Cisco IOS XE Denali 16.1.1（Catalyst 3650 スイッチ） ソフトウェアコンフィギュレーションガイド

初版：年 月 日

最終更新：年 月 日

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

Text Part Number:

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

© Cisco Systems, Inc. All rights reserved.

目 次

はじめに xcix

表記法 xcix

関連資料 ci

マニュアルの入手方法およびテクニカル サポート ci

コマンドライン インターフェイスの使用 1

コマンドライン インターフェイスの使用に関する情報 1

コマンド モード 1

コマンドの省略形 5

コマンドの no 形式および default 形式 5

CLI のエラー メッセージ 6

コンフィギュレーション ロギング 6

ヘルプ システムの使用 7

CLI を使用して機能を設定する方法 8

コマンド履歴の設定 8

コマンド履歴バッファ サイズの変更 8

コマンドの呼び出し 8

コマンド履歴機能の無効化 9

編集機能の有効化および無効化 10

キー入力によるコマンドの編集 10

画面幅よりも長いコマンドラインの編集 12

show および more コマンド出力の検索およびフィルタリング 13

スイッチ スタックでの CLI へのアクセス 14

コンソール接続または Telnet 経由での CLI へのアクセス 14

CleanAir 17

Cisco CleanAir の設定 19

機能情報の確認 19

CleanAir の前提条件 19
CleanAir の制約事項 20
CleanAir について 21
Cisco CleanAir のコンポーネント 22
Cisco CleanAir で使用される用語 23
Cisco CleanAir で検出できる干渉の種類 24
干渉デバイスのマージ 25
永続的デバイス 26
永続的デバイスの検出 26
永続的デバイスの回避 26
EDRRM および AQR の更新モード 26
CleanAir ハイ アベイラビリティ 27
CleanAir の設定方法 27
2.4 GHz 帯域の CleanAir のイネーブル化 27
2.4 GHz での電波品質とデバイスの CleanAir アラームの設定 28
2.4 GHz デバイスの干渉レポートの設定 30
5 GHz 帯域の CleanAir のイネーブル化 31
5 GHz での電波品質とデバイスの CleanAir アラームの設定 32
5 GHz デバイスの干渉レポートの設定 34
CleanAir-Events の EDRRM の設定 35
永続的デバイスの回避の設定 36
コントローラの GUI を使用した Cisco CleanAir の設定 37
Cisco Spectrum Expert の設定 37
Spectrum Expert の設定（CLI） 37
CleanAir パラメータのモニタリング 39
干渉デバイスのモニタリング 42
CleanAir の設定例 42
CleanAir に関する FAQ 43
その他の参考資料 45
インターフェイスおよびハードウェア コンポーネント 47
インターフェイス特性の設定 49
機能情報の確認 49

インターフェイス特性の設定に関する情報 49
インターフェイス タイプ 49
ポートベースの VLAN 50
スイッチ ポート 50
アクセス ポート 51
トランク ポート 51
トンネル ポート 52
ルーテッド ポート 52
スイッチ仮想インターフェイス 53
SVI 自動ステート除外 53
EtherChannel ポート グループ 54
Power over Ethernet（PoE）ポート 54
スイッチの USB ポートの使用 55
USB ミニタイプ B コンソール ポート 55
コンソール ポート変更ログ 55
インターフェイスの接続 56
イーサネット インターフェイスのデフォルト設定 56
インターフェイス速度およびデュプレックス モード 58
速度とデュプレックス モードの設定時の注意事項 58
IEEE 802.3x フロー制御 59
レイヤ 3 インターフェイス 60
インターフェイスの特性の設定方法 61
インターフェイスの設定 61
インターフェイスに関する記述の追加 62
インターフェイス範囲の設定 64
インターフェイス レンジ マクロの設定および使用方法 65
イーサネット インターフェイスの設定 67
インターフェイス速度およびデュプレックス パラメータの設定 67
IEEE 802.3x フロー制御の設定 69
レイヤ 3 インターフェイスの設定 71
論理レイヤ 3 GRE トンネル インターフェイスの設定 72
SVI 自動ステート除外の設定 74

インターフェイスのシャットダウンおよび再起動 75
コンソール メディア タイプの設定 77
USB 無活動タイムアウトの設定 78
インターフェイス特性のモニタ 79
インターフェイス ステータスのモニタ 79
インターフェイスおよびカウンタのクリアとリセット 81
インターフェイス特性の設定例 81
インターフェイスの説明の追加：例 81
インターフェイス範囲の設定：例 81
インターフェイス レンジ マクロの設定および使用方法：例 82
インターフェイス速度およびデュプレックス モードの設定：例 83
レイヤ 3 インターフェイスの設定：例 83
コンソール メディア タイプの設定：例 83
USB 無活動タイムアウトの設定：例 84
インターフェイス特性機能の追加情報 84
インターフェイス特性の設定の機能履歴と情報 85
Auto-MDIX の設定 87
Auto-MDIX の前提条件 87
Auto-MDIX の制約事項 88
Auto-MDIX の設定に関する情報 88
インターフェイスでの Auto-MDIX 88
Auto-MDIX の設定方法 89
インターフェイスでの Auto-MDIX の設定 89
Auto-MDIX の設定例 90
その他の参考資料 91
Auto-MDIX の機能履歴と情報 92
イーサネット管理ポートの設定 93
機能情報の確認 93
イーサネット管理ポートの前提条件 93
イーサネット管理ポートに関する情報 94
スイッチへのイーサネット管理ポートの直接接続 94
ハブを使用したスタック スイッチへのイーサネット管理ポートの接続 94

イーサネット管理ポートおよびルーティング 94
サポートされるイーサネット管理ポートの機能 95
イーサネット管理ポートの設定方法 96
イーサネット管理ポートのディセーブル化およびイネーブル化 96
その他の参考資料 97
イーサネット管理ポートの機能情報 99
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定 101
機能情報の確認 101
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要 102
LLDP 102
LLDP でサポートされる TLV 102
LLDP および Cisco スイッチ のスタック 102
LLDP-MED 103
LLDP-MED でサポートされる TLV 103
ワイヤード ロケーション サービス 104
デフォルトの LLDP 設定 105
LLDP に関する制約事項 106
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定方法 107
LLDP のイネーブル化 107
LLDP 特性の設定 108
LLDP-MED TLV の設定 111
Network-Policy TLV の設定 113
ロケーション TLV およびワイヤード ロケーション サービスの設定 115
スイッチ上でのワイヤード ロケーション サービスのイネーブル化 118
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定例 120
Network-Policy TLV の設定：例 120
LLDP、LLDP-MED、ワイヤード ロケーション サービスのモニタリングとメンテナンス 120
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの追加情報 122
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの機能情報 123
システム MTU の設定 125
システム MTU の設定 125
機能情報の確認 125

MTU に関する情報 125
システム MTU の制約事項 125
システム MTU 値の適用 126
システム MTU の設定 126
システム MTU の設定 126
Protocol-Specific MTU の設定 127
システム MTU の設定例 128
例：システム MTU の設定 128
例：プロトコル固有の MTU の設定 128
システム MTU に関する追加情報 129
システム MTU の機能情報 130
内部電源装置の設定 131
内部電源装置に関する情報 131
内部電源装置の設定方法 131
内部電源装置の設定 131
内部電源装置のモニタ 132
内部電源装置の設定例 133
その他の参考資料 134
内部電源装置の機能履歴と情報 135
PoE の設定 137
機能情報の確認 137
PoE について 137
Power over Ethernet（PoE）ポート 137
サポート対象のプロトコルおよび標準 138
受電装置の検出および初期電力割り当て 138
電力管理モード 140
電力モニタリングおよび電力ポリシング 141
電力消費値 142
Cisco Universal Power Over Ethernet 143
PoE の設定方法 143
PoE ポートの電力管理モードの設定 143
シグナル/スペア ペアの電力のイネーブル化 145

電力ポリシングの設定 146
電力ステータスのモニタ 150
その他の参考資料 150
PoE の機能情報 151
EEE の設定 153
機能情報の確認 153
EEE について 154
EEE の概要 154
デフォルトの EEE 設定 154
EEE の制約事項 154
EEE の設定方法 154
EEE のイネーブル化またはディセーブル化 155
EEE のモニタリング 156
EEE の設定例 156
その他の参考資料 157
EEE 設定の機能履歴と情報 158
IPv6 159
MLD スヌーピングの設定 161
機能情報の確認 161
IPv6 MLD スヌーピングの設定に関する情報 161
MLD スヌーピングの概要 162
MLD メッセージ 163
MLD クエリー 163
マルチキャスト クライアント エージングの堅牢性 164
マルチキャスト ルータ検出 164
MLD レポート 165
MLD Done メッセージおよび即時脱退 165
トポロジ変更通知処理 166
IPv6 MLD スヌーピングの設定方法 166
MLD スヌーピングのデフォルト設定 166
MLD スヌーピング設定時の注意事項 167

スイッチでの MLD スヌーピングのイネーブル化またはディセーブル化（CLI） 168
VLAN での MLD スヌーピングのイネーブル化またはディセーブル化（CLI） 169
スタティック マルチキャスト グループの設定（CLI） 170
マルチキャスト ルータ ポートの設定（CLI） 171
MLD 即時脱退の有効化（CLI） 172
MLD スヌーピング クエリーの設定（CLI） 173
MLD リスナー メッセージ抑制の無効化（CLI） 175
MLD スヌーピング情報の表示 175
MLD スヌーピングの設定例 177
スタティックなマルチキャスト グループの設定：例 177
マルチキャスト ルータ ポートの設定：例 177
MLD 即時脱退のイネーブル化：例 177
MLD スヌーピング クエリーの設定：例 177
IPv6 ユニキャスト ルーティングの設定 179
機能情報の確認 179
IPv6 ユニキャスト ルーティングの設定について 179
IPv6 の概要 180
IPv6 Addresses 180
サポート対象の IPv6 ユニキャスト ルーティング機能 181
128 ビット幅のユニキャスト アドレス 181
IPv6 の DNS 181
IPv6 ユニキャストのパス MTU ディスカバリ 181
ICMPv6 182
ネイバー探索 182
DRP 182
IPv6 のステートレス自動設定および重複アドレス検出 182
IPv6 アプリケーション 183
DHCP for IPv6 アドレスの割り当て 183
IPv6 のスタティック ルート 183
RIP for IPv6 183
OSPF for IPv6 184

IPv6 の HSRP の設定 184
EIGRP IPv6 184
EIGRPv6 スタブ ルーティング 184
IPv6 によるSNMP と Syslog 185
IPv6 上の HTTP（S） 186
サポートされていない IPv6 ユニキャスト ルーティング機能 186
IPv6 機能の制限 187
IPv6 とスイッチ スタック 187
IPv6 のデフォルト設定 188
IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化（CLI） 188
IPv4 および IPv6 プロトコル スタックの設定（CLI） 192
デフォルト ルータ プリファレンスの設定（CLI） 195
IPv6 ICMP レート制限の設定（CLI） 196
IPv6 の CEF および dCEF の設定 197
IPv6 のスタティック ルーティングの設定（CLI） 198
RIP for IPv6 の設定（CLI） 200
OSPF for IPv6 の設定（CLI） 202
IPv6 の EIGRP の設定 205
IPv6 ユニキャスト リバース パス転送の設定 205
IPv6 の表示 206
DHCP for IPv6 アドレス割り当ての設定 207
DHCPv6 アドレス割り当てのデフォルト設定 207
DHCPv6 アドレス割り当ての設定時の注意事項 207
DHCPv6 サーバ機能のイネーブル化（CLI） 208
DHCPv6 クライアント機能のイネーブル化（CLI） 210
IPv6 ユニキャスト ルーティングの設定例 212
IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化：例 212
デフォルト ルータ プリファレンスの設定：例 212
IPv4 および IPv6 プロトコル スタックの設定：例 212
DHCPv6 サーバ機能のイネーブル化：例 213
DHCPv6 クライアント機能のイネーブル化：例 213
IPv6 ICMP レート制限の設定：例 214

IPv6 のスタティック ルーティングの設定：例 214
IPv6 の RIP の設定：例 214
IPv6 の表示：例 214
IPv6 マルチキャストの実装 215
機能情報の確認 215
IPv6 マルチキャスト ルーティングの実装に関する情報 215
IPv6 マルチキャストの概要 215
IPv6 マルチキャスト ルーティングの実装 216
IPv6 マルチキャスト リスナー ディスカバリ プロトコル 217
マルチキャスト クエリアとマルチキャスト ホスト 217
MLD アクセス グループ 217
受信側の明示的トラッキング 217
プロトコル独立マルチキャスト 218
PIM スパース モード 218
IPv6 BSR：RP マッピングの設定 219
PIM 送信元固有マルチキャスト 219
ルーティング可能アドレスの hello オプション 220
PIM IPv6 スタブ ルーティング 220
スタティック mroute 221
MRIB 222
MFIB 222
MFIB 222
IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング 223
IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 224
IPv6 マルチキャストの実装 224
IPv6 マルチキャスト ルーティングのイネーブル化 224
MLD プロトコルのカスタマイズおよび確認 225
インターフェイスでの MLD のカスタマイズおよび確認 225
MLD グループ制限の実装 227
MLD グループ制限のグローバルな実装 227
MLD グループ制限のインターフェイス単位での実装 228
受信側の明示的トラッキングによってホストの動作を追跡するための設定 229

MLD トラフィック カウンタのリセット 230
MLD インターフェイス カウンタのクリア 230
PIM の設定 231
PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示 231
PIM オプションの設定 232
PIM トラフィック カウンタのリセット 234
PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット 234
PIM IPv6 スタブ ルーティングの設定 236
PIM IPv6 スタブ ルーティングの設定時の注意事項 236
IPv6 PIM ルーティングのデフォルト設定 236
IPv6 PIM スタブ ルーティングのイネーブル化 237
IPv6 PIM スタブ ルーティングのモニタ 240
BSR の設定 240
BSR の設定および BSR 情報の確認 240
BSR への PIM RP アドバタイズメントの送信 241
限定スコープ ゾーン内で BSR を使用できるようにするための設定 242
BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定 243
SSM マッピングの設定 244
スタティック mroute の設定 245
IPv6 マルチキャストでの MFIB の使用 246
IPv6 マルチキャストでの MFIB の動作の確認 246
MFIB トラフィック カウンタのリセット 247
IPv6 クライアント IP アドレス ラーニングの設定 249
IPv6 クライアント アドレス ラーニングの前提条件 250
IPv6 クライアント アドレス ラーニングについて 250
SLAAC アドレス割り当て 250
ステートフル DHCPv6 アドレス割り当て 252
静的 IP アドレス割り当て 253
ルータ要求 253
Router Advertisement 253
ネイバー探索 254

ネイバー探索抑制 254
RA Guard 254
RA スロットリング 255
IPv6 ユニキャストの設定（CLI） 256
RA ガード ポリシーの設定（CLI） 257
RA ガード ポリシーの適用（CLI） 258
RA スロットル ポリシーの設定（CLI） 259
VLAN への RA スロットル ポリシーの適用（CLI） 260
IPv6 スヌーピングの設定（CLI） 261
IPv6 ND 抑制ポリシーの設定（CLI） 262
VLAN/PortChannel での IPv6 スヌーピングの設定 263
Switch での IPv6 の設定（CLI） 265
DHCP プールの設定（CLI） 266
DHCP を使用しないステートレス自動アドレス設定の設定（CLI） 267
DHCP によるステートレス自動アドレス設定の設定（CLI） 268
ステートフル DHCP のローカルな設定（CLI） 269
ステートフル DHCP の外部的設定（CLI） 272
IPv6 アドレス ラーニング設定の確認 274
その他の参考資料 275
IPv6 クライアント アドレス ラーニングの機能情報 276
IPv6 WLAN セキュリティの設定 277
IPv6 WLAN セキュリティの前提条件 277
IPv6 WLAN セキュリティの制限 277
IPv6 WLAN セキュリティについて 278
IPv6 WLAN セキュリティの設定方法 281
ローカル認証の設定 281
ローカル ユーザの作成 281
クライアント VLAN とインターフェイスの作成 282
EAP プロファイルの設定 283
ローカル認証モデルの作成 286
クライアント WLAN の作成 287
WPA2+AES でのローカル認証の設定 289

WPA2+AES 用クライアント VLAN の作成 291
WPA2+AES 用 WLAN の作成 292
外部 RADIUS サーバの設定 294
RADIUS 認証サーバ ホストの設定 294
RADIUS 認証サーバ グループの設定 295
クライアント VLAN の作成 297
外部 RADIUS サーバを使用した 802.1x WLAN の作成 298
その他の参考資料 300
IPv6 WLAN セキュリティの機能情報 301
IPv6 ACL の設定 303
IPv6 ACL の前提条件 303
IPv6 ACL の制限 303
IPv6 ACL について 304
IPv6 ACL の概要 304
ACL のタイプ 306
ユーザあたりの IPv6 ACL 306
フィルタ ID IPv6 ACL 306
ダウンロード可能 IPv6 ACL 306
IPv6 ACL とスイッチ スタック 306
IPv6 ACL の設定 307
IPv6 ACL のデフォルト設定 308
他の機能およびスイッチとの相互作用 308
IPv6 ACL の設定方法 308
IPv6 ACL の作成 308
インターフェイスへの IPv6 の適用 313
WLAN IPv6 ACL の作成 314
IPv6 ACL の確認 315
IPv6 ACL の表示 315
IPv6 ACL の設定例 316
例：IPv6 ACL の作成 316
例：IPv6 ACL の適用 316
例：IPv6 ACL の表示 317

例：RA スロットリングと NS 抑制の設定 317
例：RA ガード ポリシーの設定 319
例：IPv6 ネイバー バインディングの設定 320
その他の参考資料 321
IPv6 ACL の機能情報 322
IPv6 Web 認証の設定 323
IPv6 Web 認証の前提条件 323
IPv6 Web 認証の制限 323
IPv6 Web 認証について 324
Web 認証プロセス 324
IPv6 Web 認証の設定方法 325
WPA のディセーブル化 325
WLAN のセキュリティのイネーブル化 327
WLAN のパラメータ マップのイネーブル化 327
WLAN の認証リストのイネーブル化 328
グローバル Web 認証 WLAN パラメータ マップの設定 328
WLAN の設定 329
グローバル コンフィギュレーション モードの IPv6 のイネーブル化 331
IPv6 Web 認証の確認 332
パラメータ マップの確認 332
認証リストの確認 332
その他の参考資料 333
IPv6 Web 認証の機能情報 334
IPv6 クライアント モビリティの設定 337
IPv6 クライアント モビリティの前提条件 337
IPv6 クライアント モビリティの制限 337
IPv6 クライアント モビリティについて 338
ルータ アドバタイズメントの使用 339
RA スロットリングと NS 抑制 340
IPv6 アドレス ラーニング 340
複数の IP アドレスの処理 341
IPv6 Configuration 341

ハイ アベイラビリティ 341
IPv6 クライアント モビリティの確認 342
IPv6 クライアント モビリティのモニタリング 343
その他の参考資料 343
IPv6 クライアント モビリティの機能情報 344
IPv6 モビリティの設定 347
IPv6 モビリティの前提条件 347
IPv6 モビリティについて 347
コントローラ間ローミング 348
スティッキアンカリングでのサブネット内ローミング、およびサブネット間ローミング 348
IPv6 モビリティの設定方法 348
IPv6 モビリティのモニタリング 348
その他の参考資料 350
IPv6 モビリティの機能情報 352
IP 353
HSRP の設定 355
HSRP の設定 355
機能情報の確認 355
HSRP の設定に関する情報 355
HSRP の概要 355
HSRP のバージョン 357
MHSRP 358
SSO HSRP 359
HSRP およびスイッチ スタック 359
IPv6 の HSRP の設定 360
HSRP の設定方法 360
HSRP のデフォルト設定 360
HSRP HSRP 設定時の注意事項 361
HSRP のイネーブル化 361
HSRP のプライオリティの設定 363
MHSRP の設定 366
ルータ A の設定 367

ルータ B の設定 371
HSRP 認証およびタイマーの設定 375
ICMP リダイレクト メッセージの HSRP サポートのイネーブル化 377
HSRP グループおよびクラスタリングの設定 377
HSRP の確認 377
HSRP コンフィギュレーションの確認 377
HSRP の設定例 378
HSRP のイネーブル化：例 378
HSRP のプライオリティの設定：例 378
MHSRP の設定：例 378
HSRP 認証およびタイマーの設定：例 379
HSRP グループおよびクラスタリングの設定：例 379
HSRP の設定に関する追加情報 379
HSRP の設定に関する機能情報 381
レイヤ 2/3 383
スパニングツリー プロトコルの設定 385
機能情報の確認 385
STP の制約事項 385
スパニング ツリー プロトコルに関する情報 386
スパニングツリー プロトコル 386
スパニングツリー トポロジと BPDU 387
ブリッジ ID、デバイス プライオリティ、および拡張システム ID 389
ポート プライオリティとパス コスト 390
スパニングツリー インターフェイス ステート 391
ブロッキング ステート 393
リスニング ステート 393
ラーニング ステート 393
フォワーディング ステート 393
ディセーブル ステート 394
スイッチまたはポートがルート スイッチまたはルート ポートになる仕組み 394
スパニングツリーおよび冗長接続 395

スパニングツリー アドレスの管理 395
接続を維持するためのエージング タイムの短縮 396
スパニングツリー モードおよびプロトコル 396
サポートされるスパニングツリー インスタンス 397
スパニングツリーの相互運用性と下位互換性 397
STP および IEEE 802.1Q トランク 398
VLAN ブリッジ スパニングツリー 399
スパニング ツリーとスイッチ スタック 399
スパニングツリー機能のデフォルト設定 400
スパニングツリー機能の設定方法 401
スパニングツリー モードの変更（CLI） 401
スパニング ツリーのディセーブル化（CLI） 402
ルート スイッチの設定（CLI） 403
セカンダリ ルート デバイスの設定（CLI） 405
ポート プライオリティの設定（CLI） 407
パス コストの設定（CLI） 408
VLAN のデバイス プライオリティの設定（CLI） 410
hello タイムの設定（CLI） 411
VLAN の転送遅延時間の設定（CLI） 412
VLAN の最大エージング タイムの設定（CLI） 413
転送保留カウントの設定（CLI） 414
スパニングツリー ステータスのモニタリング 415
スパニング ツリー プロトコルに関する追加情報 416
STP の機能情報 417
複数のスパニング ツリー プロトコルの設定 419
機能情報の確認 419
MSTP の前提条件 419
MSTP の制約事項 420
MSTP について 421
MSTP の設定 421
MSTP 設定時の注意事項 422
ルート スイッチ 423

MST リージョン 424
IST、CIST、CST 424
MST リージョン内の動作 425
MST リージョン間の動作 426
IEEE 802.1s の用語 426
MST リージョンの図 427
ホップ カウント 428
境界ポート 429
IEEE 802.1s の実装 430
ポートの役割名の変更 430
レガシーおよび規格スイッチの相互運用 430
単一方向リンク障害の検出 431
MSTP およびスイッチ スタック 432
IEEE 802.1D STP との相互運用性 432
RSTP 概要 432
ポートの役割およびアクティブ トポロジ 432
高速コンバージェンス 434
ポート ロールの同期 435
ブリッジ プロトコル データ ユニットの形式および処理 436
優位 BPDU 情報の処理 437
下位 BPDU 情報の処理 437
トポロジの変更 437
プロトコル移行プロセス 438
MSTP のデフォルト設定 439
MSTP 機能の設定方法 440
MST リージョン設定の指定と MSTP のイネーブル化（CLI） 440
ルート スイッチの設定（CLI） 443
セカンダリ ルート スイッチの設定（CLI） 444
ポート プライオリティの設定（CLI） 446
パス コストの設定（CLI） 448
スイッチ プライオリティの設定（CLI） 449
hello タイムの設定（CLI） 451

転送遅延時間の設定（CLI） 452
最大エージング タイムの設定（CLI） 454
最大ホップ カウントの設定（CLI） 455
高速移行を確実にするためのリンク タイプの指定（CLI） 456
ネイバー タイプの設定（CLI） 457
プロトコルの移行プロセスの再開（CLI） 459
MSTP に関する追加情報 460
MSTP の機能情報 461
オプションのスパニングツリー機能の設定 463
オプションのスパニングツリー機能について 463
PortFast 463
BPDU ガード 464
BPDU フィルタリング 465
UplinkFast 465
クロススタック UplinkFast 468
クロススタック UplinkFast の動作 468
高速コンバージェンスを発生させるイベント 470
BackboneFast 471
EtherChannel ガード 473
ルート ガード 474
ループ ガード 475
オプションのスパニングツリー機能の設定方法 475
PortFast のイネーブル化（CLI） 475
BPDU ガードのイネーブル化（CLI） 477
BPDU フィルタリングのイネーブル化（CLI） 479
冗長リンクで使用するための UplinkFast のイネーブル化（CLI） 481
UplinkFast のディセーブル化（CLI） 483
BackboneFast をイネーブル化（CLI） 484
EtherChannel ガードのイネーブル化（CLI） 485
ルート ガードのイネーブル化（CLI） 486
ループ ガードのイネーブル化（CLI） 488
スパニングツリー ステータスのモニタリング 490
オプションのスパニング ツリー機能に関する追加情報 490

