructure をサポートしている 2 台の隣接デバイスの間で、自動的に構築されます。両方のデバイスのイーサネット インターフェイスが稼働状態である必要があります。また、デバイスは未設定（新規ロールアウト）であるか、自律型ネットワーキングが明示的に設定されている必要があります。
- 非自律的なレイヤ 2 クラウド（メトロイーサネット サービスなど）が介在する場合にも、自律型コントロール プレーンが 2 台の隣接デバイスの間で自動的に構築されます。これは、自律型デバイス上のチャネル検出プロトコル（CD）によって実現されています。このプロトコルは、動作している VLAN カプセル化をプローブします。
- 介在する非自律的な L3 デバイスにわたり ACP を構築するには、自律型デバイスの間にトンネルを明示的に設定し、このトンネルで自律型隣接関係検出をイネーブルにする必要があります。
- Autonomic Networking Infrastructure 機能の動作には、自律型レジストラ（一般的にレジストラと呼ばれます）が必要です。自律型ドメインに新しいデバイスを登録するには、ネットワーク内で少なくとも 1 台のデバイスがレジストラとして設定されている必要があります。すべての必要なデバイスがすでに自律型ドメインに登録されているネットワークにおいては、レジストラは不要です。

- 各レジストラは、1 つの自律型ドメインのみをサポートします。レジストラが必要になるのは、新しい自律型デバイスがドメインに参加する場合のみです。
- 自律型ドメインに登録するためにレジストラに接触するには、すべての新しいデバイスが、すでにドメインに登録されている少なくとも 1 台のデバイスに対して L2 到達可能性がある必要があります。L2 到達可能性がない場合、ユーザはデバイス間にトンネルを設定し、デバイス上に自律型隣接関係検出を設定する必要があります。
- デバイスを登録できるのは、1 つの自律型ドメインのみです。異なるドメインに登録されている 2 台のデバイスの間では、自律型コントロール プレーンは構築されません。
- 自律型インテントはレジストラにのみ設定でき、そこから、ドメイン内のすべてのデバイスに伝達されます。
- ゼロ タッチ ブートストラップを実行するには、startup-config ファイルがなく、config-register がデフォルト（0x2102）のままである必要があります。

自律型ネットワーキングの制約事項

- 自律型ネットワーキングでは、固有デバイス識別子（UDI）ベースでのみデバイスをサポートします。
- 自律型ネットワーキングとゼロ タッチ プロビジョニング（ZTP）は、異なるゼロ タッチ ソリューションです。自律型ネットワーキングと ZTP は、同時にテストまたは使用しないことを推奨します。
- 自律型ネットワーク内のすべてのデバイスは、隣接して自律している必要があります。継続性がない場合、非自律型ネットワーク経由でトンネルを設定するために手動設定が必要です。
- Cisco IOS XE Denali 16.3.1 リリースでは、Cisco Catalyst 3850 および Cisco Catalyst 3650 スイッチは、タグなしのプローブとチャネルのみサポートします。
- Cisco IOS XE Denali 16.3.x リリースを実行しているデバイスは、XE 3.18 or 15.6(01)T より前のリリースを実行しているデバイスと互換性がありません。これらのデバイス間の相互作用を促進するには、自律型隣接関係ディスカバリをインターフェイスに設定する必要があります。
- 自律型ネットワーキングを有効にしている場合は、ipv6 ユニキャスト ルーティングを手動で無効にしてはいけません。
- 自律型レジストラ機能は、Cisco Catalyst 3850 および Cisco Catalyst 3650 スイッチでサポートされていません。

自律型ネットワーキングに関する情報

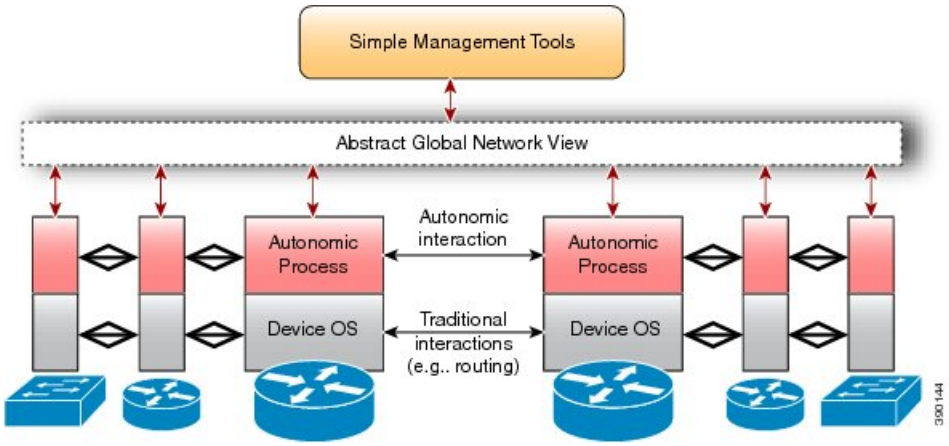
自律型ネットワーキングの概要

自律型ネットワーキングの目的は、自己管理ネットワークの構築によってインターネットや他のネットワークの急速な複雑化を克服し、さらなる成長を可能にすることです。自律的な自己

管理システムでは、ネットワーク管理が新たな役割を担うようになります。つまり、管理者は個別のネットワーク要素を直接制御する代わりに、自己管理プロセスの指針となるネットワーク全体のポリシーやルールを定義できます。

次の図は、自律型ネットワークのアーキテクチャの概要を示しています。

図 *143*：自律型ネットワークのアーキテクチャの概要



自律型ネットワーキングは、従来のオペレーティング システム上で実行される独立したソフトウェア エンティティによって制御されます。従来のオペレーティング システムには、IP や Open Shortest Path First（OSPF）などのネットワーキング コンポーネントが含まれます。従来のネットワーキング コンポーネントは変更を受けず、自律型プロセスの存在を認識しません。自律型コンポーネントは、従来のネットワーキング コンポーネントが備える通常のインターフェイスを使用して、ネットワーク内のさまざまなデバイスとやり取りします。自律型コンポーネントは安全な方法で連携し、デバイスのインテリジェンスを向上させます。これにより、自律型ネットワーク内のデバイスは、自らを自動的に設定、管理、保護、修復できるようになり、オペレータの介入が最小限に抑えられます。また、運用が安全に統合され、オペレータがネットワークを抽象化されたシンプルな形で確認できます。

Autonomic Networking Infrastructure

Autonomic Networking Infrastructure 機能によって、あらゆる種類のプレステージングの必要性がなくなり、ネットワーク ブートストラップ機能が簡素化されます。これにより、デバイスをドメインに安全に参加させ、その後でデバイスを設定できます。Autonomic Networking Infrastructure 機能の目的は、新しい未設定のデバイスにオペレータやネットワーク管理システムが安全に到達できるようにすることです。これは、次の手順で実現されます。

1. 1 台のデバイスがレジストラとして定義および設定されます。レジストラは、自律型ドメインにおける最初のデバイスです。
2. ネットワーク管理者が、ネットワークに追加するデバイスの適切なデバイス識別子のリストを収集します。このリストにより、自律型ドメインに追加されるデバイスを制御します。デバイスは固有のデバイス識別子（UDI）で識別されます。リストは単純なテキストファイルとして編集され、1 行に 1 つの UDI が記載されます。この手順は必須ではありません。ホワイトリストがない場合は、すべてのデバイスがドメインへの参加を許可されます。ホワイトリストはエンティティの許可リストで、特定の特権、サービス、モビリティ、

アクセス、認識が与えられます。ホワイトリスト化とは、アクセス権を付与することを意味します。

3. 既知のデバイスのホワイトリストが、設定の一部としてレジストラにアップロードされます。この手順は任意です。
4. レジストラ（またはすでに登録されているドメインデバイス）に直接接続された新しい自律型デバイスは、レジストラからドメイン証明書を自動的に受信します。
5. 自律型コントロールプレーンが自律型ドメインにわたって自動的に確立され、新しいデバイスに到達できるようになります。

Autonomic Networking Infrastructure のメリットは次のとおりです。

- 自律型ネイバーへの到達方法を検出することで、レイヤ2トポロジおよび接続を自律的に検出します。
- デバイス名とドメイン証明書を使用して、新しいデバイスを安全にゼロタッチで識別できます。
- 仮想の自律型コントロール プレーンにより、自律型ノード間の通信が可能になります。

自律的動作は、新しいデバイスではデフォルトでイネーブルになっています。既存のデバイスで自律的動作をイネーブルにするには、**autonomic** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

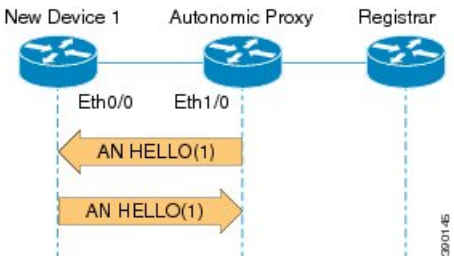
自律型ネットワーキングのコンポーネントは次のとおりです。

- **レジストラ**：特定の企業内におけるドメイン固有の登録局です。ドメイン内の新しいデバイスを検証し、それらにドメイン全体のクレデンシャルを提供し、ポリシーを決定します。ポリシー決定では、プリロードされたホワイトリストに基づいて、新しいデバイスが特定のドメインに参加できるかどうかなどを決定します。また、レジストラは、特定のドメインに参加しているデバイスやデバイスの詳細情報に関するデータベースを保持しています。
- **チャネル検出**：非自律型のレイヤ2ネットワークにわたり、自律型ノード間の到達可能性を検出するために使用されます。
- **隣接関係検出**：自律型ネイバーを検出するために使用されます。隣接関係検出はレイヤ3で実行されます。また、確立済みのレイヤ3 Generic Routing Encapsulation（GRE）トンネルにわたり、自律型ネイバーを検出することも可能です。

新しいデバイスの自律型ネットワークへの参加

次の図は、新しいデバイスが自律型ネットワークに参加する方法を示しています。

図 *144*：新しいデバイスの自律型ネットワークへの参加



1. 新しいデバイスがネイバーに hello メッセージを送信します。ここでは、ネイバーは自律型ネットワーク ドメインの一部です。
2. hello メッセージには、新しいデバイスの固有のデバイス識別子（UDI）が含まれます。
3. 自律型デバイスはプロキシとして機能し、この自律型ネットワーク ドメインへの新しいデバイスの参加を許可します。自律型ネットワーク デバイスは、レイヤ 3 ネイバーに対して、ドメイン情報を使用して自らをアドバタイズします。
4. ネイバーから自律型ネットワークの hello メッセージを受信し、UDI 情報を検出すると、新しいデバイスは自律型レジストラで検証されます。
5. 新しいデバイスはすべてのネイバーに対して、helloメッセージ内でドメイン証明書をアドバタイズします。ネイバー情報は 10 秒ごとに交換されます。

（注） ネイバー情報が変化すると、エントリは削除され、ネイバー探索が再開されます。ドメイン証明書および UDI を扱うデバイスがない場合は、UDI が 10 秒間隔で交換されます。

自律型ネットワーキングのチャネル検出

自律型ネットワーキングがデバイスで有効になっている場合、チャネル検出はすべてのインターフェイスで自動的に発生します。自律型ネットワーキングは、設定不要でデフォルトによりデバイス上で有効になっていますが（新規デバイスおよびデバイスにAN機能があることを想定）、パッシブ状態になります。それらのデバイスが行えるのは、CD プローブを受信して応答することだけです。CDプローブはL2フレームであり、ドメイン証明書を持つデバイスまたはドメインにすでに登録されているデバイスのみが CD プローブを、起動中のすべてのイーサネット インターフェイスに送信できます。この結果として、ネイバーは動的に検出されます。新しく追加されたネイバーを徐々に検出できるように、プロービングは長期にわたって続行されます。

自律型ネットワーキングにおける隣接関係の検出

チャネルが確立されると、プロキシが新しいデバイスに ND Hello を送信します。このプロキシは、ドメイン内にすでに登録済みで、ドメインに参加する新しいデバイスのプロキシの役割を果たすことができます。新しいデバイスは、プロキシに AN Hello メッセージの応答を送り返します。Hello メッセージは、UDI（固有デバイス識別子）と呼ばれる新規デバイス用の ID で構成されます。AN Hello メッセージを新しいデバイスから受信し、UDI 情報を検出後、AN プロキシは ANR（自律型ネットワーキング レジストラ）に詳細を送信し、この新しいデバイスの検証を行います。

自律型ネットワーキングのサービス検出

自律型ネットワーキングでは、マルチキャスト ドメイン ネーム システム（mDNS）インフラストラクチャを使用して、自律型ネットワーキング ドメイン内のデバイスに必要なさまざまなサービスを検出します。mDNSインフラストラクチャを使用してネットワークが検出するサービスは、AAA サーバ、コンフィギュレーション サーバ、syslog サーバ、自律型ネットワーキング レジストラなどです。自律型ネットワーキングでは、ドメイン内のすべてのデバイスにつ

いて、mDNS アドバタイズメントをリッスンします。サービスをホストしているデバイスから、自律型ネットワーキングが mDNS アドバタイズメントを開始します。

自律型コントロール プレーン

ドメイン内の新しいデバイスは、ドメイン証明書を受信した際に、ネイバーとの hello メッセージでドメイン証明書を交換します。これにより、同一ドメインの 2 台の自律型デバイスの間に、自律型コントロールプレーンが作成されます。デバイスの各種の機能に応じて、さまざまなタイプの自律型コントロール プレーンを作成できます。自律型コントロール プレーンは、以下の方法で確立されます。

- ループバック インターフェイスの設定。
- ループバック インターフェイスへの IPv6 アドレスの動的な割り当て。
- 自律型 VPN ルーティングおよび転送（VRF）の設定。

自律型ネットワーキングの設定方法

レジストラの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**autonomic** 例： `Device# autonomic`	自律型ネットワーキングをイネーブルにします。
ステップ 4	**autonomic registrar** 例： `Device(config)# autonomic registrar`	デバイスをレジストラとしてイネーブルにして、レジストラ コンフィギュレーション モードを開始します。 （注） Cisco IOS XE Denali 16.3.1 では、自律型レジストラの機能は、Cisco Catalyst スイッチ 3850 と 3650 ではサポートされません。

	コマンドまたはアクション	目的
ステップ 5	**domain-id** *domain-name* 例： `Device(config-registrar)# domain-id abc.com`	レジストラに登録しているすべてのデバイスの共通グループを示します。
ステップ 6	**device-accept** *udi* 例： `Device(config-registrar)# device-accept PID:A901-12C-FT-D SN:CAT1902U88Y`	（オプション）自律型ドメインで承認する検疫済みデバイスの固有のデバイス識別子（UDI）を指定します。 （注） このコマンドは、レジストラの設定時には必要ではありません。これが必要になるのは、レジストラがイネーブルになった後で、以前に検疫されたデバイスを承認する場合のみです。
ステップ 7	**whitelist** *filename* 例： `Device(config-registrar)# whitelist flash:whitelist.txt`	（オプション）特定のドメイン内で承認するデバイスのリストを含んだファイルを、ローカルデバイス上から読み込めるようにします。 • このファイルでは、1 行に 1 つの UDI エントリを記載する必要があります。 （注） このコマンドを設定しない場合は、すべてのデバイスのドメインへの参加が承認されます。
ステップ 8	**no shut** 例： `Device(config-registrar)# no shut`	自律型レジストラをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-registrar)# exit`	レジストラ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

自律型ネットワーキング コンフィギュレーションの検証とモニタリング

手順

ステップ 1 enable

例：

```
Device> enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 show autonomic device

例：

```
Device# show autonomic device

        Status                          Enabled
        Type                            Autonomic Node
        UDI                             PID:WS-C3850-24U SN:FCW1934C05R
        Device ID                       0021.d8d4.2900-1
        Domain ID                       cisco.com
       Domain Certificate            (sub:) ou=cisco.com+serialNumber=PID:WS-C3850-24U-E
 SN:FOC1847X17A,cn=0021.d8d4.2900-1
        Certificate Serial Number       0F
        Device Address                  FDF6:DBA2:13B6:0:21:D8D4:2900:1
        Domain Cert is Valid
```

グローバルな詳細情報を含む、自律型デバイスの現在の状態を表示します。

ステップ 3 show autonomic neighbors [detail]

例：

```
Device# show autonomic neighbors detail

UDI: "PID:WS-C3850-24U-E SN:FOC1847X17A"

       Device ID                      0021.d8d4.2900-4
       Domain ID                      cisco.com
       Address                        FDF6:DBA2:13B6:0:21:D8D4:2900:4
       State                          Nbr inside the Domain
       Credential                     Domain Cert
       Credential Validation          Passed
       Last Validated Time            2016-06-10 06:07:23 UTC
       Certificate Expiry Date        2017-06-08 14:54:09 UTC
       Certificate Expire Countdown   31394668 (secs)
       Number of Links connected      1

        Link:
            Local Interface:          ANI2
            Remote Interface:         ANI2
            IP Address:               FE80::D66D:50FF:FEAD:2C83
            Uptime(Discovered Time):  00:30:35 ( 2016-06-10 05:39:06 UTC)
            Last Refreshed time:      0 seconds ago
```

検出したネイバーに関する情報を表示します。

ステップ 4 show autonomic control-plane [detail]

例：

```
Device# show autonomic control-plane

VRF Name                        cisco_autonomic
Device Address                  FD08:2EEF:C2EE:0:E865:493B:ACFB:7
RPL                            floating-node, Dag-id = FD08:2EEF:C2EE:0:E865:493B:ACFB:5

Neighbor                           ACP            Channel ACP Security
-------------------------------------------------------------------------------
PID:WS-C3850-24U SN:FCW1934D05Z   Tunnel100002   DIKE
```

```
Device# show autonomic control-plane detail

VRF Name                        cisco_autonomic
Device Address                  FD08:2EEF:C2EE:0:E865:493B:ACFB:7
RPL                            grounded-node, Dag-id = FD08:2EEF:C2EE:0:E865:493B:ACFB:1

Neighbor: PID:WS-C3850-24U SN:FCW1934D05Z
Uptime(Created Time): 00:12:16 ( 2016-07-15 05:38:53 UTC)
Supported ACP Channel: IPv6 GRE Tunnel
Negotiated ACP Channel: IPv6 GRE Tunnel
Tunnel Name Tunnel100000
Tunnel Source Interface ANI1
Tunnel Source FE80::5AAC:78FF:FE09:F383
Tunnel Destination FE80::3A20:56FF:FEF3:7158
Supported ACP Security: IPSec, DIKE
Negotiated ACP Security: DIKE
```

自律型コントロール プレーンに関する情報を表示します。

ステップ 5 **show autonomic l2-channels [detail]**

例：

```
Device# show autonomic l2-channels

AN L2 Channel Discovery Info :
Nbr UDI                          Encap    Our Intf   State   Retry
-------------------------------------------------------------------------------
PID:WS-C3850-24U SN:FCW1934D05Z  4018    Gi1/0/3      Active  1
```

```
Device# show autonomic l2-channels detail

AN L2 Channel Discovery Info :
-------------------------------------------------------------------------------
Nbr UDI                : PID:WS-C3850-24U SN:FCW1934D05Z
ANI Intf               : ANI1
Encap                  : 0
Nbr Intf               : GigabitEthernet1/0/3
Our Intf               : GigabitEthernet1/0/3
Keepalives Missed      : 0
Channel Status         : Active
```

チャネル検出の結果を表示します

ステップ 6 **show autonomic interfaces**

例：

```
Device# show autonomic interfaces
```

```
Interface                 Channel Disc    AD Enabled      Intf Type
-------------------------------------------------------------------------------
GigabitEthernet0/0        None       No              L2 untagged If
GigabitEthernet1/0/1      None       No              L2 untagged If
GigabitEthernet1/0/2      None       No              L2 untagged If
GigabitEthernet1/0/3      Probing    No              L2 untagged If
GigabitEthernet1/0/4      None       No              L2 untagged If
GigabitEthernet1/0/5      None       No              L2 untagged If
GigabitEthernet1/0/6      None       No              L2 untagged If
GigabitEthernet1/0/7      None       No              L2 untagged If
GigabitEthernet1/0/8      None       No              L2 untagged If
GigabitEthernet1/0/9      None       No              L2 untagged If
GigabitEthernet1/0/10     None       No              L2 untagged If
GigabitEthernet1/0/11     None       No              L2 untagged If
GigabitEthernet1/0/12     None       No              L2 untagged If
GigabitEthernet1/0/13     None       No              L2 untagged If
GigabitEthernet1/0/14     None       No              L2 untagged If
GigabitEthernet1/0/15     None       No              L2 untagged If
GigabitEthernet1/0/16     None       No              L2 untagged If
GigabitEthernet1/0/17     None       No              L2 untagged If
GigabitEthernet1/0/18     None       No              L2 untagged If
GigabitEthernet1/0/19     None       No              L2 untagged If
GigabitEthernet1/0/20     None       No              L2 untagged If
GigabitEthernet1/0/21     None       No              L2 untagged If
GigabitEthernet1/0/22     None       No              L2 untagged If
GigabitEthernet1/0/23     None       No              L2 untagged If
GigabitEthernet1/0/24     None       No              L2 untagged If
GigabitEthernet1/1/1      None       No              L2 untagged If
GigabitEthernet1/1/2      None       No              L2 untagged If
TenGigabitEthernet1/1/3   None       No              L2 untagged If
TenGigabitEthernet1/1/4   None       No              L2 untagged If
Vlan1                     None       No              Virtual If
ANI1                      None       Yes             Virtual If
Loopback100000            None       No              Virtual If
Tunnel100002              None       No              Virtual If
```

自律型ドメイン内のインターフェイスに関する情報を表示します。

ステップ 7 **debug autonomic** {**Bootstrap** | **Channel-Discovery** | **Infra** | **Intent** | **Neighbor-Discovery** | **Registrar** | **Services** } {**aaa** | **all** | **ntp** | **events** | **packets**} {**info** | **moderate** | **severe**}

自律型ネットワークのデバッグをイネーブルにします。

ステップ 8 **clear autonomic** {**device** | **neighbor** *UDI* | **registrar accepted-device** *device UDI*}

自律型ネットワークに関する情報をクリアまたはリセットします。

- **clear autonomic device** コマンドは、デバイス固有の AN 情報のすべてをクリアまたはリセットします（ブートストラップ プロセスで取得した情報を含みます）。
- **clear autonomic neighbor** コマンドは、ネイバー探索で取得したネイバーに関する情報をクリアします。ネイバーを指定しない場合は、ネイバー データベース全体がクリアされます。
- **clear autonomic registrar accepted-device** コマンドを使用すると、レジストラに登録された各デバイスに保存されている公開キーが消去されます。

第 128 章

Right-To-Use ライセンスの設定

- 機能情報の確認 （2833 ページ）
- RTU ライセンスの設定に関する制約事項 （2833 ページ）
- RTU ライセンスの設定に関する情報 （2834 ページ）
- RTU ライセンスの設定方法 （2838 ページ）
- RTU ライセンスのモニタリングおよびメンテナンス （2842 ページ）
- RTU ライセンスの設定例 （2843 ページ）
- RTU ライセンスに関する追加情報 （2848 ページ）
- RTU ライセンスの機能履歴と情報 （2849 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

RTU ライセンスの設定に関する制約事項

次に、RTU ライセンスの設定および使用に関する制約事項を示します。

- AP-Count ライセンスは注文が可能で、スイッチ上で事前にアクティブ化できます。
- イメージ ベースのライセンスは、アップグレードできます。AP-Count ライセンスは非アクティブ化したり、スイッチとコントローラとの間で移動したりできます。

- 永久ライセンスをアクティブ化するには、新しいイメージレベルを設定した後にスイッチを再起動する必要があります。AP-Count ライセンスをアクティブ化するために再起動する必要はありません。
- 期限切れのイメージベースの評価ライセンスは、再起動後は再アクティブ化できません。
- スイッチ スタックのスタック メンバは同一のライセンス レベルを実行する必要があります。
- スイッチは、注文したイメージとともに事前にインストールされています。イメージを事前に注文していなかった場合、スイッチはデフォルトで LAN ベース イメージで起動します。
- 追加 AP-Count ライセンスは、工場出荷時にインストールされます。

関連トピック

イメージ ベース ライセンスのアクティブ化 （2838 ページ）
例：RTU イメージ ベースのライセンスのアクティブ化 （2843 ページ）

RTU ライセンスの設定に関する情報

Right-To-Use ライセンス

Right-To-Use（RTU）ライセンスでは、特定のライセンス タイプおよびレベルを注文してアクティブ化し、ライセンスの使用状況をスイッチで管理することができます。注文できるライセンスは次のとおりです。

- 永久ライセンス：特定の機能を備え、有効期限のないライセンスを購入できます。
- 評価ライセンス：スイッチに事前にインストールされています。使用有効期間は 90 日です。

永久ライセンスまたは評価ライセンスをアクティブ化するには、エンドユーザ ライセンス契約（EULA）を承認する必要があります。評価ライセンスの場合は、90 日の期限が切れる前に永久ライセンスを購入するか、ライセンスを非アクティブ化するように通知されます。

永久ライセンスは 1 つのデバイスから別のデバイスに移動できます。ライセンスをアクティブ化するには、スイッチを再起動する必要があります。

評価ライセンスはスイッチのマニュファクチャリング イメージであり、別のスイッチに移動できません。このタイプのライセンスは、再起動後は再アクティブ化できません。

関連トピック

イメージ ベース ライセンスのアクティブ化 （2838 ページ）
例：RTU イメージ ベースのライセンスのアクティブ化 （2843 ページ）

Right-To-Use イメージ ベースのライセンス

Right-To-Use イメージ ライセンスは、特定のイメージ ベースに基づき、次の一連の機能をサポートします。

- LAN Base：レイヤ 2 の機能。
- IP Base：レイヤ 2 およびレイヤ 3 の機能。
- IP Services：レイヤ 2、レイヤ 3、IPv6 の機能（スイッチにのみ適用され、コントローラには適用されません）。

デフォルトのイメージ ベースのライセンスは LAN Base です。

Right-To-Use ライセンスの状態

特定のライセンス タイプとレベルを設定した後は、ライセンスの状態をモニタすることでライセンスを管理できます。

表 *181 : RTU* ライセンスの状態

License State	説明
Active, In Use	EULA が承認され、デバイス再起動後にライセンスが使用されています。
Active, Not In Use	EULA が承認され、ライセンスが有効になった時点で、スイッチを使用する準備が整っています。
非アクティブ化	EULA が承認されませんでした。

イメージ ベースのライセンスの状態をモニタする場合のガイドラインは次のとおりです。

- 購入した永久ライセンスは、スイッチの再起動後のみに *Active, In Use* 状態に設定されます。
- 複数のライセンスを購入した場合は、再起動すると最も高い機能セットのライセンスがアクティブ化されます。たとえば、IP Services ライセンスがアクティブ化され、LAN Base ライセンスはアクティブ化されません。
- スイッチの再起動後も、購入済みの残りのライセンスは **Active, Not In Use** 状態のままです。

（注） AP-Count ライセンスの場合に状態を「Active, In Use」に変更するには、まず、評価 AP-Count ライセンスが非アクティブ化されているようにする必要があります。

スイッチ スタックのライセンスのアクティブ化

Right-To-Use ライセンスはスイッチ スタックでサポートされます。スイッチは、、StackWise-480 ポートを介して接続された最大 9 個のスタッキング対応スイッチのセットです。接続できるのはスタック内の 1 つのタイプのスイッチのみです。スタック内の 1 個のスイッチはアクティブなスイッチとして識別され、残りのスイッチはスタンバイ スイッチになります。アクティブなスイッチは、RTU ライセンスを使用し、アクティブなコンソールからアクティブ化されたスイッチです。スタック内のスタンバイ スイッチのライセンス レベルは、同時にアクティブ化できます。

（注） スイッチ スタックに、混在したスイッチ プラットフォームと混在したライセンス レベルを含めることはできません。スタック内のスイッチは、同じプラットフォームと同じライセンスである必要があります。

モビリティ コントローラ モード

AP-Count ライセンスは、スイッチがモビリティ コントローラ モードになっている場合にのみ使用します。MC は、AP-CountAP-Count ライセンスをトラッキングするゲートキーパであり、アクセス ポイント参加を許可または拒否できます。

AP-Count ライセンスはを、CLI で設定可能なモビリティ コントローラ モードで実行して管理します。

関連トピック

モビリティ モードの変更 （2841 ページ）

Right-To-Use AP-Count ライセンス

Right-To-Use（RTU）ライセンスにより、特定のライセンス タイプを注文およびアクティブ化してライセンスの使用状況をで管理することができます。

特定の数の追加アクセス ポイント数ライセンスとともにデバイスを注文できますが、注文するライセンスの総数は 50 を超えることはできません。デバイスを受け取った後でも追加アクセス ポイント数のライセンスを注文できます。

たとえば、 50 の新しい追加ライセンスを注文した場合、それらの注文した追加ライセンスのみをデバイスに追加できます。ライセンスの追加単位は 1 です。ただし、デバイスに追加するライセンスの総数が 50 を超えないようにします。

アクセス ポイント数ライセンスを管理し、CLI で現在使用中のアクセス ポイント数を確認できるようにスイッチを設定できます。

以下では、2 種類のアクセス ポイント ライセンスについて説明します。

1. アクセス ポイントの永久ライセンス

- 追加アクセス ポイント数ライセンス：後でデバイスのキャパシティを増やすために追加ライセンスを購入できます。追加アクセス ポイント数ライセンスをあるデバイスから別のコントローラに換えることができます。

2. アクセス ポイントの評価ライセンス
   - ライセンスを購入する前に、評価ライセンスをアクティブ化して、多くのアクセス ポイントを評価できます。
   - 評価できるアクセス ポイントの最大数は 50 です。
   - アクセス ポイント ライセンスを使用した評価期間は 90 日です。
   - CLI から評価ライセンスのアクティブ化と非アクティブ化が行えます。

関連トピック

ap-count ライセンスのアクティブ化 （2839 ページ）
アップグレード ライセンスまたはキャパシティ Adder ライセンスの取得 （2840 ページ）
ライセンスの再ホスト （2841 ページ）

Right-to-Use AP-Count 評価ライセンス

アクセス ポイント数の多いライセンスにアップグレードする場合は、永久バージョンのライセンスにアップグレードする前に評価ライセンスを試すことができます。たとえば、使用している永久ライセンスのアクセス ポイント数が 50 の場合に、アクセス ポイント数が 100 の評価ライセンスを 90 日間試用できます。

評価ライセンスがアクティブ化されると、AP-Count 永久ライセンスは無視されます。最大でサポート対象の1,000 のアクセス ポイントのライセンスを 90 日間利用できます。

操作の中断を避けるために、デバイスは、評価ライセンスの有効期限が切れてもライセンスを変更しません。期限切れ警告メッセージは有効期限日の 5 日前から毎日表示されます。90 日後に、評価ライセンスは期限切れになり、警告メッセージが表示されます。評価ライセンスをディセーブルにし、永久ライセンスを購入する必要があります。

評価ライセンスの期限が切れた後にデバイスを再起動すると、ライセンスのデフォルトが永久ライセンスに設定されます。

関連トピック

ap-count ライセンスのアクティブ化 （2839 ページ）
アップグレード ライセンスまたはキャパシティ Adder ライセンスの取得 （2840 ページ）
ライセンスの再ホスト （2841 ページ）

Right-To-Use Adder AP-Count 再ホスト ライセンス

あるデバイスのライセンスを無効にして、別のデバイスにインストールする操作を再ホストと呼びます。デバイスの目的を変更するために、ライセンスのリホストが必要になる場合があり

ます。たとえば、Office Extend または屋内アクセス ポイントを別のデバイスに移動する場合、あるデバイスから別のコントローラに基本ライセンスを移行できます。

ライセンスを再ホストするには、あるデバイスの Adder AP-Count ライセンスを非アクティブ化し、別のデバイスで同じライセンスをアクティブ化します。

評価ライセンスを再ホストすることはできません。

RTU ライセンスの設定方法

イメージ ベース ライセンスのアクティブ化

手順

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use activate** {**ipbase** | **ipservices** | **lanbase**} {**all** | **evaluation all** } [**slot** *slot-number*] [**acceptEULA**] 例： `Device# license right-to-use activate ipservices all acceptEULA`	イメージ ベース ライセンスのタイプをアクティブ化します。すべてのスイッチ上でアクティブ化され、EULA への同意が含まれることもあります。 （注） EULA に同意しない場合は、変更した設定はリロード後に反映されません。デフォルトのライセンス（または非アクティブ化されたライセンス）がリロード後にアクティブになります。

ステップ 2	**reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]
	例：
	`Device# reload slot 1`
	`Proceed with reload? [confirm] y`
		特定のスタック メンバをリロードし、RTU 追加 AP-Count ライセンスのアクティブ化プロセスを完了します。
		（注） これまでに同意していなかった場合は、リロード後に同意を促すメッセージが表示されます。

ステップ 3	**show license right-to-use usage** [**slot** *slot-number*]
	例：
	`Device# show license right-to-use usage`
	
	`Slot#  License Name  Type`
		詳細な使用状況に関する情報を表示します。

	コマンドまたはアクション	目的
	usage-duration(y:m:d) In-Use EULA ---------- 1 ipservices permanent 0 :10 :0 yes yes 1 ipbase permanent 0 :0 :0 no no 1 ipbase evaluation 0 :0 :0 no no 1 lanbase permanent 0 :0 :7 no yes 1 apcount evaluation 0 :0 :0 no no 1 apcount base 0 :0 :0 no no 1 apcount adder 0 :0 :0 no no Switch#	

関連トピック

RTU ライセンスの設定に関する制約事項 （2833 ページ）
Right-To-Use ライセンス （2834 ページ）
RTU ライセンスのモニタリングおよびメンテナンス （2842 ページ）
例：RTU イメージ ベースのライセンスのアクティブ化 （2843 ページ）

ap-count ライセンスのアクティブ化

手順

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use activate**{**apcount** *ap-number* **slot** *slot-num*} | **evaluation**} [**acceptEULA**] 例： Device# **license right to use activate apcount 5 slot 1 acceptEULA**	1 つ以上の追加 AP-Count ライセンスをアクティブ化し、ただちに EULA に同意します。
ステップ 2	**show license right-to-use usage** [**slot** *slot-number*] 例： Device# **show license right-to-use usage** Slot# License Name Type usage-duration(y:m:d) In-Use EULA ----------	詳細な使用状況に関する情報を表示します。

	コマンドまたはアクション	目的

	`1 ipservices permanent 0 :3 :29 yes yes`
	`1 ipservices evaluation 0 :0 :0 no no`
	`1 ipbase permanent 0 :0 :0 no no`
	`1 ipbase evaluation 0 :0 :0 no no`
	`1 lanbase permanent 0 :0 :0 no no`
	`1 apcount evaluation 0 :3 :11 no no`
	`1 apcount base 0 :0 :0 no yes`
	`1 apcount adder 0 :0 :17 yes yes`
	
	`Switch#`	

関連トピック

RTU ライセンスのモニタリングおよびメンテナンス （2842 ページ）
Right-To-Use AP-Count ライセンス （2836 ページ）
Right-to-Use AP-Count 評価ライセンス （2837 ページ）

アップグレード ライセンスまたはキャパシティ Adder ライセンスの取得

キャパシティ Adder ライセンスを使用して、デバイスがサポートするアクセス ポイントの数を増やすことができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use** {**activate** | **deactivate**} **apcount** {*ap-number* | **evaluation** } **slot** *slot-num* [**acceptEULA**] 例： `Device# license right to use activate apcount 5 slot 2 acceptEULA`	1 つ以上の追加 AP-Count ライセンスをアクティブ化し、ただちに EULA に同意します。

関連トピック

Right-to-Use AP-Count 評価ライセンス （2837 ページ）
Right-To-Use AP-Count ライセンス （2836 ページ）

ライセンスの再ホスト

ライセンスを再ホストするには、1 つの デバイス のライセンスを非アクティブ化し、別の デバイス で同じライセンスをアクティブ化します。

手順

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use deactivate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**] 例： `Device# license right to use deactivate apcount 1 slot 1 acceptEULA`	1 つのデバイスのライセンスを非アクティブ化します。
ステップ 2	**license right-to-use activate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**] 例： `Device# license right to use activate apcount 2 slot 2 acceptEULA`	別のデバイスのライセンスを非アクティブ化します。

関連トピック

Right-To-Use AP-Count ライセンス （2836 ページ）
Right-to-Use AP-Count 評価ライセンス （2837 ページ）

モビリティ モードの変更

手順

	コマンドまたはアクション	目的

ステップ 1	**wireless mobility controller**
	例：
	`Device(config)# wireless mobility controller`
	`%`
	`Mobility role changed to Mobility Controller.`
	`Please save config and reboot the whole stack.`
		モビリティ エージェント モードのスイッチをモビリティ コントローラ モードに変更します。

ステップ 2	**write memory**
	例：
	`Device# write memory`
	
	`Building configuration...`
	`Compressed configuration from 13870`	

	コマンドまたはアクション	目的
	bytes to 5390 bytes[OK] Device#	
ステップ 3	**reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**] 例： Device# **reload slot 3** Proceed with reload? [confirm] **y**	
ステップ 4	**no wireless mobility controller** 例： Device(config)# **no wireless mobility controller** % Mobility role changed to Mobility Agent. Please save config and reboot the whole stack. Switch(config)#	モビリティ コントローラ モードのスイッチをモビリティ エージェント モードに変更します。
ステップ 5	**write memory** 例： Device# **write memory** Building configuration... Compressed configuration from 13870 bytes to 5390 bytes[OK] Device#	
ステップ 6	**reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**] 例： Device# **reload slot 3** Proceed with reload? [confirm] **y**	

関連トピック

モビリティ コントローラ モード （2836 ページ）

RTU ライセンスのモニタリングおよびメンテナンス

コマンド	目的
show license right-to-use default	デフォルトのライセンス情報を表示します。

コマンド	目的
show license right-to-use detail	スイッチ スタック内のすべてのライセンスの詳細情報を表示します。
show license right-to-use eula {adder | evaluation | permanent}	エンドユーザ ライセンス契約を表示します。
show license right-to-use mismatch	一致しないライセンス情報を表示します。
show license right-to-use slot *slot-number*	スイッチ スタック内の特定のスロットのライセンス情報を表示します。
show license right-to-use summary	スイッチ スタック全体のライセンス情報の要約を表示します。
show license right-to-use usage [**slot** *slot-number*]	スイッチ スタック内のすべてのライセンスの使用状況に関する詳細情報を表示します。
show switch	ライセンスのステータスを含むスイッチスタック内のすべてのメンバの詳細情報を表示します。

関連トピック

イメージ ベース ライセンスのアクティブ化 （2838 ページ）
例：RTU イメージ ベースのライセンスのアクティブ化 （2843 ページ）
ap-count ライセンスのアクティブ化 （2839 ページ）

RTU ライセンスの設定例

例：RTU イメージ ベースのライセンスのアクティブ化

次に、IP Services イメージ ライセンスをアクティブ化し、特定のスロットの EULA を受け入れる例を示します。

```
Switch# license right-to-use activate ipservices slot 1 acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

次に、評価用ライセンスをアクティブ化する例を示します。

```
Switch# license right-to-use activate ipservices evaluation acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

関連トピック

イメージ ベース ライセンスのアクティブ化 （2838 ページ）

RTU ライセンスの設定に関する制約事項 （2833 ページ）
Right-To-Use ライセンス （2834 ページ）
RTU ライセンスのモニタリングおよびメンテナンス （2842 ページ）

例：RTU ライセンス情報の表示

次に、スイッチ スタックのアクティブ スイッチからの統合 RTU ライセンス情報の例を示します。スタック内のすべてのメンバのライセンス レベルは同じです。評価 AP-Count ライセンスをアクティブ化すると、追加 AP-Count ライセンスは無視されます。Ap-Count ライセンスの最大数は、評価がイネーブルの場合に使用できます。

```
Switch# show license right-to-use summary

 License Name    Type           Count   Period left
-------------------------------------------------------
  ipservices     permanent        10      Lifetime
  apcount        evaluation       40        90

-------------------------------------------------------

License Level In Use: ipservices
License Level on Reboot: ipbase
Evaluation AP-Count: Enabled
Total AP Count Licenses: 50
AP Count Licenses In-use: 10
AP Count Licenses Remaining: 40
```

次に、永久ライセンスと追加ライセンスのサマリーを示します。評価 AP-Count ライセンスはディセーブルで、スイッチ スタック内でアクティブ化された追加 AP-Count ライセンスの総数が示されています。使用中の AP-Count ライセンスは、それらのライセンスが接続されていることを意味します。

```
Switch# show license right-to-use summary

  License Name    Type          Count      Period left
-------------------------------------------------------------
  ipservices     permanent      N/A         Lifetime
  apcount        base           0
  apcount        adder          40          Lifetime

-------------------------------------------------------------

License Level In Use: ipservices
License Level on Reboot: ipservices eval
Evaluation AP-Count: Disabled
Total AP Count Licenses: 40
AP Count Licenses In-use: 10
AP Count Licenses Remaining: 30
```

次に、RTU のデフォルトのライセンスを示します。デフォルトのライセンスは事前にインストールされており、削除したり、移動したりできません。アクティブ化されているライセンスがない場合、スイッチは再起動後にデフォルトのライセンスを使用します。

```
Switch# show license right-to-use default

 Slot#    License Name    Type           Count
-----------------------------------------------------
 1        ipservices      permanent     N/A
 1        apcount         base          0
 1        apcount         adder         10

 Slot#    License Name    Type           Count
-----------------------------------------------------
 2        ipservices      permanent     N/A
 2        apcount         base          0
 2        apcount         adder         10

 Slot#    License Name    Type           Count
-----------------------------------------------------
 3        ipservices      permanent     N/A
 3        apcount         base          0
 3        apcount         adder         10
```

次に、コントローラの統合 RTU ライセンス情報の例を示します。評価 AP-Count ライセンスがアクティブ化されると、基本および追加の AP-Count ライセンスは無視されます。AP-Count ライセンスの最大数は、評価がイネーブルの場合に使用できます。

次に、RTU のデフォルトのライセンスを示します。デフォルトのライセンスは事前にインストールされており、削除したり、移動したりできません。アクティブ化されているライセンスがない場合、コントローラは再起動後にデフォルトのライセンスを使用します。

```
controller# show license right-to-use  default
Slot#    License Name    Type           Count
-----------------------------------------------------
  1        apcount         base          10
```

例：RTU ライセンスの詳細の表示

次に、スロット 1 の RTU ライセンスのすべての詳細情報の例を示します。

```
Switch# show license right-to-use detail slot 1

Index 1:  License Name: ipservices
           Period left: Lifetime
           License Type: permanent
           License State: Active, In use
           License Count: Non-Counted
           License Location: Slot 1
Index 2:  License Name: ipservices
           Period left: 90
           License Type: evaluation
           License State: Not Activated
           License Count: Non-Counted
           License Location: Slot 1
Index 3:  License Name: ipbase
           Period left: Lifetime
           License Type: permanent
           License State: Active, Not In use
           License Count: Non-Counted
           License Location: Slot 1
```

```
Index 4:  License Name: ipbase
           Period left: 90
           License Type: evaluation
           License State: Not Activated
           License Count: Non-Counted
           License Location: Slot 1
           License Location: Standby Switch 1
Index 5:  License Name: lanbase
           Period left: Lifetime
           License Type: permanent
           License State: Not Activated
           License Count: Non-Counted
           License Location: Slot 1
Index 6:  License Name: apcount
           Period left: 90
           License Type: evaluation
           License State: Active, In use
           License Count: 50
           License Location: Slot 1
Index 7:  License Name: apcount
           Period left: Lifetime
           License Type: base
           License State: Active, Not In use
           License Count: 0
           License Location: Slot 1
Index 8:  License Name: apcount
           Period left: Lifetime
           License Type: adder
           License State: Active, Not In use
           License Count: 10
           License Location: Slot 1
```

```
Controller# show license right-to-use detail slot 1
Index 6:  License Name: apcount
          Period left: Expired
          License Type: evaluation
          License State: Active, In use
          License Count: 1000
          License Location: Slot 1
Index 7:  License Name: apcount
          Period left: Lifetime
          License Type: base
          License State: Active, Not In use
          License Count: 0
          License Location: Slot 1
Index 8:  License Name: apcount
          Period left: Lifetime
          License Type: adder
          License State: Not Activated
          License Count: 0
          License Location: Slot 1
```

例：RTU ライセンスの不一致の表示

この例では、スタック内のスイッチのライセンス情報と、メンバ スイッチの不一致ステータスを示します。メンバ スイッチがアクティブ スイッチと一致している必要があります。

```
Switch# show switch

Switch/Stack Mac Address : 6400.f125.0c80
                                                    H/W   Current
Switch#   Role        Mac Address     Priority Version  State
-------------------------------------------------------------------------------
 1       Standby     6400.f125.1b00     1      0        Ready
*2       Active      6400.f125.0c80     1      V01      Ready
 3       Member      6400.f125.1780     1      0        Lic-Mismatch
```

（注） ライセンスの不一致を解決するには、まず、RTU ライセンスのサマリーを確認します。

```
Switch# show switch right-to-use summary
```

次に、アクティブ スイッチと同じライセンス レベルとなるように、一致していないスイッチのライセンス レベルを変更します。この例では、アクティブ スイッチと一致するように IP Base ライセンスをメンバ スイッチに対してアクティブ化したことを示します。

```
Switch# license right-to-use activate ipbase slot 1 acceptEULA
```

例：RTU ライセンス使用状況の表示

次に、スイッチ スタックの詳細なライセンス使用状況の例を示します。スロット 1 の IP Services ライセンスは永久ライセンスで、1 日使用しています。スロット 2 の AP-Count ライセンスは、評価に使用できる状態です。EULA に同意しており、使用中の状態であることが示されていますが、再起動後に評価ライセンスは非アクティブ化されます。

```
Switch# show license right-to-use usage

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-----------------------------------------------------------------------------------------

 1      ipservices     permanent      0 :0 :1            yes     yes
 1      ipservices     evaluation     0 :0 :0            no      no
 1      ipbase         permanent      0 :0 :0            no      yes
 1      ipbase         evaluation     0 :0 :0            no      no
 1      lanbase        permanent      0 :0 :0            no      no
 1      apcount        evaluation     0 :0 :0            yes     yes
 1      apcount        base           0 :0 :0            no      yes
 1      apcount        adder          0 :0 :0            no      yes
```

```
 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-----------------------------------------------------------------------------------------

 2      ipservices     permanent       0 :0 :1           yes     no
 2      ipservices     evaluation      0 :0 :0           no      yes
 2      ipbase         permanent       0 :0 :0           no      yes
 2      ipbase         evaluation      0 :0 :0           no      no
 2      lanbase        permanent       0 :0 :0           no      no
 2      apcount        evaluation      0 :0 :0           yes     yes
 2      apcount        base            0 :0 :0           no      yes
 2      apcount        adder           0 :0 :0           no      no

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-----------------------------------------------------------------------------------------

 3      ipservices     permanent       0 :0 :1           yes     yes
 3      ipservices     evaluation      0 :0 :0           no      no
 3      ipbase         permanent       0 :0 :0           no      no
 3      ipbase         evaluation      0 :0 :0           no      no
 3      lanbase        permanent       0 :0 :0           no      no
 3      apcount        evaluation      0 :0 :0           yes     yes
 3      apcount        base            0 :0 :0           no      yes
 3      apcount        adder           0 :0 :0           no      no
```

次に、コントローラの詳細なライセンス使用状況の例を示します。

```
Controller# show license right-to-use usage
Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-----------------------------------------------------------------------
1      apcount        evaluation   0 :3 :3                yes   yes
1      apcount        base         0 :0 :0                no    yes
1      apcount        adder        0 :0 :0                no    no
```

RTU ライセンスに関する追加情報

関連資料

関連項目	マニュアル タイトル
RTU コマンド	『*System Management Command Reference (Catalyst 3850 Switches)*』
RTU AP イメージ プレロード機能	*System Management Configuration Guide*（*Cisco WLC 5700 Series*）

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

RTU ライセンスの機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

第 129 章

管理者のユーザ名とパスワードの設定

- 機能情報の確認 （2851 ページ）
- 管理者のユーザ名とパスワードの設定について （2851 ページ）
- 管理者のユーザ名とパスワードの設定 （2852 ページ）
- 例：管理者のユーザ名とパスワードの設定 （2854 ページ）
- 管理者のユーザ名とパスワードに関する追加情報 （2855 ページ）
- 管理者のユーザ名とパスワードの設定の機能履歴と情報 （2856 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

管理者のユーザ名とパスワードの設定について

管理者のユーザ名とパスワードを設定しておくと、権限のないユーザによるデバイスの設定変更や設定情報の表示を防ぐことができます。この項では、初期設定とパスワードリカバリの手順を説明します。

デバイスに関連付けられた一つ以上のアクセス ポイントを管理および設定する管理者のユーザ名とパスワードを設定することもできます。

強力なパスワード

管理者ユーザがアクセス ポイントを管理するため、ASCII キーによる暗号化パスワードなどの強力な管理者パスワードを設定できます。

強力なパスワードを作成する場合は、次のガイドラインに従ってください。

- 次のカテゴリ（小文字、大文字、数字、特殊文字）のうち、少なくとも3つが必要です。

（注） GUI のログインでは、ユーザ名とパスワードでの特殊文字の使用はサポートされません。

- 新しいパスワードは、関連付けられているユーザ名と同じにしたり、ユーザ名を反転させたりすることはできません。
- パスワードの文字を 4 回以上連続して繰り返すことはできません。
- パスワードに **cisco**、**ocsic**、**admin**、**nimda** を使用することはできません。また、これらの文字のいくつかを大文字にしたり、i を「1」、「|」、または「!」に、「o」を「0」に、または「s」を「$」に置き換えたりすることもできません。
- ユーザ名およびパスワードで許容される最大文字数は 32 文字です。

暗号化パスワード

パスワードには 3 種類のキーを設定できます。

- ランダムに生成されたキー：このキーはランダムに生成され、最も安全なオプションです。1 台のシステムから別のシステムへコンフィギュレーションファイルをエクスポートするには、キーもエクスポートする必要があります。
- 静的キー：最も単純なオプションは固定（静的）暗号キーを使用することです。固定キーを使用すれば、キー管理は必要ありませんが、キーが何らかの方法で検出されると、データはそのキーの知識を持つ任意のユーザによって復号化できます。これは、セキュアなオプションではなく、CLI では難読化と呼ばれます。
- ユーザによって定義されたキー：ユーザ自身がキーを定義できます。1 台のシステムから別のシステムへコンフィギュレーションファイルをエクスポートするには、双方のシステムで同じキー設定する必要があります。

管理者のユーザ名とパスワードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless security strong-password** 例：	管理者ユーザのための強力なパスワードポリシーをイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config)# wireless security strong-password`	
ステップ 3	**username** *admin-username* **password {0** *unencrypted_password* | **7** *hidden_password*| *unencrypted_text*} 例： `Device(config)# username adminuser1 password 0 QZsek239@`	管理者のユーザ名とパスワードを指定します。 管理者は、デバイスを設定し、設定情報を表示できます。
ステップ 4	**username** *admin-username* **secret {0** *unencrypted_secret_text* | **4** *SHA256 encrypted_secret_text*| **5** *MD5 encrypted_secret_text*| **LINE}** 例： `Device(config)# username adminuser1 secret 0 QZsek239@`	管理者のシークレットを指定します。
ステップ 5	**ap mgmtuser username** *username* **password{0** *unencrypted password* | **8** *AES encrypted password*}**secret{0** *unencrypted password* | **8** *AES encrypted password*} 例： `Device(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!`	デバイスへ設定されたすべてのアクセスポイントを管理するため、システムの管理者のユーザ名とパスワードを指定します。 特権アクセスポイント管理のためのシークレット テキストを含めることもできます。 （注） パスワードが強力なパスワード ポリシーを満たしていない場合、パスワードは有効なエラー メッセージとともに拒否されます。たとえば、次のパスワードは、強力なパスワードでないため、拒否されます。 `Device# ap mgmtuser username cisco password 0 abcd secret 0 1234`
ステップ 6	**ap dot1x username** *username* **password{0** *unencrypted password* | **8** *AES encrypted password*} 例： `Device(config)# ap dot1x username cisco password 0 Qwci12@`	デバイスへ設定されたすべてのアクセスポイントを管理するため、802.1X のユーザ名とパスワードを指定します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**ap nameapnamemgmtuser username** *username***password** *password***secret** *secret_text* 例： `Device# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qne35! secret Nzep592$`	デバイスに設定された特定のアクセス ポイントを管理するための管理者のユーザ名、パスワード、およびシークレット テキストを設定します。
ステップ 9	**apnameapnamedot1x-user** *username***password** *password* 例： `Device# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qne35!`	特定のアクセス ポイントの 802.1X ユーザ名とパスワードを設定します。

例

例：管理者のユーザ名とパスワードの設定

次に、コンフィギュレーション モードで、管理者のユーザ名と、厳格なパスワード ポリシーに則ったパスワードを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless security strong-password
Device(config)# username adminuser1 password 0 QZsek239@
Device(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!
Device(config)# ap dot1x username cisco password 0 Qwci12@
Device# end
```

次に、グローバル EXEC モードで、管理者のユーザ名およびパスワードをアクセス ポイントに設定する例を示します。

```
Device# wireless security strong-password
Device# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qwci12@ secret Qwci14@
Device# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qwci12@
Device# end
```

管理者のユーザ名とパスワードに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference Guide (Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

管理者のユーザ名とパスワードの設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

第 130 章

802.11 パラメータおよび帯域選択の設定

- 機能情報の確認 （2857 ページ）
- 帯域選択の制約事項、802.11 帯域とパラメータ （2857 ページ）
- 帯域選択、802.11 帯域およびパラメータについて （2858 ページ）
- 802.11 帯域とそのパラメータを設定する方法 （2860 ページ）
- 帯域選択、802.11 帯域およびパラメータの設定のモニタリング （2868 ページ）
- 帯域選択、802.11 帯域およびパラメータの設定例 （2873 ページ）
- 802.11 パラメータおよび帯域選択に関する追加情報 （2875 ページ）
- 802.11 パラメータおよび帯域選択設定の機能履歴と情報 （2876 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

帯域選択の制約事項、802.11 帯域とパラメータ

- 帯域選択が有効になっている WLAN では、ローミングの遅延が発生するので、音声やビデオのような、遅延に敏感なアプリケーションはサポートされません。
- 帯域選択は、Cisco Aironet 1140、1250、1260、1550、2600、3500、3600、 シリーズ アクセス ポイントでのみ使用できます。
- Mid RSSI は、Cisco Aironet 1600 シリーズ アクセス ポイントではサポートされていません。
- 帯域選択は、Cisco Aironet 1040、OEAP 600 シリーズ アクセスポイントではサポートされていません。

- 帯域選択が動作するのは、コントローラに接続されたアクセス ポイントに対してのみです。コントローラに接続しない FlexConnect アクセス ポイントは、リブート後に帯域選択を実行しません。
- 帯域選択アルゴリズムによるデュアル バンド クライアントの誘導は、同じアクセス ポイントの 2.4 GHz 無線から 5 GHz 無線へに限られます。このアルゴリズムが機能するのは、アクセス ポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。
- コントローラ上で帯域選択とアグレッシブ ロード バランシングの両方を有効にすることができます。これらは独立して動作し、相互に影響を与えることはありません。
- コントローラ GUI またはコントローラ CLI を使用して、帯域選択とクライアント ロード バランシングをグローバルで有効または無効にすることはできません。ただし、特定の WLAN の帯域選択とクライアント ロード バランシングを有効または無効にできます。帯域選択とクライアント ロード バランシングは、デフォルトではグローバルで有効になっています。

帯域選択、802.11 帯域およびパラメータについて

帯域選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、混雑の少ない 5 GHz アクセス ポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセス ポイントからの同一チャネル干渉も発生します。802.11b/g では、重複しないチャネルが 3 つしかないからです。このような原因による干渉を防ぎ、ネットワーク全体のパフォーマンスを向上させるには、デバイスで帯域選択を設定します。

クライアントに対するプローブ応答を調整すると帯域選択が機能し、WLAN 単位で有効にできます。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。アクセス ポイントでは、帯域選択表は show dot11 band-select コマンドで表示できます。帯域選択表は、show cont d0/d1 | begin Lru でも表示できます。

（注） WMM のデフォルト設定は、[show running-config] 出力には表示されません。

帯域選択アルゴリズム

帯域選択アルゴリズムは 2.4 GHz GHz 帯を使用するクライアントに反映されます。最初に、クライアントがアクセス ポイントにプローブ要求を送信すると、対応するクライアント プローブのアクティブ値とカウント値（帯域選択に表示）が 1 になります。以下のシナリオによるアルゴリズム機能を示します。

- シナリオ 1 - クライアント RSSI（**show cont d0/d1 | begin RSSI**で表示）は、中間 RSSI と受け入れ可能クライアント RSSI のどちらよりも強い。
  - デュアル バンド クライアント：2.4 GHz プローブ応答はいつでも表示されず、すべての 5 Ghz プローブ要求に 5 GHz プローブ応答が表示されます。
  - シングル バンド（2.4 GHz）クライアント：プローブ抑制サイクルの後にのみ 2.4 GHz プローブ応答が表示されます。
  - 設定したプローブ サイクル カウントにクライアントのプローブ カウントが達すると、アルゴリズムはエージング アウト抑止時間を待ち、プローブのアクティブ値を 0 にマークします。そして、アルゴリズムが再起動します。
- シナリオ 2 - クライアント RSSI（**show cont d0/d1 | begin RSSI**で表示）は、中間 RSSI と受け入れ可能クライアント RSSI の間になります。
  - 2.4 GHz プローブ要求と 5 GHz プローブ要求はすべて制限なしで応答します。
  - このシナリオは、帯域選択無効時と似ています。

（注） クライアントの RSSI 値（[sh cont d0] | [begin RSSI] で表示）は、受信したクライアント パケットの平均値であり、中間 RSSI 機能は、プローブ パケットの RSSI の瞬時値です。**sh cont d0begin RSSI**そのため、クライアント RSSI は設定した中間 RSSI 値（7 dB デルタ）より弱くなります。クライアントからのプローブ 802.11b は、802.11a バンドに関連付けるためクライアントをプッシュするように抑制されます。

802.11 帯域

自国の法的な規制基準を遵守するために、コントローラの 802.11b/g/n（2.4GHz）帯域と 802.11a/n（5GHz）帯域を設定できます。デフォルトでは、802.11b/g/n と 802.11a/n の両方がイネーブルになっています。

コントローラが 802.11g トラフィックだけを許可するように設定されている場合、802.11b クライアント デバイスはアクセス ポイントに正常に接続できますが、トラフィックを送信できません。802.11g トラフィック専用にコントローラを設定する場合、必須として 11g レートをマークする必要があります。

802.11n パラメータ

この項では、ネットワーク上の 802.11n デバイス（Cisco Aironet 1140 および 3600 シリーズ アクセス ポイントなど）を管理する手順を説明します。802.11n デバイスでは、2.4GHz 帯域と 5GHz 帯域をサポートしており、高スループット データ レートを提供します。

802.11n の高スループット データ レートは、すべての 802.11n アクセス ポイントで使用できます。この場合、WLAN で WMM が使用されていることと、レイヤ 2 暗号化なしであるか WPA2/AES 暗号化が有効化されていることが必要です。

（注） Cisco 802.11n AP は、偽の wIPS アラームをトリガーする可能性がある誤ったビーコン フレームを断続的に送信する場合があります。これらのアラームを無視することをお勧めします。この問題は Cisco 802.11n AP の 1140、1250、2600、3500、および 3600 で確認されています。

802.11h パラメータ

802.11h では、チャネルの変更がクライアント デバイスに通知されます。また、クライアント デバイスの送信電力を制限できるようになっています。

802.11 帯域とそのパラメータを設定する方法

帯域選択の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless client band-select cycle-count** *cycle_count* 例： `Device(config)# wireless client band-select cycle-count 3`	帯域選択のプローブ サイクル カウントを設定します。 *cycle_count* パラメータには、1 ～ 10 の範囲内の値を入力できます。
ステップ 3	**wireless client band-select cycle-threshold** *milliseconds* 例： `Device(config)# wireless client band-select cycle-threshold 5000`	新規スキャン周期の時間のしきい値を設定します。 *milliseconds* パラメータには、しきい値として 1 ～ 1000 の範囲内の値を入力できます。
ステップ 4	**wireless client band-select expire suppression** *seconds* 例：	抑制の期限切れを帯域幅選択に設定します。

	コマンドまたはアクション	目的
	`Device(config)# wireless client band-select expire suppression 100`	*seconds* パラメータには、抑制期間として 10 ～ 200 の範囲内の値を入力できます。
ステップ 5	**wireless client band-select expire dual-band** *seconds* 例： `Device(config)# wireless client band-select expire dual-band 100`	デュアル バンドの期限を設定します。 *seconds* パラメータには、デュアル バンド用に 10 ～ 300 の範囲内の値を入力できます。
ステップ 6	**wireless client band-select client-rssi** *client_rssi* 例： `Device(config)# wireless client band-select client-rssi 40`	クライアント RSSI しきい値を設定します。 *client_rssi* パラメータには、プローブに応答するクライアント RSSI の最小 dBm として 20 ～ 90 の範囲内の値を入力できます。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ステップ 8	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **band-select**
	例：
	`Device(config)# wlan wlan1 25 ssid12`
	`Device(config-wlan)# band-select`
		特定の WLAN で帯域選択を設定します。
		wlan_ID パラメータには、1 ～ 512 の範囲内の値を入力できます。
		SSID_network_name パラメータには、最大 32 文字の英数字を入力できます。

ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 帯域の設定（CLI）

802.11 帯域およびパラメータを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 5ghz shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	802.11a 帯域をディセーブルにします。 （注） 802.11a ネットワーク パラメータを設定する前に、802.11a 帯域をディセーブルにする必要があります。
ステップ 3	**ap dot11 24ghz shutdown** 例： `Device(config)# ap dot11 24ghz shutdown`	802.11b 帯域をディセーブルにします。 （注） 802.11b ネットワーク パラメータを設定する前に、802.11b 帯域をディセーブルにする必要があります。
ステップ 4	**ap dot11 {5ghz | 24ghz} beaconperiod** *time_unit* 例： `Device(config)# ap dot11 5ghz beaconperiod 500`	アクセスポイントによる SSID のブロードキャスト レートを指定します。 ビーコン間隔は時間単位（TU）で測定されます。1 TU は 1024 マイクロ秒です。20 ～ 1000 ミリ秒ごとにビーコンを送信するように、アクセスポイントを設定できます。
ステップ 5	**ap dot11 {5ghz | 24ghz} fragmentation** *threshold* 例： `Device(config)# ap dot11 5ghz fragmentation 300`	パケットを断片化するサイズを指定します。 しきい値は、256 ～ 2346 バイト（両端の値を含む）です。接続不良や多くの無線干渉が発生している領域では、この値を小さくします。

ステップ 6	**ap dot11 {5ghz | 24ghz} dtpc**
	例：
	`Device(config)# ap dot11 5ghz dtpc`
	`Device(config)# no ap dot11 24ghz dtpc`
		アクセスポイントによる、チャネルのアドバタイズ、ビーコンの電力レベル送信、応答プローブをイネーブルにします。
		デフォルト値はイネーブルです。Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）を使用するクライアントデバイスは、アクセス ポイントからチャネルおよび電力レベル情報

	コマンドまたはアクション	目的
		を受信して、自身の設定を自動的に調整します。たとえば、主に日本で使用されているクライアントデバイスをイタリアに移送し、そこのネットワークに追加した場合、チャネルと電力設定の自動調整を DTPC に任せることができます。 （注） Cisco IOS ソフトウェアを実行するアクセス ポイントでは、この機能はワールドモードと呼ばれます。 このコマンドの **no** 形式は、802.11a または 802.11b DTPC 設定をディセーブルにします。
ステップ 7	**wireless client association limit** *number* **interval** *milliseconds* 例： `Device(config)# wireless client association limit 50 interval 1000`	設定できるクライアントの最大数を指定します。 単一アクセスポイントスロットの、所定の間隔内におけるアソシエーション要求の最大数を設定できます。設定できるアソシエーション制限の範囲は 1 ～ 100 です。 アソシエーション要求制限間隔は 100 ～ 10000 ミリ秒です。
ステップ 8	**ap dot11 {5ghz | 24ghz} rate** *rate {disable | mandatory | supported}* 例： `Device(config)# ap dot11 5ghz rate 36 mandatory`	データをコントローラとクライアント間で送信できる速度を指定します。 • *disabled*：クライアントが通信に使用するデータ レートを指定するように定義します。 • *mandatory*：クライアントがコントローラのアクセスポイントにアソシエートするにはこのデータ レートをサポートする必要があると定義します。 • *supported*：アソシエートしたクライアントは、このデータ レートをサポートしていれば、このレートを使用してアクセスポイントと通信することができます。ただし、

	コマンドまたはアクション	目的
		クライアントがこのレートを使用できなくても、アソシエートは可能です。 • *rate*：データが送信されるレートを指定します。802.11a、802.11b 帯域では、データは 1、2、5.5、6、9、11、12、18、24、36、48、または 54 Mbps のレートで送信されます。
ステップ 9	**no ap dot11 5ghz shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	802.11a 帯域をイネーブルにします。 （注） デフォルト値はイネーブルです。
ステップ 10	**no ap dot11 24ghz shutdown** 例： `Device(config)# no ap dot11 24ghz shutdown`	802.11b 帯域をイネーブルにします。 （注） デフォルト値はイネーブルです。
ステップ 11	**ap dot11 24ghz dot11g** 例： `Device(config)# ap dot11 24ghz dot11g`	802.11g ネットワークのサポートをイネーブルまたはディセーブルにします。 デフォルト値はイネーブルです。このコマンドは、802.11b 帯域が有効になっている場合のみ使用できます。この機能を無効にすると、802.11b 帯域は 802.11g をサポートせずに有効になります。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

802.11n のパラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**ap dot11 {5ghz | 24ghz} dot11n** 例： `Device(config)# ap dot11 5ghz dot11n`	ネットワークで 802.11n サポートをイネーブルします。 このコマンドの **no** 形式は、ネットワーク上の 802.11n サポートをディセーブルにします。
ステップ 3	**ap dot11 {5ghz | 24ghz} dot11n mcs tx** *rtu* 例： `Device(config)# ap dot11 5ghz dot11n mcs tx 20`	データをアクセスポイントとクライアント間で送信できる変調および符号化方式（MCS）レートを指定します。**mcs tx** パラメータには、0 ～ 23 の値が設定できます。 このコマンドの **no** 形式は、設定された MCS レートをディセーブルに設定します。

ステップ 4	**wlan***wlan_profile_name wlan_ID SSID_network_name* **wmm require**
	例：
	`Device(config)# wlan wlan1 25 ssid12`
	`Device(config-wlan)# wmm require`
		WLAN で WMM をイネーブルにし、設定した 802.11n データ レートを使用します。
		require パラメータは、クライアントデバイスに WMM の使用を要求します。WMM をサポートしていないデバイスは WLAN に接続できません。

ステップ 5	**ap dot11 {5ghz | 24ghz} shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	ネットワークをディセーブルにします。
ステップ 6	**{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}** 例： `Device(config)# ap dot11 5ghz dot11n a-mpdu tx priority all`	802.11n パケットに使用する集約方法を指定します。 集約は、パケットデータ フレームを個別に伝送するのではなく、グループにまとめるプロセスです。集約方法には、Aggregated MAC Protocol Data Unit（A-MPDU）と Aggregated MAC Service Data Unit（A-MSDU）の 2 種類があります。A-MPDU と A-MSDU は、両方ともソフトウェアで実行されます。 集約方法は、アクセスポイントからクライアントへのトラフィックのタイプごとに指定できます。

	コマンドまたはアクション	目的
		次の表は、トラフィック タイプごとに割り当てられる優先レベル（0～7）の説明です。

表 *182*：トラフィック タイプの優先レベル

ユーザ優先度	トラフィック タイプ
0	ベスト エフォート
1	バックグラウンド
2	予備
3	エクセレント エフォート
4	制御された負荷
5	ビデオ、遅延およびジッタは 100 ミリ秒未満
6	音声、遅延およびジッタは 100 ミリ秒未満
7	ネットワーク制御

各優先レベルを個別に設定するか、all パラメータを使用して一度にすべての優先レベルを設定できます。トラフィックが A-MPDU 送信または A-MSDU 伝送を使用するよう、プライオリティ レベルを設定できます。

- 他のオプションとともに **ap** コマンドを使用すると、そのプライオリティ レベルに関連付けられたトラフィックは、A-MPDU 送信に関連付けらます。
- 他のオプションとともに **no ap** コマンドを使用すると、そのプライオリティ レベルに関連付けられたトラフィックは、A-MSDU 送信に関連付けられます。

クライアントが使用する集約方法に合わせて優先度を設定します。

	コマンドまたはアクション	目的
		デフォルトでは、A-MPDU は、優先レベル 0、4、および 5 に対して有効になっており、それ以外は無効になっています。デフォルトでは、A-MPDU は、6 と 7 以外のすべての優先度に対して有効になっています。
ステップ 7	**no ap dot11 {5ghz | 24ghz} shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	ネットワークを再度イネーブルにします。
ステップ 8	**ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}** 例： `Device(config)# ap dot11 5ghz dot11n guard-interval long`	ネットワークのガード間隔を設定します。
ステップ 9	**ap dot11 {5ghz | 24ghz} dot11n rifs rx** 例： `Device(config)# ap dot11 5ghz dot11n rifs rx`	ネットワークの Reduced Interframe Space（RIFS）を設定します。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

802.11h のパラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 5ghz shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	802.11a ネットワークをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**{ap | no ap} dot11 5ghz channelswitch mode** *switch_mode* 例： `Device(config)# ap dot11 5ghz channelswitch mode 0`	アクセス ポイントの、新しいチャネルに切り替わった際のアナウンス機能をイネーブルまたはディセーブルにします。 **channelswitch** パラメータには 0 または 1 を入力できます。チャネルが実際に切り替えられるまで送信を制限する場合は 0 を入力し、制限しない場合は 1 を入力します。デフォルト値は [disabled] です。
ステップ 4	**ap dot11 5ghz power-constraint** *value* 例： `Device(config)# ap dot11 5ghz power-constraint 200`	802.11h 電力制限値を 0 から 255 の範囲で設定します。 value パラメータのデフォルト値は 3 dB です。
ステップ 5	**no ap dot11 5ghz shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	802.11a ネットワークを再度イネーブルします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

帯域選択、802.11 帯域およびパラメータの設定のモニタリング

帯域選択と 802.11 帯域を使用した設定のモニタリング コマンド

このセクションでは、帯域選択および 802.11 帯域の新しいコマンドについて説明します。

次のコマンドは、 の帯域選択と 802.11 帯域、およびパラメータのモニタリングに使用できます。

表 *183 :* 帯域選択と *802.11* 帯域を使用した設定のモニタリング コマンド

コマンド	目的
show ap dot11 5ghz network	802.11a 帯域ネットワーク パラメータ、802.11a 運用率、802.11n MCS 設定および 802.11n ステータス情報を表示します。

show ap dot11 24ghz network	802.11b 帯域ネットワーク パラメータ、802.11b/g 運用率、802.11n MCS 設定および 802.11n ステータス情報を表示します。
show wireless dot11h	802.11h 設定パラメータを表示します。
show wireless band-select	帯域選択設定を表示します。

例：5 GHz 帯域の設定の確認

```
Device# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
```

```
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

例：24 GHz 帯域の設定の確認

```
Device# show ap dot11 24ghz network
802.11b Network : Enabled
11gSupport : Enabled
11nSupport : Enabled

  802.11b/g Operational Rates
  802.11b 1M : Mandatory
  802.11b 2M : Mandatory
  802.11b 5.5M : Mandatory
  802.11g 6M : Supported
  802.11g 9M : Supported
```

```
  802.11b 11M : Mandatory
  802.11g 12M : Supported
  802.11g 18M : Supported
  802.11g 24M : Supported
  802.11g 36M : Supported
  802.11g 48M : Supported
  802.11g 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
  Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable Mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 11
Default Tx Power Level : 1
DTPC Status : true
Call Admission Limit : 105
G711 CU Quantum : 15
ED Threshold : -50
```

```
Fragmentation Threshold : 2346
PBCC Mandatory : Disabled
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

例：802.11h パラメータの状態の確認

```
Device# show wireless dot11h
Power Constraint: 0
Channel Switch: 0
Channel Switch Mode: 0
```

例：帯域選択設定の確認

```
Device# show wireless band-select
Band Select Probe Response    : per WLAN enabling
Cycle Count                  : 2
Cycle Threshold (millisec)   : 200
Age Out Suppression (sec)    : 20
Age Out Dual Band (sec)      : 60
Client RSSI (dBm)            : 80
```

帯域選択、802.11 帯域およびパラメータの設定例

例：帯域選択の設定

次に、帯域選択の新規スキャン周期のプローブ サイクル カウントおよび時間しきい値を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 3
Device(config)# wireless client band-select cycle-threshold 5000
Device(config)# end
```

次に、抑制の期限を帯域選択に設定する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 100
Device(config)# end
```

次に、デュアル バンドの期限を帯域選択に設定する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select expire dual-band 100
Device(config)# end
```

次に、クライアント RSSI しきい値を帯域選択に設定する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select client-rssi 40
Device(config)# end
```

次に、特定の WLAN 上で帯域選択を設定する例を示します。

```
Device# configure terminal
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# band-select
Device(config)# end
```

例：802.11 帯域設定

次に、ビーコン間隔、フラグメンテーション、および動的な送信電力コントロールを使用して 802.11 帯域を設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 24ghz shutdown
Device(config)# ap dot11 5ghz beaconperiod 500
Device(config)# ap dot11 5ghz fragmentation 300
Device(config)# ap dot11 5ghz dtpc
Device(config)# wireless client association limit 50 interval 1000
```

```
Device(config)# ap dot11 5ghz rate 36 mandatory
Device(config)# no ap dot11 5ghz shutdown
Device(config)# no ap dot11 24ghz shutdown
Device(config)# ap dot11 24ghz dot11g
Device(config)#end
```

例：802.11n 設定

次に、集約方法を使って 5 GHz 帯域の802.11n パラメータを設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
Device(config)# no ap dot11 5ghz shutdown
Device(config)#exit
```

次に、5 GHz 帯域でガード インターバルを設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# no ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n guard-interval long
Device(config)#end
```

次に、5 GHz 帯域で RIFS を設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n rifs rx
Device(config)#end
```

例：802.11h 設定

次に、制限伝送を使用して、アクセスポイントをいつ新しいチャネルに切り替えるかをアナウンスするために、そのアクセスポイントを設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz channelswitch mode 0
```

```
Device(config)# no ap dot11 5ghz shutdown
Device(config)#end
```

次に、5 GHz 帯域で 802.11h 電力制限を設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz power-constraint 200
Device(config)# no ap dot11 5ghz shutdown
Device(config)#end
```

802.11 パラメータおよび帯域選択に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

802.11 パラメータおよび帯域選択設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

第 131 章

アグレッシブ ロード バランシングの設定

- 機能情報の確認 （2877 ページ）
- アグレッシブ ロード バランシングの制約事項 （2877 ページ）
- アグレッシブ ロード バランシング パラメータの設定情報 （2878 ページ）
- アグレッシブ ロード バランシングの設定方法 （2880 ページ）
- アグレッシブ ロード バランシングのモニタリング （2881 ページ）
- アグレッシブ ロード バランシングに関する追加情報 （2881 ページ）
- アグレッシブ ロード バランシングの設定の機能履歴と情報 （2882 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

アグレッシブ ロード バランシングの制約事項

- コマンドライン インターフェイスからのみアグレッシブ ロード バランシングを設定できます。
- アグレッシブ ロード バランシングは、手動で有効にしなければなりません。デフォルトでは無効になっています。
- 帯域選択設定と別にでも一緒にでもロード バランシングをイネーブルにできます。
- 帯域選択がデュアル バンド クライアントでイネーブルの場合、ロード バランシング パラメータは 5 GHz 無線から、無線の負荷が最小のもののみ選択します。2.4 GHz クライアントでは、5 GHz クライアントのプローブ情報がないため、ロード バランシング アルゴリズムは 2.4 GHz 無線でのみ選択できます。

- 同じデバイスのアクセス ポイント間でクライアントのロード バランシングを実行できますが、異なるデバイスのアクセス ポイント間のクライアントでは実行できません。
- ロードバランシングは無線クライアントの数に基づいて既存の関連付け拒否メカニズムを使用し、帯域選択はアクセスポイントでのプローブ応答分散の抑制によってのみ実装されます。

アグレッシブ ロード バランシング パラメータの設定情報

アグレッシブ ロード バランシング

コントローラ上でアグレッシブ ロード バランシングを有効にすると、ワイヤレス クライアントの負荷を Lightweight アクセス ポイント間で分散することができます。アグレッシブ ロード バランシングはコントローラを使用して有効にできます。

ワイヤレス クライアントが Lightweight アクセス ポイントへのアソシエートを試みると、アソシエーション応答パケットとともに 802.11 応答パケットがクライアントに送信されます。この 802.11 応答パケットの中にステータス コード 17 があります。コード 17 は AP がビジー状態であることを示します。AP のしきい値に達成しなければ、AP からは「success」を示すアソシエーション応答は返りません。AP 使用率のしきい値を超えると、コード 17（AP ビジー）が返り、処理能力に余裕がある別の AP がクライアント要求を受け取ります。

たとえば、AP1 上のクライアント数が、AP2 のクライアント数とロード バランシング ウィンドウの和を上回っている場合は、AP1 の負荷は AP2 よりも高いと判断されます。クライアントが AP1 にアソシエートしようとすると、ステータス コード 17 が含まれている 802.11 応答パケットがクライアントに送信されます。アクセスポイントの負荷が高いことがこのステータス コードからわかるので、クライアントは別のアクセス ポイントへのアソシエーションを試みます。

コントローラは、クライアントアソシエーションを 10 回まで拒否するように設定できます（クライアントがアソシエーションを 11 回試みた場合、11 回目の試行時にアソシエーションが許可されます）。また、特定の WLAN 上でロード バランシングを有効にするか、無効にするかも指定できます。これは、特定のクライアント グループ（遅延に敏感な音声クライアントなど）に対してロード バランシングを無効にする場合に便利です。

（注） 300 ミリ秒を超えて遅延を設定すると、音声クライアントは認証しません。これを避けるには、中央認証（CCKM による WLAN のローカル スイッチング）を設定し、さらに AP と WLC 間に遅延 600 ms（UP と DOWN それぞれ 300 ms）の Pagent ルータを設定して、音声クライアントをアソシエートします

アクセス ポイントがサポートできるクライアント アソシエーションの最大数は、次の要因に依存しています。

- Lightweight アクセス ポイントと Autonomous Cisco IOS アクセス ポイントの場合、クライアント アソシエーションの最大数は異なります。
- 無線単位の制限と、AP 単位の全体的な制限が存在する場合があります。
- AP ハードウェア（16 MB の AP では、32 MB 以上の AP よりも制限が厳しくなります）

Lightweight アクセス ポイントのクライアント アソシエーションの制限は次のとおりです。

- 16 MB の AP の場合、AP ごとに 128 台のクライアントに制限されます。この制限は、1100 および 1200 シリーズ AP に適用されます。
- 32 MB 以上の AP の場合、AP 単位の制限は存在しません。

すべての Cisco IOS AP の最大クライアント アソシエーションの制限は、1 無線につき 200 アソシエーションです。

（注） 32 MB 以上の Lightweight Cisco IOS AP では、無線が 2 つの場合、最大で 200 + 200 = 400 アソシエーションがサポートされます。

Autonomous Cisco IOS アクセス ポイントあたりの最大クライアント アソシエーションの制限は、AP あたり約 80 ～ 127 クライアントです。この数は、次の要因に応じて変化します。

- AP モデル（16 MB か、32 MB 以上か）
- Cisco IOS ソフトウェア リリース
- ハードウェア構成（無線が 2 つの場合、1 つの場合よりも多くのメモリを使用します）
- 有効にしている機能（特に WDS 機能）

無線単位の制限は、およそ200アソシエーションです。アソシエーションは、多くの場合、AP 単位の制限に先に達します。Cisco Unified Wireless Network とは異なり、Autonomous Cisco IOS では、SSID 単位/AP 単位のアソシエーション制限がサポートされています。この制限は、dot11 SSID の下で、max-associations CLI を使用して設定されます。最大数は 255 アソシエーションです（これはデフォルト値でもあります）。

（注） FlexConnect AP の場合は、アソシエーションがローカルに処理されます。ロードバランシングの判断は、Cisco WLC で行われます。FlexConnect AP は、Cisco WLC の計算結果を確認する前に、まず、クライアントに応答を返します。FlexConnect AP がスタンドアロン モードの場合は、ロード バランシングが適用されません。

FlexConnect AP は、ローカル モードの AP と同様にロード バランシング用のステータス 17 で（再）アソシエーション応答を送信しません。代わりに、ステータス 0（成功）で（再）アソシエーションを送信してから、理由 5 で認証解除を送信します。

アグレッシブ ロード バランシングの設定方法

アグレッシブなロード バランシングの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、アグレッシブ ロード バランシング用のクライアント ウィンドウを設定します。

wireless load-balancing window *client_count*

client_count パラメータには、0 ～ 20 の範囲内の値を入力できます。

ステップ 2 次のコマンドを入力して、ロード バランシング用の拒否回数を設定します。

wireless load-balancing denial *denial_count*

denial_count パラメータには、1 ～ 10 の範囲内の値を入力できます。

ステップ 3 次のコマンドを入力して、変更を保存します。

write memory

ステップ 4 次のコマンドを入力して、WLAN コンフィギュレーション モードを開始します。

wlan *profile-name wlan_ID SSID*

profile-name には、32 文字以内の英数字のプロファイル名を入力できます。*wlan_ID* パラメータには、1 ～ 512 の範囲内の値を入力できます。*SSID* パラメータには、32 文字以内の英数字のネットワーク名を入力できます。

ステップ 5 特定の WLAN 上でロード バランシングを有効にするには、次のコマンドを入力します。

load-balance

ロード バランシングを無効にするには、**no load-balance** コマンドを使用します。.