オプションのスパニングツリー機能の機能情報 491

EtherChannel の設定 493

機能情報の確認 493

EtherChannel の制約事項 493

EtherChannel について 494

EtherChannel の概要 494

EtherChannel のモード 495

スイッチ上の EtherChannel 496

EtherChannel リンクのフェールオーバー 497

チャネル グループおよびポートチャネル インターフェイス 497

Port Aggregation Protocol; ポート集約プロトコル 499

PAgP モード 499

サイレント モード 500

PAgP 学習方式およびプライオリティ 501

PAgP と他の機能との相互作用 502

Link Aggregation Control Protocol 502

LACP モード 503

LACP とリンクの冗長性 504

LACP と他の機能との相互作用 504

EtherChannel の On モード 504

ロードバランシングおよび転送方式 505

MAC アドレス転送 505

IP アドレス転送 506

ロードバランシングの利点 506

EtherChannel およびスイッチ スタック 508

スイッチ スタックおよび PAgP 508

スイッチ スタックおよび LACP 508

EtherChannel のデフォルト設定 508

EtherChannel 設定時の注意事項 510

レイヤ 2 EtherChannel 設定時の注意事項 512

レイヤ 3 EtherChannel 設定時の注意事項 513

EtherChannel の設定方法 513

レイヤ 2 EtherChannel の設定 （CLI） 513

レイヤ 3 EtherChannel の設定 （CLI） 516

EtherChannel ロードバランシングの設定（CLI） 518

EtherChannel 拡張ロードバランシングの設定（CLI） 520

PAgP 学習方式およびプライオリティの設定 （CLI） 521

LACP ホット スタンバイ ポートの設定 523

LACP 最大バンドル機能の設定（CLI） 523

LACP ポート チャネルの最小リンク機能の設定（CLI） 524

LACP システム プライオリティの設定（CLI） 526

LACP ポート プライオリティの設定（CLI） 527

EtherChannel、PAgP、および LACP ステータスのモニタ 529

EtherChannel の設定例 530

レイヤ 2 EtherChannel の設定：例 530

レイヤ 3 EtherChannel の設定：例 531

LACP ホット スタンバイ ポートの設定：例 531

EtherChannels の追加リファレンス 532

EtherChannels の機能情報 533

単方向リンク検出の設定 535

機能情報の確認 535

UDLD 設定の制約事項 535

UDLD について 536

動作モード 536

通常モード 536

アグレッシブ モード 537

単一方向の検出方法 537

ネイバー データベース メンテナンス 538

イベントドリブン検出およびエコー 538

UDLD リセット オプション 538

UDLD のデフォルト設定 539

UDLD の設定方法 540

UDLD のグローバルなイネーブル化（CLI） 540

インターフェイスでの UDLD のイネーブル化（CLI） 541

UDLD のモニタおよびメンテナンス 543
UDLD の追加リファレンス 543
UDLD の機能情報 544
Lightweight アクセス ポイント 545
アクセス ポイント ディスカバリ用のスイッチの設定 547
機能情報の確認 547
アクセス ポイント ディスカバリ用のスイッチの設定の前提条件 547
アクセス ポイント ディスカバリ用のスイッチの設定の制約事項 548
アクセス ポイント ディスカバリ用のスイッチの設定に関する情報 549
アクセス ポイント通信プロトコル 549
アクセス ポイントの join 情報の表示 549
アクセス ポイント接続プロセスのトラブルシューティング 549
アクセス ポイント ディスカバリの設定方法 551
アクセス ポイントの Syslog サーバの設定（GUI） 551
アクセス ポイントの Syslog サーバの設定（CLI） 551
アクセス ポイントの join 情報のモニタリング（CLI） 552
アクセス ポイント ディスカバリ用のスイッチの設定例 553
すべてのアクセス ポイントの MAC アドレスの表示：例 553
Lightweight Cisco Aironet アクセス ポイントの DHCP オプション 43 の設定例 554
AP パス スルーの設定方法 554
AP パススルーについて 554
AP のパススルーの設定 555
データ暗号化の設定 557
機能情報の確認 557
データ暗号化を設定するための前提条件 557
データ暗号化の設定に関する制約事項 558
データの暗号化について 558
データ暗号化の設定方法 558
データ暗号化の設定（CLI） 558
データ暗号化の設定例 559
すべてのアクセス ポイントのデータ暗号化の状態の表示：例 559

再送信間隔および再試行回数の設定 561
機能情報の確認 561
アクセス ポイントの再送信間隔と再試行回数の設定の前提条件 561
再送信間隔および再試行回数について 562
アクセス ポイントの再送信間隔と再試行回数の設定方法 562
アクセス ポイントの再送信間隔と再試行回数の設定（CLI） 562
CAPWAP の最大伝送単位情報の表示（CLI） 563
アクセス ポイントの再送信間隔と再試行回数の設定例 564
CAPWAP 再送信の詳細の表示：例 564
最大伝送単位情報の表示：例 564
適応型ワイヤレス侵入防御システムの設定 565
機能情報の確認 565
wIPS 設定の前提条件 565
アクセス ポイントでの wIPS の設定方法 566
アクセス ポイントでの wIPS の設定（CLI） 566
wIPS 情報のモニタリング 567
アクセス ポイントでの wIPS の設定例 569
モニタ設定チャネル セットの表示：例 569
wIPS 情報の表示：例 569
アクセス ポイントの認証の設定 571
機能情報の確認 571
アクセス ポイントの認証を設定するための前提条件 571
アクセス ポイントの認証を設定する際の制限 572
アクセス ポイントに対する認証の設定について 572
アクセス ポイントの認証の設定方法 573
アクセス ポイントのグローバル資格情報の設定（CLI） 573
アクセス ポイントのグローバル資格情報の設定（GUI） 574
アクセス ポイントの認証の設定（CLI） 576
認証のスイッチの設定（CLI） 578
アクセス ポイントの認証の設定例 580
アクセス ポイントの認証設定の表示：例 580
自律アクセス ポイントの Lightweight モードへの変換 581

機能情報の確認 581
Lightweight モードに自律アクセス ポイントを変換するための前提条件 582
Lightweight モードに変換される Autonomous アクセス ポイントについて 582
Lightweight モードから Autonomous モードへの復帰 582
DHCP オプション 43 および DHCP オプション 60 の使用 582
変換したアクセス ポイントがクラッシュ情報をスイッチに送信する方法 583
変換したアクセス ポイントからのメモリ コア ダンプのアップロード 583
変換されたアクセス ポイントの MAC アドレスの表示 583
Lightweight アクセス ポイントの静的 IP アドレスの設定 583
Lightweight アクセス ポイントの Autonomous アクセス ポイントへの再変換方法 584
Lightweight アクセス ポイントを Autonomous モードに戻す方法（CLI） 584
モード ボタンと TFTP サーバを使用して Lightweight アクセス ポイントを Autonomous モードに戻す方法 585
アクセス ポイントの認可（CLI） 585
変換したアクセス ポイントでの Reset ボタンのディセーブル化（CLI） 587
AP クラッシュ ログ情報のモニタリング 588
アクセス ポイントでの固定 IP アドレスの設定方法 589
アクセス ポイントでの固定 IP アドレスの設定（CLI） 589
TFTP リカバリ手順を使用したアクセス ポイントのリカバリ 591
Autonomous アクセス ポイントを Lightweight モードに変換する場合の設定例 591
アクセス ポイントの IP アドレス設定の表示：例 591
アクセス ポイントのクラッシュ ファイル情報の表示：例 591
Cisco ワークグループ ブリッジの使用 593
機能情報の確認 593
Cisco ワークグループ ブリッジと Cisco 以外のワークグループ ブリッジについて 593
ワークグループ ブリッジ状態のモニタリング 594
WGB の問題のデバッグ（CLI） 595
ワークグループ ブリッジの設定例 596
WGB の設定：例 596
プローブ要求フォワーディングの設定 599

機能情報の確認 599
プローブ要求フォワーディングの設定について 599
プローブ要求フォワーディングの設定方法（CLI） 599
RFID トラッキングの最適化 601
機能情報の確認 601
アクセス ポイントでの RFID トラッキングの最適化 601
アクセス ポイントでの RFID トラッキングの最適化方法 602
アクセス ポイントでの RFID トラッキングの最適化（CLI） 602
RFID トラッキングの最適化の設定例 603
モニタ モードでのすべてのアクセス ポイントの表示：例 603
国番号の設定 605
機能情報の確認 605
国番号の設定に関する前提条件 605
国番号の設定について 606
国番号の設定方法（CLI） 607
国番号の設定例 609
国番号のチャネル リストの表示：例 609
リンク遅延の設定 611
機能情報の確認 611
リンク遅延を設定するための前提条件 611
リンク遅延を設定する際の制限 612
リンク遅延の設定について 612
TCP MSS 612
リンク テスト 612
リンク遅延の設定方法 614
リンク遅延の設定（CLI） 614
TCP MSS の設定方法 616
TCP MSS の設定（CLI） 616
リンク テストの実行（CLI） 617
リンク遅延の設定例 618
リンク テストの実行：例 618
リンク遅延情報の表示：例 618

TCP MSS 設定の表示：例 619
Power over Ethernet の設定 621
機能情報の確認 621
Power over Ethernet の設定について 621
Power over Ethernet の設定方法 622
Power over Ethernet の設定（CLI） 622
Power over Ethernet の設定例 623
Power over Ethernet 情報の表示：例 623
Mobility 625
モビリティについて 627
概要 627
有線およびワイヤレス モビリティ 628
モビリティの機能 628
低遅延ローミングを実現するスティッキ アンカリング 630
ブリッジ ドメイン ID および L2/L3 ローミング 631
リンク ダウンの動作 631
モビリティ コントローラのプラットフォーム固有のスケール要件 631
モビリティ ネットワーク要素 633
Mobility Agent 633
モビリティ コントローラ 634
Mobility Oracle 635
ゲスト コントローラ 636
モビリティ制御プロトコル 637
モビリティ制御プロトコルについて 637
最初のアソシエーションとローミング 637
最初のアソシエーション 638
スイッチ内のハンドオフ 640
スイッチ ピア グループ内のハンドオフ 640
スイッチ ピア グループ間のハンドオフ 641
サブ ドメイン間のハンドオフ 642
モビリティ グループ間のハンドオフ 643
モビリティの設定 645
モビリティ コントローラの設定 645

統合アクセス コントローラの設定 645
ピア グループ、ピア グループ メンバー、ブリッジ ドメイン ID の作成（CLI） 645
ローカル モビリティ グループの設定（CLI） 647
ピア モビリティ グループの追加（CLI） 648
ローミング動作のオプション パラメータの設定 649
モビリティ コントローラの Mobility Oracle への指定（CLI） 650
ゲスト コントローラの設定 650
ゲスト アンカーの設定 652
モビリティ エージェントの設定 653
モビリティ コントローラの指定によるモビリティ エージェントの設定（CLI） 653
モビリティ エージェントのモビリティ コントローラの設定（CLI） 654
モビリティ エージェントへのモビリティ コントローラ ロールの追加 654
モビリティ エージェントのオプション パラメータの設定（CLI） 655
モビリティ エージェントを管理するモビリティ コントローラ 656
概要 656
機能制限 658
MA を管理する MC の設定（GUI） 659
例 659
MA を管理する MC の設定（CLI） 660
例 663
Network Management 669
Cisco IOS Configuration Engine の設定 671
機能情報の確認 671
Configuration Engine を設定するための前提条件 671
Configuration Engine の設定に関する制約事項 672
Configuration Engine の設定について 672
Cisco Configuration Engine ソフトウェア 672
コンフィギュレーション サービス 673
イベント サービス 674
ネームスペース マッパー 674

Cisco Networking Service ID およびデバイスのホスト名 674
ConfigID 675
DeviceID 675
ホスト名および DeviceID 675
ホスト名、DeviceID、および ConfigID 676
Cisco IOS CNS エージェント 676
初期設定 676
差分（部分的）設定 677
コンフィギュレーションの同期 678
自動 CNS 設定 678
Configuration Engine の設定方法 679
CNS イベント エージェントのイネーブル化 679
Cisco IOS CNS エージェントのイネーブル化 681
Cisco IOS CNS エージェントの初期設定のイネーブル化 683
DeviceID の更新 689
Cisco IOS CNS エージェントの部分的設定のイネーブル化 691
CNS 設定のモニタリング 693
その他の参考資料 694
Cisco Discovery Protocol の設定 697
機能情報の確認 697
CDP に関する情報 697
CDP の概要 697
CDP のデフォルト設定 698
CDP の設定方法 699
CDP 特性の設定 699
CDP のディセーブル化 701
Enabling CDP 702
インターフェイス上での CDP のディセーブル化 704
インターフェイス上での CDP のイネーブル化 705
CDP のモニタおよびメンテナンス 707
その他の参考資料 708
簡易ネットワーク管理プロトコルの設定 711
機能情報の確認 711

SNMP の前提条件 712
SNMP の制約事項 714
SNMP に関する情報 715
SNMP の概要 715
SNMP マネージャ機能 715
SNMP エージェント機能 716
SNMP コミュニティ ストリング 716
SNMP MIB 変数アクセス 717
SNMP 通知 717
SNMP ifIndex MIB オブジェクト値 718
SNMP のデフォルト設定 718
SNMP 設定時の注意事項 718
SNMP の設定方法 719
SNMP エージェントのディセーブル化 719
コミュニティ ストリングの設定 721
SNMP グループおよびユーザの設定 724
SNMP 通知の設定 730
エージェント コンタクトおよびロケーションの設定 737
SNMP を通して使用する TFTP サーバの制限 738
SNMP のトラップフラグの設定 740
SNMP ワイヤレス トラップ通知のイネーブル化 742
SNMP ステータスのモニタリング 744
SNMP の例 745
その他の参考資料 746
簡易ネットワーク管理プロトコルの機能の履歴と情報 747
サービス レベル契約の設定 749
機能情報の確認 749
SLA の制約事項 750
SLA について 750
Cisco IOS IP サービス レベル契約（SLA） 750
Cisco IOS IP SLA でのネットワーク パフォーマンスの測定 751
IP SLA レスポンダおよび IP SLA 制御プロトコル 752

IP SLA の応答時間の計算 753
IP SLA 動作のスケジューリング 754
IP SLA 動作のしきい値のモニタリング 754
UDP ジッター 755
IP SLA 動作の設定方法 756
デフォルト設定 756
設定時の注意事項 756
IP SLA レスポンダの設定 757
IP SLA ネットワーク パフォーマンス測定の実装 759
UDP ジッター動作を使用した IP サービス レベルの分析 763
ICMP エコー動作を使用した IP サービス レベルの分析 767
IP SLA 動作のモニタリング 770
IP SLA 動作のモニタリングの例 771
その他の参考資料 772
ローカル ポリシーの設定 775
機能情報の確認 775
ローカル ポリシーの設定に関する制限 775
ローカル ポリシーの設定に関する情報 776
ローカル ポリシーの設定方法 778
ローカル ポリシーの設定（CLI） 778
インターフェイス テンプレートの作成（CLI） 778
パラメータ マップの作成（CLI） 779
クラス マップの作成（CLI） 780
ポリシー マップの作成（CLI） 781
WLAN 上のデバイスのローカル ポリシーの適用（CLI） 782
ローカル ポリシーの監視 784
例：ローカル ポリシーの設定 785
ローカル ポリシーの設定に関する追加情報 786
ローカル ポリシーの設定の実行に関する機能履歴 787
SPAN および RSPAN の設定 789
機能情報の確認 789
SPAN および RSPAN の前提条件 790

SPAN および RSPAN の制約事項 790
SPAN および RSPAN について 792
SPAN および RSPAN 792
ローカル SPAN 792
リモート SPAN 794
SPAN と RSPAN の概念および用語 795
SPAN セッション 795
モニタ対象トラフィック 796
送信元ポート 798
送信元 VLAN 798
VLAN フィルタリング 799
宛先ポート 799
RSPAN VLAN 800
SPAN および RSPAN と他の機能の相互作用 801
SPAN と RSPAN とデバイス スタック 802
フローベースの SPAN 803
SPAN および RSPAN のデフォルト設定 804
設定時の注意事項 804
SPAN 設定時の注意事項 804
RSPAN 設定時の注意事項 804
FSPAN および FRSPAN 設定時の注意事項 805
SPAN および RSPAN の設定方法 806
ローカル SPAN セッションの作成 806
ローカル SPAN セッションの作成および着信トラフィックの設定 809
フィルタリングする VLAN の指定 811
RSPAN VLAN としての VLAN の設定 814
RSPAN 送信元セッションの作成 816
フィルタリングする VLAN の指定 818
RSPAN 宛先セッションの作成 821
RSPAN 宛先セッションの作成および着信トラフィックの設定 823
FSPAN セッションの設定 826
FRSPAN セッションの設定 829

SPAN および RSPAN 動作のモニタリング 833
SPAN および RSPAN の設定例 833
例：ローカル SPAN の設定 833
例：RSPAN VLAN の作成 835
その他の参考資料 836
SPAN および RSPAN の機能の履歴と情報 837
パケット キャプチャの設定 839
機能情報の確認 839
パケット キャプチャの前提条件 839
パケット キャプチャの前提条件 839
パケット キャプチャの制約事項 840
パケット キャプチャの制約事項 840
パケット キャプチャの概要 843
パケット キャプチャ ツールの概要 843
Wireshark について 844
Wireshark の概要 844
キャプチャ ポイント 844
接続ポイント 845
Filters 846
Actions 847
キャプチャ パケットのメモリ内のバッファへのストレージ 847
.pcap ファイルにキャプチャされたパケットのストレージ 847
パケットのデコードおよび表示 848
パケットのストレージおよび表示 849
Wireshark キャプチャ ポイントのアクティブ化および非アクティブ化 849
Wireshark 機能 850
Wireshark のガイドライン 852
デフォルトの Wireshark の設定 855
Embedded Packet Capture について 855
Embedded Packet Capture の概要 855
組み込みパケット キャプチャの利点 856
パケット データ キャプチャ 856
パケット キャプチャの設定 857

Wireshark の設定方法 857
キャプチャ ポイントの定義 857
キャプチャ ポイント パラメータの追加または変更 862
キャプチャ ポイント パラメータの削除 865
キャプチャ ポイントの削除 867
キャプチャ ポイントをアクティブまたは非アクティブにする 868
キャプチャ ポイント バッファのクリア 872
Embedded Packet Capture の実装方法 874
パケット データ キャプチャの管理 874
キャプチャされたデータのモニタリングとメンテナンス 876
パケット キャプチャのモニタリング 878
Wireshark の設定例 878
例：.pcap ファイルからの概要出力の表示 878
例：.pcap ファイルからの詳細出力の表示 879
例：.pcap ファイルからパケット ダンプ出力の表示 880
例：表示フィルタを使用した .pcap ファイルからのパケットの表示 880
例: .pcap ファイルにキャプチャされたパケットの数を表示 881
例：.pcap ファイルから単一パケット ダンプの表示 881
例: .pcap ファイルにキャプチャされたパケットの統計情報を表示 881
例：単純なキャプチャおよび表示 881
例：単純なキャプチャおよび保存 883
例：バッファのキャプチャの使用 885
例：出方向のパケットの簡単なキャプチャおよび保存 891
組み込みパケット キャプチャの設定例 893
例：パケット データ キャプチャの管理 893
例：キャプチャされたデータのモニタリングおよびメンテナンス 893
その他の参考資料 895
QoS 897
QoS の設定 899
機能情報の確認 899
QoS の前提条件 900
QoS コンポーネント 900

QoS の用語 901
QoS の概要 901
QoS の概要 901
モジュラ QoS コマンドライン インターフェイス 902
ワイヤレス QoS の概要 902
ワイヤレス用の QoS および IPv6 903
有線およびワイヤレス アクセスでサポートされる機能 903
ワイヤレス ターゲットでサポートされる QoS 機能 905
ポート ポリシー 907
ポート ポリシーの形式 907
無線ポリシー 909
SSID ポリシー 910
クライアント ポリシー 910
階層型 QoS 911
階層型ワイヤレス QoS 912
ワイヤレス パケット形式 913
階層型 AFD 913
QoS の実装 913
レイヤ 2 フレームのプライオリティ ビット 914
レイヤ 3 パケットのプライオリティ ビット 915
分類を使用したエンドツーエンドの QoS ソリューション 915
パケット分類 915
パケットと合わせて伝搬される情報に基づく分類 916
レイヤ 3 またはレイヤ 4 ヘッダーに基づく分類 916
レイヤ 2 ヘッダーに基づく分類 917
デバイス固有の情報に基づく分類（QoS グループ） 917
階層型分類 918
QoS 有線モデル 918
入力ポートのアクティビティ 918
出力ポートのアクティビティ 919
分類 919
アクセス コントロール リスト 919

クラス マップ 920
ポリシー マップ 920
物理ポートのポリシー マップ 921
VLAN のポリシー マップ 922
ワイヤレス QoS マルチキャスト 922
ポリシング 922
トークンバケット アルゴリズム 923
マーキング 923
パケット ヘッダーのマーキング 924
スイッチ固有の情報のマーキング 924
テーブル マップのマーキング 924
トラフィックの調整 926
ポリシング 927
シングルレート 2 カラー ポリシング 927
デュアルレート 3 カラー ポリシング 928
シェーピング 928
クラスベース トラフィック シェーピング 929
平均レート シェーピング 929
階層型シェーピング 929
キューイングおよびスケジューリング 930
帯域幅 930
帯域幅の割合 930
帯域幅余剰比率 930
重み付けテール ドロップ 931
重み付けテール ドロップのデフォルト値 932
プライオリティ キュー 932
キュー バッファ 933
キュー バッファの割り当て 934
ダイナミックなしきい値および拡張 934
ワイヤレスでのキューイング 935
信頼動作 935
有線およびワイヤレス ポートの信頼動作 935

Cisco IP Phone の信頼境界機能のポート セキュリティ 937
ワイヤレス QoS モビリティ 938
スイッチ間ローミング 938
スイッチ内ローミング 939
ワイヤレス QoS の貴金属ポリシー 939
標準 QoS のデフォルト設定 940
デフォルトの有線 QoS 設定 940
DSCP マップ 940
デフォルトの CoS/DSCP マップ 940
デフォルトの IP Precedence/DSCP マップ 940
デフォルトの DSCP/CoS マップ 941
デフォルトのワイヤレス QoS 設定 942
QoS ポリシーのガイドライン 942
有線ターゲットの QoS に関する制約事項 942
ワイヤレス ターゲットの QoS に関する制約事項 945
QoS の設定方法 949
クラス、ポリシー、およびテーブル マップの設定 949
トラフィック クラスの作成（CLI） 949
トラフィック ポリシーの作成（CLI） 952
クライアント ポリシーの設定 957
クラスベースのパケット マーキングの設定（CLI） 958
音声およびビデオに対するクラス マップの設定（CLI） 963
トラフィック ポリシーのインターフェイスへの付加（CLI） 964
WLAN での SSID またはクライアント ポリシーの適用（CLI） 966
ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング（CLI） 968
ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング（CLI） 972
テーブル マップの設定（CLI） 975
信頼の設定 978
ワイヤレス トラフィックの信頼動作の設定（CLI） 978
QoS の特性と機能の設定 979

コール アドミッション制御の設定（CLI） 979
帯域幅の設定（CLI） 987
ポリシングの設定（CLI） 989
プライオリティの設定（CLI） 992
キューとシェーピングの設定 995
出力キューの特性の設定 995
キュー バッファの設定（CLI） 995
キュー制限の設定（CLI） 998
シェーピングの設定（CLI） 1001
貴金属ポリシーの設定（CLI） 1002
QoS のモニタリング 1004
QoS の設定例 1008
例：アクセス コントロール リストによる分類 1008
例：サービス クラス レイヤ 2 の分類 1008
例：サービス クラス DSCP の分類 1009
例：VLAN ID レイヤ 2 の分類 1009
例：DSCP 値または precedence 値による分類 1009
例：階層型分類 1010
例：階層型ポリシーの設定 1010
例：音声およびビデオの分類 1011
例：音声、ビデオ、およびマルチキャスト トラフィックで分類されたワイヤレス QoS ポリシー 1013
例：ダウンストリーム SSID ポリシーの設定 1013
例：入力 SSID ポリシー 1014
例：クライアント ポリシー 1015
例：平均レート シェーピングの設定 1018
例：キュー制限の設定 1019
例：キュー バッファの設定 1020
例：ポリシング アクションの設定 1020
例：ポリサーの VLAN 設定 1021
例：ポリシングの単位 1021
例：シングルレート 2 カラー ポリシング設定 1022