ステップ 6 次のコマンドを入力して、設定を確認します。

show wireless load-balancing

```
Aggressive Load Balancing.............................: per WLAN enabling
Aggressive Load Balancing Window (clients)..................:: 5
Aggressive Load Balancing Denial Count......................:: 3

Statistics
Total Denied Count (clients)................................:: 0
Total Denial Sent (messages)................................:: 0
Exceeded Denial Max Limit Count (times)......................:: 0
None 5G Candidate Count (times)..............................:: 0
None 2.4G Candidate Count (times)............................:: 0
```

ステップ 7 次のコマンドを入力して、変更を保存します。

write memory

アグレッシブ ロード バランシングのモニタリング

ここでは、アグレッシブ ロード バランシング用の新しいコマンドについて説明します。

次のコマンドが上でアグレッシブ ロード バランシングをモニタするために使用できます。

表 *184*：アグレッシブ ロード バランシング コマンドの監視

コマンド	目的
show wireless load-balancing	ロードバランシング機能のステータスを表示します。

アグレッシブ ロード バランシングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

アグレッシブロードバランシングの設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

第 132 章

クライアント ローミングの設定

- 機能情報の確認 （2883 ページ）
- クライアント ローミングの設定の制約事項 （2883 ページ）
- クライアント ローミングについて （2884 ページ）
- レイヤ 2 またはレイヤ 3 のローミング設定方法 （2887 ページ）
- クライアントのローミング パラメータのモニタリング （2894 ページ）
- モビリティ設定のモニタ （2894 ページ）
- クライアント ローミング設定に関する追加情報 （2896 ページ）
- クライアント ローミング設定の機能履歴と情報 （2897 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

クライアント ローミングの設定の制約事項

以下は、クライアント ローミングを設定する際に注意が必要な制約事項です。

- Cisco Compatible Extensions（CCX）サポートは、デバイス上の各 WLAN について自動的にイネーブルになり、ディセーブルにできません。デバイスは、クライアントのCCXバージョンを自身のクライアント データベースに格納します。この情報に基づいて、CCX フレームを生成するとともに、CCX フレームに応答します。これらのローミング拡張機能を使用するには、クライアントでCCXv4かCCXv5（または、アクセス ポイント経由ローミングの場合 CCXv2）がサポートされている必要があります。
- 600 シリーズ アクセス ポイント間のクライアント ローミングはサポートされません。

クライアント ローミングについて

コントローラは、ワイヤレスネットワークをローミングするクライアントにハイエンドのワイヤレス サービスを提供します。今では、ワイヤレス サービスはスイッチと統合され、付加価値が高く新しい、シスコの統合されたモビリティアーキテクチャを提供します。この統合されたアーキテクチャにより、ワイヤレスおよび有線クライアントの両方に対して、シームレスで高速なクライアント ローミング サービスが可能になります。

新しいモビリティ アーキテクチャは、モビリティ ドメイン（MD）、モビリティ グループ（MG）、モビリティサブドメイン（MSD）にネットワークの論理分類を使用して高速なクライアント ローミング サービスをサポートし、Mobility Oracle（MO）、モビリティ コントローラ（MC）、モビリティ エージェント（MA）などのシステムを使用してスイッチ ピア グループ（SPG）をサポートします。

- **モビリティ ドメイン**は、クライアント ローミングがサポートされているすべてのドメインです。モビリティ ドメインはモビリティ グループの集合です。たとえば、キャンパスネットワークは、モビリティ ドメインと見なすことができます。
- **モビリティ グループ**は、高速ローミングがサポートされるモビリティ サブドメインの集合です。モビリティグループは、頻繁にローミングがサポートされているキャンパス内の複数の建物である可能性があります。
- **モビリティ サブドメイン**は、モビリティ ドメイン ネットワークの自律的な部分です。それぞれのモビリティ サブドメインには、1 台のモビリティ コントローラおよび SPG の集合があります。サブドメインは 802.11r キーのドメインと同じです。
- **スイッチ ピア グループ**はモビリティ エージェントの集合です。
- **Mobility Oracle** はモビリティ サブドメインで発生したモビリティ イベントの接続ポイントとして機能します。Mobility Oracle は、モビリティ ドメイン全体、自宅、および現在のサブドメインの各クライアントのローカルデータベースも管理します。MO はモビリティドメイン全体に対して 1 つだけです。Cisco WLC の 5700 シリーズ コントローラまたは Cisco Unified Wireless Network ソリューション コントローラは、MO として機能します。
- **モビリティ コントローラ**は、SPG 間の ローミング イベントにモビリティ管理サービスを提供します。MC は、そのサブドメインに属するすべてのモビリティ エージェントに、SPG 名や SPG ピア メンバ リストなどの設定を送信します。Cisco WLC 5700 シリーズ コントローラ、Cisco Catalyst 3850 スイッチ、または Cisco Unified Wireless Network ソリューション コントローラは、MC として機能します。MC には、その中で内部的に実行されている MC 機能および MA 機能があります。
- **モビリティ エージェント**は、モバイルクライアント用のクライアントモビリティのステート マシンを維持するコンポーネントです。すべての AP は、モビリティ エージェントに接続されます。

新しいモビリティ アーキテクチャは、次のようなシナリオでのシームレスなローミングをサポートします。

- スイッチ内のローミング：同じモビリティ エージェントが管理する AP 間でのクライアント ローミング。
- SPG 内のローミング：同じ SPG のモビリティ エージェント間でのクライアント ローミング。
- SPG 内、サブドメイン内のローミング：同じサブドメイン内の異なる SPG のモビリティ エージェント間でのクライアント ローミング。
- サブドメイン内のローミング：サブドメインでのモビリティエージェント間のクライアント ローミング。

高速ローミング

新しいモビリティ アーキテクチャは、完全な認証の必要性を排除することによって、クライアントがモビリティ グループ内でローミングするときの高速なローミングをサポートします。セキュリティ ポリシーは、高速ローミングのためのスイッチ間で同じである必要があります。

ローカル、アンカー、外部 MA および MC

クライアントが MA に最初に参加し、接続ポイントが変更されていない場合、その MA はローカル MA または関連 MA と呼ばれます。この MA が関連づけられている MC は、ローカル MC または関連 MC と呼ばれます。

クライアントが 2 つの MA 間をローミングすると、クライアントが以前関連付けられていた MA は、アンカー MA（接続ポイント）になり、クライアントが現在関連付けられている MA は、外部 MA または関連 MA（プレゼンス ポイント）になります。これらの MA が関連づけられている MC は、アンカー、外部、または関連 MC とそれぞれ呼ばれます。

サブネット間ローミング

同様に、マルチコントローラ展開では、異なるサブネット上の同一モビリティ グループ内のコントローラによって管理されるアクセス ポイント間のクライアント ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、クライアントは同じ DHCP 割り当てまたはクライアント割り当て IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。IP アドレス 0.0.0.0、または自動 IP アドレス 169.254.*.* のクライアントが DHCP Discover を送信するか、オペレータが設定した時間が経過してタイムアウトになると、トンネルが切断され、クライアントの再認証が必要になります。

VoIP による通話ローミング

802.11 Voice-over-IP（VoIP）通話は、RF 信号が最も強いアソシエーションを見つけ出すことで、最適な Quality of Service（QoS）と最高のスループットを実現します。VoIP 通話には、ローミング ハンドオーバーの遅延時間が 20 ミリ秒以下という最小要件がありますが、シスコ ワイヤレス ソリューションならばこの要件を容易に満たすことができます。このソリューションでは、オープン認証が使用されていれば、平均ハンドオーバー遅延時間は 5 ミリ秒以下です。こ

の短い遅延時間は、個々のアクセス ポイントにローミング ハンドオーバーのネゴシエートを許可せずにコントローラによって制御されます。

シスコ ワイヤレス ソリューションでは、コントローラが同一のモビリティ グループに属している場合、異なるサブネット上のコントローラによって管理される lightweight アクセス ポイント間での 802.11 VoIP 通話ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、VoIP 通話は同じ DHCP 割り当て IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。VoIP クライアントが VoIP 通話 IP アドレス 0.0.0.0 を使用して DHCP Discover を送信するか、VoIP 通話自動 IP アドレス 169.254.*.* を使用するか、またはオペレータが設定した時間が経過してタイムアウトになると、トンネルが切断され、VoIP クライアントの再認証が必要になります。

CCX レイヤ 2 クライアント ローミング

コントローラでは、次の 5 つの CCX レイヤ 2 クライアント ローミング拡張機能がサポートされています。

- アクセスポイント経由ローミング：この機能により、クライアントはスキャン時間を節約できます。CCXv2 クライアントがアクセス ポイントにアソシエートする際、新しいアクセスポイントに以前のアクセスポイントの特徴をリストする情報パケットを送信します。各クライアントがアソシエートされていた以前のアクセスポイントと、アソシエーション直後にクライアントに送信（ユニキャスト）されていた以前のアクセスポイントをすべてまとめて作成したアクセスポイントのリストがクライアントによって認識および使用されると、ローミング時間が短縮します。アクセスポイントのリストには、チャネル、クライアントの現在の SSID をサポートするネイバー アクセス ポイントの BSSID、およびアソシエーション解除からの経過時間が含まれます。

- 拡張ネイバー リスト：特に音声アプリケーションを提供する際に、CCXv4 クライアントのローミング能力とネットワーク エッジのパフォーマンスを向上させるための機能です。アクセス ポイントは、ネイバー リストのユニキャスト更新メッセージを使用して、アソシエートされたクライアントのネイバーに関する情報を提供します。

- 拡張ネイバー リスト要求（E2E）：End-2-End 仕様は、音声/ローミング能力の全体的向上のために新しいプロトコルとインターフェイスを定義する、Cisco と Intel の共同プログラムです。これは、CCX 環境の Intel クライアントにのみ適用されます。これにより、Intel クライアントは自由にネイバー リストを要求できるようになります。要求すると、アクセスポイントはコントローラに要求を転送します。コントローラは要求を受信し、クライアントがアソシエートされているアクセス ポイントに対するネイバーの現在の CCX ローミング サブリストで応答します。

（注） 特定のクライアントが E2E をサポートするかどうかを調べるには、コントローラの GUI で [Wireless] > [Clients] の順に選択し、そのクライアントの [Detail] リンクをクリックして、[Client Properties] 領域の [E2E Version] テキスト ボックスを確認します。

- ローミング理由レポート：CCXv4 クライアントが新しいアクセス ポイントにローミングした理由を報告するための機能です。また、ネットワーク管理者はローミング履歴を作成およびモニタできるようになります。
- ダイレクトされたローミング要求：クライアントがアソシエートしているアクセスポイントよりもサービス能力が高いアクセスポイントが他にある場合に、ローミング要求をコントローラからクライアントに送信できるようになります。この場合、コントローラはクライアントに join できる最適なアクセス ポイントの一覧を送信します。クライアントはダイレクトされたローミング要求を受け入れることも、無視することもできます。CCX 以外のクライアントおよび CCXv3 以下を実行するクライアントは、どちらの操作も行う必要がありません。この機能を使用するために設定する必要はありません。

レイヤ 2 またはレイヤ 3 のローミング設定方法

レイヤ 2 またはレイヤ 3 のローミング設定

始める前に

レイヤ 2 またはレイヤ 3 ローミングをモビリティ エージェントに設定するには、次の必要条件を考慮する必要があります。

- レイヤ 2 とレイヤ 3 ローミングのための SSID およびセキュリティ ポリシーは、MA 全体で同じである必要があります。
- クライアント VLAN ID は、レイヤ 2 ローミングでは同じで、レイヤ 3 ローミングでは異なっている必要があります。
- ブリッジ ドメイン ID とクライアント VLAN ID は、レイヤ 2 ローミングで同じである必要があります。ブリッジ ドメイン ID とクライアント VLAN ID のうち、一方または両方が、レイヤ 3 ローミングで異なる必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan_profile_name wlan_ID SSID_network_name* 例： `Device(config)#wlan wlan1`	WLAN コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**no mobility anchor sticky** 例： `Device(config-wlan)#no mobility anchor sticky`	（任意）レイヤ2アンカーをディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

CCX クライアント ローミング パラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 {5ghz | 24ghz} l2roam rf-params** {**default | custom** *min-rssi roam-hyst scan-thresh trans-time*} 例： `Device#ap dot11 5ghz l2roam rf-params custom -80`	CCX レイヤ 2 クライアント ローミング パラメータを設定します。 デフォルトRFパラメータを選択するには、**default** オプションを入力します。 クライアント ローミングに影響を与える RF パラメータを最適化するには、**custom** オプションを入力してから、次のオプションのいずれかを入力してください。 • [Minimum RSSI]：クライアントがアクセス ポイントにアソシエートするために必要な最小の受信信号強度インジケータ（RSSI）を示します。 クライアントの平均の受信信号の強度がこのしきい値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。

	コマンドまたはアクション	目的
		最小の RSSI 値を -50 ～ -90 dBm の範囲で設定できます。また、デフォルト値は -85 dBm です。 • [Hysteresis]：クライアントが近隣のアクセス ポイントにローミングするときに必要な信号強度の値を示します。 このパラメータは、クライアントが 2 つのアクセス ポイント間のボーダー近くに物理的に存在している場合に、アクセス ポイント間のローミングの量を減らすことを意図しています。 [Hysteresis] は、3 ～ 20 dB の範囲で設定できます。デフォルトは 3 dB です。 • [Scan Threshold]：クライアントがより適切なアクセス ポイントにローミングするまでに許可される最小 RSSI を示します。 RSSI が指定された値より低い場合、クライアントは指定遷移時間内により強い信号のあるアクセス ポイントへローミングできる必要があります。このパラメータはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。 RSSI 値を -50 ～ -90 dBm の範囲で設定できます。また、デフォルト値は -72 dBm です。 • [Transition Time]：クライアントのアソシエートされたアクセス ポイントからの RSSI がスキャンしきい値より低くなった場合に、クライア

	コマンドまたはアクション	目的
		ントがローミングに適した近傍のアクセス ポイントの検出およびローミングにかけられる最大許容時間を示します。 [Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータを使用すると、最も高いクライアント速度とローミング ヒステリシスが得られるだけでなく、アクセス ポイント間の一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。 1 ～ 5 秒の範囲で時間を設定できます。デフォルトの時間は5秒です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

モビリティ Oracle の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless mobility oracle** 例： `Device(config)# wireless mobility oracle`	コントローラのモビリティ Oracle をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

モビリティ コントローラの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless mobility controller** 例： `Device(config)# wireless mobility controller`	ワイヤレス モビリティ コントローラをイネーブルにします。
ステップ 3	**wireless mobility controller peer-group** *switch-peer-group-name* 例： `Device(config)# wireless mobility controller peer-group SPG1`	スイッチ ピア グループ名を設定します。グループ名には、最大 31 文字の印字可能な ASCII 文字（大文字小文字が区別されます）を入力できます。モビリティ グループ名には、スペースは使用できません。 （注） このコマンドの **No** 形式を使用すると、スイッチ ピア グループを削除します。
ステップ 4	**wireless mobility controller peer-group** *switch-peer-group-name* **member ip** *ip-address* {**public-ip** *public-ip-address*} 例： `Device(config)# wireless mobility controller peer-group SPG1 member ip 10.0.0.1`	スイッチ ピア グループにモビリティ グループ メンバを追加します。 （注） このコマンドの **No** 形式を使用すると、スイッチ ピア グループからメンバを削除します。

	コマンドまたはアクション	目的
ステップ 5	**wireless mobility controller peer-group** *switch-peer-group-name* **multicast** 例： `Device(config)# wireless mobility controller peer-group SPG1 multicast`	スイッチ ピア グループ内でマルチキャスト モードを設定します。
ステップ 6	**wireless mobility controller peer-group** *switch-peer-group-name* **multicast ip** *peer-group-multicast-ip-addr* 例： `Device(config)# wireless mobility controller peer-group SPG1 multicast ip 10.0.0.4`	スイッチ ピア グループのマルチキャスト IP アドレスを設定します。 （注） このコマンドの **No** 形式を使用すると、スイッチ ピア グループからマルチキャスト IP を削除します。
ステップ 7	**wireless mobility controller peer-group***switch-peer-group-name* **bridge-domain-id** *id* 例： `Device(config)# wireless mobility controller peer-group SPG bridge-domain-id 10.0.0.5`	スイッチ ピア グループのブリッジ ドメイン ID を設定します。デフォルトは 0 です。 （注） このコマンドの **No** 形式を使用すると、ブリッジ ドメイン ID をデフォルトの値に設定します。
ステップ 8	**wireless mobility group member ip** *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*] 例： `Device(config)# wireless mobility group member ip 10.0.0.1`	モビリティ グループ メンバを追加します。 （注） このコマンドの **No** 形式を使用すると、グループからメンバを削除します。デフォルトのグループ名は MC のグループ名です。
ステップ 9	**wireless mobility dscp** *value* 例： `Device(config)# wireless mobility dscp 46`	モビリティ制御パケットの DSCP 値を設定します。 DSCP 値に指定できる範囲は 0 ～ 63 です。デフォルト値は 46 です。
ステップ 10	**wireless mobility group keepalive** {*count* | *interval*} 例： `Device(config)# wireless mobility group keepalive count`	ワイヤレス モビリティ グループのキープアライブ数（メンバのステータスが DOWN するまでのキープアライブの試行回数、および 2 つのキープアライブ間の間隔であるキープアライブ インターバル）を設定します。

	コマンドまたはアクション	目的
ステップ 11	**wireless mobility group name** *name* 例： `Device(config)# wireless mobility group name group1`	最大 31 文字の印字可能な ASCII 文字（大文字小文字が区別されます）で、ワイヤレスモビリティグループ名を指定します。
ステップ 12	**wireless mobility oracle ip***mo-ip-address* 例： `Device(config)# wireless mobility oracle ip 10.0.0.5`	Mobility Oracle に IP アドレスを設定します。
ステップ 13	**wireless management interface** *interface-name* 例： `Device(config)# wireless management interface Vlan21`	ワイヤレス管理インターフェイスを設定します。
ステップ 14	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

例

モビリティ エージェントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless mobility controller ip** *ip-address* 例： `Device(config)# wireless mobility controller ip 10.10.10.20`	モビリティ コントローラの IPアドレスを設定します。
ステップ 3	**wireless mobility load-balance** 例： `Device(config)# wireless mobility load-balance`	ワイヤレス モビリティ ロード バランシングを設定します。

	コマンドまたはアクション	目的
ステップ 4	**wireless mobility load-balance threshold** *threshold-value* 例： `Device(config)# wireless mobility load-balance threshold 100`	ローカル、または MA にアンカーできるクライアント数を設定します。100～2000 の範囲でしきい値を設定できます。デフォルト値は 1000 です。
ステップ 5	**wireless management interface** *interface-name* 例： `Device(config)# wireless management interface Vlan21`	モビリティ エージェントのワイヤレス管理インターフェイスを設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

クライアントのローミング パラメータのモニタリング

このセクションでは、クライアント パラメータ用の新しいコマンドについて説明します。

次のコマンドが のクライアント ローミング パラメータをモニタするために使用できます。

表 *185 :* クライアント ローミング パラメータ モニタリング コマンド

コマンド	目的
show ap dot11 {5ghz | 24ghz} l2roam rf-param	802.11a または 802.11b/g ネットワーク上でクライアント ローミングに設定されている現在の RF パラメータを表示します。
show ap dot11 {5ghz | 24ghz} l2roam statistics	802.11a または 802.11b/g ネットワークの CCX レイヤ 2 クライアント ローミング統計を表示します。
show ap dot11 {5ghz | 24ghz} l2roam mac-address *mac-address* **statistics**	特定のアクセス ポイントの CCX レイヤ 2 クライアント ローミング統計を表示します。

モビリティ設定のモニタ

このセクションでは、モビリティ設定をモニタするための新しいコマンドについて説明します。

次のコマンドは、Mobility Oracle、モビリティ コントローラとモビリティ エージェントのモビリティ設定のモニタリングに使用できます。

表 *186* : モビリティ コントローラおよびモビリティ エージェント用モビリティ設定モニタリング コマンド

コマンド	目的
show wireless mobility summary	モビリティ コントローラとモビリティ エージェントのサマリー情報を表示します。
show wireless mobility statistics	モビリティの統計情報を表示します。
show wireless mobility dtls connections	確立した DTLS 接続を表示します。

表 *187* : *Mobility Oracle* 用モビリティ設定モニタリング コマンド

コマンド	目的
show wireless mobility oracle summary	Mobility Oracle が認識するモビリティ コントローラの状態を表示します。
show wireless mobility oracle client summary	Mobility Oracle データベース内クライアントの情報を表示します。
show wireless mobility oracle client detail *client -mac-address*	Mobility Oracle データベース内の、特定のクライアントの詳細情報を表示します。
show wireless mobility oracle *mc-ip*	指定のモビリティ コントローラにアンカーされている、または関連付けられている Mobility Oracle データベース内クライアント一覧の情報を表示します。

表 *188* : モビリティ コントローラ用モビリティ設定モニタリング コマンド

コマンド	目的
show wireless mobility controller client summary	サブドメインのクライアントのリストを表示します。
show wireless mobility controller client *mac-address***detail**	サブドメインのクライアントに関する詳細情報を表示します。
show wireless mobility agent *ma-ip***client summary**	指定のモビリティ エージェントにアンカーされている、または関連付けられているクライアントのリストを表示します。
show wireless mobility ap-list	モビリティ グループに認識される Cisco AP のリストを表示します。

表 *189*：モビリティ エージェント用モビリティ設定モニタリング コマンド

コマンド	目的
show wireless mobility load-balance summary	モビリティ ロード バランス プロパティの概要を表示します。

クライアント ローミング設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
モビリティ設定	『*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』
モビリティ関連のコマンド	『*Mobility Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

クライアント ローミング設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

第 133 章

有線ネットワークでの Application Visibility and Control の設定

Application Visibility and Control（AVC）は、アプリケーション レベルの分類、モニタリング、およびトラフィック制御による、ビジネス クリティカルなアプリケーション パフォーマンスの改善、容量の管理とプランニングの促進、およびネットワーク運用コストの削減を実現するシスコ ネットワーク デバイスのソリューションです。Cisco AVC ソリューションは、ブランチ ルータおよびアグリゲーション ルータ、シスコ スイッチ、シスコのワイヤレス コントローラおよびアクセス ポイント内で提供されます。

シスコ スイッチでの AVC については、「有線ネットワークでの *Application Visibility and Control* の設定」を参照してください。

シスコのワイヤレス コントローラおよびアクセス ポイントでの AVC については、「*Application Visibility and Control* の設定」を参照してください。

- 機能情報の確認 （2899 ページ）
- 有線ネットワークでの Application Visibility and Control について （2900 ページ）
- サポートされる AVC クラス マップおよびポリシー マップのフォーマット （2900 ページ）
- 有線 Application Visibility and Control の制限 （2902 ページ）
- Application Visibility and Control の設定方法 （2903 ページ）
- Application Visibility and Control のモニタリング （2919 ページ）
- 例：Application Visibility and Control （2920 ページ）
- 基本的なトラブルシューティング（質問と回答） （2922 ページ）
- Application Visibility and Control に関する追加情報 （2923 ページ）
- 有線ネットワークでの Application Visibility and Control の機能履歴と情報 （2924 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

有線ネットワークでの Application Visibility and Control について

Application Visibility and Control（AVC）は、アプリケーションへの適応力やアプリケーションへのインテリジェンス性に基づいて、厳密なパケットおよび接続からブランチおよびキャンパス ソリューションを発展させるためのシスコの取り組みの重要な部分です。Application Visibility and Control（AVC）は、ネットワークベースのアプリケーション認識（NBAR2）エンジンによるディープ パケット インスペクション技術を使用してアプリケーションを分類します。Cisco IOS XE Denali 16.3.1 以降では、有線アクセス ポートでの AVC のサポートが、スタンドアロン スイッチおよびスイッチ スタックに対し有効になっています。NBAR2 は、プロトコル検出を有効にすることによって明示的に、または **match protocol** 分類子を含む QoS ポリシーを接続することによって暗黙的に、インターフェイス上でアクティブにできます。Cisco IOS XE Denali 16.3.2 以降では、基本的な有線 AVC FNF のサポートが有線アクセス ポートで有効になっています。有線 AVC FNF は、インターフェイスごとにクライアント、サーバおよびアプリケーションの統計情報を提供します。レコードは、**application-statistics** および **application-perforrnance** プロファイルで使用可能な ezPM の **application-client-server-stats** トラフィック監視と同様です。

サポートされる AVC クラス マップおよびポリシー マップのフォーマット

サポートされる AVC クラス マップのフォーマット

クラスマップのフォーマット	クラスマップの例	方向
match protocol プロトコル名	`class-map match-any NBAR-VOICE` `match protocol ms-lync-audio`	入力と出力の両方

組み合わせフィルタ	`class-map match-any NBAR-VOICE`
	`match protocol ms-lync-audio`
	`match dscp 45`
		出力のみ

サポートされる AVC ポリシーのフォーマット

ポリシーのフォーマット	QoS 処理
match protocol フィルタに基づく出力ポリシー	マークおよびポリシー

ポリシーのフォーマット	QoS 処理
match protocol フィルタに基づく入力ポリシー	マークおよびポリシー

次の表で、AVC ポリシーの詳細なフォーマット、および例について説明します。

AVC ポリシーのフォーマット	AVC ポリシーの例	方向

ベーシック セット	`policy-map MARKING-IN`
	`class NBAR-MM_CONFERENCING`
	`set dscp af41`
		入力および出力

ベーシック ポリシー	`policy-map POLICING-IN`
	`class NBAR-MM_CONFERENCING`
	`police cir 600000`
	`set dscp af41`
		入力および出力

ベーシック セットおよびポリシー	`policy-map webex-policy`
	` class webex-class`
	` set dscp ef`
	` cos police 5000000`
		入力および出力

デフォルトを含む複数のセットおよびポリシー	`policy-map webex-policy`
	` class webex-class`
	` set dscp af31`
	` cos police 4000000`
	` class class-webex-category`
	` set dscp ef`
	` cos police 6000000`
	` class class-default`
	` set dscp <>`
		入力および出力

階層型ポリシー	`policy-map webex-policy`
	` class webex-class`
	` police 5000000`
	` service-policy client-in-police-only`
	
	` policy-map client-in-police-only`
	` class webex-class`
	` police 100000`
	` class class-webex-category`
	` set dscp ef`
	` cos police 200000`
		入力および出力

階層型セットおよびポリシー	`policy-map webex-policy`
	` class class-default`
	` police 1500000`
	` service policy client-up-child`
	` policy-map webex-policy`
	` class webex-class`
	` police 100000`
	` set dscp ef`
	` class class-webex-category`
	` police 200000`
	` set dscp af31`	

有線 Application Visibility and Control の制限

- NBAR 対応 QoS ポリシー設定は有線物理ポートでのみ許可されます。ポリシー設定は、たとえば、VLAN、ポート チャネル、および他の論理インターフェイスなどの仮想インターフェイスではサポートされていません。
- NBAR2 ベースの一致基準 **match protocol** は、マーキング アクションおよびポリシング アクションでのみ許可されます。NBAR2 一致基準は、キューイング機能が設定されているポリシーでは許可されません。
- 「一致プロトコル」：すべてのポリシーで最大 255 の同時に異なるプロトコル（8 ビットの HW 制限）。
- NBAR2 属性ベースの QOS はサポートされていません（**match protocol** 属性）。
- AVC は管理ポート（Gig 0/0）ではサポートされていません。
- IPv6 パケットの分類はサポートされていません。
- IPv4 ユニキャスト（TCP/UDP）のみがサポートされます。
- Web UI：Web UI からアプリケーションの可視性を設定し、アプリケーションのモニタリングを実行できます。アプリケーション制御は、CLI を使用してのみ実行できます。Web UI ではサポートされていません。
- NBAR および ACL のロギングは、同一スイッチ上で一緒に設定することはできません。
- プロトコル検出、アプリケーション ベースの QoS、および有線 AVC FNF は、非アプリケーション ベース FNF がある同一インターフェイス上で同時に設定することはできません。ただし、これらの有線 AVC 機能は、相互に設定できます。たとえば、プロトコル検出、アプリケーション ベースの QoS、および有線 AVC FNF は、同一インターフェイス上で同時に設定できます。
- Cisco IOS XE Denali 16.3.2 では、**show flow monitor** *flow-monitor-name* **statistics** および **show flow monitor** *flow-monitor-name* **cache** コマンドは有線 AVC にサポートされていません。これらのコマンドは、有線 AVC に固有の情報を表示しません。
- 単一の事前定義されたレコードは、有線 AVC FNF でサポートされています。
- 接続は、物理 Layer2（アクセス/トランク）および Layer3 ポートでのみ行う必要があります。アップリンクは、単一のアップリンクであり、ポートチャネルの一部でなければ接続できます。
- パフォーマンス：各スイッチ メンバーは、50% 未満の CPU 使用率で、1 秒あたり 500 の接続（CPS）を処理できます。
- 拡張性：48 個のアクセス ポートごとに最大 10,000 の双方向フローと、24 個のアクセス ポートごとに 5000 の双方向フローを処理できます。（アクセス ポートごとに～ 200 フロー）。

Application Visibility and Control の設定方法

有線ネットワークでの Application Visibility and Control の設定

有線ポートで Application Visibility and Control を設定するには、次の手順を実行します。

可視性の設定

- インターフェイス コンフィギュレーション モードで **ip nbar protocol-discovery** コマンドを使用してインターフェイス上でプロトコル検出を有効にすることで、NBAR2 エンジンをアクティブ化します。インターフェイスでのアプリケーション認識の有効化 （2903 ページ） を参照してください。

制御設定：次の手順に従って、アプリケーションに基づいて QoS ポリシーを設定します。

1. AVC QoS ポリシーの作成。AVC QoS ポリシーの作成 （2904 ページ） を参照してください。
2. インターフェイスへの AVC QoS ポリシーの適用。スイッチ ポートへの QoS ポリシーの適用 （2907 ページ） を参照してください。

アプリケーション ベースの Flexible Netflow の設定：

- フローにキー フィールドおよび非キー フィールドを指定して、フロー レコードを作成します。フロー レコードの作成 （2908 ページ） を参照してください。
- フローエクスポータを作成してフロー レコードをエクスポートします。フローエクスポータの作成 （2911 ページ） を参照してください。
- フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを作成します。フロー モニタの作成 （2912 ページ） を参照してください。
- インターフェイスにフロー モニタを接続します。インターフェイスへのフロー モニタの関連付け （2913 ページ） を参照してください。

プロトコル検出、アプリケーション ベースの QoS およびアプリケーション ベースの FNF は、すべて独立した機能です。単独で設定することも、または同じインターフェイスで同時に設定することもできます。

インターフェイスでのアプリケーション認識の有効化

インターフェイス上でアプリケーション認識をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	プロトコル検出をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip nbar protocol-discovery** 例： `Device(config-if)# ip nbar protocol-discovery`	NBAR2 エンジンをアクティブ化することで、インターフェイスでアプリケーション認識を有効にします。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

AVC QoS ポリシーの作成

AVC QoS ポリシーを作成するには、次の一般的な手順を実行します。

1. match protocol フィルタでクラス マップを作成します。
2. ポリシー マップを作成します。
3. インターフェイスにポリシー マップを適用します。

クラス マップの作成

match protocol フィルタを設定する前に、クラス マップを作成する必要があります。マーキングやポリシングなどの QoS アクションをトラフィックに適用できます。AVC の match protocol フィルタは、有線アクセス ポートに適用されます。サポートされているプロトコルの詳細については、http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** *class-map-name* 例： `Device(config)# class-map webex-class`	クラス マップを作成します。

ステップ 3	**match protocol** *application-name*
	例：
	`Device(config)# class-map webex-class`
	`Device(config-cmap)# match protocol webex-media`
		アプリケーション名との一致を指定します。

ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシー マップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map** *policy-map-name* 例： `Device(config)# policy-map webex-policy`	ポリシーマップ名を入力することによってポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。

	コマンドまたはアクション	目的
		（注） 既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**class** [*class-map-name* | **class-default**] 例： `Device(config-pmap)# class webex-class`	トラフィックの分類を定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップおよびクラスマップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **class-default** トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシーマップの最後に配置されます。暗黙の **match any** が **class-default** クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは **class-default** と一致します。 （注） 既存のクラス マップを削除するには、**no class** *class-map-name* ポリシー マップ コンフィギュレーション コマンドを使用します。
ステップ 4	**police** *rate-bps burst-byte* 例： `Device(config-pmap-c)# police 100000 80000`	分類したトラフィックにポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。指定できる範囲は 8000 ～ 10000000000 です

	コマンドまたはアクション	目的
		• *burst-byte* には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ～ 1000000 です。
ステップ 5	**set** { **dscp** *new-dscp* | **cos** *cos-value* } 例： `Device(config-pmap-c)# set dscp 45`	パケットに新しい値を設定することによって、IP トラフィックを分類します。 • **dscp** *new-dscp* には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

スイッチ ポートへの QoS ポリシーの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface Gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**service-policy input** *policymapname* 例： `Device(config-if)# service-policy input MARKING_IN`	インターフェイスにローカル ポリシーを適用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

有線 AVC Flexible Netflow の設定

フロー レコードの作成

1 つのフロー レコードを設定して、フロー モニタに関連付けることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flowrecord** *flow_record_name* 例： `Device(config)# flow record flow-record-1`	フロー レコードコンフィギュレーション モードを開始します。
ステップ 3	**description** 説明 例： `Device(config-flow-record)# description flow-record-1`	（任意）フロー レコードの説明を作成します。
ステップ 4	**matchipv4version** 例： `Device (config-flow-record)# match ipv4 version`	IPv4 ヘッダーからの IP バージョンとの一致を指定します。
ステップ 5	**matchipv4protocol** 例： `Device (config-flow-record)# match ipv4 protocol`	IPv4 プロトコルとの一致を指定します。
ステップ 6	**matchapplicationname** 例： `Device (config-flow-record)# match application name`	アプリケーション名との一致を指定します。 （注） この操作は、AVC サポートでは必須です。フローがアプリケーションと一致することが可能になるためです。
ステップ 7	**match connection client ipv4 address** 例： `Device (config-flow-record)# match connection client ipv4 address`	クライアント（フローイニシエータ）の IPv4 アドレスとの一致を指定します。

	コマンドまたはアクション	目的
ステップ 8	**match connection server ipv4 address** 例： `Device (config-flow-record)# match connection server ipv4 address`	サーバ（フロー レスポンダ）の IPv4 アドレスとの一致を指定します。
ステップ 9	**match connection server transport port** 例： `Device (config-flow-record)# match connection server transport port`	サーバのトランスポートポートとの一致を指定します。
ステップ 10	**match flow observation point** 例： `Device (config-flow-record)# match flow observation point`	フロー観測メトリックの観測ポイント ID との一致を指定します。
ステップ 11	**collect flow direction** 例： `Device (config-flow-record)# collect flow direction`	次の手順で **collect connection initiator** コマンドの **initiator** キーワードで指定される双方向フローの関連する側（イニシエータまたはレスポンダ）の方向（入力または出力）を収集するように指定します。**initiator** キーワードで指定される値に応じて、**flow direction** キーワードは次の値をとります。 • 0x01 = 入力フロー • 0x02 = 出力フロー **initiator** キーワードがイニシエータに設定されている場合、フローの方向はフローのイニシエータ側から指定されます。initiator キーワードがレスポンダに設定されている場合、フローの方向はフローのレスポンダ側から指定されます。有線 AVC では、**initiator** キーワードは常にイニシエータに設定されています。
ステップ 12	**collect connection initiator** 例： `Device (config-flow-record)# collect connection initiator`	**collect flow direction** コマンドで指定されたフローの方向に関連するフローの側（イニシエータまたはレスポンダ）を収集するように指定します。**initiator** キーワードは、フローの方向に関する次の情報を提供します。

	コマンドまたはアクション	目的
		• 0x01 = イニシエータ：フローの送信元は接続のイニシエータです 有線 AVC では、**initiator** キーワードは常にイニシエータに設定されています。
ステップ 13	**collect connection client counter packets long** 例： `Device (config-flow-record)# collect connection client counter packets long`	クライアントが送信したパケット数を収集するように指定します。
ステップ 14	**collect connection client counter bytes network long** 例： `Device (config-flow-record)# collect connection client counter bytes network long`	クライアントが送信したバイト数の合計を収集するように指定します。
ステップ 15	**collect connection server counter packets long** 例： `Device (config-flow-record)# collect connection server counter packets long`	サーバが送信したパケット数を収集するように指定します。
ステップ 16	**collect connection server counter bytes network long** 例： `Device (config-flow-record)# collect connection server counter bytes network long`	サーバが送信したバイト数の合計を収集するように指定します。
ステップ 17	**collect timestamp absolute first** 例： `Device (config-flow-record)# collect timestamp absolute first`	最初のパケットがフローで確認されたときの時間をミリ秒単位で収集するように指定します。
ステップ 18	**collect timestamp absolute last** 例： `Device (config-flow-record)# collect timestamp absolute last`	最新のパケットがフローで確認されたときの時間をミリ秒単位で収集するように指定します。
ステップ 19	**collect connection new-connections** 例：	観測された接続開始の数を収集するように指定します。

	コマンドまたはアクション	目的
	`Device (config-flow-record)# collect connection new-connections`	
ステップ 20	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 21	**show flow record** 例： `Device # show flow record`	すべてのフロー レコードに関する情報を表示します。

フロー エクスポータの作成

フロー エクスポータを作成すると、フローのエクスポート パラメータを定義できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flowexporter** *flow_exporter_name* 例： `Device(config)# flow exporter flow-exporter-1`	フロー エクスポータ コンフィギュレーション モードを開始します。
ステップ 3	**description** 説明 例： `Device(config-flow-exporter)# description flow-exporter-1`	（任意）フロー エクスポータの説明を作成します。
ステップ 4	**destination** { *hostname* | *ipv4-address* | *ipv6-address* } 例： `Device (config-flow-exporter)# destination 10.10.1.1`	エクスポータでデータを送信する宛先システムのホスト名、IPv4 または IPv6 アドレスを指定します。
ステップ 5	**option application-table** [**timeout** *seconds*] 例： `Device (config-flow-exporter)# option application-table timeout 500`	（任意）フロー エクスポータのアプリケーション テーブルのオプションを設定します。**timeout** オプションを使用すると、フロー エクスポータの再送信時間を秒単位で設定できます。有効な範囲は 1 ～ 86400 秒です。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 7	**show flow exporter** 例： `Device # show flow exporter`	すべてのフロー エクスポータに関する情報を表示します。
ステップ 8	**show flow exporter statistics** 例： `Device # show flow exporter statistics`	フロー エクスポータの統計情報を表示します。

フロー モニタの作成

フロー モニタを作成して、フロー レコードに関連付けることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flow monitor** *monitor-name* 例： `Device (config)# flow monitor flow-monitor-1`	フロー モニタを作成し、フロー モニタ コンフィギュレーション モードを開始します。
ステップ 3	**description** 説明 例： `Device (config-flow-monitor)# description flow-monitor-1`	（任意）フロー モニタの説明を作成します。
ステップ 4	**record** *record-name* 例： `Device (config-flow-monitor)# record flow-record-1`	事前に作成されたレコードの名前を指定します。
ステップ 5	**exporter** *exporter-name* 例： `Device (config-flow-monitor)# exporter flow-exporter-1`	事前に作成されたエクスポータの名前を指定します。

	コマンドまたはアクション	目的

ステップ 6	**cache type normal** ｛ **timeout** ｛**active** ｜ **inactive**｝ ｜ **type normal** ｝
	例：
	`Device (config-flow-monitor)# cache timeout active 1800`
	例：
	`Device (config-flow-monitor)# cache timeout inactive 200`
	例：
	`Device (config-flow-monitor)# cache type normal`
		（任意）フロー キャッシュ パラメータを設定するように指定します。
		（注） 標準のキャッシュ タイプのみがサポートされます。キャッシュ サイズの設定はサポートされません。キャッシュには、一定サイズ 10,000 が事前定義されています。

ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show flow monitor** 例： `Device # show flow monitor`	すべてのフロー モニタに関する情報を表示します。 （注） **show flow monitor** *flow-monitor-name* **statistics** and **show flow monitor** *flow-monitor-name* **cache** commands are not supported for wired AVC.これらのコマンドは、有線 AVC に固有の情報を表示しません。**show flow exporter statistics** コマンドは、フロー モニタの統計情報を表示する **show flow monitor** *flow-monitor-name* **cache** コマンドの限定された代替手段として使用できます。

インターフェイスへのフロー モニタの関連付け

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface Gigabitethernet 1/0/1`	インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	**ip flow monitor** *monitor-name*{ **input** | **output** } 例： `Device (config-if) # ip flow monitor flow-monitor-1 input`	入力パケットと出力パケットの両方またはいずれか用のインターフェイスにフロー モニタを関連付けます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

NBAR2 カスタム アプリケーション

NBAR2 では、カスタム プロトコルを使用してカスタム アプリケーションを識別できます。カスタム プロトコルは、プロトコルとアプリケーションをサポートしますが、現在のところ、NBAR2 はサポートしていません。

すべての展開において、シスコが提供する NBAR2 プロトコル パックの対象外であるローカル アプリケーションおよび特定のアプリケーションがあります。ローカルアプリケーションは主に次のように分類されます。

- 組織への特定のアプリケーション
- 地域特有のアプリケーション

NBAR2 では、このようなローカル アプリケーションを手動でカスタマイズする方法を提供しています。グローバル コンフィギュレーション モードで **ip nbar custom** *myappname* コマンドを使用して、手動でアプリケーションをカスタマイズできます。カスタム アプリケーションは、組み込みプロトコルより優先されます。それぞれのカスタムプロトコルでは、ユーザは、レポート目的に使用できるセレクタ ID を定義できます。

さまざまなタイプのアプリケーション カスタマイズがあります。

一般的なプロトコルのカスタマイズ

- HTTP
- SSL
- DNS

コンポジット：複数の基本的なプロトコルに基づくカスタマイズ： **server-name**

レイヤ 3/レイヤ 4 のカスタマイズ

- IPv4 アドレス
- DSCP 値
- TCP/UDP ポート
- フロー送信元または宛先の方向

バイト オフセット：ペイロードの特定のバイト値に基づくカスタマイズ

HTTP のカスタマイズ

HTTP のカスタマイズは、次の HTTP フィールドの組み合わせに基づいて実行できます。

- **cookie** ：HTTP クッキー
- **host** ：リソースを含む元のサーバのホスト名
- **method** ：HTTP メソッド
- **referrer** ：リソース リクエストの取得元のアドレス
- **url** ：Uniform Resource Locator のパス
- **user-agent** ：要求を送信するエージェントによって使用されているソフトウェア
- **version** ：HTTP バージョン
- **via** ：HTTP 経由フィールド

HTTP のカスタマイズ

セレクタ ID 10 が付いた HTTP ホスト「*mydomain.com」を使用する MYHTTP と呼ばれるカスタム アプリケーション。

```
Device# configure terminal
Device(config)# ip nbar custom MYHTTP http host *mydomain.com id 10
```

SSL のカスタマイズ

SSL サーバ名指定（SNI）または共通名（CN）から抽出した情報を使用して、SSL 暗号化トラフィックでカスタマイズを行うことができます。

SSL のカスタマイズ

セレクタ ID 11 が付いた SSL 固有名「mydomain.com」を使用する MYSSL と呼ばれるカスタム アプリケーション。

```
Device# configure terminal
Device(config)#ip nbar custom MYSSL ssl unique-name *mydomain.com id 11
```

DNS のカスタマイズ

NBAR2 は、DNS 要求および応答トラフィックを確認し、アプリケーションへの DNS 応答に関連付けることができます。DNS 応答から戻された IP アドレスはキャッシュされ、その特定のアプリケーションに関連付けられているその後のパケット フローに使用されます。

ip nbar custom *application-name* **dns** *domain-name* **id** *application-id* コマンドは、DNS のカスタマイズに使用されます。既存のアプリケーションを拡張するには、**ip nbar custom** *application-name* **dns domain-name** *domain-name* **extends** *existing-application* コマンドを使用します。

DNS ベースのカスタマイズの詳細については、http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/xe-3s/asr1000/qos-nbar-xe-3s-asr-1000-book/nbar-custapp-dns-xe.html を参照してください。

DNS のカスタマイズ

セレクタ ID 12 が付いた DNS ドメイン名「mydomain.com」を使用する MYDNS と呼ばれるカスタム アプリケーション。

```
Device# configure terminal
Device(config)# ip nbar custom MYDNS dns domain-name *mydomain.com id 12
```

複合カスタマイズ

NBAR2 では、HTTP、SSL または DNS に現れるドメイン名に基づいてアプリケーションをカスタマイズする方法が提供されます。

複合カスタマイズ

セレクタ ID 13 が付いた HTTP、SSL または DNS ドメイン名「mydomain.com」を使用する MYDOMAIN と呼ばれるカスタム アプリケーション。

```
Device# configure terminal
Device(config)# ip nbar custom MYDOMAIN composite server-name *mydomain.com id 13
```

L3/L4 のカスタマイズ

レイヤ3/レイヤ4のカスタマイズは、パケットタプルに基づいており、フローの最初のパケットで常に一致します。

L3/L4 のカスタマイズ

IP アドレス 10.56.1.10 および 10.56.1.11、セレクタ ID 14 が付いた TCP および DSCP ef に一致する LAYER4CUSTOM と呼ばれるカスタム アプリケーション。

```
Device# configure terminal
Device(config)# ip nbar custom LAYER4CUSTOM transport tcp id 14
```

```
Device(config-custom)# ip address 10.56.1.10 10.56.1.11
Device(config-custom)# dscp ef
```

例：カスタム アプリケーションのモニタリング

カスタム アプリケーションのモニタリングのための show コマンド

show ip nbar protocol-id | inc Custom

```
Device# show ip nbar  protocol-id | inc Custom
LAYER4CUSTOM                14              Custom
MYDNS                       12              Custom
MYDOMAIN                    13              Custom
MYHTTP                      10              Custom
MYSSL                       11              Custom
```

show ip nbar protocol-discovery protocol *CUSTOM_APP*

```
WSW-157# show ip nbar  protocol-id MYSSL
Protocol Name               id              type
-----------------------------------------------
MYSSL                       11              Custom
```

NBAR2 ダイナミック ヒットレス プロトコル パックのアップグレード

プロトコル パックは、デバイスのシスコ ソフトウェアを置き換えることなく、デバイスの NBAR2 プロトコル サポートを更新するソフトウェア パッケージです。プロトコル パックには、NBAR2 によって正式にサポートされている、コンパイル済みでパック済みのアプリケーションに関する情報が含まれています。各アプリケーションについて、プロトコル パックには、アプリケーション署名とアプリケーション属性の情報が含まれています。各ソフトウェア リリースには、組み込みのプロトコル パックがバンドルされています。

プロトコル パックには次の特長があります。

- ロードが容易で高速。
- 高いバージョンのプロトコルパックにアップグレードしたり、低いバージョンのプロトコル パックに戻したりするのが容易。
- スイッチのリロードを必要としない。

NBAR2 プロトコル パックは、次の URL から Cisco Software Center でダウンロードできます：https://software.cisco.com/download/navigator.html

NBAR2 プロトコル パックの前提条件

新しいプロトコル パックをロードする前に、すべてのスイッチ メンバー上でプロトコル パックをフラッシュにコピーする必要があります。

プロトコルパックをロードするには、例：NBAR2プロトコルパックのロード（2919ページ）を参照してください。

NBAR2 プロトコル パックのロード

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**ipnbarprotocol-pack** *protocol-pack* [**force**]
	例：
	`Device(config)# ip nbar protocol-pack flash:defProtoPack`
	例：
	`Device(config)# default ip nbar protocol-pack`
		プロトコル パックをロードします。
		• 基本のプロトコル パック バージョンとは異なる、より低いバージョンのプロトコルパックを指定し、ロードするには、**force** キーワードを使用します。これにより、スイッチの現在のプロトコル パックでサポートされていない設定も削除されます。
		組み込みのプロトコル パックに戻るには、次のコマンドを使用します。

ステップ 4	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**showipnbarprotocol-pack** {protocol-pack | **active**} [**detail**] 例： `Device# show ip nbar protocol-pack active`	プロトコル パック情報を表示します。 • このコマンドを使用して、ロードされたプロトコル パックのバージョン、パブリッシャ、その他の詳細を確認します。 • 指定されたプロトコル パックの情報を表示するには、*protocol-pack* 引数を使用します。

	コマンドまたはアクション	目的
		• アクティブなプロトコル パックの情報を表示するには、**active** キーワードを使用します。 • 詳細なプロトコル パックの情報を表示するには、**detail** キーワードを使用します。

例：NBAR2 プロトコル パックのロード

次の例に、新しいプロトコル パックをロードする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip nbar protocol-pack flash:newDefProtoPack
Device(config)# exit
```

次の例に、**force** キーワードを使用して下位バージョンのプロトコル パックをロードする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip nbar protocol-pack flash:OldDefProtoPack force
Device(config)# exit
```

次の例に、組み込みのプロトコル パックに戻す方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# default ip nbar protocol-pack
Device(config)# exit
```

Application Visibility and Control のモニタリング

Application Visibility and Control のモニタリング（CLI）

このセクションでは、アプリケーションの可視性に関する新しいコマンドについて説明します。

次のコマンドは、およびアクセス ポートのアプリケーションの可視性をモニタするために使用できます。

表 *190：* のアプリケーションの可視性モニタリング コマンド

コマンド	目的

show ip nbar protocol-discovery [**interface** *interface-type interface-number*] [**stats** {**byte-count** | **bit-rate** | **packet-count** | **max-bit-rate**}] [**protocol** *protocol-name* | **top-n** *number*]	NBAR Protocol Discovery 機能によって収集された統計情報を表示します。 • （任意）表示される統計情報を最適化するには、キーワードおよび引数を入力します。キーワードのそれぞれの詳細については、『Cisco IOS Quality of Service Solutions Command Reference』の**show ip nbar protocol-discovery** コマンドを参照してください。
show policy-map interface *interface-type interface-number*	インターフェイスに適用したポリシー マップについての情報を表示します。
show platform software fed switch スイッチ *ID* **wdavc flows**	指定したスイッチのすべてのフローに関する統計情報を表示します。

例：Application Visibility and Control

例：Application Visibility and Control の設定

次に、match protocol でアプリケーション名のフィルタを適用してクラス マップを作成する例を示します。

```
Device# configure terminal
Device(config)# class-map match-any NBAR-VOICE
Device(config-cmap)# match protocol ms-lync-audio
Device(config-cmap)#end
```

次に、ポリシー マップを作成し、出力 QoS の既存のクラス マップを定義する例を示します。

```
Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 150000
Device(config-pmap-c)# set dscp 12
Device(config-pmap-c)#end
```

次に、ポリシー マップを作成し、入力 QoS の既存のクラス マップを定義する例を示します。

```
Device# configure terminal
Device(config)# policy-map test-avc-down
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 200000
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)#end
```

次に、ポリシー マップをスイッチ ポートに適用する例を示します。

```
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 20
```

```
Device(config-if)# service-policy type control subscriber POLICING_IN
Device(config-if)#end
```

show コマンドによる設定の表示

show ip nbar protocol-discovery

インターフェイスごとのプロトコル検出統計情報のレポートを表示します。

次に、インターフェイスごとの統計情報の出力例を示します。

```
Deviceqos-cat3k-reg2-r1# show ip nbar protocol-discovery int GigabitEthernet1/0/1
GigabitEthernet1/0/1

Last clearing of "show ip nbar protocol-discovery" counters 00:03:16

                                   Input
Output
                                   -----
------
Protocol                           Packet Count
Packet Count
                                   Byte Count
Byte Count
                                   30sec Bit Rate (bps)
30sec Bit Rate (bps)
                                   30sec Max Bit Rate (bps)
30sec Max Bit Rate (bps)
------------------------ ------------------------
-----------------------------------------------------
ms-lync                            60580
55911
                                   31174777
28774864
                                   3613000
93000
                                   3613000
3437000
Total                              60580
55911
                                   31174777
28774864
                                   3613000
93000
                                   3613000
3437000
```

show policy-map interface

すべてのインターフェイス上のQoS統計情報および設定済みのポリシーマップを表示します。

次に、すべてのインターフェイスに設定されたポリシー マップの出力例を示します。

```
Deviceqos-cat3k-reg2-r1# show policy-map int
GigabitEthernet1/0/1
```

```
Service-policy input: MARKING-IN

  Class-map: NBAR-VOICE (match-any)
    718 packets
    Match: protocol ms-lync-audio
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp ef

  Class-map: NBAR-MM_CONFERENCING (match-any)
    6451 packets
    Match: protocol ms-lync
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol ms-lync-video
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp af41

  Class-map: class-default (match-any)
    34 packets
    Match: any
```

基本的なトラブルシューティング（質問と回答）

以下に、有線 Application Visibility and Control のトラブルシューティングに関する基本的な質問と回答を示します。

1. **質問**：IPv6 トラフィックが分類されていません。

   回答：現在は IPv4 トラフィックのみがサポートされています。

2. **質問**：マルチキャスト トラフィックが分類されていません。

   回答：現在はユニキャスト トラフィックのみがサポートされています。

3. **質問**：ping を送信したときに、分類されているかを確認できません。

   回答：TCP/UDP プロトコルのみがサポートされています。

4. **質問**：SVI に NBAR を接続できないのはなぜですか。

   回答：NBAR は物理インターフェイスでのみサポートされています。

5. **質問**：ほどんとのトラフィックが CAPWAP トラフィックになっているのですが、なぜですか。

   回答：ワイヤレス アクセス ポートに接続されていないアクセス ポートで NBAR が有効になっていることを確認してください。AP から着信するすべてのトラフィックは capwap として分類されます。この場合、実際の分類は AP または WLC で行われます。

6. **質問**：プロトコル検出で、トラフィックが片側でしか確認できません。さらに、多くの未知のトラフィックがあります。

   回答：これは通常、NBAR が非対称トラフィックを確認していることを示します。片側のトラフィックは 1 つのスイッチ メンバーに分類され、もう一方は別のメンバーに分類されます。トラフィックの両側が確認されるアクセス ポートにのみNBARを接続することを推奨します。複数のアップリンクがある場合は、この問題のためそれらにNBARを接続することはできません。ポート チャネルの一部であるインターフェイスにNBARを設定した場合にも同様の問題が発生します。

7. **質問**：プロトコル検出で、すべてのアプリケーションの集約ビューが表示されます。時間経過に伴うトラフィック分布を確認するにはどうしたらいいですか。

   回答：WebUI を使用して、過去 48 時間の経時的なトラフィックを表示できます。

8. **質問**：**match protocol** *protocol-name* コマンドを使用してキューベースのイーグレス ポリシーを設定できません。

   回答：NBAR2 ベースの分類子が含まれるポリシーでは、**shape** および **set DSCP** のみがサポートされています。一般的な方法としては、入力で DSCP を設定し、DSCP に基づいて出力でシェーピングを実行します。

9. **質問**：インターフェイスに接続しているNBAR2はありませんが、NBAR2がいまだにアクティブになっています。

   回答：**match protocol** *protocol-name* を含むクラス マップがあると、NBAR はスタックでグローバルにアクティブになりますが、トラフィックはNBAR分類の対象にはなりません。これは予期された動作であり、リソースを消費しません。

10. **質問**：デフォルトの QOS キューの下にトラフィックがあります。どうしてですか。

    回答：新しい各フローでは、フローを分類してハードウェアに結果をインストールするためにいくつかのパケットが使われます。この間に、分類は「不明」となり、トラフィックはデフォルト キューに入ります。

Application Visibility and Control に関する追加情報

関連資料

関連項目	マニュアル タイトル
QoS	*NBAR Configuration Guide, Cisco IOS XE 16*
NBAR2プロトコル パック ヒットレス アップグレード	*NBAR Configuration Guide, Cisco IOS XE 16*

シスコのテクニカル サポート

説明	リンク
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

有線ネットワークでの Application Visibility and Control の機能履歴と情報

リリース	機能情報
Cisco IOS XE Denali 16.3.1	この機能が導入されました。

第 134 章

ワイヤレス ネットワークでの Application Visibility and Control の設定

Application Visibility and Control（AVC）は、アプリケーション レベルの分類、モニタリング、およびトラフィック制御による、ビジネス クリティカルなアプリケーション パフォーマンスの改善、容量の管理とプランニングの促進、およびネットワーク運用コストの削減を実現するシスコ ネットワーク デバイスのソリューションです。Cisco AVC ソリューションは、ブランチ ルータおよびアグリゲーション ルータ、シスコ スイッチ、シスコのワイヤレス コントローラおよびアクセス ポイント内で提供されます。

シスコ スイッチでの AVC については、「有線ネットワークでの *Application Visibility and Control* の設定」を参照してください。

シスコのワイヤレス コントローラおよびアクセス ポイントでの AVC については、「ワイヤレス ネットワークでの *Application Visibility and Control* の設定」を参照してください。

- 機能情報の確認 （2926 ページ）
- Application Visibility and Control について （2926 ページ）
- サポートされる AVC クラスマップおよびポリシーマップのフォーマット （2927 ページ）
- Application Visibility and Control の前提条件 （2929 ページ）
- Application Visibility and Control によるDevice間ローミングに関するガイドライン （2930 ページ）
- Application Visibility and Control の制限 （2930 ページ）
- Application Visibility and Control の設定方法 （2932 ページ）
- Application Visibility and Control のモニタリング （2946 ページ）
- 例：Application Visibility and Control （2948 ページ）
- Application Visibility and Control に関する追加情報 （2950 ページ）
- Application Visibility and Control の機能履歴と情報 （2952 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

Application Visibility and Control について

Application Visibility and Control（AVC）は、ネットワークベースのアプリケーション認識エンジンによるディープ パケット インスペクション技法でアプリケーションを分類し、無線ネットワークにアプリケーション レベルの可視性と制御（QoS）を提供します。アプリケーションの認識後は、AVC 機能によってデータ トラフィックをドロップ、マーク、またはポリシングできます。

AVC はプロトコルと一致するように QoS クライアント ポリシー内のクラス マップを定義することによって設定されます。

AVC を使用して、1000 以上のアプリケーションを検出できます。AVC により、リアルタイム分析を実施し、ネットワークの輻輳、コストの掛かるネットワーク リンクの使用、およびインフラストラクチャの更新を削減するためのポリシーを作成することができるようになります。

（注） UI の [Monitor Summary] セクションで、[Top Applications] に 30 のアプリケーションのリストを表示できます。

トラフィック フローは、アクセス ポイントの NBAR2 エンジンを通して分析および認識されます。NBAR2 プロトコル ライブラリの詳細については、http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.htmlを参照してください。特定のフローが WebEx などの認識されたプロトコルまたはアプリケーションでマークされます。このフロー単位の情報は Flexible NetFlow（FNF）によるアプリケーションの可視化に使用できます。

AVC QoS アクションは、AVC フィルタを通してアップストリームとダウンストリームの両方向に適用されます。アップストリーム フローに対してサポートされる QoS アクションはドロップ、マーク、およびポリシングで、ダウンストリーム フローに対してサポートされるアクションはマークとポリシングです。AVC QoS は、アプリケーションが正しく分類され、ポリシー マップ内のクラス マップ フィルタに一致する場合にだけ適用できます。たとえば、ポリシーにアプリケーション名に基づくフィルタが含まれており、トラフィックも同じアプリケーション名に分類されている場合は、ポリシー内でこの一致に対して指定されたアクションが適用さ

れます。すべての QoS アクションについては、サポートされる AVC クラス マップおよびポリシー マップのフォーマット （2927 ページ）を参照してください。

Application Visibility and Control プロトコル パック

プロトコル パックとは、 スイッチ ソフトウェアのリリース トレーニング以外のプロトコル アップデートを配布する方法です。 スイッチ ソフトウェアを交換せずに スイッチにロードできます。

Application Visibility and Control プロトコル パック（AVC プロトコル パック）は、複数のプロトコル記述言語（PDL）ファイルとマニフェスト ファイルを含む単一の圧縮ファイルです。必要なプロトコルのセットをロードすることができ、ネットワークでの分類のために追加プロトコルを認識する際に役立ちます。マニフェスト ファイルは、プロトコル パックの名前、バージョン、およびプロトコル パック内の利用可能な PDL の情報など、プロトコル パックに関する情報を提供します。

AVC プロトコル パックは、特定の AVC エンジン バージョン向けにリリースされています。スイッチ プラットフォームのエンジン バージョンがプロトコル パックに必要なバージョン以降であれば、プロトコル パックをロードできます。

サポートされる AVC クラス マップおよびポリシー マップのフォーマット

サポートされる AVC クラス マップのフォーマット

クラス マップのフォーマット	クラスマップの例	方向
match protocol プロトコル名	`class-map match-any webex-class` `match protocol webex-media`	アップストリームおよびダウンストリームの両方で
match protocolattribute category *category-name*	`class-map match-any IM` `match protocol attribute category instant-messaging`	アップストリームおよびダウンストリームの両方で
match protocolattribute sub-category *sub-category-name*	`class-map match-any realtimeconferencing` `match protocol attribute sub-category voice-video-chat-collaboration`	アップストリームおよびダウンストリームの両方で
match protocolattribute application-group *application-group-name*	`class-map match-any skype` `match protocol attribute application-group skype-group`	アップストリームおよびダウンストリームの両方で

クラス マップのフォーマット	クラスマップの例	方向

組み合わせフィルタ	`class-map match-any webex-class`
	`match protocol webex`
	`match dscp 45`
	`match wlan user-priority 6`
		アップストリームのみ

サポートされる AVC ポリシーのフォーマット

ポリシーのフォーマット	QoS 処理
match protocol フィルタに基づいてクライアント ポリシーをアップストリーム	マーク、ポリシー、およびドロップ
match protocol フィルタに基づいてクライアント ポリシーをダウンストリーム	マークおよびポリシー

次の表で、AVC ポリシーの詳細なフォーマット、および例について説明します。

AVC ポリシーのフォーマット	AVC ポリシーの例	方向

ベーシック セット	`policy-map webex-policy`
	` class webex-class`
	` set dscp ef //or set up,cos`
		アップストリームおよびダウンストリーム

ベーシック ポリシー	`policy-map webex-policy`
	` class webex-class`
	` police 5000000`
		アップストリームおよびダウンストリーム

ベーシック セットおよびポリシー	`policy-map webex-policy`
	` class webex-class`
	` set dscp ef //or set up,cos`
	` police 5000000`
		アップストリームおよびダウンストリーム

デフォルトを含む複数のセットおよびポリシー	`policy-map webex-policy`
	` class webex-class`
	` set dscp af31 //or set up,cos`
	` police 4000000`
	` class class-webex-category`
	` set dscp ef //or set up,cos`
	` police 6000000`
	` class class-default`
	` set dscp <>`
		アップストリームおよびダウンストリーム

AVC ポリシーのフォーマット	AVC ポリシーの例	方向

階層型ポリシー	`policy-map webex-policy`
	`class webex-class`
	`police 5000000`
	`service-policy client-in-police-only`
	
	`policy-map client-in-police-only`
	`class webex-class`
	`police 100000`
	`class class-webex-category`
	`set dscp ef //or set up,cos`
	`police 6000000`
	`police 200000`
		アップストリームおよびダウンストリーム

階層型セットおよびポリシー	`policy-map webex-policy`
	`class class-default`
	`police 1500000`
	`service policy client-up-child`
	`policy-map webex-policy`
	`class webex-class`
	`police 100000`
	`set dscp ef`
	`class class-webex-category`
	`police 200000`
	`set dscp af31`	

ドロップ アクション	上記のいずれかの例を、この追加例とともにこのフォーマットに適用します。
	`policy-map webex-policy`
	`class webex-class`
	`drop`
	`class netflix`
	`set dscp ef //or set up,cos`
	`police 6000000`
	`class class-default`
	`set dscp <>`
		アップストリームのみ

Application Visibility and Control の前提条件

- アクセスポイントは、AVC 対応である必要があります
- AVC（QoS）の制御部分を機能させるには、FNF 付きのアプリケーションの可視化機能を設定する必要があります。

Application Visibility and Control によるDevice間ローミングに関するガイドライン

不正な形式の QoS ポリシーによりクライアントが除外されるのを防ぐには、次のガイドラインに従います。

- 新しい QoS ポリシーをデバイスに追加する場合、同じ名前の QoS ポリシーは、同じローミングまたはモビリティ ドメイン内の他のデバイスに追加する必要があります。
- デバイスに新しいリリースのソフトウェアイメージがロードされると、新しいポリシー形式がサポートされます。以前のリリースから新しいリリースにソフトウェア イメージをアップグレードした場合は、設定を別々に保存する必要があります。以前のリリースのイメージがロードされると、一部の QoS ポリシーがサポートされていないと表示される場合があり、それらの QoS ポリシーをサポートされるポリシー形式に復元する必要があります。

Application Visibility and Control の制限

- AVC は次のアクセス ポイントでのみサポートされます。
  - Cisco Aironet 1260 シリーズ アクセス ポイント
  - Cisco Aironet 1600 シリーズ アクセス ポイント
  - Cisco Aironet 2600 シリーズ アクセス ポイント
  - Cisco Aironet 2600 シリーズ ワイヤレス アクセス ポイント
  - Cisco Aironet 2700 シリーズ アクセス ポイント
  - Cisco Aironet 3500 シリーズ アクセス ポイント
  - Cisco Aironet 3600 シリーズ アクセス ポイント
- AVC は、Cisco Aironet 702W、702I（128 M メモリ）、および 1530 シリーズ アクセス ポイントではサポートされません。
- データ トラフィック（コントロール部分）の廃棄またはマーキングは、ソフトウェア リリース 3.3 ではサポートされません。
- データ トラフィック（コントロール部分）の廃棄またはマーキングは、ソフトウェア リリース 3E でサポートされます。
- アプリケーションの可視性で認識されるアプリケーションのみ、QoS 制御の適用に使用できます。
- マルチキャスト トラフィック分類はサポートされていません。
- App の可視性と認識されているアプリケーションのみ、QoS 制御の適用に使用できます。
- ICMPv6 トラフィック分類を含む IPv6 はサポートされていません。
- データリンクは AVC の NetFlow フィールドではサポートされていません。

- 次のコマンドは、AVC フロー レコードではサポートされていません。
  - **collect flow username**
  - **collect interface** {**input** | **output**}
  - **collect wireless client ipv4 address**
  - **match interface** {**input** | **output**}
  - **match transport igmp type**
- テンプレート タイムアウトは AVC が設定されたエクスポータで変更できません。テンプレートタイムアウト値が別の値に設定されていても、デフォルト値の 600 秒だけが使用されます。
- AVC ベースのレコード テンプレートのユーザ名情報については、ユーザ名マッピングに対してユーザ MAC アドレスを取得するように**records** オプションを設定する必要があります。詳細については、フローエクスポータの作成（オプション）（2934 ページ）を参照してください。
- 3600 などの AVC 対応の AP と、1140 などの非 AVC 対応の AP があり、クライアントに対して選択されたポリシーが AVC 対応の場合は、ポリシーは、AVC をサポートできない AP には送信されません。
- 入力 AVC の統計情報のみがサポートされます。統計情報を更新する頻度は、その時点で、AP にロードされているクライアントの数によって異なります。大規模ポリシー フォーマット サイズでは、統計情報はサポートされません。
- ダウンストリーム AVC QoS がサポートされる、クライアントごとのフローの合計数は 1000 です。
- 、Catalyst 3850 シリーズ スイッチは 48 K です。
- これらは、クラス マップとポリシー マップの関連の制限です。サポートされるポリシー フォーマットについては、「サポートされる AVC クラス マップおよびポリシー マップのフォーマット（2927 ページ）」を参照してください。
  - AVC および非 AVC クラスは、ダウンストリーム方向のポリシーとして共に定義することはできません。たとえば、match protocol クラス マップがある場合、ダウンストリーム方向のポリシーマップ内では、一致フィルタの他のタイプは使用できません。
  - ドロップ アクションは、ダウンストリーム AVC QoS ポリシーには適用できません。
  - match protocol は、SSID ポリシーの入力または出力ではサポートされません。
- Google は、一部のトラフィックは 1 つのアプリケーションに固有であるとは言い切れないという理由で、複数のサービス間でリソースを共有しています。そのため、識別できないトラフィック用に google-services が追加されました。この動作は想定されています。
- AVC は管理ポート（Gig 0/0）ではサポートされていません。
- NBAR 対応 QoS ポリシー設定は有線物理ポートでのみ許可されます。ポリシー設定は、たとえば、VLAN、ポート チャネル、および他の論理インターフェイスなどの仮想インターフェイスではサポートされていません。

• NBAR および NetFlow は同じインターフェイスで同時に設定できません。

Application Visibility and Control の設定方法

Application Visibility and Control の設定（CLI）

アプリケーションの可視性を設定するには、次の手順を実行します。

1. フローにキー フィールドおよび非キー フィールドを指定して、フロー レコードを作成します。
2. オプションとしてフロー レコードを指定して、任意のフローエクスポータを作成します。
3. フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを作成します。
4. Ipv4 入力または出力方向にフロー モニタを適用するように WLAN を設定します。

アプリケーションの制御を設定するには、次の手順を実行します。

1. AVC QoS ポリシーを作成します。
2. 次の 3 つの方法のいずれかを使用してクライアントに AVC QoS ポリシーを接続します。WLAN の設定、ACS または ISE の使用、またはローカル ポリシーの追加。

インターフェイスでアプリケーション認識を有効にするには、「インターフェイスでのアプリケーション認識の有効化」を参照してください。

フロー レコードの作成

デフォルトでは、**wireless avc basic**（フロー レコード）の使用が可能です。GUI から [Apply] をクリックすると、レコードはフロー モニタにマッピングされます。

デフォルトのフロー レコードは、編集も削除もできません。新しいフロー レコードが必要な場合、1 つを作成し、CLI からのフロー モニタにマップする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**flowrecord** *flow_record_name*
	例：
	`Device(config)# flow record record1`
	`Device (config-flow-record)#`
		フロー レコード コンフィギュレーション モードを開始します。

ステップ 3	**description** *string* 例：	（任意）最大 63 文字で、このフロー レコードの説明を指定します。

	コマンドまたはアクション	目的
	Device(config-flow-record)# **description IPv4flow**	
ステップ 4	**matchipv4protocol** 例： Device (config-flow-record)# **match ipv4 protocol**	IPv4 プロトコルとの一致を指定します。
ステップ 5	**matchipv4sourceaddress** 例： Device (config-flow-record)# **match ipv4 source address**	IPv4 送信元アドレス ベースのフィールドとの一致を指定します。
ステップ 6	**matchipv4destinationaddress** 例： Device (config-flow-record)# **match ipv4 destination address**	IPv4 宛先アドレス ベースのフィールドとの一致を指定します。
ステップ 7	**matchtransportsource-port** 例： Device (config-flow-record)# **match transport source-port**	トランスポート層の発信元ポートのフィールドとの一致を指定します。
ステップ 8	**matchtransportdestination-port** 例： Device (config-flow-record)# **match transport destination-port**	トランスポート層の宛先ポートのフィールドとの一致を指定します。
ステップ 9	**matchflowdirection** 例： Device (config-flow-record)# **match flow direction**	フローがモニタされる方向との一致を指定します。
ステップ 10	**matchapplicationname** 例： Device (config-flow-record)# **match application name**	アプリケーション名との一致を指定します。 （注） この操作は、AVC サポートでは必須です。フローがアプリケーションと一致することが可能になるためです。
ステップ 11	**matchwirelessssid** 例： Device (config-flow-record)# **match wireless ssid**	ワイヤレス ネットワークを特定する SSID 名との一致を指定します。

	コマンドまたはアクション	目的
ステップ 12	**collectcounterbyteslong** 例： `Device (config-flow-record)# collect counter bytes long`	カウンタ フィールドの合計バイトを収集するように指定します。
ステップ 13	**collectcounterpacketslong** 例： `Device (config-flow-record)# collect counter bytes long`	カウンタ フィールドの合計パケットを収集するように指定します。
ステップ 14	**collectwirelessapmacaddress** 例： `Device (config-flow-record)# collect wireless ap mac address`	ワイヤレス クライアントが関連付けられているアクセス ポイントの MAC アドレスの BSSID を収集するように指定します。
ステップ 15	**collect wireless client mac address** 例： `Device (config-flow-record)# collect wireless client mac address`	ワイヤレス ネットワークのクライアントの MAC アドレスを収集するように指定します。 （注） **collect wireless client mac address** は、ワイヤレス AVC で必須の設定です。
ステップ 16	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

フロー エクスポータの作成（オプション）

フロー エクスポートを作成すると、フローのエクスポート パラメータを定義できます。これは、フロー パラメータを設定するためのオプションの手順です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**flowexporter** *flow_exporter_name*
	例：
	`Device(config)# flow exporter record1`
	`Device (config-flow-exporter)#`
		フローエクスポータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**description** *string* 例： `Device(config-flow-exporter)# description IPv4flow`	最大 63 文字で、フロー レコードの説明を示します。
ステップ 4	**destination** *{hostname | ip-address}* 例： `Device (config-flow-exporter) # destination 10.99.1.4`	エクスポータでデータを送信する宛先システムのホスト名またはIPv4アドレスを指定します。
ステップ 5	**transport udp** *port-value* 例： `Device (config-flow-exporter) # transport udp 2`	UDPプロトコルのポートの値を設定します。
ステップ 6	**optionapplication-tabletimeout** *seconds***(optional)** 例： `Device (config-flow-exporter)# option application-table timeout 500`	（任意）application table timeout オプションを指定します。有効な範囲は 1 ～ 86400 秒です。
ステップ 7	**optionusermac-tabletimeout** *seconds***(optional)** 例： `Device (config-flow-exporter)# option usermac-table timeout 1000`	（任意）wireless usermac-to-username table オプションを指定します。有効な範囲は 1 ～ 86400 秒です。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。
ステップ 9	**show flow exporter** 例： `Device # show flow exporter`	設定を確認します。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

フロー モニタの作成

フロー モニタを作成して、フロー レコードおよびフロー エクスポータと関連付けることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flow monitor** *monitor-name* 例： `Device (config)# flow monitor flow-monitor-1`	フロー モニタを作成し、フロー モニタ コンフィギュレーション モードを開始します。
ステップ 3	**description** 説明 例： `Device (config-flow-monitor)# description flow-monitor-1`	フロー モニタの説明を作成します。
ステップ 4	**record** *record-name* 例： `Device (config-flow-monitor)# record flow-record-1`	事前に作成されたレコーダの名前を指定します。
ステップ 5	**exporter** *exporter-name* 例： `Device (config-flow-monitor)# exporter flow-exporter-1`	事前に作成されたエクスポータの名前を指定します。

ステップ 6	**cachetimeout** { **active** | **inactive** } **(Optional)**
	例：
	`Device (config-flow-monitor)# cache timeout active 1800`
	`Device (config-flow-monitor)# cache timeout inactive 200`
		フロー キャッシュ パラメータを設定するように指定します。1 ～ 604800 秒の時間範囲で設定できます（任意）。
		（注） AVC フローモニタで最適な結果を得るためには、非アクティブなキャッシュのタイムアウト値を90秒よりも長く設定することをお勧めします。

ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show flow monitor** 例： `Device # show flow monitor`	設定を確認します。

AVC QoS ポリシーの作成

AVC QoS ポリシーを作成するには、次の一般的な手順を実行します。

1. match protocol フィルタでクラス マップを作成します。
2. ポリシー マップを作成します。
3. 次のいずれかの方法でクライアントにポリシー マップを適用します。
   1. CLI または GUI から WLAN 上にポリシー マップを適用します。
   2. CLI から AAA サーバ（ACS サーバまたは ISE）を使用してポリシー マップを適用します。

      詳細については、『*Cisco Identity Services Engine User Guide*』および『*Cisco Secure Access Control System User Guide*』を参照してください。
   3. CLI または GUI からローカル ポリシーを適用します。

クラス マップの作成

match protocol フィルタを設定する前に、クラス マップを作成する必要があります。マーキング、ポリシング、ドロップなどの QoS アクションがトラフィックに適用できます。AVC の match protocol フィルタはワイヤレス クライアントにのみ適用されます。サポートされているプロトコルの詳細については、http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** *class-map-name* 例： `Device(config)# class-map webex-class`	クラス マップを作成します。

ステップ 3	**match protocol** {*application-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application-group-name*}
	例：
	`Device(config)# class-map webex-class`
	`Device(config-cmap)# match protocol webex-media`
		アプリケーション名、カテゴリ名、サブカテゴリの名前、またはアプリケーション グループに一致するものを指定します。

	コマンドまたはアクション	目的
	Device(config)# **class-map class-webex-category** Device(config-cmap)# **match protocol attribute category webex-media** Device# **class-map class-webex-sub-category** Device(config-cmap)# **match protocol attribute sub-category webex-media** Device# **class-map class-webex-application-group** Device(config-cmap)# **match protocol attribute application-group webex-media**	
ステップ 4	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシー マップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： Device# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map** *policy-map-name* 例： Device(config)# **policy-map webex-policy** Device(config-pmap)#	ポリシーマップ名を入力することによってポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。

	コマンドまたはアクション	目的
		（注） 既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。

ステップ 3	**class** [*class-map-name* | **class-default**]
	例：
	`Device(config-pmap)# class-map webex-class`
	`Device(config-pmap-c)#`
		トラフィックの分類を定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
		デフォルトでは、ポリシー マップおよびクラスマップは定義されていません。
		すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。
		class-default トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシーマップの最後に配置されます。暗黙の **match any** が **class-default** クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは **class-default** と一致します。
		（注） 既存のクラス マップを削除するには、**no class** *class-map-name* ポリシー マップ コンフィギュレーション コマンドを使用します。

ステップ 4	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] 例： `Device(config-pmap-c)# police 100000 80000 drop`	分類したトラフィックにポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。指定できる範囲は 8000 ～ 10000000000 です

	コマンドまたはアクション	目的
		• *burst-byte* には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。（ポリシング済み DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。
ステップ 5	**set** { **dscp** *new-dscp* | **cos** *cos-value* } 例： `Device(config-pmap-c)# set dscp 45`	パケットに新しい値を設定することによって、IP トラフィックを分類します。 • **dscp** *new-dscp* には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

次のタスク

ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

ローカル ポリシーの設定（CLI）

ローカル ポリシーの設定（*CLI*）

ローカル ポリシーを設定するには、次の手順を実行します。

1. サービス テンプレートを作成します。
2. インターフェイス テンプレートを作成します。
3. パラメータ マップを作成します。
4. ポリシー マップを作成します。
5. WLAN 上でローカル ポリシーを適用します。

サービス テンプレートの作成（*CLI*）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**service-template** *service-template-name*
	例：
	`Device(config)# service-template cisco-phone-template`
	`Device(config-service-template)#`
		サービス テンプレート コンフィギュレーション モードを開始します。

ステップ 3	**access-group** *acl_list* 例： `Device(config-service-template)# access-group foo-acl`	適用するアクセス リストを指定します。
ステップ 4	**vlan** *vlan_id* 例： `Device(config-service-template)# vlan 100`	VLAN ID を指定します。1 ～ 4094 の値を指定できます。
ステップ 5	**absolute-timer** *seconds* 例： `Device(config-service-template)# absolute-timer 20`	サービス テンプレートのセッション タイムアウト値を指定します。1 ～ 65535 の値を指定できます。
ステップ 6	**service-policy qos** {**input** | **output**} 例： `Device(config-service-template)# service-policy qos input foo-qos`	クライアントの QoS ポリシーを設定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

パラメータ マップの作成（*CLI*）

クラス マップよりパラメータ マップの使用をお勧めします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map typesubscriberattribute-to-service** *parameter-map-name* 例： `Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para`	パラメータ マップのタイプと名前を指定します。
ステップ 3	*map-index* *frame*map{device-type|mac-address|oui|user-agent|username}{eq|neq|regex} 例： `Device(config-parameter-map-filter)# 10 map device-type eq "WindowsXP-Workstation"`	パラメータ マップ属性フィルタ基準を指定します。

ステップ 4	**interface-template** *interface-template-name*
	例：
	`Device(config-parameter-map-filter-submode)# interface-template cisco-phone-template`
	`Device(config-parameter-map-filter-submode)#`
		サービス テンプレート コンフィギュレーション モードを開始します。

ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報 （1282 ページ）
ローカル ポリシーの設定に関する制限 （1281 ページ）
ローカル ポリシーの監視 （1289 ページ）
例：ローカル ポリシーの設定 （1290 ページ）

ポリシー マップの作成（*CLI*）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map typecontrolsubscriber** *policy-map-name* 例： `Device(config)# policy-map type control subscriber Aironet-Policy`	ポリシー マップ タイプを指定します。
ステップ 3	**eventidentity-update** {**match-all** | **match-first**} 例： `Device(config-policy-map)# event identity-update match-all`	ポリシー マップに対する一致基準を指定します。
ステップ 4	*class_numberclass_map_name* **class** { | **always** }{**do-all** | **do-until-failure** | **do-until-success**} 例： `Device(config-class-control-policymap)# 1 class local_policy1_class do-until-success`	ローカル プロファイリング ポリシー クラス マップ番号を設定し、処理の実行方法を指定します。クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • **always**：照合を行わずに実行しますが、成功を返します。 • **do-all**：すべての処理を実行します。 • **do-until-failure**：照合が失敗するまですべての処理を実行します。これはデフォルト値です。 • **do-until-success**：照合が成功するまですべての処理を実行します。
ステップ 5	*action-index* **map attribute-to-servicetable** *parameter-map-name* 例： `Device(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-para`	使用するパラメータ マップ テーブルを指定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報 （1282 ページ）
ローカル ポリシーの設定に関する制限 （1281 ページ）
ローカル ポリシーの監視 （1289 ページ）
例：ローカル ポリシーの設定 （1290 ページ）

WLAN 上のデバイスのローカル ポリシーの適用（*CLI*）

始める前に

パラメータ マップのサービス ポリシーにデバイス タイプ ベースのルールが含まれる場合、デバイス分類子がイネーブルになっていることを確認します。

（注） **device classification** コマンドを使用して、show コマンドの出力で正しく表示されるようにデバイスを分類する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan-name* 例： `Device(config)# wlan wlan1`	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**service-policy type controlsubscriber** *policymapname* 例： `Device(config-wlan)# service-policy type control subscriber Aironet-Policy`	WLAN にローカル ポリシーを適用します。

	コマンドまたはアクション	目的
ステップ 4	**profiling local http (optional)** 例： `Device(config-wlan)# profiling local http`	HTTP プロトコルに基づいて、デバイスのプロファイリングのみをイネーブルにします（任意）。
ステップ 5	**profiling radius http (optional)** 例： `Device(config-wlan)# profiling radius http`	ISE でデバイスのプロファイリングをイネーブルにします（任意）。
ステップ 6	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をシャットダウンしないように指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報 （1282 ページ）
ローカル ポリシーの設定に関する制限 （1281 ページ）
ローカル ポリシーの監視 （1289 ページ）
例：ローカル ポリシーの設定 （1290 ページ）

IPV4 の入出力方向にフロー モニタを適用する WLAN の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan-id* 例： `Device (config) # wlan 1`	WLAN コンフィギュレーション サブモードを開始します。*wlan-id* には WLAN ID を入力します。指定できる範囲は 1 ～ 64 です。
ステップ 3	**ip flow monitor** *monitor-name*{**input** | **output**} 例：	入力または出力パケットに対応する WLAN にフロー モニタを関連付けます。

	コマンドまたはアクション	目的
	`Device (config-wlan) # ip flow monitor flow-monitor-1 input`	
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Application Visibility and Control のモニタリング

Application Visibility and Control のモニタリング（CLI）

このセクションでは、アプリケーションの可視性に関する新しいコマンドについて説明します。

次のコマンドは、 およびアクセス ポイントのアプリケーションの可視性をモニタするために使用できます。

表 *191 :* のアプリケーションの可視性モニタリング コマンド

コマンド	目的
show avc client *client-mac***top** *n***application** [**aggregate** | **upstream** | **downstream**]	指定されたクライアント MAC の上位「N」アプリケーションに関する情報を表示します。
show avc wlan *ssid***top** *n***application** [**aggregate** | **upstream** | **downstream**]	指定された SSID の上位「N」アプリケーションに関する情報を表示します。
avc top user[enable | disable]	上位「N」アプリケーションに関する情報を有効または無効にします。
show avc wlan *wlan-id* **application** *app name***top***N* [**aggregate** | **upstream** | **downstream**]	アプリケーション内のユーザごとのネットワーク利用状況が表示されます。 （注） Catalyst 4500E Supervisor Engine 8-E では、表示される上位 N ユーザの情報には、クライアントの MAC アドレスとユーザ名は表示されません。この問題は、クライアントが切断された後 90 秒以内にのみ発生します。

show wlanid *wlan-id*	AVC が特定の WLAN で有効または無効になっているかどうかについての情報が表示されます。
show flow monitor *flow_monitor_name***cache**	フロー モニタに関する情報を表示します。
show wireless client mac-address *mac-address***service-policy** {**input** | **output**}	ワイヤレス クライアントにマッピングされたポリシーに関する情報が表示されます。
show ip nbar protocol-discovery ［**interface** *interface-type interface-number*］［**stats** {**byte-count** | **bit-rate** | **packet-count** | **max-bit-rate**}］［**protocol** *protocol-name* | **top-n** *number*］	NBAR Protocol Discovery 機能によって収集された統計情報を表示します。 • （任意）表示される統計情報を最適化するには、キーワードおよび引数を入力します。キーワードのそれぞれの詳細については、『Cisco IOS Quality of Service Solutions Command Reference』の**show ip nbar protocol-discovery** コマンドを参照してください。 （注） NBAR を設定する場合、インターフェイスのプロトコル検出を有効にする必要があります。
show policy-map target **show policy-map** **show policy-map** *policy-name* **show policy-map interface** *interface-type interface-number*	ポリシーマップに関する情報を表示します。

表 *192*：アプリケーションの可視性統計情報コマンドのクリア

コマンド	目的
clearavcclient *mac***stats**	クライアントごとの統計情報をクリアします。
clearavcwlan *wlan-name***stats**	WLAN ごとの統計情報をクリアします。

例：Application Visibility and Control

例：アプリケーションの可視性設定

この例では、フロー レコードとフロー モニタの作成方法、フロー レコードをフロー モニタに適用する方法、およびフロー モニタを WLAN に適用する方法を示します。

```
Device# configure terminal
Device(config)# flow record fr_v4
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match flow direction
Device(config-flow-record)# match application name
Device(config-flow-record)# match wireless ssid
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect wireless ap mac address
Device(config-flow-record)# collect wireless client mac address
Device(config)#end
```

```
Device# configure terminal
Device# flow monitor fm_v4
Device(config-flow-monitor)# record fr_v4
Device(config-flow-monitor)# cache timeout active 1800
Device(config)#end
```

```
Device(config)#wlan wlan1
Device(config-wlan)#ip flow monitor fm_v4 input
Device(config-wlan)#ip flow mon fm-v4 output
Device(config)#end
```

例：Application Visibility and Control の QoS 設定

次に、match protocol でアプリケーション名、カテゴリ、およびサブカテゴリのフィルタを適用してクラス マップを作成する例を示します。

```
Device# configure terminal
Device(config)# class-map cat-browsing
Device(config-cmap)# match protocol attribute category browsing
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map cat-fileshare
Device(config-cmap)# match protocol attribute category file-sharing
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map match-any subcat-terminal
```

```
Device(config-cmap)# match protocol attribute sub-category terminal
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map match-any webex-meeting
Device(config-cmap)# match protocol webex-meeting
Device(config-cmap)#end
```

次に、ポリシー マップを作成し、アップストリーム QoS の既存のクラス マップを定義する例を示します。

```
Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 150000
Device(config-pmap-c)# set dscp 12
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-fileshare
Device(config-pmap-c)# police 1000000
Device(config-pmap-c)# set dscp 20
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class subcat-terminal
Device(config-pmap-c)# police 120000
Device(config-pmap-c)# set dscp 15
Device(config-pmap-c)#end

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class webex-meeting
Device(config-pmap-c)# police 50000000
Device(config-pmap-c)# set dscp 21
Device(config-pmap-c)#end
```

次に、ポリシー マップを作成し、ダウンストリーム QoS の既存のクラス マップを定義する例を示します。

```
Device# configure terminal
Device(config)# policy-map test-avc-down
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 200000
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-fileshare
Device(config-pmap-c)# police 300000
Device(config-pmap-c)# set wlan user-priority 2
Device(config-pmap-c)# set dscp 20
Device(config-pmap-c)#end
```

```
Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class subcat-terminal
Device(config-pmap-c)# police 100000
Device(config-pmap-c)# set dscp 25
Device(config-pmap-c)#end

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class webex-meeting
Device(config-pmap-c)# police 60000000
Device(config-pmap-c)# set dscp 41
Device(config-pmap-c)#end
```

次に、定義された QoS ポリシーを WLAN に適用する例を示します。

```
Device# configure terminal
Device(config)#wlan  alpha
Device(config-wlan)#shut
Device(config-wlan)#end
Device(config-wlan)#service-policy client input test-avc-up
Device(config-wlan)#service-policy client output test-avc-down
Device(config-wlan)#no shut
Device(config-wlan)#end
```

例：ローカル プロファイリング ポリシーの QoS 属性の設定

次の例は、ローカル プロファイリング ポリシーのための QoS の属性を設定する方法です：

```
Device(config)# class-map type control subscriber match-all local_policy1_class
Device(config-filter-control-classmap)# match device-type android
Device(config)# service-template local_policy1_template
Device(config-service-template)# vlan 40
Device(config-service-template)# service-policy qos output local_policy1
Device(config)# policy-map type control subscriber local_policy1
Device(config-event-control-policymap)# event identity-update match-all
Device(config-class-control-policymap)# 1 class local_policy1_class do-until-success
Device(config-action-control-policymap)# 1 activate service-template local_policy1_template
Device(config)# wlan open_auth 9
Device(config-wlan)# client vlan VLAN40
Device(config-wlan)# service-policy type control subscriber local_policy1
```

Application Visibility and Control に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

関連項目	マニュアル タイトル
Flexible NetFlow 設定	『*Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』
Flexible NetFlow コマンド	『*Flexible NetFlow Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』
QoS の設定	『*QoS Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*』
QoS コマンド	『*QoS Command Reference, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Application Visibility and Control の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。
Cisco IOS XE 3E	QoS を使用した AVC 制御が導入されました。

第 135 章

ロケーションの設定

- 機能情報の確認 （2953 ページ）
- ロケーションの設定に関する情報 （2953 ページ）
- ロケーションの設定方法 （2954 ページ）
- ロケーション設定および NMSP 設定のモニタリング （2959 ページ）
- 例：ロケーションの設定 （2960 ページ）
- 例：NMSP の設定 （2960 ページ）
- ロケーション設定に関する追加情報 （2961 ページ）
- ロケーション設定の機能履歴と情報 （2962 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

ロケーションの設定に関する情報

デバイスは、対象クライアントデバイス周辺のアクセスポイントから受信信号強度表示（RSSI）測定値を収集し、このクライアントのロケーションを特定します。デバイスは、最大 16 台のアクセス ポイントから、クライアント、RFID タグ、および不正なアクセス ポイントのロケーション レポートを取得できます。

通常のクライアントまたは調整クライアントのパス損失測定（S60）要求を設定すると、ロケーションの精度を向上させることができます。

ロケーションの設定方法

ロケーションの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**location plm** {**calibrating** [**multiband** | **uniband**] | **client** *burst_interval* 例： `Device(config)# location plm client 100`	調整または非調整クライアントのパス損失測定（S60）要求を設定します。 パス損失測定要求で、位置精度が向上します。標準の非調整クライアントに対して、0 ～ 3600 秒の範囲で **burst_interval** パラメータを設定できます。デフォルト値は 60 秒です。 関連付けされた 802.11a または 802.11b/g 無線、関連付けされた 802.11a/b/g 無線の調整クライアントにパス損失測定要求を設定できます。 クライアントからプローブが送信される頻度が低い場合や、少数のチャネルに対してしか送信されない場合は、クライアントのロケーションが更新不可能になるか、精度が低下します。**location plm** コマンドを実行すると、クライアントは強制的に、すべてのチャネルに対してパケットを送信するようになります。CCXv4 以上のクライアントがアソシエートすると、Deviceはそのクライアントにパス損失測定要求を送信します。これは、アクセスポイントが使用している帯域とチャネル（2.4 GHz のみのアクセスポイントの場合は一般にチャネル 1、6、および 11）で無期限に送信するようクライアントに指示するものです。送信する間隔は設定可能です（たとえば 60 秒）。

	コマンドまたはアクション	目的
ステップ 3	**location rssi-half-life** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *seconds* 例： `Device(config)# location rssi-half-life calibrating-client 60`	クライアント、調整クライアント、RFID タグ、不正アクセス ポイントの RSSI 半減期を設定します。 クライアント、調整クライアント、RFID タグ、不正アクセス ポイントの **location rssi-half-life** パラメータ値を入力できます。指定可能な値は、0、1、2、5、10、20、30、60、90、120、180、または 300 秒です。デフォルト値は 0 秒です。 クライアントデバイスの中には、チャネル変更直後は送信電力を下げるものがあるのと、RF は変動しやすいことから、RSSI の値がパケットごとに大きく異なることもあります。**location rssi-half-life** コマンドを実行すると、精度を向上させるために、均一でない状態で受信したデータを平均化するための半減期（ハーフライフ）を設定することができます。 （注） **location rssi-half-life** コマンドを使用したり、変更したりしないことをお勧めします。
ステップ 4	**location expiry** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *timeout* 例： `Device(config)# location expiry calibrating-client 50`	クライアント、調整クライアント、RFID タグ、不正アクセス ポイントの RSSI タイムアウト値を設定します。 クライアント、RFID タグ、不正アクセス ポイントの RSSI タイムアウト値を入力できます。範囲は 5 ～ 3600 秒で、デフォルト値は 5 秒です。 調整クライアントには 0 ～ 3600 秒の範囲で RSSI タイムアウト値を入力でき、デフォルト値は 5 秒です。 ロケーションを正確に特定するには、CPU が保持する RSSI が最近のものであることと、その値が大きいことが必要です。**location expiry** コマンドを使用すると、古い RSSI 平均が失効するまでの時間を指定できます。

	コマンドまたはアクション	目的
		（注） **location expiry** コマンドを使用したり、変更したりしないことをお勧めします。
ステップ 5	**location algorithm** {**rssi-average** | **simple**} 例： `Device(config)# location algorithm rssi-average`	RSSI および信号対雑音比（SNR）値の平均の算出に使用されるアルゴリズムを設定します。 **location algorithm rssi-average** コマンドを入力することで、より正確な、しかしより CPU オーバーヘッドの高いアルゴリズムを指定できます。または、**location algorithm simple** コマンドを入力することで、高速で CPU のオーバーヘッドが低い、しかし精度に欠けるアルゴリズムを指定することもできます。 （注） **location algorithm** コマンドは、使用したり、変更したりしないことをお勧めします。
ステップ 6	**location admin-tag** *string* 例： `Device(config)# location admin-tag`	クライアントデバイスの場所の管理タグまたはサイト情報を設定します。
ステップ 7	**location civic-location identifier** {*identifier* | **host**} 例： `Device(config)# location civic-location identifier host`	都市ロケーション情報を指定します。 文字列またはホストとして都市ロケーション識別子を設定できます。
ステップ 8	**location custom-location identifier** {*identifier* | **host**} 例： `Device(config)# location custom-location identifier host`	カスタムロケーション情報を指定します。 文字列またはホストとしてカスタムロケーション識別子を設定できます。
ステップ 9	**location geo-location identifier** {*identifier* | **host**} 例： `Device(config)# location geo-location identifier host`	クライアントデバイスの地理的なロケーション情報を指定します。 文字列またはホストとしてロケーション識別子を設定できます。

	コマンドまたはアクション	目的
ステップ 10	**location prefer** {**cdp** | **lldp-med** | **static**} **weight** *priority_value* 例： `Device(config)# location prefer weight cdp 50`	ロケーション情報のソースのプライオリティを設定します。 優先順位のウェイトは、0 から 255 の範囲で入力できます。
ステップ 11	**location rfid** {**status** | **timeout** | **vendor-name**} 例： `Device(config)# location rfid timeout 100`	RFID タグ ステータス、RFID タイムアウト値、RFID タグ ベンダー名などの RFID タグ トラッキング オプションを設定します。 60 ～ 7200 秒の範囲で RFID タイムアウト値を入力できます。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

例

クライアント、RFID タグ、および不正デバイスの NMSP 通知間隔の変更（CLI）

ネットワーク モビリティ サービス プロトコル（NMSP）によって、Mobility Services Engine とコントローラの間の発信/着信トラフィックに関する通信の管理が行われます。高い頻度でのロケーション更新を必要とするアプリケーションがある場合は、クライアント、アクティブな RFID タグ、および不正なアクセス ポイント/クライアントの NMSP 通知間隔を 1 ～ 180 秒の範囲内で変更できます。

（注） コントローラと Mobility Services Engine との通信には、TCP ポート 16113 が使用されます。コントローラと Mobility Services Engine の間にファイアウォールがある場合は、NMSP を機能させるにはこのポートが開いている（ブロックされていない）ことが必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**nmsp notification interval** {**attachment** *seconds* | **location** *seconds* | **rssi** [**clients** *interval* | **rfid** *interval* | **rogues** [**ap** | **client**] *interval*]} 例： `Device(config)# nmsp notification interval rssi rfid 50`	クライアント、RFID タグ、不正クライアント、不正アクセスポイントの NMSP 通知間隔を設定します。 1 ～ 180 秒の範囲で RSSI 測定値の NMSP 通知間隔の値を入力できます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

クライアント、RFID タグ、および不正デバイスの NMSP 通知しきい値の変更（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**location notify-threshold** {**clients** | **rogues ap** | **tags** } *threshold* 例： `Device(config)# location notify-threshold clients 5`	クライアント、RFID タグ、不正なクライアント、不正なアクセス ポイントの NMSP 通知しきい値を設定します。 RSSI しきい値は、0 ～ 10 db の範囲で入力できます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

ロケーション設定および NMSP 設定のモニタリング

ロケーション設定のモニタリング（CLI）

このセクションでは、ロケーション設定に関する新しいコマンドについて説明します。

次のコマンドは、 のロケーション設定のモニタリングに使用できます。

表 *193 :* ロケーション設定モニタリング コマンド

コマンド	目的
show location summary	現在のロケーション設定値を表示します。
show location statistics rfid	ロケーションベースの RFID 統計情報を表示します。
show location detail *client_mac_addr*	特定のクライアントの RSSI テーブルを表示します。

NMSP 設定のモニタリング（CLI）

このセクションでは、NMSP 設定に関する新しいコマンドについて説明します。

次のコマンドがの NMSP 設定のモニタリングに使用できます。

表 *194 : NMSP* 設定モニタリング コマンド

コマンド	目的
show nmsp attachment suppress interfaces	アタッチメント抑制インターフェイスを表示します。
show nmsp capability	NMSP 機能を表示します。
show nmsp notification interval	NMSP 通知間隔を表示します。
show nmsp statistics connection	接続固有の NMSP カウンタを表示します。
show nmsp statistics summary	一般的な NMSP カウンタを表示します。
show nmsp status	アクティブな NMSP 接続の状態を表示します。
show nmsp subscription detail	がサブスクライブされているモビリティ サービスをすべて表示します。

show nmsp subscription detail *ip_addr*	特定のIPアドレスにサブスクライブされたモビリティサービスについてのみ詳細を表示します。
show nmsp subscription summary	がサブスクライブされているすべてのモビリティサービスの詳細を表示します。

例：ロケーションの設定

次に、関連付けされた802.11aまたは802.11b/g無線の調整クライアント用パス損失測定（S60）要求を設定する例を示します。