例：デュアルレート 3 カラー ポリシング設定 1023
例：テーブル マップのマーキング設定 1023
例：CoS マーキングを保持するテーブル マップの設定 1024
次の作業 1025
QoS に関する追加情報 1025
QoS の機能履歴と情報 1026
無線リソース管理 1029
無線リソース管理の設定 1031
機能情報の確認 1031
無線リソース管理の設定の前提条件 1031
無線リソース管理の制約事項 1032
無線リソース管理について 1032
無線リソースの監視 1033
RF グループについて 1033
RF グループ リーダー 1034
RF Group Name 1036
モビリティ コントローラ 1036
Mobility Agent 1037
RF グループ内の不正アクセス ポイント検出について 1037
送信電力の制御 1037
最小/最大送信電力の設定による TPC アルゴリズムの無効化 1038
チャネルの動的割り当て 1038
カバレッジ ホールの検出と修正 1040
RRM の設定方法 1041
高度な RRM CCX パラメータの設定（CLI） 1041
ネイバー探索タイプの設定（CLI） 1042
RRM プロファイルしきい値、監視チャネル、および監視間隔の設定（GUI） 1042
RF グループの設定 1044
RF グループ モードの設定（GUI） 1044
RF グループ選択モードの設定（CLI） 1045
RF グループ名の設定（CLI） 1046
RF グループ名の設定（GUI） 1047

802.11 静的 RF グループのメンバの設定（CLI） 1047
送信電力制御の設定 1048
送信電力制御のしきい値の設定（CLI） 1048
送信電力レベルの設定（CLI） 1048
送信電力制御の設定（GUI） 1049
802.11 RRM パラメータの設定 1051
高度な 802.11 チャネル割り当てパラメータの設定（CLI） 1051
動的チャネル割り当ての設定（GUI） 1053
802.11 カバレッジ ホール検出の設定（CLI） 1055
カバレッジ ホールの検出の設定（GUI） 1057
802.11 イベント ロギングの設定（CLI） 1058
802.11 統計情報の監視の設定（CLI） 1059
802.11 パフォーマンス プロファイルの設定（CLI） 1061
RF グループ内の不正アクセス ポイント検出の設定 1062
RF グループ内の不正アクセス ポイント検出の設定（CLI） 1062
RF グループ内の不正アクセス ポイント検出の有効化（GUI） 1064
RRM パラメータと RF グループ ステータスの監視 1065
RRM パラメータの監視 1065
RF グループ ステータスの監視（CLI） 1066
RF グループ ステータスの監視（GUI） 1067
例：RF グループの設定 1067
ED-RRM に関する情報 1068
Cisco ワイヤレス LAN コントローラで ED-RRM の設定（CLI） 1068
ED-RRM の設定（GUI） 1069
無線リソース管理に関するその他の参考ドキュメント 1069
無線リソース管理の設定を行うための機能履歴と情報 1070
設定の最適化されたローミング 1071
ローミングの最適化に関する情報 1071
ローミングの最適化の制約事項 1072
ローミングの最適化の設定（GUI） 1072
ローミングの最適化の設定（CLI） 1073
設定の Rx SOP 1075

Rx-SOP に関する情報 1075
Rx SOP の設定（GUI） 1075
Rx SOP の設定（CLI） 1076
Routing 1077
MSDP の設定 1079
機能情報の確認 1079
MSDP の設定について 1079
MSDP の概要 1080
MSDP の動作 1080
MSDP の利点 1082
MSDP の設定方法 1082
MSDP のデフォルト設定 1082
デフォルトの MSDP ピアの設定 1082
SA ステートのキャッシング 1084
MSDP ピアからの送信元情報の要求 1086
スイッチから発信される送信元情報の制御 1087
送信元の再配信 1088
SA 要求メッセージのフィルタリング 1090
スイッチで転送される送信元情報の制御 1092
フィルタの使用法 1092
SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限 1094
スイッチで受信される送信元情報の制御 1095
MSDP メッシュ グループの設定 1098
MSDP ピアのシャットダウン 1099
境界 PIM デンス モード領域の MSDP への包含 1100
RP アドレス以外の発信元アドレスの設定 1102
MSDP のモニタリングおよびメンテナンス 1103
MSDP の設定例 1105
デフォルト MSDP ピアの設定：例 1105
SA ステートのキャッシング：例 1105
MSDP ピアからの送信元情報の要求：例 1105

スイッチから発信される送信元情報の制御：例 1105
スイッチから転送される送信元情報の制御：例 1106
スイッチで受信される送信元情報の制御：例 1106
IP ユニキャスト ルーティングの設定 1107
機能情報の確認 1108
IP ユニキャスト ルーティングの設定に関する情報 1108
IP ルーティングに関する情報 1109
ルーティング タイプ 1109
IP ルーティングおよびスイッチ スタック 1110
クラスレス ルーティング 1112
アドレス解決 1114
プロキシ ARP 1115
ICMP Router Discovery Protocol 1115
UDP ブロードキャスト パケットおよびプロトコル 1115
ブロードキャスト パケットの処理 1116
IP ブロードキャストのフラッディング 1116
IP ルーティングの設定方法 1117
IP アドレッシングの設定方法 1118
IP アドレス指定のデフォルト設定 1119
ネットワーク インターフェイスへの IP アドレスの割り当て 1120
サブネット ゼロの使用 1122
クラスレス ルーティングのディセーブル化 1123
アドレス解決方法の設定 1124
スタティック ARP キャッシュの定義 1124
ARP のカプセル化の設定 1126
プロキシ ARP のイネーブル化 1128
IP ルーティングがディセーブルの場合のルーティング支援機能 1129
プロキシ ARP 1129
デフォルト ゲートウェイ 1129
ICMP Router Discovery Protocol（IRDP） 1130
ブロードキャスト パケットの処理方法の設定 1133

ダイレクトブロードキャストから物理ブロードキャストへの変換のイネーブル化 1133
UDP ブロードキャスト パケットおよびプロトコルの転送 1135
IP ブロードキャスト アドレスの確立 1136
IP ブロードキャストのフラッディング 1138
IP アドレスのモニタリングおよびメンテナンス 1139
IP ユニキャスト ルーティングの設定方法 1140
IP ユニキャスト ルーティングのイネーブル化 1140
IP ルーティングのイネーブル化の例 1141
次の作業 1142
RIP 情報 1142
サマリー アドレスおよびスプリット ホライズン 1143
RIP の設定方法 1143
RIP のデフォルト設定 1143
基本的な RIP パラメータの設定 1144
RIP 認証の設定 1147
サマリー アドレスおよびスプリット ホライズンの設定 1148
スプリット ホライズンの設定 1150
サマリー アドレスおよびスプリット ホライズンの設定例 1151
OSPF に関する情報 1152
OSPF NSF 1153
OSPF NSF 認識 1153
OSPF NSF 対応 1153
OSPF エリア パラメータ 1154
その他の OSPF パラメータ 1154
LSA グループ ペーシング 1155
ループバック インターフェイス 1156
OSPF の設定方法 1156
OSPF のデフォルト設定 1156
基本的な OSPF パラメータの設定 1158
OSPF インターフェイスの設定 1159
OSPF エリア パラメータの設定 1162

その他の OSPF パラメータの設定 1164
LSA グループ ペーシングの変更 1166
ループバック インターフェイスの設定 1167
OSPF のモニタリング 1168
OSPF の設定例 1169
例：基本的な OSPF パラメータの設定 1169
EIGRP に関する情報 1169
EIGRP の機能 1170
EIGRP コンポーネント 1170
EIGRP NSF 1171
EIGRP NSF 認識 1171
EIGRP NSF 対応 1172
EIGRP スタブ ルーティング 1172
EIGRP の設定方法 1174
EIGRP のデフォルト設定 1174
基本的な EIGRP パラメータの設定 1176
EIGRP インターフェイスの設定 1177
EIGRP ルート認証の設定 1179
EIGRP のモニタリングおよびメンテナンス 1181
BGP に関する情報 1182
BGP ネットワーク トポロジ 1182
NSF 認識 1184
BGP ルーティングに関する情報 1184
ルーティング ポリシーの変更 1185
BGP 判断属性 1186
ルート マップ 1187
BGP フィルタリング 1187
BGP フィルタリングのプレフィックス リスト 1188
BGP コミュニティ フィルタリング 1188
BGP ネイバーおよびピア グループ 1189
集約ルート 1189
ルーティング ドメイン コンフェデレーション 1189

BGP ルート リフレクタ 1190
ルート ダンプニング 1190
BGP の追加情報 1191
BGP の設定方法 1191
BGP のデフォルト設定 1191
BGP ルーティングのイネーブル化 1195
ルーティング ポリシー変更の管理 1197
BGP 判断属性の設定 1198
ルート マップによる BGP フィルタリングの設定 1201
ネイバーによる BGP フィルタリングの設定 1202
アクセス リストおよびネイバーによる BGP フィルタリングの設定 1203
BGP フィルタリング用のプレフィックス リストの設定 1205
BGP コミュニティ フィルタリングの設定 1206
BGP ネイバーおよびピア グループの設定 1208
ルーティング テーブルでの集約アドレスの設定 1211
ルーティング ドメイン連合の設定 1213
BGP ルート リフレクタの設定 1214
ルート ダンプニングの設定 1215
BGP のモニタリングおよびメンテナンス 1217
BGP の設定例 1218
例：ルータでの BGP の設定 1218
ISO CLNS ルーティングに関する情報 1219
コネクションレス型ルーティング 1219
IS-IS ダイナミック ルーティング 1220
NSF 認識 1221
IS-IS グローバル パラメータ 1221
IS-IS インターフェイス パラメータ 1222
ISO CLNS ルーティングの設定方法 1223
IS-IS のデフォルト設定 1223
IS-IS ルーティングのイネーブル化 1224
IS-IS グローバル パラメータの設定 1227
IS-IS インターフェイス パラメータの設定 1230

ISO IGRP と IS-IS のモニタリングおよびメンテナンス 1233
ISO CLNS ルーティングの設定例 1235
例：IS-IS ルーティングの設定 1235
Multi-VRF CE に関する情報 1236
Multi-VRF CE の概要 1237
ネットワーク トポロジ 1238
パケット転送処理 1238
ネットワーク コンポーネント 1239
VRF 認識サービス 1239
Multi-VRF CE の設定方法 1240
Multi-VRF CE のデフォルト設定 1240
Multi-VRF CE の設定時の注意事項 1241
VRF の設定 1244
VRF 認識サービスの設定 1245
ARP 用 VRF 認識サービスの設定 1246
ping 用 VRF 認識サービスの設定 1246
SNMP 用 VRF 認識サービスの設定 1246
uRPF 用 VRF 認識サービスの設定 1248
VRF 認識 RADIUS の設定 1249
syslog 用 VRF 認識サービスの設定 1249
traceroute 用 VRF 認識サービスの設定 1250
FTP および TFTP 用 VRF 認識サービスの設定 1251
マルチキャスト VRF の設定 1252
VPN ルーティング セッションの設定 1254
BGP PE/CE ルーティング セッションの設定 1256
Multi-VRF CE のモニタリング 1257
Multi-VRF CE の設定例 1258
Multi-VRF CE の設定例 1258
ユニキャスト リバース パス転送の設定 1261
プロトコル独立機能 1262
分散型シスコ エクスプレス フォワーディング 1262
シスコ エクスプレス フォワーディングに関する情報 1262

シスコ エクスプレス フォワーディングの設定方法 1263
等コスト ルーティング パスの個数 1265
等コスト ルーティング パスに関する情報 1265
等コスト ルーティング パスの設定方法 1266
スタティック ユニキャスト ルート 1266
スタティック ユニキャスト ルートに関する情報 1266
スタティック ユニキャスト ルートの設定 1268
デフォルトのルートおよびネットワーク 1269
デフォルトのルートおよびネットワークに関する情報 1269
デフォルトのルートおよびネットワークの設定方法 1270
ルーティング情報を再配信するためのルート マップ 1270
ルート マップの概要 1270
ルート マップの設定方法 1271
ルート配信の制御方法 1275
Policy-Based Routing：ポリシーベース ルーティング 1277
ポリシーベース ルーティングの概要 1277
PBR の設定方法 1278
ルーティング情報のフィルタリング 1282
受動インターフェイスの設定 1282
ルーティング アップデートのアドバタイズおよび処理の制御 1284
ルーティング情報の送信元のフィルタリング 1285
認証キーの管理 1286
前提条件 1286
認証キーの設定方法 1286
IP ネットワークのモニタリングおよびメンテナンス 1288
セキュリティ 1289
不正アクセスの防止 1291
機能情報の確認 1291
不正アクセスの防止 1291
パスワードおよび権限レベルによるスイッチ アクセスの制御 1293
機能情報の確認 1293
パスワードおよび権限によるスイッチ アクセスの制御の制約事項 1293

パスワードおよび権限レベルに関する情報 1294
デフォルトのパスワードおよび権限レベル設定 1294
追加のパスワード セキュリティ 1294
パスワードの回復 1295
端末回線の Telnet 設定 1296
ユーザ名とパスワードのペア 1296
権限レベル 1296
パスワードおよび権限レベルでスイッチ アクセスを制御する方法 1297
スタティック イネーブル パスワードの設定または変更 1297
暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 1299
パスワード回復のディセーブル化 1301
端末回線に対する Telnet パスワードの設定 1302
ユーザ名とパスワードのペアの設定 1304
コマンドの特権レベルの設定 1307
回線のデフォルト特権レベルの変更 1308
権限レベルへのログインおよび終了 1310
スイッチ アクセスのモニタリング 1311
パスワードおよび権限レベルの設定例 1311
例：スタティック イネーブル パスワードの設定または変更 1311
例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 1311
例：端末回線に対する Telnet パスワードの設定 1311
例：コマンドの権限レベルの設定 1312
その他の参考資料 1312
TACACS+ の設定 1315
機能情報の確認 1315
TACACS+ の前提条件 1315
TACACS+ の概要 1317
TACACS+ およびスイッチ アクセス 1317
TACACS+ の概要 1317
TACACS+ の動作 1319
方式リスト 1320

TACACS+ 設定オプション 1320
TACACS+ ログイン認証 1320
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可 1321
TACACS+ アカウンティング 1321
TACACS+ のデフォルト設定 1321
TACACS+ を設定する方法 1322
TACACS+ サーバ ホストの指定および認証キーの設定 1322
TACACS+ ログイン認証の設定 1324
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定 1327
TACACS+ アカウンティングの起動 1328
AAA サーバが到達不能な場合のルータとのセッションの確立 1330
TACACS+ のモニタリング 1331
RADIUS の設定 1333
機能情報の確認 1333
RADIUS を設定するための前提条件 1333
RADIUS の設定に関する制約事項 1334
RADIUS に関する情報 1335
RADIUS およびスイッチ アクセス 1335
RADIUS の概要 1335
RADIUS の動作 1336
RADIUS 許可の変更 1337
Change-of-Authorization 要求 1339
RFC 5176 規定 1339
CoA 要求応答コード 1340
セッションの識別 1341
CoA ACK 応答コード 1342
CoA NAK 応答コード 1342
CoA 要求コマンド 1342
セッション再認証 1342
スイッチ スタックでのセッションの再認証 1343
セッションの終了 1343

CoA 接続解除要求 1343
CoA 要求：ホスト ポートのディセーブル化 1344
CoA 要求：バウンス ポート 1344
セッション強制終了のスタック構成ガイドライン 1345
CoA 要求バウンス ポートのスタック構成 ガイドライン 1345
CoA 要求ディセーブル ポートのスタック構成 ガイドライン 1345
RADIUS のデフォルト設定 1346
RADIUS サーバ ホスト 1346
RADIUS ログイン認証 1347
AAA サーバ グループ 1347
AAA 許可 1348
RADIUS アカウンティング 1348
ベンダー固有の RADIUS 属性 1348
ベンダー独自仕様の RADIUS サーバ通信 1364
RADIUS の設定方法 1365
RADIUS サーバ ホストの識別 1365
RADIUS ログイン認証の設定 1367
AAA サーバ グループの定義 1370
ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定 1372
RADIUS アカウンティングの起動 1374
すべての RADIUS サーバの設定 1376
ベンダー固有の RADIUS 属性を使用するスイッチ設定 1378
ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定 1379
スイッチ上での CoA の設定 1381
CoA 機能のモニタリング 1384
その他の参考資料 1385
Kerberos の設定 1387
機能情報の確認 1387
Kerberos によるスイッチ アクセスの制御の前提条件 1387
Kerberos に関する情報 1388
Kerberos とスイッチ アクセス 1388

Kerberos の概要 1388
Kerberos の動作 1391
境界スイッチに対する認証の取得 1392
KDC からの TGT の取得 1392
ネットワーク サービスに対する認証の取得 1392
Kerberos を設定する方法 1393
Kerberos 設定のモニタリング 1393
その他の参考資料 1393
ローカル認証および許可の設定 1395
機能情報の確認 1395
ローカル認証および許可の設定方法 1395
スイッチのローカル認証および許可の設定 1395
ローカル認証および許可のモニタリング 1398
その他の参考資料 1399
セキュア シェル（SSH）の設定 1401
機能情報の確認 1401
セキュア シェルを設定するための前提条件 1401
セキュア シェルの設定に関する制約事項 1402
SSH に関する情報 1403
SSH およびスイッチ アクセス 1403
SSH サーバ、統合クライアント、およびサポートされているバージョン 1403
SSH 設定時の注意事項 1404
セキュア コピー プロトコルの概要 1405
Secure Copy Protocol（SCP） 1405
SSH の設定方法 1405
SSH を実行するためのスイッチの設定 1405
SSH サーバの設定 1407
SSH の設定およびステータスのモニタリング 1410
その他の参考資料 1410
SSH 認証の X.509v3 証明書 1413
SSH 認証の X.509v3 証明書 1413
機能情報の確認 1413

SSH 認証の X.509v3 証明書 の前提条件 1413
SSH 認証の X.509v3 証明書 の制約事項 1414
SSH 認証の X.509v3 証明書について 1414
デジタル証明書 1414
X.509v3 を使用したサーバとユーザの認証 1414
SSH 認証の X.509v3 証明書の設定方法 1415
サーバ認証用のデジタル証明書を使用する IOS SSH サーバの設定 1415
ユーザ認証用のユーザのデジタル証明書を検証する IOS SSH サーバの設定 1416
サーバの設定と、デジタル証明書を使用したユーザ認証の確認 1418
SSH 認証の X.509v3 証明書の設定例 1419
例：サーバ認証用のデジタル証明書を使用する IOS SSH サーバの設定 1419
例：ユーザ認証のためのユーザのデジタル証明書を検証する IOS SSH サーバの設定 1419
SSH 認証の X.509v3 証明書に関する追加情報 1419
SSH 認証の X.509v3 証明書 の機能情報 1421
Secure Socket Layer HTTP の設定 1423
機能情報の確認 1423
Secure Sockets Layer（SSL）HTTP に関する情報 1423
セキュア HTTP サーバおよびクライアントの概要 1423
CA のトラストポイント 1424
CipherSuite 1425
SSL のデフォルト設定 1426
SSL の設定時の注意事項 1427
セキュア HTTP サーバおよびクライアントの設定方法 1427
CA のトラストポイントの設定 1427
セキュア HTTP サーバの設定 1429
セキュア HTTP クライアントの設定 1432
セキュア HTTP サーバおよびクライアントのステータスのモニタリング 1434
その他の参考資料 1434
IPv4 ACL の設定 1437
機能情報の確認 1437

IPv4 アクセス コントロール リストを設定するための前提条件 1437
IPv4 アクセス コントロール リストの設定に関する制約事項 1438
ACL によるネットワーク セキュリティに関する情報 1439
ACL の概要 1439
アクセス コントロール エントリ 1440
ACL でサポートされるタイプ 1440
サポートされる ACL 1440
ACL 優先順位 1441
ポート ACL 1442
ルータ ACL 1443
VLAN マップ 1443
ACE およびフラグメント化されるトラフィックとフラグメント化されていないトラフィック 1444
ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例 1445
ACL とスイッチ スタック 1445
アクティブ スイッチおよび ACL の機能 1446
スタック メンバおよび ACL の機能 1446
アクティブ スイッチの障害および ACL 1446
標準 IPv4 ACL および拡張 IPv4 ACL 1446
IPv4 ACL スイッチでサポートされていない機能 1447
アクセス リスト番号 1447
番号付き標準 IPv4 ACL 1448
番号付き拡張 IPv4 ACL 1448
名前付き IPv4 ACL 1449
ACL ロギング 1450
ハードウェアおよびソフトウェアによる IP ACL の処理 1450
VLAN マップの設定時の注意事項 1450
VLAN マップとルータ ACL 1451
VLAN マップとルータ ACL の設定時の注意事項 1452
ACL の時間範囲 1452
IPv4 ACL のインターフェイスに関する注意事項 1453

ACL の設定方法 1454
IPv4 ACL の設定 1454
番号付き標準 ACL の作成 1454
番号付き拡張 ACL の作成 1456
名前付き標準 ACL の作成 1460
名前付き拡張 ACL の作成 1462
ACL の時間範囲の設定 1464
端末回線への IPv4 ACL の適用 1466
インターフェイスへの IPv4 ACL の適用 1467
名前付き MAC 拡張 ACL の作成 1469
レイヤ 2 インターフェイスへの MAC ACL の適用 1471
VLAN マップの設定 1473
VLAN マップの作成 1475
VLAN への VLAN マップの適用 1476
IPv4 ACL のモニタリング 1478
ACL の設定例 1479
例：ACL での時間範囲を使用 1479
例：ACL へのコメントの挿入 1479
IPv4 ACL の設定例 1480
小規模ネットワークが構築されたオフィス用の ACL 1480
例：小規模ネットワークが構築されたオフィスの ACL 1481
例：番号付き ACL 1482
例：拡張 ACL 1482
例：名前付き ACL 1483
例：IP ACL に適用される時間範囲 1484
例：コメント付き IP ACL エントリの設定 1484
例：ACL ロギング 1485
ACL および VLAN マップの設定例 1486
例：パケットを拒否する ACL および VLAN マップの作成 1486
例：パケットを許可する ACL および VLAN マップの作成 1486
例：IP パケットのドロップおよび MAC パケットの転送のデフォルト アクション 1487

例：MAC パケットのドロップおよび IP パケットの転送のデフォルト アクション 1487
例：すべてのパケットをドロップするデフォルト アクション 1488
ネットワークでの VLAN マップの使用方法の設定例 1488
例：ワイヤリング クローゼットの設定 1488
例：別の VLAN にあるサーバへのアクセスの制限 1490
例：別の VLAN にあるサーバへのアクセスの拒否 1490
VLAN に適用されるルータ ACL と VLAN マップの設定例 1491
例：ACL およびスイッチド パケット 1491
例：ACL およびブリッジド パケット 1492
例：ACL およびルーテッド パケット 1492
例：ACL およびマルチキャスト パケット 1493
その他の参考資料 1494
IPv6 ACL の設定 1497
機能情報の確認 1497
IPv6 ACL の概要 1497
スイッチ スタックおよび IPv6 ACL 1498
他の機能およびスイッチとの相互作用 1498
IPv6 ACL の制限 1499
IPv6 ACL のデフォルト設定 1500
IPv6 ACL の設定 1500
インターフェイスへの IPv6 ACL の付加 1504
IPv6 ACL のモニタリング 1506
その他の参考資料 1507
DHCP の設定 1509
機能情報の確認 1509
DHCP に関する情報 1509
DHCP サーバ 1509
DHCP リレー エージェント 1510
DHCP スヌーピング 1510
Option 82 データ挿入 1512
Cisco IOS DHCP サーバ データベース 1515

DHCP スヌーピング バインディング データベース 1515
DHCP スヌーピングおよびスイッチ スタック 1517
DHCP 機能の設定方法 1517
DHCP スヌーピングのデフォルト設定 1517
DHCP スヌーピング設定時の注意事項 1518
DHCP サーバの設定 1519
DHCP サーバとスイッチ スタック 1519
DHCP リレー エージェントの設定 1519
パケット転送アドレスの指定 1521
DHCP スヌーピングおよび Option 82 を設定するための前提条件 1523
DHCP スヌーピングおよび Option 82 のイネーブル化 1525
Cisco IOS DHCP サーバ データベースのイネーブル化 1528
DHCP スヌーピング情報のモニタリング 1528
DHCP サーバ ポートベースのアドレス割り当ての設定 1529
DHCP サーバ ポートベースのアドレス割り当ての設定の概要 1529
ポートベースのアドレス テーブルのデフォルト設定 1529
ポートベースのアドレス割り当て設定時の注意事項 1529
DHCP スヌーピング バインディング データベース エージェントのイネーブル化 1530
DHCP サーバ ポートベースのアドレス割り当てのイネーブル化 1532
DHCP サーバ ポートベースのアドレス割り当てのモニタリング 1534
その他の参考資料 1535
IP ソース ガードの設定 1537
機能情報の確認 1537
IP ソース ガードの概要 1538
IP ソース ガード 1538
スタティック ホスト用 IP ソース ガード 1538
IP ソース ガードの設定時の注意事項 1539
IP ソース ガードの設定方法 1540
IP ソース ガードのイネーブル化 1540
レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定 1542
IP ソース ガードのモニタリング 1544