```
Device# configure terminal
Device(config)# location plm calibrating uniband
Device(config)# end
Device# show location summary
```

次に、不正アクセス ポイントの RSSI 半減期を設定する例を示します。

```
Device# configure terminal
Device(config)# location rssi-half-life rogue-aps 20
Device(config)# end
Device# show location summary
```

例：NMSP の設定

次に、RFID タグの NMSP 通知間隔を設定する例を示します。

```
Device# configure terminal
Device(config)# nmsp notification interval rssi rfid 50
Device(config)# end
Device# show nmsp notification interval
```

次に、クライアントの NMSP 通知しきい値を設定する例を示します。

```
Device# configure terminal
Device(config)# nmsp notify-threshold 5
Device(config)# end
Device# show nmsp statistics summary
```

ロケーション設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ロケーション設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

第 136 章

音声パラメータとビデオ パラメータの設定

- 機能情報の確認 （2963 ページ）
- 音声およびビデオのパラメータの前提条件 （2963 ページ）
- 音声およびビデオのパラメータの制約事項 （2964 ページ）
- 音声パラメータとビデオ パラメータの設定について （2964 ページ）
- 音声パラメータとビデオ パラメータの設定方法 （2970 ページ）
- 音声およびビデオ パラメータのモニタリング （2980 ページ）
- 音声およびビデオ パラメータの設定例 （2983 ページ）
- 音声およびビデオ パラメータに関する追加情報 （2984 ページ）
- 音声およびビデオ パラメータ設定の機能履歴と情報 （2985 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

音声およびビデオのパラメータの前提条件

音声およびビデオのパラメータを設定する前に、次のポイントをご確認ください。

- デバイスに接続するアクセス ポイントが設定されていることを確認します。
- SSID を設定します。

音声およびビデオのパラメータの制約事項

以下は、音声およびビデオについてのパラメータを設定する際に考慮する必要のある制限事項です。

- SIP CAC は TSPEC ベースのアドミッション コントロールをサポートする Cisco Phone 9971 を使用できます。また、ステータス コード 17 をサポートする電話を使用できます。
- 非 TSPEC SIP 電話に音声優先対応を提供するために、SIP スヌーピングがサポートされています。
- ビデオ CAC 用 TSPEC はサポートされません。
- Cisco 792x IP Phone は、11K が有効な非 WMM デバイスとして許可されると、電話での音声の問題が発生します。

（注） 11K が有効な非 WMM デバイスとして許可されているすべての Cisco 792x IP Phone の音声 WLAN の 11K を無効にします。この問題を解決するには、Cisco Unified Call Manager のファームウェアを 1.4.5 にアップグレードします。詳細については、『Cisco Unified Call Manager Configuration Guide』を参照してください。

音声パラメータとビデオ パラメータの設定について

デバイスには、音声またはビデオ、あるいはその両方の品質に影響を及ぼす次の 3 つのパラメータがあります。

- Call Admission Control（コール アドミッション制御）
- Expedited bandwidth requests
- Unscheduled automatic power save delivery

コール アドミッション制御（CAC）および UAPSD は Cisco Compatible Extensions（CCX）v4 および v5 でサポートされますが、これらのパラメータは、CCX がなくても、（802.1e をサポートする）WMM を実装するデバイスであればサポートされます。Expedited Bandwidth Requests は、CCXv5 でのみサポートされます。

音声の品質に関する問題の監視およびレポートには、Traffic Stream Metrics（TSM）を使用します。

Call Admission Control（コール アドミッション制御）

コール アドミッション制御（CAC）を使用すると、ワイヤレス LAN で輻輳が発生したときに、アクセス ポイントは制御された Quality of Service（QoS）を維持できます。CCXv4 に展開された WMM プロトコルは異なるネットワーク負荷の下で QoS を維持します。

Over-the-Air（OTA）という 2 種類の CAC（静的ベースの CAC および負荷ベースの CAC）が使用可能です。

デバイスは次の QoS ポリシーをサポートします。

- ユーザ定義のポリシー：独自の QoS ポリシーを定義できます。こうしたポリシーを既存のメタル ポリシーより細かく制御できます。
- システム定義の重要なメタル ポリシー：下位互換性をサポートします。
  - Platinum：VoIP クライアントに使用されます。
  - Gold：ビデオ クライアント用に使用されます。
  - Silver：ベスト エフォート型トラフィックに使用されます。
  - Bronze：NRT トラフィックに使用されます。

静的ベースの CAC

WMM および TSPEC をサポートする Voice over WLAN アプリケーションでは、コールを開始するために必要になる帯域幅または共有メディア時間を指定できます。帯域幅ベースまたは静的な CAC によりアクセス ポイントは、特定のコールに対応できるかどうかを判断できます。アクセス ポイントでは、許容される品質でコールの最大数を維持するために、必要であればコールを拒否します。

WLAN の QoS 設定により、帯域幅ベースの CAC サポートのレベルが決定します。音声アプリケーションで帯域幅ベースの CAC を使用するには、WLAN を Platinum QoS に対して設定する必要があります。帯域幅ベースの CAC により、アクセス ポイントの帯域幅のアベイラビリティは、アクセス ポイント クライアントによる帯域幅の現使用量に基づいて決定され、Voice over WLAN アプリケーションによって要求された帯域幅がアクセス ポイント クライアントに追加されます。この合計が設定された帯域幅しきい値を超えると、新しいコールは拒否されます。

（注） WMM が有効化されている CCX v4 クライアントに対して Admission Control（ACM; アドミッション コントロール）を有効にする必要があります。そうしない場合、帯域幅ベースの CAC はこれらの CCXv4 クライアントに対して正しく動作しません。

load-based の CAC

load-based の CAC では、音声アプリケーションまたはビデオ アプリケーションに対し、すべての種類のトラフィック（クライアントからのトラフィックなど）、共通チャネル アクセス ポイントの負荷、および共通割り当てチャネルの干渉などによる帯域幅の消費を考慮した測定方法を利用できるようになります。load-based の CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。

負荷ベース CAC では、アクセス ポイントでは RF チャネルの使用率（消費された帯域幅の割合）、チャネル干渉、およびアクセス ポイントで許可される追加のコールが継続的に測定、更新されます。アクセス ポイントは、コールをサポートするのに十分なだけの未使用帯域幅がチャネルにある場合に限り、新規のコールを許可します。このようにすることで、load-based の CAC は、チャネルのオーバーサブスクリプションを防ぎ、WLAN の負荷および干渉のあらゆる状況下で QoS を維持します。

（注） load-based の CAC を無効にすると、アクセス ポイントが帯域幅ベースの CAC を使用するようになります。

IOSd コール アドミッション制御

IOSd コール アドミッション制御（CAC）は、デバイスからアクセス ポイントの間の帯域幅のアベイラビリティを制御します。

スイッチにクラスベースの無条件パケット マーキング機能を設定し、CAC を管理できます。

CAC は、音声およびビデオ トラフィックのみに適用される概念で、データ トラフィックには適用されません。データ トラフィックが増加すると、ネットワーク、キューイング、バッファリングの特定のリンクでオーバーサブスクリプションが発生し、パケット ドロップの決定によって輻輳状態が解消されます。増加したトラフィックは、トラフィックを送信するインターフェイスが使用可能になるまで遅延するか、またはトラフィックがドロップされた場合、プロトコル、またはエンドユーザがタイムアウトを開始し、情報の再送信を要求するまで遅延状態となります。

遅延とパケット損失の両方の影響を受けやすいリアルタイムのトラフィックの場合、この方法では、このトラフィックのユーザが要求する Quality of Service（QoS）を維持しながらネットワークの輻輳を解決することはできません。音声など、リアルタイムの遅延の影響を受けやすいトラフィックの場合、ネットワークのドロップや遅延が発生し、QoS が損なわれたり、お客様の不満を引き起こすよりも、輻輳状態でのネットワーク アクセスを拒否することをお勧めします。

したがって CAC では、音声コールの確立前に行われ、必要なネットワーク リソースが新しいコールに適した QoS を実現できるかどうかによる、情報に基づく決定と安定性がもたらされます。

既存の CAC アルゴリズムおよび許可 CAC CLI 設定に基づいて、デバイスにより、TSPEC のビデオ再生または SIP スヌーピングを利用できるようになります。**admit cac** CLI は、音声コールのパススルーに必須です。

BSSID のポリサーが音声またはビデオのトラフィック用に設定されている場合、パケットで追加チェックが実行されます。

Expedited Bandwidth Requests

Expedited Bandwidth Request 機能を使用すると、CCXv5 クライアントは WLAN への緊急の WMM Traffic Specifications（TSPEC）要求（e911 コールなど）を示すことができるようになります。コントローラがこの要求を受信すると、コントローラは、処理中の他の TSPEC コールの質を変えることなく、緊急のコールに対応しようとします。

Expedited Bandwidth Requests は、帯域幅ベースの CAC と load-based の CAC の両方に適用できます。Expedited Bandwidth Requests はデフォルトでは無効になっています。この機能が無効の場合、コントローラはすべての緊急の要求を無視し、TSPEC 要求は通常の TSPEC 要求として処理します。

次の表に、通常の TSPEC 要求と Expedited Bandwidth Requests についての、TSPEC 要求処理の例を示します。

表 *195 : TSPEC* 要求処理の例

CAC モード	音声コール用に予約されている帯域幅	使用率	通常の TSPEC 要求	Expedited Bandwidth Request を使用した TSPEC
帯域幅ベースの CAC	75%（デフォルト設定）	75% 未満	許可	許可
		75% ～ 90%（音声コール用に予約された帯域幅が消費される）	却下	許可
		90% 以上	却下	却下
load-based の CAC		75% 未満	許可	許可
		75% ～ 85%（音声コール用に予約された帯域幅が消費される）	却下	許可
		85% 以上	却下	却下

[26] 帯域幅ベースの CAC では、音声コールの帯域幅利用率はアクセス ポイント無線単位であり、共通チャネル アクセス ポイントは考慮されません。load-based の CAC の場合、音声コールの帯域幅利用率は、チャネル全体に対して測定されます。

[27] 帯域幅ベースの CAC（消費された音声帯域幅とビデオ帯域幅）または load-based の CAC（チャネル使用率 [Pb]）

（注） TSPEC G711-20 ms および G711-40 ms のコーデック タイプのアドミッション制御がサポートされます。

U-APSD

Unscheduled automatic power save delivery（U-APSD）は、モバイル クライアントのバッテリ寿命を延ばす IEEE 802.11e で定義されている QoS 機能です。バッテリ寿命を延ばすだけでなく、この機能は無線メディアで配送されるトラフィック フローの遅延時間を短縮します。U-APSD は、アクセス ポイントでバッファされる個々のパケットをポーリングするようにクライアントに要求しないため、単一のアップリンク トリガー パケットを送信することにより、複数のダウンリンク パケットの送信が許可されます。WMM が有効化されると、U-APSD は自動的に有効化されます。

Traffic Stream Metrics

voice-over-wireless LAN（VoWLAN）展開では、クライアントとアクセス ポイント間のエア インターフェイスでの音声関連のメトリクスの測定には、Traffic Stream Metrics（TSM）が使用されます。TSM ではパケット遅延とパケット損失の両方がレポートされます。これらのレポートを調べることにより、劣悪な音声品質の問題を分離できます。

このメトリクスは、CCX v4 以降のリリースをサポートするアクセス ポイントとクライアント デバイス間のアップリンク（クライアント側）統計とダウンリンク（アクセス ポイント側）統計の集合から成ります。クライアントが CCX v4 または CCXv5 に準拠していない場合、ダウンリンク統計のみが取得されます。クライアントとアクセス ポイントで、これらのメトリクスが測定されます。アクセス ポイントではまた、5 秒おきに測定値が収集されて、90 秒のレポートが作成された後、レポートがコントローラに送信されます。コントローラは、アップリンクの測定値はクライアント単位で保持し、ダウンリンクの測定値はアクセス ポイント単位で保持します。履歴データは 1 時間分を保持します。このデータを格納するには、アップリンク メトリクス用に 32MB、ダウンリンク メトリクス用に 4.8MB の追加のメモリがコントローラに必要です。

無線帯域別ベースで（たとえば、すべての 802.11a ラジオ）、GUI または CLI により TSM を設定できます。コントローラは、リブート後も持続するように、フラッシュ メモリに設定を保存します。アクセス ポイントにより、コントローラからの設定が受信された後、指定された無線帯域で TSM が有効化されます。

この表に、別のコントローラ シリーズでの TSM エントリの上限を示します。

TSM エントリ	5700
最大 AP TSM エントリ数	100

TSM エントリ	5700
最大クライアント TSM エントリ数	250
最大 TSM エントリ数	100*250=25000

（注） 上限に到達すると、追加の TSM エントリを保存し、WCS または NCS に送信することができなくなります。クライアント TSM エントリが満杯で、AP TSM エントリにまだ空きがある場合、AP エントリのみが保存されます（逆もまた同様）。これにより、出力が不完全になります。TSM クリーンアップは、1 時間ごとに行われます。エントリは、対応する AP とクライアントがシステム内に存在しない場合にのみ削除されます。

優先コール番号を使用した音声優先制御の設定について

TSPEC ベースのコールをサポートしない VoWLAN クライアントからの SIP コールをサポートするようにデバイスを設定できます。この機能は、SIP CAC サポートと呼ばれます。帯域幅が、設定された voice プールで使用可能な場合は、 SIP コールが通常のフローを使用し、デバイスがこれらのコールに帯域幅を割り当てます。

また、最大 6 つの優先コール番号に順位を設定できます。コールが、設定された優先番号の 1 つに送信された場合、デバイスは設定された最大音声帯域幅を検査しません。デバイスは、音声CACに設定されている音声の最大帯域幅を超えてもコールに必要な帯域幅を割り当てます。優先コールは、帯域幅割り当てが無線の帯域幅の 85% を超えた場合、拒否されます。帯域割り当ては、帯域幅プール全体（設定された最大音声プールからだけではない）の 85 % になります。帯域割り当ては、ローミング コールの場合であっても同じです。

音声優先制御を設定する前に、次のパラメータを設定しておく必要があります。

- 音声コールがパススルーできるように WLAN QoS を設定します。
- 無線の ACM を有効にします。
- WLAN 上で SIP コール スヌーピングを有効にします。

EDCA パラメータについて

拡張型分散チャネルアクセス（EDCA）パラメータは、音声、ビデオ、およびその他の Quality of Service（QoS）トラフィックのために優先的な無線チャネルアクセスを提供するように設計されています。

音声パラメータとビデオ パラメータの設定方法

音声パラメータの設定（CLI）

始める前に

SIP ベースの CAC が設定されていることを確認します。

この手順を開始する前に CAC のクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**show wlan summary** 例： `Device# show wlan summary`	デバイスに設定されているすべての WLAN を指定します。
ステップ 2	**show wlan** *wlan_id* 例： `Device# show wlan 25`	変更する WLAN を指定します。Voice over WLAN の場合、WLAN が WMM に対して設定されており、QoS レベルが Platinum に設定されていることを確認します。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 4	**policy-map** *policy-map name*
	例：
	`Device(config)# policy-map test_2000`
	`Device(config-pmap)#`
		ポリシーマップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。
		WLANでは、これらのコマンドを有効にするには、service-policy を設定する必要があります。

ステップ 5	**class** {*class-name* | **class-default**}
	例：
	`Device(config-pmap)# class test_1000`
	`Device(config-pmap-c)#`
		ポリシー クラス マップ コンフィギュレーションモードを開始します。ポリシーを作成または変更するクラスの名前を指定します。

	コマンドまたはアクション	目的
		ポリシーを作成または変更するクラスの名前を指定します。 未分類のパケットのシステムデフォルト クラスも作成できます。

ステップ 6	**admitcacwmm-tspec**
	例：
	`Device(config-pmap-c)# admit cac wmm-tspec`
	`Device(config-pmap-c)#`
		（任意）ポリシーマップのコールアドミッション制御（CAC）の要求を許可します。

ステップ 7	**service-policy** *policy-map name*
	例：
	`Device(config-pmap-c)# service-policy test_2000`
	`Device(config-pmap-c)#`
		QoS サービス ポリシーを設定します。

ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

ステップ 9	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **wlan shutdown**
	例：
	`Device(config)# wlan wlan1`
	`Device(config-wlan)# wlan shutdown`
		ビデオ パラメータの変更前に、WMM がイネーブルになっている WLAN をすべてディセーブルにします。

ステップ 10	**wlan** *wlan_profile_name wlan_ID SSID_network_name*
	例：
	`Device(config)# wlan wlan1`
	`Device(config-wlan)# wlan shutdown`
		音声パラメータの変更前に、WMM がイネーブルになっている WLAN をすべてディセーブルにします。

ステップ 11	**wlan** *wlan_name* **call-snoop** 例： `Device(config)# wlan wlan1 call-snoop`	特定の WLAN のコール スヌーピングをイネーブルにします。

ステップ 12	**wlan** *wlan_name* **service-policy input** *input_policy_name*
	例：
	`Device(config)# wlan wlan1`
	`Device(config-wlan)# service-policy input platinum-up`
		特定の WLAN の入力 SSID ポリシーを音声に設定します。

	コマンドまたはアクション	目的

ステップ 13	**wlan** *wlan_name* **service-policy output** *ouput_policy_name*
	例：
	`Device(config)# wlan wlan1`
	`Device(config-wlan)# service-policy output platinum`
		特定の WLAN の出力 SSID ポリシーを音声に設定します。

ステップ 14	**wlan** *wlan_name* **service-policy input** *ingress_policy_name*
	例：
	`Device(config)# wlan wlan1`
	`Device(config-wlan)# service-policy input policy1`
		特定の WLAN の入力 SSID ポリシーをユーザ定義ポリシーとして設定します。

ステップ 15	**wlan** *wlan_name* **service-policy output** *egress_policy_name*
	例：
	`Device(config)# wlan wlan1`
	`Device(config-wlan)# service-policy output policy2`
		特定の WLAN の出力 SSID ポリシーをユーザ定義ポリシーとして設定します。

ステップ 16	**ap dot11 {5ghz | 24ghz} shutdown** 例：	無線ネットワークをディセーブルにします。 `Device(config)# ap dot11 5ghz shutdown`
ステップ 17	**ap dot11 {5ghz | 24ghz} cac voice sip** 例： `Device(config)# ap dot11 5ghz cac voice sip`	802.11a または 802.11b/g ネットワークについて、SIP IOSd CAC をイネーブルまたはディセーブルにします。
ステップ 18	**ap dot11 {5ghz | 24ghz} cac voice acm** 例： `Device(config)# ap dot11 5ghz cac voice acm`	802.11a または 802.11b/g ネットワークについて、帯域幅ベースの音声 CAC をイネーブルまたはディセーブルにします。
ステップ 19	**ap dot11 {5ghz | 24ghz} cac voice max-bandwidth** 帯域幅 例： `Device(config)# ap dot11 5ghz cac voice max-bandwidth 85`	802.11a または 802.11b/g ネットワーク上で音声アプリケーション用にクライアントに割り当てられている最大帯域幅の割合を設定します。 帯域幅の範囲は 5 ～ 85 % で、デフォルト値は 75% です。クライアントが指定値に達すると、このネットワーク上での新しいビデオはアクセスポイントで拒否されます。

	コマンドまたはアクション	目的
ステップ 20	**ap dot11 {5ghz | 24ghz} cac voice roam-bandwidth** 帯域幅 例： `Device(config)# ap dot11 5ghz cac voice roam-bandwidth 10`	割り当てられた最大帯域幅のうち、ローミングする音声クライアント用に予約する割合を設定します。 帯域幅の範囲は 0 ～ 25% で、デフォルト値は 6% です。デバイスは、割り当てられた最大帯域幅のうち、この割合の帯域幅をローミングする音声クライアント用に予約します。
ステップ 21	**no wlan shutdown** 例： `Device(config-wlan)# no wlan shutdown`	WMM がイネーブルになっているすべての WLAN を再度イネーブルにします。
ステップ 22	**no ap dot11 {5ghz | 24ghz} shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	無線ネットワークを再度イネーブルにします。
ステップ 23	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

例

ビデオ パラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**show wlan summary** 例： `Device# show wlan summary`	デバイスに設定されているすべての WLAN を指定します。
ステップ 2	**show wlan** *wlan_id* 例： `Device# show wlan 25`	変更する WLAN を指定します。

	コマンドまたはアクション	目的
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 4	**policy-map** *policy-map name*
	例：
	`Device(config)# policy-map test_2000`
	`Device(config-pmap)#`
		ポリシーマップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。
		WLAN では、これらのコマンドを有効にするには、service-policy を設定する必要があります。

ステップ 5	**class** {*class-name* | **class-default**}
	例：
	`Device(config-pmap)# class test_1000`
	`Device(config-pmap-c)#`
		ポリシー クラス マップ コンフィギュレーションモードを開始します。ポリシーを作成または変更するクラスの名前を指定します。
		ポリシーを作成または変更するクラスの名前を指定します。
		未分類のパケットのシステムデフォルト クラスも作成できます。

ステップ 6	**admitcacwmm-tspec**
	例：
	`Device(config-pmap-c)# admit cac wmm-tspec`
	`Device(config-pmap-c)#`
		（任意）ポリシーマップのコールアドミッション制御（CAC）の要求を許可します。

ステップ 7	**service-policy** *policy-map name*
	例：
	`Device(config-pmap-c)# service-policy test_2000`
	`Device(config-pmap-c)#`
		QoS サービス ポリシーを設定します。

ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

	コマンドまたはアクション	目的

ステップ 9	**wlan***wlan_profile_name*
	例：
	`Device(config)# wlan wlan1`
	`Device(config-wlan)# wlan shutdown`
		ビデオ パラメータの変更前に、WMM がイネーブルになっている WLAN をすべてディセーブルにします。

ステップ 10	**ap dot11 {5ghz | 24ghz} shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	無線ネットワークをディセーブルにします。
ステップ 11	**ap dot11 {5ghz | 24ghz} cac video acm** 例： `Device(config)# ap dot11 5ghz cac video acm`	802.11a または 802.11b/g ネットワークについて、帯域幅ベースのビデオ CAC をイネーブルまたはディセーブルにします。
ステップ 12	**ap dot11 {5ghz | 24ghz} cac video load-based** 例： `Device(config)# ap dot11 5ghz cac video load-based`	負荷ベース CAC の方式を設定します。 このコマンドを入力しない場合は、デフォルトのスタティック CAC が適用されます。
ステップ 13	**ap dot11 {5ghz | 24ghz} cac video max-bandwidth** 帯域幅 例： `Device(config)# ap dot11 5ghz cac video max-bandwidth 20`	802.11a または 802.11b/g ネットワーク上でビデオアプリケーション用にクライアントに割り当てられている最大帯域幅の割合を設定します。 帯域幅の範囲は 5 ～ 85 % で、デフォルト値は 75% です。デフォルト値は 0 で、帯域幅の要求は制御されません。音声帯域幅とビデオ帯域幅の合計が、85% または設定した最大メディア帯域幅を超えないようにする必要があります。
ステップ 14	**ap dot11 {5ghz | 24ghz} cac video roam-bandwidth** 帯域幅 例： `Device(config)# ap dot11 5ghz cac video roam-bandwidth 9`	割り当てられた最大帯域幅のうち、ローミングするビデオクライアント用に予約する割合を設定します。 bandwidth の範囲は 0 ～ 25% で、デフォルト値は 0% です。
ステップ 15	**no wlan shutdown** *wlan_id* 例： `Device(config-wlan)# no wlan shutdown 25`	WMM がイネーブルになっているすべての WLAN を再度イネーブルにします。

	コマンドまたはアクション	目的
ステップ 16	**no ap dot11 {5ghz | 24ghz} shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	無線ネットワークを再度イネーブルにします。
ステップ 17	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

例

SIP ベースの CAC の設定（CLI）

SIP CAC は、実行できる SIP 呼び出しの総数を制御します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**wlan** *wlan-name*
	例：
	`Device(config)# wlan qos-wlan`
	`Device(config-wlan)#`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	**call-snoop** 例： `Device(config-wlan)# call-snoop`	特定の WLAN のコール スヌーピング機能をイネーブルにします。
ステップ 4	**service-policy** [**client**] **input** *policy-map name* 例： `Device(config-wlan)# service-policy input platinum-up`	WLAN 入力トラフィックにポリシーマップを割り当てます。入力トラフィックの音声に QoS ポリシーを指定していることを確認します。
ステップ 5	**service-policy** [**client**] **output** *policy-map name* 例：	WLAN 出力トラフィックにポリシーマップを割り当てます。出力トラ

	コマンドまたはアクション	目的
	`Device(config-wlan)# service-policy output platinum`	フィックに音声にQoSポリシーを指定していることを確認します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。
ステップ 7	**show wlan** {*wlan-id* | *wlan-name*} 例： `Device# show wlan qos-wlan`	WLANの設定済みのQoSポリシーを検証します。
ステップ 8	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーションモードを開始します。
ステップ 9	**ap dot11 {5ghz | 24ghz} cac {voice | video} acm** 例： `Device(config)# ap dot11 5ghz cac voice acm`	無線の静的 ACM をイネーブルにします。 SIP スヌーピングをイネーブルにする場合、静的CACではなく、負荷ベースの CAC を使用します。
ステップ 10	**ap dot11 {5ghz | 24ghz} cac voice sip** 例： `Device(config)# ap dot11 5ghz cac voice sip`	SIP-Based CAC を設定します。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

例

優先コール番号の設定（CLI）

始める前に

優先コール番号を設定する前に、次のパラメータを設定する必要があります。

- WLAN QoS を音声に設定します。
- 無線の ACM を有効にします。

- WLAN 上で SIP コール スヌーピングを有効にします。
- SIP ベース CAC をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**wlan** *wlan-name* **qos platinum**
	例：
	`Device(config)# wlan wlan1`
	`Device(config-wlan)# qos platinum`
		特定の WLAN の QoS を音声に設定します。

ステップ 3	**ap dot11 {5ghz | 24ghz} cac {voice | video} acm** 例： `Device(config)# ap dot11 5ghz cac voice acm`	無線の静的 ACM をイネーブルにします。 SIP スヌーピングをイネーブルにする場合、静的 CAC ではなく、負荷ベースの CAC を使用します。

ステップ 4	**wlan** *wlan-name*
	例：
	`Device(config)# wlan wlan1`
	`Device(config-wlan)# call-snoop`
		特定の WLAN のコール スヌーピング機能をイネーブルにします。

ステップ 5	**wireless sip preferred-call-no** *call_index call_number* 例： `Device(config)# wireless sip preferred-call-no 1 555333`	新しい優先コールを追加します。
ステップ 6	**no wireless sip preferred-call-no** *call_index* 例： `Device(config)# no wireless sip preferred-call-no 1`	優先コールを削除します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

EDCA パラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 {5ghz | 24ghz } shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	無線ネットワークをディセーブルにします。
ステップ 3	**ap dot11 {5ghz | 24ghz} edca-parameters {custom-voice | optimized-video-voice | optimized-voice | svp-voice | wmm-default}** 例： `Device(config)# ap dot11 5ghz edca-parameters optimized-voice`	802.11a または 802.11b/g ネットワークに対する特定の EDCA パラメータをイネーブルにします。 • [custom-voice]：802.11a または 802.11b/g ネットワーク用のカスタム音声パラメータをイネーブルにします。 • [optimized-video-voice]：802.11a または 802.11b/g ネットワークに対する EDCA 音声およびビデオ最適化パラメータをイネーブルにします。 ネットワーク上で音声サービスとビデオ サービスを両方とも展開する場合に、このオプションを選択します。 • [optimized-voice]：SpectraLink 以外の音声用に最適化された 802.11a または 802.11b/g ネットワークに対するプロファイルパラメータをイネーブルにします。 ネットワーク上で SpectraLink 以外の音声サービスを展開する場合に、このオプションを選択します。

	コマンドまたはアクション	目的
		• [svp-voice]：802.11a または 802.11b/g ネットワークに対する SpectraLink 音声優先パラメータをイネーブルにします。 コールの品質を向上させるためにネットワーク上で SpectraLink の電話を展開する場合に、このオプションを選択します。 • [wmm-default]：802.11a または 802.11b/g ネットワークに対する Wi-Fi Multimedia（WMM）デフォルト パラメータをイネーブルにします。 これはデフォルト値です。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。
ステップ 4	**show ap dot11 {5ghz | 24ghz} network** 例： `Device(config)# show ap dot11 5ghz network`	音声用の MAC 最適化の現在のステータスを表示します。
ステップ 5	**no ap dot11 {5ghz | 24ghz} shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	無線ネットワークを再度イネーブルにします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

音声およびビデオ パラメータのモニタリング

このセクションでは、音声およびビデオパラメータに関する新しいコマンドについて説明します。

次のコマンドは、音声およびビデオ パラメータをモニタするために使用できます。

表 *196*：音声およびビデオ パラメータ コマンド

コマンド	目的
show ap dot11 {5ghz | 24ghz} network	無線ベースの音声統計情報を表示します。
show ap name *ap_name***dot11 24ghz tsm all**	TSM の音質メトリックと、音声用の MAC 最適化の現在のステータスを表示します。
show ap name *apname***cac voice**	特定アクセス ポイントの CAC に関する情報を表示します。
show client detail *client_mac*	特定のクライアントの U-APSD 状態を表示します。
show policy-map interface wireless client	ビデオ クライアント ポリシーの詳細を表示します。
show access-list	デバイス由来のビデオクライアントダイナミック アクセス リストを表示します。
show wireless client voice diag status	音声診断がイネーブルになっているかディセーブルになっているかについて表示します。イネーブルになっている場合は、ウォッチ リスト内のクライアントに関する情報とボイスコール診断の残り時間も表示します。 （注） 音声診断 CLI で機能するためには、次のコマンドを入力する必要があります。**debug voice-diagnostic mac-addr** *client_mac_01 client_mac_02*
show wireless client voice diag tspec	音声診断が有効になっているクライアントから送信された TSPEC 情報が表示されます。
show wireless client voice diag qos-map	QoS/DSCP マッピングに関する情報と 4 つのキュー（VO、VI、BE、BK）それぞれのパケット統計が表示されます。各種 DSCP 値も表示されます。
show wireless client voice diag rssi	音声診断が有効になっている場合、クライアントの過去 5 秒間の RSSI 値が表示されます。
show client voice-diag roam-history	過去3回のローミング コールに関する情報が表示されます。出力には、タイムスタンプ、ローミングに関連したアクセス ポイント、およびローミングの理由が含まれ、ローミングに失敗した場合にはその理由も含まれます。
show policy-map interface wireless mac *mac-address*	音声およびビデオデータのパケット統計情報を表示します。
show wireless media-stream client summary	メディア ストリームおよびビデオ クライアント情報のサマリーを表示します。

show controllers d0 | b queue	アクセス ポイントにおいて、パケットが通過するキューを表示します。
show platform qos queue stats *interface*	デバイスからのパケットが通過するキューを表示します。

次のコマンドを使用してビデオ パラメータをモニタできます。

表 *197 :* ビデオ パラメータ モニタリング コマンド

コマンド	目的
show ap join stats summary *ap_mac*	特定のアクセス ポイントにおける、最後の接続エラーの詳細を表示します。
show ip igmp snooping wireless mgid	TSM の音質メトリックと、音声用の MAC 最適化の現在のステータスを表示します。
show wireless media-stream multicast-direct state	メディア ストリーム マルチキャストダイレクト パラメータを表示します。
show wireless media-stream group summary	メディア ストリームとクライアント情報のサマリーを表示します。
show wireless media-stream group detail *group_name*	特定のメディアストリーム グループの詳細を表示します。
show wireless media-stream client summary	メディア ストリーム クライアント セットの詳細を表示します。
show wireless media-stream client detail *group_name*	メディア ストリーム クライアント セットの詳細を表示します。
show ap dot11 {5ghz | 24ghz) media-stream rrc	メディア ストリームの詳細を表示します。
show wireless media-stream message details	メッセージ設定に関する情報を表示します。
show ap name *ap-name***auto-rf dot11 5ghz | i Util**	チャネル使用率の詳細を表示します。
show controllers d0 | b queue	2.4 GHz、5 GHz 帯域ベースのアクセス ポイントにおいて、パケットがどのキューを通過しているかを表示します。
show controllers d1 | b queue	2.4 GHz、5 GHz 帯域ベースのアクセス ポイントにおいて、パケットがどのキューを通過しているかを表示します。

show cont d1 | b Media	帯域 A または B のビデオ メトリックの詳細を表示します。
show capwap mcast mgid all	アクセスポイントに関連付けられたすべてのマルチキャストグループとそれらに対応するマルチキャストグループ ID（MGIDs）に関する情報を表示します。
show capwap mcast mgid id *id*	特定の MGID のマルチキャスト グループに属するすべてのビデオ クライアントに関する情報を表示します。

音声およびビデオ パラメータの設定例

例：音声およびビデオの設定

音声およびビデオ用の出力 SSID ポリシーの設定

次に、音声およびビデオ用の出力 SSID ポリシー を作成して設定する例を示します。

```
table-map egress_ssid_tb
 map from 24 to 24
 map from 34 to 34
 map from 46 to 46
 default copy

class-map match-any voice
  match  dscp ef
class-map match-any video
  match  dscp af41

policy-map ssid-cac
class class-default
    shape average 25000000
   set dscp dscp table egress_ssid_tb
   queue-buffers ratio 0
   service-policy ssid-child-cac

policy-map ssid-child-cac
 class voice
    priority level 1
    police 5000000
     conform-action transmit
     exceed-action drop
    admit cac wmm-tspec
      rate 1000
      wlan-up  6 7
 class video
    priority level 2
    police 10000000
      conform-action transmit
      exceed-action drop
    admit cac wmm-tspec
      rate 3000
      wlan-up  4 5
```

音声およびビデオ用の入力 SSID ポリシーの設定

次に、音声およびビデオ用の入力 SSID ポリシー を作成して設定する例を示します。

```
table-map up_to_dscp
 map from 0 to 0
 map from 1 to 8
 map from 2 to 8
 map from 3 to 0
 map from 4 to 34
 map from 5 to 34
 map from 6 to 46
 map from 7 to 48
 default copy

policy-map ingress_ssid
 class class-default
   set dscp wlan user-priority table up_to_dscp
```

音声およびビデオ用の出力ポート ポリシーの設定

次に、音声およびビデオ用の出力ポート ポリシー を作成して設定する例を示します。

```
policy-map port_child_policy
 class non-client-nrt-class
 bandwidth remaining ratio 10

 class voice
 priority level 1
 police rate 3000000

 class video
 priority level 2
 police rate 4000000
```

WLAN の音声とビデオに関する入出力 SSID ポリシーの適用

次に、WLAN の音声とビデオに関する入出力 SSID ポリシーを適用する例を示します。

```
wlan voice_video 1 voice_video
 service-policy input ingress_ssid
 service-policy output ssid-cac
```

音声およびビデオ パラメータに関する追加情報

関連資料

関連項目	マニュアル タイトル
マルチキャストの設定	*Multicast Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
VideoStream 設定	*VideoStream Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

音声およびビデオ パラメータ設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

第 137 章

RFID タグ追跡の設定

- 機能情報の確認 （2987 ページ）
- RFID タグ追跡の設定について （2987 ページ）
- RFID タグ トラッキングの設定方法 （2988 ページ）
- RFID タグ トラッキング情報のモニタリング （2989 ページ）
- RFID タグ トラッキングに関する追加情報 （2989 ページ）
- RFID タグ トラッキング設定の機能履歴と情報 （2990 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

RFID タグ追跡の設定について

Deviceでは、Radio-Frequency Identification（RFID）タグ トラッキングを設定できます。RFID タグは、資産の位置をリアルタイムで追跡するために取り付けられる、小型の無線装置です。タグは、その位置を専用の 802.11 パケットを使用してアドバタイズします。このパケットは、アクセス ポイント、コントローラ、およびロケーション アプライアンスで処理されます。

RFID タグ トラッキングの設定方法

RFID タグ追跡の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**location rfid status** 例： `Device(config)# location rfid status`	RFID タグ追跡をイネーブルにします。 デフォルトでは、RFID タグ トラッキングはイネーブルになっています。
ステップ 2	（任意） **no location rfid status** 例： `Device(config)# no location rfid status`	RFID タグ トラッキングをディセーブルにします。
ステップ 3	**location rfid timeout** *seconds* 例： `Device(config)# location rfid timeout 1500`	静的なタイムアウト値（60 ～ 7200 秒）を指定します。 静的なタイムアウト値は、タグを失効させずにデバイスが保持する期間です。たとえば、タグが 30 秒ごとにビーコンするよう設定されている場合は、タイムアウト値を 90 秒（ビーコン値の約 3 倍）に設定することをお勧めします。デフォルト値は 1200 秒です。
ステップ 4	**location rfid mobility vendor-name** *name* 例： `Device(config)# location rfid mobility vendor-name Aerosct`	特定のタグについて RFID タグ モビリティをイネーブルにします。**location rfid mobility vendor-name** コマンドを入力すると、タグが設定を選択および/またはダウンロードしようとするとき、クライアント モードの DHCP アドレスを取得できません。 （注） これらのコマンドは Pango タグに対してのみ使用できます。したがって、**vendor_name** に指定できる値は、すべて小文字の「pango」のみとなります。

	コマンドまたはアクション	目的
ステップ 5	（オプション）**no location rfid mobility** *name* 例： `Device(config)# no location rfid mobility test`	特定のタグについて RFID タグ モビリティをディセーブルにします。**no location rfid mobility** コマンドを入力すると、タグは DHCP アドレスを取得できます。タグがあるサブネットから別のサブネットへ移動すると、タグは、アンカー状態を維持するのではなく、新しいアドレスを取得します。

RFID タグ トラッキング情報のモニタリング

このセクションでは、RFID タグ トラッキング情報に関する新しいコマンドについて説明します。

次のコマンドはの RFID タグ トラッキング情報をモニタするために使用できます。

表 *198 : RFID* タグ トラッキング情報モニタリング コマンド

コマンド	目的
show location rfid config	RFID タグ トラッキングの現在の設定を表示します。
show location rfid detail *mac_address*	特定の RFID タグの詳細情報を表示します。
show location rfid summary	現在に接続されているすべての RFID タグのリストを表示します。
show location rfid client	クライアントとしてに関連付けられている RFID タグのリストを表示します。

RFID タグ トラッキングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

RFID タグ トラッキング設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

第 138 章

ロケーションの設定

- 機能情報の確認 （2991 ページ）
- ロケーションの設定に関する情報 （2991 ページ）
- ロケーションの設定方法 （2992 ページ）
- ロケーション設定および NMSP 設定のモニタリング （2997 ページ）
- 例：ロケーションの設定 （2998 ページ）
- 例：NMSP の設定 （2998 ページ）
- ロケーション設定に関する追加情報 （2999 ページ）
- ロケーション設定の機能履歴と情報 （3000 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

ロケーションの設定に関する情報

デバイスは、対象クライアントデバイス周辺のアクセスポイントから受信信号強度表示（RSSI）測定値を収集し、このクライアントのロケーションを特定します。デバイスは、最大 16 台のアクセス ポイントから、クライアント、RFID タグ、および不正なアクセス ポイントのロケーション レポートを取得できます。

通常のクライアントまたは調整クライアントのパス損失測定（S60）要求を設定すると、ロケーションの精度を向上させることができます。

ロケーションの設定方法

ロケーションの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**location plm** {**calibrating** [**multiband** | **uniband**] | **client** *burst_interval* 例： `Device(config)# location plm client 100`	調整または非調整クライアントのパス損失測定（S60）要求を設定します。 パス損失測定要求で、位置精度が向上します。標準の非調整クライアントに対して、0 ～ 3600 秒の範囲で **burst_interval** パラメータを設定できます。デフォルト値は 60 秒です。 関連付けされた 802.11a または 802.11b/g 無線、関連付けされた 802.11a/b/g 無線の調整クライアントにパス損失測定要求を設定できます。 クライアントからプローブが送信される頻度が低い場合や、少数のチャネルに対してしか送信されない場合は、クライアントのロケーションが更新不可能になるか、精度が低下します。**location plm** コマンドを実行すると、クライアントは強制的に、すべてのチャネルに対してパケットを送信するようになります。CCXv4 以上のクライアントがアソシエートすると、Deviceはそのクライアントにパス損失測定要求を送信します。これは、アクセスポイントが使用している帯域とチャネル（2.4 GHz のみのアクセスポイントの場合は一般にチャネル 1、6、および 11）で無期限に送信するようクライアントに指示するものです。送信する間隔は設定可能です（たとえば 60 秒）。

	コマンドまたはアクション	目的
ステップ 3	**location rssi-half-life** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *seconds* 例： `Device(config)# location rssi-half-life calibrating-client 60`	クライアント、調整クライアント、RFID タグ、不正アクセス ポイントの RSSI 半減期を設定します。 クライアント、調整クライアント、RFID タグ、不正アクセス ポイントの **location rssi-half-life** パラメータ値を入力できます。指定可能な値は、0、1、2、5、10、20、30、60、90、120、180、または 300 秒です。デフォルト値は 0 秒です。 クライアントデバイスの中には、チャネル変更直後は送信電力を下げるものがあるのと、RF は変動しやすいことから、RSSI の値がパケットごとに大きく異なることもあります。**location rssi-half-life** コマンドを実行すると、精度を向上させるために、均一でない状態で受信したデータを平均化するための半減期（ハーフライフ）を設定することができます。 （注） **location rssi-half-life** コマンドを使用したり、変更したりしないことをお勧めします。
ステップ 4	**location expiry** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *timeout* 例： `Device(config)# location expiry calibrating-client 50`	クライアント、調整クライアント、RFID タグ、不正アクセス ポイントの RSSI タイムアウト値を設定します。 クライアント、RFID タグ、不正アクセス ポイントの RSSI タイムアウト値を入力できます。範囲は 5 ～ 3600 秒で、デフォルト値は 5 秒です。 調整クライアントには 0 ～ 3600 秒の範囲で RSSI タイムアウト値を入力でき、デフォルト値は 5 秒です。 ロケーションを正確に特定するには、CPU が保持する RSSI が最近のものであることと、その値が大きいことが必要です。**location expiry** コマンドを使用すると、古い RSSI 平均が失効するまでの時間を指定できます。

	コマンドまたはアクション	目的
		（注） **location expiry** コマンドを使用したり、変更したりしないことをお勧めします。
ステップ 5	**location algorithm** {**rssi-average** | **simple**} 例： `Device(config)# location algorithm rssi-average`	RSSI および信号対雑音比（SNR）値の平均の算出に使用されるアルゴリズムを設定します。 **location algorithm rssi-average** コマンドを入力することで、より正確な、しかしより CPU オーバーヘッドの高いアルゴリズムを指定できます。または、**location algorithm simple** コマンドを入力することで、高速で CPU のオーバーヘッドが低い、しかし精度に欠けるアルゴリズムを指定することもできます。 （注） **location algorithm** コマンドは、使用したり、変更したりしないことをお勧めします。
ステップ 6	**location admin-tag** *string* 例： `Device(config)# location admin-tag`	クライアントデバイスの場所の管理タグまたはサイト情報を設定します。
ステップ 7	**location civic-location identifier** {*identifier* | **host**} 例： `Device(config)# location civic-location identifier host`	都市ロケーション情報を指定します。 文字列またはホストとして都市ロケーション識別子を設定できます。
ステップ 8	**location custom-location identifier** {*identifier* | **host**} 例： `Device(config)# location custom-location identifier host`	カスタムロケーション情報を指定します。 文字列またはホストとしてカスタムロケーション識別子を設定できます。
ステップ 9	**location geo-location identifier** {*identifier* | **host**} 例： `Device(config)# location geo-location identifier host`	クライアントデバイスの地理的なロケーション情報を指定します。 文字列またはホストとしてロケーション識別子を設定できます。

	コマンドまたはアクション	目的
ステップ 10	**location prefer** {**cdp** | **lldp-med** | **static**} **weight** *priority_value* 例： `Device(config)# location prefer weight cdp 50`	ロケーション情報のソースのプライオリティを設定します。 優先順位のウェイトは、0 から 255 の範囲で入力できます。
ステップ 11	**location rfid** {**status** | **timeout** | **vendor-name**} 例： `Device(config)# location rfid timeout 100`	RFID タグ ステータス、RFID タイムアウト値、RFID タグ ベンダー名などの RFID タグ トラッキング オプションを設定します。 60 ～ 7200 秒の範囲で RFID タイムアウト値を入力できます。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

例

クライアント、RFID タグ、および不正デバイスの NMSP 通知間隔の変更（CLI）

ネットワーク モビリティ サービス プロトコル（NMSP）によって、Mobility Services Engine とコントローラの間の発信/着信トラフィックに関する通信の管理が行われます。高い頻度でのロケーション更新を必要とするアプリケーションがある場合は、クライアント、アクティブな RFID タグ、および不正なアクセス ポイント/クライアントの NMSP 通知間隔を 1 ～ 180 秒の範囲内で変更できます。

（注） コントローラと Mobility Services Engine との通信には、TCP ポート 16113 が使用されます。コントローラと Mobility Services Engine の間にファイアウォールがある場合は、NMSP を機能させるにはこのポートが開いている（ブロックされていない）ことが必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**nmsp notification interval** {**attachment** *seconds* | **location** *seconds* | **rssi** [**clients** *interval* | **rfid** *interval* | **rogues** [**ap** | **client**] *interval*]} 例： `Device(config)# nmsp notification interval rssi rfid 50`	クライアント、RFID タグ、不正クライアント、不正アクセスポイントの NMSP 通知間隔を設定します。 1 ～ 180 秒の範囲で RSSI 測定値の NMSP 通知間隔の値を入力できます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

クライアント、RFID タグ、および不正デバイスの NMSP 通知しきい値の変更（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**location notify-threshold** {**clients** | **rogues ap** | **tags** } *threshold* 例： `Device(config)# location notify-threshold clients 5`	クライアント、RFID タグ、不正なクライアント、不正なアクセス ポイントの NMSP 通知しきい値を設定します。 RSSI しきい値は、0 ～ 10 db の範囲で入力できます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

ロケーション設定および NMSP 設定のモニタリング

ロケーション設定のモニタリング（CLI）

このセクションでは、ロケーション設定に関する新しいコマンドについて説明します。

次のコマンドは、 のロケーション設定のモニタリングに使用できます。

表 *199 :* ロケーション設定モニタリング コマンド

コマンド	目的
show location summary	現在のロケーション設定値を表示します。
show location statistics rfid	ロケーションベースの RFID 統計情報を表示します。
show location detail *client_mac_addr*	特定のクライアントの RSSI テーブルを表示します。

NMSP 設定のモニタリング（CLI）

このセクションでは、NMSP 設定に関する新しいコマンドについて説明します。

次のコマンドがの NMSP 設定のモニタリングに使用できます。

表 *200 : NMSP* 設定モニタリング コマンド

コマンド	目的
show nmsp attachment suppress interfaces	アタッチメント抑制インターフェイスを表示します。
show nmsp capability	NMSP 機能を表示します。
show nmsp notification interval	NMSP 通知間隔を表示します。
show nmsp statistics connection	接続固有の NMSP カウンタを表示します。
show nmsp statistics summary	一般的な NMSP カウンタを表示します。
show nmsp status	アクティブな NMSP 接続の状態を表示します。
show nmsp subscription detail	がサブスクライブされているモビリティ サービスをすべて表示します。

show nmsp subscription detail *ip_addr*	特定のIPアドレスにサブスクライブされたモビリティサービスについてのみ詳細を表示します。
show nmsp subscription summary	がサブスクライブされているすべてのモビリティサービスの詳細を表示します。

例：ロケーションの設定

次に、関連付けされた802.11aまたは802.11b/g無線の調整クライアント用パス損失測定（S60）要求を設定する例を示します。

```
Device# configure terminal
Device(config)# location plm calibrating uniband
Device(config)# end
Device# show location summary
```

次に、不正アクセス ポイントの RSSI 半減期を設定する例を示します。

```
Device# configure terminal
Device(config)# location rssi-half-life rogue-aps 20
Device(config)# end
Device# show location summary
```

例：NMSP の設定

次に、RFID タグの NMSP 通知間隔を設定する例を示します。

```
Device# configure terminal
Device(config)# nmsp notification interval rssi rfid 50
Device(config)# end
Device# show nmsp notification interval
```

次に、クライアントの NMSP 通知しきい値を設定する例を示します。

```
Device# configure terminal
Device(config)# nmsp notify-threshold 5
Device(config)# end
Device# show nmsp statistics summary
```

ロケーション設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ロケーション設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

第 139 章

Cisco Hyperlocation

- 機能情報の確認 （3001 ページ）
- Cisco Hyperlocation の制約事項 （3001 ページ）
- Cisco Hyperlocation について （3001 ページ）
- Cisco Hyperlocation の設定：グローバル設定（CLI） （3003 ページ）
- AP グループへの Cisco Hyperlocation の設定（CLI） （3005 ページ）
- HyperLocation BLE ビーコン パラメータの設定 （3007 ページ）
- AP への Hyperlocation BLE ビーコン パラメータの設定 （3008 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Cisco Hyperlocation の制約事項

- FlexConnect モードはサポートされていません。
- IPv4 アドレスのみが NTP サーバでサポートされています。
- 個々の AP で Cisco Hyperlocation を無効にすることはできません。

Cisco Hyperlocation について

Cisco Hyperlocation は、1 メートルの精度でワイヤレス クライアントの場所を追跡できる、比類なく精密なロケーション ソリューションです。これは、Cisco Aironet 3600 および 3700 シ

リーズアクセスポイントの一部である Cisco Hyperlocation 無線モジュールによって可能となっています。この強力なモジュールは、Wi-Fi および Bluetooth Low Energy（BLE）技術と組み合わさることで、ビーコン、インベントリおよび個人のモバイルデバイスを正確に示すことができます。

Cisco Hyperlocation の無線モジュールには、以下の機能があります。

- 以下の拡張性を備えた WSM 無線モジュール機能：
  - 802.11ac
  - Wi-Fi 送信
  - 20 MHz、40 MHz、80 GHz チャネル帯域幅に拡張された WSM、RRM チャネル スキャン。
- 拡張ロケーション機能：
  - 低遅延ロケーション最適化チャネルのスキャン
  - 32 アンテナ到達角度（AoA）

Cisco Hyperlocation は、シスコ コネクテッド モバイル エクスペリエンス（CMX）と連動して機能します。Cisco Catalyst 3850 または 3650 シリーズ スイッチの Cisco Hyperlocation 機能と CMX デバイスを組み合わせることで、ロケーション精度が向上し、より的を絞ったコンテンツをユーザに配信できます。Cisco CleanAir の周波数スキャンとともに CMX を使用する場合は、失敗したビーコン、失われたビーコン、また不正なビーコンでさえ見つけることが簡単です。

Cisco IOS XE Denali 16.3.1 リリースでの機能拡張

- 統合 BLE 無線を備えた Cisco Hyperlocation 無線モジュールでは、最大 5 つの BLE トランスミッタを使用して、Bluetooth Low Energy（BLE）ブロードキャスト メッセージを送信することができます。Cisco Catalyst 3850/3650 スイッチは、ビーコンの間隔、UUID、送信電力などの送信パラメータを、ビーコンごとにすべてのアクセスポイントに対しグローバルに設定するために使用されます。また、Cisco Catalyst 3850/3650 スイッチは、各アクセスポイントのメジャー、マイナー、および送信電力値を設定できるため、ビーコンの精度がより高まります。この機能は、Cisco Hyperlocation 無線モジュールおよび Hyperlocation 機能と共に動作します。

  （注） Hyperlocation BLE が機能するには、Cisco Hyperlocation 機能を AP で有効にする必要があります。

- Cisco Hyperlocation 無線モジュールが AP にインストールされていない場合に、データ パケット RSSI を経由するロケーション パフォーマンスが CPU サイクル スティーリングによるローカル モード無線を通じて報告されるように、Cisco Hyperlocation 機能は強化されています。この機能拡張は次の AP で使用できます。

- Cisco Aironet 700 シリーズ AP
- Cisco Aironet 1700 シリーズ AP
- Cisco Aironet 2600 シリーズ AP
- Cisco Aironet 2700 シリーズ AP
- Cisco Aironet 3600 シリーズ AP
- Cisco Aironet 3700 シリーズ AP

- AP グループに対し Cisco Hyperlocation を設定できます。以前は、Cisco Hyperlocation の設定はすべての AP にグローバルに適用可能でした。

その他の参考資料

Cisco Hyperlocation の詳細については、次の文書を参照してください。

- 『Cisco Hyperlocation Solution』
- 『Cisco CMX 10.2 Configuration Guide to enable Cisco Hyperlocation』
- 『Cisco ASA 10.2 Release Notes』

Cisco Hyperlocation の設定：グローバル設定（CLI）

手順

- **configureterminal**

  例：

  ```
  Device# configure terminal
  ```

  グローバル コンフィギュレーション モードを開始します。

- **[no] ap hyperlocation**

  例：

  ```
  Device(config)# [no] ap hyperlocation
  ```

  すべての AP で Hyperlocation を有効または無効にします。

- **[no] ap hyperlocation threshold detection** *value-in-dBm*

  例：

  ```
  Device(config)# [no] ap hyperlocation threshold detection -100
  ```

  低い RSSI を持つパケットを除外するためのしきい値を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。

- **[no] ap hyperlocation threshold reset** *value-btwn-0-99*

  例：

  ```
  Device(config)# [no] ap hyperlocation threshold reset 8
  ```

  トリガー後のスキャン サイクルの値をリセットします。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。

- **[no] ap hyperlocation threshold trigger** *value-btwn-1-100*

  例：

  ```
  Device(config)# [no] ap hyperlocation threshold trigger 10
  ```

  BAR をクライアントに送信する前のスキャン サイクルの数を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。

- **[no] ap ntp ip** *ipv4-address-of-ntp-server*

  例：

  ```
  Device(config)# [no] ap ntp ip 9.0.0.4
  ```

  アクセス ポイントによって直接到達可能な、NTP サーバの IPv4 アドレスを設定します。このコマンドの **[no]** 形式を使用すると、NTP 値が 0.0.0.0 にリセットされます。

- **show ap hyperlocation summary**

  例：

  ```
  Device# show ap hyperlocation summary

  Site Name: default-group
  Site Description:
  Hyperlocation operational status: Up
  Reason: N/A
  Hyperlocation NTP server currently used: 9.0.0.4
  Hyperlocation admin status: Enabled
  Hyperlocation detection threshold: -100 dBm
  Hyperlocation trigger threshold: 10
  Hyperlocation reset threshold: 8
  ```

  デフォルトの AP グループの全体の設定値および動作ステータスとパラメータを表示します。

- **show ap hyperlocation detail**

  例：

  ```
  Device# show ap hyperlocation detail

  Site Name: default-group
  Site Description:
  Hyperlocation operational status: Up
  Reason: N/A
  Hyperlocation NTP server currently used: 9.0.0.4
  Hyperlocation admin status: Enabled
  Hyperlocation detection threshold: -100 dBm
  Hyperlocation trigger threshold: 10
  Hyperlocation reset threshold: 8

  Values for APs in all AP Groups:
  ```

```
AP Name                 Radio MAC        Method    Hyperlocation
-----------------------------------------------------------------
APf07f.0635.2d40        f07f.0676.3b89   WSM       Enabled
APf4cf.e272.4ed0        f4cf.e223.ba31   Local     Enabled
```

全体的な設定値と AP ごとの設定値の両方と動作ステータスを表示します。AP 行の [Method] 列には、ローカル モード FastLocate での AP の「ローカル」が表示されます。Hyperlocation のステータスとパラメータに表示される値は、デフォルト AP グループの値を反映します。

- **set platform software trace wireless switch active R0 hyperlocation** {**debug** | **emergency** | **error** | **info** | **noise** | **notice** | **verbose** | **warning**}

  Cisco Hyperlocation に固有のトレース コマンドは次のとおりです。

  - **debug**：デバッグ メッセージ
  - **emergency**：緊急事態が考えられるメッセージ
  - **error**：エラー メッセージ
  - **info**：情報メッセージ
  - **noise**：考えられる最大のメッセージ
  - **notice**：通知メッセージ
  - **verbose**：詳細デバッグ メッセージ
  - **warning**：警告メッセージ

AP グループへの Cisco Hyperlocation の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap group** *ap-group-name* 例： `Device(config)# ap group my-ap-group`	アクセス ポイント グループを作成します。

	コマンドまたはアクション	目的
ステップ 3	**[no] hyperlocation** 例： `Device(config-apgroup)# [no] hyperlocation`	AP グループ *my-ap-group* の Hyperlocation を有効または無効にします。
ステップ 4	**[no] hyperlocation threshold detection** *value-in-dBm* 例： `Device(config-apgroup)# [no] hyperlocation threshold detection -100`	低い RSSI を持つパケットを除外するためのしきい値を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
ステップ 5	**[no] hyperlocation threshold reset** *value-btwn-0-99* 例： `Device(config-apgroup)# [no] hyperlocation threshold reset 8`	トリガー後のスキャンサイクルの値をリセットします。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
ステップ 6	**[no] hyperlocation threshold trigger** *value-btwn-1-100* 例： `Device(config-apgroup)# [no] hyperlocation threshold trigger 10`	BAR をクライアントに送信する前のスキャンサイクルの数を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
ステップ 7	**[no] ntp ip** *ipv4-address-of-ntp-server* 例： `Device(config-apgroup)# [no] ntp ip 9.0.0.4`	AP グループの AP によって直接到達可能な、NTP サーバの IPv4 アドレスを設定します。このコマンドの **[no]** 形式を使用すると、NTP 値が 0.0.0.0 にリセットされます。

ステップ 8	**show ap group** *ap-group-name* **hyperlocation summary**
	例：
	`Device# show ap group my-ap-group hyperlocation summary`
	
	`Site Name: my-ap-group`
	`Site Description: This is an AP group`
	`Hyperlocation operational status: Up`
	`Reason: N/A`
	`Hyperlocation NTP server currently used: 9.0.0.4`
	`Hyperlocation admin status: Enabled`
	`Hyperlocation detection threshold: -100 dBm`
	`Hyperlocation trigger threshold: 11`
	`Hyperlocation reset threshold: 9`
		AP グループ *my-ap-group* の全体の設定値（AP グループ固有）および動作ステータスとパラメータを表示します。

	コマンドまたはアクション	目的

ステップ 9	**show ap group** *ap-group-name* **hyperlocation detail**
	例：
	`Device# show ap group my-ap-group hyperlocation detail`
	
	`Site Name: my-ap-group`
	`Site Description: This is an AP group`
	`Hyperlocation operational status: Up`
	`Reason: N/A`
	`Hyperlocation NTP server currently used: 9.0.0.4`
	`Hyperlocation admin status: Enabled`
	`Hyperlocation detection threshold: -100 dBm`
	`Hyperlocation trigger threshold: 11`
	`Hyperlocation reset threshold: 9`
	
	`Values for APs in all AP Groups:`
	
	`AP Name  Radio MAC  Method  Hyperlocation`
	`APf07f.0635.2d40  f07f.0676.3b89  WSM  Enabled`
	`APf4cf.e272.4ed0  f4cf.e223.ba31  Local  Enabled`
		AP グループ *my-ap-group* の全体（AP グループ固有）の設定値および AP ごとの設定値と動作ステータスを表示します。リストされている AP は、AP グループに属するもののみです。

ステップ 10	**show ap groups**
	例：
	`Device# show ap groups`
	
	`Site Name: my-ap-group`
	`Site Description: This is an AP group`
	`...`
	`Hyperlocation operational status: Up`
	`...`
		各 AP グループの Hyperlocation の動作ステータスを表示します。

HyperLocation BLE ビーコン パラメータの設定

Hyperlocation BLE ビーコン パラメータを設定するには、次の手順を実行します。

手順

ステップ 1 **configure terminal**

例：

```
Controller# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **ap hyperlocation ble-beacon** {*beacon-id* | **interval** *interval-value*}

例：

```
Controller(config)# ap hyperlocation ble-beacon 3
```

BLE ビーコン パラメータを指定して、BLE コンフィギュレーション モードを開始します。

ステップ 3 **config-ble** { **default** {**enable** | **txpwr** | **uuid** } | **enable** | **exit** | **no** {**enable** | **txpwr** | **uuid** } | **txpwr** *att-value* | **uuid** *uuid-name*}

例：

```
Controller(config-ble)# enable
```

BLE ビーコン値を設定します。

ステップ 4 **show ap hyperlocation ble-beacon**

例：

```
Controller# show ap hyperlocation ble-beacon

BLE Beacon interval (Hertz): 1

ID UUID     TX Power(dBm) Status
-----------------------------------------------------------------
0 00000000-0000-0000-0000-000000000000  -34   Disabled
1 00000000-0000-0000-0000-000000000000  0   Disabled
2 00000000-0000-0000-0000-000000000000  0   Disabled
3 00000000-0000-0000-0000-000000000000  0   Disabled
4 00000000-0000-0000-0000-000000000000  0   Disabled
```

設定済み BLE ビーコンのリストを表示します。

AP への Hyperlocation BLE ビーコン パラメータの設定

AP に Hyperlocation BLE ビーコン パラメータを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name***hyperlocation ble-beacon** *beacon-id* {**major** *major-value* | **minor** *minor-value* | **txpwr** *att-value* } 例： `Controller# ap name test-ap hyperlocation ble-beacon 3 major 65535`	AP に Hyperlocation と関連パラメータを設定します。

	コマンドまたはアクション	目的

ステップ 2	**show ap name** *ap-name***hyperlocation ble-beacon**
	例：
	`Controller# show ap name test-ap hyperlocation ble-beacon`
	`ID  Major  Minor  TX Power(dBm)`
	`---`
	`0  0  0  0`
	`1  0  0  0`
	`2  0  0  0`
	`3  0  0  0`
		設定済み BLE ビーコンのリストを表示します。

第 140 章

フロー制御のモニタリング

- 機能情報の確認 （3011 ページ）
- フロー制御の概要 （3011 ページ）
- フロー制御のモニタリング （3011 ページ）
- 例：フロー制御のモニタリング （3012 ページ）
- フロー制御のモニタリングに関する追加情報 （3013 ページ）
- フロー制御のモニタリングに関する機能履歴および情報 （3014 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

フロー制御の概要

デフォルトでは、デバイスでフロー制御がイネーブルになっています。

フロー制御は信頼できる IPC に WCM と Cisco IOS のシム レイヤを提供します。WCM のすべてのコンポーネントに専用チャネルがあります。フロー制御を利用する WCM のコンポーネントはわずかです。CLI からのフロー制御の設定はありません。すべてのチャネルのフロー制御をモニタできます。

フロー制御のモニタリング

このセクションでは、フロー制御の新しいコマンドについて説明します。

次のコマンドがデバイスフロー制御のモニタに使用できます。

表 *201 :* フロー制御のモニタリング

コマンド	目的
show wireless flow-control *channel -id*	特定のチャネルのフロー制御に関する情報を表示します。
show wireless flow-control *channel-id* **statistics**	特定のチャネルのフロー制御に関する統計情報を表示します。

例：フロー制御のモニタリング

次に、チャネルに関する情報を表示する例を示します。

```
Device# show wireless flow-control 3
Device#

Channel Name        : CAPWAP
FC State            : Disabled
Remote Server State : Enabled
Pass-thru Mode      : Disabled
EnQ Disabled        : Disabled
Queue Depth         : 2048
Max Retries         : 5
Min Retry Gap (mSec): 3
```

次に、特定チャネルのフロー制御を表示する例を示します。

```
Device# show wireless flow-control 3
Device#

Channel Name                                : CAPWAP
# of times channel went into FC             : 0
# of times channel came out of FC           : 0
Total msg count received by the FC Infra    : 1
Pass-thru msgs send count                   : 0
Pass-thru msgs fail count                   : 0
# of msgs successfully queued               : 0
# of msgs for which queuing failed          : 0
# of msgs sent thru after queuing           : 0
# of msgs sent w/o queuing                  : 1
# of msgs for which send failed             : 0
# of invalid EAGAINS received               : 0
Highest watermark reached                   : 0
# of times Q hit max capacity               : 0
Avg time channel stays in FC (mSec)         : 0
```

フロー制御のモニタリングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

フロー制御のモニタリングに関する機能履歴および情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 141 章

SDM テンプレートの設定

- 機能情報の確認 （3015 ページ）
- SDM テンプレートの設定に関する情報 （3015 ページ）
- SDM テンプレートの設定方法 （3017 ページ）
- SDM テンプレートのモニタリングおよびメンテナンス （3019 ページ）
- SDM テンプレートの設定例 （3019 ページ）
- SDM テンプレートに関する追加情報 （3020 ページ）
- SDM テンプレートの設定の機能履歴と情報 （3021 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

SDM テンプレートの設定に関する情報

SDM テンプレート

SDM テンプレートを使用してシステム リソースを設定すると、特定の機能に対するサポートをネットワーク内でのデバイスの使用方法に応じて最適化することができます。一部の機能に最大システム使用率を提供するようにテンプレートを選択できます。

デバイスでサポートされているテンプレートは次のとおりです。

- Advanced：Advanced テンプレートはこのリリースでサポートされているすべてのイメージで利用できます。これは、NetFlow、マルチキャスト グループ、セキュリティ ACE、QoS ACE などの機能のシステム リソースを最大化します。
- VLAN：VLAN テンプレートは LAN Base ライセンスでのみ使用できます。VLAN テンプレートは、ルーティングを無効にし、最大数のユニキャスト MAC アドレスをサポートします。通常は、レイヤ 2 デバイス用に選択されます。

テンプレートを変更し、システムを再起動したら、**show sdm prefer** 特権 EXEC コマンドを使用して、新しいテンプレート設定を確認できます。**reload** 特権 EXEC コマンドを入力する前に、**show sdm prefer** コマンドを入力すると、**show sdm prefer** コマンドにより、現在使用しているテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。

デフォルトは Advanced テンプレートです。

表 *202*：テンプレートで許容される機能リソースの概算

Resource	Advanced	VLAN
Number of VLANs	4094	4094
ユニキャスト MAC アドレス	32 K	32 K
オーバーフロー ユニキャスト MAC アドレス	512	512
IGMP グループとマルチキャスト ルート	4 K	4 K
オーバーフロー IGMP グループおよびマルチキャスト ルート	512	512
• 直接接続ルート	16 K	16 K
• 間接接続 IP ホスト	7 K	7 K
ポリシーベース ルーティング ACE	1024	0
QoS 分類 ACE	3 K	3 K
セキュリティの ACE	3 K	3 K
NetFlow ACE	1024	1024
入力マイクロフロー ポリサーの ACE:	256 K	0
出力マイクロフロー ポリサーの ACE：	256 K	0
FSPAN ACE	256	256
コントロール プレーン エントリ：	512	512

Resource	Advanced	VLAN
入力 NetFlow フロー：	8 K	8 K
出力 NetFlow フロー：	16 K	16 K

（注） スイッチがワイヤレスモビリティエージェントとして使用される場合、許可されるテンプレートは Advanced テンプレートのみです。

（注） SDM テンプレートは VLAN を作成しません。SDM テンプレートにコマンドを追加する前に、VLAN を作成する必要があります。

表には、テンプレートが選択されたときに設定される、おおよそのハードウェア上限が示されています。ハードウェア リソースのある部分がいっぱいの場合は、処理のオーバーフローはすべて CPU に送られ、スイッチのパフォーマンスに重大な影響が出ます。

SDM テンプレートとスイッチ スタック

1 つのスイッチ スタックで、すべてのスタック メンバにより、アクティブなスイッチに保存された同一の SDM テンプレートを使用する必要があります。新規スイッチがスタックに追加されると、アクティブ スイッチに保存された SDM コンフィギュレーションは、個々のスイッチに設定されているテンプレートを上書きします。

show switch 特権 EXEC コマンドを使用すると、スタック メンバが SDM 不一致モードになっているかどうかを確認できます。

SDM テンプレートの設定方法

SDM テンプレートの設定

スイッチ SDM テンプレートの設定

SDM テンプレートの設定

SDM テンプレートを使用して機能動作を最適にサポートするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**sdm prefer advanced** | **vlan** 例： `Device(config)# sdm prefer advanced`	スイッチで使用する SDM テンプレートを指定します。キーワードの意味は次のとおりです。 • **advanced**：NetFlow などの高度な機能をサポートします。 • **vlan**：ハードウェアでのルーティングをサポートしないスイッチでの VLAN 設定を最適化します。 （注） **no sdm prefer** コマンドとデフォルト テンプレートはサポートされません。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**reload** 例： `Device# reload`	オペレーティング システムをリロードします。

SDM テンプレートのモニタリングおよびメンテナンス

コマンド	目的
show sdm prefer	使用中の SDM テンプレートを表示します。
reload	スイッチをリロードして、新しく設定した SDM テンプレートをアクティブにします。
no sdm prefer	デフォルトの SDM テンプレートを設定します。

SDM テンプレートの設定例

例：SDM テンプレートの設定

次に、VLAN テンプレートの設定方法の例を示します。

```
Device(config)# sdm prefer vlan
Device(config)# exit
Device# reload
  Proceed with reload? [confirm]
```

例：SDM テンプレートの表示

次に、詳細なテンプレート情報を表示した出力例を示します。

```
Device# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
  Number of VLANs:                                4094
  Unicast MAC addresses:                          32768
  Overflow Unicast MAC addresses:                 512
  IGMP and Multicast groups:                      8192
  Overflow IGMP and Multicast groups:             512
  Directly connected routes:                      32768
  Indirect routes:                                8192
  Security Access Control Entries:                3072
  QoS Access Control Entries:                     2816
  Policy Based Routing ACEs:                      1024
  Netflow ACEs:                                   1024
```

```
  Input Microflow policer ACEs:                    256
  Output Microflow policer ACEs:                   256
  Flow SPAN ACEs:                                  256
  Tunnels:                                         256
  Control Plane Entries:                           512
  Input Netflow flows:                             8192
  Output Netflow flows:                            16384
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.


Device#
```

次に、VLAN テンプレート情報を表示した出力例を示します。

```
Device# show sdm prefer vlan

Showing SDM Template Info

This is the VLAN template for a typical Layer 2 network.
  Number of VLANs:                                 4094
  Unicast MAC addresses:                           32768
  Overflow Unicast MAC addresses:                  512
  IGMP and Multicast groups:                       8192
  Overflow IGMP and Multicast groups:              512
  Directly connected routes:                       32768
  Indirect routes:                                 8192
  Security Access Control Entries:                 3072
  QoS Access Control Entries:                      3072
  Policy Based Routing ACEs:                       0
  Netflow ACEs:                                    1024
  Input Microflow policer ACEs:                    0
  Output Microflow policer ACEs:                   0
  Flow SPAN ACEs:                                  256
  Tunnels:                                         0
  Control Plane Entries:                           512
  Input Netflow flows:                             16384
  Output Netflow flows:                            8192
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

Device#
```

SDM テンプレートに関する追加情報

関連資料

関連項目	マニュアル タイトル
SDM コマンド リファレンス	*System Management Command Reference*（*Catalyst 3850 Switches*）
VLAN 構成ガイド	*VLAN Configuration Guide (Catalyst 3850 Switches)*

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

SDM テンプレートの設定の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 142 章

システム メッセージ ログの設定

- 機能情報の確認 （3023 ページ）
- システム メッセージ ログの設定に関する情報 （3023 ページ）
- システム メッセージ ログの設定方法 （3026 ページ）
- システム メッセージ ログのモニタリングおよびメンテナンス （3036 ページ）
- システム メッセージ ログの設定例 （3036 ページ）
- システム メッセージ ログに関する追加情報 （3037 ページ）
- システム メッセージ ログの機能履歴と情報 （3038 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

システム メッセージ ログの設定に関する情報

システム メッセージ ロギング

スイッチはデフォルトで、システム メッセージおよび **debug** 特権 EXEC コマンドの出力をロギング プロセスに送信します。スタック メンバーはシステム メッセージをトリガーできます。システム メッセージを生成するスタック メンバは、ホスト名を hostname-n の形式で付加し（n はスイッチ1～4 の範囲）、出力をアクティブ スイッチのロギング プロセスにリダイレクトします。アクティブ スイッチはスタック メンバですが、そのホスト名はシステム メッセージの末尾に追加されません。ロギング プロセスはログ メッセージを各宛先（設定に応じて、ログ

バッファ、端末回線、UNIX Syslog サーバなど）に配信する処理を制御します。ロギング プロセスは、コンソールにもメッセージを送信します。

ロギング プロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。メッセージがアクティブなコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。ログ メッセージにタイム スタンプを設定したり、Syslog 送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。表示されるメッセージについては、このリリースに対応するシステム メッセージ ガイドを参照してください。

ロギングされたシステム メッセージにアクセスするには、スイッチのコマンドラインインターフェイス（CLI）を使用するか、または適切に設定された Syslog サーバにこれらのシステム メッセージを保存します。スイッチ ソフトウェアは、Syslog メッセージをスタンドアロン スイッチ上の内部バッファに保存します。スイッチ スタックの場合は、アクティブ スイッチ上に保存します。スタンドアロン スイッチまたはスタック マスターに障害が発生すると、ログをフラッシュ メモリに保存していなかった場合、ログは失われます。

システム メッセージをリモートで監視するには、Syslog サーバ上でログを表示するか、あるいは Telnet、コンソール ポート、またはイーサネット管理ポート経由でスイッチにアクセスします。スイッチ スタックでは、すべてのスタック メンバ コンソールにより、同じコンソール出力が用意されます。

（注） Syslog フォーマットは 4.3 Berkeley Standard Distribution（BSD）UNIX と互換性があります。

システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字とパーセント記号（%）、およびその前に配置されるオプションのシーケンス番号やタイム スタンプ情報（設定されている場合）で構成されています。スイッチに応じて、メッセージは次のいずれかの形式で表示されます。

- *seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)*
- *seq no:timestamp: %facility-severity-MNEMONIC:description*

パーセント記号の前にあるメッセージの部分は、次のグローバル コンフィギュレーション コマンドの設定によって異なります。

- **service sequence-numbers**
- **service timestamps log datetime**
- **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]
- **service timestamps log uptime**

表 *203* : システム ログ メッセージの要素

要素	説明
seq no:	**service sequence-numbers** グローバル コンフィギュレーション コマンドが設定されている場合だけ、ログ メッセージにシーケンス番号をスタンプします。
timestamp のフォーマット： *mm/dd hh:mm:ss* または *hh:mm:ss*（短時間） または *d h*（長時間）	メッセージまたはイベントの日時です。**service timestamps log** [**datetime** | **log**] グローバル コンフィギュレーション コマンドが設定されている場合だけ、この情報が表示されます。
facility	メッセージが参照する機能（SNMP、SYS など）です。
severity	メッセージの重大度を示す 0 ～ 7 の 1 桁のコードです。
MNEMONIC	メッセージを一意に示すテキスト ストリングです。
説明	レポートされているイベントの詳細を示すテキスト ストリングです。
hostname-n（ホスト名 *-n*）	スタック メンバーのホスト名およびスタック内のスイッチ番号。アクティブ スイッチはスタック メンバですが、そのホスト名はシステム メッセージの末尾に追加されません。

デフォルトのシステム メッセージ ロギングの設定

表 *204* : デフォルトのシステム メッセージ ロギングの設定

機能	デフォルト設定
コンソールへのシステム メッセージ ロギング	イネーブル
コンソールの重大度	デバッグ
ログ ファイル設定	ファイル名の指定なし
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1 メッセージ

機能	デフォルト設定
タイム スタンプ	ディセーブル
同期ロギング	ディセーブル
ロギング サーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
サーバ機能	local7
サーバの重大度	Informational

syslog メッセージの制限

snmp-server enable trap グローバル コンフィギュレーション コマンドを使用して、SNMP ネットワーク管理ステーション（NMS）に送信されるように Syslog メッセージ トラップがイネーブルに設定されている場合は、スイッチの履歴テーブルに送信および格納されるメッセージの重大度を変更できます。また、履歴テーブルに格納されるメッセージの数を変更することもできます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。デフォルトでは、Syslog トラップが有効でない場合も、レベルが **warning** であるメッセージや数値的に下位レベルのメッセージの 1 つが履歴テーブルに格納されます。

履歴テーブルがいっぱいの場合（**logging history size** グローバル コンフィギュレーション コマンドで指定した最大メッセージ エントリ数が格納されている場合）は、新しいメッセージ エントリを格納できるように、最も古いエントリがテーブルから削除されます。

履歴テーブルは、level キーワードおよび重大度を示します。SNMP を使用している場合は、重大度の値が 1 だけ増えます。たとえば、*emergencies* は 0 ではなく 1 に、*critical* は 2 ではなく 3 になります。

システム メッセージ ログの設定方法

メッセージ表示宛先デバイスの設定

メッセージロギングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging buffered** [*size*] 例： `Device(config)# logging buffered 8192`	スタンドアロン スイッチ上か、または、スイッチ スタックの場合はアクティブ スイッチ上で、ログ メッセージを内部バッファに保存します。指定できる範囲は 4096 ～ 2147483647 バイトです。デフォルトのバッファ サイズは 4096 バイトです。 スタンドアロン スイッチまたはアクティブ スイッチに障害が発生すると、ログ ファイルをフラッシュ メモリに保存していなかった場合、ログ ファイルは失われます。ステップ 4 を参照してください。 （注） バッファ サイズを大きすぎる値に設定しないでください。他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサ メモリを表示するには、**show memory** 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値であるため、バッファ サイズをこの値に設定しないでください。
ステップ 3	**logging** ホスト 例： `Device(config)# logging 125.1.1.100`	UNIX Syslog サーバ ホストにメッセージを保存します。 *host* には、syslog サーバとして使用するホストの名前または IP アドレスを指定します。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。

	コマンドまたはアクション	目的
ステップ 4	**logging file flash:** *filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*] 例： `Device(config)# logging file flash:log_msg.txt 40960 4096 3`	スタンドアロンスイッチ上か、または、スイッチ スタックの場合はアクティブスイッチ上で、フラッシュ メモリにあるファイルにログ メッセージを保存します。 • *filename*：ログ メッセージのファイル名を入力します。 • （任意）**max-file-size**：ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ～ 2147483647 です。デフォルトは 4096 バイトです。 • （任意）*min-file-size*：ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ～ 2147483647 です。デフォルトは 2048 バイトです。 • （任意）*severity-level-number* | *type*：ロギングの重大度またはロギングタイプを指定します。重大度に指定できる範囲は 0 ～ 7 です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**terminalmonitor** 例： `Device# terminal monitor`	現在のセッション間、非コンソール端末にメッセージを保存します。 端末パラメータ コンフィギュレーション コマンドはローカルに設定され、セッションの終了後は無効になります。デバッグ メッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。

ログ メッセージの同期化

特定のコンソール ポート回線または仮想端末回線に対して、非送信請求メッセージおよび **debug** 特権 EXEC コマンドの出力を送信請求デバイスの出力およびプロンプトと同期させることができます。重大度に応じて非同期に出力されるメッセージのタイプを特定できます。また、端末の非同期メッセージが削除されるまで保存しておくバッファの最大数を設定することもできます。

非送信請求メッセージおよび **debug** コマンド出力の同期ロギングがイネーブルの場合、送信請求デバイス出力がコンソールに表示または印刷された後に、非送信請求デバイスからの出力が表示または印刷されます。非送信請求メッセージおよび **debug** コマンドの出力は、ユーザ入力用プロンプトが返された後に、コンソールに表示されます。したがって、非送信請求メッセージおよび **debug** コマンドの出力は、送信請求デバイス出力およびプロンプトに割り込まれることはありません。非送信請求メッセージが表示された後に、コンソールはユーザ プロンプトを再表示します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console** | **vty**] *line-number* [*ending-line-number*] 例： `Device(config)# line console`	メッセージの同期ロギングに設定する回線を指定します。 • **console** ：スイッチ コンソール ポートまたはイーサネット管理ポートでの設定を指定します。 • **line vty** *line-number*：どの vty 回線の同期ロギングをイネーブルにするかを指定します。Telnet セッションを介して行われる設定には、vty 接続を使用します。回線番号に指定できる範囲は 0 ～ 15 です。 16 個の vty 回線の設定をすべて一度に変更するには、次のように入力します。 line vty 0 15 また、現在の接続に使用されている 1 つの vty 回線の設定を変更することもでき

	コマンドまたはアクション	目的
		ます。たとえば、vty 回線 2 の設定を変更するには、次のように入力します。 line vty 2 このコマンドを入力すると、ライン コンフィギュレーション モードになります。
ステップ 3	**logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*] 例： `Device(config)# logging synchronous level 3 limit 1000`	メッセージの同期ロギングをイネーブルにします。 • （任意）**level** *severity-level*：メッセージの重大度レベルを指定します。重大度がこの値以上であるメッセージは、非同期に出力されます。値が小さいほど重大度は大きく、値が大きいほど重大度は小さくなります。デフォルトは 2 です。 • （任意）**level all**：重大度に関係なく、すべてのメッセージが非同期に出力されます。 • （任意）**limit** *number-of-buffers*：キューイングされる端末のバッファ数を指定します。これを超える新しいメッセージは廃棄されます。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

メッセージ ロギングのディセーブル化

メッセージロギングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージロギングをイネーブルにする必要があります。メッセージ ロギングがイネーブルの場合、ログ メッセージはロギング プロセスに送信されます。ロギング プロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

ロギング プロセスをディセーブルにすると、メッセージがコンソールに書き込まれるまでプロセスは処理続行を待機する必要があるため、スイッチの処理速度が低下することがあります。ロギング プロセスがディセーブルの場合、メッセージは生成後すぐに（通常はコマンド出力に割り込む形で）コンソールに表示されます。

logging synchronous グローバル コンフィギュレーション コマンドも、コンソールへのメッセージ表示に影響します。このコマンドをイネーブルにすると、Return を押さなければメッセージが表示されません。

メッセージ ロギングをディセーブルにした後に再びイネーブルにするには、**logging on** グローバル コンフィギュレーション コマンドを使用します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no logging console** 例： `Device(config)# no logging console`	メッセージ ロギングをディセーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化

デフォルトでは、ログ メッセージにはタイム スタンプが適用されません。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを使用します。
	• **servicetimestampsloguptime**
	• **service timestamps log datetime**[**msec** | **localtime** | **show-timezone**]
	例：
	`Device(config)# service timestamps log uptime`
	または
	`Device(config)# service timestamps log datetime`
		ログのタイムスタンプをイネーブルにします。
		• **log uptime**：ログ メッセージのタイムスタンプをイネーブルにして、システムの再起動以降の経過時間を表示します。
		• **log datetime**：ログ メッセージのタイムスタンプをイネーブルにします。選択したオプションに応じて、ローカル タイム ゾーンを基準とした日付、時間（ミリ秒）、タイム ゾーン名をタイム スタンプとして表示できます。

ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ログメッセージのシーケンス番号のイネーブル化およびディセーブル化

タイムスタンプが同じログ メッセージが複数ある場合、これらのメッセージを表示するには、シーケンス番号を使用してメッセージを表示できます。デフォルトでは、ログ メッセージにシーケンス番号は表示されません。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**service sequence-numbers** 例： `Device(config)# service sequence-numbers`	シーケンス番号をイネーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

メッセージ重大度の定義

メッセージの重大度を指定して、選択したデバイスに表示されるメッセージを制限します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging console** *level* 例： `Device(config)# logging console 3`	コンソールに保存するメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 3	**logging monitor** *level* 例： `Device(config)# logging monitor 3`	端末回線に出力するメッセージを制限します。 デフォルトで、端末はデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します。

	コマンドまたはアクション	目的
ステップ 4	**logging trap** *level* 例： `Device(config)# logging trap 3`	Syslog サーバに保存するメッセージを制限します。 デフォルトで、Syslog サーバは通知メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

履歴テーブルおよび SNMP に送信される syslog メッセージの制限

このタスクでは、履歴テーブルおよび SNMP に送信される syslog メッセージを制限する方法について説明します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging history** *level* 例： `Device(config)# logging history 3`	履歴ファイルに保存され、SNMP サーバに送信される syslog メッセージのデフォルト レベルを変更します。 デフォルトでは、**warnings**、**errors**、**critical**、**alerts**、および **emergencies** のメッセージが送信されます。
ステップ 3	**logging history size** *number* 例： `Device(config)# logging history size 200`	履歴テーブルに保存できる Syslog メッセージの数を指定します。 デフォルトでは 1 つのメッセージが格納されます。指定できる範囲は 0 ～ 500 です。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	

UNIX Syslog デーモンへのメッセージのロギング

このタスクはオプションです。

（注） 最新バージョンの UNIX Syslog デーモンの中には、デフォルトでネットワークからの Syslog パケットを受け入れないものがあります。このようなシステムの場合に、Syslog メッセージのリモート ロギングをイネーブルにするには、Syslog コマンド ラインに追加または削除する必要があるオプションを、UNIX の **man syslogd** コマンドを使用して判別します。

始める前に

- root としてログインします。
- システム ログ メッセージを UNIX Syslog サーバに送信する前に、UNIX サーバ上で Syslog デーモンを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	/etc/syslog.conf ファイルに次の行を追加します。 例： **local7.debug /usr/adm/logs/***cisco.log*	• **local7**：ロギング機能を指定します。 • **debug**：syslog レベルを指定します。このファイルは、syslog デーモンに書き込み権限がある既存ファイルである必要があります。
ステップ 2	UNIX シェル プロンプトに次のコマンドを入力します。 例： $ **touch /var/log/***cisco.log* $ **chmod 666 /var/log/***cisco.log*	ログ ファイルを作成します。syslog デーモンは、このレベルまたはこのファイルのより高い重大度レベルでメッセージを送信します。
ステップ 3	Syslog デーモンに新しい設定を認識させます。 例：	詳細については、ご使用の UNIX システムの **man syslog.conf** および **man syslogd** コマンドを参照してください。

	コマンドまたはアクション	目的
	`$ kill -HUP `cat /etc/syslog.pid`	

システムメッセージログのモニタリングおよびメンテナンス

コンフィギュレーション アーカイブ ログのモニタリング

コマンド	目的
show archive log config {**all** | **number** [*end-number*] | **user** *username* [**session** *number*] *number* [*end-number*] | **statistics**} [**provisioning**]	コンフィギュレーションログ全体、または指定されたパラメータのログを表示します。

システム メッセージ ログの設定例

例：システム メッセージのスタック構成

次の例に、アクティブ スイッチおよびスタック メンバの部分的なスイッチ システム メッセージを示します（ホスト名は *Switch-2*）。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed
 state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/2, changed state to up (Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
(Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/1, changed
 state to down 2 (Switch-2)
```

例：スイッチ システム メッセージ

次に、スイッチ上のスイッチ システム メッセージの一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

システム メッセージ ログに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference (Catalyst 3850 Switches)*』
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*）
プラットフォームに依存しない設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*） *IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*）

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

システム メッセージ ログの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 143 章

オンライン診断の設定

- 機能情報の確認 （3039 ページ）
- オンライン診断の設定に関する情報 （3039 ページ）
- オンライン診断の設定方法 （3040 ページ）
- オンライン診断のモニタリングおよびメンテナンス （3046 ページ）
- オンライン診断テストの設定例 （3046 ページ）
- オンライン診断に関する追加情報 （3049 ページ）
- オンライン診断設定の機能履歴と情報 （3050 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

オンライン診断の設定に関する情報

オンライン診断

オンライン診断では、デバイスが稼働中のネットワークに接続している間に、デバイスのハードウェア機能をテストし、確認できます。

オンライン診断には、異なるハードウェア コンポーネントをチェックするパケット交換テストが含まれ、データ パスおよび制御信号が確認されます。

オンライン診断では、次の領域の問題が検出されます。

- ハードウェア コンポーネント
- インターフェイス（イーサネット ポートなど）
- はんだ接合

オンライン診断は、オンデマンド診断、スケジュール診断、ヘルスモニタリング診断に分類できます。オンデマンド診断は、CLI から実行されます。スケジュールされた診断は、動作中のネットワークにデバイスが接続されているときに、ユーザが指定した間隔または指定した時刻に実行されます。ヘルスモニタリングは、バックグラウンドでユーザが指定した間隔で実行されます。デフォルトでは、30 秒ごとにヘルス モニタリング テストが実行されます。

オンライン診断を設定したあと、手動で診断テストを開始したり、テスト結果を表示したりできます。また、デバイスまたはスイッチ スタックに設定されているテストの種類、およびすでに実行された診断テスト名を確認できます。

オンライン診断の設定方法

オンライン診断テストの開始

スイッチで実行する診断テストを設定しデバイス、**diagnostic start** 特権 EXEC コマンドを使用して診断テストを開始します。

テストを開始したら、テスト プロセスの停止はできません。

手動でオンライン診断テストを開始するには、次の特権 EXEC コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**diagnostic start switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**} **例**： `Device# diagnostic start switch 2 test basic`	診断テストを開始します。 **switch** *number* キーワードは、スタック構成デバイスのみでサポートされます。指定できる範囲は 1 ～ 4 です。 次のいずれかのオプションを使用してテストを指定できます。 • *name*：テストの名前を入力します。 • *test-id*：テストの ID 番号を入力します。 • *test-id-range*：カンマとハイフンで区切ってテスト ID の範囲を整数で入力します。

	コマンドまたはアクション	目的
		• **all**：すべてのテストを開始します。 • **basic**：基本テスト スイートを開始します。 • **complete**：完全なテスト スイートを開始します。 • **minimal**：最小限のブートアップテスト スイートを開始します。 • **non-disruptive**：ノンディスラプティブ テスト スイートを開始します。 • **per-port**：ポート単位のテスト スイートを開始します。

オンライン診断の設定

診断モニタリングをイネーブルにする前に、障害しきい値およびテストの間隔を設定する必要があります。

オンライン診断のスケジューリング

特定のデバイスについて指定した時間、または日、週、月単位でオンライン診断をスケジューリングできます。スケジューリングを削除するには、コマンドの **no** 形式を入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**diagnostic schedule switch** *number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**} {**daily** | **on** *mm dd yyyy hh:mm* | **port** *inter-port-number port-number-list* | **weekly** *day-of-week hh:mm*} 例： `Device(config)# diagnostic schedule`	特定日時のオンデマンド診断テストをスケジュールします。 **switch** *number* キーワードは、スタック構成スイッチだけでサポートされます。指定できる範囲は 1 ～ 4 です。 スケジュールするテストを指定する場合は、次のオプションを使用します。

	コマンドまたはアクション	目的
	`switch 3 test 1-5 on July 3 2013 23:10`	• *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべてのテスト ID • **basic**：基本的なオンデマンドの診断テストを開始します。 • **complete**：完全なテスト スイートを開始します。 • **minimal**：最小限のブートアップ テスト スイートを開始します。 • **non-disruptive**：ノンディスラプティブ テスト スイートを開始します。 • **per-port**：ポート単位のテスト スイートを開始します。 テストは次のようにスケジュールできます。 • 毎日：**daily** *hh:mm* パラメータを使用します。 • 特定日時：**on** *mm dd yyyy hh:mm* パラメータを使用します。 • 毎週：**weekly** *day-of-week hh:mm* パラメータを使用します。

ヘルス モニタリング診断の設定

デバイスが稼働中のネットワークに接続されている間に、スイッチに対しヘルス モニタリング診断テストを設定できます。ヘルス モニタリング テストの実行間隔を設定したり、テスト失敗時のデバイスのsyslogメッセージ生成をイネーブルにしたり、特定のテストをイネーブルにできます。

テストをディセーブルにするには、コマンドの **no** 形式を入力します。

デフォルトでは、ヘルス モニタリングはディセーブルですが、デバイスはテストの失敗時に Syslog メッセージを生成します。

ヘルス モニタリング診断テストを設定し、イネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**diagnostic monitor interval switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day* 例： `Device(config)# diagnostic monitor interval switch 2 test 1 12:30:00 750 5`	指定のテストに対し、ヘルス モニタリングの実行間隔を設定します。 **switch** *number* キーワードは、スタック構成スイッチだけでサポートされます。範囲は 1 ～ 9 です。 テストを指定する場合は、次のいずれかのパラメータを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべての診断テスト。 間隔を指定する場合は、次のパラメータを設定します。 • *hh:mm:ss*：モニタリング間隔（時間、分、秒）。指定できる範囲は

	コマンドまたはアクション	目的
		hh が 0～24、*mm* および *ss* が 0～60 です。 • *milliseconds*：モニタリング間隔（ミリ秒（ms））。指定できる範囲は 0 ～ 999 です。 • *day*：モニタリング間隔（日数）。指定できる範囲は 0 ～ 20 です。
ステップ 4	**diagnostic monitor syslog** 例： `Device(config)# diagnostic monitor syslog`	（任意）ヘルス モニタリング テストの失敗時にスイッチが Syslog メッセージを生成するように設定します。
ステップ 5	**diagnostic monitor threshold switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count* 例： `Device(config)# diagnostic monitor threshold switch 2 test 1 failure count 20`	（任意）ヘルス モニタリング テストの失敗しきい値を設定します。 **switch** *number* キーワードは、スタック構成スイッチだけでサポートされます。指定できる範囲は 1 ～ 9 です。 テストを指定する場合は、次のいずれかのパラメータを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべての診断テスト。 失敗しきい値 *count* に指定できる範囲は 0 ～ 99 です。
ステップ 6	**diagnostic monitor switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} 例： `Device(config)# diagnostic monitor switch 2 test 1`	指定のヘルス モニタリング テストをイネーブルにします。 **switch** *number* キーワードは、スタック構成スイッチだけでサポートされます。指定できる範囲は 1 ～ 9 です。

	コマンドまたはアクション	目的
		テストを指定する場合は、次のいずれかのパラメータを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべての診断テスト。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

間隔をデフォルトの値またはゼロに変更するには、**no diagnostic monitor interval test***test-id* | *test-id-range* } グローバル コンフィギュレーション コマンドを使用します。ヘルスモニタリング テストに失敗した場合、**no diagnostic monitor syslog** コマンドを使用して、Syslog メッセージの生成をディセーブルに設定します。失敗しきい値を削除するには、**diagnostic monitor threshold test***test-id* | *test-id-range* }**failure count** コマンドを使用します。

オンライン診断のモニタリングおよびメンテナンス

オンライン診断テストとテスト結果の表示

デバイスまたはデバイススタックに設定されているオンライン診断テストを表示し、この表に示す **show** 特権 EXEC コマンドを使用してテスト結果を確認することができます。

表 *205 :* 診断テストの設定および結果用のコマンド

コマンド	目的
show diagnostic content switch [*number* | **all**]	スイッチに対して設定されたオンライン診断を表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic status	現在実行中の診断テストを表示します。
show diagnostic result switch [*number* | **all**] [**detail** | **test** {*name* | *test-id* | *test-id-range* | **all**} [**detail**]]	オンライン診断テストの結果を表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic switch [*number* | **all**] [**detail**]	オンライン診断テストの結果を表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic schedule switch [*number* | **all**]	オンライン診断テストのスケジュールを表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic post	POST 結果を表示します（この出力は、**show post** コマンドの出力と同じです）。

オンライン診断テストの設定例

例：診断テストの開始

次に、テスト名を指定して診断テストを開始する例を示します。

```
Device# diagnostic start switch 2 test TestInlinePwrCtlr
```

次に、すべての基本診断テストを開始する例を示します。

```
Device# diagnostic start switch 1 test all
```

例：ヘルス モニタリング テストの設定

次に、ヘルス モニタリング テストを設定する例を示します。

```
Device(config)# diagnostic monitor threshold switch 1 test 1 failure count 50
Device(config)# diagnostic monitor interval switch 1 test TestPortAsicStackPortLoopback
```

例：診断テストのスケジューリング

次に、特定のスイッチに対して、特定の日時に診断テストを実行するようにスケジューリングする例を示します。

```
Device(config)# diagnostic schedule test DiagThermalTest on June 3 2013  22:25
```

次の例では、指定されたスイッチで毎週特定の時間に診断テストを実行するようにスケジューリングする方法を示します。

```
Device(config)# diagnostic schedule switch 1 test 1,2,4-6 weekly saturday 10:30
```

例：オンライン診断の表示

次に、オンデマンド診断設定を表示する例を示します。

```
Device# show diagnostic ondemand settings

Test iterations = 1
Action on test failure = continue
```

次に、障害の診断イベントを表示する例を示します。

```
Device# show diagnostic events event-type error

Diagnostic events (storage for 500 events, 0 events recorded)
Number of events matching above criteria = 0

No diagnostic log entry exists.
```

次に、診断テストの説明を表示する例を示します。

```
Device# show diagnostic description switch 1 test all
```

```
DiagGoldPktTest :
        The GOLD packet Loopback test verifies the MAC level loopback
        functionality. In this test, a GOLD packet, for which doppler
        provides the support in hardware, is sent. The packet loops back
        at MAC level and is matched against the stored packet. It is a non
        -disruptive test.

DiagThermalTest :
        This test verifies the temperature reading from the sensor is below the yellow
        temperature threshold. It is a non-disruptive test and can be run as a health
monitoring test.

DiagFanTest :
        This test verifies all fan modules have been inserted and working properly on
the board
        It is a non-disruptive test and can be run as a health monitoring test.

DiagPhyLoopbackTest :
        The PHY Loopback test verifies the PHY level loopback
        functionality. In this test, a packet is sent which loops back
        at PHY level and is matched against the stored packet. It is a
        disruptive test and cannot be run as a health monitoring test.

DiagScratchRegisterTest :
        The Scratch Register test monitors the health of application-specific
        integrated circuits (ASICs) by writing values into registers and reading
        back the values from these registers. It is a non-disruptive test and can
        be run as a health monitoring test.

DiagPoETest :
        This test checks the PoE controller functionality. This is a disruptive test
        and should not be performed during normal switch operation.

DiagStackCableTest :
        This test verifies the stack ring loopback functionality
        in the stacking environment. It is a disruptive test and
        cannot be run as a health monitoring test.

DiagMemoryTest :
        This test runs the exhaustive ASIC memory test during normal switch operation
        NG3K utilizes mbist for this test. Memory test is very disruptive
        in nature and requires switch reboot after the test.

Device#
```

次に、ブートアップ レベルを表示する例を示します。

```
Device# show diagnostic bootup level

Current bootup diagnostic level: minimal

Device#
```

オンライン診断に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference (Catalyst 3850 Switches)*』
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*）
プラットフォームに依存しない設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*）

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

オンライン診断設定の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 144 章

コンフィギュレーション ファイルの管理

- コンフィギュレーション ファイルの管理の前提条件 （3051 ページ）
- コンフィギュレーション ファイルの管理の制約事項 （3051 ページ）
- コンフィギュレーション ファイルの管理について （3052 ページ）
- コンフィギュレーション ファイル情報の管理方法 （3060 ページ）
- その他の参考資料 （3091 ページ）

コンフィギュレーション ファイルの管理の前提条件

- ユーザには、少なくとも Cisco IOS 環境とコマンドライン インターフェイスに関する基本的な知識が必要です。
- システムでは、少なくとも最小限の設定が実行されていることが必要です。基本コンフィギュレーション ファイルは、**setup** コマンドを使用して作成できます。

コンフィギュレーション ファイルの管理の制約事項

- このドキュメントで説明されている Cisco IOS コマンドの多くが使用可能であり機能するのは、デバイスの特定のコンフィギュレーション モードでのみです。
- Cisco IOS コンフィギュレーション コマンドのいくつかは、特定のデバイス プラットフォームでのみ使用可能であり、コマンド構文はプラットフォームによって異なる可能性があります。

コンフィギュレーション ファイルの管理について

コンフィギュレーション ファイルのタイプ

コンフィギュレーションファイルには、Ciscoデバイスの機能をカスタマイズするためのCisco IOS ソフトウェア コマンドが含まれています。コマンドは、システムを起動したとき（startup-configファイルから）、またはコンフィギュレーションモードでCLIにコマンドを入力したときに、Cisco IOS ソフトウェアによって解析（変換および実行）されます。

スタートアップ コンフィギュレーションファイル（startup-config）は、ソフトウェアを設定するためにシステムの起動時に使用されます。実行コンフィギュレーション ファイル（running-config）には、ソフトウェアの現在の設定が含まれています。2つのコンフィギュレーションファイルは別々の設定にできます。たとえば、コンフィギュレーションを永続的ではなく短期間で変更する場合があります。このような場合、**configure terminal** EXEC コマンドを使用して実行コンフィギュレーションを変更しますが、**copy running-config startup-config** EXEC コマンドを使用して設定を保存することはありません。

実行コンフィギュレーションを変更するには、コンフィギュレーションファイルの変更（CLI）の説明に従って、**configure terminal** コマンドを使用します。Cisco IOS コンフィギュレーション モードの使用時には、通常コマンドはすぐに実行され、入力直後またはコンフィギュレーション モードを終了した時点で実行コンフィギュレーション ファイルに保存されます。

スタートアップ コンフィギュレーション ファイルを変更するには、**copy running-config startup-config** EXEC コマンドを使用してスタートアップ コンフィギュレーションに実行コンフィギュレーションファイルを保存するか、ファイルサーバからスタートアップコンフィギュレーションにコンフィギュレーション ファイルをコピーします（詳細については、TFTP サーバからデバイスへのコンフィギュレーションファイルのコピー（CLI）を参照してください）。

コンフィギュレーション モードおよびコンフィギュレーション ソースの選択

デバイス上でコンフィギュレーションモードを開始するには、特権EXECプロンプトで**configure** コマンドを入力します。Cisco IOS ソフトウェアは次のプロンプトで応答し、端末、メモリ、またはネットワーク サーバ（ネットワーク）上に格納されたファイルのいずれかを、コンフィギュレーション コマンドのソースとして指定するように要求されます。

```
Configuring from terminal, memory, or network [terminal]?
```

端末からの設定では、コマンドラインにコンフィギュレーションコマンドを入力できます（次の項を参照してください）。 詳細については、スタートアップ コンフィギュレーション ファイルでのコンフィギュレーション コマンドの再実行（CLI）の項を参照してください。

ネットワークからの設定では、ネットワーク経由でコンフィギュレーションコマンドをロードして実行できます。詳細については、TFTP サーバからデバイスへのコンフィギュレーション ファイルのコピー（CLI）の項を参照してください。

CLI を使用したコンフィギュレーション ファイルの変更

Cisco IOS ソフトウェアは、1 行につき 1 つのコンフィギュレーション コマンドを受け入れます。コンフィギュレーションコマンドは、必要なだけ入力できます。コンフィギュレーション ファイルには、入力したコマンドを説明するコメントを追加できます。コメントの先頭には、感嘆符（!）を付けます。コメントは NVRAM にもコンフィギュレーション ファイルのアクティブ コピーにも格納されないため、**show running-config** または **more system:running-config** EXEC コマンドでアクティブな設定のリストを表示しても、コメントは表示されません。**show startup-config** または **more nvram:startup-config** EXEC モード コマンドでスタートアップ コンフィギュレーションのリストを表示しても、コメントは表示されません。コメントは、コンフィギュレーション ファイルがデバイスにロードされたときにコンフィギュレーション ファイルから削除されます。ただし、ファイル転送プロトコル（FTP）、リモート コピープロトコル（RCP）、または Trivial File Transfer Protocol（TFTP）サーバ上に格納されているコンフィギュレーション ファイルのコメントのリストは表示できます。CLI を使用してソフトウェアは設定するときは、ユーザの入力に従ってソフトウェアによりコマンドが実行されます。

コンフィギュレーション ファイルの場所

コンフィギュレーション ファイルは、次の場所に格納されます。

- 実行コンフィギュレーションは RAM に格納されます。
- クラス A フラッシュ ファイル システム プラットフォーム以外のすべてのプラットフォーム上では、スタートアップ コンフィギュレーションは不揮発性 RAM（NVRAM）に格納されます。
- クラス A フラッシュ ファイル システム プラットフォーム上では、スタートアップ コンフィギュレーションは CONFIG_FILE 環境変数で指定された場所に格納されます（詳細については、セクションクラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定（CLI）を参照してください）。CONFIG_FILE 変数は、デフォルトでは NVRAM になりますが、次のファイル システムのファイルも指定できます。
  - **nvram:**（NVRAM）
  - **bootflash:**（内部フラッシュ メモリ）
  - **usbflash0:**（フラッシュ ファイル システム）

ネットワーク サーバからデバイスへのコンフィギュレーション ファイルのコピー

TFTP、rcp、または FTP サーバからデバイスの実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーできます。この機能は、次のいずれかの理由により実行する場合があります。

- バックアップ コンフィギュレーション ファイルを復元するため。
- 別のデバイスにコンフィギュレーションファイルを使用するため。たとえば、別のデバイスをネットワークに追加して、そのコンフィギュレーションを元のデバイスと同様にする場合です。新しいデバイスにファイルをコピーすることにより、ファイル全体を再作成するのではなく、該当部分を変更できます。
- 同一のコンフィギュレーション コマンドをネットワーク内のすべてのデバイスにロードして、すべてのデバイスのコンフィギュレーションを同様にするため。

コマンドラインにコマンドを入力した場合と同様に、**copy**{**ftp:**|**rcp:**|**tftp:system:running-config**} EXEC コマンドはデバイスにコンフィギュレーションファイルをロードします。コマンドを追加する前に、デバイスにより既存の実行コンフィギュレーションが消去されることはありません。コピーされたコンフィギュレーションファイル内のコマンドによって既存のコンフィギュレーションファイル内のコマンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定のコマンドの IP アドレスが、既存のコンフィギュレーションに格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内の一部のコマンドには、置き換えられたり無効になったりしないものもあります。このようなコマンドがある場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルが組み合わされた（コピーされたコンフィギュレーション ファイルが優先する）コンフィギュレーション ファイルが作成されます。

コンフィギュレーションファイルをサーバ上に格納されているファイルの正確なコピーとして復元するには、そのコンフィギュレーションファイルをスタートアップコンフィギュレーションに直接コピーし（**copy ftp:**| **rcp:**| **tftp:**} **nvram:startup-config** コマンドを使用）、デバイスをリロードする必要があります。

サーバからデバイスへコンフィギュレーションファイルをコピーするには、次の項で説明する作業を実行します。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および rcp のトランスポート メカニズムは、TFTP よりも高速でデータ配信の信頼性も優れています。これらの改善は、FTP および rcp のトランスポート メカニズムがコネクション型の TCP/IP スタック上に構築されており、これを使用しているために可能になりました。

Deviceから TFTP サーバへのコンフィギュレーション ファイルのコピー

一部の TFTP 実装では、TFTP サーバ上にダミー ファイルを作成し、読み取り、書き込み、および実行を許可してから、ダミーファイルを上書きする形でファイルをコピーする必要があります。詳細については、ご使用の TFTP のマニュアルを参照してください。

デバイスから RCP サーバへのコンフィギュレーション ファイルのコピー

デバイスから RCP サーバへコンフィギュレーション ファイルをコピーできます。

ネットワークを UNIX コミュニティでリソースとして使用する最初の試みの 1 つは、リモート シェル（RSH）およびリモート コピー（rcp）機能が含まれた、リモート シェル プロトコルの設計および実装につながりました。rsh および rcp により、ユーザはリモートでコマンドを実行し、ネットワーク上のリモート ホストまたはサーバにあるファイル システムからまたはファイル システムへファイルをコピーすることが可能になります。シスコの rsh および rcp 実装は、標準実装と相互運用できます。

rcp の **copy** コマンドは、リモート システム上の rsh サーバ（またはデーモン）に依存します。rcp を使用してファイルをコピーするために、TFTP のようにファイル配布用のサーバを作成する必要はありません。必要なのは、リモート シェル（rsh）をサポートするサーバへのアクセスだけです（ほとんどの UNIX システムは rsh をサポートしています）。ファイルをある場所から別の場所へコピーするため、コピー元ファイルに対する読み取り権限と、コピー先ファイルに対する書き込み権限が必要です。コピー先ファイルが存在しない場合は、rcp により作成されます。

シスコの rcp 実装は UNIX の rcp 実装（ネットワーク上のシステム間でファイルをコピー）の関数をエミュレートしたものですが、シスコのコマンド構文は UNIX の rcp コマンド構文とは異なります。シスコの rcp サポートは、rcp をトランスポート メカニズムとして使用する一連の **copy** コマンドを提供しています。これらの rcp **copy** コマンドは、シスコの TFTP **copy** コマンドに類似していますが、高速で信頼性の高いデータ配信を実現する代替方法を備えているという点が異なります。これらの改善は、rcp のトランスポート メカニズムがコネクション型の TCP/IP スタック上に構築されており、これを使用しているために可能になりました。rcp コマンドを使用して、デバイスからネットワークサーバ、またはその逆へシステムイメージおよびコンフィギュレーション ファイルをコピーできます。

また、rcp サポートをイネーブルにし、リモート システムのユーザがデバイスから、またはその逆へファイルをコピーできるようにすることも可能です。

リモート ユーザによるデバイスとのファイルのコピーができるように Cisco IOS ソフトウェアを設定するには、**ip rcmd rcp-enable** グローバル コンフィギュレーション コマンドを使用します。

[Restrictions（機能制限）]

RCP プロトコルでは、クライアントは RCP 要求ごとにリモート ユーザ名をサーバに送信する必要があります。RCP を使用してデバイスからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアによって、次の順番で最初に発見された有効なユーザ名が送信されます。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip rcmd remote-username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 現在の TTY（端末）プロセスに関連付けられているリモート ユーザ名。たとえば、ユーザが Telnet を介してデバイスに接続されており、**username** コマンドを介して認証された場

合は、Telnetユーザ名がリモートユーザ名としてデバイス ソフトウェアによって送信されます。

4. デバイスの管理ホスト名。

RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。このサーバがディレクトリ構造をとっている場合、コンフィギュレーション ファイルまたはイメージは、サーバ上のリモート ユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定できます。

ip rcmd remote-username コマンドを使用して、すべてのコピーに対してユーザ名を指定します。（rcmd は、スーパーユーザ レベルで使用される UNIX ルーチンで、予約されたポート番号に基づいた認証スキームを使用してリモート マシン上でコマンドを実行します。rcmd は「Remote Command（リモート コマンド）」の略です）。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

サーバに書き込む場合、デバイス上のユーザからの RCP 書き込み要求を受け入れるよう、RCP サーバを適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の .rhosts ファイルにエントリを追加する必要があります。たとえば、デバイスに次の設定行が含まれているとします。

```
hostname Device1
ip rcmd remote-username User0
```

デバイスの IP アドレスが デバイス1.example.com に変換される場合、RCP サーバ上の User0 の .rhosts ファイルには、次の行が含まれることになります。

```
Device1.example.com Device1
```

RCP ユーザ名に関する要件

RCP プロトコルでは、クライアントは RCP 要求ごとにリモート ユーザ名をサーバに送信する必要があります。RCP を使用してデバイスからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアによって、次の順番で最初に発見された有効なユーザ名が送信されます。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip rcmd remote-username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 現在の TTY（端末）プロセスに関連付けられているリモートユーザ名。たとえば、ユーザが Telnet を介してデバイスに接続されており、**username** コマンドを介して認証された場合は、Telnetユーザ名がリモートユーザ名としてデバイス ソフトウェアによって送信されます。
4. デバイスの管理ホスト名。

RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。このサーバがディレクトリ構造をとっている場合、コンフィギュレーション ファイルまたはイメージは、サーバ上のリモート ユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホームディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

詳細については、ご使用の RCP サーバのマニュアルを参照してください。

デバイスから FTP サーバへのコンフィギュレーション ファイルのコピー

デバイスから FTP サーバへコンフィギュレーション ファイルをコピーできます。

FTP ユーザ名およびパスワードの概要

FTPプロトコルでは、FTP要求ごとにリモートユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してデバイスからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは、次の順番で最初に発見した有効なユーザ名を送信します。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip ftp username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. Anonymous

デバイスは次の順番で最初に発見した有効なパスワードを送信します。

1. **copy** コマンドで指定されたパスワード（パスワードが指定されている場合）。
2. **ip ftp password** コマンドで設定されたパスワード（コマンドが設定されている場合）。
3. デバイスは、*username*@デバイス*name.domain* というパスワードを生成します。変数 *username* は現在のセッションと関連付けられたユーザ名、デバイス*name* は設定済みホスト名、*domain* はデバイスのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合、デバイス上のユーザからのFTP書き込み要求を受け入れるよう、FTP サーバを適切に設定する必要があります。

このサーバがディレクトリ構造をとっている場合、コンフィギュレーションファイルまたはイメージは、サーバ上のユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

詳細については、ご使用の FTP サーバのマニュアルを参照してください。

ip ftp username および **ip ftp password** グローバル コンフィギュレーション コマンドを使用して、すべてのコピーに対してユーザ名とパスワードを指定します。当該のコピー操作だけに対してユーザ名を指定する場合は、**copy** EXEC コマンドにユーザ名を含めます。

VRF によるファイルのコピー

copy コマンドで指定した VRF インターフェイス経由でファイルをコピーできます。設定の変更リクエストを使用せずに直接送信元インターフェイスを変更できるので、**copy** コマンドで VRF を指定するほうが簡単で効率的です。

例

次の例に、**copy** コマンドを使用して、VRF 経由でファイルをコピーする方法を示します。

```
Device# copy scp: flash-1: vrf test-vrf
Address or name of remote host [10.1.2.3]?
Source username [ScpUser]?
Source filename [/auto/tftp-server/ScpUser/vrf_test.txt]?
Destination filename [vrf_test.txt]?
Getting the vrf name as test-vrf
Password:
Sending file modes: C0644 10 vrf_test.txt
!
223 bytes copied in 22.740 secs (10 bytes/sec)
```

スイッチから別のスイッチへのコンフィギュレーションファイルのコピー

あるスイッチから別のスイッチに設定をコピーすることができます。これは2ステッププロセスです。スイッチから TFTP サーバに設定をコピーし、次に TFTP から別のスイッチに設定をコピーします。

スイッチから現在の設定をコピーするには、**copy startup-config tftp:** コマンドを実行し、続く指示に従います。設定が TFTP サーバにコピーされます。

次に、別のスイッチへログインし、**copy tftp: startup-config** コマンドを実行して、続く指示に従います。これで、設定は別のスイッチにコピーされます。

設定をコピーした後、その設定を保存するには、**write memory** コマンドを使用し、その後スイッチをリロードするか、または **copy startup-config running-config** コマンドを実行します。

詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 16.1 (Catalyst 3850 Switches)*』を参照してください。

NVRAM より大きいコンフィギュレーション ファイル

NVRAM より大きいコンフィギュレーションファイルを維持管理するには、以降の項の情報を知っておく必要があります。

コンフィギュレーション ファイルの圧縮

service compress-config グローバル コンフィギュレーション コマンドは、コンフィギュレーション ファイルを圧縮して NVRAM に格納することを指定します。コンフィギュレーション ファイルが圧縮されると、デバイスは正常に機能します。システムの起動時に、システムはコンフィギュレーション ファイルが圧縮されていることを認識し、圧縮されたコンフィギュレーション ファイルを展開して、正常に処理を進めます。**more nvram:startup-config** EXEC コマンドにより、コンフィギュレーションが展開されてから表示されます。

コンフィギュレーション ファイルを圧縮する前に、適切なハードウェアのインストレーションおよびメンテナンス マニュアルを参照してください。ご利用のシステムの ROM がファイル圧縮をサポートしていることを確認します。サポートしていない場合、ファイル圧縮をサポートしている新しい ROM をインストールできます。

コンフィギュレーションのサイズは、NVRAM のサイズの 3 倍を超えてはいけません。NVRAM のサイズが 128 KB の場合、展開できる最大のコンフィギュレーション ファイルのサイズは 384 KB です。

service compress-config グローバル コンフィギュレーション コマンドは、Cisco IOS ソフトウェア リリース 10.0 以降のブート ROM を使用している場合に限り実行できます。新しい ROM をインストールするのは 1 回限りの操作で、ROM に Cisco IOS Release 10.0 がない場合だけ必要です。ブート ROM が圧縮コンフィギュレーションを認識しない場合は、次のメッセージが表示されます。

```
Boot ROMs do not support NVRAM compression Config NOT written to NVRAM
```

コンフィギュレーションのクラス A フラッシュ ファイル システム上のフラッシュ メモリへの格納

クラス A フラッシュ ファイル システムのデバイス上では、内部フラッシュ メモリのファイルまたは PCMCIA スロットのフラッシュ メモリのファイルに **CONFIG_FILE** 環境変数を設定することにより、スタートアップ コンフィギュレーションをフラッシュ メモリに格納できます。

詳細については、クラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定（CLI）を参照してください。

大きいコンフィギュレーションを編集または変更する場合は、注意する必要があります。フラッシュ メモリ領域は **copy system:running-config nvram:startup-config** EXEC コマンドが発行されるたびに使用されます。フラッシュ メモリのファイル管理（空き領域の最適化などの）は自動的には行われないため、利用可能なフラッシュ メモリに十分注意を払う必要があります。**squeeze** コマンドを使用して、使用済み領域を再要求します。20 MB 以上の大容量フラッシュ カードを使用することを推奨します。

ネットワークからのコンフィギュレーション コマンドのロード

コンフィギュレーションが大きい場合は、FTP、RCP、TFTP のいずれかのサーバに格納しておき、システムの起動時にダウンロードすることもできます。ネットワーク サーバを大きいコンフィギュレーションの保存に使用するためのコマンドの詳細については、セクションDeviceか

らTFTPサーバへのコンフィギュレーション ファイルのコピー（CLI）およびコンフィギュレーション ファイルをダウンロードするデバイスの設定を参照してください。

コンフィギュレーションファイルをダウンロードするデバイスの設定

システムの起動時に1つまたは2つのコンフィギュレーション ファイルをロードするようにデバイスを設定できます。コンフィギュレーション ファイルは、コマンドラインにコマンドを入力した場合と同様に、メモリにロードされ読み込まれます。そのため、デバイスのコンフィギュレーションは、元のスタートアップ コンフィギュレーションと 1 つまたは 2 つのダウンロードされたコンフィギュレーション ファイルが混在したものになります。

ネットワークとホストのコンフィギュレーション ファイル

歴史的な理由から、デバイスが最初にダウンロードするファイルは、ネットワーク コンフィギュレーション ファイルと呼ばれます。デバイスが2番目にダウンロードするファイルは、ホスト コンフィギュレーション ファイルと呼ばれます。2 つのコンフィギュレーション ファイルは、ネットワーク上のすべてのデバイスが同一コマンドの多くを使用する場合に使用できます。ネットワーク コンフィギュレーション ファイルには、すべてのデバイスを設定するために使用される標準コマンドが含まれます。ホスト コンフィギュレーション ファイルには、特定の 1 つのホストに固有のコマンドが含まれます。2 つのコンフィギュレーション ファイルをロードする場合、ホスト コンフィギュレーション ファイルを、もう 1 つのファイルより優先させる必要があります。ネットワーク コンフィギュレーション ファイルとホスト コンフィギュレーション ファイルの両方とも、TFTP、RCP、FTP のいずれかを介して到達可能なネットワーク サーバ上にあり、読み取り可能である必要があります。

コンフィギュレーション ファイル情報の管理方法

コンフィギュレーション ファイル情報の表示（CLI）

コンフィギュレーション ファイルに関する情報を表示するには、このセクションの手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showboot** 例：	BOOT 環境変数の内容（設定されている場合）、CONFIG_FILE 環境変数によっ

	コマンドまたはアクション	目的
	`Device# show boot`	て指定されているコンフィギュレーション ファイルの名前、および BOOTLDR 環境変数の内容を示します。
ステップ 3	**more** *file-url* 例： `Device# more 10.1.1.1`	指定されたファイルの内容を表示します。
ステップ 4	**showrunning-config** 例： `Device# show running-config`	実行コンフィギュレーション ファイルの内容を表示します（**more system:running-config** コマンドのコマンド エイリアス）。
ステップ 5	**showstartup-config** 例： `Device# show startup-config`	スタートアップ コンフィギュレーション ファイルの内容を表示します。（**more nvram:startup-config** コマンドのコマンド エイリアス）。 クラス A フラッシュ ファイル システム プラットフォーム以外のすべてのプラットフォーム上では、通常、デフォルトの startup-config ファイルは NVRAM に格納されます。 クラス A フラッシュ ファイル システム プラットフォーム上では、CONFIG_FILE 環境変数はデフォルトの startup-config ファイルを指定します。 CONFIG_FILE 変数のデフォルトは NVRAM になります。

コンフィギュレーション ファイルの変更（CLI）

Cisco IOS ソフトウェアは、1 行につき 1 つのコンフィギュレーション コマンドを受け入れます。コンフィギュレーションコマンドは、必要なだけ入力できます。コンフィギュレーション ファイルには、入力したコマンドを説明するコメントを追加できます。コメントの先頭には、感嘆符（!）を付けます。コメントは NVRAM にもコンフィギュレーション ファイルのアクティブ コピーにも格納されないため、**show running-config** または **moresystem:running-config** EXEC コマンドでアクティブな設定のリストを表示しても、コメントは表示されません。また、**show startup-config** または **more nvram:startup-config** EXEC モード コマンドでスタートアップ コンフィギュレーションのリストを表示しても、コメントは表示されません。コメントは、コンフィギュレーションファイルがデバイスにロードされたときにコンフィギュレーション ファイルから削除されます。ただし、ファイル転送プロトコル（FTP）、リモート コピー

プロトコル（RCP）、または Trivial File Transfer Protocol（TFTP）サーバ上に格納されているコンフィギュレーション ファイルのコメントのリストは表示できます。CLI を使用してソフトウェアは設定するときは、ユーザの入力に従ってソフトウェアによりコマンドが実行されます。CLI を使用してソフトウェアを設定するには、特権 EXEC モードを開始して次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**configurationcommand** 例： `Device(config)# configuration command`	必要なコンフィギュレーション コマンドを入力します。Cisco IOS マニュアル セットに、テクノロジー別に編成されたコンフィギュレーション コマンドが説明されています。
ステップ 4	次のいずれかを実行します。 • **end** • **^Z** 例： `Device(config)# end`	コンフィギュレーション セッションを終了し、EXEC モードに戻ります。 （注） Ctrl キーと Z キーを同時に押すと、画面に ^Z と表示されます。
ステップ 5	**copysystem:running-confignvram:startup-config** 例： `Device# copy system:running-config nvram:startup-config`	実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルとして保存します。 **copy running-config startup-config** コマンド エイリアスも使用できますが、このコマンドは精度が高くないため、注意する必要があります。ほとんどのプラットフォーム上では、このコマンドによりコンフィギュレーションは NVRAM に保存されます。クラス A フラッシュ ファイル システムのプラットフォーム上では、この手順によりコンフィギュ

	コマンドまたはアクション	目的
		レーションはCONFIG_FILE 環境変数によって指定された場所に保存されます（デフォルトの CONFIG_FILE 変数では、ファイルの保存先は NVRAM に指定されています）。

例

次の例では、デバイスのデバイスプロンプト名が設定されています。感嘆符（!）で示されたコメント行では、いずれのコマンドも実行されません。**hostname** コマンドは、デバイスから new_name へデバイス名を変更するために使用されます。Ctrl-Z（^Z）キーを押すか、**end** コマンドを入力すると、コンフィギュレーション モードが終了します。**copy system:running-config nvram:startup-config** コマンドにより、現在のコンフィギュレーションがスタートアップ コンフィギュレーションに保存されます。

```
Device# configure terminal
Device(config)# !The following command provides the switch host name.
Device(config)# hostname new_name
new_name(config)# end
new_name# copy system:running-config nvram:startup-config
```

スタートアップ コンフィギュレーションが NVRAM にある場合は、現在の設定情報がコンフィギュレーション コマンドとしてテキスト形式で格納され、デフォルト以外の設定だけが記録されます。破損データから保護するために、メモリはチェックサム算出されます。

（注） 一部の特定のコマンドは、NVRAM に保存されない場合があります。これらのコマンドは、マシンをリブートしたときに再入力する必要があります。これらのコマンドは、マニュアルに記載されています。リブート後にすばやくデバイスを再設定できるように、これらの設定のリストを保管しておくことを推奨します。

DeviceからTFTPサーバへのコンフィギュレーションファイルのコピー（CLI）

TFTP ネットワーク サーバ上の設定をコピーするには、以下の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copysystem:running-configtftp:**[[[*//location*]/*directory*]/*filename*] 例： `Device# copy system:running-config tftp: //server1/topdir/file10`	TFTP サーバへ実行コンフィギュレーション ファイルをコピーします。
ステップ 3	**copynvram:startup-configtftp:**[[[*//location*]/*directory*]/*filename*] 例： `Device# copy nvram:startup-config tftp: //server1/1stdir/file10`	TFTP サーバへスタートアップ コンフィギュレーション ファイルをコピーします。

例

次に、デバイスから TFTP サーバへコンフィギュレーション ファイルをコピーする例を示します。

```
Device# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] Y
Writing tokyo-confg!!! [OK]
```

次の作業

copy コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

Deviceから RCP サーバへのコンフィギュレーション ファイルのコピー（CLI）

デバイスから RCP サーバへスタートアップ コンフィギュレーション ファイルまたは実行コンフィギュレーション ファイルをコピーするには、特権 EXEC モードを開始して次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip rcmd remote-username** *username* 例： `Device(config)# ip rcmd remote-username NetAdmin1`	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 4	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。

ステップ 5	次のいずれかを実行します。
	• **copy system:running-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]
	• **copy nvram:startup-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]
	例：
	`Device# copy system:running-config rcp:`
	`//NetAdmin1@example.com/dir-files/file1`
		• デバイスの実行コンフィギュレーション ファイルが RCP サーバ上に格納されるように指定します。
		または
		• デバイスのスタートアップ コンフィギュレーション ファイルが RCP サーバ上に格納されるように指定します。

例

RCP サーバへの実行コンフィギュレーション ファイルの格納

次に、rtr2-confg という名前の実行コンフィギュレーション ファイルを IP アドレス 172.16.101.101 のリモート ホスト上の netadmin1 ディレクトリにコピーする例を示します。

```
Device# copy system:running-config rcp://netadmin1@172.16.101.101/runfile2-confg
Write file runfile2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
```

```
Connected to 172.16.101.101
Device#
```

RCP サーバへのスタートアップ コンフィギュレーション ファイルの格納

次に、RCP を使用してファイルをコピーすることによって、サーバ上にスタートアップ コンフィギュレーション ファイルを格納する例を示します。

```
Device# configure terminal

Device(config)# ip rcmd remote-username netadmin2

Device(config)# end

Device# copy nvram:startup-config rcp:

Remote host[]? 172.16.101.101

Name of configuration file to write [start-confg]?
Write file start-confg on host 172.16.101.101?[confirm]
![OK]
```

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

デバイスから FTP サーバへのコンフィギュレーション ファイルのコピー(CLI)

デバイスから FTP サーバへスタートアップ コンフィギュレーション ファイルまたは実行コンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	デバイス上で、グローバルコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipftpusername** *username* 例： `Device(config)# ip ftp username NetAdmin1`	（任意）デフォルトのリモート ユーザ名を指定します。
ステップ 4	**ipftppassword** *password* 例： `Device(config)# ip ftp password adminpassword`	（任意）デフォルトのパスワードを指定します。
ステップ 5	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 6	次のいずれかを実行します。 • **copysystem:running-configftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] または • **copynvram:startup-config ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] 例： `Device# copy system:running-config ftp:`	FTP サーバの指定された場所へ実行コンフィギュレーションまたはスタートアップ コンフィギュレーション ファイルをコピーします。

例

FTP サーバへの実行コンフィギュレーション ファイルの格納

次に、runfile-confg という名前の実行コンフィギュレーション ファイルを IP アドレス 172.16.101.101 のリモート ホスト上の netadmin1 ディレクトリにコピーする例を示します。

```
Device# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/runfile-confg
Write file runfile-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Device#
```

FTP サーバへのスタートアップ コンフィギュレーション ファイルの格納

次に、FTP を使用してファイルをコピーすることによって、サーバ上にスタートアップ コンフィギュレーション ファイルを格納する例を示します。

```
Device# configure terminal

Device(config)# ip ftp username netadmin2

Device(config)# ip ftp password mypass

Device(config)# end

Device# copy nvram:startup-config ftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [start-confg]?
Write file start-confg on host 172.16.101.101?[confirm]
![OK]
```

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

TFTP サーバからデバイスへのコンフィギュレーション ファイルのコピー（CLI）

TFTP サーバからデバイスへコンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copytftp:**[[[*//location*]/*directory*]/*filename*] **system:running-config** 例： `Device# copy tftp://server1/dir10/datasource system:running-config`	TFTP サーバから実行コンフィギュレーションへコンフィギュレーション ファイルをコピーします。
ステップ 3	**copytftp:**[[[*//location*]/*directory*]/*filename*] **nvram:startup-config** 例：	TFTP サーバからスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします。

	コマンドまたはアクション	目的
	`Device# copy tftp://server1/dir10/datasource nvram:startup-config`	
ステップ 4	**copy tftp:[[[//location][/directory]/filename] flash:[[[//location][/directory]/startup-config]** 例： `Device# copy tftp://server1/dir10/datasource flash:startup-config`	TFTP サーバからスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします。

例

次に、IP アドレス 172.16.2.155 にある、**tokyo-confg**という名前のファイルからソフトウェアを設定する例を示します。

```
Device# copy tftp://172.16.2.155/tokyo-confg system:running-config

Configure using tokyo-confg from 172.16.2.155? [confirm] Y

Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

rcpサーバからデバイスへのコンフィギュレーションファイルのコピー（CLI）

rcp サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	（任意）端末からコンフィギュレーション モードを開始します。この手順は、デフォルトのリモート ユーザ名を上書きする場合にだけ必要です（ステップ 3 を参照）。
ステップ 3	**iprcmdremote-username** *username* 例： `Device(config)# ip rcmd remote-username NetAdmin1`	（任意）リモート ユーザ名を指定します。
ステップ 4	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 を参照）。
ステップ 5	次のいずれかを実行します。 • **copy rcp://**[*username@location/directory/filename*] **system:running-config** • **copy rcp://**[*username@location/directory/filename*] **nvram:startup-config** 例： `Device# copy rcp://[user1@example.com/dir10/fileone] nvram:startup-config`	rcp サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします。

例

RCP の Running-Config のコピー

次に、host1-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからコピーし、デバイスでコマンドをロードし実行する例を示します。

```
Device# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Device#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

RCP の Startup-Config のコピー

次に、リモートユーザ名 netadmin1 を指定する例を示します。次に host2-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからスタートアップ コンフィギュレーションへコピーします。

```
Device# configure terminal
Device(config)# ip rcmd remote-username netadmin1
Device(config)# end
Device# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Device#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from 172.16.101.101
```

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

FTP サーバからデバイスへのコンフィギュレーション ファイルのコピー（CLI）

FTP サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	（任意）グローバル コンフィギュレーション モードを開始できます。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 3 および 4 を参照）。

	コマンドまたはアクション	目的
ステップ 3	**ipftpusername** *username* 例： `Device(config)# ip ftp username NetAdmin1`	（任意）デフォルトのリモート ユーザ名を指定します。
ステップ 4	**ipftppassword** *password* 例： `Device(config)# ip ftp password adminpassword`	（任意）デフォルトのパスワードを指定します。
ステップ 5	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 3 および 4 を参照）。
ステップ 6	次のいずれかを実行します。 • **copyftp:** [[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*]**system:running-config** • **copyftp:** [[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*]**nvram:startup-config** 例： `Device# copy ftp:nvram:startup-config`	FTP を使用して、ネットワーク サーバから実行メモリまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします。

例

FTP の Running-Config のコピー

次に、host1-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからコピーし、デバイスでコマンドをロードし実行する例を示します。

```
Device# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Device#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

FTP の Startup-Config のコピー

次に、リモートユーザ名 netadmin1 を指定する例を示します。次に host2-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからスタートアップ コンフィギュレーションへコピーします。

```
Device# configure terminal
Device(config)# ip ftp username netadmin1
Device(config)# ip ftp password mypass
Device(config)# end
Device# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[host1-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Device#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from 172.16.101.101
```

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

NVRAM より大きいコンフィギュレーション ファイルの保守

NVRAM のサイズを超えるコンフィギュレーションファイルを保守するには、以降のセクションで説明するタスクを実行します。

コンフィギュレーション ファイルの圧縮（CLI）

コンフィギュレーション ファイルを圧縮するには、このセクションの手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**servicecompress-config** 例： `Device(config)# service compress-config`	コンフィギュレーション ファイルを圧縮することを指定します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	次のいずれかを実行します。 • 新しいコンフィギュレーションをコピーするには、FTP、RCP、TFTP を使用します。 • **configureterminal** 例： `Device# configure terminal`	新しいコンフィギュレーションを入力します。 • NVRAM のサイズの 3 倍以上のコンフィギュレーションをロードしようとすると、次のエラー メッセージが表示されます。 「[buffer overflow - *file-size* /*buffer-size* bytes]。」
ステップ 6	**copysystem:running-confignvram:startup-config** 例： `Device(config)# copy system:running-config nvram:startup-config`	実行コンフィギュレーションの変更が終わったら、新しいコンフィギュレーションを保存します。

例

次に、129 KB のコンフィギュレーション ファイルを 11 KB に圧縮する例を示します。

```
Device# configure terminal

Device(config)# service compress-config

Device(config)# end

Device# copy tftp://172.16.2.15/tokyo-confg system:running-config

Configure using tokyo-confg from 172.16.2.155? [confirm] y

Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
Device# copy system:running-config nvram:startup-config

Building configuration...
Compressing configuration from 129648 bytes to 11077 bytes
[OK]
```

コンフィギュレーションのクラス A フラッシュ ファイル システム上のフラッシュ メモリへの格納（CLI）

スタートアップ コンフィギュレーションをフラッシュ メモリに格納するには、このセクションの手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copynvram:startup-config** *flash-filesystem:filename* 例： `Device# copy nvram:startup-config usbflash0:switch-config`	新しい場所に現在のスタートアップ コンフィギュレーションをコピーして、コンフィギュレーション ファイルを作成します。
ステップ 3	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**bootconfigflash-filesystem:** *filename* 例： `Device(config)# boot config usbflash0:switch-config`	CONFIG_FILE 環境変数を設定することにより、フラッシュ メモリにスタートアップ コンフィギュレーション ファイルを格納することを指定します。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	次のいずれかを実行します。 • 新しいコンフィギュレーションをコピーするには、FTP、RCP、TFTP を使用します。NVRAM サイズの 3 倍を超える大きさのコンフィギュレーションをロードしようとすると、次のエラー メッセージが表示されます。「[buffer overflow - *file-size* /*buffer-size* bytes]」	新しいコンフィギュレーションを入力します。

	コマンドまたはアクション	目的
	• **configureterminal** 例： `Device# configure terminal`	
ステップ 7	**copysystem:running-configvram:startup-config** 例： `Device(config)# copy system:running-config nvram:startup-config`	実行コンフィギュレーションの変更が終わったら、新しいコンフィギュレーションを保存します。

例

以下に、usbflash0: に格納したコンフィギュレーションの例を示します。

```
Device# copy nvram:startup-config usbflash0:switch-config

Device# configure terminal

Device(config)# boot config usbflash0:switch-config

Device(config)# end

Device# copy system:running-config nvram:startup-config
```

ネットワークからのコンフィギュレーション コマンドのロード（CLI）

ネットワーク サーバを使用して、大きなコンフィギュレーションを保存するには、このセクションの手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copysystem:running-config** {**ftp:** | **rcp:** | **tftp:**} 例： `Device# copy system:running-config ftp:`	実行コンフィギュレーションを FTP、RCP、TFTP のいずれかのサーバに保存します。

	コマンドまたはアクション	目的
ステップ 3	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**bootnetwork**{**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*]} 例： `Device(config)# boot network ftp://user1:guessme@example.com/dir10/file1`	起動時にスタートアップ コンフィギュレーション ファイルをネットワーク サーバからロードすることを指定します。
ステップ 5	**serviceconfig** 例： `Device(config)# service config`	システムの起動時にコンフィギュレーション ファイルをダウンロードするようにスイッチをイネーブルにします。
ステップ 6	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 7	**copysystem:running-confignvram:startup-config** 例： `Device# copy system:running-config nvram:startup-config`	設定を保存します。

フラッシュ メモリからスタートアップまたは実行コンフィギュレーションへのコンフィギュレーション ファイルのコピー（CLI）

フラッシュ メモリから現在の NVRAM にあるスタートアップ コンフィギュレーションまたは実行コンフィギュレーションへコンフィギュレーション ファイルを直接コピーするには、ステップ 2 のいずれかのコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかを実行します。 • **copy** *filesystem*: [*partition-number*:][*filename*] **nvram:startup-config** • **copy** *filesystem*: [*partition-number*:][*filename*] **system:running-config** 例： `Device# copy usbflash0:4:ios-upgrade-1 nvram:startup-config`	• NVRAM にコンフィギュレーション ファイルを直接ロードする、または • 現在の実行コンフィギュレーションにコンフィギュレーション ファイルをコピーします。

例

次に、usbflash0 にあるフラッシュ メモリ PC カードのパーティション 4 からデバイスのスタートアップ コンフィギュレーションへ ios-upgrade-1 という名前のファイルをコピーする例を示します。

```
Device# copy usbflash0:4:ios-upgrade-1 nvram:startup-config

Copy 'ios-upgrade-1' from flash device as 'startup-config' ? [yes/no] yes

[OK]
```

フラッシュ メモリ ファイル システム間でのコンフィギュレーション ファイルのコピー（CLI）

複数のフラッシュ メモリ ファイル システムを備えたプラットフォーム上では、内部フラッシュ メモリなどのフラッシュ メモリ ファイル システムから他のフラッシュ メモリ ファイル システムへファイルをコピーできます。異なるフラッシュ メモリ ファイル システムへファイルをコピーすると、使用中のコンフィギュレーションのバックアップ コピーを作成し、他のデバイスにコンフィギュレーションを複製できます。フラッシュ メモリ ファイル システム間でコンフィギュレーション ファイルをコピーするには、EXEC モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**show** *source-filesystem*: **例：** `Device# show flash:`	フラッシュ メモリのレイアウトと内容を表示して、ファイル名を確認します。
ステップ 3	**copy** *source-filesystem*: [*partition-number*:][*filename*] *dest-filesystem*:[*partition-number*:][*filename*] **例：** `Device# copy flash: usbflash0:`	フラッシュ メモリ デバイス間でコンフィギュレーション ファイルをコピーします。 • コピー元デバイスとコピー先デバイスは同じにはできません。例えば、**copy usbflash0: usbflash0:** コマンドは無効です。

例

次に、内部フラッシュ メモリのパーティション 1 からデバイス上の usbflash0 のパーティション 1 へ running-config という名前のファイルをコピーする例を示します。この例では、コピー元のパーティションが指定されていないため、デバイスからパーティション番号を要求されます。

```
Device# copy flash: usbflash0:

System flash
Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1         4096K   3070K     1025K     4096K      Read/Write     Direct
  2        16384K   1671K    14712K     8192K      Read/Write     Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]
System flash directory, partition 1:
File  Length   Name/status
  1   3142748  dirt/network/mars-test/c3600-j-mz.latest
  2   850      running-config
[3143728 bytes used, 1050576 available, 4194304 total]
usbflash0 flash directory:
File  Length   Name/status
  1   1711088  dirt/gate/c3600-i-mz
  2   850      running-config
[1712068 bytes used, 2482236 available, 4194304 total]
Source file name? running-config

Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)...  OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'running-config' from flash: device
  as 'running-config' into usbflash0: device WITH erase? [yes/no] yes
```

```
Erasing device... eeee
```

	コマンドまたはアクション	目的
ステップ 6	**copyftp:**[[*//location*]/*directory*]/*bundle_name***flash:** 例： `Device>copy ftp://cat3k_caa-universal9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash:`	FTP を使用してネットワーク サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーします。

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

RCP サーバからフラッシュ メモリ デバイスへのコンフィギュレーション ファイルのコピー（CLI）

RCP サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	（任意）グローバル コンフィギュレーション モードを開始します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にのみ必要です（ステップ 3 を参照）。
ステップ 3	**iprcmdremote-username** *username* 例： `Device(config)# ip rcmd remote-username Admin01`	（任意）リモート ユーザ名を指定します。
ステップ 4	**end** 例：	（任意）コンフィギュレーション モードを終了します。この手順は、デフォルトのリモート ユーザ名またはパスワー

	コマンドまたはアクション	目的
	`Device(config)# end`	ドを上書きする場合にのみ必要です（ステップ 3 を参照）。
ステップ 5	**copyrcp:**[[[//[*username@*]*location*]/*directory*] /*bundle_name*]**flash:** 例： `Device# copy rcp://netadmin@172.16.101.101/bundle1 flash:`	RCP を使用してネットワーク サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーします。追加情報または確認を要求するデバイスからのプロンプトに対し応答します。このプロンプトは、**copy** コマンドで入力した情報量および **fileprompt** コマンドの現在の設定によって異なります。

TFTPサーバからフラッシュメモリデバイスへのコンフィギュレーション ファイルのコピー（CLI）

TFTP サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copytftp:**[[[*//location*]/*directory*]/bundle_name**flash:** 例： `Device# copy tftp://cat3k_caa-universal-9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash:`	TFTP サーバからフラッシュ メモリ デバイスへファイルをコピーします。追加情報または確認を要求するデバイスからのプロンプトに対し応答します。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** コマンドの現在の設定によって異なります。

例

次に、TFTP サーバから usbflash0 に挿入されているフラッシュ メモリ カードへ、switch-config という名前のコンフィギュレーション ファイルをコピーする例を示します。コピーされたファイルの名前は new-config に変更されます。

```
Device#
copy tftp:switch-config usbflash0:new-config
```

スタートアップ コンフィギュレーション ファイルでのコンフィギュレーション コマンドの再実行（CLI）

スタートアップ コンフィギュレーションファイルのコマンドを再実行するには、このセクションの手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configurememory** 例： `Device# configure memory`	スタートアップ コンフィギュレーション ファイルでコンフィギュレーション コマンドを再実行します。

スタートアップ コンフィギュレーションのクリア（CLI）

スタートアップ コンフィギュレーションから設定情報を消去できます。デバイスをスタートアップ コンフィギュレーションなしで再起動した場合は、デバイスを最初から設定できるように、デバイスは、Setup コマンド ファシリティに移行します。スタートアップ コンフィギュレーションの内容をクリアするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**erasenvram** 例：	スタートアップ コンフィギュレーションの内容をクリアします。

	コマンドまたはアクション	目的
	`Device# erase nvram`	（注） クラス A フラッシュ ファイル システムのプラットフォーム以外のすべてのプラットフォームでは、このコマンドにより NVRAM が消去されます。スタートアップ コンフィギュレーション ファイルは、いったん削除すると復元できません。クラス A フラッシュ ファイル システムのプラットフォーム上では、**erase startup-config** EXEC コマンドを使用すると、デバイスが CONFIG_FILE 環境変数により指定されたコンフィギュレーションを消去または削除します。この変数が NVRAM を指定している場合は、デバイスにより NVRAM が消去されます。CONFIG_FILE 環境変数がフラッシュ メモリ デバイスとコンフィギュレーション ファイル名を指定している場合は、デバイスによりコンフィギュレーション ファイルが削除されます。つまり、そのコンフィギュレーション ファイルは、デバイスにより消去されるのではなく、「削除済み」としてマークされます。この機能では、削除されたファイルを回復できます。

指定されたコンフィギュレーション ファイルの削除（CLI）

特定のフラッシュ デバイスの指定された設定を削除するには、このセクションの手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**delete** *flash-filesystem*:*filename* 例： `Device# delete usbflash0:myconfig`	特定のフラッシュ デバイス上の指定されたコンフィギュレーション ファイルを削除します。 （注） クラス A および B フラッシュ ファイル システムでは、フラッシュ メモリ内の特定のファイルを削除すると、そのファイルは削除済みとしてシステムによりマークされます。これにより、**undelete** EXEC コマンドを使用して、削除したファイルを後で回復できるようになります。消去されたファイルは回復できません。コンフィギュレーション ファイルを完全に消去するには、**squeeze** EXEC コマンドを使用します。クラス C フラッシュ ファイル システムでは、削除されたファイルは回復できません。CONFIG_FILE 環境変数で指定されたコンフィギュレーション ファイルを消去または削除しようとした場合、システムにより削除の確認を求めるプロンプトが表示されます。

クラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定（CLI）

クラス A フラッシュ ファイル システムでは、CONFIG_FILE 環境変数で指定されたスタートアップ コンフィギュレーション ファイルをロードするように Cisco IOS ソフトウェアを設定で

きます。CONFIG_FILE 変数のデフォルトは NVRAM になります。CONFIG_FILE 環境変数を変更するには、このセクションの手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copy**[*flash-url* | *ftp-url* | *rcp-url* | *tftp-url* | **system:running-config** | **nvram:startup-config**] *dest-flash-url* 例： `Device# copy system:running-config nvram:startup-config`	フラッシュ ファイル システムにコンフィギュレーション ファイルをコピーします。再起動時には、ここからデバイスにファイルがロードされます。
ステップ 3	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**bootconfig** *dest-flash-url* 例： `Device(config)# boot config 172.16.1.1`	CONFIG_FILE 環境変数を設定します。この手順により、実行時の CONFIG_FILE 環境変数が変更されます。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**copysystem:running-confignvram:startup-config** 例： `Device# copy system:running-config nvram:startup-config`	スタートアップ コンフィギュレーションにステップ 3 で実行されたコンフィギュレーションを保存します。
ステップ 7	**showboot** 例： `Device# show boot`	（任意）CONFIG_FILE 環境変数の内容を確認できます。

例

次の例は、実行コンフィギュレーション ファイルをデバイスにコピーします。その後、システムが再起動されるとこのコンフィギュレーションがスタートアップ コンフィギュレーションとして使用されます。

```
Device# copy system:running-config usbflash0:config2
Device# configure terminal
Device(config)# boot config usbflash0:config2
Device(config)# end
Device# copy system:running-config nvram:startup-config
[ok]
Device# show boot
BOOT variable = usbflash0:rsp-boot-m
CONFIG_FILE variable = nvram:
Current CONFIG_FILE variable = usbflash0:config2
Configuration register is 0x010F
```

次の作業

スタートアップ コンフィギュレーション ファイルの場所を指定すると、**nvram:startup-config** コマンドは、スタートアップ コンフィギュレーション ファイルの新しい場所のエイリアスとなります。**more nvram:startup-config** EXEC コマンドにより、スタートアップ コンフィギュレーションが、その場所に関係なく表示されます。**erase nvram:startup-config** EXEC コマンドにより、NVRAM の内容が消去され、CONFIG_FILE 環境変数で指定されたファイルが削除されます。

copy system:running-config nvram:startup-config コマンドを使用して設定を保存した場合、デバイスにより、コンフィギュレーション ファイルの完全バージョンはCONFIG_FILE環境変数で指定した場所に保存され、抽出バージョンはNVRAMに保存されます。抽出バージョンとは、アクセス リスト情報を含まないバージョンです。NVRAM に完全バージョンのコンフィギュレーション ファイルが含まれている場合、デバイスは、完全バージョンを抽出バージョンで上書きすることを確認するプロンプトを表示します。NVRAMに抽出コンフィギュレーションが含まれている場合、デバイスは確認のプロンプトを表示しないでNVRAMにある既存の抽出バージョンのコンフィギュレーション ファイルを上書きする処理を続行します。

（注） フラッシュ デバイスにあるファイルを CONFIG_FILE 環境変数として指定した場合、**copy system:running-config nvram:startup-config** コマンドでコンフィギュレーション ファイルを保存するたびに、古いコンフィギュレーション ファイルは「deleted」とマークされ、新しいコンフィギュレーション ファイルがそのデバイスに保存されます。それでも古いコンフィギュレーション ファイルがメモリを使用するため、最終的にフラッシュ メモリは一杯になります。**squeeze** EXEC コマンドを使用して、古いコンフィギュレーション ファイルを完全に削除してから、領域を再要求してください。

コンフィギュレーションファイルをダウンロードするデバイスの設定

ネットワーク コンフィギュレーションおよびホスト コンフィギュレーション ファイル名の順序付きリストを指定できます。Cisco IOS XE ソフトウェアは、適切なネットワークまたはホスト コンフィギュレーション ファイルをロードするまで、このリストをスキャンします。

システムの起動時にコンフィギュレーションファイルをダウンロードするようにデバイスを設定するには、次の項で説明する作業を少なくとも 1 つ実行します。

- ネットワーク コンフィギュレーションファイルをダウンロードするデバイスの設定（CLI）
- ホスト コンフィギュレーション ファイルをダウンロードするデバイスの設定（CLI）

起動中にコンフィギュレーションファイルをロードできなかった場合、要求されたファイルがホストから提供されるまで、デバイスは 10 分ごと（デフォルト設定）に再試行します。試行が失敗するごとに、デバイスにより以下のメッセージがコンソール端末に表示されます。

```
Booting host-confg... [timed out]
```

スタートアップ コンフィギュレーション ファイルになんらかの問題がある場合、またはコンフィギュレーション レジスタが NVRAM を無視するように設定されている場合は、デバイスは Setup コマンド ファシリティに移行します。

ネットワーク コンフィギュレーション ファイルをダウンロードするデバイスの設定（CLI）

起動時にサーバからネットワーク コンフィギュレーション ファイルをダウンロードするように Cisco IOS ソフトウェアを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bootnetwork** {**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*]}	起動時にダウンロードするネットワーク コンフィギュレーション ファイルおよび使用されるプロトコル（TFTP、RCP、または FTP）を指定します。

	コマンドまたはアクション	目的
	例： `Device(config)# boot network tftp:hostfile1`	• ネットワーク コンフィギュレーション ファイル名を指定しない場合、Cisco IOS ソフトウェアはデフォルトのファイル名の network-confg を使用します。アドレスを省略した場合、デバイスはブロードキャストアドレスを使用します。 • 複数のネットワーク コンフィギュレーション ファイルを指定できます。ソフトウェアは、ネットワーク コンフィギュレーション ファイルをロードできるまで、入力された順に試行します。この手順は、異なる設定情報を持つ、ネットワーク サーバ上にロードされるファイルを複数保持する場合に役立ちます。
ステップ 4	**serviceconfig** 例： `Device(config)# service config`	再起動時にネットワーク ファイルを自動的にロードするようにシステムをイネーブルにします。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**copy system:running-config nvram:startup-config** 例： `Device# copy system:running-config nvram:startup-config`	実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに保存します。

ホスト コンフィギュレーション ファイルをダウンロードするデバイスの設定（CLI）

起動時にサーバからホスト コンフィギュレーション ファイルをダウンロードするように Cisco IOS ソフトウェアを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**boothost**{**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*] } 例： `Device(config)# boot host tftp:hostfile1`	起動時にダウンロードするホスト コンフィギュレーション ファイルおよび使用されるプロトコル（FTP、RCP、または TFTP）を指定します。 • ホスト コンフィギュレーション ファイルの名前を指定しない場合、デバイスは、それ自身の名前を使用してホスト コンフィギュレーション ファイル名を形成します。このとき、その名前はすべて小文字に変換され、すべてのドメイン情報は削除され、「-config」が追加されます。ホスト名の情報を利用できない場合は、ソフトウェアはデフォルトのホスト コンフィギュレーション ファイル名の デバイス -confg を使用します。アドレスを省略した場合、デバイス はブロードキャスト アドレスを使用します。 • 複数のホストコンフィギュレーション ファイルを指定できます。Cisco IOS ソフトウェアは、ホスト コンフィギュレーションファイルをロードできるまで、入力された順に試行します。この手順は、異なる設定情報を持つ、ネットワーク サーバ上にロードされるファイルを複数保持する場合に役立ちます。

	コマンドまたはアクション	目的
ステップ 4	**serviceconfig** 例： `Device(config)# service config`	再起動時にホスト ファイルを自動的にロードするようにシステムをイネーブルにします。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**copysystem:running-confignvram:startup-config** 例： `Device# copy system:running-config nvram:startup-config`	実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに保存します。

例

次に、hostfile1 という名前のホスト コンフィギュレーション ファイルおよび networkfile1 という名前のネットワーク コンフィギュレーション ファイルをダウンロードするようにデバイスを設定する例を示します。デバイスは TFTP およびブロードキャスト アドレスを使用してファイルを取得します。

```
Device# configure terminal
Device(config)# boot host tftp:hostfile1
Device(config)# boot network tftp:networkfile1
Device(config)# service config
Device(config)# end
Device# copy system:running-config nvram:startup-config
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS コンフィギュレーション コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準

規格	Title
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
• 新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 145 章

コンフィギュレーションの置換とロールバック

- コンフィギュレーションの置換とロールバックの前提条件 （3093 ページ）
- コンフィギュレーションの置換とロールバックの制約事項 （3094 ページ）
- コンフィギュレーションの置換とロールバックについて （3094 ページ）
- コンフィギュレーションの置換とロールバックの使用方法 （3097 ページ）
- コンフィギュレーションの置換とロールバックの設定例 （3105 ページ）
- その他の参考資料 （3107 ページ）

コンフィギュレーションの置換とロールバックの前提条件

コンフィギュレーションの置換とロールバックの機能に対する入力となるコンフィギュレーション ファイルの形式は、標準の Cisco ソフトウェア コンフィギュレーション ファイルの、次に示すインデント規則に準拠している必要があります。

- 新しい行のすべてのコマンドは、コマンドがコンフィギュレーションサブモードにない限り、インデントなしで開始します。
- レベル 1 コンフィギュレーション サブモード内のコマンドは、スペース 1 個分インデントします。
- レベル 2 コンフィギュレーション サブモード内のコマンドは、スペース 2 個分インデントします。
- 以下、続くサブモード内のコマンドは、同じようにインデントします。

これらのインデント規則には、ソフトウェアが **show running-config** や **copy running-config** *destination-url* などのコマンドのコンフィギュレーション ファイルを作成する方法が記述されています。シスコ デバイスで生成されるコンフィギュレーション ファイルは、いずれもこうした規則に従います。

2つのコンフィギュレーションファイル（現在の実行コンフィギュレーションと、保存された置換用コンフィギュレーション）を合わせたサイズより大きな空きメモリが必要です。

コンフィギュレーションの置換とロールバックの制約事項

デバイスに、2 つのコンフィギュレーション ファイル（現在の実行コンフィギュレーションと、保存された置換用コンフィギュレーション）を合わせたサイズより大きな空きメモリがない場合、コンフィギュレーション置換操作は実行されません。

ネットワーク デバイスの物理コンポーネント（物理インターフェイスなど）に関連する特定の Cisco コンフィギュレーション コマンドは、実行コンフィギュレーションについて追加または削除することはできません。たとえば、コンフィギュレーション置換操作を行っても、そのインターフェイスがデバイス上に物理的に存在する場合、現在の実行コンフィギュレーションから **interface ethernet 0** コマンド行を削除することはできません。同様に、**interface ethernet 1** コマンド行は、そのようなインターフェイスがデバイス上に物理的に存在しない場合、実行コンフィギュレーションに追加することはできません。コンフィギュレーション置換操作でこのタイプの変更を試行すると、その特定のコマンド行が失敗したことを示すエラー メッセージが表示されます。

非常にまれなケースですが、ルータをリロードしないと特定の Cisco コンフィギュレーション コマンドを実行コンフィギュレーションから削除できないことがあります。コンフィギュレーション置換操作でこのタイプのコマンドの削除を試行すると、その特定のコマンド行が失敗したことを示すエラー メッセージが表示されます。

コンフィギュレーションの置換とロールバックについて

コンフィギュレーション アーカイブ

Cisco IOS コンフィギュレーション アーカイブは、**configure replace** コマンドを使用するコンフィギュレーションのロールバック機能を強化するために、Cisco IOS コンフィギュレーション ファイルのアーカイブの保存、編成、管理を行うことを目的とした機能です。この機能の導入前にも、実行コンフィギュレーションのコピーを **copy running-config** *destination-url* コマンドを使用して保存し、ローカルやリモートに置換ファイルを保管できました。ただし、この方法ではファイルの自動管理を行うことはできませんでした。一方、コンフィギュレーションの置換とロールバック機能では、実行コンフィギュレーション ファイルを自動的に Cisco IOS コンフィギュレーション アーカイブに保存できます。アーカイブされたファイルはコンフィギュレーションのチェックポイントとして参照することができ、**configure replace** コマンドを使用して以前のコンフィギュレーション状態に戻すために利用できます。

archive config コマンドを使用すると、Cisco IOS コンフィギュレーションをコンフィギュレーション アーカイブに保存できます。その場合、標準のディレクトリとファイル名のプレフィク

スが使用され、バージョン番号（およびオプションでタイムスタンプ）が自動的に付加されます。バージョン番号は連続したファイルを保存するごとに、1 つずつ大きくなります。この機能により、保存した Cisco IOS コンフィギュレーション ファイルを一貫して識別できます。アーカイブに保存する実行コンフィギュレーションの数は指定することができます。アーカイブ内のファイル数が上限値に達すると、次に最新のファイルが保存されるときに、最も古いファイルが自動的に消去されます。**show archive** コマンドを使用すると、Cisco IOS コンフィギュレーション アーカイブに保存されているすべてのコンフィギュレーション ファイルに関する情報が表示されます。

コンフィギュレーション ファイルを保存する Cisco IOS コンフィギュレーション アーカイブは、**configure replace** コマンドで使用することによって、FTP、HTTP、RCP、TFTP のファイル システム上に配置できます。

コンフィギュレーションの置換

configure replace 特権 EXEC コマンドにより、現在の実行コンフィギュレーションを、保存しておいた Cisco IOS コンフィギュレーション ファイルで置換することができます。この機能は、コンフィギュレーションを保存しておいた状態へ戻すために使用することができ、そのコンフィギュレーション状態が保存された後にどのような変更が加えられても、効果的にロールバックさせることができます。

configure replace コマンドを使用するときは、現在の実行コンフィギュレーションと置換するための、保存された Cisco IOS コンフィギュレーション ファイルを指定する必要があります。置換ファイルは、Cisco IOS デバイスによって作成された完全なコンフィギュレーション（**copy running-config** *destination-url* コマンドによって作成されたものなど）であることが必要です。置換ファイルを外部的に作成する場合は、Cisco IOS デバイスが作成するファイル形式に完全に準拠していなければなりません。**configure replace** コマンドを入力すると、現在の実行コンフィギュレーションが指定された置換コンフィギュレーションと比較され、一連の diff が生成されます。2 つのファイルの比較に使用されるアルゴリズムは、**show archive config differences** コマンドで使用されるものと同じです。置換コンフィギュレーションの状態になるよう、diff の結果が Cisco IOS パーサーによって適用されます。diff のみが適用されるため、現在の実行コンフィギュレーション上にすでに存在していた設定コマンドを再適用することにより生じる、潜在的なサービスの中断を避けられます。このアルゴリズムでは、順序に依存するコマンド（アクセス リストなど）へのコンフィギュレーション変更を、複数のパス プロセスを通して効果的に実行します。通常の環境では、コンフィギュレーション置換操作の完了に必要なパスは 3 つまでであり、ループ動作を防ぐためのパスは最大 5 つまでに制限されます。

copy *source-url* **running-config** 特権 EXEC コマンドは、保存された Cisco IOS コンフィギュレーション ファイルを実行コンフィギュレーションへコピーするためによく使用されます。**copy** *source-url* **running-config** コマンドを **configure replace** *target-url* 特権 EXEC コマンドの代わりに使用する場合、主な相違点として次の点に注意が必要です。

- **copy** *source-url* **running-config** コマンドはマージ動作であり、ソース ファイルと現在の実行コンフィギュレーションの両方のコマンドがすべて保持されます。このコマンドでは、現在の実行コンフィギュレーションにのみ含まれ、ソースファイルには存在しないコマンドが削除されることはありません。これに対し、**configure replace** *target-url* コマンドで

は、置換ファイルに存在しないコマンドは現在の実行コンフィギュレーションから削除され、現在の実行コンフィギュレーションに追加が必要なコマンドが追加されます。

- **copy** *source-url* **running-config** コマンドでは、現在の実行コンフィギュレーションにすでに存在しているかどうかにかかわらず、ソースファイル中のすべてのコマンドが適用されます。このアルゴリズムは効率的でない上、場合によってはサービスの停止が発生します。これに対し、**configure replace** *target-url* コマンドでは適用が必要なコマンドのみを適用し、現在の実行コンフィギュレーションに存在しているコマンドは再適用されません。
- **copy** *source-url* **running-config** コマンドでは部分的なコンフィギュレーション ファイルもコピー元として使用できますが、**configure replace** *target-url* コマンドの置換ファイルとして使用できるのは、完全な Cisco IOS コンフィギュレーション ファイルのみです。

コンフィギュレーション置換操作にロック機能が導入されました。**configure replace** コマンドが使用されると、コンフィギュレーション置換中、デフォルトで実行コンフィギュレーションファイルがロックされます。このロック メカニズムによって、置換動作の実行中に他のユーザが実行コンフィギュレーションを変更しようとしたために、置換動作の不正終了が発生することを防止できます。**no lock** キーワードを **configure replace** コマンドの実行時に使用すると、実行コンフィギュレーションのロックをディセーブルにできます。

実行コンフィギュレーションのロックは、コンフィギュレーションの置換動作終了時に自動的にクリアされます。**show configuration lock** コマンドを使用すると、現在実行コンフィギュレーションに適用されているロックをすべて表示できます。

コンフィギュレーション ロールバック

ロールバックの概念は、データベースの操作ではトランザクション プロセス モデルに由来します。データベース トランザクションでは、あるデータベースのテーブルに一連の変更を加えることがあります。その後、変更を実行する（変更を恒久的に適用する）か、変更をロールバックする（変更を破棄してテーブルを以前の状態に戻す）かを選択することになります。ここでロールバックが意味するのは、変更のログを含んだジャーナルファイルが破棄され、何の変更も加えられないということです。ロールバック操作の結果として、加えた変更が適用される前の状態に戻ります。

configure replace コマンドを使用することで、以前のコンフィギュレーション状態へ戻ることが可能になり、コンフィギュレーション状態の保存後に加えた変更を効率的にロールバックさせることができます。Cisco IOS コンフィギュレーション ロールバックは、適用された一連の変更をもとにロールバック動作を行うのではなく、保存された Cisco コンフィギュレーションファイルに基づいた特定のコンフィギュレーション状態へ戻るというコンセプトを採用しています。このコンセプトは、チェックポイント（データベースの保存されたバージョン）に特定の状態を保存しておくという、データベースの考え方に類似しています。

コンフィギュレーションのロールバック機能が必要な場合、コンフィギュレーションの変更に先立ってCisco IOS実行コンフィギュレーションを保存する必要があります。そして、コンフィギュレーションへの変更を入力した後に、保存しておいたコンフィギュレーションファイルを変更のロールバックに使用できます（**configure replace** *target-url* コマンドを使用）。保存された Cisco IOS コンフィギュレーション ファイルならどれでも置換コンフィギュレーションとし

て指定できるため、一部のロールバック モデルのように、ロールバックの数が制限されることもありません。

コンフィギュレーション ロールバック変更確認

コンフィギュレーション ロールバック変更確認機能により、コンフィギュレーション変更の実行に際して確認を要求するようオプションで設定できます。この確認が受信できない場合、コンフィギュレーションは変更が適用される前の状態に戻されます。このメカニズムは、ネットワーク デバイスとユーザまたは管理アプリケーションとの接続において、コンフィギュレーション変更に起因する切断を防止するものです。

コンフィギュレーションの置換とロールバックの利点

- コンフィギュレーションの変更を効率的にロールバックさせて、以前のコンフィギュレーション状態へ戻ることが可能。
- デバイスをリロードしたり、CLI で実行コンフィギュレーション ファイルに加えた変更を手動で元に戻したりすることなく、現在の実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルと置換できるため、システムのダウンタイムが減少。
- 保存しておいたどの Cisco IOS コンフィギュレーション状態に戻すことも可能。
- 追加や削除が必要なコマンドだけが影響を受ける場合、デバイスに完全なコンフィギュレーション ファイルを適用することができるため、コンフィギュレーションの変更が簡素化。
- **configurerepl**ace コマンドを **copy** *source-url***running-config** コマンドの代用として使用する場合、現在の実行コンフィギュレーションに存在しているコマンドを再度適用することがないため、効率が向上し、かつサービス停止のリスクを回避。

コンフィギュレーションの置換とロールバックの使用方法

コンフィギュレーション アーカイブの作成（CLI）

configure replace コマンドを使用するために、前提条件となる設定はありません。**configure replace** コマンドと Cisco IOS コンフィギュレーション アーカイブおよび **archive config** コマンドとの併用は任意ですが、コンフィギュレーション ロールバックの使用にあたっては大きな利点があります。**archive config** コマンドを使用する前に、コンフィギュレーション アーカイブを設定しておく必要があります。コンフィギュレーション アーカイブの特性を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**archive** 例： `Device(config)# archive`	アーカイブ コンフィギュレーション モードを開始します。
ステップ 4	**path** *url* 例： `Device(config-archive)# path flash:myconfiguration`	Cisco IOS コンフィギュレーション アーカイブの場所と、ファイル名のプレフィックスを指定します。 （注） パスのところでファイルの代わりにディレクトリを指定する場合、ディレクトリ名は path flash:/directory/ のように後ろにスラッシュを付ける必要があります。このスラッシュはファイル名の後ろでは必要ありません。ディレクトリを指定する場合にだけ使います。
ステップ 5	**maximum** *number* 例： `Device(config-archive)# maximum 14`	（任意）Cisco IOS コンフィギュレーション アーカイブに保存される実行コンフィギュレーションのアーカイブ ファイル数の上限値を設定します。 • *number* 引数は、Cisco IOS コンフィギュレーション アーカイブに保存される実行コンフィギュレーションのアーカイブ ファイル数の上限値を示します。有効な値は 1 ～ 14 で、デフォルトは 10 です。

	コマンドまたはアクション	目的
		（注） このコマンドを使用する前に、**path** コマンドを設定して Cisco IOS コンフィギュレーション アーカイブの位置とファイル名プレフィックスを指定しておく必要があります。
ステップ 6	**time-period** 分 例： `Device(config-archive)# time-period 1440`	（任意）Cisco IOS コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する間隔を設定します。 • Cisco IOS コンフィギュレーション アーカイブに現在の実行コンフィギュレーションのアーカイブ ファイルをどれほどの頻度で自動保存するかを、minutes 引数により分単位で指定します。 （注） このコマンドを使用する前に、**path** コマンドを設定して Cisco IOS コンフィギュレーション アーカイブの位置とファイル名プレフィックスを指定しておく必要があります。
ステップ 7	**end** 例： `Device(config-archive)# end`	特権 EXEC モードに戻ります。
ステップ 8	**archiveconfig** 例： `Device# archive config`	現在の実行コンフィギュレーションファイルをコンフィギュレーション アーカイブに保存します。 （注） このコマンドを使用する前に、**path** コマンドを設定する必要があります。

コンフィギュレーションの置換またはロールバックの実行（CLI）

保存された Cisco IOS コンフィギュレーション ファイルで現在の実行コンフィギュレーション ファイルを置換するには、次の作業を実行します。

（注） この手順の前に、コンフィギュレーションアーカイブを作成しておく必要があります。詳細については、コンフィギュレーション アーカイブの作成（CLI）を参照してください。次に、現在の実行コンフィギュレーションで問題が生じた場合に、アーカイブしておいたコンフィギュレーションに戻す手順の詳細を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configurereplace** *target-url* [**nolock**] [**list**] [**force**] [**ignore case**] [**revert trigger** ［**error** ］［**timer** *minutes*］｜**time** *minutes*]] 例： `Device# configure replace flash: startup-config time 120`	保存しておいた Cisco IOS コンフィギュレーション ファイルで現在の実行コンフィギュレーション ファイルを置換します。 • *target - url* 引数は、**archive config** コマンドで作成されたコンフィギュレーション ファイルなど、現在の実行コンフィギュレーションと置換する、保存された Cisco IOS コンフィギュレーション ファイルの URL です（Cisco IOS ファイル システムでアクセス可能なもの）。 • **list** キーワードは、コンフィギュレーション置換動作のパスごとに、Cisco IOS ソフトウェア パーサーによって適用されるコマンド ラインのリストを表示します。実行されたパスの総数も表示されます。 • **force** キーワードは、現在の実行コンフィギュレーションから指定した Cisco IOS コンフィギュレーション ファイルへの置換を、確認プロンプトを出さずに実行します。

	コマンドまたはアクション	目的

		• **time***minutes* キーワードおよび引数は、現在の実行コンフィギュレーション ファイルの置換確認のために **configure confirm** コマンドを入力する制限時間（分単位）を指定します。**configure confirm** コマンドが指定の制限時間内に入力されない場合、コンフィギュレーション置換操作は自動的に戻されます（つまり、現在の実行コンフィギュレーションファイルが **configure replace** コマンド入力以前のコンフィギュレーション状態へと回復されます）。
		• **nolock** キーワードは、コンフィギュレーション置換操作中に他のユーザが実行コンフィギュレーションを変更しないように実行コンフィギュレーション ファイルをロックする機能をオフにします。
		• **revert trigger** キーワードは、元のコンフィギュレーションへ戻すトリガーを次の内容から設定します。
		  • **error**：エラー時に元のコンフィギュレーションに戻します。
		  • **timer***minutes*：指定した時間が過ぎると元のコンフィギュレーションに戻します。
		• **ignore case** キーワードで、コンフィギュレーションに確認コマンドの大文字と小文字の区別を無視させることができます。

ステップ 3	**configurerevert** {**now**|**timer** {*minutes*| **idle** *minutes*} } 例： `Device# configure revert now`	（任意）時間指定ロールバックをキャンセルしてロールバックを即時トリガーする、または時間指定ロールバックのパラメータをリセットするには、特権EXECモードで **configure revert** コマンドを使用します。 • **now**：ロールバックをただちにトリガーします。

	コマンドまたはアクション	目的
		• **timer**：コンフィギュレーションを元に戻すタイマーをリセットします。 • 元に戻す時間を分単位で新たに指定するには、*minutes* 引数を **timer** キーワードとともに使用します。 • 保存されたコンフィギュレーションに戻すまでに、操作が行われないアイドル時間を最大どれほど長く許容できるかを設定するには、分単位の時間とともに **idle** キーワードを使用します。
ステップ 4	**configureconfirm** 例： `Device# configure confirm`	（任意）保存しておいた Cisco IOS コンフィギュレーション ファイルの現在の実行コンフィギュレーション ファイルへの置換を確認します。 （注） このコマンドは、**time** *seconds* キーワードと **configure replace** コマンドの引数が指定されているときのみ使用します。
ステップ 5	**exit** 例： `Device# exit`	ユーザ EXEC モードに戻ります。

機能のモニタリングおよびトラブルシューティング（CLI）

コンフィギュレーションの置換とロールバック機能をモニタおよびトラブルシューティングするには、この手順を実行します。

手順

ステップ 1 **enable**

このコマンドを使用して、特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

例：

```
Device> enable
Device#
```

ステップ 2 showarchive

Cisco IOS コンフィギュレーション アーカイブに保存されているファイルに関する情報を表示するには、次のコマンドを使用します。

例：

```
Device# show archive
There are currently 1 archive configurations saved.
The next archive file will be named flash:myconfiguration-2
 Archive #  Name
   0
   1       flash:myconfiguration-1 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10
   11
   12
   13
   14
```

次に、実行コンフィギュレーションのアーカイブ ファイルをいくつか保存した状態で**showarchive** コマンドを使用した場合の出力例を示します。この例では、保存されるアーカイブ ファイルの最大数が 3 に設定されています。

例：

```
Device# show archive
There are currently 3 archive configurations saved.
The next archive file will be named flash:myconfiguration-8
 Archive #  Name
   0
   1       :Deleted
   2       :Deleted
   3       :Deleted
   4       :Deleted
   5       flash:myconfiguration-5
   6       flash:myconfiguration-6
   7       flash:myconfiguration-7 <- Most Recent
   8
   9
   10
   11
   12
   13
   14
```

ステップ 3 debugarchiveversioning

このコマンドを使用して、Cisco IOS コンフィギュレーション アーカイブのアクティビティのデバッグを有効にして、コンフィギュレーションの置換とロールバックをモニタおよびトラブルシューティングします。

例：

```
Device# debug archive versioning
Jan  9 06:46:28.419:backup_running_config
Jan  9 06:46:28.419:Current = 7
Jan  9 06:46:28.443:Writing backup file flash:myconfiguration-7
Jan  9 06:46:29.547: backup worked
```

ステップ 4 debugarchiveconfigtimestamp

このコマンドを使用して、コンフィギュレーション置換操作の各必須段階の処理時間、および操作中のコンフィギュレーション ファイルのサイズのデバッグをイネーブルにします。

例：

```
Device# debug archive config timestamp
Device# configure replace flash:myconfiguration force
Timing Debug Statistics for IOS Config Replace operation:
       Time to read file usbflash0:sample_2.cfg = 0 msec (0 sec)
       Number of lines read:55
       Size of file        :1054
Starting Pass 1
       Time to read file system:running-config = 0 msec (0 sec)
       Number of lines read:93
       Size of file        :2539
       Time taken for positive rollback pass = 320 msec (0 sec)
       Time taken for negative rollback pass = 0 msec (0 sec)
       Time taken for negative incremental diffs pass = 59 msec (0 sec)
       Time taken by PI to apply changes = 0 msec (0 sec)
       Time taken for Pass 1 = 380 msec (0 sec)
Starting Pass 2
       Time to read file system:running-config = 0 msec (0 sec)
       Number of lines read:55
       Size of file        :1054
       Time taken for positive rollback pass = 0 msec (0 sec)
       Time taken for negative rollback pass = 0 msec (0 sec)
       Time taken for Pass 2 = 0 msec (0 sec)
Total number of passes:1
Rollback Done
```

ステップ 5 exit

このコマンドを使用して、ユーザ EXEC モードに戻ります。

例：

```
Device# exit
Device>
```

コンフィギュレーションの置換とロールバックの設定例

コンフィギュレーション アーカイブの作成

次の例は、Cisco IOS コンフィギュレーション アーカイブの初期設定を実行する方法を示しています。この例では、flash:myconfiguration がコンフィギュレーション アーカイブの保存位置およびファイル名のプレフィックスとして設定され、保存するアーカイブ ファイルが最大 10 個に設定されます。

```
configure terminal
!
archive
 path flash:myconfiguration
 maximum 10
end
```

現在の実行コンフィギュレーションを保存された Cisco IOS コンフィギュレーション ファイルで置換

次の例では、flash:myconfiguration という名前で保存された Cisco IOS コンフィギュレーション ファイルで現在の実行コンフィギュレーションを置換する方法を示します。**configure replace** コマンドでは、確認プロンプトでインタラクティブに操作を進めます。

```
Device# configure replace flash:myconfiguration
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
```

次の例では、コンフィギュレーション置換操作中に適用されるコマンドラインを表示するために、**list** キーワードを指定しています。

```
Device# configure replace flash:myconfiguration list
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
!Pass 1
!List of Commands:
no snmp-server community public ro
snmp-server community mystring ro

end
Total number of passes: 1
Rollback Done
```

スタートアップ コンフィギュレーション ファイルへの復帰

次の例に、**configure replace** コマンドを使用して Cisco IOS スタートアップ コンフィギュレーション ファイルへ復帰する方法を示します。この例は、オプションの **force** キーワードを使用して、インタラクティブ ユーザ プロンプトをオーバーライドする方法を示しています:

```
Device# configure replace flash:startup-config force
Total number of passes: 1
Rollback Done
```

configure confirm コマンドを使用したコンフィギュレーション置換操作の実行

次に、**configure replace** コマンドを **time** *minutes* キーワードおよび引数と共に使用する例を示します。現在実行中のコンフィギュレーション ファイルの置換を実行するには、指定の制限時間内に **configure confirm** コマンドを入力する必要があります。**configure confirm** コマンドが指定の制限時間内に入力されない場合、コンフィギュレーション置換操作は自動的に戻されます（つまり、現在実行中のコンフィギュレーション ファイルが **configure replace** コマンド入力以前のコンフィギュレーション状態へと回復されます）。

```
Device# configure replace flash:startup-config time 120
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
Device# configure confirm
```

次に、**configure revert** コマンドを **timer** キーワードとともに使用する例を示します。時間指定ロールバックをキャンセルしてロールバックを即時トリガーする、または時間指定ロールバックのパラメータをリセットするには、**configure revert** コマンドを入力する必要があります。

```
Device# configure revert timer 100
```

コンフィギュレーション ロールバック操作の実行

次の例は、現在実行中のコンフィギュレーションへの変更を行い、その変更をロールバックする方法を示しています。コンフィギュレーション ロールバック操作の一部として、ファイルに変更を加える前に現在の実行コンフィギュレーションを保存する必要があります。この例では、現在実行中のコンフィギュレーションの保存に **archive config** コマンドが使用されています。**configure replace** コマンドで生成された出力は、ロールバック操作を完了するために 1 つのパスのみが実行されたことを示します。

（注） **archive config** コマンドを使用する前に、**path** コマンドで Cisco IOS コンフィギュレーション アーカイブのファイルの位置とファイル名のプレフィックスを指定する必要があります。

次のように、設定アーカイブの現在実行中のコンフィギュレーションを保存します。

```
archive config
```

それから、次の例に示すようにコンフィギュレーションの変更を入力します。

```
configure terminal
!
user netops2 password rain
user netops3 password snow
exit
```

実行コンフィギュレーション ファイルに変更を加えた後、それらの変更をロールバックさせて、変更前のコンフィギュレーションに戻したくなったとします。**show archive** コマンドは、交換ファイルとして使用される設定のバージョンを確認するために使用されます。次の例に示すように、**configure replace** コマンドは交換コンフィギュレーション ファイルへ戻すために使用されます。

```
Device# show archive
There are currently 1 archive configurations saved.
The next archive file will be named flash:myconfiguration-2
 Archive #  Name
   0
   1       flash:myconfiguration-1 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10
Device# configure replace flash:myconfiguration-1
Total number of passes: 1
Rollback Done
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
設定ロック	『*Exclusive Configuration Change Access and Access Session Locking*』

関連項目	マニュアル タイトル
コンフィギュレーション ファイルを管理するためのコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
コンフィギュレーション ファイルの管理についての情報	コンフィギュレーション ファイルの管理

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準

標準	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規RFCまたは改訂RFCはありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 146 章

フラッシュ ファイル システムの操作

- フラッシュ ファイル システムについて （3111 ページ）
- 使用可能なファイル システムの表示 （3112 ページ）
- デフォルト ファイル システムの設定 （3114 ページ）
- ファイル システムのファイルに関する情報の表示 （3115 ページ）
- ディレクトリの変更および作業ディレクトリの表示（CLI） （3115 ページ）
- ディレクトリの作成（CLI） （3116 ページ）
- ファイルのコピー （3117 ページ）
- ファイルの作成、表示および抽出（CLI） （3120 ページ）
- その他の参考資料 （3122 ページ）

フラッシュ ファイル システムについて

フラッシュ ファイル システムは、ファイルを格納できる単一のフラッシュ デバイスです。ソフトウェア バンドルおよびコンフィギュレーション ファイルの管理に役立つ複数のコマンドも備えています。デバイスのデフォルトのフラッシュ ファイル システムは flash: です。