その他の参考資料 1545
ダイナミック ARP インスペクションの設定 1547
機能情報の確認 1547
ダイナミック ARP インスペクションの制約事項 1548
ダイナミック ARP インスペクションの概要 1549
インターフェイスの信頼状態とネットワーク セキュリティ 1551
ARP パケットのレート制限 1553
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ 1553
廃棄パケットのロギング 1553
ダイナミック ARP インスペクションのデフォルト設定 1554
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ 1554
非 DHCP 環境での ARP ACL の設定 1555
DHCP 環境でのダイナミック ARP インスペクションの設定 1558
着信 ARP パケットのレート制限 1561
ダイナミック ARP インスペクション検証チェックの実行 1564
DAI のモニタリング 1565
DAI の設定の確認 1566
その他の参考資料 1567
IEEE 802.1x ポートベースの認証の設定 1569
機能情報の確認 1569
802.1x ポートベース認証について 1569
ポートベース認証プロセス 1570
ポートベース認証の開始およびメッセージ交換 1572
ポートベース認証の認証マネージャ 1574
Port-Based 認証方法 1574
ユーザ単位 ACL および Filter-Id 1575
ポートベース認証マネージャ CLI コマンド 1576
許可ステートおよび無許可ステートのポート 1578
ポートベース認証とスイッチ スタック 1579
802.1X のホスト モード 1579
802.1x 複数認証モード 1580
ユーザごとのマルチ認証 VLAN 割り当て 1581

ユーザごとのマルチ認証 VLAN 割り当ての制限 1582
MAC 移動 1583
MAC 置換 1583
802.1x アカウンティング 1584
802.1x アカウンティング属性値ペア 1584
802.1x 準備状態チェック 1586
スイッチと RADIUS サーバ間の通信 1586
VLAN 割り当てを使用した 802.1x 認証 1586
ユーザ単位 ACL を使用した 802.1x 認証 1589
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証 1590
Cisco Secure ACS およびリダイレクト URL の属性と値のペア 1591
Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア 1592
VLAN ID ベース MAC 認証 1592
ゲスト VLAN を使用した 802.1x 認証 1593
制限付き VLAN による 802.1x 認証 1594
アクセス不能認証バイパスを使用した 802.1x 認証 1595
複数認証ポートのアクセス不能認証バイパスのサポート 1595
アクセス不能認証バイパスの認証結果 1596
アクセス不能認証バイパス機能の相互作用 1596
802.1x クリティカル音声 VLAN 1597
802.1x ユーザ ディストリビューション 1598
802.1x ユーザ ディストリビューションの設定時の注意事項 1598
音声 VLAN ポートを使用した IEEE 802.1x 認証 1599
ポート セキュリティを使用した IEEE 802.1x 認証 1600
WoL 機能を使用した IEEE 802.1x 認証 1600
MAC 認証バイパスを使用した IEEE 802.1x 認証 1600
Network Admission Control レイヤ 2 IEEE 802.1x 検証 1602
柔軟な認証の順序設定 1602
Open1x 認証 1603
マルチドメイン認証 1604
Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ 1605

音声認識 802.1x セキュリティ 1607
コモン セッション ID 1608
802.1x ポートベース認証の設定方法 1608
802.1x 認証のデフォルト設定 1608
802.1x 認証設定時の注意事項 1610
802.1X 認証 1610
VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス 1611
MAC 認証バイパス 1612
ポートあたりのデバイスの最大数 1613
802.1x 準備状態チェックの設定 1613
音声認識 802.1x セキュリティの設定 1615
802.1x 違反モードの設定 1617
802.1X 認証の設定 1619
802.1x ポートベース認証の設定 1620
スイッチと RADIUS サーバ間の通信の設定 1623
ホスト モードの設定 1625
定期的な再認証の設定 1626
待機時間の変更 1627
スイッチからクライアントへの再送信時間の変更 1629
スイッチからクライアントへのフレーム再送信回数の設定 1630
再認証回数の設定 1632
MAC 移動のイネーブル化 1633
MAC 置換のイネーブル化 1634
IEEE 802.1x アカウンティングの設定 1636
ゲスト VLAN の設定 1638
制限付き VLAN の設定 1639
制限付き VLAN の認証試行回数の設定 1641
クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定 1643
アクセス不能認証バイパスの設定例 1647
WoL を使用した 802.1x 認証の設定 1647

MAC 認証バイパスの設定 1648
802.1x ユーザ ディストリビューションの設定 1650
VLAN グループの設定例 1651
NAC レイヤ 2 802.1x 検証の設定 1651
NEAT を使用したオーセンティケータ スイッチの設定 1653
NEAT を使用したサプリカント スイッチの設定 1655
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定 1658
ダウンロード可能な ACL の設定 1659
ダウンロード ポリシーの設定 1660
VLAN ID ベース MAC 認証の設定 1663
柔軟な認証順序の設定 1664
Open1x の設定 1666
ポート上での 802.1x 認証のディセーブル化 1668
802.1x 認証設定のデフォルト値へのリセット 1669
802.1x の統計情報およびステータスのモニタリング 1670
その他の参考資料 1671
Web ベース認証の設定 1673
機能情報の確認 1673
Web ベース認証の概要 1673
デバイスのロール 1674
ホストの検出 1675
セッションの作成 1675
認証プロセス 1676
ローカル Web 認証バナー 1676
Web 認証カスタマイズ可能な Web ページ 1679
ガイドライン 1680
認証プロキシ Web ページの注意事項 1681
成功ログインに対するリダイレクト URL の注意事項 1682
その他の機能と Web ベース認証の相互作用 1682
ポート セキュリティ 1682
LAN ポート IP 1683

Gateway IP 1683
ACL 1683
コンテキストベース アクセス コントロール 1683
EtherChannel 1683
Web ベース認証の設定方法 1684
デフォルトの Web ベース認証の設定 1684
Web ベース認証の設定に関する注意事項と制約事項 1684
認証ルールとインターフェイスの設定 1686
AAA 認証の設定 1688
スイッチ/RADIUS サーバ間通信の設定 1690
HTTP サーバの設定 1692
認証プロキシ Web ページのカスタマイズ 1693
成功ログインに対するリダイレクション URL の指定 1695
Web ベース認証パラメータの設定 1696
Web ベース認証ローカル バナーの設定 1697
SVI なしの Web ベース認証の設定 1699
VRF 認識による Web ベース認証の設定 1700
Web ベース認証キャッシュ エントリの削除 1702
Web ベース認証ステータスのモニタリング 1703
ポート単位のトラフィック制御の設定 1705
ポートベースのトラフィック制御の概要 1705
機能情報の確認 1706
ストーム制御に関する情報 1706
ストーム制御 1706
トラフィック アクティビティの測定方法 1706
トラフィック パターン 1707
ストーム制御の設定方法 1708
ストーム制御およびしきい値レベルの設定 1708
スモール フレーム到着レートの設定 1711
保護ポートに関する情報 1714
保護ポート 1714
保護ポートのデフォルト設定 1714
保護ポートのガイドライン 1714

保護ポートの設定方法 1715
保護ポートの設定 1715
保護ポートのモニタリング 1716
ポート ブロッキングに関する情報 1717
ポート ブロッキング 1717
ポート ブロッキングの設定方法 1717
インターフェイスでのフラッディング トラフィックのブロッキング 1717
ポート ブロッキングのモニタリング 1719
ポート セキュリティの前提条件 1719
ポート セキュリティの制約事項 1719
ポート セキュリティの概要 1720
ポート セキュリティ 1720
セキュア MAC アドレスのタイプ 1720
スティッキ セキュア MAC アドレス 1720
セキュリティ違反 1721
ポート セキュリティ エージング 1722
ポート セキュリティとスイッチ スタック 1723
デフォルトのポート セキュリティ設定 1723
ポート セキュリティの設定時の注意事項 1723
ポートベースのトラフィック制御の概要 1725
ポート セキュリティの設定方法 1725
ポート セキュリティのイネーブル化および設定 1725
ポート セキュリティ エージングのイネーブル化および設定 1730
機能情報の確認 1733
ストーム制御に関する情報 1733
ストーム制御 1733
トラフィック アクティビティの測定方法 1733
トラフィック パターン 1734
ストーム制御の設定方法 1735
ストーム制御およびしきい値レベルの設定 1735
スモール フレーム到着レートの設定 1738
機能情報の確認 1740

保護ポートに関する情報 1741
保護ポート 1741
保護ポートのデフォルト設定 1741
保護ポートのガイドライン 1741
保護ポートの設定方法 1741
保護ポートの設定 1741
保護ポートのモニタリング 1743
次の作業 1743
その他の参考資料 1744
機能情報 1745
機能情報の確認 1745
ポート ブロッキングに関する情報 1745
ポート ブロッキング 1745
ポート ブロッキングの設定方法 1746
インターフェイスでのフラッディング トラフィックのブロッキング 1746
ポート ブロッキングのモニタリング 1748
次の作業 1748
その他の参考資料 1748
機能情報 1749
ポート セキュリティの設定例 1749
IPv6 ファースト ホップ セキュリティの設定 1751
機能情報の確認 1751
IPv6 でのファースト ホップ セキュリティの前提条件 1752
IPv6 でのファースト ホップ セキュリティの制約事項 1752
IPv6 でのファースト ホップ セキュリティに関する情報 1752
SISF ベースの IPv4 および IPv6 デバイス トラッキングに関する情報 1755
SISF ベース デバイス トラッキング CLI への移行時の制限 1756
新しい SISF ベースのデバイス トラッキング CLI への移行 1756
IPDT、IPv6 スヌーピング、およびデバイス トラッキング CLI の互換性 1758
SISF ベースの IP デバイス トラッキングおよびスヌーピング ポリシーを作成する方法 1758
デバイス トラッキング ポリシーをインターフェイスにアタッチする方法 1760

デバイス トラッキング ポリシーを VLAN にアタッチする方法 1761
デバイス全体のエントリをバインディング テーブルに追加する方法 1762
IPv6 スヌーピング ポリシーの設定方法 1763
IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法 1765
IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1767
IPv6 スヌーピング ポリシーを全体的に VLAN にアタッチする方法 1769
IPv6 バインディング テーブルの内容を設定する方法 1770
IPv6 ネイバー探索インスペクション ポリシーの設定方法 1771
IPv6 ネイバー探索インスペクション ポリシーをインターフェイスにアタッチする方法 1773
IPv6 ネイバー探索インスペクション ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1774
IPv6 ネイバー探索インスペクション ポリシーを全体的に VLAN にアタッチする方法 1776
IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法 1777
IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法 1780
IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1781
IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法 1782
IPv6 DHCP ガード ポリシーの設定方法 1783
IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法 1786
IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1787
IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法 1789
IPv6 ソース ガードの設定方法 1790
IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法 1791
IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1793

IPv6 プレフィックス ガードの設定方法 1794
IPv6 プレフィックス ガード ポリシーをインターフェイスにアタッチする方法 1795
IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1797
IPv6 ファースト ホップ セキュリティの設定例 1798
例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1798
例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1798
その他の参考資料 1799
Cisco TrustSec の設定 1801
Cisco TrustSec の概要 1801
機能情報の確認 1801
Cisco TrustSec の機能 1802
Cisco TrustSec の機能情報 1805
ワイヤレス ゲスト アクセスの設定 1807
機能情報の確認 1807
ゲスト アクセスの前提条件 1807
ゲスト アクセスの制約事項 1808
ワイヤレス ゲスト アクセスについて 1808
高速安全ローミング 1808
ゲスト アクセスを設定する方法 1809
ロビー管理者アカウントの作成 1809
ゲスト ユーザ アカウントの設定 1811
モビリティ エージェント（MA）の設定 1812
モビリティ コントローラの設定 1814
Web 認証証明書の入手 1815
Web 認証証明書の表示 1816
デフォルトの Web 認証ログイン ページの選択 1816
外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択 1818

WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て 1820
AAA-Override の設定 1822
クライアントの負荷分散の設定 1823
事前認証 ACL の設定 1824
IOS ACL 定義の設定 1825
Webpassthrough の設定 1826
ゲスト アクセスの設定例 1827
例：Lobby Ambassador アカウントの作成 1827
例：Web 認証証明書の入手 1827
例：Web 認証証明書の表示 1828
例：ゲスト ユーザ アカウントの設定 1829
例：モビリティ コントローラの設定 1829
例：デフォルトの Web 認証ログイン ページの選択 1830
例：外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択 1831
例：WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て 1831
例：AAA-Override の設定 1831
例：クライアントの負荷分散の設定 1832
例：事前認証 ACL の設定 1832
例：IOS ACL 定義の設定 1832
例：Webpassthrough の設定 1832
ゲスト アクセスに関する追加情報 1833
ゲスト アクセスの機能履歴と情報 1834
不正なデバイスの管理 1835
機能情報の確認 1835
不正なデバイスについて 1835
不正検出の設定方法 1841
不正検出の設定（CLI） 1841
不正検出の設定（GUI） 1842
不正検出のモニタリング 1844

例：不正検出の設定 1844
不正検出に関する追加情報 1845
不正検出設定の機能履歴と情報 1846
不正なアクセス ポイントの分類 1847
機能情報の確認 1847
不正なアクセス ポイントの分類について 1847
不正なアクセス ポイントの分類の制限 1850
不正なアクセス ポイントの分類方法 1851
不正分類ルールの設定（CLI） 1851
不正分類ルールの設定（GUI） 1854
不正なデバイスの表示および分類（GUI） 1857
例：不正なアクセス ポイントの分類 1859
不正なアクセス ポイントの分類に関する追加情報 1860
不正なアクセス ポイントの分類の機能履歴および情報 1861
wIPS の設定 1863
機能情報の確認 1863
wIPS について 1863
アクセス ポイントで wIPS を設定する方法 1871
アクセス ポイントでの wIPS の設定（CLI） 1871
アクセス ポイントでの wIPS の設定（GUI） 1872
wIPS 情報のモニタリング 1872
例：wIPS の設定 1873
wIPS の設定に関する追加情報 1873
wIPS 設定実行の機能履歴 1874
侵入検知システムの設定 1875
機能情報の確認 1875
Intrusion Detection System について 1875
侵入検知システムを設定する方法 1876
IDS センサーの設定 1876
侵入検知システムのモニタリング 1877
スタック マネージャおよびハイ アベイラビリティ 1879
スイッチ スタックの管理 1881

機能情報の確認 1881
スイッチ スタックの前提条件 1882
スイッチ スタックの制約事項 1882
スイッチ スタックに関する情報 1882
スイッチ スタックの概要 1882
スイッチ スタックでサポートされる機能 1883
暗号化機能 1883
StackWise-160 1883
スイッチ スタックのメンバーシップ 1883
スイッチ スタック メンバーシップの変更 1884
スタック メンバー番号 1885
スタック メンバーのプライオリティ値 1887
スイッチ スタック ブリッジ ID と MAC アドレス 1887
スイッチ スタック上の永続的 MAC アドレス 1888
アクティブ スイッチとスタンバイ スイッチの選択と再選択 1888
スイッチ スタックのコンフィギュレーション ファイル 1889
スタック メンバーを割り当てるためのオフライン設定 1890
割り当てられたスイッチのスイッチ スタックへの追加による影響 1891
スイッチ スタックの割り当てられたスイッチの交換による影響 1893
割り当てられたスイッチのスイッチ スタックからの削除による影響 1893
互換性のないソフトウェアを実行しているスイッチのアップグレード 1893
自動アップグレード 1893
自動アドバイス 1895
自動アドバイス メッセージの例 1895
スイッチ スタックの管理接続 1896
特定のスタック メンバーへの接続 1896
IP アドレスによるスイッチ スタックへの接続 1896
コンソール ポートまたはイーサネット管理ポートによるスイッチ スタックへの接続 1897
スイッチ スタックの設定方法 1897
永続的 MAC アドレス機能のイネーブル化 1897
スタック メンバー番号の割り当て 1899

スタック メンバー プライオリティ値の設定 1901
スイッチ スタックへの新しいメンバーのプロビジョニング 1902
割り当てられたスイッチ情報の削除 1903
スイッチ スタック内の非互換スイッチの表示 1904
スイッチ スタックでの互換性のないスイッチのアップグレード 1905
スイッチ スタックのトラブルシューティング 1906
スタック メンバーの診断コンソールへのアクセス 1906
スタック ポートの一時的なディセーブル化 1906
他のメンバーの起動中のスタック ポートの再イネーブル化 1907
スイッチ スタックのモニタリング 1908
スイッチ スタックの設定例 1909
スイッチ スタックの設定のシナリオ 1909
永続的 MAC アドレス機能のイネーブル化：例 1911
スイッチ スタックへの新しいメンバーのプロビジョニング：例 1912
show switch stack-ports summary コマンドの出力：例 1912
ソフトウェア ループバック：例 1914
スタック ケーブルが接続されたソフトウェア ループバック：例 1915
スタック ケーブルが接続されていないソフトウェア ループバック：例 1916
切断されたスタック ケーブルの特定：例 1916
スタック ポート間の不安定な接続の修正：例 1917
スイッチ スタックに関する追加情報 1918
Cisco NSF with SSO の設定 1921
機能情報の確認 1921
NSF with SSO の前提条件 1921
NSF with SSO の制約事項 1922
NSF with SSO に関する情報 1922
NSF with SSO の概要 1922
SSO の動作 1923
NSF の動作 1925
Cisco Express Forwarding; シスコ エクスプレス フォワーディング 1926
BGP の動作 1926

OSPF の動作 1927
EIGRP の動作 1928
Cisco NSF with SSO の設定方法 1929
SSO の設定 1929
SSO の設定例 1930
CEF NSF の確認 1930
NSF の BGP の設定 1931
BGP NSF の確認 1932
OSPF NSF の設定 1933
OSPF NSF の確認 1933
EIGRP NSF の設定 1934
EIGRP NSF の確認 1935
ワイヤレスハイ アベイラビリティの設定 1937
機能情報の確認 1937
ハイ アベイラビリティに関する情報 1937
冗長性に関する情報 1938
アクセス ポイントの冗長性の設定 1938
ハートビート メッセージの設定 1940
アクセス ポイントのステートフル スイッチオーバーに関する情報 1940
グレースフル スイッチオーバーの開始 1941
ハイ アベイラビリティ用の EtherChannel の設定 1941
LACP の設定 1942
ハイ アベイラビリティのトラブルシューティング 1943
スタンバイ コンソールへのアクセス 1943
スイッチオーバー前 1944
スイッチオーバー後 1946
スイッチ スタックのモニタリング 1947
LACP の設定：例 1947
システム管理 1951
システムの管理 1953
機能情報の確認 1953
スイッチの管理に関する情報 1954

システム日時の管理 1954
システム クロック 1954
ネットワーク タイム プロトコル 1954
NTP ストラタム 1956
NTP アソシエーション 1957
NTP セキュリティ 1957
NTP の実装 1957
NTP バージョン 4 1958
システム名およびシステム プロンプト 1959
スタックのシステム名およびシステム プロンプト 1959
デフォルトのシステム名とプロンプトの設定 1959
DNS 1959
DNS のデフォルト設定値 1960
ログイン バナー 1960
バナーのデフォルト設定 1960
MAC Address Table 1960
MAC アドレス テーブルの作成 1961
MAC アドレスおよび VLAN 1961
MAC アドレスおよびスイッチのスタック 1961
MAC アドレス テーブルのデフォルト設定 1962
ARP テーブルの管理 1962
スイッチを管理する方法 1963
手動による日付と時刻の設定 1963
システム クロックの設定 1963
タイム ゾーンの設定 1964
夏時間の設定 1965
1967
システム名の設定 1969
DNS の設定 1970
Message-of-the-Day ログイン バナーの設定 1972
ログイン バナーの設定 1974
MAC アドレス テーブルの管理 1975
アドレス エージング タイムの変更 1975

MAC アドレス変更通知トラップの設定 1977
MAC アドレス移動通知トラップの設定 1979
MAC しきい値通知トラップの設定 1982
スタティック アドレス エントリの追加および削除 1984
ユニキャスト MAC アドレス フィルタリングの設定 1986
スイッチのモニタリングおよび保守の管理 1987
スイッチ管理の設定例 1988
例：システム クロックの設定 1988
例：サマー タイムの設定 1989
例：MOTD バナーの設定 1989
例：ログイン バナーの設定 1989
例：MAC アドレス変更通知トラップの設定 1990
例：MAC しきい値通知トラップの設定 1990
例：MAC アドレス テーブルへのスタティック アドレスの追加 1990
例：ユニキャスト MAC アドレス フィルタリングの設定 1990
スイッチ管理に関する追加情報 1991
スイッチ管理に関する追加情報 1992
スイッチ管理の機能履歴と情報 1994
スイッチのセットアップ設定の実行 1995
機能情報の確認 1995
スイッチセットアップ設定の実行に関する情報 1995
スイッチブート プロセス 1996
ソフトウェア インストーラ機能 1997
ソフトウェアのブート モード 1997
インストール モードでのブート 1997
バンドル モードでのブート 1998
スイッチ スタックのブート モード 1999
スイッチ情報の割り当て 1999
デフォルトのスイッチ情報 2000
DHCP ベースの自動設定の概要 2000
DHCP クライアントの要求プロセス 2001
DHCP ベースの自動設定およびイメージ アップデート 2002

DHCP ベースの自動設定の制約事項 2003
DHCP 自動設定 2003
DHCP 自動イメージ アップデート 2003
DHCP サーバ設定時の注意事項 2004
TFTP サーバの目的 2005
DNS サーバの目的 2005
コンフィギュレーション ファイルの入手方法 2006
環境変数の制御方法 2007
一般的な環境変数 2007
TFTP の環境変数 2010
ソフトウェア イメージのリロードのスケジューリング 2010
スイッチ設定コンフィギュレーションの実行方法 2011
DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定 2011
DHCP 自動イメージアップデート（コンフィギュレーション ファイルおよびイメージ）の設定 2014
DHCP サーバからファイルをダウンロードするクライアントの設定 2018
複数の SVI への IP 情報の手動割り当て 2019
スイッチのスタートアップ コンフィギュレーションの変更 2021
システム コンフィギュレーションを読み書きするためのファイル名の指定 2021
スイッチの手動による起動 2023
インストール モードでスイッチ の起動 2024
バンドル モードでスイッチの起動 2026
スイッチ スタックで特定のソフトウェア イメージを起動する場合 2027
ソフトウェア イメージのリロードのスケジュール設定 2029
スイッチのセットアップ設定のモニタリング 2030
例：スイッチ実行コンフィギュレーションの確認 2030
例：インストール モードでのソフトウェアブートアップ ディスプレイ 2031
例：緊急インストール 2032
スイッチ のセットアップを実行する場合の設定例 2034
例：DHCP サーバとしてのスイッチの設定 2034
例：DHCP 自動イメージ アップデートの設定 2034

例：DHCP サーバから設定をダウンロードするためのスイッチの設定 2034
例：ソフトウェア イメージのリロードのスケジューリング 2035
スイッチのセットアップの実行に関する追加情報 2035
WCM サブパッケージのインストール 2037
利点 2037
前提条件 2037
制約事項 2038
WCM サブパッケージのインストール 2038
スイッチセットアップ設定の機能履歴と情報 2039
Right-To-Use ライセンスの設定 2041
機能情報の確認 2041
RTU ライセンスの設定に関する制約事項 2041
RTU ライセンスの設定に関する情報 2042
Right-To-Use ライセンス 2042
Right-To-Use イメージ ベースのライセンス 2043
Right-To-Use ライセンスの状態 2043
スイッチ スタックのライセンスのアクティブ化 2044
モビリティ コントローラ モード 2044
Right-To-Use AP-Count ライセンス 2044
Right-to-Use AP-Count 評価ライセンス 2045
Right-To-Use Adder AP-Count 再ホスト ライセンス 2045
RTU ライセンスの設定方法 2046
イメージ ベース ライセンスのアクティブ化 2046
ap-count ライセンスのアクティブ化 2047
アップグレード ライセンスまたはキャパシティ Adder ライセンスの取得 2048
ライセンスの再ホスト 2049
モビリティ モードの変更 2050
RTU ライセンスのモニタリングおよびメンテナンス 2051
RTU ライセンスの設定例 2052
例：RTU イメージ ベースのライセンスのアクティブ化 2052
例：RTU ライセンス情報の表示 2053
例：RTU ライセンスの詳細の表示 2054