アクティブなデバイスまたは任意のスタック メンバから参照できる flash: は、ローカル フラッシュ デバイスを指します。これは、ファイル システムが参照されているのと同じデバイスに接続されているデバイスです。デバイス スタックでは、さまざまなスタック メンバからの各フラッシュ デバイスを、アクティブなデバイスから参照できます。これらのフラッシュ ファイル システムの名前には、対応するデバイス メンバ番号が含まれています。たとえば、アクティブなデバイスから参照できる flash-3: は、スタック メンバ 3 にある flash: と同じファイル システムを指します。デバイス スタックにあるフラッシュ ファイル システムを含むすべてのファイル システムのリストを表示するには、**show file systems** 特権 EXEC コマンドを使用します。

スイッチ スタックでは、一度に 1 人のユーザのみが、ソフトウェア のバンドルおよび設定ファイルを管理できます。

使用可能なファイル システムの表示

デバイス で使用可能なファイル システムを表示するには、**show file systems** 特権 EXEC コマンドを使用します（次のスタンドアロン デバイス の例を参照）。

```
Device# show file systems
File Systems:
     Size(b)     Free(b)       Type    Flags   Prefixes
*   15998976     5135872      flash     rw     flash:
           -           -     opaque     rw     bs:
           -           -     opaque     rw     vb:
      524288      520138      nvram     rw     nvram:
           -           -    network     rw     tftp:
           -           -     opaque     rw     null:
           -           -     opaque     rw     system:
           -           -     opaque     ro     xmodem:
           -           -     opaque     ro     ymodem:
```

次の例では、デバイス スタックを示します。この例では、アクティブな デバイス がスタック メンバ 1 です。スタック メンバ 2 のファイル システムはフラッシュ 2 として表示されます。スタック メンバ 3 のファイル システムはフラッシュ 3 として表示されます。メンバ数 9 のスタックの場合、スタック メンバ 9 のファイルは、フラッシュ 9 として同様にそれぞれ表示されます。また、この例では、次のように、crashinfo ディレクトリと、アクティブな デバイス に接続された USB フラッシュ ドライブも示します。

```
Device# show file systems
File Systems:
      Size(b)        Free(b)      Type   Flags   Prefixes
     145898496      5479424       disk     rw    crashinfo:crashinfo-1:
     248512512      85983232      disk     rw    crashinfo-2:stby-crashinfo:
     146014208      17301504      disk     rw    crashinfo-3:
     146014208             0      disk     rw    crashinfo-4:
     146014208       1572864      disk     rw    crashinfo-5:
     248512512      30932992      disk     rw    crashinfo-6:
     146014208       6291456      disk     rw    crashinfo-7:
     146276352      15728640      disk     rw    crashinfo-8:
     146276352      73400320      disk     rw    crashinfo-9:
*    741621760     481730560      disk     rw    flash:flash-1:
    1622147072    1360527360      disk     rw    flash-2:stby-flash:
     729546752     469762048      disk     rw    flash-3:
     729546752     469762048      disk     rw    flash-4:
     729546752     469762048      disk     rw    flash-5:
    1622147072    1340604416      disk     rw    flash-6:
     729546752     469762048      disk     rw    flash-7:
    1749549056    1487929344      disk     rw    flash-8:
    1749549056    1487929344      disk     rw    flash-9:
             0             0      disk     rw    unix:
             -             -      disk     rw    usbflash0:usbflash0-1:
             -             -      disk     rw    usbflash0-2: stby-usbflash0:
             -             -      disk     rw    usbflash0-3:
             -             -      disk     rw    usbflash0-4:
             -             -      disk     rw    usbflash0-5:
             -             -      disk     rw    usbflash0-6:
             -             -      disk     rw    usbflash0-7:
             -             -      disk     rw    usbflash0-8:
             -             -      disk     rw    usbflash0-9:
```

```
       0            0      disk     ro    webui:
       -            -    opaque     rw    system:
       -            -    opaque     rw    tmpsys:
 2097152      2055643     nvram     rw    stby-nvram:
       -            -     nvram     rw    stby-rcsf:
       -            -    opaque     rw    null:
       -            -    opaque     ro    tar:
       -            -   network     rw    tftp:
 2097152      2055643     nvram     rw    nvram:
       -            -    opaque     wo    syslog:
       -            -   network     rw    rcp:
       -            -   network     rw    http:
       -            -   network     rw    ftp:
       -            -   network     rw    scp:
       -            -   network     rw    https:
       -            -    opaque     ro    cns:
       -            -    opaque     rw    revrcsf:
```

表 ***206 : show file systems*** のフィールドの説明

フィールド	値
Size(b)	ファイル システムのメモリ サイズ（バイト単位）です。
Free(b)	ファイル システムの空きメモリ サイズ（バイト単位）です。
タイプ	ファイル システムのタイプです。 **disk**：ファイル システムは、フラッシュ メモリ デバイス、USB フラッシュ、crashinfo ファイル用です。 **network**：ファイル システムは、FTP サーバや HTTP サーバなどのネットワーク デバイス用です。 **nvram**：ファイル システムは NVRAM（不揮発性 RAM）デバイス用です。 **opaque**：ファイル システムは、ローカルに生成された pseudo ファイル システム（system など）、またはダウンロード インターフェイス（brimux など）です。 **unknown**：ファイル システムのタイプは不明です。
Flags	ファイル システムの権限です。 **ro**：読み取り専用です。 **rw**：読み取りおよび書き込みです。 **wo**：書き込み専用です。

フィールド	値
Prefixes	ファイル システムのエイリアスです。 **crashinfo**：crashinfo ファイルです。 **flash:** ：フラッシュ ファイル システムです。 **ftp**：FTP サーバです。 **http**：HTTP サーバです。 **https**：セキュア HTTP サーバです。 **nvram:** ：NVRAM です。 **null:** ：コピーのヌル宛先です。リモート ファイルをヌルへコピーして、サイズを判別できます。 **rcp**：Remote Copy Protocol（RCP）サーバです。 **scp**：Session Control Protocol（SCP）サーバです。 **system:** ：実行コンフィギュレーションを含むシステム メモリが格納されています。 **tftp:** ：TFTP ネットワーク サーバです。 **usbflash0**：USB フラッシュ メモリです。 **xmodem:** ：XMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。 **ymodem:** ：YMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。

デフォルト ファイル システムの設定

デフォルトのファイル システムとして使用されるファイル システムまたはディレクトリを指定するには、**cd** *filesystem:* 特権 EXEC コマンドを使用します。デフォルト ファイル システムを設定すると、関連するコマンドを実行するときに *filesystem:* 引数を省略できます。たとえば、オプションの *filesystem:* 引数を持つすべての特権 EXEC コマンドでは、**cd** コマンドで指定されたファイル システムが使用されます。

デフォルトでは、デフォルト ファイル システムは *flash:* です。

cd コマンドで指定された現在のデフォルトのファイル システムを表示するには、**pwd** 特権 EXEC コマンドを使用します。

ファイル システムのファイルに関する情報の表示

ファイルシステムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイル システムに同じ名前のコンフィギュレーションファイルが格納されていないことを確認できます。同様に、フラッシュ コンフィギュレーション ファイルを別の場所にコピーする前に、ファイル名を確認して、その名前を別のコマンドで使用できます。ファイルシステムのファイルに関する情報を表示するには、次の表に記載する特権 EXEC コマンドのいずれかを使用します。

表 *207 :* ファイルに関する情報を表示するためのコマンド

コマンド	説明
dir [/all] [*filesystem:filename*]	ファイル システムのファイル リストを表示します。
show file systems	ファイル システムのファイルごとの詳細を表示します。
show file information *file-url*	特定のファイルに関する情報を表示します。
show file descriptors	開いているファイルの記述子のリストを表示します。ファイル記述子は開いているファイルの内部表現です。このコマンドを使用して、別のユーザによってファイルが開かれているかどうかを調べることができます。

たとえば、ファイル システムのすべてのファイルのリストを表示するには、次のように **dir** 特権 EXEC コマンドを使用します。

```
デバイス# dir flash:
Directory of flash:/
7386  -rwx     2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
7378  drwx        4096 Jan 23 2013 09:35:11 +00:00 mnt
7385  -rw-   221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
7389  -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
712413184 bytes total (445063168 bytes free)
デバイス#
```

ディレクトリの変更および作業ディレクトリの表示（CLI）

ディレクトリを変更し、作業ディレクトリを表示するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**dir** *filesystem:* 例： `Device# dir flash:`	指定されたファイル システムのディレクトリを表示します。 *filesystem:* には、システム ボードのフラッシュ デバイスの flash: を使用します。 スタックのデバイスメンバのフラッシュパーティションにアクセスするには、flash-*n* を使用します。*n* は、スタック メンバ番号を表します。例えば、flash-4。
ステップ 3	**cd** *directory_name* 例： `Device# cd new_configs`	指定されたディレクトリへ移動します。 コマンド例では、*new_configs* という名前のディレクトリに移動する方法を示します。
ステップ 4	**pwd** 例： `Device# pwd`	作業ディレクトリを表示します。
ステップ 5	**cd** 例： `Device# cd`	デフォルトディレクトリに移動します。

ディレクトリの作成（CLI）

特権 EXEC モードを開始して、ディレクトリを作成するには次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**dir** *filesystem:* 例：	指定されたファイル システムのディレクトリを表示します。

	コマンドまたはアクション	目的
	`Device# dir flash:`	*filesystem:* には、システム ボードのフラッシュ デバイスの flash: を使用します。
ステップ 2	**mkdir** *directory_name* 例： `Device# mkdir new_configs`	新しいディレクトリを作成します。スラッシュ (/) 間に指定できるディレクトリ名は最大 45 文字で、大文字と小文字の区別があります。ディレクトリ名には制御文字、スペース、スラッシュ、引用符、セミコロン、またはコロンは使用できません。
ステップ 3	**dir** *filesystem:* 例： `Device# dir flash:`	入力を確認します。

ディレクトリの削除

ディレクトリを、その内部のすべてのファイルおよびサブディレクトリとともに削除するには、delete /force /recursive**delete /force /recursive**filesystem:/file-url 特権 EXEC コマンドを使用します。

名前で指定されたディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。

filesystem でシステム ボードのフラッシュ デバイスを指定する場合は、**flash:** を使用します。*file-url* には、削除するディレクトリの名前を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

⚠

注意 ディレクトリが削除された場合、その内容は回復できません。

ファイルのコピー

送信元から宛先にファイルをコピーするには、**copy** *source-url destination-url* 特権 EXEC コマンドを使用します。送信元および宛先の URL には、**running-config** および **startup-config** キーワード ショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドを実行すると、現在の実行コンフィギュレーション ファイルがフラッシュ メモリの NVRAM セクションに保存され、システム初期化中のコンフィギュレーションとして使用されます。

XMODEM または YMODEM プロトコルを使用するネットワーク マシンのファイルに対する送信元として特殊なファイル システム（**xmodem:**、**ymodem:**）を指定し、そこからコピーすることもできます。

ネットワーク ファイル システムの URL には、ftp: 、rcp: 、tftp などがあり、構文は次のとおりです。

- FTP：ftp:[[//username [:password]@location]/directory]/filename
- RCP：rcp:[[//username@location]/directory]/filename
- TFTP：tftp:[[//location]/directory]/filename

ローカルにある書き込み可能なファイル システムには flash: などがあります。

送信元および宛先の組み合わせによっては、無効な場合があります。特に、次に示す組み合わせの場合は、コピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- デバイスから同じ名前のデバイスへ（たとえば、**copy flash: flash:** コマンドは無効）

スタック内のDeviceから同じスタックの別のDeviceにファイルをコピーする

スタック内のあるデバイスから同じスタック内の別のデバイスにファイルをコピーするには、**flash-X:** 表記を使用します。**X** はデバイス番号です。

スタック内のすべてのデバイスを表示するには、9 メンバーデバイス スタックの例のように、特権 EXEC モードで **show switch** コマンドを使用します。

```
Device# show switch
Switch/Stack Mac Address : 0006.f6b9.b580 - Local Mac Address Mac persistency wait time:
 Indefinite
                                            H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Active   0006.f6b9.b580     15     P3B     Ready
 2       Standby  0006.f6ba.0c80     14     P3B     Ready
 3       Member   0006.f6ba.3300     7      P3B     Ready
 4       Member   0006.f6b9.df80     6      P3B     Ready
 5       Member   0006.f6ba.3880     13     P1A     Ready
 6       Member   1ce6.c7b6.ef00     4      PP      Ready
 7       Member   2037.06ce.2580     3      P2A     Ready
 8       Member   2037.0653.7e00     2      P5A     Ready
 9       Member   2037.0653.9280     1      P5B     Ready
```

特定のデバイスのコピー可能なすべてのファイル システムを表示するには、次に示す 5 メンバー スタックの例のように、**copy** コマンドを使用します。

```
Device# copy flash: ?
```

```
  crashinfo-1:     Copy to crashinfo-1: file system
  crashinfo-2:     Copy to crashinfo-2: file system
  crashinfo-3:     Copy to crashinfo-3: file system
  crashinfo-4:     Copy to crashinfo-4: file system
  crashinfo-5:     Copy to crashinfo-5: file system
  crashinfo:       Copy to crashinfo: file system
  flash-1:         Copy to flash-1: file system
  flash-2:         Copy to flash-2: file system
  flash-3:         Copy to flash-3: file system
  flash-4:         Copy to flash-4: file system
  flash-5:         Copy to flash-5: file system
  flash:           Copy to flash: file system
  ftp:             Copy to ftp: file system
  http:            Copy to http: file system
  https:           Copy to https: file system
  null:            Copy to null: file system
  nvram:           Copy to nvram: file system
  rcp:             Copy to rcp: file system
  revrcsf:         Copy to revrcsf: file system
  running-config   Update (merge with) current system configuration
  scp:             Copy to scp: file system
  startup-config   Copy to startup configuration
  stby-crashinfo:  Copy to stby-crashinfo: file system
  stby-flash:      Copy to stby-flash: file system
  stby-nvram:      Copy to stby-nvram: file system
  stby-rcsf:       Copy to stby-rcsf: file system
  stby-usbflash0:  Copy to stby-usbflash0: file system
  syslog:          Copy to syslog: file system
  system:          Copy to system: file system
  tftp:            Copy to tftp: file system
  tmpsys:          Copy to tmpsys: file system
  usbflash0-1:     Copy to usbflash0-1: file system
  usbflash0-2:     Copy to usbflash0-2: file system
  usbflash0-3:     Copy to usbflash0-3: file system
  usbflash0-4:     Copy to usbflash0-4: file system
  usbflash0-5:     Copy to usbflash0-5: file system
  usbflash0:       Copy to usbflash0: file system

Device#
```

次の例では、デバイス 2 のフラッシュ パーティションに保存されているコンフィギュレーション ファイルをデバイス 4 のフラッシュ パーティションにコピーする方法を示しています。デバイス 2 とデバイス 4 が同じスタック内にあるとします。

```
Device# copy flash-2:config.txt flash-4:config.txt
```

ファイルの削除

フラッシュ メモリ デバイスのファイルが不要になった場合は、そのファイルを永久に削除できます。指定されたフラッシュ デバイスからファイルまたはディレクトリを削除するには、**delete** [**/force**] [**/recursive**] [*filesystem:*]*/file-url* 特権 EXEC コマンドを使用します。

ディレクトリを、その内部のすべてのサブディレクトリやファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**/force** キーワードおよび

/recursive キーワードを使用して、**archive download-sw** コマンドを使用してインストールされ、不要になった古いソフトウェア イメージを削除します。

filesystem: オプションを省略すると、デバイスは **cd** コマンドで指定したデフォルトのデバイスを使用します。*file-url* には、削除するファイルのパス（ディレクトリ）および名前を指定します。

ファイルを削除しようとすると、削除の確認を求めるプロンプトが表示されます。

注意 ファイルが削除された場合、その内容は回復できません。

ここでは、デフォルトのフラッシュ メモリ デバイスからファイル *myconfig* を削除する例を示します。

```
Device# delete myconfig
```

ファイルの作成、表示および抽出（CLI）

ファイルを作成してそこにファイルを書き込んだり、ファイル内のファイルをリスト表示したり、ファイルからファイルを抽出したりできます（次の項を参照）。

ファイルの作成、内容の表示、およびファイルの抽出を行うには、特権 EXEC コマンドで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**archive tar /create** *destination-url* **flash:** */file-url* **例：** `デバイス# archive tar /create tftp:172.20.10.30/saved. flash:/new-configs`	ファイルを作成し、そこにファイルを追加します。 destination-url には、ローカルまたはネットワーク ファイル システムの宛先 URL のエイリアス、および作成するファイルの名前を指定します。 • ローカル フラッシュ ファイル システム構文 **flash:** • FTP 構文 **ftp**:[[//*username*[:*password*]@*location*]/*directory*]/*filename*. • RCP 構文 **rcp**:[[//*username*@*location*]/*directory*]/*filename*. • TFTP 構文 **tftp**:[[//*location*]/*directory*]/*filename*.

	コマンドまたはアクション	目的
		flash:/*file-url* には、ローカル フラッシュ ファイル システム上の、新しいファイルが作成される場所を指定します。送信元ディレクトリ内に格納されている任意のファイルまたはディレクトリの一覧を指定して、新しいファイルに追加することもできます。何も指定しないと、このレベルにおけるすべてのファイルおよびディレクトリが、新規に作成されたファイルに書き込まれます。
ステップ 2	**archive tar /table** *source-url* 例： `デバイス# archive tar /table flash: /new_configs`	ファイルの内容を表示します。 *source-url* には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。*-filename.* は、表示するファイルです。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システム構文 **flash:** • FTP 構文 **ftp**:[[//*username*[:*password*]@*location*]/*directory*]/*-filename*. • RCP 構文 **rcp**:[[//*username@location*]/*directory*]/*-filename*. • TFTP 構文 **tftp**:[[//*location*]/*directory*]/*-filename*. ファイルのあとにファイルまたはディレクトリのリストを指定して、ファイルの表示を制限することもできます。指定したファイルだけが表示されます。何も指定しないと、すべてのファイルおよびディレクトリが表示されます。
ステップ 3	**archive tar /xtract** *source-url* **flash:**/*file-url* [*dir/file...*] 例： `デバイス# archive tar /xtract tftp:/172.20.10.30/saved. flash:/new-configs`	ファイルをフラッシュ ファイル システム上のディレクトリに抽出します。 *source-url* には、ローカル ファイル システムの送信元 URL のエイリアスを指定します。*-filename.* は、ファイルの抽出元のファイルです。次のオプションがサポートされています。

	コマンドまたはアクション	目的
		• ローカル フラッシュ ファイル システム構文 **flash:** • FTP 構文 **ftp**:[[//*username*[:*password*]@*location*]/*directory*]/*-filename*. • RCP 構文 **rcp**:[[//*username*@*location*]/*directory*]/*-filename*. • TFTP 構文 **tftp**:[[//*location*]/*directory*]/*-filename*. **flash:**/*file-url* [*dir/file...*] には、ファイルの抽出元にするローカル フラッシュ ファイル システム上の場所を指定します。抽出対象のファイル内のファイルまたはディレクトリのリストを指定するには、*dir/file...* オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。
ステップ 4	**more** [**/ascii** | **/binary** | **/ebcdic**] /*file-url* **例：** `デバイス# more flash:/new-configs`	リモート ファイル システム上のファイルを含めて、読み取り可能なファイルの内容を表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
flash: ファイル システムの管理コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準

標準	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規RFCまたは改訂RFCはありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 147 章

スイッチ ソフトウェアのアップグレード

- スイッチ ソフトウェアのアップグレード （3125 ページ）

スイッチ ソフトウェアのアップグレード

スイッチ ソフトウェアを Cisco IOS XE Release 3.x.x から Cisco IOS XE Denali 16.1.x にアップグレードする方法については、『Release Notes for Cisco Catalyst 3850 Series Switch, Cisco IOS XE Denali 16.1.x』を参照してください。

第 148 章

条件付きデバッグとラジオアクティブ トレース

- 機能情報の確認 （3127 ページ）
- 条件付きデバッグの概要 （3128 ページ）
- ラジオアクティブ トレースの概要 （3128 ページ）
- 条件付きデバッグおよび放射線トレース （3129 ページ）
- トレースファイルの場所 （3129 ページ）
- 条件付きデバッグの設定 （3129 ページ）
- L2 マルチキャストの放射線トレース （3132 ページ）
- トレース ファイルの推奨ワークフロー （3132 ページ）
- ボックス外へのトレース ファイルのコピー （3133 ページ）
- 条件付きデバッグの設定例 （3133 ページ）
- 条件付きデバッグのモニタリング （3134 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

条件付きデバッグの概要

条件付きデバッグ機能によって、定義した条件に基づき、特定の機能のデバッグおよびロギングを選択して有効にすることができます。この機能は、多くの機能がサポートされているシステムで有用です。

（注） Cisco IOS XE Denali 16.1.1 では、コントロール プレーン トレースのみがサポートされます。

条件付きデバッグでは、多数の機能が導入されていて大規模に稼働しているネットワークにおけるきめ細かなデバッグが可能です。これにより、システム内の細かなインスタンスに対しても、詳細なデバッグを実行できます。これは、何千ものセッションのうちの特定のセッションのみをデバッグするような場合に、非常に有用です。条件は複数指定することもできます。

条件とは、機能またはアイデンティティをいいます。アイデンティティは、インターフェイス、IP アドレス、MAC アドレスなどです。

（注） Cisco IOS XE Denali 16.1.1 では、MAC アドレスが唯一サポートされる条件です。これ以外の機能のサポートは、今後のリリースで導入されます。

これは、処理する機能オブジェクトを区別せずに出力を生成する、一般的なデバッグ コマンドとは対照的です。一般的なデバッグ コマンドは、多数のシステム リソースを消費し、システム パフォーマンスに影響します。

ラジオアクティブ トレースの概要

ラジオアクティブ トレースにより、冗長性のレベルを高めた状態で、システムの全体にわたって目的とする動作を連鎖的に実行できます。また、複数のスレッド、プロセス、および関数呼び出しにわたって、デバッグ情報を条件に基づいて（DEBUG レベルまで、または指定のレベルまで）出力する方法を提供します。

（注） Cisco IOS XE Denali 16.1.1 では、デフォルトのレベルは **DEBUG** です。ユーザは別のレベルに変更することはできません。これ以外のレベルのサポートは、今後のリリースで導入されます。

条件付きデバッグおよび放射線トレース

条件付きデバッグと組み合わせた放射線トレースによって、条件に関連するすべての実行コンテキストをデバッグする単一のデバッグ CLI を取得できます。これは、ボックス内の機能のさまざまな制御フロー プロセスを認識していなくても行うことができ、これらのプロセスでデバッグを個別に発行する必要もありません。

トレースファイルの場所

デフォルトでは、トレースファイル ログは各プロセスで生成され、**/tmp/rp/trace** または **/tmp/fp/trace** ディレクトリに保存されます。この一時ディレクトリで、トレースログがファイルに書き込まれます。各ファイルは 1 MB サイズです。このディレクトリでは、特定のプロセスのこうしたファイルを、最大 25 件保持できます。**/tmp** ディレクトリのトレースファイルがその 1 MB 制限またはブート時に設定されたサイズに達した場合、ローテーションから外れ、**tracelogs** ディレクトリの **/crashinfo** パーティションの下にあるアーカイブの場所に移動します。

/tmp ディレクトリが 1 つのプロセスで保持するトレースファイルは 1 つのみです。ファイルがそのファイル サイズの制限に達したら、ローテーションから外れ、**/crashinfo/tracelogs** に移動します。アーカイブ ディレクトリに蓄積されるファイルは最大 25 ファイルであり、その後は最も古いものから順に、**/tmp** から新たにローテーションされたファイルに置換されます。

crashinfo ディレクトリ内のトレースファイルは次の形式で配置されます。

1. Process-name_Process-ID_running-counter.timestamp.gz

   例：IOSRP_R0-0.bin_0.14239.20151101234827.gz

2. Process-name_pmanlog_Process-ID_running-counter.timestamp.bin.gz

   例：wcm_pmanlog_R0-0.30360_0.20151028233007.bin.gz

条件付きデバッグの設定

条件付デバッグを設定するには、以下の手順に従います。

-

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**debug platform condition mac** {*mac-address*} 例： `Device# debug platform condition mac bc16.6509.3314`	指定されたMACアドレスの条件付きデバッグを設定します。
ステップ 3	**debug platform condition start** 例： `Device# debug platform condition start`	条件付きデバッグを開始します（上記のいずれかの条件に一致すると放射線トレースを開始します）。

ステップ 4	**show platform condition** または **show debug**
	例：
	`Device# show platform condition`
	`Device# show debug`
		現在設定されている条件を表示します。

ステップ 5	**debug platform condition stop** 例： `Device# debug platform condition stop`	条件付きデバッグを停止します（放射線トレースを停止します）。
ステップ 6	**request platform software trace archive** [**last** {*number*} **days**] [**target** {*crashinfo:* | *flashinfo:*}] 例： `Device# request platform software trace archive last 2 days`	（任意）システムのマージされたトレースファイルの履歴ログを表示します。日数またはロケーションの組み合わせのフィルタ。
ステップ 7	**request platform software trace filter-binary** {*wire* | *wireless*} [**context** {*mac-address*} | **level** | **module**] 例： `Device# request platform software trace filter-binary wireless context bc16.6509.3314`	（任意）指定されたMACアドレスのコンテキストと情報（ネットワークまたはワイヤレス）を照合するには、モジュールをフィルタリングします。これらのログはオフラインで確認できます。 （注） Cisco IOS XE Denali 16.1.1 では、使用可能なすべてのキーワードのうち、サポートされている唯一のキーワードは、ワイヤレスです。これは、プロセス（ios、wcm、fman_rp、fman_fp）からファイルを収集します。

	コマンドまたはアクション	目的
ステップ 8	**show platform software trace [filter-binary | level | message]** 例： `Device# show platform software trace message`	（任意）最新のトレースファイルからマージされたログを表示します。アプリケーションの状態、トレース モジュール名およびトレース レベルをさまざまな組み合わせでフィルタリングします。 • **filter-binary** ：照合するモジュールをフィルタリングします。例えば、ワイヤレス。 • **level** ：トレース レベルを表示します。 • **message** ：トレースメッセージのリングの内容を表示します。 （注） ボックスでは： • Linux シェルだけでなく、IOS のコンソールからも使用できます。 • マージされたログを含むファイルをボックスで生成します。 • ステージング エリアからのみマージされたログを表示します。
ステップ 9	**clear platform condition all** 例： `Device# clear platform condition all`	すべての条件をクリアします。

次のタスク

（注） **request platform software trace filter-binary** および **show platform software trace filter-binary** コマンドは、似たように動作します。唯一の違いは次のとおりです。

- **request platform software trace filter-binary** ：データ ソースとして履歴ログを使用します。
- **show platform software trace filter-binary** ：データ ソースとしてフラッシュの一時ディレクトリを使用します。

（注） **request platform software trace filter-binary wireless** {*mac-address*} コマンドは、3 つのフラッシュ ファイルを生成します。

- *collated_log_<.date..>*
- *mac_log <..date..>*
- *mac_database .. file*

その中でも、*mac_log <..date..>* は、デバッグする MAC 用のメッセージを伝えるため、最も重要なファイルです。**show platform software trace filter-binary** コマンドも同じフラッシュ ファイルを生成し、また、画面に mac_log を出力します。

L2 マルチキャストの放射線トレース

特定のマルチキャスト受信者を特定するには、参加者または受信側クライアントの MAC アドレス、グループのマルチキャスト IP アドレスおよびスヌーピング VLAN を指定します。また、デバッグのトレース レベルを有効にします。デバッグ レベルでは、詳細なトレースとシステムへの高い可視性が提供されます。

debug platform condition feature multicast controlplane mac *client MAC address* **ip** *Group IP address* **vlan** *id* **level** *debug level*

トレース ファイルの推奨ワークフロー

トレース ファイルの推奨ワークフローの概要は次のとおりです。

1. 特定の時間帯のトレースログを要求する場合。

   たとえば 1 日。

   使用するコマンドは、次のとおりです。

   Device#**リクエストプラットフォームソフトウェアトレースアーカイブ過去 1 日間**

2. システムは、/flash: ロケーション内のトレースログの tar ball（.gz ファイル）を生成します。
3. スイッチ外にファイルをコピーします。ファイルをコピーすることによって、オフラインでトレースログが使用できます。ファイルのコピーについての詳細は、次のセクションを参照してください。
4. /flash: location からトレースログファイル（.gz）ファイルを削除します。これにより、他の操作に十分な領域がスイッチに確保されます。

ボックス外へのトレース ファイルのコピー

トレース ファイルの例を以下に示します。

```
Device# dir crashinfo:/tracelogs
Directory of crashinfo:/tracelogs/

50664 -rwx 760 Sep 22 2015 11:12:21 +00:00 plogd_F0-0.bin_0.gz
50603 -rwx 991 Sep 22 2015 11:12:08 +00:00 fed_pmanlog_F0-0.bin_0.9558.20150922111208.gz
50610 -rw- 11 Nov 2 2015 00:15:59 +00:00 timestamp
50611 -rwx 1443 Sep 22 2015 11:11:31 +00:00
auto_upgrade_client_sh_pmanlog_R0-.bin_0.3817.20150922111130.gz
50669 -rwx 589 Sep 30 2015 03:59:04 +00:00 cfgwr-8021_R0-0.bin_0.gz
50612 -rwx 1136 Sep 22 2015 11:11:46 +00:00 reflector_803_R0-0.bin_0.1312.20150922111116.gz
50794 -rwx 4239 Nov 2 2015 00:04:32 +00:00 IOSRP_R0-0.bin_0.14239.20151101234827.gz
50615 -rwx 131072 Nov 2 2015 00:19:59 +00:00 linux_iosd_image_pmanlog_R0-0.bin_0
--More—
```

トレース ファイルは、次に示すさまざまなオプションのいずれかを使用して、コピーできます。

```
Device# copy crashinfo:/tracelogs ?
  crashinfo: Copy to crashinfo: file system
  flash: Copy to flash: file system
  ftp: Copy to ftp: file system
  http: Copy to http: file system
  https: Copy to https: file system
  null: Copy to null: file system
  nvram: Copy to nvram: file system
  rcp: Copy to rcp: file system
  running-config Update (merge with) current system configuration
  scp: Copy to scp: file system
  startup-config Copy to startup configuration
  syslog: Copy to syslog: file system
  system: Copy to system: file system
  tftp: Copy to tftp: file system
  tmpsys: Copy to tmpsys: file system
```

TFTP サーバにコピーするための一般的な構文は次のとおりです。

```
Device# copy source: tftp:
Device# copy crashinfo:/tracelogs/IOSRP_R0-0.bin_0.14239.20151101234827.gz tftp:
Address or name of remote host []? 2.2.2.2
Destination filename [IOSRP_R0-0.bin_0.14239.20151101234827.gz]?
```

（注） tracelogおよび他の目的に使用可能な空き容量があることを確認するために、生成されたレポート/アーカイブ ファイルをスイッチからクリアすることが重要です。

条件付きデバッグの設定例

次に、*show platform condition* コマンドの出力例を示します。

```
Device# show platform condition
Conditional Debug Global State: Stop
Conditions Direction
-----------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
-----------------------|-----------------------|--------------------------------
Device#
```

次に、*show debug* コマンドの出力例を示します。

```
Device# show debug
IOSXE Conditional Debug Configs:
Conditional Debug Global State: Start
Conditions Direction
-----------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
-----------------------|-----------------------|--------------------------------
Packet Infra debugs:
Ip Address Port
-------------------------------------------------------|----------
Device#
```

次に、*debug platform condition stop* コマンドの例を示します。

```
Device# debug platform condition stop
Conditional Debug Global State: Stop
```

条件付きデバッグのモニタリング

以下の表に、条件付きデバッグのモニタに使用できる各種コマンドを示します。

コマンド	目的
show platform condition	現在設定されている条件を表示します。
show debug	現在設定されているデバッグ条件を表示します。
show platform software trace filter-binary	最新のトレース ファイルからマージされたログを表示します。
request platform software trace filter-binary	システムにマージされたトレース ファイルの履歴ログを表示します。

第 149 章

ソフトウェア設定のトラブルシューティング

この章では、スイッチが稼働する Cisco IOS ソフトウェアに関連する問題を特定し、解決する方法について説明します。問題の性質に応じて、コマンドラインインターフェイス（CLI）、デバイス マネージャ、または Network Assistant を使用して、問題を特定し解決できます。

LED の説明など、トラブルシューティングの詳細については、ハードウェアインストレーション ガイドを参照してください。

- 機能情報の確認 （3135 ページ）
- ソフトウェア設定のトラブルシューティングに関する情報 （3136 ページ）
- ソフトウェア設定のトラブルシューティング方法 （3146 ページ）
- ソフトウェア設定のトラブルシューティングの確認 （3159 ページ）
- ソフトウェア設定のトラブルシューティングのシナリオ （3162 ページ）
- ソフトウェアのトラブルシューティングの設定例 （3166 ページ）
- ソフトウェア設定のトラブルシューティングに関する追加情報 （3169 ページ）
- ソフトウェア設定のトラブルシューティングの機能履歴と情報 （3170 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ソフトウェア設定のトラブルシューティングに関する情報

スイッチのソフトウェア障害

スイッチ ソフトウェアがアップグレード中に破損する原因として、誤ったファイルがスイッチにダウンロードされた場合やイメージファイルが削除された場合があります。いずれの場合にも、スイッチは電源投入時自己診断テスト（POST）に失敗し、接続できなくなります。

関連トピック

ソフトウェア障害からの回復 （3146 ページ）

のパスワードを紛失したか忘れた場合 デバイス

デバイスのデフォルト設定では、デバイスに物理的にアクセスしているエンドエンド ユーザは、スイッチの電源投入中に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復できます。ここで紹介する回復手順を実行するには、デバイスに物理的にアクセスする必要があります。

（注） これらのデバイスでは、システム管理者は、デフォルト設定に戻すことに同意した場合に限り、エンド ユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできます。パスワード回復がディセーブルになっている場合に、エンドユーザがパスワードをリセットしようとすると、ステータスメッセージで回復プロセスの間はデフォルトの設定に戻すように指示されます。

関連トピック

パスワードを忘れた場合の回復 （3148 ページ）

Power over Ethernet（PoE）ポート

Power over Ethernet（PoE）スイッチ ポートでは、回路に電力が供給されていないことをスイッチが検知した場合、接続している次のデバイスに電力が自動的に供給されます。

- シスコ先行標準受電デバイス（Cisco IP Phone や Cisco Aironet アクセス ポイントなど）
- IEEE 802.3af 準拠の受電装置
- IEEE 802.3at 準拠の受電装置

受電デバイスが PoE スイッチ ポートおよび AC 電源に接続されている場合、冗長電力として利用できます。受電装置が PoE ポートにだけ接続されている場合、受電装置には冗長電力は供給されません。

受電デバイスを検出すると、スイッチは受電デバイスの電力要件を判断し、受電デバイスへの電力供給を許可または拒否します。また、スイッチは消費電力をモニタリングおよびポリシングすることで、装置の電力の消費をリアルタイムに検知できます。

詳細については、『*Interface and Hardware Component Configuration Guide*（*Catalyst 3850 Switches*）』の「Configuring Failover」の章を参照してください。

関連トピック

Power over Ethernet（PoE）に関するトラブルシューティングのシナリオ （3162 ページ）

電力消失によるポートの障害

PoE デバイス ポートに接続され、AC 電源から電力が供給されている受電デバイス（Cisco IP Phone 7910 など）に AC 電源から電力が供給されない場合、そのデバイスは errdisable ステートになることがあります。error-disabled ステートから回復するには、**shutdown** インターフェイス コンフィギュレーション コマンドを入力してから、**no shutdown** インターフェイス コマンドを入力します。デバイスで自動回復を設定し、error-disabled ステートから回復することもできます。

デバイスの場合、**errdisable recovery cause loopback** および **errdisable recovery interval** *seconds* グローバル コンフィギュレーション コマンドは、指定した期間が経過したあと自動的にインターフェイスを error-disabled ステートから復帰させます。

不正リンク アップによるポート障害

シスコ受電デバイスをポートに接続し、**power inline never** インターフェイス コンフィギュレーション コマンドを使用してポートを設定した場合は、不正リンク アップが発生し、ポートが error-disabled ステートになることがあります。ポートを error-disabled ステートから回復するには、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

power inline never コマンドで設定したポートにシスコ受電デバイスを接続しないでください。

ping

デバイスは IP の ping をサポートしており、これを使ってリモート ホストへの接続をテストできます。ping はアドレスにエコー要求パケットを送信し、応答を待ちます。ping は次のいずれかの応答を返します。

- 正常な応答：正常な応答（*hostname* が存在する）は、ネットワーク トラフィックにもよりますが、1 ～ 10 秒以内で発生します。
- 宛先の応答なし：ホストが応答しない場合、*no-answer* メッセージが返されます。
- 不明なホスト：ホストが存在しない場合、*unknown host* メッセージが返されます。

- 宛先到達不能：デフォルトゲートウェイが指定されたネットワークに到達できない場合、*destination-unreachable* メッセージが返されます。
- ネットワークまたはホストへの到達不能：ルートテーブルにホストまたはネットワークのエントリがない場合、*network or host unreachable* メッセージが返されます。

関連トピック

ping の実行 （3155 ページ）
例：IP ホストの ping （3166 ページ）

レイヤ 2 Traceroute

レイヤ 2 traceroute 機能により、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを識別できます。レイヤ 2 traceroute は、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。transroute は、パス内にあるデバイスの MAC アドレス テーブルを使用してパスを識別します。デバイスがパス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、デバイスはレイヤ 2 trace クエリーを送信し続け、タイムアウトにします。

デバイスは、送信元デバイスから宛先デバイスへのパスのみを識別できます。パケットが通過する、送信元ホストから送信元デバイスまで、または宛先デバイスから宛先ホストまでのパスは識別できません。

レイヤ 2 の traceroute のガイドライン

- ネットワーク内のすべてのデバイスで、Cisco Discovery Protocol（CDP）をイネーブルにする必要があります。レイヤ 2 traceroute が適切に動作するために、CDP をディセーブルにしないでください。

  物理パス内のデバイスが CDP に対して透過的な場合、スイッチはこれらのデバイスを通過するパスを識別できません。

- **ping** 特権 EXEC コマンドを使用して接続をテストできれば、このデバイスは別のデバイスから到達可能といえます。物理パス内のすべてのデバイスは、他のスイッチから相互に到達可能でなければなりません。
- パス内で識別可能な最大ホップ数は 10 です。
- 送信元デバイスと宛先デバイスの間の物理パス内にないデバイスで、**traceroute mac** または **traceroute mac ip** の特権 EXEC コマンドを実行できます。パス内のすべてのデバイスは、このスイッチから到達可能でなければなりません。
- **traceroute mac** コマンドの出力結果としてレイヤ 2 パスが表示されるのは、指定の送信元および宛先 MAC アドレスが、同一の VLAN に属している場合だけです。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。
- マルチキャストの送信元または宛先 MAC アドレスを指定すると、パスは識別されず、エラー メッセージが表示されます。

- 送信元または宛先MACアドレスが複数のVLANに属する場合は、送信元および宛先MACアドレスの両方が属しているVLANを指定する必要があります。VLANを指定しないと、パスは識別されず、エラー メッセージが表示されます。
- 指定した送信元および宛先のIPアドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力にレイヤ2パスが表示されます。IPアドレスを指定した場合、デバイスはAddress Resolution Protocol（ARP）を使用し、IPアドレスとそれに対応するMACアドレスおよびVLAN IDを関連付けます。
  - 指定のIPアドレスにARPのエントリが存在している場合、デバイスは関連するMACアドレスを使用して、物理パスを識別します。
  - ARPのエントリが存在しない場合、デバイスはARPクエリを送信し、IPアドレスの解決を試みます。IPアドレスが解決されない場合は、パスは識別されず、エラーメッセージが表示されます。
- 複数のデバイスがハブを介して1つのポートに接続されている場合（たとえば複数のCDPネイバーがポートで検出された場合）、レイヤ2 traceroute機能はサポートされません。複数のCDPネイバーが1つのポートで検出された場合、レイヤ2パスは特定されず、エラーメッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされません。

IP Traceroute

IP traceroute を使用すると、ネットワーク上でパケットが通過するパスをホップバイホップで識別できます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク層（レイヤ 3）デバイスが表示されます。

デバイスは、**traceroute** 特権 EXEC コマンドの送信元または宛先として指定できます。また、スイッチは **traceroute** コマンドの出力でホップとして表示される場合があります。デバイスを traceroute の宛先とすると、スイッチは、traceroute の出力で最終の宛先として表示されます。中間デバイスが同じVLAN内でポート間のパケットのブリッジングだけを行う場合、traceroute の出力に中間スイッチは表示されません。ただし、中間デバイスが、特定のパケットをルーティングするマルチレイヤ デバイスの場合、中間デバイスは traceroute の出力にホップとして表示されます。

traceroute 特権 EXEC コマンドは、IP ヘッダーの存続可能時間（TTL）フィールドを使用して、ルータおよびサーバで特定のリターン メッセージが生成されるようにします。traceroute の実行は、ユーザ データグラム プロトコル（UDP）データグラムを、TTL フィールドが 1 に設定されている宛先ホストへ送信することから始まります。ルータで TTL 値が 1 または 0 であることを検出すると、データグラムをドロップし、インターネット制御メッセージプロトコル（ICMP）time-to-live-exceeded メッセージを送信元に送信します。traceroute は、ICMP time-to-live-exceeded メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判別します。

ネクスト ホップを識別するために、traceroute は TTL 値が 2 の UDP パケットを送信します。1 番めのルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信し

ます。2 番めのルータは、TTL 値が 1 であることを確認すると、このデータグラムを廃棄し、time-to-live-exceeded メッセージを送信元へ返します。このように、データグラムが宛先ホストに到達するまで（または TTL の最大値に達するまで）TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを学習するために、traceroute は、データグラムの UDP 宛先ポート番号を、宛先ホストが使用する可能性のない大きな値に設定します。ホストが、ローカルで使用されない宛先ポート番号を持つ自分自身宛てのデータグラムを受信すると、送信元に ICMP ポート到達不能エラーを送信します。ポート到達不能エラーを除くすべてのエラーは中間ホップから送信されるため、ポート到達不能エラーを受信するということは、このメッセージが宛先ポートから送信されたことを意味します。

関連トピック

IP traceroute の実行 （3157 ページ）
例：IP ホストに対する traceroute の実行 （3167 ページ）

Time Domain Reflector ガイドライン

Time Domain Reflector（TDR）機能を使用すると、ケーブル配線の問題を診断して解決できます。TDR 稼働時、ローカル デバイスはケーブルを介して信号を送信して、最初に送信した信号と反射された信号を比べます。

TDR は、10/100/1000 銅線イーサネット ポートと、マルチギガビット イーサネット（100Mbps/1/2.5/5/10 Gbps）ポートでサポートされます。SFP モジュール ポートではサポートされません。

TDR は次のケーブル障害を検出します。

- ツイストペア ケーブルの導線のオープン、損傷、切断：導線がリモート デバイスからの導線に接続されていない状態。
- ツイストペア ケーブルの導線のショート：導線が互いに接触している状態、またはリモート デバイスからの導線に接触している状態。たとえば、ツイスト ペア ケーブルの一方の導線が、もう一方の導線にはんだ付けされている場合、ツイストペア ケーブルのショートが発生します。

  ツイストペアの導線の一方がオープンになっている場合、TDR はオープンになっている導線の長さを検出できます。

（注） マルチギガビット イーサネット ポートでこの機能を使用する場合は、オープン条件またはショート条件が検出された場合にのみケーブル長が表示されます。

次の状況で TDR を使用して、ケーブル障害を診断および解決してください。

- デバイスの交換
- 配線クローゼットの設定

- リンクが確立できない、または適切に動作していない場合における、2 つのデバイス間の接続のトラブルシューティング

TDR の実行時、次の場合にデバイスは正確な情報をレポートします。

- ギガビット リンク用のケーブルが単線コア ケーブル
- オープンエンド ケーブルが未終端

TDR の実行時、次の場合にデバイスは正確な情報をレポートしません。

- ギガビット リンク用のケーブルがツイストペア ケーブルまたは連続接続された単線コア ケーブル
- リンクが 10 Mb または 100 Mb
- より線ケーブル
- リンク パートナーが Cisco IP Phone
- リンク パートナーが IEEE 802.3 に準拠していない

debug コマンド

注意 デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

debug コマンドはすべて特権 EXEC モードで実行します。ほとんどの **debug** コマンドは引数を取りません。

関連トピック

デバッグおよびエラー メッセージ出力のリダイレクト （3157 ページ）
例：すべてのシステム診断をイネーブルにする （3168 ページ）

システム レポート

システム レポートまたは crashinfo ファイルには、シスコのテクニカル サポート担当者が Cisco IOS イメージの障害（クラッシュ）が原因で起きた問題をデバッグするときに使用する情報が保存されています。明瞭度と整合性の高い重要なクラッシュ情報を迅速かつ確実に収集することが必要です。さらに、この情報の収集とバンドルが、特定のクラッシュの発生に対し関連付けか特定ができるような方法で行われることが必要です。

システム レポートは次の状況で生成されます。

- スイッチ障害の場合：システム レポートは障害が発生したメンバーで生成されます。スタック内の他のメンバーではレポートは生成されません。
- スイッチオーバーの場合：システム レポートはハイ アベイラビリティ（HA）のメンバースイッチでのみ生成されます。非 HA メンバーについてはレポートは生成されません。

リロード時はレポートは生成されません。

クラッシュ プロセス時は、次の情報がスイッチからローカルに収集されます。

1. 完全なプロセス core
2. トレースログ
3. IOS の syslog（非アクティブなクラッシュの場合には保証されません）
4. システム プロセス情報
5. ブートアップ ログ
6. リロード ログ
7. 特定のタイプの /proc 情報

この情報は個別のファイルに格納されてから、アーカイブされて1つのバンドルに圧縮されます。これにより、クラッシュのスナップショットを1つの場所で取得して、分析のためにボックス外に移動できるようになります。このレポートは、スイッチが ROMmon/ブートローダにダウンする前に生成されます。

完全な core およびトレースログ以外はテキスト ファイルです。

crashinfo ファイル

デフォルトでは、生成されたシステム レポート ファイルは /crashinfo ディレクトリに格納されます。Ifit は、領域不足のため crashinfo パーティションに保存できません。そのため、/flash ディレクトリに保存されます。

ファイルを表示するには、**dir crashinfo:** コマンドを入力します。次に crashinfo ディレクトリの出力例を示します。

```
Switch#dir crashinfo:
Directory of crashinfo:/
46553 drwx 1024 Jun 29 2015 14:52:09 +00:00 ap_crash
12 -rw- 0 Jan 1 1970 00:00:11 +00:00 koops.dat
11 -rw- 0 Mar 22 2013 07:50:30 +00:00 deleted_crash_files
13 -rwx 594269 Mar 22 2013 07:50:30 +00:00 crashinfo_platform_mgr_20130322-075017-UTC
14 -rw- 44 Sep 9 2015 09:28:47 +00:00 last_crashinfo
15 -rw- 355 Sep 9 2015 09:29:31 +00:00 last_systemreport_log
16 -rw- 105753 Mar 22 2013 07:50:47 +00:00 system-report_1_20130322-075017-UTC.gz
17 -rw- 39 Sep 9 2015 09:29:31 +00:00 last_systemreport
18 -rwx 585996 Mar 22 2013 08:01:58 +00:00 crashinfo_platform_mgr_20130322-080144-UTC
19 -rw- 105065 Mar 22 2013 08:02:15 +00:00 system-report_1_20130322-080144-UTC.gz
20 -rwx 3426209 Sep 9 2015 06:49:12 +00:00 crashinfo_iosd_20150909-064754-UTC
21 -rwx 9540376 Sep 9 2015 06:49:13 +00:00 fullcore_iosd_20150909-064754-UTC
22 -rw- 469476 Sep 9 2015 06:49:56 +00:00 system-report_1_20150909-064754-UTC.gz
```

```
23 -rwx 3425350 Sep 9 2015 09:28:47 +00:00 crashinfo_iosd_20150909-092728-UTC
24 -rwx 9535535 Sep 9 2015 09:28:47 +00:00 fullcore_iosd_20150909-092728-UTC
25 -rw- 459709 Sep 9 2015 09:29:28 +00:00 system-report_1_20150909-092728-UTC.gz
26 -rw- 0 Sep 22 2015 11:11:33 +00:00 tracelogs.J8C

50601 drwx 10240 Oct 28 2015 22:42:50 +00:00 tracelogs

248354816 bytes total (204800000 bytes free)
```

システム レポートは、次の形式で crashinfo ディレクトリに配置されます。

```
system-report_[switch number]_[date]-[timestamp]-UTC.gz
```

スイッチがクラッシュしたら、システム レポート ファイルを確認します。最後に生成されたシステム レポート ファイルは、crashinfo ディレクトリの下に last_systemreport というファイル名で保存されます。問題のトラブルシューティングを行う際、システム レポートおよびcrashinfo ファイルが TAC の役に立ちます。

生成されたシステム レポートは、TFTP や HTTP などいくつかのオプションを使用して、さらにコピーできます。

```
Switch#copy crashinfo: ?
crashinfo:     Copy to crashinfo: file system
flash:         Copy to flash: file system
ftp:           Copy to ftp: file system
http:          Copy to http: file system
https:         Copy to https: file system
null:          Copy to null: file system
nvram:         Copy to nvram: file system
rcp:           Copy to rcp: file system
running-config Update (merge with) current system configuration
scp:           Copy to scp: file system
startup-config Copy to startup configuration
syslog:        Copy to syslog: file system
system:        Copy to system: file system
tftp:          Copy to tftp: file system
tmpsys:        Copy to tmpsys: file system
```

TFTP サーバにコピーするための一般的な構文は次のとおりです。

```
Switch#copy crashinfo: tftp:
Source filename [system-report_1_20150909-092728-UTC.gz]?
Address or name of remote host []? 1.1.1.1
Destination filename [system-report_1_20150909-092728-UTC.gz]?
```

スタックの全メンバーからのトレースログは、trace archive コマンドを発行することで取得できます。 このコマンドには、時間帯オプションがあります。コマンド構文は次のとおりです。

```
Switch#request platform software trace archive ?
last     Archive trace files of last x days
target   Location and name for the archive file
```

crashinfo: または flash: ディレクトリに格納されている過去 3650 日以内のトレースログが取得できます。

```
Switch# request platform software trace archive last ?
<1-3650> Number of days (1-3650)
Switch#request platform software trace archive last 3650 days target ?
crashinfo: Archive file name and location
flash:     Archive file name and location
```

（注） 一度コピーされたら、システム レポートやトレースのアーカイブを flash ディレクトリまたは crashinfo ディレクトリからクリアし、トレースログやその他の目的に使用できる領域を確保することが重要です。

スイッチのオンボード障害ロギング

オンボード障害ロギング（OBFL）機能を使用すれば、デバイスに関する情報を収集できます。この情報には稼働時間、温度、電圧などの情報が含まれており、シスコのテクニカルサポート担当者がデバイスの問題をトラブルシューティングする際に役立ちます。OBFL はイネーブルにしておき、フラッシュ メモリに保存されたデータは消さないようにすることを推奨します。

OBFL は、デフォルトでイネーブルになっています。デバイスおよび Small Form-Factor Pluggable（SFP）モジュールに関する情報が収集されます。デバイスは、次の情報をフラッシュ メモリに保存します。

- CLI コマンド：スタンドアロン デバイスまたはスイッチ スタック メンバに入力された OBFL CLI コマンドの記録
- 環境データ：スタンドアロンデバイスまたはスタックメンバおよび接続されているすべての FRU デバイスの一意のデバイス ID（UDI）情報、製品 ID（PID）、バージョン ID（VID）、およびシリアル番号
- メッセージ：スタンドアロンデバイスまたはスタック メンバにより生成されたハードウェア関連のシステム メッセージの記録
- イーサネット経由の電源供給（PoE）：スタンドアロンデバイスまたはスイッチスタックメンバの PoE ポートの消費電力の記録
- 温度：スタンドアロン デバイスまたはスタック メンバの温度
- 稼働時間：スタンドアロン デバイスまたはスタック メンバが起動されたときの時刻、デバイスが再起動された理由、およびデバイスが最後に再起動されて以来の稼働時間
- 電圧：スタンドアロン デバイスまたはスタック メンバのシステム電圧

システム時計は、手動で時刻を設定するか、またはネットワーク タイム プロトコル（NTP）を使用するように設定します。

デバイスの稼働中には、**show logging onboard** 特権 EXEC コマンドを使用することにより、OBFL データを取得できます。デバイスに障害が発生した場合のデータの取得方法については、お客様担当のシスコ テクニカル サポート担当者にお問い合わせください。

OBFL がイネーブルになっているデバイスが再起動された場合、新しいデータの記録が開始するまでに 10 分間の遅延があります。

関連トピック

OBFL の設定 （3158 ページ）
OBFL 情報の表示 （3159 ページ）

ファン障害

デフォルトでは、この機能はディセーブルです。現場交換可能ユニット（FRU）または電源装置の複数のファンが故障した場合、デバイスはシャットダウンせず、次のようなエラー メッセージが表示されます。

```
Multiple fan(FRU/PS) failure detected. System may get overheated. Change fan quickly.
```

デバイスが過熱状態となり、シャットダウンすることもあります。

ファン障害機能をイネーブルにするには、**system env fan-fail-action shut** 特権 EXEC コマンドを入力します。デバイス内の複数のファンに障害が発生した場合、デバイスは自動的にシャットダウンし、次のようなエラー メッセージが表示されます。

```
Faulty (FRU/PS) fans detected, shutting down system!
```

最初のファンの停止後、デバイスが 2 つめのファンの障害を検知すると、デバイスは 20 秒待機してからシャットダウンします。

デバイスを再起動するには、電源をオフにしてから再度オンにする必要があります。

CPU 使用率が高い場合に起こりうる症状

CPU使用率が高すぎることで次の症状が発生する可能性がありますが、他の原因で発生する場合もあります。

- スパニングツリー トポロジの変更
- 通信が切断されたために EtherChannel リンクがダウンした
- 管理要求（ICMP ping、SNMP のタイムアウト、低速な Telnet または SSH セッション）に応答できない
- UDLD フラッピング
- SLA の応答が許容可能なしきい値を超えたことによる IP SLA の失敗
- スイッチが要求を転送しない、または要求に応答しない場合の DHCP または IEEE 802.1x の処理の失敗

ソフトウェア設定のトラブルシューティング方法

ソフトウェア障害からの回復

始める前に

ここで紹介する回復手順を実行するには、スイッチを直接操作する必要があります。

ここで紹介する手順では、破損したイメージ ファイルまたは不適切なイメージ ファイルの回復に boot loader コマンドおよび TFTP を使用します。

手順

ステップ 1 PC 上で、Cisco.com からソフトウェア イメージ ファイル（*image.bin*）をダウンロードします。

ステップ 2 TFTP サーバにソフトウェア イメージをロードします。

ステップ 3 PC をスイッチのイーサネット管理ポートに接続します。

ステップ 4 スイッチの電源コードを取り外します。

ステップ 5 [**Mode**] ボタンを押しながら、電源コードを再度スイッチに接続します。

ステップ 6 ブートローダ（ROMMON）プロンプトで、TFTP サーバに ping を実行できることを確認します。

a) 次のコマンドを実行して、IP アドレス を設定します。**switch: set IP_ADDR** *ip_address subnet_mask*

例：

```
switch: set IP_ADDR 192.0.2.123/255.255.255.0
```

b) 次のコマンドを実行して、デフォルト ルータの IP アドレスを設定します。**switch: set DEFAULT_ROUTER** *ip_address*

例：

```
switch: set DEFAULT_ROUTER 192.0.2.1
```

c) 次のコマンドを実行して、TFTP サーバに ping を実行できることを確認します。**switch: ping** *ip_address_of_TFTP_server*

例：

```
switch: ping 192.0.2.15
ping 192.0.2.1 with 32 bytes of data...
Host 192.0.2.1 is alive.
switch:
```

ステップ 7 回復パーティション（sda9:）に回復イメージが存在することを確認します。

この回復イメージは、emergency-install 機能を使用して回復を実施する場合に必要となります。

例：

```
switch: dir sda9:
Directory of sda9:/

    2  drwx  1024       .
    2  drwx  1024       ..
   11  -rw-  18923068   c3850-recovery.bin

36939776 bytes available (20830208 bytes used)
switch:
```

ステップ 8 ブートローダ（ROMMON）プロンプトで、emergency-install 機能を開始します。この機能を使用すると、スイッチでソフトウェア イメージを容易に回復できます。

警告：emergency-install コマンドを実行すると、ブート ブラッシュ全体が消去されます。

例：

```
Switch#
emergency-install
tftp://192.0.2.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin

The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin)...
Reading full image into memory.....................done
Nova Bundle Image
-------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
 0x90000000].
@@@
```

```
Package cat3k_caa-iosd-universalk9.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.03.02.00.SE.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM +++@@@@####...++@@++@@++@@++@
```

関連トピック

スイッチのソフトウェア障害 （3136 ページ）

パスワードを忘れた場合の回復

スイッチのデフォルト設定では、スイッチを直接操作するエンドユーザが、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復できます。ここで紹介する回復手順を実行するには、スイッチを直接操作してください。

（注） これらのスイッチでは、システム管理者はデフォルト設定に戻す場合に限りエンドユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできます。パスワード回復がディセーブルになっている場合に、エンドユーザがパスワードをリセットしようとすると、回復プロセスの間、ステータス メッセージにその旨が表示されます。

手順

ステップ 1 端末または PC をスイッチに接続します。

- 端末または端末エミュレーション ソフトウェアが稼働している PC をスイッチのコンソール ポートに接続します。スイッチ スタックのパスワードを回復する場合は、アクティブ スイッチのコンソール ポートに接続するか、または
- PC をイーサネット管理ポートに接続します。スイッチ スタックのパスワードを回復する場合は、スタック メンバのイーサネット管理ポートに接続します。

ステップ 2 エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 3 スタンドアロン スイッチまたはスイッチ スタック全体の電源を切断します。

ステップ 4 電源コードまたはアクティブ スイッチを再度接続します。15 秒以内に [**Mode**] ボタンを押します。このときシステム LED はグリーンに点滅しています。すべてのシステム LED が点灯した状態になるまで、[**Mode**] ボタンを押し続けます。その後、[**Mode**] ボタンを放します。

-

```
Switch:
Xmodem file system is available.
Base ethernet MAC Address: 20:37:06:4d:e9:80
Verifying bootloader digital signature.


The system has been interrupted prior to loading the operating
system software, console will be reset to 9600 baud rate.
```

「パスワード回復がイネーブルになっている場合の手順」セクションに記載されている手順を実行します。

ステップ 5 パスワードの回復後、スイッチまたは アクティブ スイッチ をリロードします。

スイッチの場合

```
Switch> reload
Proceed with reload? [confirm] y
```

アクティブ スイッチの場合

```
Switch> reload slot <stack-active-member-number>
Proceed with reload? [confirm] y
```

ステップ 6 スタック内の残りのスイッチに電源を投入します。

関連トピック

のパスワードを紛失したか忘れた場合 デバイス （3136 ページ）

パスワード回復がイネーブルになっている場合の手順

パスワード回復動作がイネーブルになっている場合は、次のメッセージが表示されます。

手順

ステップ 1 フラッシュ ファイル システムを初期化します。

```
Device: flash_init
```

ステップ 2 次のコマンドを使用して、スタートアップ コンフィギュレーションを無視します。

```
Device: SWITCH_IGNORE_STARTUP_CFG=1
```

ステップ 3 *packages.conf* ファイルでスイッチをフラッシュからブートします。

```
Device: boot flash:packages.conf
```

ステップ 4 **No** と応答して初期設定ダイアログを終了します。

```
Would you like to enter the initial configuration dialog? [yes/no]: No
```

ステップ 5 スイッチ プロンプトで、特権 EXEC モードを開始します。

```
Device> enable
Switch#
```

ステップ 6 スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。

```
Device# copy startup-config running-config Destination filename [running-config]?
```

確認を求めるプロンプトに、Return を押して応答します。これで、コンフィギュレーション ファイルがリロードされ、パスワードを変更できます。

ステップ 7 グローバル コンフィギュレーション モードを開始して、**イネーブル** パスワードを変更します。

```
Device# configure terminal
Device(config)#
```

ステップ 8 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Device# copy running-config startup-config
```

ステップ 9 手動ブート モードがイネーブルになっていることを確認します。

```
Device# show boot

 BOOT variable = flash:packages.conf;
 Manual Boot = yes
 Enable Break = yes
```

ステップ 10 デバイスをリロードします。

```
Device# reload
```

ステップ 11 （ステップ 2 と 3 で変更した）ブートローダ パラメータを元の値に戻します。

```
Device: switch: SWITCH_IGNORE_STARTUP_CFG=0
```

ステップ 12 フラッシュからのデバイス *packages.conf* を起動します。

```
Device: boot flash:packages.conf
```

ステップ 13 デバイス のブート後に、デバイス で手動ブートをディセーブルにします。

```
Device(config)# no boot manual
```

パスワード回復がディセーブルになっている場合の手順

パスワード回復メカニズムがディセーブルの場合、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

⚠

注意 デバイスをデフォルト設定に戻すと、既存の設定がすべて失われます。システム管理者に問い合わせて、バックアップ デバイスと VLAN（仮想 LAN）コンフィギュレーション ファイルがあるかどうかを確認してください。

- **n**（no）を入力すると、Mode ボタンを押さなかった場合と同様に、通常のブート プロセスが継続されます。ブートローダ プロンプトにはアクセスできません。したがって、新しいパスワードを入力できません。次のメッセージが表示されます。

  ```
  Press Enter to continue........
  ```

- **y**（yes）を入力すると、フラッシュ メモリ内のコンフィギュレーション ファイルおよび VLAN データベース ファイルが削除されます。デフォルト設定がロードされるときに、パスワードをリセットできます。

手順

ステップ 1 パスワード回復手順の継続を選択すると、既存の設定が失われます。

```
Would you like to reset the system back to the default configuration (y/n)? Y
```

ステップ 2 フラッシュ メモリの内容を表示します。

```
Device: dir flash:
```

デバイスのファイル システムが表示されます。

```
Directory of flash:/
.
.
.i'
15494  drwx        4096   Jan 1 2000 00:20:20 +00:00  kirch
15508  -rw-   258065648   Sep 4 2013 14:19:03 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
162196684
```

ステップ 3 システムを起動します。

```
Device: boot
```

セットアップ プログラムを起動するように求められます。パスワード回復手順を継続するには、プロンプトに **N** を入力します。

```
Continue with the configuration dialog? [yes/no]: N
```

ステップ 4 デバイス プロンプトで、特権 EXEC モードを開始します。

```
Device> enable
```

ステップ 5 グローバル コンフィギュレーション モードを開始します。

```
Device# configure terminal
```

ステップ 6 パスワードを変更します。

```
Device(config)# enable secret password
```

シークレット パスワードは 1 ～ 25 文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 7 特権 EXEC モードに戻ります。

```
Device(config)# exit
Device#
```

（注） ステップ 9 に進む前に、接続されているすべてのスタック メンバの電源を入れ、それらが完全に初期化されるまで待ちます。

ステップ 8 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Device# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。

ステップ 9 ここでデバイスを再設定する必要があります。システム管理者によって、バックアップデバイスと VLAN コンフィギュレーション ファイルが使用可能に設定されている場合は、これらを使用します。

スイッチ スタック問題の回避

スイッチ スタックの問題を防止するには、次の作業を実行する必要があります。

- デバイス スタックにスイッチを追加したり、そこから取り外したりする場合には、必ずスイッチの電源を切ってください。スイッチスタックでの電源関連のあらゆる考慮事項については、ハードウェア インストレーション ガイドの「Switch Installation（スイッチのインストール）」の章を参照してください。
- スタック モード LED が点灯するまで、スタック メンバの **Mode** ボタンを押します。デバイスの最後の 2 つのポート LED がグリーンになります。デバイス モデルに応じて、最後の 2 つのポートは 10/100/1000 ポートまたは Small Form-Factor Pluggable モジュールになります。最後の 2 つのポート LED の片方または両方がグリーンになっていない場合は、スタックが全帯域幅で稼働していません。
- スイッチ スタックを管理する場合は、1 つの CLI セッションだけを使用することを推奨します。アクティブ スイッチに複数の CLI セッションを使用する場合は注意が必要です。1 つのセッションで入力したコマンドは、別のセッションには表示されません。そのため、コマンドを入力したセッションを識別できなくなることがあります。
- スタック内での位置に従ってスタック メンバ番号を手動で割り当てると、リモートから行うデバイス スタックのトラブルシューティングが容易になります。ただし、後からデバイスを追加したり、取り外したり、場所を入れ替えたりする際に、デバイスに手動で番号を割り当てたことを覚えておく必要があります。スタック メンバー番号を手動で割り当てるには、**switch** *current-stack-member-number* **renumber** *new-stack-member-number* グローバル コンフィギュレーション コマンドを使用します。

スタック メンバをまったく同じモデルで置き換えると、新しいデバイスは、置き換えられたデバイスとまったく同じ設定で稼働します。この場合、新しいデバイスは置き換えられたデバイスと同じメンバ番号を使用するものと想定されます。

電源が入った状態のスタック メンバを取り外すと、スイッチ スタックが、それぞれ同じ設定を持つ 2 つ以上のスイッチ スタックに分割（パーティション化）されます。スイッチ スタックを分離されたままにしておきたい場合は、新しく作成されたスイッチ スタックの IP アドレス（複数の場合あり）を変更してください。パーティション化されたスイッチスタックを元に戻すには、次の手順を実行します。

1. 新しく作成されたスイッチ スタックの電源を切ります。

2. 新しいスイッチ スタックを、StackWise Plus ポートを介して元のスイッチ スタックに再度接続します。
3. デバイスの電源を入れます。

スイッチ スタックおよびそのメンバのモニタリングに使用できるコマンドについては、「*Displaying Switch Stack Information*」の項を参照してください。

自動ネゴシエーションの不一致の防止

IEEE 802.3ab 自動ネゴシエーション プロトコルは速度（10 Mbps、100 Mbps、および SFP モジュール ポート以外の 1000 Mbps）およびデュプレックス（半二重または全二重）に関するデバイスの設定を管理します。このプロトコルは設定を適切に調整しないことがあり、その場合はパフォーマンスが低下します。不一致は次の条件で発生します。

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動で設定された速度またはデュプレックスのパラメータと異なっている場合。
- ポートを自動ネゴシエーションに設定したが、接続先ポートは自動ネゴシエーションを使用しない全二重に設定されている場合。

デバイスのパフォーマンスを最大限に引き出してリンクを確保するには、次のいずれかの注意事項に従って、デュプレックスおよび速度の設定を変更してください。

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 接続の両側でポートの速度とデュプレックスのパラメータを手動で設定します。

（注） 接続先装置が自動ネゴシエーションを実行しない場合は、2 つのポートのデュプレックス設定を一致させます。速度パラメータは、接続先のポートが自動ネゴシエーションを実行しない場合でも自動調整が可能です。

SFP モジュールのセキュリティと識別に関するトラブルシューティング

シスコの Small Form-Factor Pluggable（SFP）モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリティ コード、および巡回冗長検査（CRC）が格納されたシリアル EEPROM（電気的に消去可能でプログラミング可能な ROM）を備えています。デバイスに SFP モジュールを装着すると、デバイス ソフトウェアは、EEPROM を読み取ってシリアル番号、ベンダー名、およびベンダー ID を確認し、セキュリティ コードおよび CRC を再計算します。シリアル番号、ベンダー名、ベンダー ID、セキュリティ コード、または CRC が無効な場合、ソフトウェアは、セキュリティ エラー メッセージを生成し、インターフェイスを errdisable ステートにします。

（注） セキュリティ エラー メッセージは、GBIC_SECURITY 機能を参照します。デバイスは、SFP モジュールをサポートしていますが、GBIC（ギガビット インターフェイス コンバータ）モジュールはサポートしていません。エラー メッセージテキストは、GBICインターフェイスおよびモジュールを参照しますが、セキュリティ メッセージは、実際は SFP モジュールおよびモジュール インターフェイスを参照します。

他社の SFP モジュールを使用している場合、デバイスから SFP モジュールを取り外し、シスコのモジュールに交換します。シスコの SFP モジュールを装着したら、**errdisable recovery cause gbic-invalid** グローバル コンフィギュレーション コマンドを使用してポート ステータスを確認し、error-disabled ステートから回復する時間間隔を入力します。この時間間隔が経過すると、デバイスはerror-disabledステートからインターフェイスを復帰させ、操作を再試行します。**errdisable recovery** コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

モジュールがシスコ製SFPモジュールとして識別されたにもかかわらず、システムがベンダーデータ情報を読み取ってその情報が正確かどうかを確認できないと、SFP モジュール エラー メッセージが生成されます。この場合、SFPモジュールを取り外して再び装着してください。それでも障害が発生する場合は、SFP モジュールが不良品である可能性があります。

SFP モジュール ステータスのモニタリング

show interfaces transceiver 特権 EXEC コマンドを使用すると、SFP モジュールの物理または動作ステータスを確認できます。このコマンドは、温度や特定のインターフェイス上の SFP モジュールの現状などの動作ステータスと、アラーム ステータスを表示します。また、このコマンドを使用してSFPモジュールの速度およびデュプレックス設定も確認できます。詳細については、このリリースのコマンド リファレンスに記載された **show interfaces transceiver** コマンドの説明を参照してください。

ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティック ルートを定義するか、またはこれらのサブネット間でルーティングされるようにIPルーティングを設定する必要があります。

IP ルーティングは、デフォルトではすべてのデバイスでディセーブルになります。

（注） **ping** コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

このコマンドは、デバイスからネットワーク上の他のデバイスに ping を実行する目的で使用します。

コマンド	目的
ping ip *host* | *address* `Device# ping 172.20.52.3`	IP またはホスト名やネットワーク アドレスを指定してリモート ホストに ping を実行します。

関連トピック

ping （3137 ページ）
例：IP ホストの ping （3166 ページ）

温度のモニタリング

デバイスは温度条件をモニタし、温度情報を使用してファンを制御します。

温度の値、状態、しきい値を表示するには、**show env temperature status** 特権 EXEC コマンドを使用します。温度の値は、デバイス内の温度であり、外部の温度ではありません。**system env temperature threshold yellow** *value* グローバル コンフィギュレーション コマンドを使用してイエローのしきい値レベル（摂氏）だけを設定し、イエローのしきい値およびレッドのしきい値の差を設定できます。グリーンまたはレッドのしきい値は設定できません。詳細については、このリリースのコマンド リファレンスを参照してください。

物理パスのモニタリング

次のいずれかの特権EXECコマンドを使用して、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスをモニタできます。

表 *208 :* 物理パスのモニタリング

コマンド	目的
tracetroute mac [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]	指定の送信元MACアドレスから、指定の宛先MACアドレスまでをパケットが通過するレイヤ 2 パスを表示します。
tracetroute mac ip {*source-ip-address* | *source-hostname*}{*destination-ip-address* | *destination-hostname*} [**detail**]	指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示します。

IP traceroute の実行

（注） **traceroute** 特権 EXEC コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

コマンド	目的
traceroute ip ホスト `Device# traceroute ip 192.51.100.1`	ネットワーク上でパケットが通過するパスを追跡します。

関連トピック

IP Traceroute （3139 ページ）
例：IP ホストに対する traceroute の実行 （3167 ページ）

TDR の実行および結果の表示

TDR を実行する場合、**test cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを入力します。

TDR の結果を表示するには、**show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを実行します。

デバッグおよびエラー メッセージ出力のリダイレクト

ネットワーク サーバはデフォルトで、**debug** コマンドおよびシステム エラー メッセージの出力をコンソールに送信します。このデフォルトの設定を使用する場合は、コンソールポートまたはイーサネット管理ポートに接続する代わりに、仮想端末接続によってデバッグ出力をモニタできます。

指定できる宛先として、コンソール、仮想端末、内部バッファ、およびsyslogサーバを実行している UNIX ホストがあります。Syslog フォーマットは、4.3 BSD UNIX およびそのバリエーションと互換性があります。

（注） デバッグの出力先がシステムのオーバーヘッドに影響を与えることがないように注意してください。メッセージをコンソールに記録すると、非常に高いオーバーヘッドが発生します。仮想端末にメッセージを記録すると、発生するオーバーヘッドは低くなります。Syslog サーバでメッセージロギングを行うと、オーバーヘッドはさらに小さくなり、内部バッファであれば最小限ですみます。

システム メッセージのロギングに関する詳細については、「システム メッセージ ロギングの設定」を参照してください。

関連トピック

debug コマンド （3141 ページ）

show platform forward コマンドの使用

show platform forward**show platform forward**特権 EXEC コマンドの出力からは、インターフェイスに入るパケットがシステムを介して送信された場合、転送結果に関して、有意義な情報がいくつか得られます。パケットに関して入力されたパラメータに応じて、参照テーブル結果、転送宛先の計算に使用されるポートマップ、ビットマップ、および出力側の情報が表示されます。

このコマンドで出力される情報のほとんどは、主に、デバイスの用途別集積回路（ASIC）に関する詳細情報を使用するテクニカルサポート担当者に役立つものです。ただし、パケット転送情報はトラブルシューティングにも役立ちます。

show debug コマンドの使用方法

show debug コマンドは、特権 EXEC モードで入力します。このコマンドは、スイッチで使用可能なすべてのデバッグ オプションを表示します。

すべての条件付きデバッグ オプションを表示するには、コマンド **show debug condition** を実行します。コマンドは、条件 ID *<1-1000>*または *all* 条件を選択することで一覧表示できます。

デバッグを無効にするには、**no debug all** コマンドを使用します。

⚠

注意 デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 16.1 (Catalyst 3850 Switches)*』を参照してください。

OBFL の設定

⚠

注意 OBFL はディセーブルにせず、フラッシュ メモリに保存されたデータは削除しないことを推奨します。

- OBFL をイネーブルにするには、**hw-switch switch** [*switch-number*] **logging onboard** [**message level** *level*] グローバル コンフィギュレーション コマンドを使用します。スイッチの場合、

switch-number に指定できる範囲は 1 ～ 9 です。スイッチが生成してフラッシュ メモリに保存するハードウェア関連のメッセージの重大度を指定するには、**message level** *level* パラメータを使用します。

- OBFL データをローカル ネットワークまたは指定したファイル システムにコピーするには、**copy onboard switch** *switch-number* **url** *url-destination* 特権 EXEC コマンドを使用します。
- OBFL をディセーブルにするには、**no hw-switch switch** [*switch-number*] **logging onboard** [**message level**] グローバル コンフィギュレーション コマンドを使用します。
- フラッシュ メモリ内の稼働時間と CLI コマンド情報以外のすべての OBFL データをクリアするには、**clear onboard switch** *switch-number* 特権 EXEC コマンドを使用します。
- スイッチ スタックでは、**hw-switch switch** [*switch-number*] **logging onboard** [**message level** *level*] グローバル コンフィギュレーション コマンドを使用することにより、スタンドアロン スイッチまたはすべてのスタック メンバの OBFL をイネーブルにできます。
- アクティブ スイッチのメンバ スイッチの OBFL をイネーブルまたはディセーブルにできます。

ここで説明した各コマンドの詳細については、このリリースのコマンドリファレンスを参照してください。

関連トピック

スイッチのオンボード障害ロギング （3144 ページ）
OBFL 情報の表示 （3159 ページ）

ソフトウェア設定のトラブルシューティングの確認

OBFL 情報の表示

表 *209 : OBFL* 情報を表示するためのコマンド

コマンド	目的
show onboard switch *switch-number* **clilog** `Device# show onboard switch 1 clilog`	スタンドアロン スイッチまたは指定されたスタック メンバで入力された OBFL CLI コマンドを表示します。
show onboard switch *switch-number* **environment** `Device# show onboard switch 1 environment`	スタンドアロン スイッチまたは指定されたスタック メンバおよび接続されているすべての FRU デバイスの UDI 情報、PID、VID、およびシリアル番号を表示します。

コマンド	目的
show onboard switch *switch-number* **message** `Device# show onboard switch 1 message`	スタンドアロン スイッチまたは指定されたスタック メンバによって生成されたハードウェア関連のメッセージを表示します。
show onboard switch *switch-number* **counter** `Device# show onboard switch 1 counter`	スタンドアロン スイッチまたは指定したスタック メンバのカウンタ情報を表示します。
show onboard switch *switch-number* **temperature** `Device# show onboard switch 1 temperature`	スタンドアロン スイッチまたは指定されたスイッチ スタック メンバの温度を表示します。
show onboard switch *switch-number* **uptime** `Device# show onboard switch 1 uptime`	スタンドアロン スイッチまたは指定されたスタック メンバが起動した時刻、スタンドアロン スイッチまたは指定されたスタック メンバが再起動された理由、およびスタンドアロン スイッチまたは指定されたスタック メンバが最後に再起動されて以来の稼働時間を表示します。
show onboard switch *switch-number* **voltage** `Device# show onboard switch 1 voltage`	スタンドアロン スイッチまたは指定されたスタック メンバのシステム電圧を表示します。
show onboard switch *switch-number* **status** `Device# show onboard switch 1 status`	スタンドアロン スイッチまたは指定されたスタック メンバの状態を表示します。

関連トピック

スイッチのオンボード障害ロギング （3144 ページ）
OBFL の設定 （3158 ページ）

例：高い CPU 使用率に関する問題と原因の確認

CPU 使用率が高いことが問題となっているかどうか判別するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の 1 行目にある下線が付いた部分に注目してください。

```
Device# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
```

```
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

この例は、正常な CPU 使用率を示しています。この出力によると、最後の 5 秒間の使用率が 8%/0% となっていますが、この意味は次のとおりです。

- Cisco IOS の処理時間と割り込みの処理にかかった時間を合わせた CPU の合計の使用率は全体の 8%
- 割り込みの処理にかかった時間は全体の 0%

表 *210 : CPU* 使用率に関する問題のトラブルシューティング

問題のタイプ	Cause	修正措置
割り込みのパーセント値が合計の CPU 使用率の値とほぼ同程度に高い	CPU がネットワークから受信するパケット数が多すぎる。	ネットワーク パケットのソースを判別する。データの流れを遮断するか、スイッチの設定を変更します。「Analyzing Network Traffic（ネットワーク トラフィックの解析）」の項を参照してください。
割り込みの所要時間は最小限であったにもかかわらず CPU の合計使用率が 50% を超える	CPU 時間を過度に消費する Cisco IOS 処理が 1 つ以上存在する。これは通常、処理をアクティブ化するイベントによって始動されます。	異常なイベントを特定して根本的な原因を解消する。「Debugging Active Processes（アクティブなプロセスのデバッグ）」のセクションを参照してください。

ソフトウェア設定のトラブルシューティングのシナリオ

Power over Ethernet（PoE）に関するトラブルシューティングのシナリオ

表 *211 : Power over Ethernet* に関するトラブルシューティングのシナリオ

症状または問題	考えられる原因と解決法
PoE がないポートは 1 つに限りません。 1 つのスイッチ ポートに限り問題が発生する。このポートでは PoE 装置と PoE 非対応の装置のいずれも動作しないが、他のポートでは動作します。	この受電デバイスが他の PoE ポートで動作するかを確認する。 **show run**、または **show interface status** ユーザ EXEC コマンドを使用して、ポートがシャットダウンしていないか、または error-disabled になっていないかを確認します。 （注） ほとんどのスイッチはポートがシャットダウンしているときはポートの電力供給をオフにします。これは、IEEE 仕様でこれがオプションに指定されている場合も同様です。 受電デバイスからスイッチ ポートまでのイーサネット ケーブルの動作が正常であることを確認します。具体的には、既知の正常な PoE 非対応のイーサネット装置とイーサネット ケーブルを接続して、受電デバイスがリンクを確立し他のホストとトラフィックを交換することを確認します。 スイッチのフロント パネルから受電デバイスまでのケーブル長の合計が 100 メートル以下であることを確認します。 スイッチ ポートからイーサネット ケーブルを外します。短いイーサネット ケーブルを使用して、既知の正常なイーサネット装置を、スイッチのフロント パネルの（パッチ パネルではない）このポートに直接接続します。これによってイーサネット リンクが確立され他のホストとトラフィックを交換できることを確認します。あるいは、ポートの VLAN SVI で ping を実行してください。次に、受電デバイスをこのポートに接続し、電源がオンになることを確認します。 パッチ コードをスイッチ ポートに接続しても受電デバイスの電源がオンにならない場合、接続する受電デバイスの合計数とスイッチの電力バジェット（使用可能な PoE）とを比較してください。**show inline power** コマンドを使用して、利用可能な電源の量を確認します。

症状または問題	考えられる原因と解決法
すべてのポートまたは1つのポート グループで PoE が機能しない。 すべてのスイッチ ポートで問題が発生する。電力が供給されていないイーサネット装置がどのポートでもイーサネット リンクを確立できず、PoE装置の電源がオンになりません。	

症状または問題	考えられる原因と解決法
	電力に関するアラームが継続的に発生する、断続的に発生する、または再発する場合は、可能であれば電源モジュールを交換します（現場交換可能ユニットです）。そうでない場合はスイッチを交換してください。 連続する複数のポートで問題があるものの、すべてのポートで問題が発生するわけではない場合、電源の故障ではないと考えられ、スイッチのPoEレギュレータに関連した異常の可能性があります。 PoEの状況やステータスの変更について過去に報告されているアラームまたはシステムメッセージを確認するには、**show log** 特権 EXEC コマンドを使用します。 アラームがない場合は、**show interface status** コマンドを使用して、ポートがシャットダウンしていないかerrdisableになっていないかを確認します。ポートがerror-disabledの場合、**shut** および **no shut** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。 特権 EXEC コマンドの **show env power** および **show power inline** を使用して、PoEのステータスおよび電力バジェット（使用可能なPoE）を調べます。 実行コンフィギュレーションを調べて **power inline never** がこのポートに設定されていないことを確認します。 受電していないイーサネット装置をスイッチポートに直接接続します。接続には短いパッチ コードだけを使用します。既存の配線ケーブルは使用しないでください。**shut** および **no shut** インターフェイス コンフィギュレーション コマンドを入力し、イーサネットリンクが確立されていることを確認します。正しく接続している場合、短いパッチコードを使用して受電デバイスをこのポートに接続し、電源がオンになることを確認します。装置の電源がオンになったら、すべての中間パッチパネルが正しく接続されているか確認してください。 1本を除くすべてのイーサネットケーブルをスイッチポートから抜きます。短いパッチ コードを使用して、1つのPoEポートにだけ受電デバイスを接続します。スイッチポートからの受電に比較して、受電デバイスが多くの電力を必要としないことを確認してください。 **show power inline** 特権 EXEC コマンドを使用して、ポートがシャットダウンしていない場合に、受電デバイスに電力が供給されることを確認します。あるいは、受電デバイス

症状または問題	考えられる原因と解決法
	を観察して電源がオンになることを確認してください。 1 台の受電デバイスだけがスイッチに接続しているときに電力が供給される場合、残りのポートで **shut** および **no shut** インターフェイス コンフィギュレーション コマンドを入力してから、イーサネット ケーブルをスイッチの PoE ポートに 1 本ずつ再び接続してください。**show interface status** および **show power inline** 特権 EXEC コマンドを使用して、インライン電源の統計情報およびポートの状態をモニタします。 すべてのポートで、まだ PoE が機能しない場合は、電源装置の PoE セクションでヒューズを開くことができる場合があります。この場合、アラームが生成されるのが一般的です。過去にシステム メッセージでアラームが報告されていないか、ログをもう一度チェックしてください。
Cisco IP Phone が切断またはリセットされる。 正常に動作した後で、Cisco phone またはワイヤレス アクセス ポイントが断続的にリロードしたり、PoE から切断されたりします。	スイッチから受電デバイスまでのすべての電気系統を確認してください。信頼性の低い接続は、電力供給の中断や受電デバイスの機能が不安定になる原因となり、受電デバイスの断続的な切断やリロードなどが発生します。 スイッチ ポートから受電デバイスまでのケーブル長が 100 メートル以下であることを確認してください。 スイッチが配置されている場所で電気環境にどのような変化があるか、切断時に、受電デバイスに何が起きるかについて注意してください。 切断と同時にエラー メッセージが表示されたか注意します。**show log** 特権 EXEC コマンドを使用してエラー メッセージを確認します。 リロードの発生直前に IP Phone から Call Manager へのアクセスが失われていないか確認してください（PoE の障害ではなくネットワークに問題が発生している場合があります）。 受電デバイスを PoE 非対応の装置に交換し、装置が正しく動作することを確認します。PoE 非対応の装置にリンク障害または高いエラー率がある場合、スイッチ ポートと受電デバイスを接続する信頼性の低いケーブル接続が問題の可能性があります。

症状または問題	考えられる原因と解決法
シスコ以外の受電デバイスがシスコ PoE スイッチで動作しない。 シスコ PoE スイッチに接続するシスコ以外の受電デバイスに電源が供給されないか、電源投入後すぐに電源が切れます。PoE 非対応装置は正常に動作します。	**show power inline** コマンドを使用して、受電デバイスの接続前後に、スイッチの電力バジェット（使用可能な PoE）が使い果たされていないか確認してください。受電デバイスを接続する前に、このタイプの装置に十分な電力が使用可能であることを確認します。 **show interface status** コマンドを使用して、接続されている受電デバイスをスイッチが検出することを確認します。 **show log** コマンドを使用して、ポートの過電流状態を報告したシステムメッセージがないか確認します。症状を正確に特定してください。最初に電力が受電デバイスに供給され、その後、切断される状態ですか。その場合は、問題は最初のサージ電流（突入電流）が原因で、ポートの電流上限しきい値が超過した可能性があります。

関連トピック

Power over Ethernet（PoE）ポート （3136 ページ）

ソフトウェアのトラブルシューティングの設定例

例：IP ホストの ping

次に、IP ホストに ping を実行する例を示します。

```
Device# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Device#
```

表 *212 : Ping* の出力表示文字

文字	説明
!	感嘆符 1 個につき 1 回の応答を受信したことを示します。
.	ピリオド 1 個につき応答待ちの間にネットワーク サーバのタイムアウトが 1 回発生したことを示します。
U	宛先到達不能エラー PDU を受信したことを示します。
C	輻輳に遭遇したパケットを受信したことを示します。

文字	説明
I	ユーザによりテストが中断されたことを示します。
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

ping セッションを終了するには、エスケープ シーケンス（デフォルトでは Ctrl+^ X）を入力してください。Ctrl キー、Shift キー、および 6 キーを同時に押してから放し、その後 X キーを押します。

関連トピック

ping （3137 ページ）
ping の実行 （3155 ページ）

例：IP ホストに対する traceroute の実行

次に、IP ホストに **traceroute** を実行する例を示します。

```
Device# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

  1 192.0.2.1 0 msec 0 msec 4 msec
  2 192.0.2.203 12 msec 8 msec 0 msec
  3 192.0.2.100 4 msec 0 msec 0 msec
  4 192.0.2.10 0 msec 4 msec 0 msec
```

ディスプレイには、送信される 3 つのプローブごとに、ホップ カウント、ルータの IP アドレス、およびラウンドトリップ タイム（ミリ秒単位）が表示されます。

表 *213 : traceroute* の出力表示文字

文字	説明
*	プローブがタイムアウトになりました。
?	パケット タイプが不明です。
A	管理上、到達不能です。通常、この出力は、アクセス リストがトラフィックをブロックしていることを表しています。
H	ホストが到達不能です。
N	ネットワークが到達不能です。

文字	説明
P	プロトコルが到達不能です。
Q	発信元。
U	ポートが到達不能です。

実行中の追跡を終了するには、エスケープ シーケンス（デフォルトではCtrl+^ X）を入力してください。Ctrl キー、Shift キー、および 6 キーを同時に押してから放し、その後 X キーを押します。

関連トピック

IP Traceroute （3139 ページ）
IP traceroute の実行 （3157 ページ）

例：すべてのシステム診断をイネーブルにする

注意 デバッグ出力は他のネットワーク トラフィックより優先され、**debug all** 特権 EXEC コマンドは他の **debug** コマンドより出力が大量になるので、スイッチのパフォーマンスが極度に低下したり、場合によっては使用不能になったりすることがあります。状況にかかわらず、特定性の高い **debug** コマンドを使用するのが原則です。

このコマンドは、すべてのシステム診断をディセーブルにします。

```
Device# debug all
```

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。いずれかの **debug** コマンドが誤ってイネーブルのままにならないようにするには、**no debug all** コマンドを使用すると便利です。

関連トピック

debug コマンド （3141 ページ）

ソフトウェア設定のトラブルシューティングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference (Catalyst 3850 Switches)*』
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*）
Platform_independent の設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S*（*Catalyst 3850 Switches*）

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ソフトウェア設定のトラブルシューティングの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

関連トピック

機能情報の確認 （1 ページ）

第 XX 部

VideoStream

- VideoStream の設定 （3173 ページ）

第 150 章

VideoStream の設定

- 機能情報の確認 （3173 ページ）
- VideoStream の前提条件 （3173 ページ）
- VideoStream の設定に関する制限 （3174 ページ）
- VideoStream について （3174 ページ）
- VideoStream の設定方法 （3174 ページ）
- メディア ストリームの監視 （3179 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VideoStream の前提条件

マルチキャスト機能が有効であることを確認します。コントローラ上の IP マルチキャストは multicast-multicast モードで設定することをお勧めします。

クライアント マシン上の IP アドレスを確認します。マシンには、それぞれの VLAN の IP アドレスが必要です。

アクセス ポイントがコントローラに join していることを確認します。

VideoStream の設定に関する制限

このMC2UC機能を作動させるには、IGMPスヌーピングがオンになっている必要があります。

VideoStream について

IEEE 802.11 ワイヤレス マルチキャスト配信メカニズムには、パケットの消失や破損を認識するための、信頼できる方法がありません。マルチキャスト フレーム パケットは、ワイヤレス クライアントの最適なデータ レートに関係なく、所定のレートで送信されます。結果として、無線配信中にマルチキャスト パケットが消失しても再送されないため、IP マルチキャスト ストリームが表示できなくなることがあります。また、パケットが高速で渡された場合、パケットは輻輳状態になります。