例：RTU ライセンスの不一致の表示 2055
例：RTU ライセンス使用状況の表示 2056
RTU ライセンスに関する追加情報 2057
RTU ライセンスの機能履歴と情報 2058
管理者のユーザ名とパスワードの設定 2059
機能情報の確認 2059
管理者のユーザ名とパスワードの設定について 2059
管理者のユーザ名とパスワードの設定 2061
例：管理者のユーザ名とパスワードの設定 2063
管理者のユーザ名とパスワードに関する追加情報 2063
管理者のユーザ名とパスワードの設定の機能履歴と情報 2064
802.11 パラメータおよび帯域選択の設定 2065
機能情報の確認 2065
帯域選択の制約事項、802.11 帯域とパラメータ 2065
帯域選択、802.11 帯およびパラメータに関する情報 2066
帯域選択 2066
802.11 帯域 2067
802.11n パラメータ 2067
802.11h パラメータ 2067
802.11 帯とそのパラメータを設定する方法 2068
帯域選択の設定（CLI） 2068
802.11 帯域の設定（CLI） 2069
802.11n のパラメータの設定（CLI） 2072
802.11h のパラメータの設定（CLI） 2075
帯域選択、802.11 帯およびパラメータの設定のモニタリング 2076
帯域選択と 802.11 帯を使用した設定のモニタリング コマンド 2076
例：5 GHz 帯域の設定の確認 2077
例：24 GHz 帯域の設定の確認 2078
例：802.11h パラメータの状態の確認 2080
例：帯域選択設定の確認 2080
帯域選択、802.11 帯およびパラメータの設定例 2080
例：帯域選択の設定 2080

例：802.11 帯設定 2081
例：802.11n 設定 2081
例：802.11h 設定 2082
802.11 パラメータおよび帯域選択に関する追加情報 2082
802.11 パラメータおよび帯域選択設定の機能履歴と情報 2083
アグレッシブ ロード バランシングの設定 2085
機能情報の確認 2085
アグレッシブ ロード バランシングの制約事項 2085
アグレッシブ ロード バランシング パラメータの設定情報 2086
アグレッシブ ロード バランシング 2086
アグレッシブ ロード バランシングの設定方法 2088
アグレッシブなロード バランシングの設定（CLI） 2088
アグレッシブなロード バランシングの設定（GUI） 2089
アグレッシブ ロード バランシングのモニタリング 2090
アグレッシブ ロード バランシングに関する追加情報 2090
アグレッシブ ロード バランシングの設定の機能履歴と情報 2091
クライアント ローミングの設定 2093
機能情報の確認 2093
クライアント ローミングの設定の制約事項 2093
クライアント ローミングについて 2094
サブネット間ローミング 2095
VoIP による通話ローミング 2095
CCX レイヤ 2 クライアント ローミング 2096
レイヤ 2 またはレイヤ 3 のローミング設定方法 2097
レイヤ 2 またはレイヤ 3 のローミング設定 2097
CCX クライアント ローミング パラメータの設定（CLI） 2098
モビリティ Oracle の設定 2100
モビリティ コントローラの設定 2101
モビリティ エージェントの設定 2103
クライアントのローミング パラメータのモニタリング 2104
モビリティ設定のモニタ 2105
クライアント ローミング設定に関する追加情報 2106

クライアント ローミング設定の機能履歴と情報 2107

Application Visibility and Control の設定 2109

機能情報の確認 2109

Application Visibility and Control について 2110

サポートされる AVC クラス マップおよびポリシー マップのフォーマット 2111

アプリケーションの可視性およびコントロールの前提条件 2114

Application Visibility and Control によるスイッチ間ローミングに関するガイドライン 2114

Application Visibility and Control の制限 2115

Application Visibility and Control の設定方法 2115

アプリケーションの可視性およびコントロールの設定（CLI） 2115

フロー レコードの作成 2115

フロー エクスポータの作成（オプション） 2118

フロー モニタの作成 2120

AVC QoS ポリシーの作成 2121

クラス マップの作成 2121

ポリシー マップの作成 2123

ローカル ポリシーの設定（CLI） 2124

ローカル ポリシーの設定（CLI） 2124

サービス テンプレートの作成（CLI） 2124

パラメータ マップの作成（CLI） 2126

ポリシー マップの作成（CLI） 2127

WLAN 上のデバイスのローカル ポリシーの適用（CLI） 2129

ローカル ポリシーの設定（GUI） 2130

ローカル ポリシーの設定（GUI） 2130

サービス テンプレートの作成（GUI） 2130

ポリシー マップの作成（GUI） 2131

WLAN へのローカル ポリシーの適用（GUI） 2133

IPV4 の入出力方向にフロー モニタを適用する WLAN の設定 2133

Application Visibility and Control の設定（GUI） 2134

アプリケーションの可視性の設定（GUI） 2134

Application Visibility and Control の設定（GUI） 2135

Application Visibility and Control のモニタリング 2137
Application Visibility and Control のモニタリング（CLI） 2137
アプリケーションの可視性およびコントロールのモニタリング（GUI） 2138
SSID およびクライアント ポリシーの統計情報の監視（GUI） 2139
例：Application Visibility and Control 2140
例:アプリケーションの可視性設定 2140
例：Application Visibility and Control の QoS 設定 2141
例 :ローカル プロファイリング ポリシーのための QoS の属性設定 2143
Application Visibility and Control に関する追加情報 2143
Application Visibility and Control の機能履歴および情報 2144
音声パラメータとビデオ パラメータの設定 2145
機能情報の確認 2145
音声およびビデオのパラメータの前提条件 2145
音声およびビデオのパラメータの制約事項 2146
音声パラメータとビデオ パラメータの設定について 2146
コール アドミッション制御 2146
静的ベースの CAC 2147
load-based の CAC 2147
IOSd コール アドミッション制御 2148
Expedited Bandwidth Requests 2148
U-APSD 2149
Traffic Stream Metrics 2150
優先コール番号を使用した音声優先制御の設定について 2151
EDCA パラメータについて 2151
音声パラメータとビデオ パラメータの設定方法 2151
音声パラメータの設定（CLI） 2151
ビデオ パラメータの設定（CLI） 2156
SIP ベースの CAC の設定（CLI） 2159
優先コール番号の設定（CLI） 2160
EDCA パラメータの設定（CLI） 2162
音声およびビデオ パラメータのモニタリング 2164
音声およびビデオ パラメータの設定例 2166
例：音声およびビデオの設定 2166

音声およびビデオ パラメータに関する追加情報 2168
音声およびビデオ パラメータ設定の機能履歴と情報 2169
RFID タグ追跡の設定 2171
機能情報の確認 2171
RFID タグ追跡の設定について 2171
RFID タグ トラッキングの設定方法 2172
RFID タグ追跡の設定（CLI） 2172
RFID タグ トラッキング情報のモニタリング 2173
RFID タグ トラッキングに関する追加情報 2173
RFID タグ トラッキング設定の機能履歴と情報 2174
ロケーションの設定 2175
機能情報の確認 2175
ロケーションの設定に関する情報 2175
ロケーションの設定方法 2176
ロケーションの設定（CLI） 2176
クライアント、RFID タグ、および不正デバイスの NMSP 通知間隔の変更（CLI） 2179
クライアント、RFID タグ、および不正デバイスの NMSP 通知しきい値の変更（CLI） 2180
ロケーション設定および NMSP 設定のモニタリング 2180
ロケーション設定のモニタリング（CLI） 2180
NMSP 設定のモニタリング（CLI） 2181
例：ロケーションの設定 2182
例：NMSP の設定 2182
ロケーション設定に関する追加情報 2182
ロケーション設定の機能履歴と情報 2183
フロー制御のモニタリング 2185
機能情報の確認 2185
フロー制御の概要 2185
フロー制御のモニタリング 2186
例：フロー制御のモニタリング 2186
フロー制御のモニタリングに関する追加情報 2187

フロー制御のモニタリングに関する機能履歴および情報 2188
SDM テンプレートの設定 2189
機能情報の確認 2189
SDM テンプレートの設定に関する情報 2190
SDM テンプレート 2190
SDM テンプレートとスイッチ スタック 2191
SDM テンプレートの設定方法 2192
SDM テンプレートの設定 2192
スイッチ SDM テンプレートの設定 2192
SDM テンプレートの設定 2192
SDM テンプレートのモニタリングおよびメンテナンス 2193
SDM テンプレートの設定例 2194
例：SDM テンプレートの設定 2194
例：SDM テンプレートの表示 2194
Additional References for SDM Templates 2195
SDM テンプレートの設定の機能履歴と情報 2196
システム メッセージ ログの設定 2197
機能情報の確認 2197
システム メッセージ ログの設定に関する情報 2197
システム メッセージ ロギング 2197
システム ログ メッセージのフォーマット 2198
デフォルトのシステム メッセージ ロギングの設定 2199
syslog メッセージの制限 2200
システム メッセージ ログの設定方法 2201
メッセージ表示宛先デバイスの設定 2201
ログ メッセージの同期化 2202
メッセージ ロギングのディセーブル化 2204
ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化 2205
ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化 2206
メッセージ重大度の定義 2207
履歴テーブルおよび SNMP に送信される syslog メッセージの制限 2208
UNIX Syslog デーモンへのメッセージのロギング 2209

システム メッセージ ログのモニタリングおよびメンテナンス 2211
コンフィギュレーション アーカイブ ログのモニタリング 2211
システム メッセージ ログの設定例 2211
例：システム メッセージのスタック構成 2211
例：スイッチ システム メッセージ 2211
システム メッセージ ログに関する追加情報 2212
システム メッセージ ログの機能履歴と情報 2213
オンライン診断の設定 2215
機能情報の確認 2215
オンライン診断の設定に関する情報 2215
オンライン診断 2215
オンライン診断の設定方法 2216
オンライン診断テストの開始 2216
オンライン診断の設定 2217
オンライン診断のスケジューリング 2217
ヘルス モニタリング診断の設定 2219
オンライン診断のモニタリングおよびメンテナンス 2222
オンライン診断テストとテスト結果の表示 2222
オンライン診断テストの設定例 2223
例：診断テストの開始 2223
例：ヘルス モニタリング テストの設定 2223
例：診断テストのスケジューリング 2223
例：オンライン診断の表示 2223
オンライン診断に関する追加情報 2225
オンライン診断設定の機能履歴と情報 2226
コンフィギュレーション ファイルの管理 2227
コンフィギュレーション ファイルの管理の前提条件 2227
コンフィギュレーション ファイルの管理の制約事項 2227
コンフィギュレーション ファイルの管理について 2228
コンフィギュレーション ファイルのタイプ 2228
コンフィギュレーション モードとコンフィギュレーション ソースの選択 2228
CLI を使用したコンフィギュレーション ファイルの変更 2229

コンフィギュレーション ファイルの場所 2229
ネットワーク サーバからスイッチへのコンフィギュレーション ファイルのコピー 2229
スイッチから TFTP サーバへのコンフィギュレーション ファイルのコピー 2230
スイッチから RCP サーバへのコンフィギュレーション ファイルのコピー 2230
機能制限 2231
RCP ユーザ名に関する要件 2232
スイッチから FTP サーバへのコンフィギュレーション ファイルのコピー 2232
FTP ユーザ名およびパスワードの概要 2233
スイッチから別のスイッチへの設定ファイルのコピー 2233
NVRAM より大きいコンフィギュレーション ファイル 2234
コンフィギュレーション ファイルの圧縮 2234
コンフィギュレーションのクラスAフラッシュ ファイル システム上のフラッシュ メモリへの格納 2234
ネットワークからのコンフィギュレーション コマンドのロード 2235
コンフィギュレーション ファイルをダウンロードするスイッチの設定 2235
ネットワークとホストのコンフィギュレーション ファイル 2235
コンフィギュレーション ファイル情報の管理方法 2235
コンフィギュレーション ファイル情報の表示（CLI） 2235
コンフィギュレーション ファイルの変更（CLI） 2237
スイッチから TFTP サーバへのコンフィギュレーション ファイルのコピー（CLI） 2239
次の作業 2240
スイッチから RCP サーバへのコンフィギュレーション ファイルのコピー (CLI) 2240
例 2241
RCP サーバへの実行コンフィギュレーション ファイルの格納 2241
RCP サーバへのスタートアップ コンフィギュレーション ファイルの格納 2241
次の作業 2242
スイッチから FTP サーバへのコンフィギュレーション ファイルのコピー(CLI) 2242
例 2243

FTP サーバへの実行コンフィギュレーション ファイルの格納 2243
FTP サーバへのスタートアップ コンフィギュレーション ファイルの格納 2244
次の作業 2244
TFTP サーバからスイッチへのコンフィギュレーション ファイルのコピー（CLI） 2244
次の作業 2245
rcp サーバからスイッチへのコンフィギュレーション ファイルのコピー（CLI） 2245
例 2247
RCP の Running-Config のコピー 2247
RCP の Startup-Config のコピー 2247
次の作業 2247
FTP サーバからスイッチへのコンフィギュレーション ファイルのコピー（CLI） 2248
例 2249
FTP の Running-Config のコピー 2249
FTP の Startup-Config のコピー 2249
次の作業 2250
NVRAM より大きいコンフィギュレーション ファイルの保守 2250
コンフィギュレーション ファイルの圧縮（CLI） 2250
コンフィギュレーションのクラス A フラッシュ ファイル システム上のフラッシュ メモリへの格納（CLI） 2252
ネットワークからのコンフィギュレーション コマンドのロード（CLI） 2254
フラッシュ メモリからスタートアップまたは実行コンフィギュレーションへのコンフィギュレーション ファイルのコピー（CLI） 2255
フラッシュ メモリ ファイル システム間でのコンフィギュレーション ファイルのコピー（CLI） 2256
FTP サーバからフラッシュ メモリ デバイスへのコンフィギュレーション ファイルのコピー（CLI） 2258
次の作業 2259

RCP サーバからフラッシュ メモリ デバイスへのコンフィギュレーション ファイルのコピー（CLI） 2259
TFTP サーバからフラッシュ メモリ デバイスへのコンフィギュレーション ファイルのコピー（CLI） 2261
スタートアップ コンフィギュレーション ファイルでのコンフィギュレーション コマンドの再実行（CLI） 2262
スタートアップ コンフィギュレーションのクリア（CLI） 2262
指定されたコンフィギュレーション ファイルの削除（CLI） 2263
クラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定（CLI） 2264
次の作業 2266
コンフィギュレーション ファイルをダウンロードするスイッチの設定 2267
ネットワーク コンフィギュレーション ファイルをダウンロードするスイッチの設定（CLI） 2267
ホスト コンフィギュレーション ファイルをダウンロードするスイッチの設定（CLI） 2269
その他の参考資料 2271
コンフィギュレーションの置換とロールバック 2273
コンフィギュレーションの置換とロールバックの前提条件 2273
コンフィギュレーションの置換とロールバックの制約事項 2274
コンフィギュレーションの置換とロールバックについて 2274
コンフィギュレーション アーカイブ 2274
コンフィギュレーションの置換 2275
設定のロール バック 2276
コンフィギュレーション ロールバック変更確認 2277
コンフィギュレーションの置換およびロールバックの利点 2277
コンフィギュレーションの置換とロールバックの使用方法 2277
コンフィギュレーション アーカイブの作成（CLI） 2277
コンフィギュレーションの置換またはロールバックの実行（CLI） 2279
機能のモニタリングおよびトラブルシューティング（CLI） 2281
コンフィギュレーションの置換とロールバックの設定例 2284
コンフィギュレーション アーカイブの作成 2284

現在の実行コンフィギュレーションを保存されたCisco IOS コンフィギュレーション ファイルで置換する 2284
スタートアップ コンフィギュレーション ファイルへの復帰 2285
configure confirm コマンドを使用したコンフィギュレーション置換操作の実行 2285
コンフィギュレーション ロールバック操作の実行 2285
その他の参考資料 2286
フラッシュ ファイル システムの操作 2289
フラッシュ ファイル システムについて 2289
使用可能なファイル システムの表示 2290
デフォルト ファイル システムの設定 2292
ファイル システムのファイルに関する情報の表示 2293
ディレクトリの変更および作業ディレクトリの表示（CLI） 2293
ディレクトリの作成（CLI） 2295
ディレクトリの削除 2295
ファイルのコピー 2296
スタック内のスイッチから同じスタックの別のスイッチにファイルをコピーする 2296
ファイルの削除 2297
ファイルの作成、表示および抽出（CLI） 2298
その他の参考資料 2300
Cisco IOS XE ソフトウェア バンドルの使用 2303
ソフトウェアのバンドルとパッケージについて 2303
スイッチでのバンドルおよびパッケージ ファイルの場所 2303
Cisco IOS XE ソフトウェアのアップグレード 2304
Cisco IOS XE ソフトウェアのアップグレード：インストール モード 2304
Cisco IOS XE ソフトウェア インストール モードのアップグレードの例 2305
Cisco IOS XE ソフトウェアのアップグレード：バンドル モード 2305
Cisco IOS XE ソフトウェア バンドル モードのアップグレード例 2306
バンドル実行モードからインストール実行モードに変換 2306
バンドル実行モードからインストール実行モード変換例 2307

1 台のスタック メンバから他のスタック メンバへの IOS XE パッケージおよびバンドル ファイルのコピー 2308
1 つのスタック メンバから別のスタック メンバに IOS XE パッケージおよびバンドル ファイルをコピーする例 2308
互換性のないソフトウェアを実行しているスイッチのアップグレード 2309
互換性のないソフトウェアを実行するスイッチのアップグレード例 2310
互換性のない実行モードで実行中のスイッチのアップグレード 2311
互換性のない実行モードで実行中のスイッチのアップグレード例 2311
その他の参考資料 2313
条件付きデバッグおよび放射線トレース 2315
機能情報の確認 2315
条件付きデバッグの概要 2316
ラジオアクティブ トレースの概要 2316
条件付きデバッグおよび放射線トレース 2316
トレースファイルの場所 2317
条件付きデバッグの設定 2317
トレース ファイルの推奨ワークフロー 2320
ボックス外へのトレース ファイルのコピー 2320
条件付きデバッグ設定の例 2321
条件付きデバッグのモニタリング 2322
ソフトウェア設定のトラブルシューティング 2323
機能情報の確認 2323
ソフトウェア設定のトラブルシューティングに関する情報 2324
スイッチのソフトウェア障害 2324
スイッチのパスワードを紛失したか忘れた場合 2324
Power over Ethernet（PoE）ポート 2324
電力消失によるポートの障害 2325
不正リンク アップによるポート障害 2325
ping 2325
レイヤ 2 Traceroute 2326
レイヤ 2 の traceroute のガイドライン 2326
IP Traceroute 2327
Time Domain Reflector ガイドライン 2328

debug コマンド 2329

システム レポート 2329

スイッチのオンボード障害ロギング 2331

ファン障害 2332

CPU 使用率が高い場合に起こりうる症状 2333

ソフトウェア設定のトラブルシューティング方法 2333

ソフトウェア障害からの回復 2333

パスワードを忘れた場合の回復 2335

パスワード回復がイネーブルになっている場合の手順 2337

パスワード回復がディセーブルになっている場合の手順 2339

スイッチ スタック問題の回避 2340

自動ネゴシエーションの不一致の防止 2341

SFP モジュールのセキュリティと識別に関するトラブルシューティング 2342

SFP モジュール ステータスのモニタリング 2343

ping の実行 2343

温度のモニタリング 2343

物理パスのモニタリング 2344

IP traceroute の実行 2344

TDR の実行および結果の表示 2344

デバッグおよびエラー メッセージ出力のリダイレクト 2345

show platform forward コマンドの使用 2345

show debug コマンドの使用方法 2345

OBFL の設定 2346

ソフトウェア設定のトラブルシューティングの確認 2347

OBFL 情報の表示 2347

例：高い CPU 使用率に関する問題と原因の確認 2348

ソフトウェア設定のトラブルシューティングのシナリオ 2350

Power over Ethernet（PoE）に関するトラブルシューティングのシナリオ 2350

ソフトウェアのトラブルシューティングの設定例 2354

例：IP ホストの ping 2354

例：IP ホストに対する traceroute の実行 2355

例：すべてのシステム診断をイネーブルにする 2356

ソフトウェア設定のトラブルシューティングに関する追加情報 2357
ソフトウェア設定のトラブルシューティングの機能履歴と情報 2358
VideoStream 2359
VideoStream の設定 2361
機能情報の確認 2361
VideoStream の前提条件 2361
VideoStream の設定に関する制限 2362
VideoStream について 2362
VideoStream の設定方法 2362
メディア ストリームのマルチキャストダイレクトのグローバル設定 2362
802.11 帯域のメディア ストリームの設定 2364
ビデオ ストリーミング用の WLAN 設定 2366
メディア ストリームの削除 2367
メディア ストリームの監視 2368
VLAN 2369
VTP の設定 2371
機能情報の確認 2371
VTP の前提条件 2372
VTP の制約事項 2372
VTP の概要 2373
VTP 2373
VTP Domain 2373
VTP モード 2374
VTP アドバタイズ 2375
VTP バージョン 2 2376
VTP バージョン 3 2377
VTP プルーニング 2378
VTP とスイッチ スタック 2379
VTP 設定時の注意事項 2380
VTP の設定要件 2380
VTP の設定 2380
VTP 設定のためのドメイン名 2381
VTP ドメインのパスワード 2381

VTP Version 2381
VTP の設定方法 2383
VTP モードの設定（CLI） 2383
VTP バージョン 3 のパスワードの設定（CLI） 2385
VTP バージョン 3 のプライマリ サーバの設定（CLI） 2387
VTP バージョンのイネーブル化（CLI） 2388
VTP プルーニングのイネーブル化（CLI） 2390
ポート単位の VTP の設定（CLI） 2391
VTP ドメインへの VTP クライアント スイッチの追加（CLI） 2393
VTP のモニタ 2396
VTP の設定例 2397
例：スイッチをプライマリ サーバとして設定する 2397
次の作業 2397
その他の参考資料 2397
VTP の機能履歴と情報 2399
VLAN の設定 2401
機能情報の確認 2401
VLAN の前提条件 2401
VLAN の制約事項 2402
VLAN について 2402
論理ネットワーク 2402
サポートされる VLAN 2403
VLAN ポート メンバーシップ モード 2405
VLAN コンフィギュレーション ファイル 2406
標準範囲 VLAN 設定時の注意事項 2406
拡張範囲 VLAN 設定時の注意事項 2408
VLAN の設定方法 2409
標準範囲 VLAN の設定方法 2409
イーサネット VLAN の作成または変更（CLI） 2410
VLAN の削除（CLI） 2412
VLAN へのスタティック アクセス ポートの割り当て（CLI） 2414
拡張範囲 VLAN の設定方法 2417

拡張範囲 VLAN の作成（CLI） 2417

VLAN の設定方法（GUI） 2419

VLAN のモニタリング 2419

次の作業 2422

その他の参考資料 2422

VLAN の機能履歴と情報 2424

VLAN グループの設定 2425

機能情報の確認 2425

VLAN グループの前提条件 2425

VLAN グループの制約事項 2426

VLAN グループについて 2426

VLAN グループの設定方法 2427

VLAN グループの作成（CLI） 2427

VLAN グループの削除（CLI） 2428

WLAN への VLAN グループの追加（CLI） 2429

VLAN グループの VLAN の表示（CLI） 2429

次の作業 2430

その他の参考資料 2430

VLAN グループの機能履歴と情報 2432

VLAN トランクの設定 2433

機能情報の確認 2433

VLAN トランクの前提条件 2433

VLAN トランクの制約事項 2434

VLAN トランクについて 2435

トランキングの概要 2435

トランキング モード 2435

レイヤ 2 インターフェイス モード 2436

トランクでの許可 VLAN 2437

トランク ポートでの負荷分散 2438

STP プライオリティによるネットワーク負荷分散 2438

STP パス コストによるネットワーク負荷分散 2438

機能の相互作用 2438

VLAN トランクの設定方法 2439
トランク ポートとしてのイーサネット インターフェイスの設定 2439
トランク ポートの設定（CLI） 2439
トランクでの許可 VLAN の定義（CLI） 2442
プルーニング適格リストの変更（CLI） 2444
タグなしトラフィック用ネイティブ VLAN の設定（CLI） 2446
トランク ポートの負荷分散の設定 2448
STP ポート プライオリティによる負荷分散の設定（CLI） 2448
STP パス コストによる負荷分散の設定（CLI） 2453
次の作業 2456
その他の参考資料 2456
VLAN トランクの機能履歴と情報 2458
音声 VLAN の設定 2459
機能情報の確認 2459
音声 VLAN の前提条件 2459
音声 VLAN の制約事項 2460
音声 VLAN に関する情報 2460
音声 VLAN 2460
Cisco IP Phone の音声トラフィック 2460
Cisco IP Phone のデータ トラフィック 2461
音声 VLAN 設定時の注意事項 2461
音声 VLAN の設定方法 2463
Cisco IP Phone の音声トラフィックの設定（CLI） 2463
着信データ フレームのプライオリティ設定（CLI） 2465
音声 VLAN のモニタリング 2467
次の作業 2467
その他の参考資料 2468
音声 VLAN の機能履歴と情報 2469
プライベート VLAN の設定 2471
機能情報の確認 2471
プライベート VLAN の前提条件 2471
プライベート VLAN の制約事項 2472

プライベート VLAN について 2473
プライベート VLAN ドメイン 2473
Secondary VLANs 2474
プライベート VLAN ポート 2474
ネットワーク内のプライベート VLAN 2476
プライベート VLAN での IP アドレッシング方式 2476
複数のスイッチにまたがるプライベート VLAN 2477
プライベート VLAN の他機能との相互作用 2477
プライベートVLANとユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック 2477
プライベート VLAN と SVI 2478
プライベート VLAN とスイッチ スタック 2479
ダイナミック MAC アドレスを備えたプライベート VLAN 2479
スタティック MAC アドレスのプライベート VLAN 2479
プライベート VLAN と VACL/QOS との相互作用 2480
プライベート VLAN および HA サポート 2481
プライベート VLAN 設定時の注意事項 2481
プライベート VLAN のデフォルト設定 2481
セカンダリ VLAN およびプライマリ VLAN の設定 2481
プライベート VLAN ポートの設定 2483
プライベート VLAN の設定方法 2484
プライベート VLAN の設定 2484
プライベート VLAN 内の VLAN の設定および対応付け 2485
プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 2489
プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 2491
セカンダリ VLANのプライマリ VLAN レイヤ3VLANインターフェイスへのマッピング 2494
プライベート VLAN のモニタ 2496
プライベート VLAN の設定例 2496
例：プライベート VLAN 内の VLAN の設定および関連付け 2496
例：ホスト ポートとしてのインターフェイスの設定 2497
例：インターフェイスをプライベート VLAN 無差別ポートとして設定する 2498

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする 2498
例：プライベート VLAN のモニタリング 2499
次の作業 2499
その他の参考資料 2499
WLAN 2503
WLAN の設定 2505
機能情報の確認 2505
WLAN の前提条件 2505
WLAN の制約事項 2506
WLAN について 2507
バンドの選択 2508
オフチャネル スキャンの延期 2508
DTIM Period 2509
セッション タイムアウト 2510
Cisco Client Extensions 2510
ピアツーピア ブロッキング 2510
診断チャネル 2511
WLAN ごとの RADIUS 送信元サポート 2511
WLAN の設定方法 2512
WLAN の作成（CLI） 2512
WLAN の削除（CLI） 2513
WLAN の検索（CLI） 2513
WLAN のイネーブル化（CLI） 2514
WLAN のディセーブル（CLI） 2515
汎用 WLAN プロパティの設定（CLI） 2516
高度な WLAN プロパティの設定（CLI） 2519
WLAN プロパティの監視（CLI） 2522
次の作業 2522
その他の参考資料 2522
WLANs の機能情報 2524
DHCP for WLANs の設定 2525
機能情報の確認 2525

DHCP for WLANs を設定するための前提条件 2525
DHCP for WLANs の設定に関する制約事項 2527
Dynamic Host Configuration Protocol について 2527
内部 DHCP サーバ 2528
外部 DHCP サーバ 2528
DHCP 割り当て 2529
DHCP オプション 82 について 2530
DHCP スコープの設定 2531
DHCP スコープについて 2531
DHCP for WLANs の設定方法 2532
WLAN 用の DHCP 設定（CLI） 2532
DHCP スコープの設定（CLI） 2534
その他の参考資料 2535
DHCP for WLANs の機能情報 2536
WLAN セキュリティの設定 2537
機能情報の確認 2537
レイヤ 2 セキュリティの前提条件 2537
AAA Override について 2538
WLAN セキュリティの設定方法 2539
静的 WEP と 802.1X レイヤ 2 セキュリティ パラメータの設定（CLI） 2539
静的 WEP レイヤ 2 セキュリティ パラメータの設定（CLI） 2540
WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（CLI） 2541
802.1X レイヤ 2 セキュリティ パラメータの設定（CLI） 2543
その他の参考資料 2544
WLAN レイヤ 2 セキュリティに関する機能情報 2545
WLAN ごとのクライアント カウントの設定 2547
機能情報の確認 2547
WLAN ごとのクライアント カウントの設定に関する制約事項 2547
WLAN ごとのクライアント カウントの設定について 2548
WLAN ごとのクライアント カウントを設定する方法 2549
WLAN ごとのクライアント カウントの設定（CLI） 2549
WLAN ごとの各 AP のクライアント数の設定（CLI） 2550

WLAN あたりの AP 無線ごとのクライアント数の設定（CLI） 2551
クライアントの接続の監視（CLI） 2551
クライアント接続に関する追加情報 2552
WLAN ごとのクライアント接続に関する機能情報 2553
802.11w の設定 2555
機能情報の確認 2555
802.11w の前提条件 2555
802.11w の制約事項 2556
802.11w に関する情報 2556
802.11w の設定方法 2557
802.11w の設定（CLI） 2557
802.11w のディセーブル（CLI） 2559
802.11w の監視（CLI） 2561
802.11w に関する追加情報 2562
802.11w の機能に関する情報 2563
Wi-Fi Direct クライアント ポリシーの設定 2565
機能情報の確認 2565
Wi-Fi Direct クライアント ポリシーの制限 2565
Wi-Fi Direct クライアント ポリシーについて 2566
Wi-Fi Direct クライアント ポリシーの設定方法 2566
Wi-Fi Direct クライアント ポリシーの設定（CLI） 2566
Wi-Fi Direct クライアント ポリシーのディセーブル（CLI） 2568
Wi-Fi Direct クライアント ポリシーの監視（CLI） 2568
Wi-Fi Direct クライアント ポリシーに関する追加リファレンス 2569
Wi-Fi Direct クライアント ポリシーに関する機能情報 2570
802.11r BSS の高速移行の設定 2571
機能情報の確認 2571
802.11r 高速移行の制約事項 2571
802.11r の高速移行について 2572
802.11r 高速移行を設定する方法 2576
オープン WLAN での 802.11r 高速移行の設定（CLI） 2576
Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI） 2578

PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI） 2579
802.11r 高速移行のディセーブル（CLI） 2581
802.11r 高速移行の監視（GUI） 2582
802.11r 高速移行の監視（CLI） 2582
802.11r 高速移行に関する追加情報 2584
802.11r 高速移行の機能に関する情報 2585
経由ローミングの設定 2587
機能情報の確認 2587
経由ローミングの制約事項 2587
経由ローミングについて 2588
経由ローミングの設定方法 2590
経由ローミングの設定（CLI） 2590
経由ローミングの監視 2591
経由ローミングの設定例 2592
経由ローミングに関する追加情報 2593
経由ローミング設定の機能履歴と情報 2594
アクセス ポイント グループの設定 2595
機能情報の確認 2595
AP グループを設定するための前提条件 2595
アクセス ポイント グループの設定に関する制約事項 2596
アクセス ポイント グループについて 2596
アクセス ポイント グループの設定方法 2597
アクセス ポイント グループの作成 2597
AP グループへのアクセス ポイントの割り当て 2598
アクセス ポイント グループの表示 2599
その他の参考資料 2600
アクセス ポイント グループの機能履歴と情報 2601

はじめに

- 表記法，xcix ページ
- 関連資料，ci ページ
- マニュアルの入手方法およびテクニカル サポート，ci ページ

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
`太字の courier` フォント	**`太字の courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。

表記法	説明
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス　時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。ステートメント 1071

これらの注意事項を保管しておいてください。

関連資料

（注）　スイッチをインストールまたはアップグレードする前に、スイッチのリリース ノートを参照してください。

- 次の URL にある Cisco Catalyst 3650 スイッチのマニュアル：
  http://www.cisco.com/go/cat3650_docs
- 次の URL にある Cisco SFP、SFP+、および QSFP+ モジュールのマニュアル（互換性マトリクスを含む）：
  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- 次の URL にあるエラー メッセージ デコーダ：
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

コマンドライン インターフェイスの使用

- コマンドライン インターフェイスの使用に関する情報，1 ページ
- CLI を使用して機能を設定する方法，8 ページ

コマンドライン インターフェイスの使用に関する情報

コマンド モード

Cisco IOS ユーザ インターフェイスは、いくつかのモードに分かれています。使用可能なコマンドは、現在のモードによって異なります。各コマンド モードで使用できるコマンドのリストを取得するには、システム プロンプトで疑問符（?）を入力します。

CLI セッションを開始するには、コンソール接続、Telnet、SSH、またはブラウザを使用できます。

セッションを開始するときは、ユーザ モード（別名ユーザ EXEC モード）が有効です。ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。たとえばユーザ EXEC コマンドの大部分は、**show** コマンド（現在のコンフィギュレーション ステータスを表示する）、**clear** コマンド（カウンタまたはインターフェイスをクリアする）などのように、1 回限りのコマンドです。ユーザ EXEC コマンドは、スイッチをリブートするときには保存されません。

すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードが必要です。このモードでは、任意の特権 EXEC コマンドを入力でき、また、グローバル コンフィギュレーション モードを開始することもできます。

コンフィギュレーション モード（グローバル、インターフェイス、およびライン）を使用して、実行コンフィギュレーションを変更できます。設定を保存した場合はこれらのコマンドが保存され、スイッチをリブートするときに使用されます。各種のコンフィギュレーション モードにアクセスするには、まずグローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードを開始できます。

次の表に、主要なコマンド モード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。

表 *1*：コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	Telnet、SSH、またはコンソールを使用してセッションを開始します。	スイッチ>	**logout** または **quit** を入力します。	このモードを使用して次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	スイッチ#	**disable** を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	スイッチ(config)#	終了して特権 EXEC モードに戻るには、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。	このモードは、スイッチ全体に適用するパラメータを設定する場合に使用します。
VLAN コンフィギュレーション	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	スイッチ(config-vlan)#		

モード	アクセス方法	プロンプト	終了方法	モードの用途
			グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、VLAN（仮想LAN）パラメータを設定します。VTP モードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が 1006 以上）を作成してスイッチのスタートアップ コンフィギュレーション ファイルに設定を保存できます。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを入力し、インターフェイスを指定します。	`スイッチ(config-if)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、イーサネット ポートのパラメータを設定します。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで、**line vty** または **line console** コマンドを使用して回線を指定します。	`スイッチ(config-line)#`		このモードを使用して、端末回線のパラメータを設定します。

モード	アクセス方法	プロンプト	終了方法	モードの用途
			終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	