VideoStream 機能では、マルチキャスト フレームをユニキャスト ストリームにワイヤレスで変換することで、IP マルチキャスト ストリームのワイヤレス配信を信頼できるものにします。VideoStream クライアントは、それぞれビデオ IP マルチキャスト ストリームの受信を認識します。

VideoStream の設定方法

メディア ストリームのマルチキャストダイレクトのグローバル設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless multicast**	ワイヤレス転送のマルチキャストをイネーブルにします。
ステップ 3	**IP igmp snooping**	VLAN ごとに IGMP スヌーピングをイネーブルにします。グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。
ステップ 4	**IP igmp snooping querier**	クエリーを生成するマルチキャストルータが VLAN 内に存在しない場合に、イ

	コマンドまたはアクション	目的
		ンターフェイスのスヌーピング クエリアを設定します。
ステップ 5	**wireless media-stream multicast-direct** 例： `(config)#wireless media-stream multicast-direct`	コントローラのグローバルなマルチキャストダイレクト機能を設定します。

ステップ 6	**wireless media-stream message**
	例：
	`(config)#wireless media-stream message ?`
	`Email Configure Session Announcement Email`
	`Notes Configure Session Announcement notes`
	`URL Configure Session Announcement URL`
	`phone Configure Session Announcement Phone number`
	`<cr>`
		電話、URL、電子メール、メモなど、さまざまなメッセージ設定パラメータを設定します。つまり、メディア ストリームが（帯域幅制約が原因で）拒否される場合、メッセージをユーザに送信できます。これらのパラメータは、IT サポートの電子メール アドレス、メモ（ストリームが拒否された理由を説明する画面メッセージ）、ユーザがリダイレクトされる URL、拒否されたストリームについてユーザが問い合わせをする電話番号など、送信するメッセージを設定します。

ステップ 7	**wireless media-stream group**<*name*><*startIp*><*endIp*>
	例：
	`(config)#wireless media-stream group grp1 231.1.1.1 239.1.1.3`
	`(config-media-stream)#?`
	`avg-packet-size Configures average packet size`
	`default Set a command to its defaults`
	`exit Exit sub-mode`
	`max-bandwidth Configures maximum Expected Stream Bandwidth in Kbps`
	`no Negate a command or set its defaults`
	`policy Configure media stream admission policy`
	`qos Configure Over the AIR QoS class, <'video'> ONLY`
	`<cr>`
		予想されるマルチキャスト宛先アドレス、ストリームの帯域幅の使用量およびストリームの優先順位のパラメータなど、各メディア ストリームとそのパラメータを設定します。

ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 帯域のメディア ストリームの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz media-stream multicast-direct** 例： `Device(config)#ap dot11 24ghz media-stream multicast-direct`	メディアストリーム（mc2uc）で 802.11 帯域が使用できる場合に設定します
ステップ 3	**ap dot11 24ghz | 5ghz media-stream video-redirect** 例： `Device(config)#ap dot11 24ghz media-stream video-redirect`	ユニキャスト ビデオ トラフィックをベストエフォートキューにリダイレクトするように設定します。
ステップ 4	**ap dot11 24ghz | 5ghz media-stream multicast-direct admission-besteffort** 例： `Device(config)#ap dot11 24ghz media-stream multicast-direct admission-besteffort`	帯域幅のアベイラビリティの制約によりメディアストリームを優先できない場合でも、メディアストリームがベストエフォートキューを介して送信されるように設定します。帯域幅のアベイラビリティの制約によりメディアストリームを優先できない場合、**no** をコマンドに追加して、ストリームをドロップします。
ステップ 5	**ap dot11 24ghz | 5ghz media-stream multicast-direct client-maximum [<value>]** 例： `Device(config)#ap dot11 24ghz media-stream multicast-direct client-max 15`	個々のクライアントごとに許可されたメディアストリームの最大数を設定します。最大値は 15 で、デフォルトは 0 です。値 0 は、無制限のストリームを意味します。
ステップ 6	**ap dot11 24ghz | 5ghz media-stream multicast-direct radio-maximum 20**	無線ストリームの最大数を設定します。有効な範囲は 1 ～ 20 です。デフォルトは 0 です。値 0 は、無制限のストリームを意味します。

	コマンドまたはアクション	目的
ステップ 7	**ap dot11 24ghz | 5ghz cac multimedia max-bandwidth [<bandwidth>]** 例： `Device(config)#ap dot11 24ghz cac multimedia max-bandwidth 60`	最大メディア（音声およびビデオ）帯域幅を % 単位で設定します。範囲は 5 % ～ 85 % です。
ステップ 8	**ap dot11 24ghz | 5ghz cac media-stream multicast-direct min_client_rate [<dot11_rate>]** 例： `Device(config)#ap dot11 24ghz cac media-stream multicast-direct min_client_rate`	クライアントがユニキャストとしてメディアストリームを送信するために必要な最小PHY レートを設定します。これよりも低いレートで通信するクライアントは、メディアストリームをユニキャストフローとして受信しません。通常、このPHY レートは、マルチキャストフレームが送信されるレートと同じかそれ以上です。
ステップ 9	**ap dot11 5ghz cac media-stream**	メディア ストリーム アクセス カテゴリの CAC パラメータを設定します。
ステップ 10	**ap dot11 5ghz cac multimedia**	音声およびビデオに使用されるメディア アクセス カテゴリの CAC パラメータを設定します。
ステップ 11	**ap dot11 5ghz cac video**	音声シグナリングに使用されるビデオ アクセス カテゴリの CAC パラメータを設定します。
ステップ 12	**ap dot11 5ghz cac voice**	音声アクセスカテゴリのCACパラメータを設定します。
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

ビデオ ストリーミング用の WLAN 設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wlan** *wlan_name* 例： `(config)#wlan wlan50`	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**shutdown** 例： `(config-wlan)#shutdown`	パラメータを設定するために、WLAN をディセーブルにします。
ステップ 4	**media-stream multicast-direct** 例： `(config)#media-stream multicast-direct`	メディア ストリームのマルチキャスト ダイレクト機能を WLAN で設定します。
ステップ 5	**no shutdown** 例： `(config-wlan)#no shutdown`	WLAN をイネーブルにします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

メディア ストリームの削除

始める前に

メディア ストリームをイネーブルにしてから、削除を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no wireless media-stream group media_stream_name** 例： `Device(config)#no wireless media-stream grp1`	コマンドで指定する名前を持つメディア ストリームを削除します。
ステップ 3	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config)# end`	ンフィギュレーション モードを終了できます。

メディア ストリームの監視

表 *214 :* メディア ストリームの監視用のコマンド

コマンド	説明
show wireless media-stream client detail *group name*	特定のグループのメディア ストリーム クライアントの詳細を表示します。
show wireless media-stream client summary	すべてのクライアントのメディア ストリーム情報を表示します。
show wireless media-stream group detail *group name*	特定のグループのメディア ストリーム設定の詳細を表示します。
show wireless media-stream group summary	すべてのグループのメディア ストリーム設定の詳細を表示します。
show wireless media-stream message details	セッション通知メッセージの詳細を表示します。
show wireless multicast	マルチキャストダイレクト設定の状態を表示します。
show ap dot11 24ghz | 5ghz media-stream rrc	802.11 メディアのリソース予約コントロールの設定を表示します。

第 XXI 部

VLAN

- VTP の設定 （3183 ページ）
- VLAN の設定 （3211 ページ）
- VLAN グループの設定 （3233 ページ）
- VLAN トランクの設定 （3241 ページ）
- 音声 VLAN の設定 （3263 ページ）
- プライベート VLAN の設定 （3275 ページ）

第 151 章

VTP の設定

- 機能情報の確認 （3183 ページ）
- VTP の前提条件 （3183 ページ）
- VTP の制約事項 （3184 ページ）
- VTP の概要 （3185 ページ）
- VTP の設定方法 （3195 ページ）
- VTP のモニタ （3206 ページ）
- VTP の設定例 （3206 ページ）
- 次の作業 （3207 ページ）
- その他の参考資料 （3207 ページ）
- VTP の機能履歴と情報 （3209 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VTP の前提条件

VLAN を作成する前に、ネットワークで VLAN Trunking Protocol（VTP）を使用するかどうかを決定する必要があります。VTP を使用すると、1 つまたは複数のデバイス上で中央集約的に設定変更を行い、その変更を自動的にネットワーク上の他のデバイスに伝達できます。VTP を使用しない場合、VLAN 情報を他のデバイスに送信することはできません。

VTP は、1 つのデバイスで行われた更新が VTP を介してドメイン内の他のデバイスに送信される環境で動作するように設計されています。VLAN データベースに対する複数の更新が同一ドメイン内のデバイス上で同時に発生する環境の場合、VTP は適切に機能せず、VLAN データベースの不整合が生じます。

デバイスは合計 4094 の VLAN をサポートします。ただし、設定済み機能の個数によって、デバイス ハードウェアの使用状況は左右されます。VTP が新しい VLAN をデバイスに通知し、デバイスが使用可能な最大限のハードウェア リソースをすでに使用している場合、コントローラはハードウェア リソース不足を伝えるメッセージを送信して、VLAN をシャットダウンします。**show vlan** ユーザ EXEC コマンドの出力に、サスペンド ステートの VLAN が示されます。

トランク ポートは VTP アドバタイズを送受信するので、デバイスまたはデバイス スタック上で少なくとも 1 つのトランクポートが設定されており、そのトランク ポートが別のデバイスのトランク ポートに接続されていることを確認する必要があります。そうでない場合、デバイスは VTP アドバタイズを受信できません。

関連トピック

VTP アドバタイズ （3188 ページ）
VTP ドメインへの VTP クライアント の追加（CLI） （3204 ページ）
VTP Domain （3185 ページ）
VTP モード （3186 ページ）

VTP の制約事項

次に、VTP に関する制約事項を示します。

- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むデバイス スタックを含めることはできません。

⚠

注意 VTP クライアント デバイスを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のデバイスのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のデバイスは常に、VTP コンフィギュレーション リビジョン番号が最大のデバイスの VLAN コンフィギュレーションを使用します。VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つデバイスを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。

VTP の概要

VTP

VTP は、レイヤ 2 のメッセージ プロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。VTP により、VLAN 名の重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。

VTP 機能はスタック全体でサポートされており、スタック内のすべてのデバイスが、アクティブ デバイスから継承した同一の VLAN および VTP コンフィギュレーションを保持します。デバイスが VTP メッセージを通じて新しい VLAN について学習したり、ユーザが新しい VLAN を設定したりすると、新しい VLAN 情報がスタック内のすべてのデバイスに伝達されます。

デバイスがスタックに参加するか、またはスタックの結合が発生すると、新しいデバイスはアクティブ デバイスから VTP 情報を取得します。

VTP Domain

VTP ドメイン（別名 VLAN 管理ドメイン）は、1 つのデバイス、または同じ VTP ドメイン名を共有して同一管理下にある相互接続された複数のデバイスまたはデバイススタックで構成されます。デバイスは、1 つの VTP ドメインにだけ所属できます。そのドメインに対してグローバル VLAN の設定を変更します。

デフォルトの設定では、トランク リンク（複数 VLAN のトラフィックを伝送するリンク）を介してドメインについてのアドバタイズを受信しない限り、またはユーザがドメイン名を設定しない限り、デバイスは VTP 非管理ドメイン ステートです。管理ドメイン名を指定するか学習するまでは、VTP サーバ上で VLAN を作成または変更できません。また、VLAN 情報はネットワークを介して伝播されません。

デバイスが、トランク リンクを介して VTP アドバタイズを受信した場合、管理ドメイン名および VTP 設定のリビジョン番号を継承します。その後デバイスは、別のドメイン名または古いコンフィギュレーション リビジョン番号が指定されたアドバタイズについては、すべて無視します。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのデバイスに伝播されます。VTP アドバタイズは、IEEE 802.1Q を含め、すべての IEEE トランク接続に送信されます。VTP は、複数の LAN タイプにわたり、固有の名前と内部インデックスの対応によって VLAN を動的にマッピングします。このマッピングにより、ネットワーク管理者がデバイスを管理するための作業負担が大幅に軽減されます。

VTP トランスペアレント モードでデバイスを設定した場合、VLAN の作成および変更は可能ですが、その変更はドメイン内の他のデバイスには送信されません。また、変更が作用するのは、個々のデバイスに限られます。ただし、デバイスがこのモードのときに設定を変更すると、変更内容がデバイスの実行コンフィギュレーションに保存されます。この変更はデバイスのスタートアップ コンフィギュレーション ファイルに保存することもできます。

関連トピック

VTP ドメインへの VTP クライアント の追加（CLI） （3204 ページ）
VTP の前提条件 （3183 ページ）
セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング（3296 ページ）
例：セカンダリ VLANをプライマリ VLANインターフェイスにマッピングする （3301 ページ）

VTP モード

表 *215 : VTP* モード

VTP モード	説明
VTP サーバ	VTP サーバ モードでは、VLAN の作成、変更、削除ができます。また、VTP ドメイン全体に対して他のコンフィギュレーション パラメータ（VTP バージョンなど）を指定できます。VTP サーバは、同一 VTP ドメイン内の他のデバイスに自身の VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズに基づいて、自身の VLAN 設定を他のデバイスと同期させます。 VTP サーバがデフォルトのモードです。 VTP サーバ モードでは、VLAN 設定は NVRAM に保存されます。デバイスがコンフィギュレーションを NVRAM に書き込んでいる間に障害を検出すると、VTP モードはサーバ モードからクライアント モードに自動的に移行します。この場合、NVRAM が正常に動作するまで、デバイスを VTP サーバ モードに戻すことはできません。

VTP モード	説明
VTP クライアント	VTP クライアントは VTP サーバと同様に機能し、そのトランクで VTP アップデートを送受信しますが、VTP クライアント上で VLAN の作成、変更、削除を行うことはできません。VLAN は、ドメインに含まれる、他のサーバモードのデバイスで設定します。 VTP バージョン 1 および 2 の VTP クライアント モードでは、VLAN 設定は NVRAM に保存されません。VTP バージョン 3 では、VLAN 設定はクライアント モードで NVRAM に保存されます。
VTP トランスペアレント	VTP トランスペアレント デバイスは、VTP に参加しません。VTP トランスペアレント デバイスは自身の VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて自身の VLAN 設定を同期させることもありません。ただし、VTP バージョン 2 またはバージョン 3 では、トランスペアレントデバイスは、トランク インターフェイスを介して他のデバイスから受信した VTP アドバタイズを転送します。VTP トランスペアレント モードでは、デバイス上の VLAN を作成、変更、削除できます。 デバイスが VTP トランスペアレント モードの場合、VTP および VLAN の設定は NVRAM に保存されますが、他のデバイスにはアドバタイズされません。このモードでは、VTP モードおよびドメイン名はデバイスの実行コンフィギュレーションに保存されます。この情報をデバイスのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。 デバイススタックでは、実行コンフィギュレーションと保存されているコンフィギュレーションは、スタック内のすべてのデバイスについて同じです。
VTP オフ	VTP オフ モードでのデバイスの機能は、トランクを介して VTP アドバタイズを転送しないことを除くと VTP トランスペアレント デバイスとしての機能と同じです。

関連トピック

VTP の前提条件 （3183 ページ）
VTP モードの設定（CLI） （3195 ページ）

VTP アドバタイズ

VTP ドメイン内の各デバイスは、専用のマルチキャスト アドレスに対して、それぞれのトランク ポートからグローバル コンフィギュレーション アドバタイズを定期的に送信します。ネイバーデバイスは、このようなアドバタイズを受信し、必要に応じて各自のVTPおよびVLAN設定をアップデートします。

VTP アドバタイズにより、次のグローバル ドメイン情報が配信されます。

- VTP ドメイン名
- VTP 設定のリビジョン番号
- アップデート ID およびアップデート タイムスタンプ
- 各 VLAN の最大伝送単位（MTU）サイズを含む MD5 ダイジェスト VLAN コンフィギュレーション
- フレーム形式

VTP アドバタイズではさらに、設定されている各 VLAN について、次の VLAN 情報が配信されます。

- VLAN ID（IEEE 802.1Q を含む）
- VLAN 名
- VLAN タイプ
- VLAN ステート
- VLAN タイプ固有のその他の VLAN 設定情報

VTP バージョン 3 では、VTP アドバタイズにはプライマリ サーバ ID、インスタンス番号、および開始インデックスも含まれます。

関連トピック

VTP の前提条件 （3183 ページ）

VTP バージョン 2

ネットワークで VTP を使用する場合、VTP のどのバージョンを使用するかを決定する必要があります。デフォルトでは、バージョン 1 の VTP が動作します。

VTP バージョン 1 でサポートされず、バージョン 2 でサポートされる機能は、次のとおりです。

- トークンリング サポート：VTP バージョン 2 は、トークンリング ブリッジ リレー機能（TrBRF）およびトークンリング コンセントレータ リレー機能（TrCRF）VLAN をサポートします。
- 認識不能な Type-Length-Value（TLV）のサポート：VTP サーバまたは VTP クライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。認識されなかった TLV は、デバイスが VTP サーバ モードで動作している場合、NVRAM に保存されます。
- バージョン依存型トランスペアレント モード：VTP バージョン 1 の場合、VTP トランスペアレントデバイスがVTPメッセージ中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限りメッセージを転送します。VTPバージョン2がサポートするドメインは 1 つだけですが、VTP バージョン 2 トランスペアレント デバイスは、ドメイン名が一致した場合のみメッセージを転送します。
- 整合性検査：VTP バージョン 2 では、CLI または SNMP を介して新しい情報が入力された場合に限り、VLAN整合性検査（VLAN名、値など）を行います。VTPメッセージから新しい情報を取得した場合、またはNVRAMから情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

関連トピック

VTP バージョンのイネーブル化（CLI）　（3199 ページ）

VTP バージョン 3

VTP バージョン 1 または 2 でサポートされず、バージョン 3 でサポートされる機能は、次のとおりです。

- 拡張認証：認証を **hidden** または **secret** として設定できます。設定を **hidden** にしている場合、パスワード文字列からの秘密キーは VLAN のデータベース ファイルに保存されますが、設定においてプレーンテキストで表示されることはありません。代わりに、パスワードに関連付けられているキーが 16 進表記で実行コンフィギュレーションに保存されます。ドメインにテイクオーバー コマンドを入力するときは、パスワードを再入力する必要があります。キーワード **secret** を入力する場合、パスワードに秘密キーを直接設定できます。
- 拡張範囲 VLAN （VLAN 1006 ～ 4094）データベース伝播のサポート：VTP バージョン 1 および 2 では VLAN 1 ～ 1005 だけが伝播されます。

（注）　VTP プルーニングは引き続き VLAN 1 ～ 1005 にだけ適用され、VLAN 1002 ～ 1005 は予約されたままで変更できません。

- ドメイン内のデータベースのサポート：VTP 情報の伝播に加え、バージョン 3 では、Multiple Spanning Tree（MST）プロトコル データベース情報も伝播できます。VTP プロトコルの個別インスタンスが VTP を使用する各アプリケーションで実行されます。

- VTP プライマリ サーバと VTP セカンダリ サーバ：VTP プライマリ サーバは、データベース情報を更新し、システム内のすべてのデバイスに適用されるアップデートを送信します。VTP セカンダリ サーバで実行できるのは、プライマリ サーバから NVRAM に受け取ったアップデート済み VTP コンフィギュレーションのバックアップだけです。

  デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。**vtp primary** 特権 EXEC コマンドを入力してプライマリ サーバを指定することができます。プライマリ サーバのステータスは、管理者がドメインでテイクオーバー メッセージを発行する場合、データベースのアップデート用に必要となるだけです。プライマリ サーバなしで実用 VTP ドメインを持つことができます。プライマリ サーバのステータスは、デバイスにパスワードが設定されている場合でも、装置がリロードしたり、ドメインのパラメータが変更したりすると失われます。

- VTP をトランク単位（ポート単位）でオンまたオフにするオプション：ポート単位で VTP をイネーブルまたはディセーブルにするには、**[no] vtp** インターフェイス コンフィギュレーション コマンドを入力します。トランク ポート上で VTP をディセーブルにすると、そのポートのすべての VTP インスタンスがディセーブルになります。VTP の設定を、MST データベースには *off* にする一方で、同じポートの VLAN データベースには *on* にすることはできません。

  グローバルに VTP モードをオフに設定すると、システムのすべてのトランク ポートにこの設定が適用されます。ただし、VTP インスタンス ベースでこのモードのオンまたはオフを指定することはできます。たとえば、VLAN データベースには、デバイスを VTP サーバとして設定する一方で、MST データベースには VTP を *off* に設定することができます。

関連トピック

VTP バージョンのイネーブル化（CLI）　（3199 ページ）

VTP プルーニング

VTP プルーニングを使用すると、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されるので、使用可能なネットワーク帯域幅が増えます。VTP プルーニングを使用しない場合、デバイスは受信側のデバイスで廃棄される可能性があっても、VTP ドメイン内のすべてのトランク リンクに、ブロードキャスト、マルチキャスト、および不明のユニキャスト トラフィックをフラッディングします。VTP プルーニングはデフォルトでディセーブルです。

VTP プルーニングは、プルーニング適格リストに指定された VLAN トランク ポートへの不要なフラッディング トラフィックを阻止します。プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトでは、デバイスのトランク ポート上で VLAN 2 ～ 1001 がプルーニング適格です。プルーニング不適格として設定した VLAN については、引き続きフラッディングが行われます。VTP プルーニングはすべてのバージョンの VTP でサポートされます。

図 *145 : VTP* プルーニングを使用しない場合のフラッディング トラフィック

VTP プルーニングは、スイッチド ネットワークでは無効です。デバイス A のポート 1 および デバイス D のポート 2 は、Red という VLAN に割り当てられています。デバイス A に接続さ

れたホストからブロードキャストが送信された場合、デバイスAは、このブロードキャストをフラッディングします。Red VLAN にポートを持たないデバイス C、E、F も含めて、ネットワーク内のすべてのデバイスがこのブロードキャストを受信します。

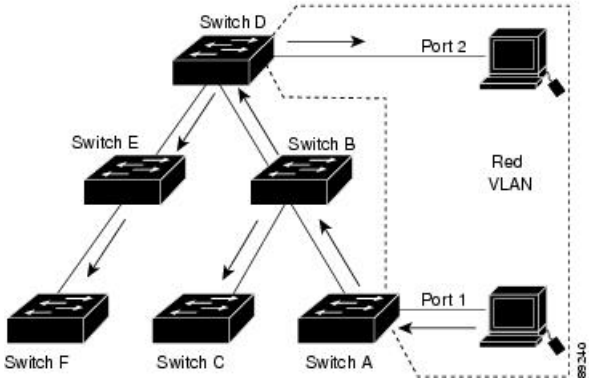
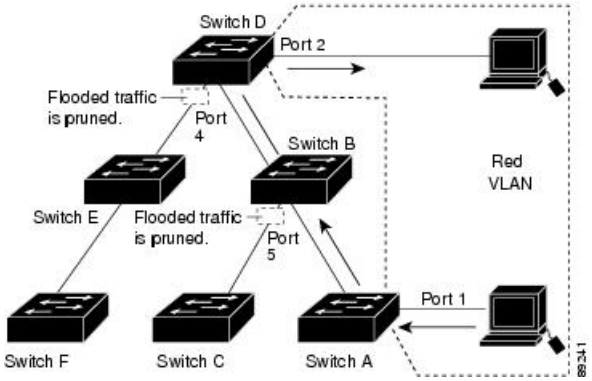


図 *146 : VTP* プルーニングによるフラッディング トラフィックの最適化

VTPプルーニングは、スイッチドネットワークでは有効です。デバイスAからのブロードキャスト トラフィックは、デバイス C、E、F には転送されません。図に示されているリンク ポート（デバイス B のポート 5、およびデバイス D のポート 4）で、Red VLAN のトラフィックがプルーニングされるからです。



VTP バージョン 1 および 2 では、VTP サーバでプルーニングをイネーブルにすると、その VTP ドメイン全体でプルーニングがイネーブルになります。VTP バージョン 3 では、ドメイン内の各デバイス上で手動によってプルーニングを有効にする必要があります。VLAN をプルーニング適格または不適格として設定する場合、影響を受けるのは、そのトランク上の VLAN のプルーニングだけです（VTP ドメイン内のすべてのデバイスに影響するわけではありません）。

VTP プルーニングは、イネーブルにしてから数秒後に有効になります。VTP プルーニング不適格の VLAN からのトラフィックは、プルーニングの対象になりません。VLAN 1 および VLAN 1002 ～ 1005 は常にプルーニング不適格です。これらの VLAN からのトラフィックはプルーニングできません。拡張範囲 VLAN（1005 を超える VLAN ID）もプルーニング不適格です。

関連トピック

VTP プルーニングのイネーブル化（CLI）　（3201 ページ）

VTP とデバイス スタック

VTP 設定は、デバイス スタックのすべてのメンバで同一です。デバイス スタックが VTP サーバ、クライアント、またはトランスペアレントモードになっている場合、スタック内のすべてのデバイスの VTP 設定が同一になります。

- スタックに参加したデバイスは、VTP および VLAN のプロパティをアクティブなスイッチから継承します。
- すべての VTP アップデートが、スタック全体で保持されます。
- スタック内のデバイスの VTP モードが変更されると、そのスタック内のその他のデバイスも VTP モードを変更し、デバイスの VLAN データベースの一貫性が保たれます。

VTP バージョン 3 は、スタンドアロン デバイスでもスタックでも同じように機能しますが、デバイス スタックが VTP データベースのプライマリ サーバである場合だけは例外です。この場合は、アクティブなスイッチの MAC アドレスがプライマリ サーバ ID として使用されます。アクティブなデバイスがリロードされるか電源オフになると、新たにアクティブなスイッチが選択されます。

- 固定 MAC アドレス機能を設定しない場合、新たにアクティブなデバイスが選択されると、現在のスタック MAC アドレスを使用してテイクオーバー メッセージを送信します。

（注） デフォルトでは、永続的 MAC アドレスがオンになっています。

VTP 設定時の注意事項

VTP の設定要件

VTP を設定する場合は、デバイスがドメイン内の他のデバイスと VTP アドバタイズを送受信できるように、トランク ポートを設定する必要があります。

VTP の設定

VTP 情報は VTP VLAN データベースに保存されます。VTP モードがトランスペアレントである場合、VTP ドメイン名およびモードはデバイスの実行コンフィギュレーション ファイルにも保存されます。この情報をデバイスのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。デバイスをリセットした場合にも、VTP モードをトランスペアレントとして保存するには、このコマンドを使用する必要があります。

デバイスのスタートアップ コンフィギュレーション ファイルに VTP 情報を保存して、デバイスを再起動すると、デバイスの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーショ

ン ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。

- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

関連トピック

ポート単位の VTP の設定（CLI）（3202 ページ）
VTP バージョン 3 のプライマリ サーバの設定（CLI）（3199 ページ）

VTP 設定のためのドメイン名

VTP を初めて設定するときは、必ずドメイン名を割り当てる必要があります。また、VTP ドメイン内のすべてのデバイスを、同じドメイン名で設定しなければなりません。VTP トランスペアレント モードのデバイスは、他のデバイスと VTP メッセージを交換しません。これらのコントローラについては VTP ドメイン名を設定する必要はありません。

（注） NVRAM および DRAM の記憶域が十分にある場合は、VTP ドメイン内のすべてのデバイスを VTP サーバ モードにする必要があります。

注意 すべてのデバイスが VTP クライアント モードで動作している場合は、VTP ドメインを設定しないでください。ドメインを設定すると、そのドメインの VLAN 設定を変更できなくなります。VTP ドメイン内の少なくとも 1 台のデバイスを VTP サーバ モードに設定してください。

関連トピック

VTP ドメインへの VTP クライアント の追加（CLI）（3204 ページ）

VTP ドメインのパスワード

VTP ドメインのパスワードは設定できますが、必須ではありません。ドメイン パスワードを設定する場合は、すべてのドメインデバイスで同じパスワードを共有し、管理ドメイン内のデバイスごとにパスワードを設定する必要があります。パスワードのないデバイス、またはパスワードが不正なコントローラは、VTP アドバタイズを拒否します。

ドメインに VTP パスワードを設定する場合、VTP 設定なしで起動したデバイスは、正しいパスワードを使用して設定しない限り、VTP アドバタイズを受信しません。設定後、デバイスは同じパスワードおよびドメイン名を使用した次の VTP アドバタイズを受信します。

VTP 機能を持つ既存のネットワークに新しいデバイスを追加した場合、その新しいデバイスに適切なパスワードを設定して初めて、そのコントローラはドメイン名を学習します。

⚠

注意 VTP ドメイン パスワードを設定したにもかかわらず、ドメイン内の各デバイスに管理ドメイン パスワードを割り当てなかった場合には、管理ドメインが正常に動作しません。

関連トピック

VTP バージョン 3 のパスワードの設定（CLI） （3197 ページ）
例：スイッチをプライマリ サーバとして設定する （3206 ページ）

VTP バージョン

実装する VTP バージョンを決定する場合は、次の注意事項に従ってください。

- VTP ドメイン内のすべてのデバイスは同じドメイン名を使用する必要がありますが、すべてが同じ VTP バージョンを実行する必要はありません。
- VTP バージョン 2 対応のデバイス上で VTP バージョン 2 がディセーブルに設定されている場合、VTP バージョン 2 対応デバイスは、VTP バージョン 1 を実行しているデバイスと同じ VTP ドメインで動作できます（デフォルトでは VTP バージョン 2 はディセーブルになっています）。
- VTP バージョン 1 を実行しているものの、VTP バージョン 2 に対応可能なデバイスが VTP バージョン 3 アドバタイズを受信すると、このコントローラは VTP バージョン 2 に自動的に移行します。
- VTP バージョン 3 を実行しているデバイスが VTP バージョン 1 を実行しているデバイスに接続すると、VTP バージョン 1 のデバイスは VTP バージョン 2 に移行し、VTP バージョン 3 のデバイスは、スケールダウンしたバージョンの VTP パケットを送信するため、VTP バージョン 2 デバイスは自身のデータベースをアップデートできます。
- VTP バージョン 3 を実行するデバイスは、拡張 VLAN を持つ場合はバージョン 1 または 2 に移行できません。
- 同一 VTP ドメイン内のすべてのデバイスがバージョン 2 に対応可能な場合を除いて、デバイス上で VTP バージョン 2 をイネーブルにしないでください。1 つのデバイスでバージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応デバイスでバージョン 2 がイネーブルになります。バージョン 1 専用のデバイスがドメインに含まれている場合、そのコントローラはバージョン 2 対応デバイスとの間で VTP 情報を交換できません。
- VTP バージョン 1 および 2 デバイスは、VTP バージョン 3 アドバタイズメントを転送できないため、ネットワークのエッジに配置することをお勧めします。
- 使用環境に TrBRF および TrCRF トークンリング ネットワークが含まれている場合に、トークンリング VLAN スイッチング機能を正しく動作させるには、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net を実行する場合は、VTP バージョン 2 をディセーブルにします。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN（VLAN 1006 ～ 4094）の設定情報を伝播しません。これらの VLAN は各装置で手動によって設定する必要があります。

VTP バージョン 3 は拡張範囲 VLAN と、拡張範囲 VLAN データベースの伝播をサポートします。

- VTP バージョン 3 装置のトランク ポートが VTP バージョン 2 装置からのメッセージを受信した場合、この装置は、VLANデータベースをスケールダウンし、その特定のトランク上で VTP バージョン 2 フォーマットを使用して送信します。VTP バージョン 3 装置は、最初にそのトランク ポートで VTP バージョン 2 パケットを受信しない限り、VTP バージョン 2 フォーマットのパケットを送信しません。
- VTP バージョン 3 装置が、あるトランク ポートで VTP バージョン 2 装置を検出した場合、両方のネイバーが同一トランク上で共存できるように、VTPバージョン2パケットだけでなく VTP バージョン 3 パケットの送信も継続します。
- VTP バージョン 3 装置は、VTP バージョン 2 またはバージョン 1 の装置からの設定情報は受け入れません。
- 2 つの VTP バージョン 3 リージョンは、VTP バージョン 1 リージョンまたはバージョン 2 リージョンでは、トランスペアレント モードでだけ通信できます。
- VTP バージョン 1 にだけ対応する装置は、VTP バージョン 3 装置との相互運用はできません。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN（VLAN 1006 ～ 4094）の設定情報を伝播しません。これらの VLAN を各装置上に手動で設定する必要があります。

関連トピック

VTP バージョンのイネーブル化（CLI）　（3199 ページ）

VTP の設定方法

VTP モードの設定（CLI）

次のいずれかに VTP モードを設定できます。

- VTP サーバ モード：VTP サーバ モードでは、VLAN の設定を変更し、ネットワーク全体に伝播させることができます。
- VTP クライアント モード：VTP クライアント モードでは、VLAN の設定を変更できません。クライアント デバイスは、VTP ドメイン内の VTP サーバから VTP アップデート情報を受信し、それに基づいて設定を変更します。
- VTP トランスペアレント モード：VTP トランスペアレント モードでは、デバイスで VTP がディセーブルになります。デバイスは VTP アップデートを送信せず、他のデバイスから受信した VTP アップデートにも反応しません。ただし、VTP バージョン 2 を実行する VTP トランスペアレント モードのデバイスは、対応するトランク リンクで、受信した VTP アドバタイズを転送します。

- VTP オフ モード：VTP オフ モードは、VTP アドバタイズが転送されない以外は、VTP トランスペアレント モードと同じです。

設定したドメイン名は、削除できません。別のドメインにデバイスを再び割り当てるしかありません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp domain** *domain-name* 例： `Device(config)# vtp domain eng_group`	VTP 管理ドメイン名を設定します。1～32 文字の名前を使用できます。同一管理下にある VTP サーバ モードまたはクライアント モードのデバイスは、すべて同じドメイン名に設定する必要があります。 サーバ モード以外にはこのコマンドは任意です。VTP サーバ モードではドメイン名が必要です。デバイスが VTP ドメインにトランク接続されている場合、デバイスはドメイン内の VTP サーバからドメイン名を取得します。 他の VTP パラメータを設定する前に、VTP ドメインを設定する必要があります。
ステップ 4	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**} 例： `Device(config)# vtp mode server`	VTP モード（クライアント、サーバ、トランスペアレント、またはオフ）のデバイスの設定。 • **vlan**：何も設定されていない場合は VLAN データベースがデフォルトです。

	コマンドまたはアクション	目的
		• **mst**：マルチ スパニング ツリー（MST）データベース。 • **unknown**：データベース タイプは不明です。
ステップ 5	**vtp password** *password* 例： `Device(config)# vtp password mypassword`	（任意）VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ～ 64 文字です。VTP パスワードを設定したにもかかわらず、ドメイン内の各デバイスに同じパスワードを割り当てなかった場合には、VTP ドメインが正常に動作しません。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show vtp status** 例： `Device# show vtp status`	表示された *[VTP Operating Mode]* および *[VTP Domain Name]* フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）スタートアップ コンフィギュレーション ファイルに設定を保存します。 デバイスの実行コンフィギュレーションに保存され、スタートアップ コンフィギュレーション ファイルにコピーできるのは、VTP モードおよびドメイン名だけです。

関連トピック

VTP モード （3186 ページ）

VTP バージョン 3 のパスワードの設定（CLI）

デバイスで VTP バージョン 3 のパスワードを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp password** *password* [**hidden** | **secret**] 例： `Device(config)# vtp password mypassword hidden`	（任意）VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ～ 64 文字です。 • （任意）**hidden**：パスワード文字列から生成される秘密キーが、nvram:vlan.dat ファイルに保存されます。VTP プライマリ サーバを設定してテイクオーバーを設定しようとすると、パスワードの再入力を要求されます。 • （任意）**secret**：パスワードを直接設定します。シークレットパスワードには16進数文字を32個含める必要があります。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp password** 例： `Device# show vtp password`	入力を確認します。次のような出力が表示されます。 VTP password: 89914640C8D90868B6A0D8103847A733
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

関連トピック

VTP ドメインのパスワード （3193 ページ）
例：スイッチをプライマリ サーバとして設定する （3206 ページ）

VTP バージョン 3 のプライマリ サーバの設定（CLI）

VTP サーバを VTP プライマリ サーバとして設定すると、テイクオーバー操作が開始されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**vtp primary** [**vlan** | **mst**] [**force**] 例： `Device# vtp primary vlan force`	デバイスの動作ステートをセカンダリ サーバ（デフォルト）からプライマリ サーバに変更し、その設定をドメインにアドバタイズします。デバイスのパスワードが **hidden** に設定されている場合は、パスワードの再入力を要求されます。 • （任意）**vlan**：テイクオーバー機能として VLAN データベースを選択します。これはデフォルトです。 • （任意）**mst**：テイクオーバー機能としてマルチ スパニング ツリー（MST）データベースを選択します。 • （任意）**force**：競合するサーバの設定が上書きされます。**force** を入力しない場合、テイクオーバーの実行前に確認を求められます。

関連トピック

VTP の設定 （3192 ページ）

VTP バージョンのイネーブル化（CLI）

デフォルトで VTP バージョン 2 およびバージョン 3 はディセーブルになっています。

- 1 つのデバイス上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内の VTP バージョン 2 に対応可能なすべてのデバイスでバージョン 2 がイネーブルになります。VTP バージョン 3 をイネーブルにするには、各デバイス上で手動によって設定する必要があります。
- VTP バージョン 1 および 2 では、このバージョンを設定できるのは、VTP サーバ モードまたはトランスペアレント モードのデバイスだけです。デバイスが VTP バージョン 3 を実行し、かつデバイスがクライアント モードの場合、既存の拡張 VLAN がなく、パスワードが非表示に設定されていないときであれば、バージョン 2 に変更できます。

  注意 同一 VTP ドメイン内のデバイス上で、VTP バージョン 1 と VTP バージョン 2 は相互運用できません。VTP ドメイン内のすべてのデバイスが VTP バージョン 2 をサポートしている場合を除き、VTP バージョン 2 をイネーブルにはしないでください。

- TrCRF および TrBRF トークンリング環境では、トークンリング VLAN スイッチング機能を正しく動作させるために、VTP バージョン 2 または VTP バージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net メディアの場合は、VTP バージョン 2 をディセーブルにします。
- **注意** VTP バージョン 3 では、プライマリ サーバとセカンダリ サーバの両方がドメイン内の 1 つのインスタンスに存在できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp version {1 | 2 | 3}** 例： `Device(config)# vtp version 2`	デバイスで VTP バージョンをイネーブルにします。デフォルトは VTP バージョン 1 です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例： `Device# show vtp status`	設定された VTP バージョンがイネーブルであることを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VTP バージョン （3194 ページ）
VTP バージョン 2 （3188 ページ）
VTP バージョン 3 （3189 ページ）

VTP プルーニングのイネーブル化（CLI）

始める前に

VTP プルーニングは VTP トランスペアレント モードでは機能しないように設計されています。ネットワーク内に VTP トランスペアレント モードのデバイスが 1 台または複数存在する場合は、次のいずれかの操作を実行する必要があります。

- ネットワーク全体の VTP プルーニングをオフにします。
- VTP トランスペアレントデバイスのアップストリーム側にあるデバイスのトランク上で、すべての VLAN をプルーニング不適格にすることによって、VTP プルーニングをオフにします。

インターフェイスに VTP プルーニングを設定するには、**switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します。VTP プルーニングは、インターフェイスがトランキングを実行している場合に作用します。VLAN プルーニングの適格性は、VTP ドメインで VTP プルーニングがイネーブルであるかどうか、特定の VLAN が存在するかどうか、およびインターフェイスが現在トランキングを実行しているかどうかにかかわらず、設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp pruning** 例： `Device(config)# vtp pruning`	VTP 管理ドメインでプルーニングをイネーブルにします。 プルーニングは、デフォルトではディセーブルに設定されています。VTP サーバ モードの 1 台のデバイス上に限ってプルーニングをイネーブルにする必要があります。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例： `Device# show vtp status`	表示された [VTP Pruning Mode] フィールドの設定を確認します。

関連トピック

VTP プルーニング （3190 ページ）

ポート単位の VTP の設定（CLI）

VTP バージョン 3 では、ポート単位で VTP をイネーブルまたはディセーブルにできます。VTP は、トランク モードのポート上でだけイネーブルにできます。VTP トラフィックの着信または発信はブロックされ、転送されません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**vtp** 例： `Device(config)# vtp`	指定したポートの VTP をイネーブルにします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet1/0/1`	ポートの変更を確認します。
ステップ 7	**show vtp status** 例： `Device# show vtp status`	設定を確認します。

関連トピック

VTP の設定 （3192 ページ）

VTP ドメインへの VTP クライアント の追加（CLI）

VTP ドメインに追加する前にデバイス上で VTP コンフィギュレーション リビジョン番号を確認およびリセットするには、次の手順に従います。

始める前に

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のデバイスのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のデバイスは常に、VTP コンフィギュレーション リビジョン番号が最大のデバイスの VLAN コンフィギュレーションを使用します。VTP バージョン 1 および 2 では、VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つデバイスを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP バージョン 3 では、VLAN 情報が消去されることはありません。

デバイス上で VTP をディセーブルにし、VTP ドメイン内の他のデバイスに影響を与えることなく VLAN 情報を変更するには、**vtp mode transparent** グローバル コンフィギュレーション コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show vtp status** 例： `Device# show vtp status`	VTP コンフィギュレーション リビジョン番号をチェックします。 番号が 0 の場合は、デバイスを VTP ドメインに追加します。 番号が 0 より大きい場合は、次の手順に従います。 • ドメイン名を書き留めます。 • コンフィギュレーション リビジョン番号を書き留めます。 • 次のステップに進んで、デバイスのコンフィギュレーション リビジョン番号をリセットします。
ステップ 3	**configureterminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 4	**vtp domain** *domain-name* 例： `Device(config)# vtp domain domain123`	ドメイン名を、ステップ 1 で表示された元の名前から新しい名前に変更します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。デバイスの VLAN 情報が更新され、コンフィギュレーション リビジョン番号が 0 にリセットされます。
ステップ 6	**show vtp status** 例： `Device# show vtp status`	コンフィギュレーション リビジョン番号が 0 にリセットされていることを確認します。
ステップ 7	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 8	**vtp domain** *domain-name* 例： `Device(config)# vtp domain domain012`	デバイスの元のドメイン名を開始します。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。デバイスの VLAN 情報が更新されます。
ステップ 10	**show vtp status** 例： `Device# show vtp status`	（任意）ドメイン名がステップ 1 のものと同じであり、コンフィギュレーション リビジョン番号が 0 であることを確認します。

関連トピック

VTP Domain （3185 ページ）

VTP の前提条件 （3183 ページ）
VTP 設定のためのドメイン名 （3193 ページ）

VTP のモニタ

ここでは、VTP の設定を表示およびモニタリングするために使用するコマンドについて説明します。

VTP の設定情報（ドメイン名、現在の VTP バージョン、VLAN 数）を表示することによって、VTP をモニタします。デバイスで送受信されたアドバタイズに関する統計情報を表示することもできます。

表 *216 : VTP* モニタ コマンド

コマンド	目的
show vtp counters	送受信された VTP メッセージに関するカウンタを表示します。
show vtp devices [**conflict**]	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。プライマリ サーバと競合する VTP バージョン 3 の装置が表示されます。**show vtp devices** コマンドは、デバイスがトランスペアレント モードまたはオフ モードのときは情報を表示しません。
show vtp interface [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。
show vtp password	VTP パスワードを表示します。表示されるパスワードの形式は、**hidden** キーワードが入力されているか、または、暗号化がデバイスでイネーブル化されているかどうかによって異なります。
show vtp status	VTP デバイス設定情報を表示します。

VTP の設定例

例：スイッチをプライマリ サーバとして設定する

次に、パスワードが非表示またはシークレットに設定されている場合に、VLAN データベースのプライマリ サーバ（デフォルト）としてデバイスを設定する方法の例を示します。

```
Device# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- -------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

関連トピック

VTP バージョン 3 のパスワードの設定（CLI）（3197 ページ）
VTP ドメインのパスワード（3193 ページ）

次の作業

VTP を設定したら、次の項目を設定できます。

- VLANs
- VLAN グループ
- VLAN トランキング
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN コマンド リファレンス (Catalyst 3850 スイッチ)* 『*Layer 2/3 コマンド リファレンス (Catalyst 3850 スイッチ)*』
追加の設定コマンドおよび手順。	『*LAN Switching コンフィギュレーション ガイド, Cisco IOS XE Release 3SE (Catalyst 3850 スイッチ)*』 『*Layer 2/3 コンフィギュレーション ガイド (Catalyst 3850 スイッチ)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

VTP の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 152 章

VLAN の設定

- 機能情報の確認 （3211 ページ）
- VLAN の前提条件 （3211 ページ）
- VLAN の制約事項 （3212 ページ）
- VLAN について （3212 ページ）
- VLAN の設定方法 （3218 ページ）
- VLAN のモニタリング （3227 ページ）
- 次の作業 （3228 ページ）
- その他の参考資料 （3229 ページ）
- VLAN の機能履歴と情報 （3231 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VLAN の前提条件

VLAN 設定時の前提条件と考慮事項を次に示します。

- VLAN を作成する前に、VLAN トランキング プロトコル（VTP）を使用してネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。
- デバイスで多数の VLAN を設定し、ルーティングをイネーブルにしない予定の場合は、Switch Database Management（SDM）機能を VLAN テンプレートに設定します。これによ

り、最大数のユニキャスト MAC アドレスをサポートするようにシステム リソースが設定されます。

- LAN ベース フィーチャ セットが稼働しているデバイスは、SVI のスタティック ルーティングのみをサポートします。
- VLAN グループに VLAN を追加できるようにするため、VLAN がデバイスに存在している必要があります。

VLAN の制約事項

次に、VLAN の制約事項を示します。

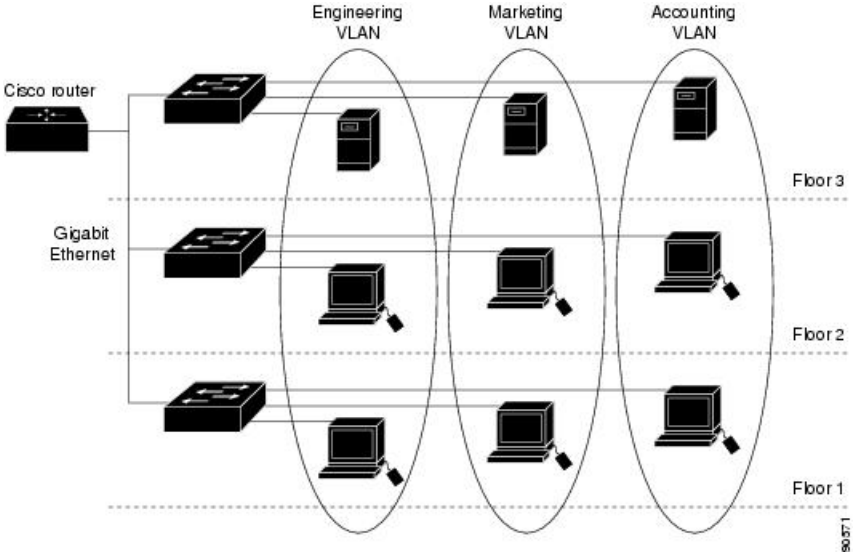
- デバイスは、最大 128 のスパニングツリー インスタンスを持つ Per-VLAN Spanning-Tree Plus（PVST+）または Rapid PVST+ をサポートします。VLAN ごとに 1 つずつスパニングツリー インスタンスを使用できます。
- デバイスは、イーサネット ポート経由の VLAN トラフィックの送信方式として、IEEE 802.1Q トランキングをサポートします。
- インターフェイス VLAN ルータの MAC アドレスの設定はサポートされていません。インターフェイス VLAN にはデフォルトですでに MAC アドレスが割り当てられています。
- プライベート VLAN はデバイスではサポートされません。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

VLAN について

論理ネットワーク

VLANは、ユーザの物理的な位置に関係なく、機能、プロジェクトチーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。どのようなデバイス ポートでも VLAN に属することができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN 内のエンド ステーションだけに転送またはフラッディングされます。各VLANは1つの論理ネットワークと見なされ、VLANに属さないステーション宛のパケットは、ルータまたはフォールバック ブリッジングをサポートするデバイスを経由して伝送しなければなりません。デバイス スタックでは、ポートを使用して VLAN をスタック全体に形成できます。VLAN はそれぞれが独立した論理ネットワークと見なされるので、VLANごとに独自のブリッジ管理情報ベース（MIB）情報があり、スパニングツリーの独自の実装をサポートできます。

図 *147*：論理的に定義されたネットワークとしての *VLAN*



VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットに含まれるエンド ステーションはすべて同じ VLAN に属します。デバイス上のインターフェイスの VLAN メンバーシップは、インターフェイスごとに手動で割り当てます。この方法でデバイス インターフェイスを VLAN に割り当てた場合、これをインターフェイス ベース（またはスタティック）VLAN メンバーシップと呼びます。

VLAN 間のトラフィックは、ルーティングする必要があります。

デバイスは、デバイス仮想インターフェイス（SVI）を使用して、VLAN 間でトラフィックをルーティングできます。VLAN 間でトラフィックをルーティングするには、SVI を明示的に設定して IP アドレスを割り当てる必要があります。

サポートされる VLAN

デバイスは、VTP クライアント、サーバ、およびトランスペアレントの各モードで VLAN をサポートしています。VLAN は、1 ～ 4094 の番号で識別します。VLAN 1 はデフォルト VLAN で、システム初期化中に作成されます。VLAN ID 1002 ～ 1005 は、トークンリングおよびファイバ分散データ インターフェイス（FDDI）VLAN 専用です。1002 ～ 1005 を除くすべての VLAN がユーザ設定のために使用できます。

VTP バージョン 1、バージョン 2、およびバージョン 3 の 3 つの VTP バージョンがあります。すべての VTP バージョンが標準および拡張範囲 VLAN の両方をサポートしますが、VTP バージョン 3 のみが デバイス 伝播拡張範囲 VLAN 設定情報を実行します。拡張範囲 VLAN が VTP バージョン 1 および 2 で作成された場合、設定情報は伝播されません。デバイス上のローカル VTP データベース エントリも更新されませんが、拡張範囲 VLAN 設定情報が作成され、実行コンフィギュレーション ファイルに保存されます。

最大 4094 の VLAN をデバイスに設定できます。

関連トピック

イーサネット VLAN の作成または変更（CLI）（3218 ページ）
VLAN の削除（CLI）（3222 ページ）
VLAN へのスタティック アクセス ポートの割り当て（CLI）（3223 ページ）
VLAN のモニタリング（3227 ページ）
拡張範囲 VLAN の作成（CLI）（3225 ページ）
内部 VLAN ID を指定した拡張範囲 VLAN の作成

VLAN ポート メンバーシップ モード

VLANに所属するポートは、メンバーシップモードを割り当てることで設定します。メンバーシップ モードは、各ポートが伝送できるトラフィックの種類、および所属できる VLAN の数を指定します。

ポートが VLAN に所属すると、デバイスは VLAN 単位で、ポートに対応するアドレスを学習して管理します。

表 *217*：ポートのメンバーシップ モードとその特性

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1つの VLAN だけに所属します。	VTP は必須ではありません。VTP にグローバルに情報を伝播させないようにする場合は、VTP モードをトランスペアレント モードに設定します。VTP に加入するには、別のデバイスまたはデバイス スタックのトランク ポートに接続されているデバイスまたはデバイス スタック上に少なくとも 1 つのトランク ポートが必要です。
トランク（IEEE 802.1Q） • IEEE 802.1Q：業界標準のトランキング カプセル化方式です。	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべての VLAN のメンバです。ただし、メンバーシップは許可 VLAN リストを設定して制限できます。また、プルーニング適格リストを変更して、リストに指定したトランク ポート上の VLAN へのフラッディング トラフィックを阻止することもできます。	VTP を推奨しますが、必須ではありません。VTP は、ネットワーク全体にわたって VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。VTP はトランク リンクを通じて他のデバイスと VLAN コンフィギュレーション メッセージを交換します。

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
音声 VLAN	音声 VLAN ポートは、Cisco IP Phone に接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データ トラフィックに別の VLAN を使用するように設定されたアクセス ポートです。	VTP は不要です。VTP は音声 VLAN に対して無効です。

関連トピック

VLAN へのスタティック アクセス ポートの割り当て（CLI） （3223 ページ）
VLAN のモニタリング （3227 ページ）

VLAN コンフィギュレーション ファイル

VLAN ID 1 ～ 1005 の設定は vlan.dat（VLAN データベース）ファイルに書き込まれます。この設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。vlan.dat ファイルはフラッシュ メモリに格納されます。VTP モードがトランスペアレント モードの場合、それらの設定もデバイスの実行コンフィギュレーション ファイルに保存されます。

デバイス スタックでは、スタック全体が同一の vlan.dat ファイルと実行コンフィギュレーションを使用します。一部のデバイスでは、vlan.dat ファイルがアクティブ デバイスのフラッシュ メモリに保存されます。

さらに、インターフェイス コンフィギュレーション モードを使用して、ポートのメンバーシップ モードの定義、VLAN に対するポートの追加および削除を行います。これらのコマンドの実行結果は、実行コンフィギュレーション ファイルに書き込まれます。このファイルを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

VLAN および VTP 情報（拡張範囲 VLAN 設定情報を含む）をスタートアップ コンフィギュレーション ファイルに保存して、デバイスを再起動すると、デバイスの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントで、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。
- VTP バージョン 1 および 2 では、VTP モードがサーバである場合、VLAN ID 1 ～ 1005 のドメイン名と VLAN 設定で VLAN データベース情報が使用されます。VTP バージョン 3 は、VLAN 1006 ～ 4094 もサポートします。

（注） スイッチの設定をリセットする前に、**write erase** コマンドを使用して、必ずコンフィギュレーション ファイルと一緒に vlan.dat ファイルを削除してください。これにより、リセット時にスイッチが正しく再起動します。

標準範囲 VLAN 設定時の注意事項

標準範囲 VLAN は、ID が 1 ～ 1005 の VLAN です。

ネットワーク内で標準範囲 VLAN を作成または変更する場合には、次の注意事項に従ってください。

- 標準範囲 VLAN は、1 ～ 1001 の番号で識別します。VLAN 番号 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 専用です。
- VLAN 1 ～ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードがトランスペアレント モードの場合、VTP と VLAN の設定もデバイスの実行コンフィギュレーション ファイルに保存されます。
- デバイスが VTP サーバ モードまたは VTP トランスペアレント モードにある場合は、VLAN データベース内の VLAN 2 ～ 1001 について設定を追加、変更、または削除できます（VLAN ID 1 および 1002 ～ 1005 は自動作成され、削除できません）。
- VTP トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースに保存されず、伝播されません。VTP バージョン 3 では、VTP サーバ モードでの拡張範囲 VLAN（VLAN 1006～4094）データベース伝播をサポートします。
- VLAN を作成する前に、デバイスを VTP サーバ モードまたは VTP トランスペアレント モードにする必要があります。デバイスが VTP サーバである場合には、VTP ドメインを定義する必要があります。VTP ドメインを定義しないと、VTP は機能しません。
- デバイスは、トークンリングまたは FDDI メディアをサポートしません。デバイスは FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを転送するのではなく、VTP を介して VLAN 設定を伝播します。
- デバイスは 128 のスパニングツリーインスタンスをサポートします。デバイスのアクティブな VLAN 数が、サポートされているスパニングツリーインスタンス数よりも多い場合、スパニングツリーは 128 の VLAN でイネーブルにできます。残りの VLAN で、スパニングツリーはディセーブルになります。デバイス上の使用可能なスパニングツリーインスタンスをすべて使い切ってしまった後に、VTP ドメインの中にさらに別の VLAN を追加すると、そのデバイス上にスパニングツリーが稼働しない VLAN が生成されます。そのデバイスのトランク ポート上でデフォルトの許可リスト（すべての VLAN を許可するリスト）が設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接デバイスでスパニングツリーインスタンスをすべて使用してしまっている場合には注意が必要です。スパニングツリーインスタンスの割

り当てを使い果たしたデバイスのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。

デバイス上の VLAN の数がサポートされているスパニングツリー インスタンスの最大数を超える場合、デバイス上に IEEE 802.1s Multiple STP（MSTP）を設定して、複数の VLAN を単一のスパニングツリー インスタンスにマッピングすることを推奨します。

- スタック内のデバイスが新しい VLAN を学習するか、または既存の VLA を削除または変更すると（ネットワーク ポートを介した VTP を通じてか、または CLI を通じて）、その VLAN 情報はすべてのスタック メンバに伝達されます。
- デバイスがスタックに参加した場合またはスタックの結合が発生した場合は、新しいデバイス上の VTP 情報（vlan.dat ファイル）とアクティブなデバイスの一貫性が維持されます。

関連トピック

イーサネット VLAN の作成または変更（CLI）（3218 ページ）
VLAN の削除（CLI）（3222 ページ）
VLAN へのスタティック アクセス ポートの割り当て（CLI）（3223 ページ）
VLAN のモニタリング（3227 ページ）

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN は、ID が 1006 ～ 4094 の VLAN です。

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- 拡張範囲の VLAN ID は、デバイスが VTP バージョン 3 を実行していない場合は VLAN データベースに保存されず、VTP で認識されません。
- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。
- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで、VTP モードをトランスペアレントに設定できます。VTP トランスペアレント モードでデバイスが始動するように、この設定をスタートアップ コンフィギュレーションに保存する必要があります。このようにしないと、デバイスをリセットした場合に、拡張範囲 VLAN 設定が失われます。VTP バージョン 3 で拡張範囲 VLAN を作成する場合は、VTP バージョン 1 または 2 に変更できません。
- デバイススタックでは、スタック全体が同一の実行コンフィギュレーションと保存されているコンフィギュレーションを使用しており、拡張範囲 VLAN 情報はスタック全体で共有されます。

関連トピック

拡張範囲 VLAN の作成（CLI）（3225 ページ）
内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN のモニタリング（3227 ページ）

VLAN の設定方法

標準範囲 VLAN の設定方法

VLAN データベースに新しい標準範囲 VLAN を作成したり、VLAN データベース内の既存の VLAN を変更したりする場合、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ
  - イーサネット
  - Fiber Distributed Data Interface [FDDI]
  - FDDI ネットワーク エンティティ タイトル [NET]
  - TrBRF または TrCRF
  - Token Ring
  - トークンリング Net
- VLAN ステート（アクティブまたは中断）
- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN のスパニングツリー プロトコル（STP）タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号

vlan.dat ファイルを手動で削除しようとすると、VLAN データベースの不整合が生じる可能性があります。VLAN 設定を変更する場合は、この項の手順に従ってください。

イーサネット VLAN の作成または変更（CLI）

始める前に

VTP バージョン 1 および 2 でデバイスが VTP トランスペアレント モードの場合は、1006 を超える VLAN ID を割り当てることができますが、それらを VLAN データベースに追加できません。

デバイスは、イーサネット インターフェイスだけをサポートしています。FDDI およびトークンリング VLAN は、ローカルではサポートされないので、FDDI およびトークンリング メディア固有の特性は、他のデバイスに対する VTP グローバル アドバタイズにのみ設定します。

このデバイスはトークンリング接続をサポートしていませんが、トークンリング接続を行っているリモート デバイスを、サポート対象デバイスのうちの 1 台から管理できます。VTP バージョン 2 が稼働しているデバイスは、次のトークンリング VLAN に関する情報をアドバタイズします。

- トークンリング TrBRF VLAN
- トークンリング TrCRF VLAN

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。 （注） このコマンドで指定できる VLAN ID 範囲は 1 ～ 4094 です。 追加の **vlan** コマンド オプションは次のとおりです。 • **access-map**：VLAN アクセスマップを作成したり、VLAN アクセスマップ コマンド モードを開始します。 • **configuration**：VLAN 機能コンフィギュレーションモードになります。 • **dot1q**：VLAN dot1q tag native パラメータを設定します。 • **filter**：VLAN フィルタ マップを VLAN リストに適用します。

	コマンドまたはアクション	目的
		• **group**：VLAN グループを作成します。
ステップ 3	**name** *vlan-name* 例： `Device(config-vlan)# name test20`	（任意）VLAN の名前を入力します。VLAN名を指定しなかった場合には、デフォルトとして、VLANという語の後ろに先行ゼロを含めた *vlan-id* 値が付加されます。たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。 次の追加 VLAN コンフィギュレーション コマンド オプションが使用可能です。 • **are**：この VLAN の All-Route Explorer（ARE）ホップの最大数を設定します。 • **backupcrf**：VLAN のバックアップ コンセントレータ リレー機能（CRF）モードをイネーブルまたはディセーブルにします。 • **bridge**：FDDI-Net またはトークン リング ネット タイプの VLAN にブリッジ番号の値を設定します。 • **exit**：変更を適用し、リビジョン番号を増分して、終了します。 • **media**：VLAN のメディア タイプを設定します。 • **no**：コマンドまたはデフォルトを拒否します。 • **parent**：FDDI の親 VLAN やトークン リング タイプの VLAN に ID の値を設定します。 • **remote-span**：リモート SPAN VLAN を設定します。 • **ring**：FDDI またはトークン リング タイプの VLAN にリング番号値を設定します。

	コマンドまたはアクション	目的
		• **said**：IEEE 802.10 SAID の値を設定します。 • **shutdown**：VLAN スイッチングをシャットダウンします。 • **state**：運用上の VLAN ステートを実行中または停止中に設定します。 • **ste**：VLAN のスパニングツリー エクスプローラ（STE）のホップの最大数を設定します。 • **stp**：VLAN のスパニングツリー特性を設定します。
ステップ 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } 例： `Device(config-vlan)# media ethernet`	VLANのメディア タイプを設定します。コマンドオプションは次のとおりです。 • **ethernet**：VLANのメディア タイプをイーサネットに設定します。 • **fd-net**：VLANのメディア タイプをFDDI-net に設定します。 • **fddi**：VLAN のメディア タイプをFDDI に設定します。 • **tokenring**：VLAN メディア タイプをトークン リングに設定します。 • **trn-net**：VLAN メディア タイプをトークン リング ネットに設定します。
ステップ 5	**remote-span** 例： `Device(config-vlan)# remote-span`	（任意）リモート スイッチド ポート アナライザ（SPAN）セッションに対するRSPAN VLAN として、VLAN を設定します。リモート SPAN の詳細については、『*Catalyst 3850* ネットワーク管理コンフィギュレーション ガイド』を参照してください。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show vlan** {**name** *vlan-name* | **id** *vlan-id*} 例： `Device# show vlan name test20 id 20`	入力を確認します。

関連トピック

サポートされる VLAN （3213 ページ）
標準範囲 VLAN 設定時の注意事項 （3216 ページ）
VLAN のモニタリング （3227 ページ）

VLAN の削除（CLI）

VTP サーバ モードのデバイスから VLAN を削除すると、VTP ドメイン内のすべてのデバイスの VLAN データベースから、その VLAN が削除されます。VTP トランスペアレント モードのデバイスから VLAN を削除した場合、その特定のデバイススイッチまたはデバイススタック上に限り VLAN が削除されます。

イーサネット VLAN 1 および FDDI、またはトークンリング VLAN 1002 ～ 1005 の、メディアタイプ別のデフォルト VLAN は削除できません。

⚠

注意 VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。これらのポートは、新しいVLANに割り当てられるまで、元のVLANに（非アクティブで）対応付けられたままです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no vlan** *vlan-id* 例：	VLAN ID を入力して、VLAN を削除します。

	コマンドまたはアクション	目的
	`Device(config)# no vlan 4`	
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vlan brief** 例： `Device# show vlan brief`	VLAN が削除されたことを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

サポートされる VLAN （3213 ページ）
標準範囲 VLAN 設定時の注意事項 （3216 ページ）
VLAN のモニタリング （3227 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI）

VTP をディセーブルにすることによって（VTP トランスペアレント モード）、VTP に VLAN 設定情報をグローバルに伝播させずに、スタティック アクセス ポートを VLAN に割り当てることができます。

クラスタ メンバ デバイス上のポートを VLAN に割り当てる場合、最初に **rcommand** 特権 EXEC コマンドを使用して、クラスタ メンバ スイッチにログインします。

存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	VLANに追加するインターフェイスを入力します。
ステップ 4	**switchport mode access** 例： `Device(config-if)# switchport mode access`	ポート（レイヤ 2 アクセス ポート）の VLAN メンバーシップ モードを定義します。
ステップ 5	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 2`	VLANにポートを割り当てます。指定できる VLAN ID の範囲は 1 ～ 4094 です。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet2/0/1`	インターフェイスのVLANメンバーシップ モードを確認します。
ステップ 8	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet2/0/1 switchport`	表示された *Administrative Mode* および *Access Mode VLAN* フィールドの設定を確認します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

サポートされる VLAN （3213 ページ）
標準範囲 VLAN 設定時の注意事項 （3216 ページ）
VLAN のモニタリング （3227 ページ）
VLAN ポート メンバーシップ モード （3214 ページ）

拡張範囲 VLAN の設定方法

サービス プロバイダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応できます。拡張範囲 VLAN ID は、VLAN ID を許可するどの **switchport** コマンドでも許可されます。

VTP バージョン 1 または 2 での拡張範囲 VLAN の設定は VLAN データベースに格納されません。ただし、VTP モードがトランスペアレントであるため、デバイスの実行コンフィギュレーション ファイルに格納されます。また、設定をスタートアップ コンフィギュレーション ファイルに保存できます。VTP バージョン 3 で作成された拡張範囲 VLAN は、VLAN データベースに保存されます。

拡張範囲 VLAN については MTU サイズおよびリモート SPAN 設定ステートしか変更できません。残りのすべての特性はデフォルト状態のままでなければなりません。

拡張範囲 VLAN の作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**vlan** *vlan-id*
	例：
	`Device(config)# vlan 2000`
	`Device(config-vlan)#`
		拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーションモードを開始します。指定できる範囲は 1006 ～ 4094 です。

ステップ 4	**remote-span** 例： `Device(config-vlan)# remote-span`	（任意）RSPAN VLAN として VLAN を設定します。

ステップ 5	**exit**
	例：
	`Device(config-vlan)# exit`
	`Device(config)#`
		コンフィギュレーションモードに戻ります。

ステップ 6	**interface vlan**
	例：
	`Device(config)# interface vlan 200`
	`Device(config-if)#`
		選択した VLAN についてインターフェイス コンフィギュレーションモードを開始します。

ステップ 7	**ip mtu** *mtu-size*
	例：
	`Device(config-if)# ip mtu 1024`
	`Device(config-if)#`
		（任意）MTU サイズを変更して、VLAN を変更します。68 ～ 1500 バイトの MTU サイズを設定できます。
		（注） CLI ヘルプにすべての VLAN コマンドが表示されますが、拡張範囲 VLAN でサポートされているのは、**ip mtu** *mtu-size* コマンド、 コマンド、**remote-span** コマンドだけです。

ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show vlan id** *vlan-id* 例：	VLAN が作成されたことを確認します。

	コマンドまたはアクション	目的
	`Device# show vlan id 2000`	
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

サポートされる VLAN （3213 ページ）
拡張範囲 VLAN 設定時の注意事項 （3217 ページ）
VLAN のモニタリング （3227 ページ）

VLAN のモニタリング

表 *218*：特権 *EXEC* 表示コマンド

コマンド	目的
show interfaces [**vlan** *vlan-id*]	デバイス上に設定されたすべてのインターフェイスまたは特定の VLAN の特性を表示します。

コマンド	目的
show vlan [**access-map** *name* | **brief** | **dot1q** { **tag native** } | **filter** [**access-map** | **vlan**] | **group** [**group-name** *name*] | **id** *vlan-id* | **ifindex** | **mtu** | **name** *name* | **remote-span** | **summary**]	デバイス上のすべての VLAN または特定の VLAN のパラメータを表示します。次のコマンド オプションが使用可能です。 • **access-map**：VLAN アクセスマップを表示します。 • **brief**：VTP VLAN のステータス概要を表示します。 • **dot1q**：dot1q パラメータを表示します。 • **filter**：VLAN フィルタ情報を表示します。 • **group**：VLAN グループをグループ名と使用可能な接続済みの VLAN と一緒に表示します。 • **id**：識別番号別に VTP VLAN ステータスを表示します。 • **ifindex**：SNMP ifIndex を表示します。 • **mtu**：VLAN MTU 情報を表示します。 • **name**：指定された名前の VTP VLAN 情報を表示します。 • **remote-span**：リモート SPAN VLAN を表示します。 • **summary**：VLAN 情報の要約を表示します。

関連トピック

サポートされる VLAN （3213 ページ）
標準範囲 VLAN 設定時の注意事項 （3216 ページ）
イーサネット VLAN の作成または変更（CLI） （3218 ページ）
VLAN の削除（CLI） （3222 ページ）
VLAN へのスタティック アクセス ポートの割り当て（CLI） （3223 ページ）
拡張範囲 VLAN 設定時の注意事項 （3217 ページ）
拡張範囲 VLAN の作成（CLI） （3225 ページ）
内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN ポート メンバーシップ モード （3214 ページ）

次の作業

VLAN を設定したら、次の項目を設定できます。

- VLAN グループ
- VLAN トランキング プロトコル（VTP）
- VLAN トランク

- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN* コマンド リファレンス *(Catalyst 3850* スイッチ*)* 『*Layer 2/3* コマンド リファレンス *(Catalyst 3850* スイッチ*)*』
VLAN アクセス マップ	*Security* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)* *Security* コマンド リファレンス *(Catalyst 3850* スイッチ*)*
VLANおよびモビリティエージェント	『*Mobility* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』
Cisco Flexible NetFlow	『*Cisco Flexible NetFlow* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』 『*Flexible Netflow* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』
IGMP スヌーピング	*IP Multicast Routing* コマンド リファレンス *(Catalyst 3850* スイッチ*)* *IP Multicast Routing* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)*
IPv6	*IPv6* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)* *IPv6* コマンド リファレンス *(Catalyst 3850* スイッチ*)*
SPAN	ネットワーク管理コマンド リファレンス *(Catalyst 3850* スイッチ*)* ネットワーク管理コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)*
プラットフォームに依存しない設定情報	『*Identity Based Networking Services* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

VLAN の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました
Cisco IOS XE 3.3SE	VLAN（GUI）サポート。

第 153 章

VLAN グループの設定

- 機能情報の確認 （3233 ページ）
- VLAN グループの前提条件 （3233 ページ）
- VLAN グループの制約事項 （3234 ページ）
- VLAN グループについて （3234 ページ）
- VLAN グループの設定方法 （3235 ページ）
- 次の作業 （3237 ページ）
- その他の参考資料 （3237 ページ）
- VLAN グループの機能履歴と情報 （3239 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VLAN グループの前提条件

- VLAN グループに VLAN を追加できるようにするため、VLAN がデバイスに存在している必要があります。
- VLAN グループが適切に機能するためには、DHCP スヌーピングを全体的にイネーブルにする他に、DHCP スヌーピングがすべての VLAN でイネーブルになっていることを確認する必要があります。

VLAN グループの制約事項

1 つの VLAN グループにマッピングされる VLAN の数は、Cisco IOS Software Release による制限を受けません。ただし、VLAN グループの VLAN の数が推奨値である 32 を超えた場合、予期されないモビリティの動作が発生し、VLAN グループ内の一部の VLAN で L2 マルチキャストが中断します。したがって、VLAN グループ内で適切な数の VLAN を設定する責任は管理者にあります。すでに 32 個の VLAN が含まれている WLAN にマップされている VLAN グループに VLAN を追加すると、警告が生成されます。ただし、32 を超える VLAN が含まれている WLAN に新しい VLAN グループがマッピングされると、エラーが生成されます。

VLAN グループが予期通り動作するためには、グループでマッピングされた VLAN がデバイスに存在している必要があります。スタティック IP クライアント動作はサポートされません。

VLAN グループについて

クライアントがワイヤレス ネットワーク（WLAN）に接続するたびに、WLAN に関連付けられている VLAN にクライアントが配置されます。講堂、競技場、会議場などといった大規模な会場では、大量のワイヤレス クラインアントが使用されており、単一の WLAN だけで多数のクライアントに対応することは困難な場合があります。

VLAN グループ機能は、複数の VLAN に対応可能な単一 WLAN を使用します。クライアントは、設定されている VLAN の 1 つに割り当てることができます。この機能は、VLAN グループを使用して WLAN を 1 つまたは複数の VLAN にマップします。ワイヤレス クライアントが WLAN に関連付けられると、ワイヤレス クライアントの MAC アドレスに基づいてアルゴリズムにより VLAN が生成されます。VLAN がクライアントに割り当てられ、クライアントが割り当てられた VLAN から IP アドレスを取得します。またこの機能は、現行の AP グループ アーキテクチャおよび AAA オーバーライド アーキテクチャを拡張します。これらのアーキテクチャでは AP グループと AAA オーバーライドが、WLAN がマップされている 1 つの VLAN または VLAN グループをオーバーライドできます。

Cisco IOS XE Release 3.7.0E で導入された動作の変更：クライアントが WLAN に関連付けられ、WLAN が VLAN グループに適用されると、クライアントの MAC アドレスと VLAN グループの VLAN の数に基づき、ハッシュ アルゴリズムを使用してインデックスが算出されます。このインデックスに基づいて、VLANがクライアントに割り当てられます。インデックスが「ダーティ」である場合、別のインデックスがラウンドロビン方式で生成され、新たに生成されたインデックスに基づいて VLAN がクライアントに割り当てられます。

クライアントが DHCP を使用して IP アドレスを受信できない場合、VLAN が 30 分間にわたり「ダーティ」としてマークされます。30 分経過しても、VLAN グループの VLAN から「ダーティ」フラグがクリアされないことがあります。これは、グローバルタイマーが期限切れになるまでに 5 分の遅延があるために、各インターフェイスのタイムスタンプを調べて 30 分よりも大きいかどうかを確認する必要があるため、予期される動作です。

関連トピック

VLAN グループの作成（CLI）（3235 ページ）

VLAN グループの設定方法

VLAN グループの作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan group** *WORD* **vlan-list** *vlan-ID* 例： `Device(config)#vlan group vlangrp1 vlan-list 91-95`	所定のグループ名（vlangrp1）で VLAN グループを作成し、コマンドに一覧表示されているすべての VLAN を追加します。VLAN リストの範囲は 1 ～ 4096 で、1 つのグループの VLAN の数として推奨される数は 32 です。
ステップ 3	**end** 例： `Device(config)#end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。また、**CTRL-Z** を押して、グローバル コンフィギュレーション モードを終了します。

関連トピック

VLAN グループについて （3234 ページ）

VLAN グループの削除（CLI）

手順

ステップ 1 **configure terminal**

例：

`Device# configure terminal`

グローバル コマンド モードを開始します。

ステップ 2 **vlan group** *WORD* **vlan-list** *vlan-ID*

例：

`Device(config)#vlan group vlangrp1 vlan-list 91-95`

所定のグループ名（vlangrp1）で VLAN グループを作成し、コマンドに一覧表示されているすべての VLAN を追加します。VLAN リストの範囲は 1 ～ 4096 で、1 つのグループの VLAN の数として推奨される数は 32 です。

ステップ 3 **no vlan group** *WORD* **vlan-list** *vlan-ID*

例：

```
Device(config)#no vlan group vlangrp1 vlan-list 91-95
```

所定のグループ名（vlangrp1）の VLAN グループが削除されます。

ステップ 4 **end**

例：

```
Device(config)#end
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。また、**CTRL-Z** を押して、グローバル コンフィギュレーション モードを終了します。

WLAN への VLAN グループの追加（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**wlan** *WORD* *number* 例： `Device(config)#wlan wlanname 512`	WLAN が ID を使用して VLAN グループをマッピングできるようにします。WLAN ID 値の範囲は 1 ～ 512 です。
ステップ 3	**client vlan** *WORD* 例： `Device(config-wlan)#client vlan vlangrp1`	VLAN ID、VLAN グループ、または VLAN 名を入力して、VLAN グループを WLAN にマッピングします。
ステップ 4	**end** 例： `Device(config-wlan)#end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。また、**CTRL-Z** を押して、グローバル コンフィギュレーション モードを終了します。

VLAN グループの VLAN の表示（CLI）

コマンド	説明
`show vlan group`	VLAN グループの名前と使用可能な VLAN のリストを表示します。
`show vlan group group-name` **`<group_name>`**	指定された VLAN グループの詳細を表示します。
`show wireless vlan group` **`<group_name>`**	指定されたワイヤレス VLAN グループの詳細を表示します。

次の作業

VLAN グループを設定したら、次の項目を設定できます。

- VLANs
- VLAN トランキング プロトコル（VTP）
- VLAN トランク
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN* コマンド リファレンス *(Catalyst 3850* スイッチ*)* 『*Layer 2/3* コマンド リファレンス *(Catalyst 3850* スイッチ*)*』
VLAN アクセス マップ	*Security* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)* *Security* コマンド リファレンス *(Catalyst 3850* スイッチ*)*
VLANおよびモビリティエージェント	『*Mobility* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』
Cisco Flexible NetFlow	『*Cisco Flexible NetFlow* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』 『*Flexible Netflow* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』

関連項目	マニュアル タイトル
IGMP スヌーピング	*IP Multicast Routing* コマンド リファレンス *(Catalyst 3850* スイッチ*)* *IP Multicast Routing* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)*
IPv6	*IPv6* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)* *IPv6* コマンド リファレンス *(Catalyst 3850* スイッチ*)*
SPAN	ネットワーク管理コマンド リファレンス *(Catalyst 3850* スイッチ*)* ネットワーク管理コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)*
プラットフォームに依存しない設定情報	『*Identity Based Networking Services* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

VLAN グループの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2E	この機能が導入されました
Cisco IOS XE 3.3SE	VLAN（GUI）サポート。

第 154 章

VLAN トランクの設定

- 機能情報の確認 （3241 ページ）
- VLAN トランクの前提条件 （3241 ページ）
- VLAN トランクの制約事項 （3242 ページ）
- VLAN トランクについて （3243 ページ）
- VLAN トランクの設定方法 （3247 ページ）
- 次の作業 （3260 ページ）
- その他の参考資料 （3260 ページ）
- VLAN トランクの機能履歴と情報 （3262 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VLAN トランクの前提条件

IEEE 802.1Q トランクは、ネットワークのトランキング方式について次の制約があります。

- IEEE 802.1Q トランクを使用して接続している Cisco デバイスのネットワークでは、デバイスはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。他社製のデバイスは、すべての VLAN でスパニングツリー インスタンスを 1 つサポートする場合があります。

IEEE 802.1Q トランクを使用して Cisco デバイスを他社製のデバイスに接続する場合、Cisco デバイスは、トランクの VLAN のスパニングツリーインスタンスを、他社製の IEEE 802.1Q デバイスのスパニングツリー インスタンスと結合します。ただし、各 VLAN のスパニングツリー情報は、他社製の IEEE 802.1Q デバイスからなるクラウドにより分離された Cisco デバイスによって維持されます。Cisco デバイスを分離する他社製の IEEE 802.1Q クラウドは、デバイス間の単一トランク リンクとして扱われます。

- IEEE 802.1Q トランクに対応するネイティブ VLAN が、トランク リンクの両側で一致していなければなりません。トランクの片側のネイティブ VLAN と反対側のネイティブ VLAN が異なっていると、スパニングツリー ループが発生する可能性があります。
- ネットワーク上のすべてのネイティブ VLAN についてスパニングツリーをディセーブルにせずに、IEEE 802.1Q トランクのネイティブ VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。IEEE 802.1Q トランクのネイティブ VLAN 上でスパニングツリーをイネーブルのままにしておくか、またはネットワーク上のすべての VLAN でスパニングツリーをディセーブルにすることを推奨します。また、ネットワークにループがないことを確認してから、スパニングツリーをディセーブルにしてください。

VLAN トランクの制約事項

次に、VLAN トランクに関する制約事項を示します。

- トランク ポートをセキュア ポートにすることはできません。
- トランク ポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内のすべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次に示すパラメータのいずれかの設定を変更すると、デバイスは、入力された設定をグループ内のすべてのポートに伝播します。
  - 許可 VLAN リスト。
  - 各 VLAN の STP ポート プライオリティ。
  - STP PortFast の設定値。
  - トランク ステータス：

    ポートグループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- Per VLAN Spanning Tree（PVST）モードでは最大 24 までのトランク ポート、マルチ スパニング ツリー（MST）モードでは最大 40 までのトランク ポートを設定することを推奨します。

- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。
- ダイナミック トランキング プロトコル（DTP）はトンネル ポートではサポートされていません。
- デバイスはレイヤ 3 トランクをサポートしません。したがって、サブインターフェイスを設定する、またはレイヤ 3 インターフェイスで **encapsulation** キーワードを使用することはできません。ただし、デバイスは、同等の機能を備えたレイヤ 2 トランクおよびレイヤ 3 VLAN インターフェイスをサポートします。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

VLAN トランクについて

トランキングの概要

トランクとは、1 つまたは複数のイーサネットデバイスインターフェイスと他のネットワーキングデバイス（ルータ、デバイスなど）の間のポイントツーポイントリンクです。イーサネットトランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張できます。

すべてのイーサネット インターフェイス上で、次のトランキング カプセル化方式を使用できます。

- IEEE 802.1Q：業界標準のトランキング カプセル化方式です。

トランキング モード

イーサネット トランク インターフェイスは、さまざまなトランキング モードをサポートします。インターフェイスをトランキングまたは非トランキングとして設定したり、ネイバーインターフェイスとトランキングのネゴシエーションを行ったりするように設定できます。トランキングを自動ネゴシエーションするには、インターフェイスが同じ VTP ドメインに存在する必要があります。

トランク ネゴシエーションは、ポイントツーポイントプロトコル（PPP）であるダイナミックトランキングプロトコル（DTP）によって管理されます。ただし、一部のインターネットワー

キング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。

関連トピック

トランク ポートの設定（CLI） （3247 ページ）
レイヤ 2 インターフェイス モード （3244 ページ）

レイヤ 2 インターフェイス モード

表 *219 :* レイヤ *2* インターフェイス モード

モード	機能
switchport mode access	インターフェイス（アクセス ポート）を永続的な非トランキング モードにして、リンクの非トランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスかどうかに関係なく、非トランク インターフェイスになります。
switchport mode dynamic auto	インターフェイスがリンクをトランク リンクに変換できるようにします。インターフェイスは、ネイバー インターフェイスが **trunk** または **desirable** モードに設定されている場合、トランク インターフェイスになります。すべてのイーサネット インターフェイスのデフォルトのスイッチポート モードは、**dynamic auto** です。
switchport mode dynamic desirable	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、ネイバー インターフェイスが **trunk**、**desirable**、または **auto** モードに設定されている場合、トランク インターフェイスになります。
switchport mode trunk	インターフェイスを永続的なトランキング モードにして、ネイバー リンクのトランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスでない場合でも、トランク インターフェイスになります。
switchport nonegotiate	インターフェイスが DTP フレームを生成しないようにします。このコマンドは、インターフェイス スイッチポート モードが **access** または **trunk** の場合だけ使用できます。トランク リンクを確立するには、手動でネイバー インターフェイスをトランク インターフェイスとして設定する必要があります。

関連トピック

トランク ポートの設定（CLI） （3247 ページ）
トランキング モード （3243 ページ）

トランクでの許可 VLAN

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランクですべての VLAN ID（1 ～ 4094）が許可されます。ただし、許可リストから VLAN を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。

スパニングツリー ループまたはストームのリスクを減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにできます。トランク ポートから VLAN 1 を削除した場合、インターフェイスは引き続き VLAN 1 内で Cisco Discovery Protocol（CDP）、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、DTP、および VTP などの管理トラフィックを送受信します。

VLAN 1 をディセーブルにしたトランク ポートが非トランク ポートになると、そのポートはアクセス VLAN に追加されます。アクセス VLAN が 1 に設定されると、**switchport trunk allowed** の設定には関係なく、ポートは VLAN 1 に追加されます。ポート上でディセーブルになっている任意の VLAN について同様のことが当てはまります。

トランク ポートは、VLAN がイネーブルになっており、VTP が VLAN を認識し、なおかつポートの許可リストにその VLAN が登録されている場合に、VLAN のメンバになることができます。VTP が新しくイネーブルにされた VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバになります。VTP が新しい VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されていない場合には、トランク ポートはその VLAN のメンバにはなりません。

関連トピック

トランクでの許可 VLAN の定義（CLI）（3249 ページ）

トランク ポートでの負荷分散

負荷分散により、デバイスに接続しているパラレル トランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、デバイス間で 1 つのパラレル リンク以外のすべてのリンクをブロックします。負荷分散を行うと、トラフィックの所属する VLAN に基づいて、リンク間でトラフィックが分散されます。

トランク ポートで負荷分散を設定するには、STP ポート プライオリティまたは STP パス コストを使用します。STP ポート プライオリティを使用して負荷分散を設定する場合には、両方の負荷分散リンクを同じデバイスに接続する必要があります。STP パスコストを使用して負荷分散を設定する場合には、それぞれの負荷分散リンクを同一のデバイスに接続することも、2 台の異なるデバイスに接続することもできます。

STP プライオリティによるネットワーク負荷分散

同一のデバイス上の 2 つのポートがループを形成すると、デバイスは STP ポート プライオリティを使用して、どのポートをイネーブルとし、どのポートをブロッキング ステートとするかを判断します。パラレル トランク ポートにプライオリティを設定することにより、そのポートに、特定の VLAN のすべてのトラフィックを伝送させることができます。VLAN に対するプライオリティの高い（値の小さい）トランク ポートがその VLAN のトラフィックを転送し

ます。同じ VLAN に対してプライオリティの低い（値の大きい）トランク ポートは、その VLAN に対してブロッキング ステートのままです。1 つのトランク ポートが特定の VLAN に関するすべてのトラフィックを送受信することになります。

関連トピック

STP ポート プライオリティによる負荷分散の設定（CLI）（3254 ページ）

STP パス コストによるネットワーク負荷分散

トランクにそれぞれ異なるパス コストを設定し、各パス コストをそれぞれ異なる VLAN 群に対応付け、各 VLAN でポートをブロックすることによって、VLAN トラフィックを分散するパラレル トランクを設定できます。VLAN はトラフィックを分離し、リンクが失われた場合に備えて冗長性を維持します。

関連トピック

STP パス コストによる負荷分散の設定（CLI）（3257 ページ）

機能の相互作用

トランキングは他の機能と次のように相互作用します。

- トランク ポートをセキュア ポートにすることはできません。
- トランク ポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内のすべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次に示すパラメータのいずれかの設定を変更すると、デバイスは、入力された設定をグループ内のすべてのポートに伝播します。
  - 許可 VLAN リスト。
  - 各 VLAN の STP ポート プライオリティ。
  - STP PortFast の設定値。
  - トランク ステータス：

    ポートグループ内の1つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- Per VLAN Spanning Tree（PVST）モードでは最大 24 までのトランク ポート、マルチ スパニング ツリー（MST）モードでは最大 40 までのトランク ポートを設定することを推奨します。
- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとすると、

エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。

VLAN トランクの設定方法

トランクの誤設定を避けるために、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように（つまり DTP をオフにするように）設定してください。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

トランク ポートとしてのイーサネット インターフェイスの設定

トランク ポートの設定（CLI）

トランク ポートは VTP アドバタイズを送受信するので、VTP を使用する場合は、デバイス上で少なくとも 1 つのトランク ポートが設定されており、そのトランク ポートが別のデバイスのトランク ポートに接続されていることを確認する必要があります。そうでない場合、デバイスは VTP アドバタイズを受信できません。

始める前に

デフォルトでは、インターフェイスはレイヤ 2 モードです。レイヤ 2 インターフェイスのデフォルト モードは、**switchport mode dynamic auto** です。隣接インターフェイスがトランキングをサポートし、トランキングを許可するように設定されている場合、リンクはレイヤ 2 トランクです。また、インターフェイスがレイヤ 3 モードの場合は、**switchport** インターフェイス コンフィギュレーション コマンドを入力するとレイヤ 2 トランクになります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	トランクに設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**} 例： `Device(config-if)# switchport mode dynamic desirable`	インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートであり、トランキング モードを設定する場合に限り必要となります）。 • **dynamic auto**：ネイバー インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。これはデフォルトです。 • **dynamic desirable**：ネイバー インターフェイスが trunk、desirable、または auto モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 • **trunk**：ネイバー インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リンクに変換するようにネゴシエートします。
ステップ 5	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 200`	（任意）インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。

	コマンドまたはアクション	目的
ステップ 6	**switchport trunk native vlan** *vlan-id* 例： `Device(config-if)# switchport trunk native vlan 200`	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet1/0/2 switchport`	インターフェイスのスイッチポート設定を表示します。[Administrative Mode] および [Administrative Trunking Encapsulation] フィールドに表示されます。
ステップ 9	**show interfaces** *interface-id***trunk** 例： `Device# show interfaces gigabitethernet1/0/2 trunk`	インターフェイスのトランクの設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

トランキング モード （3243 ページ）
レイヤ 2 インターフェイス モード （3244 ページ）

トランクでの許可 VLAN の定義（CLI）

VLAN 1 は、すべての Cisco デバイスのすべてのトランク ポートのデフォルト VLAN です。以前は、すべてのトランク リンクで VLAN 1 を必ずイネーブルにする必要がありました。VLAN 1 の最小化機能を使用して、個々の VLAN トランク リンクで VLAN 1 をディセーブルに設定できます。これにより、ユーザ トラフィック（スパニングツリー アドバタイズなど）は VLAN 1 で送受信されなくなります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 5	**switchport trunk allowed vlan** { *word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list* 例： `Device(config-if)# switchport trunk allowed vlan remove 2`	（任意）トランク上で許容される VLAN のリストを設定します。 *vlan-list* パラメータは、1 ～ 4094 の単一の VLAN 番号、または 2 つの VLAN 番号（小さい方が先、ハイフンで区切る）で指定された VLAN 範囲です。カンマで区切った VLAN パラメータの間、またはハイフンで指定した範囲の間には、スペースを入れないでください。 デフォルトでは、すべての VLAN が許可されます。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet1/0/1 switchport`	表示された [Trunking VLANs Enabled] フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