コマンドの省略形

スイッチでコマンドが一意に認識される長さまでコマンドを入力します。

show configuration 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
スイッチ# show conf
```

コマンドの no 形式および default 形式

大部分のコンフィギュレーション コマンドに、**no** 形式があります。**no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスのシャットダウンが取り消されます。**no** キーワードなしでコマンドを使用すると、ディセーブルにされた機能を再度イネーブルにしたり、デフォルトでディセーブルになっている機能をイネーブルにすることができます。

コンフィギュレーション コマンドには、**default** 形式もあります。コマンドの **default** 形式は、コマンドの設定値をデフォルトに戻します。大部分のコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じになります。ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。これらのコマンドについては、**default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI のエラー メッセージ

次の表に、CLI を使用してスイッチを設定するときに表示される可能性のあるエラー メッセージの一部を紹介します。

表 *2*：*CLI* の代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	スイッチがコマンドとして認識できるだけの文字数が入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを入れません。 コマンドとともに使用できるキーワードが表示されます。
`% Incomplete command.`	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。間違っている箇所をキャレット（^）記号で示しています。	疑問符（?）を入力すると、そのコマンド モードで利用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギング

スイッチの設定変更を記録して表示させることができます。Configuration Change Logging and Notification 機能を使用することで、セッションまたはユーザ ベースごとに変更内容をトラッキングできます。ログに記録されるのは、適用された各コンフィギュレーション コマンド、コマンドを入力したユーザ、コマンドの入力時間、コマンドに対するパーサからのリターン コードです。この機能には、登録しているアプリケーションの設定が変更されるときに通知される非同期通知方式もあります。Syslog へこの通知を送信することも選択できます。

（注） CLI または HTTP の変更のみがログとして記録されます。

ヘルプ システムの使用

システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。

手順の概要

1. **help**
2. *abbreviated-command-entry***?**
3. *abbreviated-command-entry* <Tab>
4. **?**
5. *command***?**
6. *command keyword***?**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**help** 例： スイッチ# **help**	コマンド モードのヘルプ システムの簡単な説明を表示します。
ステップ 2	*abbreviated-command-entry***?** 例： スイッチ# **di?** dir disable disconnect	特定のストリングで始まるコマンドのリストを表示します。
ステップ 3	*abbreviated-command-entry* <Tab> 例： スイッチ# **sh conf**<tab> スイッチ# **show configuration**	特定のコマンド名を補完します。
ステップ 4	**?** 例： スイッチ> **?**	特定のコマンド モードで使用可能なすべてのコマンドをリストします。
ステップ 5	*command***?** 例： スイッチ> **show ?**	コマンドに関連するキーワードを一覧表示します。

	コマンドまたはアクション	目的
ステップ 6	*command keyword*? 例： スイッチ(config)# **cdp holdtime ?** <10-255> Length of time (in sec) that receiver must keep this packet	キーワードに関連する引数を一覧表示します。

CLI を使用して機能を設定する方法

コマンド履歴の設定

入力したコマンドは、ソフトウェア側にコマンド履歴として残されます。コマンド履歴機能は、アクセスコントロールリストの設定時など、長い複雑なコマンドまたはエントリを何度も入力しなければならない場合、特に便利です。必要に応じて、この機能をカスタマイズできます。

コマンド履歴バッファ サイズの変更

デフォルトでは、スイッチは履歴バッファにコマンドライン10行を記録します。現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。この手順は任意です。

手順の概要

1. **terminal history** [**size** *number-of-lines*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal history** [**size** *number-of-lines*] 例： スイッチ# **terminal history size 200**	特権 EXEC モードで現在のターミナル セッション中にスイッチが記録するコマンドラインの数を変更します。サイズは 0 から 256 までの間で設定できます。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、次の表に示すいずれかの操作を行います。これらの操作は任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

手順の概要

1. **Ctrl+P** または**上矢印**キー
2. **Ctrl+N** または**下矢印**キー
3. **show history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**Ctrl+P** または**上矢印**キー	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
ステップ 2	**Ctrl+N** または**下矢印**キー	**Ctrl+P** または上矢印キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。
ステップ 3	**show history** 例： `スイッチ# show history`	特権 EXEC モードで、直前に入力したコマンドをいくつか表示します。表示されるコマンドの数は、**terminal history** グローバル コンフィギュレーション コマンドおよび **history** ライン コンフィギュレーション コマンドの設定値によって制御されます。

コマンド履歴機能の無効化

コマンド履歴機能は、自動的にイネーブルになっています。現在の端末セッションまたはコマンドラインでディセーブルにできます。この手順は任意です。

手順の概要

1. **terminal no history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal no history** 例： スイッチ# **terminal no history**	特権 EXEC モードで現在のターミナル セッション中のこの機能を無効にします。

編集機能の有効化および無効化

拡張編集モードは自動的にイネーブルに設定されますが、ディセーブルにしたり、再びイネーブルにしたりできます。

手順の概要

1. **terminal editing**
2. **terminal no editing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal editing** 例： スイッチ# **terminal editing**	特権 EXEC モードで現在のターミナル セッションにおける拡張編集モードを再び有効にします。
ステップ 2	**terminal no editing** 例： スイッチ# **terminal no editing**	特権 EXEC モードで現在のターミナル セッションにおける拡張編集モードを無効にします。

キー入力によるコマンドの編集

キーストロークは、コマンドラインの編集に役立ちます。これらのキーストロークは任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 *3* : 編集コマンド

編集コマンド	説明
Ctrl+B または**左矢印**キー	カーソルを 1 文字後退させます。
Ctrl+F または**右矢印**キー	カーソルを 1 文字前進させます。
Ctrl+A	コマンドラインの先頭にカーソルを移動します。
Ctrl+E	カーソルをコマンド ラインの末尾に移動します。
Esc B	カーソルを 1 単語後退させます。
Esc F	カーソルを 1 単語前進させます。
Ctrl+T	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
Delete キーまたは **Backspace** キー	カーソルの左にある文字を消去します。
Ctrl+D	カーソル位置にある文字を削除します。
Ctrl+K	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
Ctrl+U または **Ctrl+X**	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
Ctrl+W	カーソルの左にある単語を削除します。
Esc D	カーソルの位置から単語の末尾までを削除します。
Esc C	カーソル位置のワードを大文字にします。
Esc L	カーソルの場所にある単語を小文字にします。
Esc U	カーソルの位置から単語の末尾までを大文字にします。
Ctrl+V または **Esc Q**	特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。

Return キー	1 行または 1 画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 （注） **show** コマンドの出力など、端末画面に一度に表示できない長い出力では、More プロンプトが使用されます。More プロンプトが表示された場合は、Return キーおよび Space キーを使用してスクロールできます。
Space バー	1 画面分下にスクロールします。
Ctrl+L または **Ctrl+R**	スイッチから画面に突然メッセージが出力された場合に、現在のコマンドラインを再表示します。

画面幅よりも長いコマンドラインの編集

画面上で 1 行分を超える長いコマンドラインについては、コマンドのラップアラウンド機能を使用できます。カーソルが右マージンに達すると、そのコマンドラインは 10 文字分だけ左へシフトされます。コマンドラインの先頭から 10 文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。これらのキー操作は任意です。

コマンドの先頭にスクロールして入力内容をチェックするには、Ctrl+B キーまたは左矢印キーを繰り返し押します。コマンドラインの先頭に直接移動するには、Ctrl+A を押します。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次に、画面上で 1 行を超える長いコマンドラインを折り返す例を示します。

手順の概要

1. **access-list**
2. **Ctrl+A**
3. **Return** キー

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**access-list** 例： スイッチ(config)# **access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35** スイッチ(config)# $ **101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25** スイッチ(config)# $**t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq** スイッチ(config)# $**15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45**	1 行分を超えるグローバル コンフィギュレーション コマンド入力を表示します。 最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。ドル記号（$）は、その行が左へスクロールされたことを表します。カーソルが行末に達するたびに、その行は再び 10 文字分だけ左へシフトされます。
ステップ 2	**Ctrl+A** 例： スイッチ(config)# **access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$**	完全な構文をチェックします。 行末に表示されるドル記号（$）は、その行が右へスクロールされたことを表します。
ステップ 3	**Return** キー	コマンドを実行します。 ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。画面の幅が異なる場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。 ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンド エントリを呼び出して変更できます。

show および more コマンド出力の検索およびフィルタリング

show および **more** コマンドの出力を検索およびフィルタリングできます。この機能は、大量の出力をソートする場合や、出力から不要な情報を除外する場合に役立ちます。これらのコマンドの使用は任意です。

手順の概要

1. {**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	{**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression* 例： スイッチ# **show interfaces | include protocol** Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up	出力を検索およびフィルタリングします。 文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、**output** を含む行は表示されませんが、**Output** を含む行は表示されます。

スイッチ スタックでの CLI へのアクセス

CLI にはコンソール接続、Telnet、SSH、またはブラウザを使用することによってアクセスできます。

スイッチ スタックおよびスタック メンバ インターフェイスは、アクティブ スイッチを経由して管理します。スイッチごとにスタック メンバを管理することはできません。1 つまたは複数のスタック メンバーのコンソール ポートまたはイーサネット管理ポートを経由してアクティブ スイッチへ接続できます。アクティブ スイッチで複数の CLI セッションを使用する場合は注意してください。1 つのセッションで入力したコマンドは、別のセッションには表示されません。したがって、コマンドを入力したセッションを追跡できない場合があります。

（注） スイッチ スタックを管理する場合は、1 つの CLI セッションを使用することを推奨します。

特定のスタック メンバ ポートを設定する場合は、CLI コマンド インターフェイス表記にスタック メンバ番号を含めてください。

スタンバイ スイッチをデバッグするには、アクティブなスイッチから **session standby ios** 特権 EXEC コマンドを使用してスタンバイ スイッチの IOS コンソールにアクセスします。特定のスタック メンバをデバッグするには、アクティブなスイッチから **session switch***stack-member-number* 特権 EXEC コマンドを使用して、スタック メンバの診断シェルにアクセスします。これらのコマンドの詳細情報については、スイッチ コマンド リファレンスを参照してください。

コンソール接続または Telnet 経由での CLI へのアクセス

CLI にアクセスするには、端末または PC をスイッチ コンソールに接続した後、または PC をイーサネット管理ポートに接続した後に、スイッチの電源をオンにする必要があります。その手順については、スイッチに付属のハードウェア インストール ガイドに記載されています。

スイッチがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッションによって CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にスイッチを設定しておく必要があります。

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチ コンソール ポートを管理ステーションまたはダイヤルアップ モデムに接続するか、イーサネット管理ポートを PC に接続します。コンソール ポートまたはイーサネット管理ポートへの接続方法については、スイッチのハードウェア インストレーション ガイドを参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化セキュア シェル（SSH）パッケージを使用します。スイッチは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、スイッチにイネーブル シークレット パスワードを設定しておくことも必要です。
  - スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。
  - スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

  コンソール ポート、イーサネット管理ポート、Telnet セッション、または SSH セッションを通じて接続すると、管理ステーション上にユーザ EXEC プロンプトが表示されます。

第 I 部

CleanAir

- Cisco CleanAir の設定，19 ページ

第 2 章

Cisco CleanAir の設定

- 機能情報の確認，19 ページ
- CleanAir の前提条件，19 ページ
- CleanAir の制約事項，20 ページ
- CleanAir について，21 ページ
- CleanAir の設定方法，27 ページ
- コントローラの GUI を使用した Cisco CleanAir の設定，37 ページ
- Cisco Spectrum Expert の設定，37 ページ
- CleanAir パラメータのモニタリング，39 ページ
- CleanAir の設定例，42 ページ
- CleanAir に関する FAQ，43 ページ
- その他の参考資料，45 ページ

機能情報の確認

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

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

CleanAir の前提条件

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

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

- Local：このモードでは、Cisco CleanAir 対応の各アクセス ポイント無線によって、現在の動作チャネルだけに関する電波品質と干渉検出のレポートが作成されます。
- Monitor：Cisco CleanAir が監視モードで有効になっていると、そのアクセス ポイントによって、モニタされているすべてのチャネルに関する電波品質と干渉検出のレポートが作成されます。

  次のオプションを使用できます。

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

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

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

関連トピック

2.4 GHz 帯域の CleanAir のイネーブル化, （27 ページ）
2.4 GHz での電波品質とデバイスの CleanAir アラームの設定, （28 ページ）
2.4 GHz デバイスの干渉レポートの設定, （30 ページ）
5 GHz 帯域の CleanAir のイネーブル化, （31 ページ）
5 GHz での電波品質とデバイスの CleanAir アラームの設定, （32 ページ）
5 GHz デバイスの干渉レポートの設定, （34 ページ）

CleanAir の制約事項

- 監視モードのアクセス ポイントは、Wi-Fi トラフィックまたは 802.11 パケットを送信しません。これらは Radio Resource Management（RRM）計画から除外され、隣接アクセス ポイン

トのリストに含まれません。IDR クラスタリングは、スイッチがネットワーク内の隣接アクセス ポイントを検出する機能に依存しています。複数のアクセス ポイントから関係する干渉デバイスを検出する機能を使用できるのは、監視モードのアクセス ポイント間に限られます。

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

関連トピック

2.4 GHz 帯域の CleanAir のイネーブル化, （27 ページ）
2.4 GHz での電波品質とデバイスの CleanAir アラームの設定, （28 ページ）
2.4 GHz デバイスの干渉レポートの設定, （30 ページ）
5 GHz 帯域の CleanAir のイネーブル化, （31 ページ）
5 GHz での電波品質とデバイスの CleanAir アラームの設定, （32 ページ）
5 GHz デバイスの干渉レポートの設定, （34 ページ）

CleanAir について

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

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

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

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

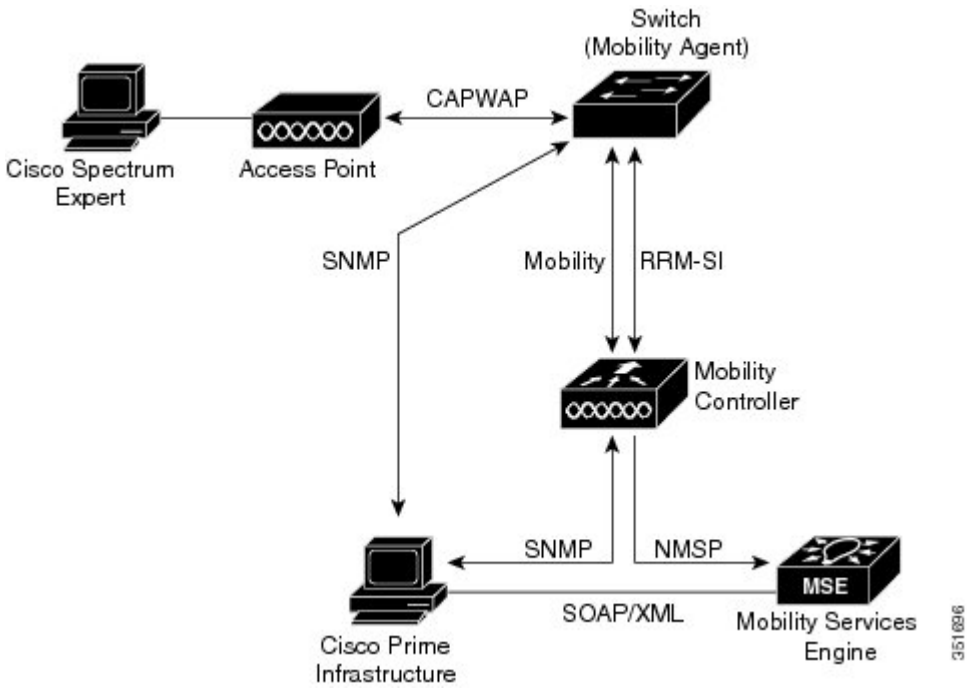
ワイヤレス LAN システムは、ライセンス不要の 2.4 GHz および 5 GHz ISM 帯域で動作します。この帯域では電子レンジ、コードレス電話、Bluetooth デバイスなどの多数の機器が動作しているため、Wi-Fi の動作に悪影響が生じる可能性があります。

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

Cisco CleanAir のコンポーネント

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

図 *1*：*Cisco CleanAir* ソリューション



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

モビリティ コントローラ（MC）は CleanAir 対応のアクセス ポイントを制御および設定し、スペクトラム データを収集し、それを処理して PI および MSE に提供します。MC は CleanAir の基本機能およびサービスを設定し、現在のスペクトラム情報を表示するローカルユーザインターフェイス（GUI および CLI）を提供します。また、MC は、RRM TPC と DCM を使用して、干渉デバ

イスを検出、マージ、および軽減します。干渉デバイスのマージの詳細については、干渉デバイスのマージ，（25 ページ）を参照してください。

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

Cisco MSE は、干渉デバイスの場所および履歴の追跡に必要となるもので、複数のコントローラにわたる干渉レポートを調整および統合します。MSE は、包括的な Over-the-Air 脅威の検出、特定および軽減を行う適応型ワイヤレス侵入防御システム（WIPS）サービスも提供します。また、MSE は、すべての干渉データをマージします。

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

Cisco CleanAir システムにおいて、スイッチは次のような処理を実行します。

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

Cisco CleanAir で使用される用語

表 *4*：*CleanAir* 関連の用語

用語	説明
AQI	電波品質の指標。AQI は空気汚染物質に基づいた電波品質の指標です。AQI が 0 の場合は不良で、AQI が 85 より大きいと良好です。
AQR	電波品質レポート。AQR には特定されたすべての発生源からの干渉全体に関する情報（AQI で表される）や、最も重大な干渉カテゴリの概要が示されます。AQR は 15 分ごとにモビリティ コントローラに送信され、30 秒ごとに迅速モードで送信されます。

用語	説明
DC	デューティ サイクル。チャネルがデバイスで使用される時間の割合。
EDRRM	EDRRM イベント駆動型 RRM。EDRRM は、緊急事態にあるアクセス ポイントが、正常な RRM 間隔をバイパスし、すぐにチャネルを変更できるようにします。
IDR	アクセス ポイントがコントローラに送信する干渉デバイス レポート。
ISI	干渉の重大度指標。ISI は、干渉の重大度の指標です。
MA	モビリティ エージェント。MA は、ワイヤレス モジュールが実行されているアクセス スイッチか、内部 MA が実行されている MC です。MA は、モバイル クライアント（MA が実行されているデバイスへのアクセス ポイントに接続されている）用のクライアント モビリティのステート マシンを維持するワイヤレス コンポーネントです。
MC	モビリティ コントローラ。MC は、ピア グループ間のローミング イベントのモビリティ管理サービスを提供します。MC は管理用の一元的な接続ポイントを提供し、すべてのモビリティ エージェントのモビリティ設定、ピア グループ メンバーシップ、およびメンバーのリストのサブドメインに、設定を送信します。
RSSI	受信信号強度インジケータ。RSSI は受信した無線信号における電力の測定値です。アクセス ポイントはこの電力で干渉デバイスを認識します。

Cisco CleanAir で検出できる干渉の種類

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

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

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

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

- 永続的干渉

- 突発的干渉

永続的干渉イベントは、本質的に固定型のデバイスから発生し、断続的ではあるものの、干渉が大規模に反復して繰り返されるものを指します。たとえば、休憩室に設置してある電子レンジの場合を考えます。このような装置が動作するのは、1 回に付き 1 ～ 2 分程度です。しかし一旦動作すると、ワイヤレス ネットワークと、関係するクライアントのパフォーマンスに非常に大きな影響が生じます。Cisco CleanAir を使用すると、電子レンジなどの装置を無秩序なノイズとしてではなく明確に識別できるようになります。また、その装置によって影響を受ける帯域の部分を正確に特定できます。そして、その設置場所も特定できるため、最も大きな影響を受けるアクセス ポイントを判別することができます。そして、この情報を使用して RRM に指示し、範囲内にあるアクセス ポイントに対してこの干渉源を避けるようなチャネル計画を選択させることができます。この干渉は 1 日の大部分にわたって発生するものではないため、既存の RF 管理アプリケーションによって、影響を受けるアクセス ポイントのチャネルの再変更が試みられている場合もあります。しかし、永続的デバイスの回避は、干渉源が周期的に検出されて永続的な状態が新たに発生する限り影響があり続けるという点で独特です。Cisco CleanAir システムでは、電子レンジが存在することを認識し、それを将来のすべての計画に取り込みます。電子レンジまたはその近くのアクセス ポイントを移動させた場合は、このアルゴリズムによって RRM が自動的に更新されます。

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

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

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

干渉デバイスのマージ

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

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

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

永続的デバイス

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

永続的デバイスの検出

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

永続的デバイスの回避

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

EDRRM および AQR の更新モード

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

AQR は MC 上でのみ利用できます。モード設定およびタイマーは MA の無線制御ブロック（RCB）で保持されます（MA に接続された AP の場合）。EMS/NMS で利用できる最新の API の変更はありません。RCB（スペクトラムの設定およびタイマー）はローカルで使用可能なため、直接接続された AP には変更は必要ありません。リモート AP（MA に接続された AP）の場合は、3 つの新

しい制御メッセージが追加されています。この 3 つのメッセージは、特定の AP MAC アドレスおよびスロットに対するイネーブル、タイマーの再起動、迅速な更新モードのディセーブルについてです。

関連トピック

CleanAir-Events の EDRRM の設定, （35 ページ）

CleanAir ハイ アベイラビリティ

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

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

CleanAir の設定方法

2.4 GHz 帯域の CleanAir のイネーブル化

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz cleanair**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz cleanair** 例： スイッチ(config)#**ap dot11 24ghz cleanair**	802.11b ネットワークでの CleanAir 機能をイネーブルにします。802.11b ネットワークでの CleanAir をディセーブルにするには、このコマンドに no を追加します。

	コマンドまたはアクション	目的
	スイッチ(config)#**no ap dot11 24ghz cleanair**	
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件, （19 ページ）
CleanAir の制約事項, （20 ページ）
CleanAir に関する FAQ, （43 ページ）

2.4 GHz での電波品質とデバイスの CleanAir アラームの設定

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz cleanair alarm air-quality threshold** *threshold_value*
3. **ap dot11 24ghz cleanair alarm device** {**bt-discovery | bt-link | canopy | cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile | xbox | zigbee** }
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz cleanair alarm air-quality threshold** *threshold_value* 例： スイッチ(config)#**ap dot11 24ghz cleanair alarm air-quality threshold 50**	すべての 2.4 GHz デバイスについて、電波品質のしきい値のアラームを設定します。アラームをディセーブルにするには、このコマンドの no 形式を追加します。

	コマンドまたはアクション	目的
ステップ 3	**ap dot11 24ghz cleanair alarm device** {**bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee** } 例： `スイッチ(config)#ap dot11 24ghz cleanair alarm device canopy`	2.4 GHz デバイスのアラームを設定します。アラームをディセーブルにするには、no 形式のコマンドを追加します。 • **bt-discovery**：Bluetooth の検出。 • **bt-link**：Bluetooth リンク。 • **canopy**：Canopy デバイス。 • **cont-tx**：連続トランスミッタ。 • **dect-like**：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話。 • **fh**：802.11 周波数ホッピング デバイス。 • **inv**：スペクトラム反転 WiFi 信号を使用するデバイス。 • **jammer**：電波妨害装置。 • **mw-oven**：電子レンジ。 • **nonstd**：非標準 Wi-Fi チャネルを使用するデバイス。 • **report**：干渉デバイスのレポート。 • **superag**：802.11 SuperAG デバイス。 • **tdd-tx**：TDD トランスミッタ。 • **video**：ビデオ カメラ。 • **wimax-fixed**：WiMax 固定。 • **wimax-mobile**：WiMax モバイル。 • **xbox**：Xbox。 • **zigbee**：802.15.4 デバイス。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件, （19 ページ）
CleanAir の制約事項, （20 ページ）
CleanAir に関する FAQ, （43 ページ）

2.4 GHz デバイスの干渉レポートの設定

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz cleanair device**{**bt-discovery | bt-link | canopy | cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile | xbox | zigbee** }
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz cleanair device**{**bt-discovery	bt-link	canopy	cont-tx	dect-like	fh	inv	jammer	mw-oven	nonstd	report	superag	tdd-tx	video	wimax-fixed	wimax-mobile	xbox	zigbee** } 例： スイッチ(config)# **ap dot11 24ghz cleanair device bt-discovery** スイッチ(config)# **ap dot11 24ghz cleanair device bt-link** スイッチ(config)# **ap dot11 24ghz cleanair device canopy** スイッチ(config)# **ap dot11 24ghz cleanair device cont-tx** スイッチ(config)# **ap dot11 24ghz cleanair device dect-like** スイッチ(config)# **ap dot11 24ghz cleanair device fh** スイッチ(config)# **ap dot11 24ghz cleanair device inv** スイッチ(config)# **ap dot11 24ghz cleanair device jammer** スイッチ(config)# **ap dot11 24ghz cleanair device mw-oven** スイッチ(config)# **ap dot11 24ghz cleanair device nonstd** スイッチ(config)# **ap dot11 24ghz cleanair device**	スイッチに報告するように 2.4 GHz 干渉デバイスを設定します。設定をディセーブルにするには、このコマンドの no 形式を使用します。 • **bt-discovery**：Bluetooth の検出 • **bt-link**：Bluetooth リンク • **canopy**：Canopy デバイス • **cont-tx**：連続トランスミッタ • **dect-like**：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話 • **fh**：802.11 周波数ホッピング デバイス • **inv**：スペクトラム反転 WiFi 信号を使用するデバイス • **jammer**：電波妨害装置 • **mw-oven**：電子レンジ • **nonstd**：非標準 WiFi チャネルを使用するデバイス • **report**：説明なし • **superag**：802.11 SuperAG デバイス • **tdd-tx**：TDD トランスミッタ

	コマンドまたはアクション	目的
	report スイッチ(config)# **ap dot11 24ghz cleanair device superag** スイッチ(config)# **ap dot11 24ghz cleanair device tdd-tx** スイッチ(config)# **ap dot11 24ghz cleanair device video** スイッチ(config)# **ap dot11 24ghz cleanair device wimax-fixed** スイッチ(config)# **ap dot11 24ghz cleanair device wimax-mobile** スイッチ(config)# **ap dot11 24ghz cleanair device xbox** スイッチ(config)# **ap dot11 24ghz cleanair device zigbee**	• **video**：ビデオ カメラ • **wimax-fixed**：WiMax 固定 • **wimax-mobile**：WiMax モバイル • **xbox**：Xbox • **zigbee**：802.15.4 デバイス
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件, （19 ページ）
CleanAir の制約事項, （20 ページ）
CleanAir に関する FAQ, （43 ページ）

5 GHz 帯域の CleanAir のイネーブル化

手順の概要

1. **configure terminal**
2. **ap dot11 5ghz cleanair**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 5ghz cleanair** 例： スイッチ(config)#**ap dot11 5ghz cleanair** スイッチ(config)#**no ap dot11 5ghz cleanair**	802.11a ネットワークでの CleanAir 機能をイネーブルにします。802.11a ネットワークでの CleanAir をディセーブルにするには、このコマンドに no を追加します。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件, （19 ページ）
CleanAir の制約事項, （20 ページ）
CleanAir に関する FAQ, （43 ページ）

5 GHz での電波品質とデバイスの CleanAir アラームの設定

手順の概要

1. **configure terminal**
2. **ap dot11 5ghz cleanair alarm air-quality threshold** *threshold_value*
3. **ap dot11 5ghz cleanair alarm device**{**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **radar** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**}
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 5ghz cleanair alarm air-quality threshold** *threshold_value* 例： スイッチ(config)#**ap dot11 5ghz cleanair alarm air-quality threshold 50**	すべての 5 GHz デバイスについて、電波品質のしきい値のアラームを設定します。アラームをディセーブルにするには、このコマンドの no 形式を追加します。
ステップ 3	**ap dot11 5ghz cleanair alarm device**{**canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile**} 例： スイッチ(config)#**ap dot11 5ghz cleanair alarm device**	5 GHz デバイスのアラームを設定します。アラームをディセーブルにするには、このコマンドの no 形式を追加します。 • **canopy**：Canopy デバイス。 • **cont-tx**：連続トランスミッタ。 • **dect-like**：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話。 • **fh**：802.11 周波数ホッピング デバイス。 • **inv**：スペクトラム反転 WiFi 信号を使用するデバイス。 • **jammer**：電波妨害装置。 • **nonstd**：非標準 WiFi チャネルを使用するデバイス。 • **radar**：レーダー。 • **report**：干渉デバイスのレポート。 • **superag**：802.11 SuperAG デバイス。 • **tdd-tx**：TDD トランスミッタ。 • **video**：ビデオ カメラ。 • **wimax-fixed**：WiMax 固定。 • **wimax-mobile**：WiMax モバイル。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件, （19 ページ）
CleanAir の制約事項, （20 ページ）
CleanAir に関する FAQ, （43 ページ）

5 GHz デバイスの干渉レポートの設定

手順の概要

1. **configure terminal**
2. **ap dot11 5ghz cleanair device{canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile}**
3. **end**

手順の詳細

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

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

	コマンドまたはアクション	目的
	スイッチ(config)#**ap dot11 5ghz cleanair device radar** スイッチ(config)#**ap dot11 5ghz cleanair device report** スイッチ(config)#**ap dot11 5ghz cleanair device superag** スイッチ(config)#**ap dot11 5ghz cleanair device tdd-tx** スイッチ(config)#**ap dot11 5ghz cleanair device video** スイッチ(config)#**ap dot11 5ghz cleanair device wimax-fixed** スイッチ(config)#**ap dot11 5ghz cleanair device wimax-mobile**	• **superag**：802.11 SuperAG デバイス • **tdd-tx**：TDD トランスミッタ • **video**：ビデオ カメラ • **wimax-fixed**：WiMax 固定 • **wimax-mobile**：WiMax モバイル
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

CleanAir の前提条件, （19 ページ）
CleanAir の制約事項, （20 ページ）
CleanAir に関する FAQ, （43 ページ）

CleanAir-Events の EDRRM の設定

手順の概要

1. **configure terminal**
2. **ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event**
3. **ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** [**sensitivity** {**high** | **low** | **medium**}]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** 例： スイッチ(config)#**ap dot11 24ghz rrm channel cleanair-event** スイッチ(config)#**no ap dot11 24ghz rrm channel cleanair-event**	EDRRM の cleanair イベントをイネーブルにします。EDRRM をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** [**sensitivity** {**high** | **low** | **medium**}] 例： スイッチ(config)#**ap dot11 24ghz rrm channel cleanair-event sensitivity high**	cleanair-event の EDRRM の感度を設定します。 • [High]：電波品質（AQ）の値で示される、非 Wi-Fi 干渉に対する最も高い感度を指定します。 • [Low]：AQ の値で示される、非 Wi-Fi 干渉に対する最も低い感度を指定します。 • [Medium]：AQ の値で示される、非 Wi-Fi 干渉に対する中程度の感度を指定します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

EDRRM および AQR の更新モード，（26 ページ）

永続的デバイスの回避の設定

手順の概要

1. **configure terminal**
2. **ap dot11** {**24ghz** | **5ghz**} **rrm channel device**
3. **end**

手順の詳細

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

コントローラの GUI を使用した Cisco CleanAir の設定

Cisco Spectrum Expert の設定

Spectrum Expert の設定（CLI）

はじめる前に

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

- **show ap name** *ap_name* **config dot11** {**24ghz** | **5ghz**} コマンドを使用して、スイッチ CLI から NSI キーを確認できます。

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

例：
```
スイッチ#ap name Cisco_AP3500 mode se-connect
```

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

ステップ 3 次のコマンドを入力して、アクセス ポイントの NSI キーを表示します。
show ap name *ap_name* **config dot11** {**24ghz** | **5ghz**}

例：
```
スイッチ#show ap name Cisco_AP3500 config dot11 24ghz

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

<snippet>
```

次の作業

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

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

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

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

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

CleanAir パラメータのモニタリング

次のコマンドを使用して CleanAir パラメータをモニタできます。

表 *5*：*CleanAir* のモニタリング用コマンド

コマンド	説明
show ap dot11 24ghz cleanair air-quality summary	2.4 GHz 帯域の CleanAir 電波品質（AQ）のデータを表示します
show ap dot11 24ghz cleanair air-quality worst	2.4 GHz 帯域の CleanAir 電波品質（AQ）の最悪のデータを表示します
show ap dot11 24ghz cleanair config	2.4 GHz 帯域の CleanAir の設定を表示します
show ap dot11 24ghz cleanair device type all	2.4 GHz 帯域のすべての CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type bt-discovery	2.4 GHz 帯域の BT Discovery タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type bt-link	2.4 GHz 帯域の BT Link タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type canopy	2.4 GHz 帯域の Canopy タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type cont-tx	2.4 GHz 帯域の Continuous transmitter タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type dect-like	2.4 GHz 帯域の DECT Like タイプの CleanAir 干渉源を表示します

コマンド	説明
show ap dot11 24ghz cleanair device type fh	2.4 GHz 帯域の 802.11FH タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type inv	2.4 GHz 帯域の WiFi Inverted タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type jammer	2.4 GHz 帯域の Jammer タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type mw-oven	2.4 GHz 帯域の MW Oven タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type nonstd	2.4 GHz 帯域の WiFi Inv.Ch タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type persistent	2.4 GHz 帯域の Persistent タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type superag	2.4 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type tdd-tx	2.4 GHz 帯域の TDD Transmit タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type video	2.4 GHz 帯域の Video Camera タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type wimax-fixed	2.4 GHz 帯域の WiMax Fixed タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type wimax-mobile	2.4 GHz 帯域の WiMax Mobile タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type xbox	2.4 GHz 帯域の Xbox タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type zigbee	2.4 GHz 帯域の zigbee タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair air-quality summary	5 GHz 帯域の CleanAir 電波品質（AQ）のデータを表示します
show ap dot11 5ghz cleanair air-quality worst	5 GHz 帯域の CleanAir 電波品質（AQ）の最悪のデータを表示します

コマンド	説明
show ap dot11 5ghz cleanair config	5 GHz 帯域の CleanAir の設定を表示します
show ap dot11 5ghz cleanair device type all	5 GHz 帯域のすべての CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type canopy	5 GHz 帯域の Canopy タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type cont-tx	5 GHz 帯域の Continuous TX タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type dect-like	5 GHz 帯域の DECT Like タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type inv	5 GHz 帯域の WiFi Inverted タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type jammer	5 GHz 帯域の Jammer タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type nonstd	5 GHz 帯域の WiFi Inv.Ch タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type persistent	5 GHz 帯域の Persistent タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type superag	5 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type tdd-tx	5 GHz 帯域の TDD Transmit タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type video	5 GHz 帯域の Video Camera タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type wimax-fixed	5 GHz 帯域の WiMax Fixed タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type wimax-mobile	5 GHz 帯域の WiMax Mobile タイプの CleanAir 干渉源を表示します

干渉デバイスのモニタリング

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

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

CleanAir の設定例

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

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

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

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

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

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

5 GHz デバイスの干渉レポートの設定：例

次に、5 GHz デバイスの干渉レポートを設定する例を示します。

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

CleanAir-Events の EDRRM の設定：例

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

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

永続的デバイスの回避の設定：例

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

```
スイッチ#configure terminal
スイッチ(config)#ap dot11 24ghz rrm channel device
スイッチ(config)#end
```

SE-Connect モードのアクセス ポイントの設定：例

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

```
スイッチ#ap name Cisco_AP3500 mode se-connect
```

CleanAir に関する FAQ

Q. MC が稼働しているかどうかを確認するにはどうすればよいですか。

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

次に、モビリティ サマリーを表示する例を示します。

```
スイッチ#show wireless mobility summary

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

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

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

Q. スイッチを使用して 2 台のモニタ モード アクセス ポイントをマージできますか。

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

Q. ネイバー アクセス ポイントを表示するにはどうすればよいですか。

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

次に、ネイバー アクセス ポイントを表示する例を示します。

```
スイッチ#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz

<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0                          :  -12 dBm on   1 (10.10.0.5)
  AP 0C85.25AB.CCA0 slot 0                          :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25C7.B7A0 slot 0                          :  -26 dBm on  11 (10.10.0.5)
  AP 0C85.25DE.2C10 slot 0                          :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25DE.C8E0 slot 0                          :  -14 dBm on  11 (10.10.0.5)
  AP 0C85.25DF.3280 slot 0                          :  -31 dBm on   6 (10.10.0.5)
  AP 0CD9.96BA.5600 slot 0                          :  -44 dBm on   6 (10.0.0.2)
  AP 24B6.5734.C570 slot 0                          :  -48 dBm on  11 (10.0.0.2)
<snippet>
```

Q. CleanAir で利用可能なデバッグ コマンドはどれですか。

A. CleanAir のデバッグ コマンドは次のとおりです。

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

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

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

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

Q. Cisco Catalyst 3850 および 3650 シリーズ スイッチは、モビリティ エージェント（MA）として機能できますか。

A. はい。Cisco Catalyst 3850 および 3650 シリーズ スイッチは MA として機能できます。

Q. CleanAir 設定は MA で使用できますか。

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

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

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

関連トピック

2.4 GHz 帯域の CleanAir のイネーブル化, （27 ページ）
2.4 GHz での電波品質とデバイスの CleanAir アラームの設定, （28 ページ）
2.4 GHz デバイスの干渉レポートの設定, （30 ページ）
5 GHz 帯域の CleanAir のイネーブル化, （31 ページ）
5 GHz での電波品質とデバイスの CleanAir アラームの設定, （32 ページ）
5 GHz デバイスの干渉レポートの設定, （34 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CleanAir コマンドと詳細	*CleanAir Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
ハイ アベイラビリティ構成	*High Availability Configuration Guide, Cisco IOS XE Release 3SE (Cisco 5700 Series Wireless Controllers)*
ハイ アベイラビリティ コマンドと詳細	*High Availability Command Reference, Cisco IOS XE Release 3SE (Cisco 5700 Series Wireless Controllers)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

第 II 部

インターフェイスおよびハードウェア コンポーネント

- インターフェイス特性の設定，49 ページ
- Auto-MDIX の設定，87 ページ
- イーサネット管理ポートの設定，93 ページ
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定，101 ページ
- システム MTU の設定，125 ページ
- 内部電源装置の設定，131 ページ
- PoE の設定，137 ページ
- EEE の設定，153 ページ

第 3 章

インターフェイス特性の設定

- 機能情報の確認，49 ページ
- インターフェイス特性の設定に関する情報，49 ページ
- インターフェイスの特性の設定方法，61 ページ
- インターフェイス特性のモニタ，79 ページ
- インターフェイス特性の設定例，81 ページ
- インターフェイス特性機能の追加情報，84 ページ
- インターフェイス特性の設定の機能履歴と情報，85 ページ

機能情報の確認

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

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

インターフェイス特性の設定に関する情報

インターフェイス タイプ

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

（注） このスタック対応スイッチの背面にあるスタック ポートはイーサネット ポートではないため、設定できません。

ポートベースの VLAN

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

VLAN に分割することにより、VLAN 内でトラフィック用の堅固なファイアウォールを実現します。また、各 VLAN には固有の MAC アドレス テーブルがあります。VLAN が認識されるのは、ローカル ポートが VLAN に対応するように設定されたとき、VLAN トランキング プロトコル（VTP）トランク上のネイバーからその存在を学習したとき、またはユーザが VLAN を作成したときです。スタック全体のポートを使用して VLAN を形成できます。