トランクでの許可 VLAN （3245 ページ）

プルーニング適格リストの変更（CLI）

プルーニング適格リストは、トランク ポートだけに適用されます。トランク ポートごとに独自の適格リストがあります。この手順を有効にするには、VTP プルーニングがイネーブルに設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	VLAN プルーニングを適用するトランク ポートを選択し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan* [,*vlan* [,,,]]	トランクからのプルーニングを許可する VLAN のリストを設定します。 **add**、**except**、**none**、および **remove** キーワードの使用方法については、このリリースに対応するコマンド リファレンスを参照してください。 連続していない VLAN ID は、カンマ（スペースなし）で区切ります。ID の範囲はハイフンで指定します。有効な ID 範囲は 2 ～ 1001 です。拡張範囲 VLAN（VLAN ID 1006 ～ 4094）はプルーニングできません。 プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。 デフォルトでは、プルーニングが許可される VLAN のリストには、VLAN 2 ～ 1001 が含まれます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet2/0/1 switchport`	表示された [Pruning VLANs Enabled] フィールドの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

タグなしトラフィック用ネイティブ VLAN の設定（CLI）

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、デバイスはタグなしトラフィックを、ポートに設定されたネイティブ VLAN に転送します。ネイティブ VLAN は、デフォルトでは VLAN 1 です。

ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

パケットの VLAN ID が出力ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、デバイスはそのパケットをタグ付きで送信します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	IEEE 802.1Q トランクとして設定するインターフェイスを定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport trunk native vlan** *vlan-id* 例： `Device(config-if)# switchport trunk native vlan 12`	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。 *vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet1/0/2 switchport`	[Trunking Native Mode VLAN] フィールドの設定を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

トランク ポートの負荷分散の設定

STP ポート プライオリティによる負荷分散の設定（CLI）

デバイスがデバイス スタックのメンバである場合、**spanning-tree** [**vlan** *vlan-id*] **port-priority** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree** [**vlan** *vlan-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させるインターフェイスには、低いコスト値を割り当て、最後に選択させるインターフェイスには高いコスト値を割り当てます。

次の手順では、STP ポート プライオリティを使用した負荷分散を指定してネットワークを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	デバイス A で、グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp domain** *domain-name* 例： `Device(config)# vtp domain workdomain`	VTP 管理ドメインを設定します。 1 ～ 32 文字のドメイン名を使用できます。
ステップ 4	**vtp mode server** 例：	デバイス A を VTP サーバとして設定します。

	コマンドまたはアクション	目的
	`Device(config)# vtp mode server`	
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show vtp status** 例： `Device# show vtp status`	デバイス A およびデバイス B の両方で、VTP 設定を確認します。 表示された *VTP Operating Mode* および *VTP Domain Name* フィールドをチェックします。
ステップ 7	**show vlan** 例： `Device# show vlan`	デバイス A のデータベースに VLAN が存在していることを確認します。
ステップ 8	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 9	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	ポートをトランク ポートとして設定します。
ステップ 11	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 12	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet1/0/1 switchport`	VLAN の設定を確認します。
ステップ 13	デバイスAで、デバイスまたはデバイス スタック の2番目のポートに対して前述の手順を繰り返します。	
ステップ 14	デバイス B で前述の手順を繰り返し、デバイスAで設定したトランク ポートに接続するトランク ポートを設定します。	
ステップ 15	**show vlan** 例： `Device# show vlan`	トランク リンクがアクティブになると、VTP がデバイス B に VTP および VLAN 情報を渡します。このコマンドは、デバイス B が VLAN 設定を学習したことを確認します。
ステップ 16	**configure terminal** 例： `Device# configure terminal`	デバイス A で、グローバル コンフィギュレーションモードを開始します。
ステップ 17	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 18	**spanning-tree vlan** *vlan-range***port-priority** *priority-value* 例： `Device(config-if)# spanning-tree vlan 8-10 port-priority 16`	指定された VLAN 範囲にポート プライオリティを割り当てます。0 ～ 240 のポート プライオリティ値を入力します。ポート プライオリティ値は 16 ずつ増分します。
ステップ 19	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 20	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 21	**spanning-tree vlan** *vlan-range* **port-priority** *priority-value* 例： `Device(config-if)# spanning-tree vlan 3-6 port-priority 16`	指定された VLAN 範囲にポート プライオリティを割り当てます。0 ～ 240 のポート プライオリティ値を入力します。ポート プライオリティ値は 16 ずつ増分します。
ステップ 22	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 23	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 24	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

STP プライオリティによるネットワーク負荷分散 （3245 ページ）

STP パス コストによる負荷分散の設定（CLI）

次の手順では、STP パス コストを使用した負荷分散を指定してネットワークを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	デバイス A で、グローバル コンフィギュレーションモードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 4	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	ポートをトランク ポートとして設定します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーションモードに戻ります。
ステップ 6	デバイス A またはデバイス A スタック内の別のインターフェイスでステップ 2 ～ 4 を繰り返します。	
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。画面で、インターフェイスがトランク ポートとして設定されていることを確認してください。

	コマンドまたはアクション	目的
ステップ 9	**show vlan** 例： `Device# show vlan`	トランク リンクがアクティブになると、デバイス A がもう一方のデバイスから VTP 情報を受信します。このコマンドは、デバイス A が VLAN コンフィギュレーションを学習したことを確認します。
ステップ 10	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 11	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	STP コストを設定するインターフェイスを定義し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 12	**spanning-tree vlan** *vlan-range* **cost** *cost-value* 例： `Device(config-if)# spanning-tree vlan 2-4 cost 30`	VLAN 2 ～ 4 のスパニングツリー パス コストを 30 に設定します。
ステップ 13	**end** 例： `Device(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	デバイス A に設定したもう一方のトランク インターフェイスでステップ 9 ～ 13 を繰り返し、VLAN 8、9、および 10 のスパニングツリー パス コストを 30 に設定します。	
ステップ 15	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 16	**show running-config** 例： `Device# show running-config`	入力を確認します。両方のトランクインターフェイスに対してパスコストが正しく設定されていることを表示で確認します。
ステップ 17	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

STP パス コストによるネットワーク負荷分散 （3246 ページ）

次の作業

VLAN トランクを設定したら、次の項目を設定できます。

- VLANs
- VLAN グループ
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN コマンド リファレンス (Catalyst 3850 スイッチ)* 『*Layer 2/3 コマンド リファレンス (Catalyst 3850 スイッチ)*』
スパニング ツリー プロトコル（STP）	ネットワーク管理コマンド リファレンス *(Catalyst 3850 スイッチ)* ネットワーク管理コンフィギュレーション ガイド *(Catalyst 3850 スイッチ)*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

VLAN トランクの機能履歴と情報

リリース	変更内容

第 155 章

音声 VLAN の設定

- 機能情報の確認 （3263 ページ）
- 音声 VLAN の前提条件 （3263 ページ）
- 音声 VLAN の制約事項 （3264 ページ）
- 音声 VLAN に関する情報 （3264 ページ）
- 音声 VLAN の設定方法 （3267 ページ）
- 音声 VLAN のモニタリング （3271 ページ）
- 次の作業 （3271 ページ）
- その他の参考資料 （3271 ページ）
- 音声 VLAN の機能履歴と情報 （3273 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

音声 VLAN の前提条件

音声 VLAN の前提条件は、次のとおりです。

- 音声 VLAN 設定はデバイスのアクセス ポートだけでサポートされており、トランク ポートではサポートされていません。

（注） トランク ポートは、標準VLANと同様に、任意の数の音声VLANを伝送できます。トランク ポートでは、音声 VLAN の設定がサポートされません。

- 音声 VLAN を有効にする前に、 **trust device cisco-phone** インターフェイス設定コマンドを入力し、デバイス上の QoS をイネーブルにします。Auto QoS 機能を使用すると、これらは自動的に設定されます。
- IP Phone にコンフィギュレーションを送信するために、Cisco IP Phone に接続するデバイス ポート上で CDP をイネーブルにする必要があります（デフォルト設定では、CDP がすべてのデバイス インターフェイスでグローバルにイネーブルになっています）。

音声 VLAN の制約事項

音声 VLAN には、スタティック セキュア MAC アドレスを設定できません。

音声 VLAN に関する情報

音声 VLAN

音声 VLAN 機能を使用すると、アクセス ポートで IP Phone からの IP 音声トラフィックを伝送できます。デバイスを Cisco 7960 IP Phone に接続すると、IP Phone はレイヤ 3 IP 値およびレイヤ 2 サービス クラス（CoS）値を使用して、音声トラフィックを送信します。どちらの値もデフォルトでは 5 に設定されます。データ送信が均質性に欠ける場合、IP Phone の音質が低下することがあります。そのため、このデバイスは IEEE 802.1p CoS に基づく Quality of Service（QoS）をサポートしています。QoS は、分類およびスケジューリングを使用して、デバイスからのネットワーク トラフィックを予測可能な方法で送信します。

デフォルトでは、音声 VLAN 機能は無効になっています。この機能が有効の場合、すべてのタグなしトラフィックはポートのデフォルトの CoS プライオリティに従って送信されます。CoS 値は、IEEE 802.1Q および 802.1p タグ付きトラフィックでは信頼されません。

Cisco7960 IP Phone は設定可能なデバイスであり、IEEE 802.1p プライオリティに基づいてトラフィックを転送するように設定できます。Cisco IP Phone によって割り当てられたトラフィックの優先度を信頼したり、オーバーライドしたりするようにデバイスを設定できます。

Cisco IP Phone の音声トラフィック

Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。Cisco Discovery Protocol（CDP）パケットを送信するよう、デバイス上の

アクセス ポートを設定できます。CDP パケットは、接続する IP Phone に対して、次のいずれかの方法で音声トラフィックをデバイスに送信するよう指示します。

- レイヤ 2 CoS プライオリティ値のタグ付き音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値のタグ付きアクセス VLAN による送信
- タグなし（レイヤ 2 CoS プライオリティ値なし）のアクセス VLAN による送信

（注） いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（音声トラフィックはデフォルトで 5、音声制御トラフィックは 3）を伝送します。

関連トピック

Cisco IP Phone の音声トラフィックの設定（CLI） （3267 ページ）
音声 VLAN のモニタリング （3271 ページ）

Cisco IP Phone のデータ トラフィック

デバイスは、Cisco IP Phone のアクセス ポートに接続されたデバイスから送られる、タグ付きデータ トラフィック（IEEE 802.1Q または IEEE 802.1p フレーム タイプのトラフィック）を処理することもできます。CDP パケットを送信するよう、デバイス上のレイヤ 2 アクセス ポートを設定できます。CDP パケットは、接続する IP Phone に対して、次のいずれかのモードで IP Phone アクセス ポートを設定するよう指示します。

- trusted（信頼性がある）モードでは、Cisco IP Phone のアクセス ポート経由で受信したすべてのトラフィックがそのまま IP Phone を通過します。
- untrusted（信頼性がない）モードでは、Cisco IP Phone のアクセス ポート経由で受信した IEEE 802.1Q および IEEE 802.1p フレームのすべてのトラフィックに、設定されたレイヤ 2 CoS 値を与えます。デフォルトのレイヤ 2 CoS 値は 0 です。信頼できないモードがデフォルト設定です。

（注） Cisco IP Phone に接続されたデバイスからのタグなしトラフィックは、IP Phone のアクセス ポートの信頼状態に関係なく、そのまま IP Phone を通過します。

関連トピック

着信データ フレームのプライオリティ設定（CLI） （3269 ページ）
音声 VLAN のモニタリング （3271 ページ）

音声 VLAN 設定時の注意事項

- Cisco7960 IP Phone は、PC やその他のデバイスとの接続もサポートしているので、デバイスを Cisco IP Phone に接続するポートは、さまざまな種類のトラフィックを伝送できます。

ポートを設定することによって、Cisco IP Phone による音声トラフィックおよびデータ トラフィックの伝送方法を決定できます。

- IP Phone で音声 VLAN 通信が適切に行われるには、デバイス上に音声 VLAN が存在し、アクティブになっている必要があります。VLAN が存在しているかどうかを確認するには、**show vlan** 特権 EXEC コマンドを使用します（リストで表示されます）。VLAN がリストされていない場合は、音声 VLAN を作成します。
- Power Over Ethernet（PoE）デバイスは、シスコ先行標準の受電デバイスまたは IEEE 802.3af 準拠の受電デバイスが AC 電源から電力を供給されてない場合に、それらの受電デバイスに自動的に電力を供給できます。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。
- Cisco IP Phone とその IP Phone に接続されたデバイスが同じ VLAN 上にある場合、両方とも同じ IP サブネットに属していなければなりません。次の条件が満たされている場合は、同じ VLAN 上にあります。
  - 両方とも IEEE 802.1p またはタグなしフレームを使用する。
  - Cisco IP Phone が IEEE 802.1p フレームを使用し、デバイスがタグなしフレームを使用する。
  - Cisco IP Phone がタグなしフレームを使用し、デバイスが IEEE 802.1p フレームを使用する。
  - Cisco IP Phone が IEEE 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである。
- Cisco IP Phone と IP Phone に接続されたデバイスは、同一 VLAN、同一サブネット上にあっても、使用するフレーム タイプが異なる場合は通信できません。トラフィックは同一サブネット上でルーティングされないからです（ルーティングによってフレーム タイプの相違が排除されます）。
- 音声 VLAN ポートには次のポート タイプがあります。
  - ダイナミック アクセス ポート。
  - IEEE 802.1x 認証ポート。

    （注） 音声 VLAN が設定され Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x を有効にした場合、その IP Phone からデバイスへの接続が最大 30 秒間失われます。

  - 保護ポート。
  - SPAN または RSPAN セッションの送信元ポートまたは宛先ポート。
  - セキュア ポート。

（注） 音声 VLAN も設定しているインターフェイス上でポート セキュリティをイネーブルにする場合、ポートで許容されるセキュアアドレスの最大数を、アクセス VLAN におけるセキュア アドレスの最大数に 2 を足した数に設定する必要があります。ポートを Cisco IP Phone に接続している場合、IP Phone に最大で 2 つの MAC アドレスが必要になります。IP Phone のアドレスは、音声 VLAN で学習され、アクセス VLAN でも学習される場合があります。PC を IP Phone に接続する場合、追加の MAC アドレスが必要になります。

音声 VLAN の設定方法

Cisco IP Phone の音声トラフィックの設定（CLI）

Cisco IP Phone に CDP パケットを送信して IP Phone による音声トラフィックの送信方法を設定するように、IP Phone に接続するポートを設定できます。IP Phone は指定された音声 VLAN に、レイヤ 2 CoS 値を使用して、IEEE 802.1Q フレームの音声トラフィックを伝送できます。IEEE 802.1p のプライオリティ タグを使用すると、音声トラフィックにさらに高いプライオリティを与え、すべての音声トラフィックをネイティブ（アクセス）VLAN 経由で転送できます。Cisco IP Phone はタグなしの音声トラフィックを送信する、または独自の設定を使用してアクセス VLAN で音声トラフィックを送信することもできます。いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（デフォルトは 5）を伝送します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**trust device cisco-phone** 例： `Device(config-if)# trust-device cisco-phone`	Cisco IP Phone の着信トラフィック パケットを信頼するようにインターフェイスを設定します。
ステップ 4	**switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**} 例： `Device(config-if)# switchport voice vlan dot1p`	音声 VLAN を設定します。 • *vlan-id*：すべての音声トラフィックが特定の VLAN を経由して転送されるように IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。指定できる VLAN ID の範囲は 1 ～ 4094 です。 • **dot1p**：VLAN ID 0（ネイティブ VLAN）のタグが付けられた音声およびデータ IEEE 802.1p プライオリティ フレームを受け入れるよう、デバイスを設定します。デフォルトでは、デバイスは VLAN 0 のタグが付いたすべての音声およびデータ トラフィックをドロップします。802.1p に対応するよう設定されると、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用してトラフィックを転送します。 • **none**：IP Phone で独自の設定を使ってタグなし音声トラフィックを送信できるようにします。 • **untagged**：タグなしの音声トラフィックを送信するように電話を設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	次のいずれかを使用します。 • **show interfaces** *interface-id***switchport**	音声 VLAN の設定、または QoS および音声 VLAN の設定を確認します。

	コマンドまたはアクション	目的

	• **show running-config interface** *interface-id*
	例：
	`Device# show interfaces gigabitethernet1/0/1 switchport`
	または
	`Device# show running-config interface gigabitethernet1/0/1`	

ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

Cisco IP Phone の音声トラフィック （3264 ページ）
音声 VLAN のモニタリング （3271 ページ）

着信データ フレームのプライオリティ設定（CLI）

PC またはその他のデータ デバイスを Cisco IP Phone ポートに接続できます。タグ付きデータ トラフィック（IEEE 802.1Q または IEEE 802.1p フレーム）を処理するために、CDP パケットを送信するようデバイスを設定できます。CDP パケットは Cisco IP Phone に対して、IP Phone 上のアクセス ポートに接続されたデバイスからのデータ パケット送信方法を指示します。PC は、CoS 値が割り当てられたパケットを生成できます。接続デバイスから IP Phone のポートに届いたフレームのプライオリティを変更しない（信頼する）または変更する（信頼しない）ように、IP Phone を設定できます。

Cisco IP Phone で非音声ポートから受信するデータ トラフィックのプライオリティを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	Cisco IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport priority extend** {**cos** *value* | **trust**} 例： `Device(config-if)# switchport priority extend trust`	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプライオリティを次のように設定します。 • **cos** *value*：PC または接続しているデバイスから受信したプライオリティを、指定の CoS 値にオーバーライドするよう、IP Phone を設定します。値は 0 ～ 7 です。7 が最高のプライオリティです。デフォルトのプライオリティは **cos** 0 です。 • **trust**：PC または接続しているデバイスから受信したプライオリティを信頼するよう IP Phone アクセス ポートを設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

関連トピック

Cisco IP Phone のデータ トラフィック （3265 ページ）
音声 VLAN のモニタリング （3271 ページ）

音声 VLAN のモニタリング

インターフェイスの音声 VLAN 設定を表示するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを使用します。

関連トピック

Cisco IP Phone の音声トラフィックの設定（CLI） （3267 ページ）
Cisco IP Phone の音声トラフィック （3264 ページ）
着信データ フレームのプライオリティ設定（CLI） （3269 ページ）
Cisco IP Phone のデータ トラフィック （3265 ページ）

次の作業

音声 VLAN を設定した後は、次の設定を行うことができます。

- VLANs
- VLAN グループ
- VLAN トランキング
- VTP

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN コマンド リファレンス (Catalyst 3850 スイッチ)* 『*Layer 2/3 コマンド リファレンス (Catalyst 3850 スイッチ)*』

関連項目	マニュアル タイトル
追加の設定コマンドおよび手順。	『*LAN Switching* コンフィギュレーション ガイド, *Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』 『*Layer 2/3* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)*』
プラットフォームに依存しない設定情報	『*Identity Based Networking Services* コンフィギュレーション ガイド, *Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

音声 VLAN の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 156 章

プライベート VLAN の設定

- 機能情報の確認 （3275 ページ）
- プライベート VLAN の前提条件 （3275 ページ）
- プライベート VLAN の制約事項 （3276 ページ）
- プライベート VLAN について （3277 ページ）
- プライベート VLAN の設定方法 （3288 ページ）
- プライベート VLAN のモニタ （3298 ページ）
- プライベート VLAN の設定例 （3299 ページ）
- 次の作業 （3301 ページ）
- その他の参考資料 （3302 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

プライベート VLAN の前提条件

プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は、VTP 3 のサーバ モードでもサポートされます。

プライベート VLAN をデバイスに設定するときに、ユニキャスト ルートとレイヤ 2 エントリとの間のシステム リソースのバランスを取るために、常にデフォルトの Switch Database Management（SDM）テンプレートを使用してください。別の SDM テンプレートが設定されて

いる場合、デフォルト テンプレートを設定するのに **sdm prefer default** グローバル コンフィギュレーション コマンドを使用します。

プライベート VLAN の制約事項

（注） 一部の状況では、エラーメッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

- プライベート VLAN が設定されているデバイスでは、フォールバック ブリッジングを設定しないでください。
- リモート SPAN（RSPAN）をプライベート VLAN のプライマリまたはセカンダリ VLAN として設定しないでください。
- 次のような機能が設定されているインターフェイスにプライベート VLAN ポートを設定しないでください。
  - ダイナミック アクセス ポート VLAN メンバーシップ
  - ダイナミック トランキング プロトコル（DTP）
  - IPv6 Security Group（SG）
  - ポート集約プロトコル（PAgP）
  - リンク集約制御プロトコル（LACP）
  - マルチキャスト VLAN レジストレーション（MVR）
  - 音声 VLAN
  - Web Cache Communication Protocol（WCCP）
- IEEE 802.1x ポートベース認証をプライベート VLAN ポートに設定できますが、802.1x とポート セキュリティ、音声 VLAN、またはポート単位のユーザ ACL は、プライベート VLAN ポートに設定できません。
- プライベート VLAN ホストまたは無差別ポートは SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートに設定した場合、ポートは非アクティブになります。
- プライマリ VLAN の無差別ポートでスタティック MAC アドレスを設定する場合は、すべての関連セカンダリ VLAN に同じスタティック アドレスを追加する必要はありません。同様に、セカンダリ VLAN のホスト ポートでスタティック MAC アドレスを設定する場合は、関連プライマリ VLAN に同じスタティック MAC アドレスを追加する必要はありません。さらに、スタティック MAC アドレスをプライベート VLAN ポートから削除する際

に、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要はありません。

（注） プライベート VLAN のセカンダリ VLAN で学習したダイナミック MAC アドレスは、関連プライマリ VLAN で複製されます。プライマリ VLANからトラフィックが入力される場合でも、すべての MAC エントリはセカンダリ VLANで学習されます。MAC アドレスがプライマリ VLAN で動的に学習される場合は、関連セカンダリ VLAN では複製されません。

- レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。

プライベート VLAN について

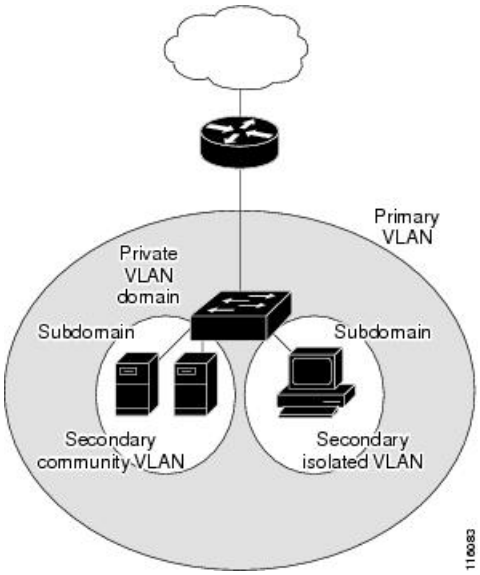
プライベート VLAN ドメイン

PVLAN 機能を使用すると、サービス プロバイダーが VLAN を使用したときに直面する 2 つの問題に対処できます。

- IP Base イメージまたは IP Services イメージを実行している場合、最大で 4094 個のアクティブ VLAN がデバイスでサポートされます。サービス プロバイダーが 1 カスタマーあたり 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数はこれに制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てますが、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。

図 *148 :* プライベート *VLAN* ドメイン

プライベート VLAN の使用でスケーラビリティの問題に対処でき、サービス プロバイダーにとってはIPアドレス管理上の利得がもたらされ、カスタマーに対してはレイヤ2セキュリティを提供できます。プライベート VLAN では、通常の VLAN ドメインをサブドメインに分割します。サブドメインは、プライマリ VLAN とセカンダリ VLAN のペアで表されます。プライベート VLAN には複数の VLAN ペアを設定可能で、各サブドメインにつき 1 ペアになります。プライベート VLAN 内のすべての VLAN ペアは同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、各サブドメインの区別に使用されます。



Secondary VLANs

セカンダリ VLAN には、次の 2 種類があります。

- 独立 VLAN：独立 VLAN 内のポートは、レイヤ 2 レベルでは相互に通信できません。
- コミュニティ VLAN：コミュニティ VLAN 内のポートは互いに通信できますが、レイヤ 2 レベルにある他のコミュニティ内のポートとは通信できません。

関連トピック

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング（3296 ページ）
例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする（3301 ページ）

プライベート VLAN ポート

プライベート VLAN では、同じプライベート VLAN 内のポート間をレイヤ 2 で分離します。プライベート VLAN ポートは、次のいずれかの種類に属するアクセス ポートです。

- 無差別：無差別ポートは、プライベート VLAN に属し、プライマリ VLAN と関連しているセカンダリ VLAN に属するコミュニティ ポートや独立ホスト ポートなどの、すべてのインターフェイスと通信できます。
- 独立：独立ポートは、独立セカンダリ VLAN に属しているホスト ポートです。これは、無差別ポートを除く、同じプライベート VLAN 内の他のポートからレイヤ 2 で完全に分離されています。プライベート VLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。

- コミュニティ：コミュニティ ポートは、1 つのコミュニティ セカンダリ VLAN に属しているホスト ポートです。コミュニティ ポートは、同一コミュニティ VLAN のその他のポート、および無差別ポートと通信します。これらのインターフェイスは、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN 内の独立ポートとレイヤ 2 で分離されます。

（注） トランク ポートは、通常の VLAN からのトラフィックを伝送し、またプライマリ、独立、およびコミュニティ VLAN からのトラフィックも伝送します。

プライマリおよびセカンダリ VLAN には次のような特性があります。

- プライマリ VLAN：プライベート VLAN には、プライマリ VLAN を 1 つだけ設定できます。プライベート VLAN 内のすべてのポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、無差別ポートからの単一方向トラフィックのダウンストリームを、（独立およびコミュニティ）ホスト ポートおよび他の無差別ポートへ伝送します。
- 独立 VLAN：プライベート VLAN の独立 VLAN は 1 つだけです。独立 VLAN はセカンダリ VLAN であり、ホストから無差別ポートおよびゲートウェイに向かう単一方向トラフィック アップストリームを搬送します。
- コミュニティ VLAN：コミュニティ VLAN は、アップストリーム トラフィックをコミュニティ ポートから無差別ポート ゲートウェイおよび同じコミュニティ内の他のホスト ポートに伝送するセカンダリ VLAN です。複数のコミュニティ VLAN を 1 つのプライベート VLAN に設定できます。

無差別ポートは、1 つのプライマリ VLAN、1 つの独立 VLAN、複数のコミュニティ VLAN だけで動作できます。レイヤ 3 ゲートウェイは通常、無差別ポートを介してデバイスに接続されます。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションから監視したりバックアップしたりするのに、無差別ポートを使用できます。

関連トピック

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 （3293 ページ）
プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 （3294 ページ）
例：ホスト ポートとしてのインターフェイスの設定 （3299 ページ）
例：プライベート VLAN 無差別ポートとしてのインターフェイスの設定 （3300 ページ）

ネットワーク内のプライベート VLAN

スイッチング環境では、個々のエンド ステーションに、または共通グループのエンド ステーションに、個別のプライベート VLAN や、関連する IP サブネットを割り当てることができま

す。エンド ステーションはデフォルト ゲートウェイとの通信を行うだけで、プライベート VLAN の外部と通信することができます。

プライベートVLANを使用し、次の方法でエンドステーションへのアクセスを制御できます。

- エンドステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ2の通信をしないようにします。たとえば、エンドステーションがサーバの場合、この設定によりサーバ間のレイヤ 2 通信ができなくなります。
- デフォルトゲートウェイおよび選択したエンドステーション（バックアップサーバなど）に接続されているインターフェイスを無差別ポートとして設定し、すべてのエンドステーションがデフォルト ゲートウェイにアクセスできるようにします。

複数のデバイスにわたるようにプライベート VLAN を拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他のデバイスにトランキングします。使用するプライベート VLAN 設定のセキュリティを確保して、プライベート VLAN として設定された VLAN が他の目的に使用されないようにするには、プライベート VLAN ポートがないデバイスを含めて、すべての中間デバイスでプライベート VLAN を設定します。

プライベート VLAN での IP アドレッシング方式

各カスタマーに個別の VLAN を割り当てると、次のように IP アドレッシング方式が非効率的になります。

- カスタマー VLAN にアドレスのブロックを割り当てると、未使用 IP アドレスが発生することがあります。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

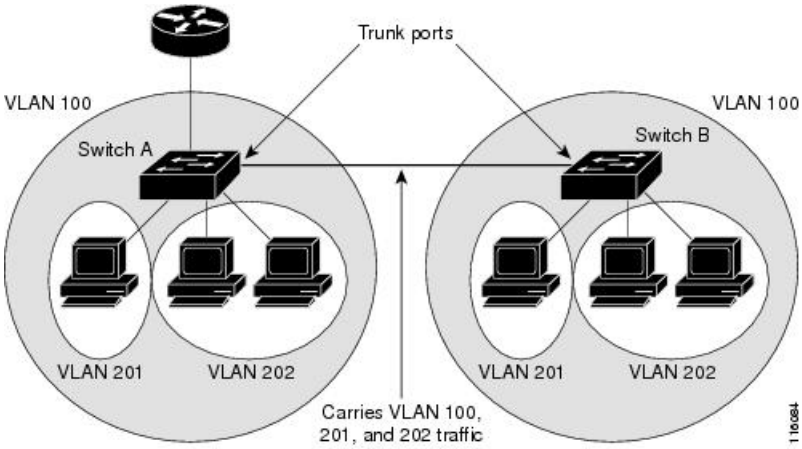
この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベート VLAN のすべてのメンバーが、プライマリ VLAN に割り当てられている共通アドレス空間を共有するためです。ホストはセカンダリ VLAN に接続され、プライマリ VLAN に割り当てられているアドレスのブロックから IP アドレスが DHCP サーバによってホストに割り当てられますが、同一プライマリ VLAN 内のセカンダリ VLAN には割り当てられません。さまざまなセカンダリ VLAN のカスタマー デバイスには後続 IP アドレスが割り当てられます。新しいデバイスを追加すると、サブネットアドレスの巨大プールから次に使用できるアドレスが、DHCP サーバによって割り当てられます。

複数のデバイスにまたがるプライベート VLAN

図 *149 :* 複数のスイッチにまたがるプライベート *VLAN*

通常の VLAN と同様に、プライベート VLAN を複数のデバイスにまたがるように設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN をネイバーデバイス に伝送します。トランク ポートはプライベート VLAN を他の VLAN として扱います。複数のデバイ

スにまたがるプライベート VLAN の機能の特徴として、デバイス A にある独立ポートからのトラフィックはデバイス B に到達しません。



VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community VLAN

プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は VTP 3 のサーバ モードでもサポートされます。VTP 3 を使用して設定したサーバ クライアントがある場合、サーバに設定されているプライベート VLAN をクライアント上に反映させる必要があります。

プライベート VLAN の他機能との相互作用

プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック

通常の VLAN では、同じ VLAN にあるデバイスはレイヤ 2 レベルで互いに通信しますが、別の VLAN にあるインターフェイスに接続されたデバイスとはレイヤ 3 レベルで通信する必要があります。プライベート VLAN の場合、無差別ポートはプライマリ VLAN のメンバーであり、ホスト ポートはセカンダリ VLAN に属します。セカンダリ VLAN はプライマリ VLAN に対応付けられているため、これらの VLAN のメンバーはレイヤ 2 レベルで互いに通信できます。

通常の VLAN の場合、ブロードキャストはその VLAN のすべてのポートに転送されます。プライベート VLAN のブロードキャストの転送は、次のようにブロードキャストを送信するポートによって決まります。

- 独立ポートは、無差別ポートまたはトランク ポートだけにブロードキャストを送信します。
- コミュニティ ポートは、すべての無差別ポート、トランク ポート、同一コミュニティ VLAN のポートにブロードキャストを送信します。

- 無差別ポートは、プライベート VLAN のすべてのポート（その他の無差別ポート、トランク ポート、独立ポート、コミュニティ ポート）にブロードキャストを送信します。

マルチキャスト トラフィックのルーティングとブリッジングは、プライベート VLAN 境界を横断して行われ、単一コミュニティ VLAN 内でも行われます。マルチキャスト トラフィックは、同一独立 VLAN のポート間、または別々のセカンダリ VLAN のポート間で転送されません。

プライベート VLAN のマルチキャスト転送は次の状況をサポートします。

- 送信側が VLAN 外に存在する可能性があり、受信側が VLAN ドメイン内に存在している可能性がある。
- 送信側が VLAN 内に存在する可能性があり、受信側が VLAN ドメイン外に存在している可能性がある。
- 送信側と受信側が同一のコミュニティ VLAN に存在している可能性がある。

プライベート VLAN と SVI

レイヤ 3 スイッチデバイスでは、デバイス仮想インターフェイス（SVI）が VLAN のレイヤ 3 インターフェイスを表します。レイヤ 3 デバイスは、セカンダリ VLAN ではなく、プライマリ VLAN だけを介してプライベート VLAN と通信します。レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。レイヤ 3 VLAN インターフェイスをセカンダリ VLAN 用に設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI はアクティブになりません。

- SVI がアクティブである VLAN をセカンダリ VLAN として設定する場合、SVI をディセーブルにしないと、この設定は許可されません。
- セカンダリ VLAN として設定されている VLAN に SVI を作成しようとしてセカンダリ VLAN がすでにレイヤ 3 にマッピングされている場合、SVI は作成されず、エラーが返されます。SVI がレイヤ 3 にマッピングされていない場合、SVI は作成されますが、自動的にシャットダウンされます。

プライマリ VLAN をセカンダリ VLAN と関連付けてマッピングすると、プライマリ VLAN の設定がセカンダリ VLAN の SVI に伝播されます。たとえば、プライマリ VLAN の SVI に IP サブネットを割り当てると、このサブネットは、プライベート VLAN 全体の IP サブネット アドレスになります。

プライベート VLAN とデバイススタック

プライベート VLAN はデバイススタック内で動作することができ、プライベート VLAN ポートはさまざまなスタック メンバーに存在することができます。ただし、スタックを次のように変更すると、プライベート VLAN の動作に影響が及ぶ可能性があります。

- スタックにプライベート VLAN 無差別ポートが 1 つだけ含まれ、このポートを含めたスタック メンバーがスタックから削除された場合、プライベート VLAN のホスト ポートとプライベート VLAN 外との接続が不能になります。

- スタック内にプライベート VLAN 無差別ポートが 1 つだけあるスタック マスターに障害が発生した場合、またはスタックを残し、新しいスタック マスターが選択された場合、古いスタック マスターに無差別ポートがあるプライベート VLAN のホスト ポートとプライベート VLAN 外との接続が不能になります。
- 2 つのスタックが統合された場合、権利を獲得したスタックのプライベート VLAN は影響を受けませんが、デバイスを再起動したときに、権利を獲得しなかったデバイスのプライベート VLAN 設定が失われます。

ダイナミック MAC アドレスを備えたプライベート VLAN

セカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN で複製されますが、その逆はありません。これにより、ハードウェアの L2 CAM スペースを節約できます。プライマリ VLAN は常に、両方向で正引きを実行するのに使用されます。

ダイナミック MAC アドレスは、プライベート VLAN のプライマリ VLAN で学習されると、必要に応じて、セカンダリ VLAN で複製されます。たとえば、MAC アドレスがセカンダリ VLAN で動的に受信されると、プライマリ VLAN の一部として学習されます。隔離 VLAN の場合、同じ MAC のブロックされたエントリは MAC アドレス テーブルのセカンダリ VLAN に追加されます。このため、セカンダリ ドメインのホスト ポートで学習された MAC は、ブロックされたタイプのエントリとしてインストールされます。プライマリ VLAN からトラフィックが入力される場合でも、すべての MAC エントリはセカンダリ VLAN で学習されます。

MAC アドレスがプライマリ VLAN で動的に学習される場合、関連セカンダリ VLAN では複製されません。

スタティック MAC アドレスを備えたプライベート VLAN

ユーザは、従来型のようにプライベート VLAN のホストにスタティック MAC アドレス CLI を複製する必要はありません。

例：

- 従来のモデルでは、ユーザはスタティック MAC アドレスを設定すると、関連 VLAN 内にも同じスタティック MAC アドレスを追加する必要がありました。たとえば、MAC アドレス A が VLAN 101 のポート 1/0/1 でユーザ設定され、VLAN 101 ではセカンダリ VLAN で、VLAN 100 がプライマリ VLAN である場合は、ユーザは設定する必要があります。

```
mac-address static A vlan 101 interface G1/0/1
mac-address static A vlan 100 interface G1/0/1
```

- このデバイスでは、ユーザは関連 VLAN に MAC アドレスを複製する必要はありません。上記の例のみで、ユーザは設定する必要があります。

```
mac-address static A vlan 101 interface G1/0/1
```

プライベート VLAN と VACL/QOS との相互作用

プライベート VLAN は、このデバイスの場合、他のプラットフォームの「単方向」と比べ、双方向です。

レイヤ 2 の正引き後には、適切な出力 VLAN マッピングが行われ、すべての出力 VLAN ベースの機能による処理が出力 VLAN のコンテキストで実行されます。

レイヤ2のフレームがプライベートVLAN内で転送されると、入力側と出力側とでVLANマップが適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベートVLANマップが入力側に適用されます。同様に、フレームが外部ポートからプライベート VLAN にルーティングされると、プライベート VLAN は出力側に適用されます。これは、ブリッジされたトラフィックとルーティングされたトラフィックの両方に適用されます。

ブリッジング：

- セカンダリ VLAN からプライマリ VLAN へのアップストリーム トラフィックの場合、セカンダリ VLAN の MAP は入力側に適用され、プライマリ VLAN の MAP は出力側に適用されます。
- プライマリ VLAN からセカンダリ VLAN へのダウンストリーム トラフィックの場合は、プライマリ VLAN の MAP は入力方向で適用され、セカンダリ VLAN のMAP は出力方向で適用されます。

Routing

プライベート VLAN ドメインが 2 つ（PV1（sec1、prim1）および PV2（sec2、prim2））ある場合を想定します。PV1 から PV2 にルーティングされるフレームについては次のようになります。

- sec1 の MAP および prim1 の L3 ACL は、入力ポートに適用されます。
- sec2 の MAP および prim2 の L3 ACL は、出力ポートに適用されます。

分離されたホストポートから無差別ポートへのアップストリームまたはダウンストリームに従うパケットの場合、分離された VLAN の VACL は入力方向に適用され、プライマリ VLAN の VACL は出力方向に適用されます。これにより、ユーザは同じプライマリ VLAN ドメインの別のセカンダリ VLAN に異なる VACL を設定することができます。

（注） このデバイスでのプライベートVLANは常に双方向であるため、双方向のコミュニティ VLAN は不要です。

プライベート VLAN および HA サポート

PVLANは、高可用性（HA）機能とシームレスに連携します。スイッチオーバーの前に、マスターにあるプライベート VLAN は、スイッチオーバー後と同じである必要があります（新しいマスターはIOS側および、FED側両方で以前のマスターと同様のPVLAN設定が必要です）。

プライベート VLAN 設定時の注意事項

プライベート VLAN のデフォルト設定

プライベート VLAN は設定されていません。

セカンダリ VLAN およびプライマリ VLAN の設定

プライベート VLAN の設定時は、次の注意事項に従ってください。

- プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。デバイスで VTP バージョン 1 または 2 が稼働している場合は、VTP をトランスペアレントモードに設定する必要があります。プライベートVLANを設定した後で、VTPモードをクライアントまたはサーバに変更できません。VTP バージョン 3 は、すべてのモードでプライベート VLAN をサポートします。
- VTP バージョン 1 または 2 でプライベート VLAN を設定した後、**copy running-config startup config** 特権 EXEC コマンドを使用して、VTP トランスペアレント モード設定とプライベート VLAN 設定を デバイス スタートアップ コンフィギュレーション ファイルに保存します。保存しないと、デバイスをリセットした場合にデフォルトのVTPサーバモードになり、プライベート VLAN をサポートしなくなります。VTP バージョン 3 ではプライベート VLAN をサポートします。
- VTP バージョン 1 および 2 では、プライベート VLAN 設定の伝播は行われません。プライベートVLANポートが必要なデバイスでVTPバージョン3が実行されていない場合は、VTP3 はプライベート VLAN を伝播するため、そのデバイス上でプライベート VLAN を設定する必要があります。
- VLAN 1 または VLAN 1002 ～ 1005 をプライマリ VLAN またはセカンダリ VLAN として設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）はプライベート VLAN に属することができます。
- プライマリ VLAN には、1 つの独立 VLAN および複数のコミュニティ VLAN を関連付けることができます。独立 VLAN またはコミュニティ VLAN には、1 つのプライマリ VLAN だけを関連付けることができます。
- プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行可能なスパニングツリー プロトコル（STP）インスタンスは 1 つだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。
- TFTP サーバから PVLAN 設定をコピーし、それを実行中の設定に適用しても、PVLAN の関連付けは形成されません。プライマリ VLAN がすべてのセカンダリ VLAN に確実に関連付けられていることを確認する必要があります。

  また、**copy flash:config_file running-config** の代わりに **configure replace flash:config_file force** も使用できます。

- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、DHCP スヌーピングはセカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定しても、プライマリ VLAN をすでに設定している場合、DHCP 設定は有効になりません。
- プライベート VLAN ポートで IP ソース ガードをイネーブルにする場合は、プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。
- プライベート VLAN でトラフィックを伝送しないデバイスのトランクから、プライベート VLAN をプルーニングすることを推奨します。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の Quality of Service（QoS）設定を適用できます
- sticky ARP には、次の考慮事項があります。
  - sticky ARP エントリとは、SVI およびレイヤ 3 インターフェイス上で学習されるエントリです。これらのエントリは、期限切れになることはありません。
  - **ip sticky-arp** グローバル コンフィギュレーション コマンドは、プライベート VLAN に属する SVI でだけサポートされます。
  - **ip sticky-arp** インターフェイス コンフィギュレーション コマンドは、以下でのみサポートされます。
    - レイヤ 3 インターフェイス
    - 標準 VLAN に属する SVI
    - プライベート VLAN に属する SVI

    ip sticky-arp グローバル コンフィギュレーション コマンドおよび **ip sticky-arpinterface** コンフィギュレーション コマンドの使用の詳細については、このリリースのコマンド リファレンスを参照してください。
- プライマリ VLAN およびセカンダリ VLAN で VLAN マップを設定できますただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- PVLAN は双方向です。これらは、入力側と出力側の両方に適用されます。

  レイヤ 2 のフレームがプライベート VLAN 内で転送されると、入力側と出力側で VLAN マップが適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。同様に、フレームが外部ポートからプライベート VLAN にルーティングされると、プライベート VLAN は出力側に適用されます。

  ブリッジング

  - セカンダリ VLAN からプライマリ VLAN へのアップストリーム トラフィックの場合、セカンダリ VLAN の MAP は入力側に適用され、プライマリ VLAN の MAP は出力側に適用されます。

- プライマリ VLAN からセカンダリ VLAN へのダウンストリーム トラフィックの場合は、プライマリ VLAN の MAP は入力方向で適用され、セカンダリ VLAN のMAP は出力方向で適用されます。

Routing

プライベート VLAN ドメインが 2 つ（PV1（sec1、prim1）および PV2（sec2、prim2））ある場合を想定します。PV1 から PV2 にルーティングされるフレームについては次のようになります。

- sec1 の MAP および prim1 の L3 ACL は入力ポートに適用されます。
- sec1 の MAP および prim2 の L3 ACL は出力ポートに適用されます。
- 分離されたホスト ポートから無差別ポートへのアップストリームまたはダウンストリームに従うパケットの場合、分離された VLAN の VACL は入力方向に適用され、プライマリ VLAN の VACL は出力方向に適用されます。これにより、ユーザは同じプライマリ VLAN ドメインの別のセカンダリ VLAN に異なる VACL を設定することができます。

プライベート VLAN の特定 IP トラフィックをフィルタリングするには、プライマリ VLAN およびセカンダリ VLAN の両方に VLAN マップを適用する必要があります。

- プライマリ VLAN SVI にだけルータ ACL を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。
- プライベート VLAN がレイヤ 2 でホストを分離していても、ホストはレイヤ 3 で互いに通信できます。
- プライベート VLAN では、次のスイッチド ポート アナライザ（SPAN）機能がサポートされます。
  - プライベート VLAN を SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN ベースの SPAN（VSPAN）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別に監視することができます。

プライベート VLAN ポートの設定

プライベート VLAN ポートの設定時は、次の注意事項に従ってください。

- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てるには、プライベート VLAN コンフィギュレーション コマンドだけを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定する VLAN に割り当てられているレイヤ 2 アクセス ポートは、この VLAN がプライベート VLAN の設定に含まれている場合、非アクティブです。レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。

- PAgP または LACP EtherChannel に属するポートを、プライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN の設定に含まれている間は、そのポートの EtherChannel 設定はいずれも非アクティブです。
- 設定ミスによる STP ループの発生を防ぎ、STP コンバージェンスを高速化するには、独立ホスト ポートおよびコミュニティ ホスト ポート上で PortFast および BPDU ガードをイネーブルにします。イネーブルの場合、STP はすべての PortFast が設定されたレイヤ 2 LAN ポートに BPDU ガード機能を適用します。PortFast および BPDU ガードを無差別ポートでイネーブルにしないでください。
- プライベート VLAN の設定で使用される VLAN を削除すると、この VLAN に関連付けられたプライベート VLAN ポートが非アクティブになります。
- ネットワーク デバイスをトランク接続し、プライマリ VLAN およびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートはさまざまなネットワーク デバイス上で使用できます。

プライベート VLAN の設定方法

プライベート VLAN の設定

プライベート VLAN を設定するには、次の手順を実行します。

（注） プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は、VTP 3 のサーバ モードでもサポートされます。

手順

ステップ 1 VTP モードを **transparent** に設定します。

（注） 注：VTP3 の場合、サーバまたはトランスペアレント モードのいずれにもモードを設定できます。

ステップ 2 プライマリおよびセカンダリ VLAN を作成してこれらを対応付けします。

See the プライベート VLAN 内の VLAN の設定および対応付け （3289 ページ）

（注） VLAN がまだ作成されていない場合、プライベート VLAN 設定プロセスでこれを作成します。

ステップ 3 インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバーシップを割り当てます。

See the プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 （3293 ページ）

ステップ 4 インターフェイスを無差別ポートとして設定し、無差別ポートをプライマリおよびセカンダリ VLAN のペアにマッピングします。

See the プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 （3294 ページ）

ステップ 5 VLAN 間ルーティングを使用している場合、プライマリ SVI を設定し、セカンダリ VLAN をプライマリ SVI にマッピングします。

See the セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング （3296 ページ）

ステップ 6 プライマリ VLAN 設定を確認します。

プライベート VLAN 内の VLAN の設定および対応付け

private-vlan コマンドは VLAN コンフィギュレーション モードを終了するまで機能しません。

プライベート VLAN 内で VLAN を設定し、関連付けるには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp mode transparent** 例： `Device(config)# vtp mode transport`	VTP モードをトランスペアレントに設定します（VTP をディセーブルにします）。 （注） VTP3 の場合、サーバまたはトランスペアレントモードのいずれにもモードを設定できます。

	コマンドまたはアクション	目的
ステップ 4	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 5	**private-vlan primary** 例： `Device(config-vlan)# private-vlan primary`	VLAN をプライマリ VLAN として指定します。
ステップ 6	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**vlan** *vlan-id* 例： `Device(config)# vlan 501`	（任意）VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 8	**private-vlan isolated** 例： `Device(config-vlan)# private-vlan isolated`	VLAN を独立 VLAN として指定します。
ステップ 9	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**vlan** *vlan-id* 例： `Device(config)# vlan 502`	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 11	**private-vlan community** 例：	VLAN をコミュニティ VLAN として指定します。

	コマンドまたはアクション	目的
	`Device(config-vlan)# private-vlan community`	
ステップ 12	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**vlan** *vlan-id* 例： `Device(config)# vlan 503`	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 14	**private-vlan community** 例： `Device(config-vlan)# private-vlan community`	VLAN をコミュニティ VLAN として指定します。
ステップ 15	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	ステップ 4 で指定したプライマリ VLAN に関して VLAN コンフィギュレーション モードを開始します。
ステップ 17	**private-vlan association** [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-vlan)# private-vlan association 501-503`	セカンダリ VLAN をプライマリ VLAN に関連付けます。単一のプライベート VLAN ID でも、またはハイフンで連結したプライベート VLAN ID でもかまいません。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフ

	コマンドまたはアクション	目的
		ンで連結したプライベート VLAN ID です。 • *secondary_vlan_list* パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。 • *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN を関連付けます。 • セカンダリ VLAN とプライマリ VLAN 間の関連付けをクリアするには、*secondary_vlan_list* に **remove** キーワードを使用します。 • このコマンドは、VLAN コンフィギュレーションモードを終了するまで機能しません。
ステップ 18	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 19	**show vlan private-vlan** [**type**] または **show interfaces status** 例： `Device# show vlan private-vlan`	設定を確認します。
ステップ 20	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN ホスト ポートとして設定し、これをプライマリおよびセカンダリ VLAN に関連付けるには、次の手順を実行します。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/22`	設定するレイヤ2インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode private-vlan host** 例： `Device(config-if)# switchport mode private-vlan host`	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 5	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id* 例： `Device(config-if)# switchport private-vlan host-association 20 501`	レイヤ 2 ポートをプライベート VLAN と関連付けます。 （注） これは、レイヤ 2 インターフェイスに PVLAN を関連付けるために必要な手順です。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `Device# show interfaces gigabitethernet1/0/22 switchport`	設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

プライベート VLAN ポート （3278 ページ）
例：ホスト ポートとしてのインターフェイスの設定 （3299 ページ）
例：プライベート VLAN 無差別ポートとしてのインターフェイスの設定 （3300 ページ）

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN 無差別ポートとして設定し、これをプライマリおよびセカンダリ VLAN にマッピングするには、次の手順を実行します。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するレイヤ2インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode private-vlan promiscuous** 例： `Device(config-if)# switchport mode private-vlan promiscuous`	レイヤ 2 ポートをプライベート VLAN 無差別ポートとして設定します。
ステップ 5	**switchport private-vlan mapping** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list* 例： `Device(config-if)# switchport private-vlan mapping 20 add 501-503`	プライベート VLAN 無差別ポートをプライマリ VLAN、および選択したセカンダリ VLAN にマッピングします。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。 • セカンダリ VLAN とプライマリ VLAN をプライベート VLAN 無差別ポートにマッピングするには、*secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用します。 • セカンダリ VLAN とプライベート VLAN 無差別ポートのマッピングを解除するには、**remove** キーワードを指定した *secondary_vlan_list* を使用します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `Device# show interfaces gigabitethernet1/0/2 switchport`	設定を確認します。
ステップ 8	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

関連トピック

プライベート VLAN ポート （3278 ページ）
例：ホスト ポートとしてのインターフェイスの設定 （3299 ページ）
例：プライベート VLAN 無差別ポートとしてのインターフェイスの設定 （3300 ページ）

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング

プライベート VLAN が VLAN 間ルーティングに使用される場合、SVI をプライマリ VLAN に設定してセカンダリ VLAN を SVI にマッピングできます。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

セカンダリ VLAN をプライマリ VLAN の SVI にマッピングしてプライベート VLAN トラフィックのレイヤ 3 スイッチングを可能にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface vlan** *primary_vlan_id* 例： `Device(config)# interface vlan 20`	プライマリ VLAN でインターフェイス コンフィギュレーション モードを開始して、VLAN を SVI として設定します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 4	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-if)# private-vlan mapping 501-503`	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。 （注） **private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされているプライベート VLAN トラフィックにだけ影響を与えます。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。 • *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN をプライマリ VLAN にマッピングします。 • **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN のマッピングを解除します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interface private-vlan mapping** 例： `Device# show interfaces private-vlan mapping`	設定を確認します。
ステップ 7	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

関連トピック

VTP Domain （3185 ページ）
Secondary VLANs （3278 ページ）
例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする （3301 ページ）

プライベート VLAN のモニタ

次の表に、プライベート VLAN をモニタするために使用するコマンドを記載します。

表 *220*：プライベート *VLAN* モニタリング コマンド

コマンド	目的
show interfaces status	所属する VLAN を含む、インターフェイスのステータスを表示します。
show vlan private-vlan [type]	Deviceまたは Device スタックのプライベート VLAN 情報を表示します。
show interface switchport	インターフェイス上のプライベート VLAN 設定を表示します。
show interface private-vlan mapping	VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。

コマンド	目的
show platform vlan pvlan	FED 側の PVLAN 情報を表示します。
show platform vlan pvlan hardware	FED 側の PVLAN で保持されているすべてのハードウェア リソースを表示します。

プライベート VLAN の設定例

例：プライベート VLAN 内の VLAN の設定および関連付け

次に、VLAN 20 をプライマリ VLAN、VLAN 501 を独立 VLAN、VLAN 502 および 503 をコミュニティ VLAN として設定し、これらをプライベート VLAN 内で関連付けして、設定を確認する例を示します。

```
Device# configure terminal
Device(config)# vlan 20
Device(config-vlan)# private-vlan primary
Device(config-vlan)# exit
Device(config)# vlan 501
Device(config-vlan)# private-vlan isolated
Device(config-vlan)# exit
Device(config)# vlan 502
Device(config-vlan)# private-vlan community
Device(config-vlan)# exit
Device(config)# vlan 503
Device(config-vlan)# private-vlan community
Device(config-vlan)# exit
Device(config)# vlan 20
Device(config-vlan)# private-vlan association 501-503
Device(config-vlan)# end
Device# show vlan private-vlan
Primary   Secondary      Type
--------- -------------- -----------------
20        501            isolated
20        502            community
20        503            community
```

例：ホスト ポートとしてのインターフェイスの設定

次に、インターフェイスをプライベート VLAN ホスト ポートとして設定し、それをプライベート VLAN ペアに関連付けて、その設定を確認する例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/22
Device(config-if)# switchport mode private-vlan host
Device(config-if)# switchport private-vlan host-association 20 501
Device(config-if)# end
Device# show interfaces gigabitethernet1/0/22 switchport
```

```
Name: Gi1/0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 501
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 501

<output truncated>
```

関連トピック

プライベート VLAN ポート （3278 ページ）
プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 （3293 ページ）
プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 （3294 ページ）

例：プライベート VLAN 無差別ポートとしてのインターフェイスの設定

次の例では、インターフェイスをプライベート VLAN 無差別ポートとして設定し、それをプライベート VLAN にマッピングする方法を示します。インターフェイスは、プライマリ VLAN 20 のメンバで、セカンダリ VLAN 501 ～ 503 がマッピングされます。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport mode private-vlan promiscous
Device(config-if)# switchport private-vlan mapping 20 add 501-503
Device(config-if)# end
```

show vlan private-vlan または **show interface status** 特権 EXEC コマンドを使用してプライマリおよびセカンダリ VLAN と Device 上のプライベート VLAN ポートを表示します。

関連トピック

プライベート VLAN ポート （3278 ページ）
プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 （3293 ページ）

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 （3294 ページ）

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする

次に、VLAN 501 および 502 のインターフェイスをプライマリ VLAN 10 にマッピングする例を示します。これにより、プライベート VLAN 501 および 502 からのセカンダリ VLAN 入力トラフィックのルーティングが可能になります。

```
Device# configure terminal
Device(config)# interface vlan 20
Device(config-if)# private-vlan mapping 501-503
Device(config-if)# end
Device# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan20    501            isolated
vlan20    502            community
vlan20    503            community
```

関連トピック

VTP Domain （3185 ページ）
Secondary VLANs （3278 ページ）
セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング （3296 ページ）

例：プライベート VLAN のモニタリング

次に、**show vlan private-vlan** コマンドの出力例を示します。

```
Device# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated          Gi1/0/22, Gi1/0/2
20      502       community         Gi1/0/2
20      503       community         Gi1/0/2
```

次の作業

次の設定を行えます。

- VTP
- VLANs
- VLAN トランキング

- VLAN メンバーシップ ポリシー サーバ（VMPS）
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CLI コマンド	LAN Switching Command Reference, Cisco IOS Release

標準および RFC

標準/RFC	タイトル
RFC 1573	
RFC 1757	
RFC 2021	

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB • BRIDGE-MIB（RFC1493） • CISCO-BRIDGE-EXT-MIB • CISCO-CDP-MIB • CISCO-PAGP-MIB • CISCO-PRIVATE-VLAN-MIB • CISCO-LAG-MIB • CISCO-L2L3-INTERFACE-CONFIG-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • IEEE8023-LAG-MIB • IF-MIB（RFC 1573） • RMON-MIB（RFC 1757） • RMON2-MIB（RFC 2021）	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 XXII 部

WLAN

- WLAN の設定 （3307 ページ）
- リモート LAN の設定 （3325 ページ）
- DHCP for WLANs の設定 （3333 ページ）
- WLAN セキュリティの設定 （3345 ページ）
- WLAN ごとのクライアント カウントの設定 （3355 ページ）
- 802.11w の設定 （3361 ページ）
- Wi-Fi Direct クライアント ポリシーの設定 （3371 ページ）
- 802.11r BSS の高速移行の設定 （3377 ページ）
- 経由ローミングの設定 （3389 ページ）
- アクセス ポイント グループの設定 （3397 ページ）

第 157 章

WLAN の設定

- 機能情報の確認 （3307 ページ）
- WLAN の前提条件 （3307 ページ）
- WLAN の制約事項 （3308 ページ）
- WLAN について （3309 ページ）
- WLAN の設定方法 （3314 ページ）
- WLAN プロパティの監視（CLI） （3322 ページ）
- 次の作業 （3323 ページ）
- その他の参考資料 （3323 ページ）
- WLAN の機能情報 （3324 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

WLAN の前提条件

- 最大 16 個の WLAN を各アクセス ポイント グループにアソシエートし、各グループに個々のアクセス ポイントを割り当てることができます。各アクセス ポイントは、有効化されている WLAN のうち、そのアクセス ポイント グループに属する WLAN だけをアドバタイズします。アクセス ポイント グループで無効化されている WLAN または別のグループに属する WLAN はアドバタイズしません。

- デバイスが VLAN トラフィックを正常にルーティングできるように、WLAN と管理インターフェイスにはそれぞれ別の VLAN を割り当てることをお勧めします。

関連トピック

WLAN の作成（CLI）（3314 ページ）
汎用 WLAN プロパティの設定（CLI）（3317 ページ）
WLAN の削除（CLI）（3315 ページ）
高度な WLAN プロパティの設定（CLI）（3319 ページ）
バンドの選択（3309 ページ）
オフチャネル スキャンの延期
DTIM 周期
セッション タイムアウト
Cisco Client Extensions（3312 ページ）
ピアツーピア ブロッキング（3312 ページ）
診断チャネル
WLAN ごとのクライアント カウント
WLAN のイネーブル化（CLI）（3316 ページ）
WLAN のディセーブル（CLI）（3317 ページ）

WLAN の制約事項

- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- 最大 2000 台のクライアントを設定できます。
- WLAN 名と SSID は 32 文字以内にする必要があります。スペースは WLAN プロファイル名と SSID では許可されません。WLAN 名はキーワードにすることができません。たとえば、**wlan s**というコマンドを入力して、「s」という名前でWLANを作成すると、「s」はシャットダウン用のキーワードとして使用されているため、すべてのWLANがシャットダウンします。
- WLAN から VLAN0 へのマッピング、VLAN 1002～1006 のマッピングはできません。
- 固定 IPv4 アドレスのデュアル スタック クライアントはサポートされません。
- 同じ SSID を持つ WLAN を作成するときには、各 WLAN に対して一意のプロファイル名を作成する必要があります。
- 同じ SSID を持つ複数の WLAN を同じ AP 無線に割り当てる場合は、クライアントがその中から安全に選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。
- WLAN がローカル スイッチングの場合、AVC が有効化されているローカル スイッチング WLAN にクライアントを関連付けます。AVC の統計 90 秒後を確認した時、クライアントからトラフィックを送信します。Cisco WLC はトップ アプリケーション下では表示されますが、クライアントには表示されません。タイマーの問題があるため、CiscoWLC の最初のスロットはクライアントの統計が表示されないことがあります。以前に 1 秒のみのクラ

イアントの統計が、AP および WLC のタイマーが 89 秒でオフになっている時に見られました。現在統計の削除は 180 秒後であるため、91 秒から 179 秒までのクライアントの統計情報が表示されます。これは、各クライアントあたり 2 つのコピーの統計がメモリの制約で 5500 に保持することができないために起こります。

⚠

注意 一部のクライアントが複数のセキュリティ ポリシーで同じ SSID を検出すると WLAN に正しく接続できない場合があります。この機能を使用する際は、十分注意してください。

関連トピック

WLAN の作成（CLI） （3314 ページ）
汎用 WLAN プロパティの設定（CLI） （3317 ページ）
WLAN の削除（CLI） （3315 ページ）
高度な WLAN プロパティの設定（CLI） （3319 ページ）
バンドの選択 （3309 ページ）
オフチャネル スキャンの延期
DTIM 周期
セッション タイムアウト
Cisco Client Extensions （3312 ページ）
ピアツーピア ブロッキング （3312 ページ）
診断チャネル
WLAN ごとのクライアント カウント
WLAN のイネーブル化（CLI） （3316 ページ）
WLAN のディセーブル（CLI） （3317 ページ）

WLAN について

この機能により、Lightweight アクセス ポイント全体に対して、最大 64 の WLAN を制御できます。各 WLAN には識別子である WLAN ID、プロファイル名、および WLAN SSID があります。すべてのデバイスは接続している各アクセス ポイントに対して最大 16 の WLAN を公開しますが、管理しやすくするため、サポートされる最大数の WLAN を作成し、これらの WLAN を異なるアクセス ポイントに選択的に公開する（アクセス ポイント グループを使用）ことができます。

異なる SSID または同じ SSID で WLAN を設定できます。SSID は、デバイスがアクセスする必要がある特定の無線ネットワークを識別します。

バンドの選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、混雑の少ない 5 GHz アクセス ポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、および

コードレス電話機からの干渉を受けるだけでなく、他のアクセスポイントからの同一チャネル干渉も発生します。802.11b/g では、重複しないチャネルが 3 つしかないからです。このような原因による干渉を防ぎ、ネットワーク全体のパフォーマンスを向上させるには、デバイスで帯域選択を設定します。

クライアントに対するプローブ応答を調整すると帯域選択が機能し、WLAN 単位で有効にできます。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。アクセス ポイントでは、帯域選択表は show dot11 band-select コマンドで表示できます。帯域選択表は、show cont d0/d1 | begin Lru でも表示できます。

（注） WMM のデフォルト設定は、[show running-config] 出力には表示されません。

関連トピック

高度な WLAN プロパティの設定（CLI） （3319 ページ）
WLAN の前提条件 （3307 ページ）
WLAN の制約事項 （3308 ページ）

オフチャネル スキャンの延期

特定の省電力モードのクライアントが展開される環境で、小容量クライアント（たとえば、省電力モードを使用し定期的にテレメトリ情報を送信する医療用デバイス）からの重要情報の欠落を防ぐために、場合によっては、無線リソース管理（RRM）の正常なオフチャネル スキャンを延期する必要があります。この機能は、Quality of Service（QoS）と RRM スキャン延期機能との相互作用の方法を向上させます。

クライアントの Wi-Fi マルチメディア（WMM）UP マーキングを使用して、UP がマークされたパケットを受信した場合に、設定可能な期間中オフチャネル スキャンを延期するアクセス ポイントを設定することができます。

[Off-Channel Scanning Defer] は、ノイズや干渉など代替チャネル選択に関する情報を収集する RRM を使用するときに重要となります。また、[Off-Channel Scanning Defer] は、不正検出を行います。[Off-Channel Scanning Defer] を提供する必要があるデバイスは、可能な限り、同じ WLAN を使用する必要があります。このようなデバイスが多くある場合（この機能を使用して Off-Channel Defer スキャンが完全に無効化されている可能性があります）、モニタ アクセス ポイントや、この WLAN が割り当てられていない同じ位置にあるその他のアクセス ポイントなど、代わりにローカル AP で [Off-Channel Scanning Defer] を実装する必要があります。

QoS ポリシー（Bronze、Silver、Gold、Platinum）を WLAN に割り当てることで、クライアントからアップリンクでどのように受信されたかに関係なく、パケットがアクセスポイントからのダウンリンク接続でどのようにマーキングされるかを制御できます。UP=1,2 は最低の優先順位で、UP=0,3 はその次に高い優先順位です。各 QoS ポリシーのマーキング結果は次のとおりです。

- ブロンズは、すべてのダウンリンク トラフィックを UP= 1 にマーキングします。
- シルバーは、すべてのダウンリンク トラフィックを UP=0 にマーキングします。

- ゴールドは、すべてのダウンリンク トラフィックを UP= 4 にマーキングします。
- プラチナは、すべてのダウンリンク トラフィックを UP= 6 にマーキングします。

DTIM 期間

802.11 ネットワークでは、Lightweight アクセス ポイントは、Delivery Traffic Indication Map (DTIM) と一致するビーコンを定期的に送信します。アクセス ポイントでビーコンがブロードキャストされると、DTIM period で設定した値に基づいて、バッファされたブロードキャスト フレームおよびマルチキャスト フレームが送信されます。この機能により、ブロードキャスト データやマルチキャスト データが予想されると、適切なタイミングで省電力クライアントを再起動できます。

通常、DTIM の値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）または 2（ビーコン 1 回おきに送信）のいずれかに設定されます。たとえば、802.11 ネットワークのビーコン間隔が 100 ミリ秒で DTIM 値が 1 に設定されている場合、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 10 回送信します。ビーコン期間が 100ms で DTIM 値が 2 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 5 回送信します。これらの設定はいずれも、ブロードキャスト フレームおよびマルチキャスト フレームの頻度を想定する、Voice over IP（VoIP）を含むアプリケーションに適しています。

ただし、DTIM 値は、802.11 のすべてのクライアントで省電力モードがイネーブルである場合、255 まで設定できます（255 回のビーコンごとにブロードキャスト フレームおよびマルチキャスト フレームを送信します）。クライアントは DTIM 期間に達したときのみリッスンする必要があるため、ブロードキャストとマルチキャストをリッスンする頻度を少なく設定することで、結果的にバッテリー寿命を長くできます。たとえば、ビーコン期間が 100 ms、DTIM 値を 100 に設定すると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを 10 秒ごとに 1 回送信します。このレートにより省電力クライアントで、ブロードキャストとマルチキャストをリッスンし、ウェイク アップするまでのスリープ状態が長くなり、バッテリ寿命を長くできます。

（注） ビーコン期間は、デバイスでミリ秒単位で指定され、ソフトウェアによって、802.11 の時間単位（TU）（1 TU = 1.024 ミリ秒）に、内部的に変換されます。Cisco の 802.11n アクセス ポイントでは、この値は直近の 17 TU の倍数に丸められます。たとえば、100 ミリ秒に設定されたビーコン間隔は 104 ミリ秒の実際のビーコン間隔の結果です。

多くのアプリケーションでは、ブロードキャスト メッセージとマルチキャスト メッセージとの間隔を長くすると、プロトコルとアプリケーションのパフォーマンスが低下します。このようなクライアントをサポートする 802.11 ネットワークでは、低い DTIM 値を推奨します。

セッション タイムアウト

WLAN にセッション タイムアウトを設定できます。セッション タイムアウトとは、クライアント セッションが再認証を要求することなくアクティブである最大時間を指します。

Cisco Client Extensions

Cisco Client Extensions（CCX）ソフトウェアは、サードパーティ製クライアント デバイスの製造業者およびベンダーに対してライセンスされます。これらのクライアント上の CCX コードにより、サードパーティ製クライアント デバイスは、シスコ製のアクセス ポイントと無線で通信できるようになり、セキュリティの強化、パフォーマンスの向上、高速ローミング、電源管理などの、他のクライアントデバイスがサポートしていないシスコの機能もサポートできるようになります。

- ソフトウェアは、CCX バージョン 1 ～ 5 をサポートします。これによって、デバイスとそのアクセス ポイントは、CCX をサポートするサードパーティ製クライアント デバイスと無線で通信できます。CCX サポートは、デバイス上の各 WLAN に対して自動的に有効になり、無効にすることはできません。ただし、Aironet Information Element（IE）を設定できます。
- Aironet IE のサポートが有効になっている場合、アクセス ポイントは、Aironet IE 0x85（アクセス ポイント名、ロード、アソシエートされたクライアントの数などを含む）をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセス ポイントが再アソシエーション要求内の Aironet IE 0x85 を受信する場合、デバイスは、Aironet IEs 0x85 および 0x95（デバイスの管理 IP アドレスおよびアクセス ポイントの IP アドレスを含む）を再アソシエーション応答に格納して送信します。

関連トピック

高度な WLAN プロパティの設定（CLI）（3319 ページ）
WLAN の前提条件（3307 ページ）
WLAN の制約事項（3308 ページ）

ピアツーピア ブロッキング

ピアツーピア ブロッキングは個別の WLAN に対して適用され、各クライアントが、アソシエート先の WLAN のピアツーピア ブロッキング設定を継承します。ピア ツー ピアにより、トラフィックをリダイレクトする方法を制御できます。たとえば、トラフィックがデバイス内でローカルにブリッジされたり、デバイスによってドロップされたり、またはアップストリーム VLAN へ転送されるように選択することができます。

ローカル スイッチングの WLAN にアソシエートしたクライアントに対して、ピアツーピアブロッキングはサポートされています。

関連トピック

高度な WLAN プロパティの設定（CLI）（3319 ページ）
WLAN の前提条件（3307 ページ）

WLAN の制約事項 （3308 ページ）

診断チャネル

クライアントの WLAN による通信で問題が生じる理由についてトラブルシューティングする診断チャネルを選択できます。クライアントで発生している問題を識別し、ネットワーク上でクライアントを動作させるための修正措置を講じるために、クライアントとアクセスポイントをテストできます。診断チャネルを有効にするには、デバイスの GUI または CLI を使用します。また、診断テストを実行するには、デバイスの CLI を使用します。

（注） 診断チャネル機能は、管理インターフェイスを使用するアンカーされていない SSID に対してのみ有効にすることをお勧めします。CCX 診断機能は Cisco ADU カードを持つクライアントでのみテストされています。

WLAN ごとの RADIUS 送信元サポート

デバイスのダイナミック インターフェイスのいずれかを介してアクセス可能な VLAN 上に設定済みの RADIUS サーバが存在しない場合は、デバイスがその管理インターフェイスの IP アドレスから RADIUS トラフィックを送信します。RADIUS サーバがデバイスのダイナミック インターフェイスを介して到達可能な場合は、その特定の RADIUS サーバへの RADIUS 要求が対応するダイナミック インターフェイスを介してコントローラから取得されます。

デフォルトで、デバイスから取得された RADIUS パケットによって、そのパケットの 送信元 IP アドレス（トポロジに応じて管理またはダイナミック）に関係なく、NAS-IP-Address 属性が管理インターフェイスの IP アドレスの属性に設定されます。

WLAN 単位の RADIUS 送信元サポート（RADIUS サーバ上書きインターフェイス）が有効になっている場合は、NAS-IP-Address 属性がデバイスによって送信元のインターフェイスを反映するように上書きされます。また、それに応じて、RADIUS 属性が Identity に一致するように変更されます。この機能は、各 WLAN が別個のレイヤ 3 Identity を持つ可能性がある場合に、WLAN ごとの RADIUS トラフィックでデバイスを効果的に仮想化します。この機能は、ACS ネットワーク アクセス制限、およびネットワーク アクセス プロファイルと統合する展開に役立ちます。

WLAN をフィルタ処理するには、RFC 3580 で APMAC:SSID 形式に設定された callStationID を使用します。また、NAS-IP-Address 属性を使用することで、認証サーバ上のフィルタリングを WLAN ごとの送信元インターフェイス上にまで拡張できます。

アドレスの送信元として WLAN ごとの動的インターフェイスを用いる管理インターフェイスなどを使用するいくつかの WLAN および通常の RADIUS トラフィックの送信元と、WLAN ごとの RADIUS 送信元サポートを組み合わせることができます。

WLAN の設定方法

WLAN の作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name wlan-id* [*ssid*] 例： `Device(config)# wlan mywlan 34 mywlan-ssid`	WLAN の名前と ID を指定します。 • *profile-name* に、プロファイル名を入力します。 入力できる範囲は英数字で 1 ～ 32 文字です。 • *wlan-id*に、WLAN ID を入力します。 範囲は 1 ～ 512 です。 • *ssid* では、この WLAN に対する Service Set Identifier (SSID) を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。 （注） WLAN はデフォルトでディセーブルにされています。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN の前提条件 （3307 ページ）
WLAN の制約事項 （3308 ページ）

WLAN の削除（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no wlan** *wlan-name wlan-id ssid* 例： `Device(config)# no wlan test2`	WLAN を削除します。引数は次のとおりです。 • *wlan-name*は WLAN プロファイル名です。 • *wlan-id*は、WLAN ID です。 • *ssid* は WLAN に設定された WLAN SSID 名前です。 （注） AP グループに属する WLAN を削除すると、WLAN は AP グループと AP の無線から削除されます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN の前提条件 （3307 ページ）
WLAN の制約事項 （3308 ページ）

WLAN の検索（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**show wlan summary** 例： `Device# show wlan summary`	デバイスに設定されているすべての WLAN のリストを表示します。出力内で WLAN を検索できます。

例

```
Device# show wlan summary
Number of WLANs: 4

WLAN Profile Name                      SSID                            VLAN Status
-------------------------------------------------------------------------------
1    test1                              test1-ssid                      137  UP
3    test2                              test2-ssid                      136  UP
2    test3                              test3-ssid                      1    UP
45   test4                              test4-ssid                      1    DOWN
```

WLAN を検索するときにワイルドカードを使用できます。例：**show wlan summary include** | *variable*。variable は、出力内の検索文字列です。

```
Device# show wlan summary | include test-wlan-ssid
1    test-wlan                        test-wlan-ssid                    137   UP
```

WLAN のイネーブル化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN の前提条件 （3307 ページ）
WLAN の制約事項 （3308 ページ）

WLAN のディセーブル（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Device(config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**show wlan summary** 例： `Device# show wlan summary`	デバイスに設定されているすべての WLAN のリストを表示します。出力内で WLAN を検索できます。

関連トピック

WLAN の前提条件 （3307 ページ）
WLAN の制約事項 （3308 ページ）

汎用 WLAN プロパティの設定（CLI）

次のパラメータを設定できます。

- メディア ストリーム
- ブロードキャスト SSID
- コール スヌーピング
- Radio
- インターフェイス
- Status（ステータス）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Device# shutdown`	パラメータを設定する前に、WLAN をディセーブルにします。
ステップ 4	**broadcast-ssid** 例： `Device(config-wlan)# broadcast-ssid`	この WLAN の SSID をブロードキャストします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 5	**radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**} 例： `Device# radio all`	WLAN で無線をイネーブルにします。キーワードは次のとおりです。 • **all**：の無線帯域で WLAN を設定します。 • **dot1a**：802.11a の無線帯域だけに WLAN を設定します。 • **dot11g**：802.11ag の無線帯域でのみ WLAN を設定します。 • **dot11bg**：802.11b/g の無線帯域でのみ WLAN を設定します（802.11g が無効の場合、802.11b のみ）。 • **dot11ag**：802.11g の無線帯域だけに無線 LAN を設定します。
ステップ 6	**client vlan** *vlan-identifier* 例： `Device# client vlan test-vlan`	WLAN のインターフェイス グループをイネーブルにします。 *vlan-identifier*：VLAN ID を指定します。次に、VLAN 名、VLAN ID、または VLAN グループ名を指定できます。

	コマンドまたはアクション	目的
ステップ 7	**ip multicast vlan** *vlan-name* 例： `Device(config-wlan)# ip multicast vlan test`	WLANのマルチキャストをイネーブルにします。キーワードは次のとおりです。 • **vlan**：VLAN ID を指定します。 • *vlan-name*：VLAN 名を指定します。
ステップ 8	**media-stream multicast-direct** 例： `Device(config-wlan)# media-stream multicast-direct`	この WLAN でマルチキャスト VLAN をイネーブルにします。
ステップ 9	**call-snoop** 例： `Device(config-wlan)# call-snoop`	コールスヌーピングサポートをイネーブルにします。
ステップ 10	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

関連トピック

WLAN の前提条件 （3307 ページ）
WLAN の制約事項 （3308 ページ）

高度な WLAN プロパティの設定（CLI）

次の高度なプロパティを設定できます。

- AAA オーバーライド
- カバレッジ ホールの検出
- セッション タイムアウト
- Cisco Client Extensions
- 診断チャネル
- インターフェイス オーバーライド ACL

- P2P ブロッキング
- Client Exclusion
- WLAN ごとの最大クライアント数
- オフ チャネル スキャンの延期

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**aaa-override** 例： `Device(config-wlan)# aaa-override`	AAA オーバーライドをイネーブルにします。
ステップ 4	**chd** 例： `Device(config-wlan)# chd`	この WLAN のカバレッジ ホールの検出をイネーブルにします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 5	**session-timeout** *time-in-seconds* 例： `Device(config-wlan)# session-timeout 450`	セッションタイムアウトを秒単位で設定します。範囲とデフォルト値は、セキュリティ設定によって異なります。WLAN セキュリティが dot1x に設定されている場合、範囲は 300～86400 秒で、デフォルト値は 1800 秒です。他のすべての WLAN セキュリティ設定では、有効範囲は 1～65535 秒であり、デフォルト値は 0 秒です。値 0 は、セッションタイムアウトなしを示します。
ステップ 6	**ccx aironet-iesupport** 例： `Device(config-wlan)# ccx aironet-iesupport`	この WLAN の Aironet IE のサポートをイネーブルにします。このフィールドは、デフォルトでイネーブルにされています。

	コマンドまたはアクション	目的
ステップ 7	**diag-channel** 例： `Device(config-wlan)# diag-channel`	WLANでクライアントの通信の問題を修復するための診断チャネルのサポートをイネーブルにします。
ステップ 8	**ip access-group** [web] *acl-name* 例： `Device(config)# ip access-group test-acl-name`	WLAN ACL グループを設定します。可変 *acl* 名前はユーザ定義する IPv4 ACL の名前を指定します。キーワード **web** は、IPv4 web ACL を指定します。
ステップ 9	**peer-blocking** ［**drop** ｜ **forward-upstream**］ 例： `Device(config)# peer-blocking drop`	ピアツーピアブロッキングパラメータを設定します。キーワードは次のとおりです。 • **drop**：ドロップアクションのピアツーピアブロッキングをイネーブルにします。 • **forward-upstream**：アップストリーム転送処理のピアツーピアブロッキングをイネーブルにします。
ステップ 10	**exclusionlist** *time-in-seconds* 例： `Device(config)# exclusionlist 10`	タイムアウトを秒単位で指定します。0 ～ 2147483647 の範囲の値を指定できます。タイムアウトなしでは、0 を入力します。ゼロ（0）タイムアウトは、クライアントが除外リストに追加されたことを示しています。
ステップ 11	**client association limit** *max-number-of-clients* 例： `Device(config)# client association limit 200`	WLANで設定できる最大クライアント数を設定します。
ステップ 12	**channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} 例： `Device(config)# channel-scan defer-priority 6`	チャネル スキャンの延期プライオリティと延期時間を設定します。引数は次のとおりです。 • **defer-priority**：オフチャネル スキャンを延期できるパケットのプライオリティマーキングを指定します。有効な範囲は 0 ～ 7 です。デフォルトは 3 です。

	コマンドまたはアクション	目的
		• **defer-time**：延期時間（ミリ秒単位）。範囲は 0 ～ 6000 です。デフォルトは 100 です。
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

関連トピック

バンドの選択 （3309 ページ）
オフチャネル スキャンの延期
DTIM 周期
セッション タイムアウト
Cisco Client Extensions （3312 ページ）
ピアツーピア ブロッキング （3312 ページ）
診断チャネル
WLAN ごとのクライアント カウント
WLAN の前提条件 （3307 ページ）
WLAN の制約事項 （3308 ページ）
AAA Override について （3346 ページ）
レイヤ 2 セキュリティの前提条件 （3345 ページ）

WLAN プロパティの監視（CLI）

コマンド	説明
show wlan id *wlan-id*	WLAN ID に基づいて WLAN プロパティを表示します。
show wlan name *wlan-name*	WLAN 名に基づいて WLAN プロパティを表示します。
show wlan all	設定されているすべての WLAN の WLAN プロパティを表示します。

コマンド	説明
show wlan summary	すべての WLAN の要約を表示します。サマリー詳細には、次の情報が含まれます。 • WLAN ID • プロファイル名 • SSID • VLAN • Status（ステータス）
show running-config wlan *wlan-name*	WLAN の名前に基づいて WLAN の実行コンフィギュレーションを表示します。
show running-config *wlan*	すべての WLAN の実行コンフィギュレーションを表示します。

次の作業

DHCP for WLANs の設定に進みます

その他の参考資料

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	『*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』
Mobility Anchor の設定	『*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』
WebAuth の設定	『*Security Configuration Guide (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

WLAN の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
WLAN の機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 158 章

リモート LAN の設定

- 機能情報の確認 （3325 ページ）
- **リモート LAN の設定に関する前提条件** （3325 ページ）
- **リモート LAN の制約事項** （3326 ページ）
- **リモート LAN について** （3326 ページ）
- **リモート LAN の設定（CLI）** （3326 ページ）
- リモート LAN の設定例 （3328 ページ）
- **AP グループ固有の CLI の設定** （3331 ページ）
- ポートへの PoE の設定 （3332 ページ）
- AP への LAN オーバーライドの設定 （3332 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

リモート LAN の設定に関する前提条件

- リモート LAN 機能は、Cisco IOS XE Denali 16.3.1 以降のリリースでサポートされています。この機能は、コンパクトでウォールプレートに設置可能なアクセス ポイントを提供する、Cisco Aironet 1810W シリーズ AP で利用できます。

リモート LAN の制約事項

- 同じプロファイル名または ID を、WLAN とリモート LAN の両方に使用することはできません。
- ローカル ギガビット イーサネット ポートを介して Cisco Aironet 1810W シリーズ AP に接続できるのは、3 つのクライアントのみです。ポートごとに、1 つのクライアントだけがサポートされます。
- リモート LAN プロファイルは、AP グループのみにマッピングできます。したがって、リモート LAN プロファイルをローカル ギガビット イーサネット ポートに設定するには、AP が AP グループに含まれている必要があります。
- デフォルトの AP グループをリモート LAN に設定することはできません。

リモート LAN について

リモート LAN は WLAN に似ています。唯一の違いは、WLAN はワイヤレス接続に使用されるのに対し、リモート LAN は有線ポートに使用される点です。Cisco Aironet 1810W シリーズ AP には、3 つのローカル ギガビット イーサネット ポート、1 つのアップリンク ギガビット イーサネット ポート、および 1 つのパッシブ パススルー RJ-45 ポートが搭載されています。ローカル ギガビット イーサネット ポートでリモート LAN プロファイルを設定することで、有線デバイスからのトラフィックを、ワイヤレス コントローラに戻るためにトンネリングされたポートに接続することができます。

リモート LAN の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**remote-lan** *profile-name id* 例： `Device(config)# remote-lan test-lan 3`	リモート LAN プロファイル名を指定します。 • id：設定タスク時に入力した一意の番号。指定できる値の範囲は 1 ～ 64 です。
ステップ 2	**session-timeout** *session-time* 例： `Device(config-remote-lan)# session-timeout 50`	セッションの期間を秒数で設定します。指定できる値の範囲は 0 ～ 86400 です。

	コマンドまたはアクション	目的
ステップ 3	**client vlan** *vlan-identifier* 例： `Device(config-remote-lan)# client vlan test-vlan`	リモート LAN のインターフェイス グループをイネーブルにします。 • vlan-identifier：VLAN 識別子を指定します。VLAN 名、VLAN ID、または VLAN グループ名を指定できます。
ステップ 4	**client association limit** *max-number-of-clients* 例： `Device(config-remote-lan)# client association limit 200`	リモート LAN プロファイルに接続できるクライアントの最大数を設定します。
ステップ 5	**ip access-group** *acl-name* 例： `Device(config-remote-lan)# ip access-group  acl-name`	IPv4 ACL 名または ID を設定します。
ステップ 6	**security webauth parameter-map parameter-name** 例： `Device(config-remote-lan)# security web-auth parameter-map parameter-22`	パラメータ マップ名を指定します。
ステップ 7	**security dot1x** 例： `Device(config-remote-lan)# security dot1x`	802.1X セキュリティを指定します。
ステップ 8	**security dot1x authentication** *list-name* 例： `Device(config-remote-lan)# security dot1x authentication-list LIST1`	認証リスト名を設定します。
ステップ 9	**exclusionlist timeout** *time-sec* 例： `Device(config-remote-lan)# exclusionlist timeout 30`	クライアントが除外されるまでの時間を秒数で設定します。範囲は 0 ～ 2147483647 です。値 0 はタイムアウトなしを意味します。
ステップ 10	**aaa-override** 例： `Device(config-remote-lan)# aaa-override`	AAA ポリシーを上書きします。

	コマンドまたはアクション	目的
ステップ 11	**local-auth EAP-Profile** 例： `Device(config-remote-lan)# local-auth EAP-Profile`	リモート LAN で EAP プロファイルを有効にします。
ステップ 12	**ip dhcp server** *ip-address* 例： `Device(config-remote-lan)# ip dhcp server 10.76.47.11`	リモート LAN で DHCP パラメータを設定します。
ステップ 13	**ip access-group web** *acl-name* 例： `Device(config-remote-lan)# ip access-group web acl-test`	IPv4 リモート LAN Web ACL を設定します。
ステップ 14	**accounting-list** *list-name* 例： `Device(config-remote-lan)# accounting-list list-LIST1`	IEEE 802.1x のアカウンティング リストを設定します。
ステップ 15	**mac-filtering** *list-name* 例： `Device(config-remote-lan)# mac-filtering test-10`	リモート LAN で MAC フィルタリングのサポートを設定します。
ステップ 16	**no shutdown** 例： `Device(config-remote-lan)# no shutdown`	リモート LAN を有効にします。

リモート LAN の設定例

次の例に、すべてのリモート LAN のサマリーを示します。

```
Device# show remote-lan summary
Number of Remote-LANs: 1

Remote-LAN Profile Name                     VLAN Status
-------------------------------------------------------
2          test                             1    DOWN
```

次の例に、ID によるリモート LAN 設定を示します。

```
Device# show remote-lan id 2
Remote-LAN Profile Name     : test
===============================================
Identifier                                    : 2
```

```
Status                                          : Disabled
Universal AP Admin                              : Disabled
Max Associated Clients per Remote-LAN           : 0
AAA Policy Override                             : Enabled
Number of Active Clients                        : 0
Exclusionlist Timeout                           : 21474
Session Timeout                                 : 864 seconds
Interface                                       : default
Interface Status                                : Up
Remote-LAN ACL                                   : testacl
DHCP Server                                     : 10.5.7.9
DHCP Address Assignment Required                : Disabled
Local EAP Authentication                        : testeapprofile
Mac Filter Authorization list name              : testmaclist
Accounting list name                            : testlist
802.1x authentication list name                 : dotxauth
Security
    802.11 Authentication                       : Open System
    802.1X                                      : Enabled
        Encryption                              : 104-bit WEP
```

次の例に、プロファイル名によるリモート LAN 設定を示します。

```
Device#  show remote-lan name test
Remote-LAN Profile Name : test
================================================
Identifier : 1
Status : Disabled
Universal AP Admin : Disabled
Max Associated Clients per Remote-LAN : 0
AAA Policy Override : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
Interface : default
Interface Status : Up
Remote-LAN ACL : unconfigured
DHCP Server : 0.0.0.0
DHCP Address Assignment Required : Disabled
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name : Disabled
802.1x authentication list name : Disabled
Security
802.11 Authentication : Open System
802.1X : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
```

次の例に、設定済みのすべてのリモート LAN のリモート LAN プロパティを示します。

```
Device# show remote-lan all
Remote-LAN Profile Name : test
================================================
Identifier : 1
Status : Disabled
Universal AP Admin : Disabled
```

```
Max Associated Clients per Remote-LAN : 0
AAA Policy Override : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
Interface : default
Interface Status : Up
Remote-LAN ACL : unconfigured
DHCP Server : 0.0.0.0
DHCP Address Assignment Required : Disabled
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name : Disabled
802.1x authentication list name : Disabled
Security
802.11 Authentication : Open System
802.1X : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
```

次の例に、リモート LAN 設定を示します。

```
Device# show running-config remote-lan test
remote-lan test 1
aaa-override
accounting-list test-all-list
exclusionlist timeout 100
ip access-group test-acl
ip dhcp server 10.100.12.5
mac-filtering test-mac-list
security dot1x authentication-list test-dot1x-list
session-timeout 100
shutdown
```

次の例に、AP グループの詳細を示します。

```
Device# show ap groups
Site Name: test-ap-group
Site Description:
Hyperlocation Operational Status: Down

WLAN ID WLAN Name Interface
-----------------------------------------------------

LAN Status PoE Remote-LAN
-------------------------------------------------------
1 Down Disabled None
2 Down None
3 Down None
```

次の例に、LAN ポートの詳細を示します。

```
Device# show ap name AP00FE.C82D.E7B0 lan port 1
LAN Port status for AP AP00FE.C82D.E7B0

LanOverride Enabled

PortId Status VlanId PoE
```

```
-----------------------------------------------
LAN1 Enabled 0 Disabled
```

次の例に、LAN ポート サマリーの詳細を示します。

```
Device# show ap name AP00FE.C82D.E7B0 lan port summary
LAN Port status for AP AP00FE.C82D.E7B0

LanOverride Enabled

Port ID Status Vlan ID PoE
-----------------------------------
LAN1 Enabled 0 Disable
LAN2 Disabled 0 Disable
LAN3 Disabled 0 Disable
```

AP グループ固有の CLI の設定

AP グループに LAN ポート パラメータを設定するには、次の手順を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**remote-lan** *remote-lan-name* 例： `Device(config-apgroup)# remote-lan test-lan`	AP グループにリモート LAN を追加します。
ステップ 2	**port** *port-id* 例： `Device(config-apgroup)# port 1`	AP グループのポート ID を設定します。
ステップ 3	**poe** 例： `Device(config-port-apgroup)# poe`	ポートで PoE をイネーブルにします。 （注） PoE はポート 1 に対してのみ設定できます。
ステップ 4	**remote-lan** *remote-lan-name* 例： `Device(config-port-apgroup)# remote-lan test-lan`	リモート LAN ID を追加します。
ステップ 5	**no shutdown** 例： `Device(config-port-apgroup)# no shutdown`	LAN ポートを有効にします。

ポートへの PoE の設定

Cisco Aironet 1810W シリーズは、Power over Ethernet（PoE）による有線アクセスが可能です。この機能により、IP 電話、セキュリティ カメラ、プリンタ、コピー機などのデバイスに PoE を使用して有線アクセスを提供できます。有効または無効にする PoE に対し、LAN ポート 1 のみを設定します。デフォルトでは、PoE はポートに対して無効になっています。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name***lan port-id** *port-id***poe** 例： `Device# ap name AP00FE.C82D.DFB0 lan port-id 1 poe`	AP の LAN ポートで PoE を有効にします。 （注） PoE はポート 1 に対してのみ設定できます。

AP への LAN オーバーライドの設定

LAN オーバーライドを有効にして、特定の AP の LAN ポート設定を上書きすることができます。AP LAN ポートごとの設定は、LAN オーバーライドが有効になっているときにのみ機能します。デフォルトでは、LAN オーバーライドはディセーブルに設定されています。LAN オーバーライドが無効になっている場合、AP は AP グループの LAN ポート設定を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name***lan override** 例： `Device# ap name AP00FE.C82D.DFB0 lan override`	AP グループの LAN ポート設定のオーバーライドを有効にします。

第 159 章

DHCP for WLANs の設定

- 機能情報の確認 （3333 ページ）
- DHCP for WLANs を設定するための前提条件 （3333 ページ）
- DHCP for WLANs の設定に関する制約事項 （3335 ページ）
- Dynamic Host Configuration Protocol について （3335 ページ）
- DHCP for WLANs の設定方法 （3339 ページ）
- その他の参考資料 （3342 ページ）
- DHCP for WLANs の機能情報 （3343 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

DHCP for WLANs を設定するための前提条件

- DHCP オプション 82 を使用するには、Cisco IOS ソフトウェアで DHCP を設定します。デフォルトでは、DHCP オプション 82 は、すべてのクライアントに対してイネーブルにされます。WLAN サブオプションを使用して無線クライアントの動作を制御できます。
- シスコのスマート サービス機能のプラットフォームでは、内部 DHCP サーバ機能をサポートしています。ただし、大規模なエンタープライズクラスのネットワークを構築する一般的な導入ガイドラインとして、無線クライアントにダイナミック IP アドレスを提供するために、外部 DHCP サーバの使用をお勧めします。このような分散機能は、ネットワーク

デバイスにかかる処理および設定の負荷を低減し、大規模環境で効率的に動作させることができます。

- DHCP スヌーピング設定：DHCP スヌーピング設定は、クライアントの参加機能をすばやく上で設定するために必要なベストプラクティスです。DHCP スヌーピングは各クライアント VLAN 上で有効にする必要があります。WLAN でオーバーライドが適用される場合は、オーバライド VLAN も対象となります。

DHCP スヌーピング設定の例

1. グローバル DHCP スヌーピングの設定：
   1. `Device(config)#ip dhcp snooping`

      `Device(config)#ip dhcp snooping vlan 100`
   2. `Bootp-broadcast` コマンドを有効にします。これは、ブロードキャスト アドレスを使用して DHCP メッセージを送信するクライアントに必要で、ブロードキャスト ビットが DHCP メッセージに設定されます。

      `Device(config)#ip dhcp snooping wireless bootp-broadcast enable`
   3. DHCP オプション情報を付加しないためには、次のコマンドを入力します。

      `Device(config)#no ip dhcp snooping information option`
2. インターフェイス上で、次のように設定します。

（注） IP DHCP snooping trust は、ポート チャネル インターフェイスのメンバ リンクおよびポート チャネル インターフェイスで必要です。

```
Device(config)#interface range TenGigabitEthernet 1/0/1 - 2
Device(config-if)#switchport mode trunk
Device(config-if)#switchport trunk allowed vlan 100
Device(config-if)#ip dhcp snooping trust

Device(config)#interface port-channel 1
Device(config-if)#switchport mode trunk
Device(config-if)#switchport trunk allowed vlan 100
Device(config-if)#ip dhcp snooping trust
```

（注） DHCP スヌーピングは、上記の設定と同様に、ゲスト アクセス用のゲスト アンカー で設定する必要があります。

関連トピック

WLAN 用の DHCP 設定（CLI） （3339 ページ）
Dynamic Host Configuration Protocol について （3335 ページ）
内部 DHCP サーバ （3336 ページ）
外部 DHCP サーバ （3336 ページ）
DHCP 割り当て （3337 ページ）
DHCP オプション 82 について （3338 ページ）
DHCP スコープの設定 （3339 ページ）
DHCP スコープについて （3339 ページ）

DHCP for WLANs の設定に関する制約事項

- WLAN で DHCP サーバをオーバーライドすると、DHCP サーバが到達可能であることを確認するために、基盤となる Cisco IOS 設定を行う必要があります。
- DHCP WLAN オーバーライドは DHCP サービスがデバイス上で有効な場合にだけ動作します。

  次の方法で、DHCP サービスを設定できます。

  - デバイスで DHCP プールを設定します。
  - SVI で DHCP リレー エージェントを設定します。注: SVI の VLAN は DHCP のオーバーライドが設定された WLAN にマッピングする必要があります。

関連トピック

WLAN 用の DHCP 設定（CLI） （3339 ページ）
Dynamic Host Configuration Protocol について （3335 ページ）
内部 DHCP サーバ （3336 ページ）
外部 DHCP サーバ （3336 ページ）
DHCP 割り当て （3337 ページ）
DHCP オプション 82 について （3338 ページ）
DHCP スコープの設定 （3339 ページ）
DHCP スコープについて （3339 ページ）

Dynamic Host Configuration Protocol について

WLAN では、同じ Dynamic Host Configuration Protocol（DHCP）サーバまたは異なる DHCP サーバを使用するか、または DHCP サーバを使用しないように設定できます。DHCP サーバには、内部 DHCP サーバと外部 DHCP サーバの 2 つのタイプがあります。

関連トピック

WLAN 用の DHCP 設定（CLI） （3339 ページ）

DHCP for WLANs を設定するための前提条件 （3333 ページ）
DHCP for WLANs の設定に関する制約事項 （3335 ページ）

内部 DHCP サーバ

デバイスは、内部DHCPサーバを持っています。このサーバは、一般的に、DHCPサーバを持たないブランチ オフィスで使用されます。無線ネットワークには、通常、デバイスと同じ IP サブネット上にある最大 10 台のアクセス ポイントが含まれます。内部サーバは、ワイヤレス クライアント、ダイレクトコネクト アクセス ポイント、およびアクセス ポイントからリレーされた DHCP 要求に対して DHCP アドレスを提供します。Lightweight アクセス ポイントのみサポートされています。内部DHCPサーバを使用する場合は、デバイスの管理インターフェイスの IP アドレスを DHCP サーバの IP アドレスとして設定する必要があります。

内部サーバでは、DHCP オプション 43 はサポートされていません。したがって、アクセス ポイントは、ローカル サブネット ブロードキャスト、ドメイン ネーム システム（DNS）、またはプライミングなどの別の方法を使用してデバイスの管理インターフェイスの IP アドレスを見つける必要があります。

内部 DHCP サーバ プールは、そのデバイスの無線クライアントだけをサポートし、他のデバイスのクライアントはサポートしません。また、内部DHCPサーバは、無線クライアントだけをサポートし、有線クライアントをサポートしません。

クライアントがデバイスの内部 DHCP サーバを使用する場合、IP アドレスは、再起動後には保持されません。その結果、複数のクライアントに同じ IP アドレスが割り当てられることがあります。IP アドレスの競合を解決するには、クライアントは既存の IP アドレスを解放し、新しいアドレスを要求する必要があります。有線ゲストクライアントは常に、ローカルまたは外部デバイスに接続されたレイヤ 2 ネットワークにあります。

（注） DHCPv6 は内部 DHCP サーバではサポートされません。

関連トピック

WLAN 用の DHCP 設定（CLI） （3339 ページ）
DHCP for WLANs を設定するための前提条件 （3333 ページ）
DHCP for WLANs の設定に関する制約事項 （3335 ページ）

外部 DHCP サーバ

オペレーティング システムは、DHCP リレーをサポートする業界標準の外部 DHCP サーバを使用することにより、ネットワークに対してはDHCPリレーとして機能し、クライアントに対してはDHCPサーバとして機能するように設計されています。これは、各デバイスは、DHCP サーバに対しては DHCP リレー エージェントとして機能し、無線クライアントに対しては仮想 IP アドレスでの DHCP サーバとして機能することを意味します。

デバイスは DHCP サーバから取得したクライアント IP アドレスをキャプチャするため、デバイス内、デバイス間、およびサブネット間でのクライアントローミング時に、各クライアントに対して同じ IP アドレスが保持されます。

（注） 外部 DHCP サーバは DHCPv6 をサポートします。

関連トピック

WLAN 用の DHCP 設定（CLI） （3339 ページ）
DHCP for WLANs を設定するための前提条件 （3333 ページ）
DHCP for WLANs の設定に関する制約事項 （3335 ページ）

DHCP 割り当て

DHCP はインターフェイスごとに、または WLAN ごとに設定できます。特定のインターフェイスに割り当てられたプライマリ DHCP サーバのアドレスを使用することをお勧めします。

個々のインターフェイスに DHCP サーバを割り当てることができます。プライマリおよびセカンダリ DHCP サーバの管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスの設定、DHCP サーバをイネーブルまたはディセーブルするためのサービス ポート インターフェイスの設定を行うことができます。WLAN で DHCP サーバを定義することもできます。この場合、サーバは、WLAN に割り当てられたインターフェイスの DHCP サーバアドレスを上書きします。

セキュリティに関する注意事項

高度なセキュリティが必要な場合は、すべてのクライアントが DHCP サーバから IP アドレスを取得するように設定してください。この要件を適用するために、DHCP アドレスですべての WLAN を設定できます。Assignment Required 設定で設定して、クライアントの固定 IP アドレスが禁止されるようにします。DHCP Addr.Assignment Required が選択されている場合、クライアントは DHCP を使って IP アドレスを取得する必要があります。固定 IP アドレスを持つクライアントはすべて、ネットワーク上で許可されなくなります。クライアントの DHCP プロキシとして動作するデバイスが、DHCP トラフィックを監視します。

（注）
- 無線による管理をサポートする WLAN では、管理（デバイスサービシング）クライアントが DHCP サーバから IP アドレスを取得できるようにする必要があります。

セキュリティが多少劣ってもかまわない場合は、DHCP Addr.Assignment Required を無効に設定して WLAN を作成できます。その後クライアントは、固定 IP アドレスを使用するか、指定された DHCP サーバの IP アドレスを取得するかを選択できます。

（注） DHCP アドレス有線ゲスト LAN に対する Assignment Required は、サポートされていません。

個別の WLAN は、[DHCP Address Assignment Required] を無効にして作成できます。これは、デバイスの DHCP プロキシがイネーブルの場合だけです。DHCP プロキシをディセーブルにする必要があるプライマリ/セカンダリ コンフィギュレーションの DHCP サーバを定義しないでください。このような WLAN では、すべての DHCP 要求がドロップするため、クライアントは固定 IP アドレスを使用しなければなりません。これらの WLAN は、無線接続による管理をサポートしていません。

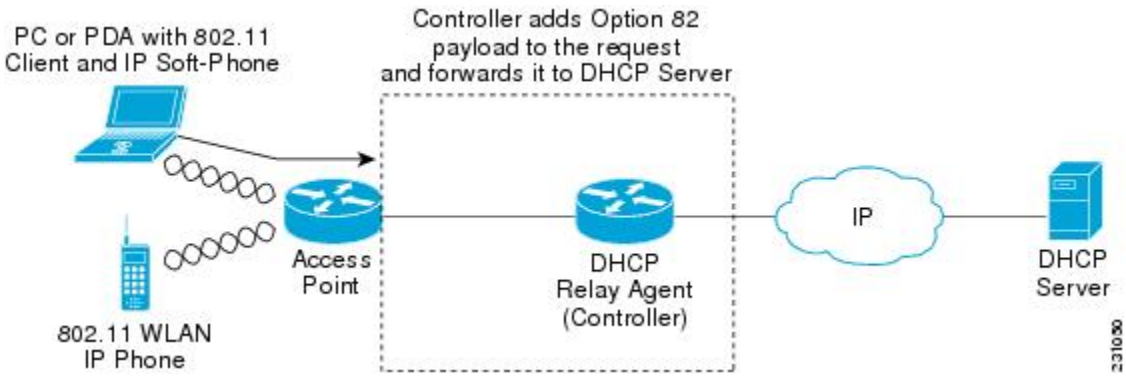
関連トピック

WLAN 用の DHCP 設定（CLI） （3339 ページ）
DHCP for WLANs を設定するための前提条件 （3333 ページ）
DHCP for WLANs の設定に関する制約事項 （3335 ページ）

DHCP オプション 82 について

DHCP オプション 82 では、DHCP を使用してネットワーク アドレスを割り当てる場合のセキュリティが強化されます。デバイスが DHCP リレー エージェントとして動作して、信頼できないソースからの DHCP クライアント要求を阻止できるようにします。DHCP サーバに転送するようにクライアントからの DHCP 要求にオプション 82 情報を追加するようにデバイスを設定できます。

図 *150 : DHCP オプション 82*



アクセス ポイントは、クライアントからのすべての DHCP 要求をデバイスに転送します。デバイスは、DHCP オプション 82 ペイロードを追加してから要求を DHCP サーバに転送します。このオプションの設定方法によって、ペイロードには MAC アドレス、または MAC アドレスとアクセス ポイントの SSID が含まれます。

（注） すでにリレー エージェント オプションが含まれている DHCP パケットは、デバイスでドロップされます。

DHCP オプション 82 が正しく動作するには、DHCP プロキシが有効でなければなりません。

関連トピック

WLAN 用の DHCP 設定（CLI） （3339 ページ）
DHCP for WLANs を設定するための前提条件 （3333 ページ）
DHCP for WLANs の設定に関する制約事項 （3335 ページ）

DHCP スコープの設定

関連トピック

WLAN 用の DHCP 設定（CLI） （3339 ページ）
DHCP for WLANs を設定するための前提条件 （3333 ページ）
DHCP for WLANs の設定に関する制約事項 （3335 ページ）

DHCP スコープについて

デバイスには組み込みの DHCP リレー エージェントがあります。ただし、別個の DHCP サーバを持たないネットワーク セグメントが必要な場合、デバイスに IP アドレスとサブネット マスクを無線クライアントに割り当てる組み込みの DHCP スコープを設定できます。一般に、1 つのデバイスには、それぞれある範囲の IP アドレスを指定する 1 つ以上の DHCP スコープを設定できます。

DHCP スコープは内部 DHCP が機能するために必要となります。デバイスで DHCP が定義されると、管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスのプライマリ DHCP サーバの IP アドレスをデバイスの管理インターフェイスにポイントすることができます。

関連トピック

WLAN 用の DHCP 設定（CLI） （3339 ページ）
DHCP for WLANs を設定するための前提条件 （3333 ページ）
DHCP for WLANs の設定に関する制約事項 （3335 ページ）
DHCP スコープの設定（CLI） （3342 ページ）

DHCP for WLANs の設定方法

WLAN 用の DHCP 設定（CLI）

WLAN で次の DHCP パラメータを設定するには、次の手順に従います。

- DHCP オプション 82 ペイロード
- DHCP（必須）
- DHCP オーバーライド

始める前に

- WLAN を設定するには admin 権限がなければなりません。
- DHCP のオーバーライドを設定するには、DHCP サーバの IP アドレスが必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**shutdown** 例： `Device(config)# shutdown`	WLAN をシャットダウンします。
ステップ 3	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。

ステップ 4	**ip dhcp opt82** {**ascii** | **format** {*add-ssid* | *ap-ethmac*} | **rid**}
	例：
	`Device(config)# ip dhcp opt82 format add-ssid`
		WLAN で DHCP82 ペイロードを指定します。キーワードおよび引数は、次のとおりです。
		• **ascii**：DHCP オプション 82 の ASCII を設定します。これが設定されていない場合、オプション 82 の形式は ASCII 形式に設定されます。
		• **format**：DHCP オプション 82 の形式を指定します。次のオプションを使用できます。
		  • *add-ssid*：AP 無線の MAC アドレスおよび SSID である RemoteID 形式を設定します。
		  • *ap-ethmac*：AP Ethernet MAC アドレスである RemoteID 形式を設定します。
		（注） フォーマット オプションが設定されていない場合、AP 無線の MAC アドレスだけが使用されます。

	コマンドまたはアクション	目的
		• **rid**：DHCP オプション 82 に Cisco 2 バイト RID を追加します。
ステップ 5	**ip dhcp required** 例： `Device(config-wlan)# ip dhcp required`	DHCP サーバから IP アドレスをクライアントが取得することを必須にします。スタティック クライアントは許可されません。
ステップ 6	**ip dhcp server** *ip-address* 例： `Device(config-wlan)# ip dhcp server 200.1.1.2`	WLAN に割り当てられたインターフェイスの DHCP サーバ アドレスを上書きする WLAN 上の DHCP サーバを定義します。
ステップ 7	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN を再起動します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 9	**show wlan** *wlan-name* 例： `Device(config-wlan)# show wlan test-wlan`	DHCP の設定を確認します。

関連トピック

Dynamic Host Configuration Protocol について （3335 ページ）
内部 DHCP サーバ （3336 ページ）
外部 DHCP サーバ （3336 ページ）
DHCP 割り当て （3337 ページ）
DHCP オプション 82 について （3338 ページ）
DHCP スコープの設定 （3339 ページ）
DHCP スコープについて （3339 ページ）
DHCP for WLANs を設定するための前提条件 （3333 ページ）
DHCP for WLANs の設定に関する制約事項 （3335 ページ）

DHCP スコープの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool** *pool-name* 例： `Device(config)#ip dhcp pool test-pool`	DHCP プール アドレスを設定します。
ステップ 3	**network** *network-name mask-address* 例： `Device(dhcp-config)#network 209.165.200.224 255.255.255.0`	ドット付き 10 進表記とマスク アドレスでネットワーク番号を指定します。
ステップ 4	**dns-server** *hostname* 例： `Device(dhcp-config)#dns-server example.com`	DNS ネーム サーバを指定します。IP アドレスまたはホスト名を指定できます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

DHCP スコープについて （3339 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
システム管理	『*System Management Configuration Guide (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DHCP for WLANs の機能情報

機能名	リリース	機能情報
WLAN の DHCP 機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 160 章

WLAN セキュリティの設定

- 機能情報の確認 （3345 ページ）
- レイヤ 2 セキュリティの前提条件 （3345 ページ）
- AAA Override について （3346 ページ）
- WLAN セキュリティの設定方法 （3347 ページ）
- その他の参考資料 （3352 ページ）
- WLAN レイヤ 2 セキュリティに関する機能情報 （3353 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

レイヤ 2 セキュリティの前提条件

同じ SSID を持つ WLAN は、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントが WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。使用可能なレイヤ 2 セキュリティ ポリシーは、次のとおりです。

- なし（オープン WLAN）
- Static WEP または 802.1X

（注）

- Static WEP と 802.1X は両方とも、ビーコン応答とプローブ応答で同じビットによってアドバタイズされるので、クライアントはこれらを区別できません。したがって、同じ SSID を持つ複数の WLAN では、Static WEP と 802.1X の両方を使用できません。
- WLAN WEP は、1810w アクセス ポイントではサポートされません。

- WPA/WPA2

（注）

- 同じ SSID を持つ複数の WLAN で WPA と WPA2 を使用することはできませんが、同じ SSID を持つ 2 つの WLAN は、PSK を使用する WPA/TKIP と 802.1X を使用する Wi-Fi Protected Access（WPA）/Temporal Key Integrity Protocol（WPA）で設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES で設定することができます。
- TKIP サポートが設定された WLAN は RM3000AC モジュールで有効にされません。

関連トピック

静的 WEP および 802.1X レイヤ 2 セキュリティ パラメータの設定（CLI）（3347 ページ）
静的 WEP レイヤ 2 セキュリティ パラメータの設定（CLI）（3348 ページ）
WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（CLI）（3349 ページ）
802.1X レイヤ 2 セキュリティ パラメータの設定（CLI）（3350 ページ）
高度な WLAN プロパティの設定（CLI）（3319 ページ）
AAA Override について（3346 ページ）

AAA Override について

WLAN の AAA Override オプションを使用すると、WLAN で Identity ネットワーキングを設定できます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、Quality Of Service (QoS)、およびアクセス コントロール リスト (ACL) を適用することができます。

関連トピック

高度な WLAN プロパティの設定（CLI）（3319 ページ）
レイヤ 2 セキュリティの前提条件（3345 ページ）

WLAN セキュリティの設定方法

静的WEPおよび802.1Xレイヤ2セキュリティパラメータの設定（CLI）

始める前に

管理者特権が必要です。

手順

	コマンドまたはアクション	目的
ステップ1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ3	**security static-wep-key** {**authentication** {**open** | **sharedkey**} | **encryption** {**104** | **40**} [**ascii** | **hex**] {**0** | **8**}} *wep-key wep-key-index1-4* 例： `Device(config-wlan)# security static-wep-key encryption 40 hex 0 test 2`	WLAN の静的 WEP セキュリティを設定します。次のキーワードと引数があります。 • **authentication**：802.11 認証を設定します。 • **encryption**：静的 WEP キーとインデックスを設定します。 • **open**：オープン システム認証を設定します。 • **sharedkey**：共有キー認証を設定します。 • **104, 40**：WEP キーのサイズを指定します。 • **hex, ascii**：キーの入力形式を指定します。 • *wep-key-index*、*wep-key-index1-4* 指定するパスワードのタイプです。値が 0 である場合は、暗号化されないパスワードを指定することを示しま

	コマンドまたはアクション	目的
		す。値が 8 である場合は、AES 暗号化を指定することを示します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件 （3345 ページ）

静的 WEP レイヤ 2 セキュリティ パラメータの設定（CLI）

始める前に

管理者特権が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**security static-wep-key** ［**authentication** {**open** | **shared**} | **encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]] 例： `Device(config-wlan)# security static-wep-key authentication open`	キーワードは次のとおりです。 • **static-wep-key**：静的な WEP キー認証を設定します。 • **authentication**：設定する認証タイプを指定します。値は、open および shared です。 • **encryption**：設定する暗号化タイプを指定します。有効な値は 104 と 40 です。40 ビットキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。104 ビットキーには、ASCII テキスト文字が

	コマンドまたはアクション	目的
		13 文字と 16 進数文字が 26 文字必要です。 • **ascii**：キー形式を ASCII に指定します。 • **hex**：キー形式を HEX に指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件 （3345 ページ）

WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（CLI）

（注） デフォルト セキュリティ ポリシーは、WPA2 です。

始める前に

管理者特権が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**security wpa** 例： `Device(config-wlan)# security wpa`	WPA をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**security wpa wpa1** 例： `Device(config-wlan)# security wpa wpa1`	WPA1 をイネーブルにします。
ステップ 5	**security wpa wpa1 ciphers** [**aes** | **tkip**] 例： `Device(config-wlan)# security wpa wpa1 ciphers aes`	WPA1 暗号を指定します。次のいずれかの暗号化タイプを選択します。 • **aes**：WPA/AES のサポートを指定します。 • **tkip**：WPA/TKIP のサポートを指示します。
ステップ 6	**security wpa wpa2** 例： `Device(config-wlan)# security wpa`	WPA 2 をイネーブルにします。
ステップ 7	**security wpa wpa2 ciphers** [**aes** | **tkip**] 例： `Device(config-wlan)# security wpa wpa2 ciphers tkip`	WPA2 暗号化を設定します。次のいずれかの暗号化タイプを選択します。 • **aes**：WPA/AES のサポートを指定します。 • **tkip**：WPA/TKIP のサポートを指示します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件 （3345 ページ）

802.1X レイヤ 2 セキュリティ パラメータの設定（CLI）

始める前に

管理者特権が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**security dot1x** 例： `Device(config-wlan)# security dot1x`	802.1X セキュリティを指定します。
ステップ 4	**security** [**authentication-list** *auth-list-name* | **encryption** {**0** | **104** | **40**} 例： `Device(config-wlan)# security encryption 104`	次のキーワードと引数があります。 • **authentication-list**：IEEE 802.1x の認証リストを指定します。 • **encryption**：CKIP 暗号化キーの長さを指定します。有効な値は、0、40、および 104 です。ゼロ（0）では暗号化されません。これはデフォルトです。 （注） WLAN 内のすべてのキーは、同じサイズでなければなりません。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件 （3345 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	『*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』
セキュリティ コンフィギュレーション ガイド	『*Security Configuration Guide (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

WLAN レイヤ 2 セキュリティに関する機能情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
WLAN のセキュリティ機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 161 章

WLAN ごとのクライアント カウントの設定

- 機能情報の確認 （3355 ページ）
- WLAN ごとのクライアント カウントの設定に関する制約事項 （3355 ページ）
- WLAN ごとのクライアント カウントの設定について （3356 ページ）
- WLAN ごとのクライアント カウントを設定する方法 （3356 ページ）
- クライアントの接続の監視（CLI） （3358 ページ）
- クライアント接続に関する追加情報 （3359 ページ）
- WLAN ごとのクライアント接続に関する機能情報 （3360 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

WLAN ごとのクライアント カウントの設定に関する制約事項

- WLAN が接続クライアントの最大数の制限に達しているか、AP 無線および新しいクライアントが WLAN に参加しようとしている場合、クライアントは既存のクライアントが切断されるまで WLAN に接続できません。
- ローミング クライアントは新しいクライアントと見なされます。クライアントの接続数の最大制限に到達している WLAN に対して新しいクライアントは、既存のクライアントが切断されたときにのみ接続できます。

（注） サポートされているクライアント数の詳細については、デバイスの製品データ シートを参照してください。

関連トピック

WLAN ごとのクライアント カウントの設定（CLI） （3356 ページ）
WLAN ごとの各 AP のクライアント数の設定（CLI） （3357 ページ）
WLAN あたりの AP 無線ごとのクライアント数の設定（CLI） （3358 ページ）
WLAN ごとのクライアント カウントの設定について （3356 ページ）

WLAN ごとのクライアント カウントの設定について

WLANに接続できるクライアントの数に制限を設定できます。これは、デバイスに接続できるクライアントの数に制限があるシナリオで役立ちます。たとえば、デバイスが WLAN 上の最大256個のクライアントに対応でき、これらのクライアントが企業ユーザ（従業員）およびゲスト ユーザ間で共有される場合について考えます。特定の WLAN にアクセス可能なゲスト クライアントの数に制限を設定できます。WLAN ごとに設定できるクライアントの数は、使用しているプラットフォームによって異なります。

関連トピック

WLAN ごとのクライアント カウントの設定（CLI） （3356 ページ）
WLAN ごとの各 AP のクライアント数の設定（CLI） （3357 ページ）
WLAN あたりの AP 無線ごとのクライアント数の設定（CLI） （3358 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項 （3355 ページ）
クライアントの接続の監視（CLI） （3358 ページ）

WLAN ごとのクライアント カウントを設定する方法

WLAN ごとのクライアント カウントの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例：	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設

	コマンドまたはアクション	目的
	`Device# wlan test4`	定されている WLAN のプロファイル名です。
ステップ 3	**client associationlimit** *limit* 例： `Device(config-wlan)# client association limit 2000`	WLAN ごとのクライアント アソシエーションの最大数を設定します。有効な範囲は 0 ～ 2000 ですデフォルト値は 0 です（制限なし）。
ステップ 4	**end** 例： `Device(wlan-config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN ごとのクライアント カウントの設定について （3356 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項 （3355 ページ）
クライアントの接続の監視（CLI） （3358 ページ）

WLAN ごとの各 AP のクライアント数の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client association limit ap** *ap-limit* 例： `Device(config-wlan)# client association limit ap 250`	WLAN ごとの AP あたりの最大クライアント数を設定します。範囲は 1 ～ 400 です。
ステップ 4	**end** 例： `Device(wlan-config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN ごとのクライアント カウントの設定について （3356 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項 （3355 ページ）
クライアントの接続の監視（CLI） （3358 ページ）

WLAN あたりの AP 無線ごとのクライアント数の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client association limit radio** *max-client-connections* 例： `Device(config-wlan)# client association limit radio 180`	WLAN あたりの AP 無線ごとのクライアント接続の最大数を設定します。a、b、および g 無線でこの範囲は 0～ 200 です。
ステップ 4	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN ごとのクライアント カウントの設定について （3356 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項 （3355 ページ）
クライアントの接続の監視（CLI） （3358 ページ）

クライアントの接続の監視（CLI）

次のコマンドがデバイスクライアント接続の監視に使用できます。

コマンド	説明

show wlan name *wlan-name*	WLAN プロパティを表示します。次に例を示します。
	
	`. . . .`
	`Max Associated Clients per WLAN :0`
	`Max Associated Clients per AP per WLAN :0`
	`Max Associated Clients per AP Radio per WLAN :0`
	`. . .`
	`. . .`

show wlan id *wlan-id*	WLAN のプロパティを表示します。ここに一例を上げます:
	
	`. . . .`
	`Max Associated Clients per WLAN :0`
	`Max Associated Clients per AP per WLAN :0`
	`Max Associated Clients per AP Radio per WLAN :0`
	`. . .`
	`. . .`

関連トピック

WLAN ごとのクライアント カウントの設定（CLI） （3356 ページ）
WLAN ごとの各 AP のクライアント数の設定（CLI） （3357 ページ）
WLAN あたりの AP 無線ごとのクライアント数の設定（CLI） （3358 ページ）
WLAN ごとのクライアント カウントの設定について （3356 ページ）

クライアント接続に関する追加情報

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	『*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
このリリースのすべての MIB です。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

WLAN ごとのクライアント接続に関する機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能名	リリース	機能情報
WLAN、AP、AP 無線ごとのクライアント接続	Cisco IOS XE 3.3SE	この機能が導入されました。

第 162 章

802.11w の設定

- 機能情報の確認 （3361 ページ）
- 802.11w の前提条件 （3361 ページ）
- 802.11w の制約事項 （3362 ページ）
- 802.11w に関する情報 （3362 ページ）
- 802.11w の設定方法 （3363 ページ）
- 802.11w のディセーブル（CLI） （3365 ページ）
- 802.11w の監視（CLI） （3366 ページ）
- 802.11w に関する追加情報 （3367 ページ）
- 802.11w の機能に関する情報 （3369 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

802.11w の前提条件

- 任意および必須の 802.11w 機能を設定するには、WPA および AKM を設定する必要があります。

（注） Robust Secure Network（RNS）IE は AES 暗号化とともにイネーブルにする必要があります。

- 必須として 802.11w を設定するには、WPA AKM に加えて PMF AKM を有効にします。

関連トピック

802.11w の設定（CLI）（3363 ページ）
802.11w のディセーブル（CLI）（3365 ページ）
802.11w に関する情報（3362 ページ）

802.11w の制約事項

- 802.11w は、オープン WLAN、 WEP 暗号化 WLAN、または TKIP 暗号化 WLAN に適用できません。
- 802.11w が設定された WLAN では、WPA2-PSK または WPA2-802.1x セキュリティを設定する必要があります。

関連トピック

802.11w の設定（CLI）（3363 ページ）
802.11w のディセーブル（CLI）（3365 ページ）
802.11w に関する情報（3362 ページ）

802.11w に関する情報

Wi-Fi は、正規のデバイスまたは不法なデバイスのいずれであっても、あらゆるデバイスで傍受または参加が可能なブロードキャスト メディアです。認証/認証解除、アソシエーション/ディスアソシエーション、ビーコンおよびプローブなどの制御/管理フレームは、無線クライアントによって、AP を選択し、ネットワーク サービスのセッションを開始するために使用されます。

機密保持レベルを提供する暗号化可能なデータ トラフィックとは異なり、これらのフレームは、すべてのクライアントによって解釈されることが必要であり、したがってオープンまたは非暗号化形式で送信されます。これらのフレームは暗号化できませんが、攻撃から無線メディアを保護するために偽造を防止することが必要になります。 たとえば、攻撃者はクライアントと AP の間のセッションを切断するために、AP から管理フレームをスプーフィングする可能性があります。

802.11w プロトコルは、管理フレーム保護（PMF）サービスによって保護された一連の強力な管理フレームにのみ適用されます。これらには、ディスアソシエーション、認証解除、ロバスト アクション フレームが含まれます。

したがって、ロバストアクションであり、保護されているものと見なされる管理フレームは次のとおりです。

- スペクトル管理
- QoS

- ブロック ACK
- SA クエリ
- ベンダー固有保護

802.11w が無線メディアで実行されると、次のことが行われます。

- ディスアソシエーション フレームと認証解除フレームに対して、（MIC 情報要素を含めることにより）AP の暗号保護によるクライアント保護が追加されます。これによって、DoS 攻撃でのスプーフが防止されます。
- アソシエーションの復帰期間と SA クエリーの手順から構成されるセキュリティ アソシエーション（SA）ティア ダウン保護メカニズムを追加することによって、インフラストラクチャの保護が追加され、スプーフィングされた要求によるすでに接続済みのクライアントの切断が防止されます。

関連トピック

802.11w の設定（CLI）（3363 ページ）
802.11w のディセーブル（CLI）（3365 ページ）
802.11w の前提条件（3361 ページ）
802.11w の制約事項（3362 ページ）
802.11w の監視（CLI）（3366 ページ）

802.11w の設定方法

802.11w の設定（CLI）

始める前に

WPA および AKM を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。

	コマンドまたはアクション	目的
ステップ 3	**shutdown** 例： `Device shutdown`	PMF を設定する前に WLAN をシャットダウンします。
ステップ 4	**security pmf** {**association-check** *association-comeback-time-in-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-in-milliseconds*} 例： `Device(config-wlan)# security pmf saquery-retry-time 200`	次のオプションにより PMF パラメータを設定します。 • **association-comeback**：802.11w アソシエーション復帰時間を設定します。 範囲は、1 ～ 20 秒です。 • **mandatory**：クライアントが WLAN の 802.11w PMF 保護をネゴシエートすることを要求します。 • **optional**：WLAN の 802.11w PMF 保護を有効にします。 • **saquery**：SA クエリの応答を受け取るまでの時間（ミリ秒単位）。デバイスが応答を受け取らなかった場合、別の SQ クエリーが試行されます。 指定できる範囲は 100 ～ 500 ミリ秒です。値には 100 ミリ秒の倍数を指定する必要があります。
ステップ 5	**no shutdown** 例： `Device no shutdown`	変更内容を反映するために、WLAN サーバを再起動します。
ステップ 6	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11w に関する情報 （3362 ページ）
802.11w の前提条件 （3361 ページ）
802.11w の制約事項 （3362 ページ）
802.11w の監視（CLI） （3366 ページ）

802.11w のディセーブル（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Device shutdown`	PMF を設定する前に WLAN をシャットダウンします。
ステップ 4	**no security pmf [association-comeback** *association-check-comback-interval-seconds* | | | *saquery-time-interval-milliseconds*]**mandatoryoptionalsaquery** 例： `Device(config-wlan)# no security pmf`	WLAN の PMF をディセーブルにします。次の属性を使用できます。 • **association-comeback**：802.11w アソシエーション復帰時間をディセーブルにします。 • **mandatory**：クライアントが WLAN の 802.11w PMF 保護をネゴシエートすることをディセーブルにします。 • **optional**：WLAN の 802.11w PMF 保護をディセーブルにします。 • **saquery**：アソシエーションを再試行する前に、すでにアソシエートされているクライアントへのアソシエーション応答で特定される時間間隔。アソシエーションの復帰期間中、この時間間隔により、クライアントが実際のクライアントであり、不正なクライアントではないかどうかが確認されます。クライアントがこの時間内に応答しない場合は、クライアント アソシエーションがデバイスから削除されます。

	コマンドまたはアクション	目的
		指定できる範囲は100～500ミリ秒です。値には100ミリ秒の倍数を指定する必要があります。
ステップ5	**no shutdown** 例： `Device no shutdown`	変更内容を反映するために、WLANサーバを再起動します。
ステップ6	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11w に関する情報 （3362 ページ）
802.11w の前提条件 （3361 ページ）
802.11w の制約事項 （3362 ページ）
802.11w の監視（CLI） （3366 ページ）

802.11w の監視（CLI）

802.11w の監視に使用できるコマンドは次のとおりです。

コマンド	説明

show wlan name *wlan-profile-name*	WLAN の WLAN パラメータを表示します。PMF パラメータが表示されます。次に例を示します。
	
	`. . . .`
	`. . . .`
	`Auth Key Management`
	`  802.1x :`
	` Disabled`
	`  PSK :`
	` Enabled`
	`  CCKM :`
	` Disabled`
	`  FT dot1x :`
	` Disabled`
	`  FT PSK :`
	` Disabled`
	`  PMF dot1x :`
	` Disabled`
	`  PMF PSK :`
	` Enabled`
	`  FT Support :`
	` Disabled`
	`  FT Reassociation Timeout :`
	` 20`
	`  FT Over-The-DS mode :`
	` Disabled`
	`  PMF Support :`
	` Required`
	`  PMF Association Comeback Timeout :`
	` 9`
	`  PMF SA Query Time :`
	` 200`
	`. . . .`
	`. . . .`

関連トピック

802.11w の設定（CLI）（3363 ページ）
802.11w のディセーブル（CLI）（3365 ページ）
802.11w に関する情報（3362 ページ）

802.11w に関する追加情報

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	『*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』
WLAN セキュリティ	このマニュアルの *WLAN* セキュリティの設定の章

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
802.11W	IEEE 802.11w 保護管理フレーム

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

802.11w の機能に関する情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能名	リリース	機能情報
802.11w	Cisco IOS XE 3.3SE	この機能が導入されました。

第 163 章

Wi-Fi Direct クライアント ポリシーの設定

- 機能情報の確認 （3371 ページ）
- Wi-Fi Direct クライアント ポリシーの制限 （3371 ページ）
- Wi-Fi Direct クライアント ポリシーについて （3372 ページ）
- Wi-Fi Direct クライアント ポリシーの設定方法 （3372 ページ）
- Wi-Fi Direct クライアント ポリシーに関する追加リファレンス （3375 ページ）
- Wi-Fi Direct クライアント ポリシーに関する機能情報 （3376 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Wi-Fi Direct クライアント ポリシーの制限

- Wi-Fi Direct クライアント ポリシーは、ローカル モードの AP が含まれる WLAN のみに適用できます。
- WLAN クライアントに適用されるポリシーが無効の場合、クライアントは「クライアント QoS ポリシー障害」という項目理由のため除外されます。

Wi-Fi Direct クライアント ポリシーについて

Wi-Fi Direct 対応のデバイスは迅速な相互接続が可能で、印刷、同期、データ共有などのタスクを効率的に実行できますWi-Fi Directデバイスは、複数のピアツーピア（P2P）デバイスおよびインフラストラクチャ無線LAN（WLAN）に同時にアソシエートしている場合があります。デバイスを使用して、Wi-Fi Direct クライアント ポリシーを WLAN 単位で設定できます。その際、Wi-Fiデバイスとインフラストラクチャ WLAN のアソシエーションを許可または禁止するか、WLAN に対して Wi-Fi Direct クライアント ポリシーをすべて無効にすることができます。

関連トピック

Wi-Fi Direct クライアント ポリシーの設定（CLI）（3372 ページ）
Wi-Fi Direct クライアント ポリシーのディセーブル（CLI）（3374 ページ）
Wi-Fi Direct クライアント ポリシーの監視（CLI）（3374 ページ）

Wi-Fi Direct クライアント ポリシーの設定方法

Wi-Fi Direct クライアント ポリシーの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**wifidirect policy** {**permit** | **deny** } 例： `Device(config-wlan)# wifidirect policy permit`	次のいずれかを使用して WLAN の Wi-Fi Direct クライアント ポリシーを設定します • **permit**：Wi-Fi Direct クライアントを有効にして WLAN とアソシエートします。 • **deny**：Wi-Fi Direct ポリシーが「拒否」に設定されている場合は、デバイスの機能に基づいて、デバイスが Wi-Fi Direct デバイスを許可または拒否します。Wi-Fi Direct デバイス

	コマンドまたはアクション	目的
		は、デバイスへのアソシエーション要求でこれらの機能をにレポートします。これは、このデバイスの Wi-Fi 機能に基づいて行われます。次の作業を行います。 • 同時操作 • 相互接続 （注） コマンド **no wifidirect policy** は、クライアントの Wi-Fi Direct ステータスを無視します。さらに、アクセス ポイントはビーコンおよびプローブをアドバタイズしません。実際には、このコマンドの **no** 形式では、WLAN の Wi-Fi Direct 機能はディセーブルになります。 Wi-Fi デバイスが同時操作または相互接続、あるいはその両方をサポートする場合は、クライアントの関連付けは拒否されます。クライアントは、デバイスが同時操作と相互接続をサポートしない場合に関連付けることができます。
ステップ 4	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

Wi-Fi Direct クライアント ポリシーについて （3372 ページ）
Wi-Fi Direct クライアント ポリシーの監視（CLI） （3374 ページ）

Wi-Fi Direct クライアント ポリシーのディセーブル（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**no wifidirect policy** 例： `Device(config)# no wifidirect policy`	クライアントの Wi-Fi Direct ステータスを無視し、それによって Wi-Fi Direct クライアントのアソシエーションを許可します
ステップ 4	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

Wi-Fi Direct クライアント ポリシーについて （3372 ページ）
Wi-Fi Direct クライアント ポリシーの監視（CLI） （3374 ページ）

Wi-Fi Direct クライアント ポリシーの監視（CLI）

次のコマンドが Wi-Fi Direct クライアント ポリシーを監視するために使用できます。

コマンド	説明
show wireless client wifidirect stats	関連付けられたクライアントの総数と、Wi-Fi Direct クライアント ポリシーを有効にした場合に拒否されたアソシエーション要求の数が表示されます。
show wlan summary	WLAN での Wi-Fi Direct の状態を表示します。
show wireless cli mac-address *mac-address*	クライアントの詳細情報を表示します。

関連トピック

Wi-Fi Direct クライアント ポリシーの設定（CLI） （3372 ページ）
Wi-Fi Direct クライアント ポリシーのディセーブル（CLI） （3374 ページ）

Wi-Fi Direct クライアント ポリシーについて （3372 ページ）

Wi-Fi Direct クライアント ポリシーに関する追加リファレンス

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	『*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Wi-Fi Direct クライアント ポリシーに関する機能情報

機能名	リリース	機能情報
Wi-Fi Direct の機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 164 章

802.11r BSS の高速移行の設定

- 機能情報の確認 （3377 ページ）
- 802.11R 高速移行の制約事項 （3377 ページ）
- 802.11R 高速移行について （3378 ページ）
- 802.11r 高速移行を設定する方法 （3380 ページ）
- 802.11r 高速移行に関する追加情報 （3387 ページ）
- 802.11r 高速移行の機能に関する情報 （3388 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

802.11R 高速移行の制約事項

- EAP LEAP 方式はサポートされません。
- TSpec は 802.11r 高速ローミングではサポートされません。したがって、RIC IE の処理はサポートされません。
- WAN リンク遅延がある場合、高速ローミングも遅延します。音声またはデータの最大遅延を確認する必要があります。Cisco WLC は、Over-the-Air および Over-the-DS DS 方式の両方をローミングする間、802.11r Fast Transition の認証要求を処理します。
- この機能は、オープンで WPA2 設定の WLAN でのみサポートされます。

- レガシー クライアントは、Robust Security Network Information Exchange（RSN IE）の解析を担当するサプリカントのドライバが古く、IE 内の追加 AKM を認識しない場合、802.11r が有効にされている WLAN にアソシエートできません。この制限のため、クライアントは、WLAN にアソシエーション要求を送信できません。ただし、これらのクライアントは、非 802.11r WLAN とアソシエートできます。802.11r 対応クライアントは、802.11r と 802.11i の両方の認証キー管理スイートが有効にされている WLAN の 802.11i クライアントとしてアソシエートできます。

  回避策は、レガシー クライアントのドライバを新しい 802.11r AKM で動作するようにするか、またはアップグレードすることです。そうすることで、レガシークライアントは、802.11r 対応 WLAN と正常にアソシエートできます。

  もう 1 つの回避策は、同じ名前で異なるセキュリティ設定（FT および非 FT）の 2 つの SSID を持つことです。

- 高速移行のリソース要求プロトコルは、クライアントがこのプロトコルをサポートしていないため、サポートされません。また、リソース要求プロトコルはオプションのプロトコルです。

- サービス不能（DoS）攻撃を回避するため、Cisco WLC では、異なる AP と最大 3 つの高速移行ハンドシェイクが可能です。

- 非 802.11r 対応デバイスは FT 対応 WLAN にアソシエートできなくなります。

- 802.11r FT + PMF はお勧めしません。

- 802.11r FT Over-the-Air ローミングは FlexConnect 導入にお勧めします。

関連トピック

オープン WLAN での 802.11r 高速移行の設定（CLI）（3380 ページ）
802.11r 高速移行のディセーブル（CLI）（3384 ページ）
Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI）（3382 ページ）
PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI）（3383 ページ）
802.11R 高速移行について（3378 ページ）

802.11R 高速移行について

高速ローミングの IEEE 標準である 802.11r は、クライアントがターゲット AP にローミングする前でも、新しい AP との最初のハンドシェイクが実行される、高速移行（FT）と呼ばれるローミングの新しい概念が導入されています。初期ハンドシェイクによって、クライアントと AP が事前に Pairwise Transient Key（PTK）計算をできるようになります。これらの PTK キーは、クライアントが新しいターゲット AP の再アソシエーション要求または応答の交換をした後で、クライアントと AP に適用されます。

802.11r は、次の 2 通りのローミングを提供します。

- Over-the-Air

- Over-the-DS（分散システム）

FT キー階層は、クライアントが各 AP での再認証なしで、AP 間の高速 BSS 移行ができるように設計されています。WLAN 設定には、FT（高速移行）と呼ばれる、新しい認証キー管理（AKM）タイプが含まれています。

リリース 3E から、WPAv2 WLAN でもある 802.11r WLAN を作成できます。以前のリリースでは、802.11r の WLAN と通常のセキュリティ用にそれぞれ個別の WLAN を作成する必要がありました。802.11r WLAN が非 802.11r アソシエーションを受け入れることができるため、非 802.11r クライアントが 802.11r WLAN 対応 WLAN に接続できるようになりました。混合モードまたは 802.11r 接続をサポートしないクライアントは、非 802.11r WLAN に接続できます。FT PSK 以降を設定すると、PSK を混合モードで WLAN を結合できる PSK だけ結合できるクライアントを定義します。

クライアントのローミング方法

FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の 2 つの方法のいずれかを使用して行われます。

- Over-the-Air：クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。
- Over-the-DS：クライアントは、現在の AP を介してターゲット AP と通信します。クライアントとターゲット AP との間の通信は、クライアントと現在の AP 間の FT アクションフレームで実行されてから、デバイスによって送信されます。

図 *151 : Over the Air* クライアントのローミングの設定時のメッセージ交換

この図は、Over the Air クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

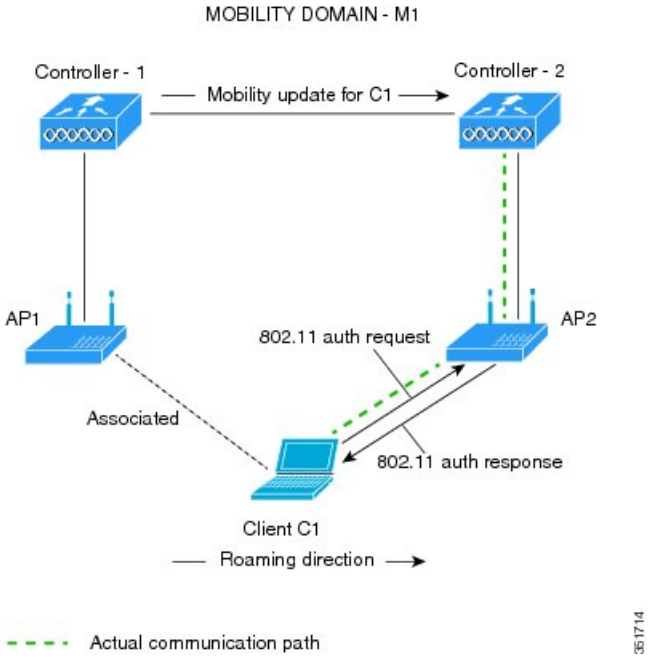
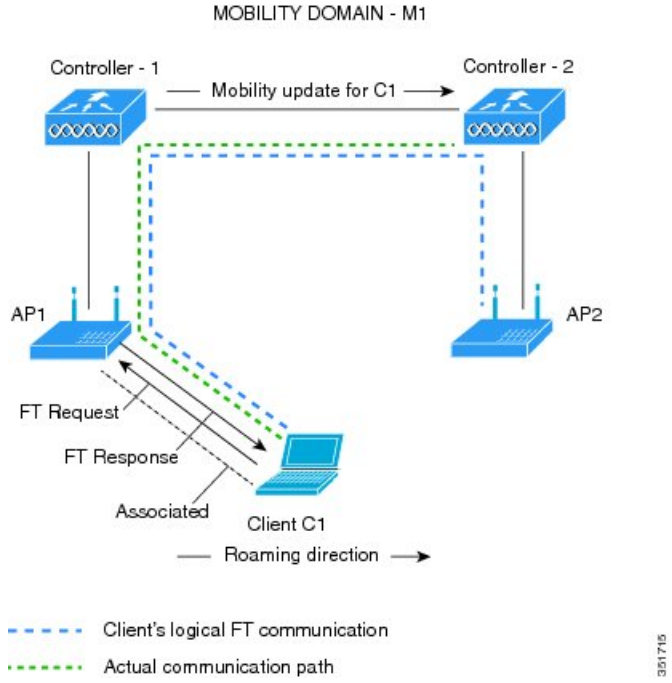


図 *152 : Over the Air* クライアントのローミングの設定時のメッセージ交換

この図は、Over the DS クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。



関連トピック

オープン WLAN での 802.11r 高速移行の設定（CLI）（3380 ページ）
802.11r 高速移行のディセーブル（CLI）（3384 ページ）
Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI）（3382 ページ）
PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI）（3383 ページ）
802.11r 高速移行の監視（CLI）（3385 ページ）
802.11R 高速移行の制約事項（3377 ページ）

802.11r 高速移行を設定する方法

オープン WLAN での 802.11r 高速移行の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-id* 例： `Device(config-wlan)# client vlan 0120`	WLAN にクライアント VLAN を関連付けます。
ステップ 4	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティをディセーブルにします。
ステップ 5	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対して AKM セキュリティをディセーブルにします。
ステップ 6	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 7	**no wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 8	**security ft** 例： `Device(config-wlan)# security ft`	802.11r 高速移行パラメータを指定します。
ステップ 9	**no shutdown** 例： `Device(config-wlan)# shutdown`	WLAN を停止します。
ステップ 10	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11R 高速移行について （3378 ページ）
802.11r 高速移行の監視（CLI） （3385 ページ）

802.11R 高速移行の制約事項 （3377 ページ）

Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-name* 例： `Device(config-wlan)# client vlan 0120`	この WLAN にクライアント VLAN を関連付けます。
ステップ 4	**local-auth** *local-auth-profile-eap* 例： `Device(config-wlan)# local-auth`	local auth EAP プロファイルをイネーブルにします。
ステップ 5	**security dot1x authentication-list default** 例： `Device(config-wlan)# security dot1x authentication-list default`	dot1x セキュリティ用のセキュリティ認証リストをイネーブルにします。この設定は、dot1x セキュリティ WLAN に似ています。
ステップ 6	**security ft** 例： `Device(config-wlan)# security ft`	WLAN 上で 802.11r 高速移行をイネーブルにします。
ステップ 7	**security wpa akm ft dot1x** 例： `Device(config-wlan)# security wpa akm ft dot1x`	WLAN 上で 802.1x セキュリティをイネーブルにします。
ステップ 8	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例：	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config-wlan)# end`	ンフィギュレーション モードを終了できます。

関連トピック

802.11R 高速移行について （3378 ページ）
802.11r 高速移行の監視（CLI） （3385 ページ）
802.11R 高速移行の制約事項 （3377 ページ）

PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-name* 例： `Device(config-wlan)# client vlan 0120`	この WLAN にクライアント VLAN を関連付けます。
ステップ 4	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**security wpa akm ft psk** 例： `Device(config-wlan)# security wpa akm ft psk`	FT PSK サポートを設定します。
ステップ 6	**security wpa akm psk set-key** {**ascii** {**0** | **8**} | **hex** {**0** | **8**}} 例： `Device(config-wlan)# security wpa akm psk set-key ascii 0 test`	PSK AKM の共有キーを設定します。

	コマンドまたはアクション	目的
ステップ 7	**security ft** 例： `Device(config-wlan)# security ft`	802.11r 高速移行を設定します。
ステップ 8	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11R 高速移行について （3378 ページ）
802.11r 高速移行の監視（CLI） （3385 ページ）
802.11R 高速移行の制約事項 （3377 ページ）

802.11r 高速移行のディセーブル（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*] 例： `Device(config-wlan)# no security ft over-the-ds`	WLAN の 802.11r 高速移行をディセーブルにします。 （注） データ ソースに対して 802.11r 高速移行をディセーブルにすると、Over the Air の高速移行がイネーブルになります。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config)# end`	ンフィギュレーション モードを終了できます。

関連トピック

802.11R 高速移行について （3378 ページ）
802.11r 高速移行の監視（CLI） （3385 ページ）
802.11R 高速移行の制約事項 （3377 ページ）

802.11r 高速移行の監視（GUI）

クライアントの認証キー管理の詳細情報を表示できます。

[Monitor] > [Client] を選択します。[Clients] ページが表示されます。クライアントの詳細を表示するには、該当するクライアントを選択します。[General] タブで、FT、PSK、802.1X、CCKM、802.1x+CCKM など、クライアントの認証キー管理を確認できます。 AKM が 802.11r 混合モード用の場合、FT-802.1x、FT-802.1x-CCKM、または FT-PSK が表示されます。

802.11r 高速移行の監視（CLI）

次のコマンドを使用して、802.11r の高速移行を監視できます。

コマンド	説明
showwlanname *wlan-name*	WLAN に設定されているパラメータの要約を表示します。

コマンド	説明

showwirelessclientmac-address *mac-address*	クライアントの 802.11r 認証キー管理の設定の概要を表示します。
	
	`. . .`
	`. . .`
	`Client Capabilities`
	`  CF Pollable : Not implemented`
	`  CF Poll Request : Not implemented`
	`  Short Preamble : Not implemented`
	`  PBCC : Not implemented`
	`  Channel Agility : Not implemented`
	`  Listen Interval : 15`
	`  Fast BSS Transition : Implemented`
	`Fast BSS Transition Details :`
	`Client Statistics:`
	`  Number of Bytes Received : 9019`
	`  Number of Bytes Sent : 3765`
	`  Number of Packets Received : 130`
	`  Number of Packets Sent : 36`
	`  Number of EAP Id Request Msg Timeouts : 0`
	
	`  Number of EAP Request Msg Timeouts : 0`
	`  Number of EAP Key Msg Timeouts : 0`
	`  Number of Data Retries : 1`
	`  Number of RTS Retries : 0`
	`  Number of Duplicate Received Packets : 1`
	`  Number of Decrypt Failed Packets : 0`
	`  Number of Mic Failured Packets : 0`
	`  Number of Mic Missing Packets : 0`
	`  Number of Policy Errors : 0`
	`  Radio Signal Strength Indicator : -48 dBm`
	
	`  Signal to Noise Ratio : 40 dB`
	`. . .`
	`. . .`
	
	クライアントの AKM が 802.11r 混合モードの場合、次の情報が出力に表示されます。
	
	`. . .`
	`. . .`
	`Authentication Key Management : FT-PSK`
	`. . .`
	`. . .`

関連トピック

オープン WLAN での 802.11r 高速移行の設定（CLI）（3380 ページ）
802.11r 高速移行のディセーブル（CLI）（3384 ページ）
Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI）（3382 ページ）
PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI）（3383 ページ）
802.11R 高速移行について（3378 ページ）

802.11r 高速移行に関する追加情報

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	『*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
IEEE 802.11r。	802.11r 用の IEEE 規格

MIB

MIB	MIB のリンク
このリリースでサポートされるすべての MIB です。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

802.11r 高速移行の機能に関する情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能名	リリース	機能情報
802.11r の高速移行	Cisco IOS XE 3.3SE	この機能が導入されました。

第 165 章

経由ローミングの設定

- 機能情報の確認 （3389 ページ）
- 経由ローミングの制約事項 （3389 ページ）
- 経由ローミングについて （3390 ページ）
- 経由ローミングの設定方法 （3391 ページ）
- 経由ローミングの監視 （3393 ページ）
- 経由ローミングの設定例 （3393 ページ）
- 経由ローミングに関する追加情報 （3394 ページ）
- 経由ローミング設定の機能履歴と情報 （3395 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

経由ローミングの制約事項

- 経由ローミング機能は、複数のデバイスでサポートされます。
- この機能は、802.11n 対応の屋内アクセス ポイントでのみサポートされています。 シングル バンド構成の場合は、最大 6 つのネイバーがネイバー リストに表示されます。デュアル バンド構成の場合、最大 12 のネイバーが表示されます。
- デバイス CLI をのみを使用して経由ローミングを設定できます。

関連トピック

経由ローミングについて （3390 ページ）
経由ローミングの設定（CLI） （3391 ページ）

経由ローミングについて

802.11k 標準では、クライアントがサービス セットの移行の候補となる既知のネイバー アクセス ポイントに関する情報を含むネイバー レポートを要求することができます。802.11k ネイバー リストを使用すると、アクティブおよびパッシブ スキャンを軽減できます。

経由ローミング機能は、インテリジェントでクライアントによって最適化されたネイバー リストに基づいています。

Cisco Client Extension（CCX）ネイバー リストとは異なり、802.11k ネイバー リストは動的かつオンデマンドで生成されます。デバイス上では維持されません。802.11k ネイバー リストは、クライアントのロケーションに基づくもので、Mobility Services Engine (MSE) を必要としません。同じデバイス上であっても異なる AP の 2 クライアントが、周囲の AP の個々の関係に応じて提供される異なるネイバー リストを設定できます。

デフォルトでは、ネイバー リストには、クライアントがアソシエートされている同じ帯域のネイバーだけが含まれます。ただし、両方の帯域のネイバーを返すために、802.11k を可能にするスイッチが存在します。

クライアントは、ビーコン内の RRM（無線リソース管理）機能の情報要素（IE）をアドバタイズする AP に関連付けた後でのみ、ネイバー リストの要求を送信します。ネイバー リストには、隣接する無線の BSSID、チャネル、および処理の詳細についての情報が含まれます。

ネイバー リストの作成と最適化

802.11k ネイバー リスト要求をデバイスが受信すると、次の処理が実行されます。

1. デバイスは、クライアントが現在関連付けられている AP と同じ帯域で、ネイバー リストについて RRM ネイバー テーブルを検索バンドします。
2. デバイスは、帯域ごとにネイバー リストを 6 つに削減するために、AP 間の RSSI（Received Signal Strength Indication）、現在の AP の現在のロケーション、Cisco Prime インフラストラクチャからのネイバー AP のフロア情報、デバイス上でのローミング履歴情報に従ってネイバーをチェックします。このリストは、同じフロアの AP に対して最適化されています。

非 802.11k クライアントの経由ローミング

非 802.11k クライアントのローミングを最適化することもできます。クライアントが 802.11k ネイバー リスト要求を送信する必要なく、各クライアントの予測ネイバー リストを生成できます。成功した各クライアント アソシエーション/再アソシエーションの後、WLAN でこれが有効である場合、ネイバー リストを生成し、モバイル ステーションのソフトウェア データ構造にリストを格納するために、同じネイバー リストの最適化を非 802.11k クライアントに適用する必要があります。クライアント プローブが異なるネイバーによって異なる RSSI 値により

認識されるため、異なるロケーションのクライアントが異なるリストを持ちます。クライアントは、通常はアソシエーションまたは再アソシエーションの前にプローブするため、このリストは、更新されたほとんどのプローブデータによって構築され、クライアントがローミングする可能性が高い次の AP を予測します。

AP へのアソシエーション要求が保存された予測ネイバー リストのエントリに一致しない場合に、アソシエーションを拒否することによって、あまり望ましくないネイバーへのクライアントのローミングを抑止します。

アグレッシブ ロード バランシングに加えて、経由ローミング機能を毎 WLAN ごとおよびグローバルにオンにするスイッチがあります。次のオプションを使用できます。

- Denial count：クライアントでアソシエーションが拒否される最大回数です。
- Prediction threshold：経由ローミング機能をアクティブにするために、予測リスト内で必要なエントリの最小数です。

ロード バランシングおよび経由ローミングの両方で、クライアントがアソシエートする AP に影響を与えるように設計されているため、WLAN で両オプションを同時にイネーブルにすることはできません。

関連トピック

経由ローミングの設定（CLI）（3391 ページ）
経由ローミングの制約事項（3389 ページ）
経由ローミングの監視（3393 ページ）
経由ローミングの設定例（3393 ページ）

経由ローミングの設定方法

経由ローミングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless assisted-roaming floor-bias** *dBm* 例： `Device(config)# wireless assisted-roaming floor-bias 20`	ネイバー フロア ラベル バイアスを設定します。有効な範囲は –5 ～ 25 dBm で、デフォルト値は –15 dBm です。

	コマンドまたはアクション	目的
ステップ 3	**wlan** *wlan-id* 例： `Device(config)# wlan wlan1`	WLAN コンフィギュレーション サブモードを開始します。*wlan-name* は設定されている WLAN のプロファイル名です。
ステップ 4	**assisted-roaming neighbor-list** 例： `Device(wlan)# assisted-roaming neighbor-list`	WLAN の 802.11k ネイバー リストを設定します。WLANを作成すると、デフォルトでネイバー リストで経由ローミングがイネーブルになります。コマンドの **no**形式では、経由ローミングのネイバー リストが無効になります。
ステップ 5	**assisted-roaming dual-list** 例： `Device(wlan)# assisted-roaming dual-list`	WLAN のデュアル バンド 802.11k デュアル リストを設定します。WLAN を作成すると、デフォルトでデュアル リストで経由ローミングがイネーブルになります。コマンドの **no** 形式では、経由ローミングのデュアル リストが無効になります。
ステップ 6	**assisted-roaming prediction** 例： `Device(wlan)# assisted-roaming prediction`	WLAN の経由ローミング予測リスト機能を設定します。デフォルトでは、経由ローミング予測リストはディセーブルです。 （注） ロードバランシングが WLAN に対してすでにイネーブルである場合、警告メッセージが表示され、ロード バランシングが WLAN に対してディセーブルになります。
ステップ 7	**wireless assisted-roaming prediction-minimum** *count* 例： `Device# wireless assisted-roaming prediction-minimum`	予測リスト機能が動作するために必要な予測 AP の最小数を設定します。デフォルト値は 3 です。 （注） クライアントに割り当てられた Forecast、AP が指定した数よりもこの値が小さい場合、経由ローミング機能はこのルールに適用されません。
ステップ 8	**wireless assisted-roaming denial-maximum** *count* 例：	AP に送信されたアソシエーション要求が予測の AP に一致しない場合に、クライアントでアソシエーションを拒否でき

	コマンドまたはアクション	目的
	`Device# wireless assisted-roaming denial-maximum 8`	る最大回数を設定します。有効な範囲は 1 ～ 10 で、デフォルト値は 5 です。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

経由ローミングについて （3390 ページ）
経由ローミングの制約事項 （3389 ページ）
経由ローミングの監視 （3393 ページ）
経由ローミングの設定例 （3393 ページ）

経由ローミングの監視

WLAN に設定された経由ローミングを監視するために次のコマンドが使用できます。

コマンド	説明
show wlan id *wlan-id*	WLAN の WLAN パラメータを表示します。

関連トピック

経由ローミングについて （3390 ページ）
経由ローミングの設定（CLI） （3391 ページ）

経由ローミングの設定例

次に、ネイバー フロア ラベル バイアスを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless assisted-roaming floor-bias 10
Device(config)# end
Device# show wlan id 23
```

次に、特定の WLAN のネイバー リストをディセーブルにする例を示します。

```
Device# configure terminal
Device(config)# wlan test1
Device(config (wlan)# no assisted-roaming neighbor-list
Device(config)(wlan)# end
Device# show wlan id 23
```

次に、特定の WLAN の予測リストを設定する例を示します。

```
Device# configure terminal
Device(config)# wlan test1
Device(config)(wlan)# assisted-roaming prediction
Device(config)(wlan)# end
Device# show wlan id 23
```

次に、特定の WLAN の経由ローミングの予測しきい値および最大の拒否数に基づいて予測リストを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless assisted-roaming prediction-minimum 4
Device(config)# wireless assisted-roaming denial-maximum 4
Device(config)(wlan)# end
Device# show wlan id 23
```

関連トピック

経由ローミングについて （3390 ページ）
経由ローミングの設定（CLI） （3391 ページ）

経由ローミングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
802.11k	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

経由ローミング設定の機能履歴と情報

機能名	リリース	機能情報
経由ローミング	Cisco IOS XE 3.2SE	この機能が導入されました。

第 166 章

アクセス ポイント グループの設定

- 機能情報の確認 （3397 ページ）
- AP グループを設定するための前提条件 （3397 ページ）
- アクセス ポイント グループの設定に関する制約事項 （3398 ページ）
- アクセス ポイント グループについて （3399 ページ）
- アクセス ポイント グループの設定方法 （3399 ページ）
- その他の参考資料 （3401 ページ）
- アクセス ポイント グループの機能履歴と情報 （3402 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

AP グループを設定するための前提条件

次に、デバイスでアクセス ポイント グループを作成するための前提条件を示します。

- VLAN またはサブネットにサービスを提供するルータ上で、必要なアクセス コントロール リスト（ACL）を定義する必要があります。
- アクセス ポイント グループ VLAN では、マルチキャスト トラフィックがサポートされます。ただし、クライアントがあるアクセス ポイントから別のアクセス ポイントにローミングする場合、IGMP スヌーピングが有効になっていないと、クライアントによってマルチキャスト トラフィックの受信が停止されることがあります。

関連トピック

アクセス ポイント グループについて （3399 ページ）
アクセス ポイント グループの設定に関する制約事項 （3398 ページ）

アクセス ポイント グループの設定に関する制約事項

（注） Cisco IOS XE Denali 16.3.5 では、AP グループを WLAN にマッピングする動作が変更されています。このリリースからは、WLAN を設定してから AP グループにマッピングする必要があります。同様に、WLAN を削除するには、その前に WLAN から AP グループのマッピングを解除する必要があります。

以前は、WLAN が先に設定されていなくても WLAN を AP グループにマッピングできました。また、AP グループにマッピングしたままでも WLAN を削除できました。

- AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN インターフェイスと同じであるとします。WLANインターフェイスが変更されると、AP グループ テーブル内の WLAN に対するインターフェイス マッピングも新しい WLAN インターフェイスに変わります。

  AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN に定義されたインターフェイスと異なるとします。WLANインターフェイスが変更されても、AP グループ テーブル内の WLAN に対するインターフェイス マッピングは新しい WLAN インターフェイスに変わりません。

- デバイス上の設定をクリアすると、アクセス ポイント グループのすべてが非表示となります。ただし、デフォルトのアクセス ポイント グループである「default-group」（自動的に作成される）は例外です。

- デフォルトのアクセス ポイント グループには、最大 16 の WLAN を関連付けることができます。デフォルトのアクセス ポイント グループの WLAN ID は、16 以下である必要があります。大規模なデフォルトのアクセス ポイント グループ内で ID が 16 以上の WLAN が作成されると、WLAN SSID はブロードキャストされません。デフォルトのアクセス ポイント グループのすべての WLAN ID で ID が 16 以下であることが必要です。16 を超える ID を含む WLAN は、カスタム アクセス ポイント グループに割り当てることができます。

- 同じ AP グループと同じ FlexConnect グループに属しているメッシュ ツリー（同じセクター）内のすべての フレックス + ブリッジ AP は WLAN-VLAN マッピングを正しく継承するように設定することをお勧めします。

関連トピック

アクセス ポイント グループについて （3399 ページ）
AP グループを設定するための前提条件 （3397 ページ）

アクセス ポイント グループについて

デバイス上に最大512のWLANを作成した後では、さまざまなアクセス ポイントにWLANを選択的に公開（アクセス ポイント グループを使用して）することで、ワイヤレス ネットワークをより適切に管理できます。一般的な展開では、WLAN上のすべてのユーザはデバイス上の1つのインターフェイスにマップされます。したがって、WLANに接続しているすべてのユーザは、同じサブネットまたはVLANに存在します。しかし、複数のインターフェイス間で負荷を分散すること、またはアクセスポイントグループを作成して、個々の部門（たとえばマーケティング部門）などの特定の条件に基づくグループユーザへと負荷を分配することを選択できます。さらに、ネットワーク管理を簡素化するために、これらのアクセス ポイント グループを別個のVLANで設定できます。

関連トピック

アクセス ポイント グループの作成 （3399 ページ）
アクセス ポイント グループの表示 （3401 ページ）
AP グループへのアクセス ポイントの割り当て （3400 ページ）
AP グループを設定するための前提条件 （3397 ページ）
アクセス ポイント グループの設定に関する制約事項 （3398 ページ）

アクセス ポイント グループの設定方法

アクセス ポイント グループの作成

始める前に

この操作を実行するには、管理者特権が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap group** *ap-group-name* 例： `Device(config)# ap group my-ap-group`	アクセス ポイント グループを作成します。
ステップ 3	**wlan** *wlan-name* 例： `Device(config-apgroup)# wlan wlan-name`	WLANにAPグループを関連付けます。

	コマンドまたはアクション	目的
ステップ 4	（任意） **vlan** *vlan-name* 例： `Device(config-apgroup)# vlan test-vlan`	VLAN にアクセス ポイント グループを割り当てます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

次に、AP グループを作成する例を示します。

```
Device# configure terminal
Device(config-apgroup)# ap group test-ap-group-16
Device(config-wlan-apgroup)# wlan test-ap-group-16
Device(config-wlan-apgroup)# vlan VLAN1300
```

関連トピック

アクセス ポイント グループについて （3399 ページ）

AP グループへのアクセス ポイントの割り当て

始める前に

この操作を実行するには、管理者特権が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name* **ap-group-name** *ap-group* 例： `Device# ap name 1240-101 ap-groupname apgroup_16`	アクセス ポイント グループにアクセス ポイントを割り当てます。次のキーワードと引数があります。 • **name**：このキーワードに続く引数がデバイスに関連付けられている AP の名前であることを指定します。 • *ap-name*：AP グループに関連付けたい AP。 • **ap-group-name**：このキーワードに続く引数が、デバイスで設定された

	コマンドまたはアクション	目的
		AP グループの名前となるように指定します。 • *ap-group*：デバイスで設定されたアクセス ポイント グループの名前。

関連トピック

アクセス ポイント グループについて （3399 ページ）

アクセス ポイント グループの表示

始める前に

この操作を実行するには、管理者特権が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**show ap groups** [**extended**] 例： `Device# show ap groups`	デバイスで設定された AP グループを表示します。**extended** キーワードは、システムで詳細に定義されているすべての AP グループ情報を表示します。

関連トピック

アクセス ポイント グループについて （3399 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
WLAN コマンド	『*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』
Lightweight アクセス ポイント コンフィギュレーション	『*Lightweight Access Point Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』
Lightweight アクセス ポイント コマンド	『*Lightweight Access Point Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

アクセス ポイント グループの機能履歴と情報

次の表で、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
AP グループ数	Cisco IOS XE 3.2SE	この機能が導入されました。

第 XXIII 部

データ モデル

- YANG データモデルの設定 （3405 ページ）
- プログラマビリティ：ネットワーク ブートローダ （3411 ページ）

第 167 章

YANG データモデルの設定

- 機能情報の確認 （3405 ページ）
- データ モデルの概要：プログラムによる設定と各種の標準規格に準拠した設定 （3405 ページ）
- データ モデルの設定方法 （3407 ページ）
- データ モデルに関する追加情報 （3409 ページ）
- データ モデルの機能情報 （3410 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

データモデルの概要：プログラムによる設定と各種の標準規格に準拠した設定

ネットワーク デバイスを管理する従来の方法は、階層的データ（設定コマンド）および運用データ（show コマンド）用のコマンドライン インターフェイス（CLI）を使用することです。ネットワーク管理の場合、特にさまざまなネットワーク デバイス間で管理情報を交換するために、Simple Network Management Protocol（SNMP）が広く使用されています。頻繁に使用されている CLI と SNMP ですが、これにはいくつかの制約事項があります。CLI は非常に独自的であり、テキストベースの仕様を理解し、解釈するには人間の介入が必要です。SNMP は、階層的データと運用データを区別しません。

これを解決するには、手作業で設定作業を行うのではなく、プログラムを使用したり、各種の標準規格に準拠してネットワーク デバイスの設定を記述します。Cisco IOS XE で動作するネットワーク デバイスは、データ モデルを使用するネットワーク上の複数のデバイスの設定の自動化をサポートしています。データ モデルは、業界で定義された標準的な言語で開発され、ネットワークの設定とステータス情報を定義できます。

Cisco IOS XE は、Yet Another Next Generation（YANG）データ モデリング言語をサポートしています。YANG をネットワーク設定プロトコル（NETCONF）で使用すると、自動化されたプログラミング可能なネットワーク操作の望ましいソリューションが実現します。NETCONF（RFC 6241）は、クライアント アプリケーションがデバイスからの情報を要求してデバイスに設定変更を加えるために使用する XML ベースのプロトコルです。YANG は主に、NETCONF 操作で使用される設定とステート データをモデル化するために使用されます。

Cisco IOS XE では、モデル ベースのインターフェイスは、既存のデバイス CLI、Syslog、および SNMP インターフェイスと相互運用します。必要に応じて、これらのインターフェイスは、ネットワーク デバイスからノースバウンドに公開されます。YANG は、RFC 6020 に基づいて各プロトコルをモデル化するために使用されます。

（注） 開発者に分かりやすい方法で Cisco YANG モデルにアクセスするには、*GitHub リポジトリ*を複製し、*vendor/cisco* サブディレクトリに移動します。ここでは、IOS XE、IOS-XR、および NX-OS プラットフォームのさまざまなリリースのモデルを使用できます。

NETCONF

NETCONF は、ネットワーク デバイスの設定をインストール、操作、削除するためのよりシンプルなメカニズムです。

コンフィギュレーション データとプロトコル メッセージに Extensible Markup Language（XML）ベースのデータ符号化を使用します。

NETCONF は、シンプルな RPC（リモート プロシージャ コール）ベースのメカニズムを使用してクライアントとサーバ間の通信を促進します。通常、クライアントはネットワーク マネージャの一部として実行されているスクリプトやアプリケーションです。通常、サーバはネットワーク デバイス（スイッチまたはルータ）です。サーバは、ネットワーク デバイス全体のトランスポート層としてセキュア シェル（SSH）を使用します。

NETCONF は、機能検出およびモデルのダウンロードもサポートしています。サポート対象のモデルは、*ietf-netconf-monitoring* モデルを使用して検出されます。各モデルに対する改定日付は、機能の応答に示されています。データ モデルは、*get-schema* rpc を使用したデバイスからのオプションのダウンロードに使用できます。これらの YANG モデルを使用して、データ モデルを理解したりエクスポートしたりできます。

詳細については、RFC 6241 を参照してください。

データ モデルの設定方法

NETCONF の設定

始める前に

次のように NETCONF-YANG を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**netconf-yang** 例： `Device (config)# netconf-yang`	ネットワーク デバイスで NETCONF インターフェイスを有効にします。 （注） CLI による最初のイネーブル化の後、ネットワーク デバイスをモデル ベースのインターフェイスを通じて管理できるようになります。モデル ベースのインターフェイス プロセスの完全なアクティベーションには、最大 90 秒かかることがあります。
ステップ 4	**exit** 例： `Device (config)# exit`	グローバル コンフィギュレーション モードを終了します。

NETCONF オプションの設定

SNMP の設定

NETCONF を有効にして、サポートされている MIB から生成された YANG モデルを使用して SNMP MIB データにアクセスしたり、IOS でサポートされている SNMP トラップを有効にして、サポートされているトラップから NETCONF 通知を受信するには、IOS で SNMP サーバを有効にします。

次の操作を行ってください。

手順

ステップ 1 IOS で SNMP 機能を有効にします。

例：

```
configure terminal
logging history debugging
logging snmp-trap emergencies
logging snmp-trap alerts
logging snmp-trap critical
logging snmp-trap errors
logging snmp-trap warnings
logging snmp-trap notifications
logging snmp-trap informational
logging snmp-trap debugging
!
snmp-server community public RW
snmp-server trap link ietf
snmp-server enable traps snmp authentication linkdown linkup snmp-server enable traps
syslog
snmp-server manager
exit
```

ステップ 2 NETCONF-YANG が起動した後、次の RPC <edit-config> メッセージを NETCONF-YANG ポートに送信して、SNMP トラップのサポートを有効にします。

例：

```
<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
  <edit-config>
    <target>
      <running/>
    </target>
    <config>
      <netconf-yang xmlns="http://cisco.com/yang/cisco-self-mgmt">
        <cisco-ia xmlns="http://cisco.com/yang/cisco-ia">
          <snmp-trap-control>
            <trap-list>
              <trap-oid>1.3.6.1.4.1.9.9.41.2.0.1</trap-oid>
            </trap-list>
            <trap-list>
              <trap-oid>1.3.6.1.6.3.1.1.5.3</trap-oid>
            </trap-list>
            <trap-list>
              <trap-oid>1.3.6.1.6.3.1.1.5.4</trap-oid>
```

```
            </trap-list>
          </snmp-trap-control>
        </cisco-ia>
      </netconf-yang>
    </config>
  </edit-config>
</rpc>
```

ステップ 3 次の RPC メッセージを NETCONF-YANG ポートに送信して、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

例：

```
<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
  <cisco-ia:save-config xmlns:cisco-ia="http://cisco.com/yang/cisco-ia"/>
</rpc>
```

データ モデルに関する追加情報

関連資料

関連項目	マニュアル タイトル
IOS-XE、IOS-XR、および NX-OS プラットフォームのさまざまなリリースの YANG データ モデル	開発者に分かりやすい方法で Cisco YANG モデルにアクセスするには、*GitHub リポジトリ*を複製し、*vendor/cisco* サブディレクトリに移動します。ここでは、IOS XE、IOS-XR、および NX-OS プラットフォームのさまざまなリリースのモデルを使用できます。

標準および RFC

標準/RFC	タイトル
RFC 6020	*YANG：Network Configuration Protocol*（*NETCONF*）向けデータ モデリング言語
RFC 6241	ネットワーク設定プロトコル（*NETCONF*）

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

データ モデルの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *221 :* データ モデルの機能情報

機能名	リリース	機能情報
データ モデル	Cisco IOS XE Denali 16.3.1	データ モデル機能によって、プログラムによる各種の標準規格に準拠した方法で、設定の記述やネットワーク デバイスからの運用データの読み取りが容易になります。 **netconf-yang** コマンドが導入されました。

第 168 章

プログラマビリティ：ネットワーク ブートローダ

次のプログラマビリティ機能は、Cisco IOS XE Denali 16.3.2 ではサポートされています。

- ネットワーク ブートローダ
- プラグアンドプレイ（PnP）エージェントの起動

- 機能情報の確認 （3411 ページ）
- プログラマビリティに関する情報 （3412 ページ）
- プログラマビリティの設定方法：ネットワーク ブートローダ （3415 ページ）
- プログラマビリティの設定例：ネットワーク ブートローダ （3416 ページ）
- プログラマビリティに関するその他の参考資料：ネットワーク ブートローダ （3416 ページ）
- プログラマビリティの機能情報：ネットワーク ブートローダ （3417 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

プログラマビリティに関する情報

ネットワーク ブートローダの概要

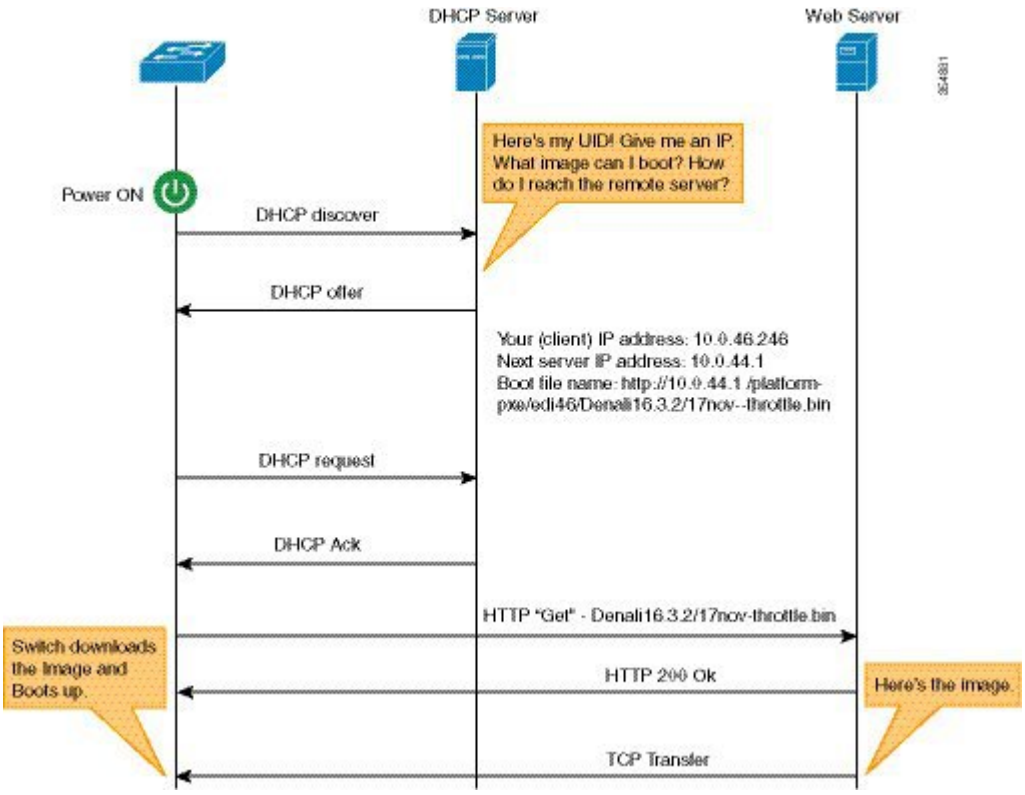
ネットワーク ブートローダは、ネットワーク ベースの送信元からのブート処理をサポートします。ブートローダは、HTTP、FTP、および TFTP サーバにあるイメージを起動します。ネットワーク ブート ソースは、iPXE のようなソリューションを使用して自動検出されます。

iPXE は、ブート前実行環境（PXE）のオープン ソース実装です。これにより、オフラインのデバイスのネットワーク ブートが有効になります。iPXE ブート モードのタイプには次の 3 つがあります。

- iPXE タイムアウト：IPXE_TIMEOUT ROMmon 変数を使用して、iPXE ネットワーク ブートのタイムアウトを秒単位で設定します。タイムアウトが経過すると、スイッチはデバイス ブートに戻ります。
- iPXE 期限なし：iPXE ネットワーク ブートを介して起動します。**bootipxeforever** コマンドが設定されている場合、スイッチは Dynamic Host Control Protocol（DHCP）要求を期限なしで送信します。これは iPXE のみのブートです（これについてもう少し詳しく説明お願いできますか）。
- デバイス：**bootipxe** コマンドを使用してデバイス ブートを設定します。デバイス ブートが設定された場合、設定されている IPXE_TIMEOUT ROMmon 変数は無視されます。

ここでは、iPXE ブートローダの動作について説明します。

図 *153 : iPXE* ブートローダのワークフロー



1. ブートローダが DHCP 要求を送信します。
2. DHCP 応答には、IP アドレスとのブート ファイル名が含まれています。ブート ファイル名は、ブート イメージが TFTP サーバ（tftp://server/filename）、FTP サーバ（ftp://userid:password@server/filename）、または HTTP サーバ（http://server/filename）から取得されることを示しています。現在の iPXE 実装は管理ポート（GigabitEthernet0/0）のみを経由して動作するため、前面パネル ポートを介して送信される DHCP 要求はサポートされていません。
3. ブートローダがネットワーク送信元からイメージをダウンロードして起動します。
4. DHCP 応答が受信されない場合、ブートローダはブートローダ設定に基づいて、DHCP 要求を期限なしで、または指定された期間の間送信し続けます。タイムアウトが発生すると、ブートローダはデバイスベースのブートに戻ります。設定されたブート モードが **ipxe-forever** である場合にのみ、スイッチは DHCP 要求を期限なしで送信します。**ipxe-timeout** ブート モード コマンドが設定されている場合、DHCP 要求は指定された時間の間送信され、タイムアウトが経過すると、スイッチはデバイス ブートに戻ります。

手動ブートが無効になっている場合、ブートローダは、設定された iPXE ROMMON 変数の値に基づいて、デバイス ブートを実行するかネットワーク ブートを実行するかを決定します。手動ブートが有効か無効かにかかわらず、ブートローダは BOOTMODE 変数を使用して、デバイス ブートとネットワーク ブートのどちらを実行するかを決定します。手動ブートとは、起動プロセスを開始するには、ユーザが手動で **boot manual switch** コマンドを入力する必要があ

ることを意味します。手動ブートが無効になっている場合に、スイッチをリロードすると、起動プロセスが自動的に開始されます。

iPXE が無効になっている場合は、デバイスの起動方法の決定に、既存の BOOT 変数のコンテンツが使用されます。BOOT 変数には、ネットワークベースの Uniform Resource Identifier（URI）（たとえば、http://、ftp://、tftp://）が含まれている場合があり、ネットワーク ブートが開始されます。しかし、ネットワーク イメージ パスの取得に DHCP は使用されません。デバイス IP アドレスは、IP_ADDR 変数から取得されます。BOOT 変数には、デバイスベースのパスが含まれている場合もあり、この場合は、デバイスベースのブートが開始されます。

起動目的でリモート DHCP サーバ上で UUT を識別するには、シャーシのシリアル番号（DHCP オプション 61 で使用可能）、製品 ID（PID）（DHCP オプション 60 で使用可能）、またはスイッチの MAC アドレスを使用します。**showinventory** および **showswitch** コマンドを使用した場合も、スイッチにこれらの値が表示されます。

次に、show inventory コマンドの出力例を示します。

```
Switch# show inventory

NAME:“c38xx Stack”, DESCR:“c38xx Stack”
PID:WS-3850-12X-48U-L, VID:V01 ,  SN: F0C1911V01A

NAME:“Switch 1”, DESCR:“WS-C3850-12X48U-L”
PID:WS-C3850-12X48U-L, VID:V01 , SN:F0C1911V01A

NAME:”Switch1 -Power Supply B”, DESCR:“Switch1 -Power Supply B”
PID:PWR-C1-1100WAC, VID:V01, SN:LIT1847146Q
```

次の ROMmon 変数が iPXE に設定されている必要があります。

- BOOTMODE = ipxe-forever | ipxe-timeout | device
- IPXE_TIMEOUT = seconds

プラグ アンド プレイ エージェントの概要

シスコ プラグ アンド プレイ（PnP）エージェントは、プラットフォームのブートストラップ エージェントとして動作します。デバイスベースのブートストラップ エージェントは、指定されたブートストラップ サーバで相互運用します。

プラットフォームのブートストラップ エージェントおよび PnP エージェントは、次の一般的な要件をサポートしています。

- オンプレミス、アウトオブバンド ブートストラップ：管理ポート経由の DHCP を使用します。
- オフプレミス、アウトオブバンドブートストラップ：管理ポート経由のクラウドベース接続を使用します。たとえば、DNS および Cisco PnP プロトコルの使用など。
- オフプレミス、インバンド ブートストラップ：データ ポート経由のクラウドベース接続を使用します。たとえば、DNS および Cisco PnP プロトコルの使用など。

プログラマビリティの設定方法：ネットワーク ブートローダ

ブートローダの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**boot ipxe** {**forever** | **timeout** *seconds*} *switch number* 例： `Switch(config)# boot ipxe forever switch 2`	IPXE-FOREVER として BOOTMODE ROMmon 変数を設定します。 • **timeout** キーワードを使用すると、ROMmon 変数の IPXE_TIMEOUT 値が秒単位で設定されます。
ステップ 4	**boot system** {**flash:** | **ftp:** | **http:** | **switch:**| **tftp:**} 例： `Switch(config)# boot system http:`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**end** 例： `Switch(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

プログラマビリティの設定例：ネットワーク ブートローダ

例：ブートローダの設定

次の例は、スイッチがイメージでブートされるまで、ブートローダが DHCP 要求を無期限に送信し続けることを示しています。

```
Switch# configure terminal
Switch(config)# boot ipxe forever switch 2
Switch(config)# boot system http: image-filename
Switch(config)# end
```

次に、ブートローダ構成に設定されたタイムアウトの例を示します。タイムアウトが発生すると、ブートローダはデバイスベースのブートに戻ります。

```
Switch# configure terminal
Switch(config)#  boot ipxe timeout 200 switch 2
Switch(config)# boot system ftp: image-filename
Switch(config)#end
```

プログラマビリティに関するその他の参考資料：ネットワーク ブートローダ

関連資料

関連項目	マニュアル タイトル
YANG データ モデル	*YANG データ モデルの設定*

標準および RFC

標準/RFC	Title
RFC 3986	*Uniform Resource Identifier (URI): Generic Syntax*

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

プログラマビリティの機能情報：ネットワーク ブートローダ

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *222*：プログラマビリティの機能情報：ネットワーク ブートローダ

機能名	リリース	機能情報
プログラマビリティ：ネットワーク ブートローダ	Cisco IOS XE Denali 16.3.2	ネットワーク ブートローダは、デバイス ベースまたはネットワーク ベースの送信元からのブート処理をサポートします。ネットワーク ブート ソースは、iPXE のようなソリューションを使用して自動的に検出される必要があります。
プログラマビリティ：プラグ アンド プレイ エージェント	Cisco IOS XE Denali 16.3.2	PnP エージェントは、プラットフォームのブートストラップ エージェントとして動作します。