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

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

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

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

スイッチ ポート

スイッチ ポートは、物理ポートに対応付けられたレイヤ 2 専用インターフェイスです。スイッチ ポートは 1 つまたは複数の VLAN に所属します。スイッチ ポートは、アクセス ポートまたはトランク ポートにも使用できます。ポートは、アクセス ポートまたはトランク ポートに設定でき

ます。また、ポート単位で Dynamic Trunking Protocol（DTP）を稼働させ、リンクのもう一端のポートとネゴシエートすることで、スイッチポートモードも設定できます。スイッチポートは、物理インターフェイスおよび関連付けられているレイヤ2プロトコルの管理に使用され、ルーティングやブリッジングは処理しません。

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

アクセス ポート

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

2 種類のアクセス ポートがサポートされています。

- スタティック アクセス ポート。このポートは、手動で VLAN に割り当てます（IEEE 802.1x で使用する場合は RADIUS サーバを使用します。
- ダイナミック アクセス ポートの VLAN メンバーシップは、着信パケットを通じて学習されます。デフォルトでは、ダイナミック アクセス ポートはどの VLAN のメンバーでもなく、ポートとの伝送はポートの VLAN メンバーシップが検出されたときにだけイネーブルになります。スイッチ上のダイナミック アクセス ポートは、VLAN メンバーシップ ポリシー サーバ（VMPS）によって VLAN に割り当てられます。Catalyst 6500 シリーズ スイッチを VMPS にできます。このスイッチを VMPS サーバにすることはできません。

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

トランク ポート

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

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

トンネル ポート

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

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

ルーテッド ポート

ルーテッド ポートは物理ポートであり、ルータ上にあるポートのように動作しますが、ルータに接続されている必要はありません。ルーテッド ポートは、アクセス ポートとは異なり、特定のVLAN に対応付けられていません。VLAN サブインターフェイスをサポートしない点を除けば、通常のルータ インターフェイスのように動作します。ルーテッド ポートは、レイヤ 3 ルーティング プロトコルで設定できます。ルーテッド ポートはレイヤ 3 インターフェイス専用で、DTP や STP などのレイヤ 2 プロトコルはサポートしません。

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

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

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

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

スイッチ仮想インターフェイス

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

（注） インターフェイス VLAN 1 は削除できません。

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

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

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

SVI 自動ステート除外

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

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

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

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

ブルである場合、**autostate exclude** は、ポート上でイネーブルであるすべての VLAN に適用されます。

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

EtherChannel ポート グループ

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

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

Power over Ethernet（PoE）ポート

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

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

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

スイッチの USB ポートの使用

USB ミニタイプ B コンソール ポート

スイッチには、次のコンソール ポートがあります。

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

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

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

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

コンソール ポート変更ログ

ソフトウェア起動時に、ログに USB または RJ-45 コンソールのいずれがアクティブであるかが示されます。スタック内の各スイッチがこのログを発行します。すべてのスイッチが最初に RJ-45 メディア タイプを常に表示します。

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

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

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

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

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

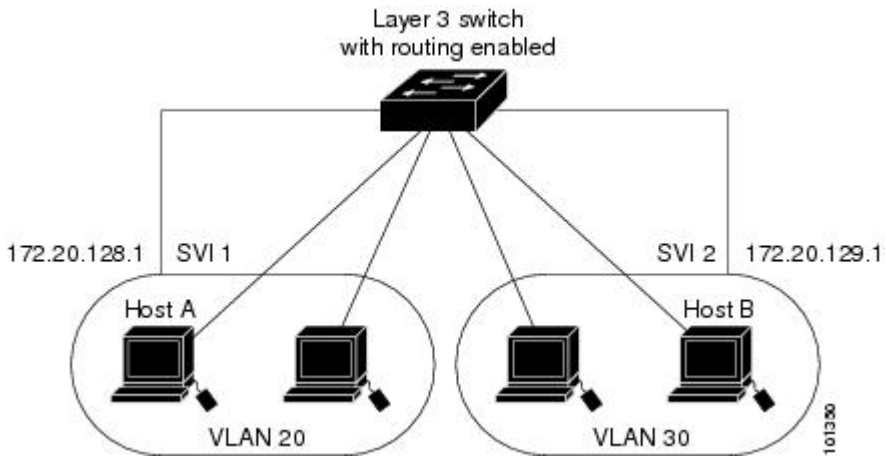
```
switch-stack-1
Mar  1 00:20:48.635: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

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

インターフェイスの接続

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

図 *2*：スイッチと *VLAN* との接続



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

イーサネット インターフェイスのデフォルト設定

インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 3 モードのインターフェイスをレイヤ 2 モー

ドにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。

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

表 *6*：レイヤ *2* イーサネット インターフェイスのデフォルト設定

機能	デフォルト設定
動作モード	レイヤ2またはスイッチング モード（**switchport** コマンド）
VLAN 許容範囲	VLAN 1 ～ 4094
デフォルト VLAN（アクセス ポート用）	VLAN 1（レイヤ 2 インターフェイスだけ）
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1（レイヤ 2 インターフェイスだけ）
VLAN トランキング	Switchport mode dynamic auto（DTP をサポート）（レイヤ 2 インターフェイスだけ）
ポート イネーブル ステート	すべてのポートがイネーブル
ポート記述	未定義
速度	自動ネゴシエーション（10 ギガビット インターフェイス上では未サポート）
デュプレックス モード	自動ネゴシエーション（10 ギガビット インターフェイス上では未サポート）
フロー制御	フロー制御は **receive: off** に設定されます。送信パケットでは常にオフです。
EtherChannel（PAgP）	すべてのイーサネット ポートでディセーブル。
ポート ブロッキング（不明マルチキャストおよび不明ユニキャスト トラフィック）	ディセーブル（ブロッキングされない）（レイヤ 2 インターフェイスだけ）。
ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御	ディセーブル
保護ポート	ディセーブル（レイヤ 2 インターフェイスだけ）。
ポート セキュリティ	ディセーブル（レイヤ 2 インターフェイスだけ）。

機能	デフォルト設定
PortFast	ディセーブル
Auto-MDIX	イネーブル （注） 受電デバイスがクロス ケーブルでスイッチに接続されている場合、スイッチは、IEEE 802.3af に完全には準拠していない、Cisco IP Phone やアクセス ポイントなどの準規格の受電をサポートしていない場合があります。これは、スイッチ ポート上で Automatic Medium-Dependent Interface Crossover（Auto-MIDX）がイネーブルかどうかは関係ありません。
Power over Ethernet（PoE）	イネーブル（auto）

インターフェイス速度およびデュプレックス モード

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

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

速度とデュプレックス モードの設定時の注意事項

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

- 10 ギガビット イーサネット ポートは、速度機能およびデュプレックス機能をサポートしていません。これらのポートは、10,000 Mbps、全二重モードでだけ動作します。
- ギガビット イーサネット（10/100/1000 Mbps）ポートは、すべての速度オプションとデュプレックス オプション（自動、半二重、全二重）をサポートします。ただし、1000 Mbps で稼働させているギガビット イーサネット ポートは、半二重モードをサポートしません。
- SFP モジュール ポートの場合、次の SFP モジュール タイプによって速度とデュプレックスの CLI（コマンドライン インターフェイス）オプションが変わります。

- 1000 BASE-*x*（*x* は、BX、CWDM、LX、SX、および ZX）SFP モジュール ポートは、**speed** インターフェイス コンフィギュレーション コマンドで **nonegotiate** キーワードをサポートします。デュプレックス オプションはサポートされません。
- 1000BASE-T SFP モジュール ポートは、10/100/1000 Mbps ポートと同一の速度とデュプレックス オプションをサポートします。

- 回線の両側で自動ネゴシエーションがサポートされる場合は、デフォルトの **auto** ネゴシエーションを使用することを強くお勧めします。
- 一方のインターフェイスが自動ネゴシエーションをサポートし、もう一方がサポートしない場合は、両方のインターフェイス上でデュプレックスと速度を設定します。サポートする側で **auto** 設定を使用しないでください。
- STP がイネーブルの場合にポートを再設定すると、スイッチがループの有無を調べるために最大で 30 秒かかる可能性があります。STP の再設定が行われている間、ポート LED はオレンジに点灯します。

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

IEEE 802.3x フロー制御

フロー制御により、接続しているイーサネット ポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。あるポートで輻輳が生じ、それ以上はトラフィックを受信できなくなった場合、ポーズ フレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズフレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、輻輳時のデータ パケット損失が防止されます。

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

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

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

デバイスのフロー制御設定には、次のルールが適用されます。

- **receive on**（または **desired**）：ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要のある、または送信できる接続デバイスと組み合わせて使用できます。ポーズ フレームの受信は可能です。

- **receive off**：フロー制御はどちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。

（注） コマンドの設定と、その結果生じるローカルおよびリモート ポートでのフロー制御解決の詳細については、このリリースのコマンド リファレンスに記載された **flowcontrol** インターフェイス コンフィギュレーション コマンドを参照してください。

レイヤ 3 インターフェイス

スイッチは、次のレイヤ 3 インターフェイスのタイプをサポートします。

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

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

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

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

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

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

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

- 新たなルーテッド ポートを作成しようとすると、スイッチはインターフェイスをルーテッド ポートに変換するための十分なリソースがないことを示すメッセージを表示し、インターフェイスはスイッチポートのままとなります。

- 拡張範囲の VLAN を作成しようとすると、エラー メッセージが生成され、拡張範囲の VLAN は拒否されます。

- VLANトランキングプロトコル（VTP）が新たなVLANをスイッチに通知すると、使用可能な十分なハードウェア リソースがないことを示すメッセージを送り、その VLAN をシャットダウンします。**show vlan** ユーザ EXEC コマンドの出力に、サスペンド ステートの VLAN が示されます。
- スイッチが、ハードウェアのサポート可能な数を超える VLAN とルーテッド ポートが設定されたコンフィギュレーションを使って起動を試みると、VLAN は作成されますが、ルーテッド ポートはシャットダウンされ、スイッチはハードウェア リソースが不十分であるという理由を示すメッセージを送信します。

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

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

インターフェイスの特性の設定方法

インターフェイスの設定

次の一般的な手順は、すべてのインターフェイス設定プロセスに当てはまります。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface** 例： スイッチ(config)# **interface gigabitethernet1/0/1** スイッチ(config-if)#	インターフェイスタイプ、スイッチ番号（スタック対応スイッチのみ）、およびコネクタの数を識別します。 （注） インターフェイス タイプとインターフェイス番号の間にスペースを入れる必要はありません。たとえば、前出の行の場合は、**gigabitethernet 1/0/1**、**gigabitethernet1/0/1**、**gi 1/0/1**、または **gi1/0/1** のいずれかを指定できます。
ステップ 4	各 **interface** コマンドの後ろに、インターフェイスに必要なインターフェイス コンフィギュレーション コマンドを続けて入力します。	インターフェイス上で実行するプロトコルとアプリケーションを定義します。別のインターフェイス コマンドまたは**end** を入力して特権 EXEC モードに戻ると、コマンドが収集されてインターフェイスに適用されます。
ステップ 5	**interface range** or **interface range macro**	（任意）インターフェイスの範囲を設定します。 （注） ある範囲内で設定したインターフェイスは、同じタイプである必要があります。また、同じ機能オプションを指定して設定しなければなりません。
ステップ 6	**show interfaces**	スイッチ上のまたはスイッチに対して設定されたすべてのインターフェイスのリストを表示します。デバイスがサポートする各インターフェイスまたは指定したインターフェイスのレポートが出力されます。

インターフェイスに関する記述の追加

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **description***string*
5. **end**
6. **show interfaces***interface-id***description**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	記述を追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**description***string* 例： スイッチ(config-if)# **description Connects to Marketing**	インターフェイスに関する説明を追加します（最大240 文字）。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces***interface-id***description**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイス範囲の設定

同じ設定パラメータを持つ複数のインターフェイスを設定するには、**interface range** グローバル コンフィギュレーション コマンドを使用します。インターフェイス レンジ コンフィギュレーション モードを開始すると、このモードを終了するまで、入力されたすべてのコマンド パラメータはその範囲内のすべてのインターフェイスに対するものと見なされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface range** {*port-range* | **macro***macro_name*}
4. **end**
5. **show interfaces** [*interface-id*]
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface range** {*port-range* | **macro***macro_name*} 例： `スイッチ(config)# interface range macro`	設定するインターフェイス範囲（VLAN または物理ポート）を指定し、インターフェイス コンフィギュレーション モードを開始します。 • **interface range** コマンドを使用すると、最大 5 つのポート範囲または定義済みマクロを 1 つ設定できます。 • **macro** 変数については、インターフェイス レンジ マクロの設定および使用方法, （65 ページ）を参照してください。 • カンマで区切った *port-range* では、各エントリに対応するインターフェイス タイプを入力し、カンマの前後にスペースを含めます。

	コマンドまたはアクション	目的
		• ハイフンで区切った *port-range* では、インターフェイス タイプの再入力は不要ですが、ハイフンの前後にスペースを入力する必要があります。 （注） この時点で、通常のコンフィギュレーション コマンドを使用して、範囲内のすべてのインターフェイスにコンフィギュレーション パラメータを適用します。各コマンドは、入力されたとおりに実行されます。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** [*interface-id*] 例： `スイッチ# show interfaces`	指定した範囲内のインターフェイスの設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイス レンジ マクロの設定および使用方法

インターフェイス レンジ マクロを作成すると、設定するインターフェイスの範囲を自動的に選択できます。**interface range macro** グローバル コンフィギュレーション コマンドで **macro** キーワードを使用するには、まず **define interface-range** グローバル コンフィギュレーション コマンドでマクロを定義する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **define interface-range***macro_name interface-range*
4. **interface range macro***macro_name*
5. **end**
6. **show running-config|include define**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**define interface-range***macro_name interface-range* 例： スイッチ(config)# **define interface-range enet_list gigabitethernet1/0/1 - 2**	インターフェイス範囲マクロを定義して、NVRAM に保存します。 • *macro_name* は、最大 32 文字の文字列です。 • マクロには、カンマで区切ったインターフェイスを 5 つまで指定できます。 • それぞれの *interface-range* は、同じポート タイプで構成されていなければなりません。 （注） **interface range macro** グローバル コンフィギュレーション コマンドで **macro** キーワードを使用するには、まず **define interface-range** グローバル コンフィギュレーション コマンドでマクロを定義する必要があります。
ステップ 4	**interface range macro***macro_name* 例： スイッチ(config)# **interface range**	*macro_name* の名前でインターフェイス範囲マクロに保存された値を使用することによって、設定するインターフェイスの範囲を選択します。

	コマンドまたはアクション	目的
	macro enet_list	ここで、通常のコンフィギュレーションコマンドを使用して、定義したマクロ内のすべてのインターフェイスに設定を適用できます。
ステップ **5**	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ **6**	**show running-config|include define** 例： スイッチ# **show running-config | include define**	定義済みのインターフェイス範囲マクロの設定を表示します。
ステップ **7**	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

イーサネット インターフェイスの設定

インターフェイス速度およびデュプレックス パラメータの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **speed** {**10** | **100** | **1000** | **2500** | **5000** | **10000** | **auto** [**10** | **100** | **1000** | **2500** | **5000** | **10000**] | **nonegotiate**}
5. **duplex** {**auto** | **full** | **half**}
6. **end**
7. **show interfaces***interface-id*
8. **copyrunning-configstartup-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/3**	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**speed** {**10** | **100** | **1000** | **2500** | **5000** | **10000** | **auto** [**10** | **100** | **1000** | **2500** | **5000** | **10000**] | **nonegotiate**} 例： スイッチ(config-if)# **speed 10**	インターフェイスに対する適切な速度パラメータを入力します。 • インターフェイスの特定の速度を設定するには、**10**、**100**、**10002500**、**5000**、または **10000** を入力します。 • インターフェイスに接続されたデバイスと自動ネゴシエーションが行えるようにするには、**auto** を入力します。速度を指定しする際に **auto** キーワードも設定する場合、ポートは指定の速度でのみ自動ネゴシエートします。 • **nonegotiate** キーワードを使用できるのは、SFP モジュール ポートに対してだけです。SFP モジュール ポートは 1000 Mbps だけで動作しますが、自動ネゴシエーションをサポートしていないデバイスに接続されている場合は、ネゴシエートしないように設定できます。
ステップ 5	**duplex** {**auto** | **full** | **half**} 例： スイッチ(config-if)# **duplex half**	このコマンドは、10 ギガビット イーサネット インターフェイスでは使用できません。 インターフェイスのデュプレックス パラメータを入力します。 半二重モードをイネーブルにします（10 または 100Mbps のみで動作するインターフェイスの場合）。1000 Mbps で動作するインターフェイスには半二重モードを設定できません。 デュプレックス設定を行うことができるのは、速度が **auto** に設定されている場合です。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces***interface-id* 例： スイッチ# **show interfaces gigabitethernet1/0/3**	インターフェイス速度およびデュプレックス モードの設定を表示します。
ステップ 8	**copyrunning-configstartup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IEEE 802.3x フロー制御の設定

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **flowcontrol** {**receive**} {**on** | **off** | **desired**}
4. **end**
5. **show interfaces***interface-id*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**flowcontrol** {**receive**} {**on** | **off** | **desired**} 例： スイッチ(config-if)# **flowcontrol receive on**	ポートのフロー制御モードを設定します。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces***interface-id* 例： スイッチ# **show interfaces gigabitethernet1/0/1**	インターフェイス フロー制御の設定を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

レイヤ 3 インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** {**gigabitethernet***interface-id*} | {**vlan***vlan-id*} | {**port-channel***port-channel-number*}
4. **no switchport**
5. **ip address***ip_address subnet_mask*
6. **no shutdown**
7. **end**
8. **show interfaces** [*interface-id*]
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {**gigabitethernet***interface-id*}	{**vlan***vlan-id*}	{**port-channel***port-channel-number*} 例： スイッチ(config)# **interface gigabitethernet1/0/2**	レイヤ 3 インターフェイスとして設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no switchport** 例： スイッチ(config-if)# **no switchport**	物理ポートに限り、レイヤ 3 モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**ip address***ip_address subnet_mask* 例： `スイッチ(config-if)# ip address 192.20.135.21 255.255.255.0`	IP アドレスおよび IP サブネットを設定します。
ステップ 6	**no shutdown** 例： `スイッチ(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 7	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** [*interface-id*]	設定を確認します。
ステップ 9	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

論理レイヤ 3 GRE トンネル インターフェイスの設定

はじめる前に

総称ルーティングカプセル化（GRE）は、仮想ポイントツーポイントリンク内でネットワーク層プロトコルをカプセル化するために使用されるトンネリングプロトコルです。GRE トンネルは、カプセル化のみを提供し、暗号化は提供しません。

注目 Cisco IOS XE Release 3.7.2E 以降では、GRE トンネルは Cisco Catalyst スイッチのハードウェアでサポートされます。GRE でトンネル オプションを設定しない場合、パケットはハードウェアでスイッチングされます。GRE でトンネル オプション（キーやチェックサムなど）を設定すると、パケットはソフトウェアでスイッチングされます。最大 10 個の GRE トンネルがサポートされます。

（注） アクセス コントロール リスト（ACL）や Quality of Service（QoS）などその他の機能は、GRE トンネルではサポートされません。

GRE トンネルを設定する手順は、次のとおりです。

手順の概要

1. **interface tunnel***number*
2. **ip address***ip_addresssubnet_mask*
3. **tunnel source**{*ip_address*|*type_number*}
4. **tunnel destination**{*host_name* | *ip_address*}
5. **tunnel mode gre ip**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface tunnel***number* 例： スイッチ(config)#**interface tunnel 2**	インターフェイスでトンネリングをイネーブルにします。
ステップ 2	**ip address***ip_addresssubnet_mask* 例： スイッチ(config)#**ip address 100.1.1.1 255.255.255.0**	IP アドレスおよび IP サブネットを設定します。
ステップ 3	**tunnel source**{*ip_address*|*type_number*} 例： スイッチ(config)#**tunnel source 10.10.10.1**	トンネル送信元を設定します。
ステップ 4	**tunnel destination**{*host_name*	*ip_address*} 例： スイッチ(config)#**tunnel destination 10.10.10.2**	トンネル宛先を設定します。
ステップ 5	**tunnel mode gre ip** 例： スイッチ(config)#**tunnel mode gre ip**	トンネル モードを設定します。
ステップ 6	**end** 例： スイッチ(config)#**end**	コンフィギュレーション モードを終了します。

SVI 自動ステート除外の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **switchport autostate exclude**
5. **end**
6. **show running config interface***interface-id*
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	レイヤ 2 インターフェイス（物理ポートまたはポート チャネル）を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport autostate exclude** 例： スイッチ(config-if)# **switchport autostate exclude**	SVI ライン ステート（アップまたはダウン）のステータスを定義する際、アクセスまたはトランク ポートを除外します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running config interface***interface-id*	（任意）実行コンフィギュレーションを表示します。 設定を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスのシャットダウンおよび再起動

インターフェイスをシャットダウンすると、指定されたインターフェイスのすべての機能がディセーブルになり、使用不可能であることがすべてのモニタ コマンドの出力に表示されます。この情報は、すべてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。ルーティング アップデートには、インターフェイス情報は含まれません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** {**vlan***vlan-id*} | {**gigabitethernet***interface-id*} | {**port-channel***port-channel-number*}
4. **shutdown**
5. **no shutdown**
6. **end**
7. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {**vlan***vlan-id*} | {**gigabitethernet***interface-id*} | {**port-channel***port-channel-number*} 例： スイッチ(config)# **interface gigabitethernet1/0/2**	設定するインターフェイスを選択します。
ステップ 4	**shutdown** 例： スイッチ(config-if)# **shutdown**	インターフェイスをシャットダウンします。
ステップ 5	**no shutdown** 例： スイッチ(config-if)# **no shutdown**	インターフェイスを再起動します。
ステップ 6	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。

コンソール メディア タイプの設定

コンソール メディア タイプを RJ-45 に設定するには、次の手順を実行します。RJ-45 としてコンソールを設定すると、USB コンソール オペレーションはディセーブルになり、入力は RJ-45 コネクタからのみ供給されます。

この設定はスタックのすべてのスイッチに適用されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **lineconsole 0**
4. **media-typerj45**
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lineconsole 0** 例： スイッチ(config)# **line console 0**	コンソールを設定し、ライン コンフィギュレーション モードを開始します。
ステップ 4	**media-typerj45** 例： スイッチ(config-line)# **media-type rj45**	コンソール メディア タイプが RJ-45 ポート以外に設定されないようにします。このコマンドを入力せず、両方のタイプが接続された場合は、デフォルトで USB ポートが使用されます。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

USB 無活動タイムアウトの設定

無活動タイムアウトを設定している場合、USB コンソールポートがアクティブ化されているものの、指定された時間内にポートで入力アクティビティがないときに、RJ-45 コンソール ポートが再度アクティブになります。タイムアウトのために USB コンソールポートは非アクティブ化された場合、USB ポートを切断し、再接続すると、動作を回復できます。

（注） 設定された無活動タイムアウトはスタックのすべてのスイッチに適用されます。しかし、あるスイッチのタイムアウトはスタック内の別のスイッチにタイムアウトを発生させません。

手順の概要

1. **enable**
2. **configureterminal**
3. **lineconsole 0**
4. **usb-inactivity-timeout** *timeout-minutes*
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lineconsole 0** 例： スイッチ(config)# **line console 0**	コンソールを設定し、ライン コンフィギュレーション モードを開始します。
ステップ 4	**usb-inactivity-timeout** *timeout-minutes* 例： スイッチ(config-line)# **usb-inactivity-timeout 30**	コンソール ポートの無活動タイムアウトを指定します。指定できる範囲は 1 ～ 240 分です。デフォルトでは、タイムアウトが設定されていません。
ステップ 5	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイス特性のモニタ

インターフェイス ステータスのモニタ

特権 EXEC プロンプトにコマンドを入力することによって、ソフトウェアおよびハードウェアのバージョン、コンフィギュレーション、インターフェイスに関する統計情報などのインターフェイス情報を表示できます。

表 *7*：インターフェイス用の ***show*** コマンド

コマンド	目的
show interfaces*interface-id* **status** [**err-disabled**]	インターフェイスのステータスまたはerrdisableステートにあるインターフェイスのリストを表示します。
show interfaces [*interface-id*] **switchport**	スイッチング（非ルーティング）ポートの管理上および動作上のステータスを表示します。このコマンドを使用すると、ポートがルーティングまたはスイッチングのどちらのモードにあるかが判別できます。
show interfaces [*interface-id*] **description**	1つのインターフェイスまたはすべてのインターフェイスに関する記述とインターフェイスのステータスを表示します。
show ip interface [*interface-id*]	IP ルーティング用に設定されたすべてのインターフェイスまたは特定のインターフェイスについて、使用できるかどうかを表示します。
show interface [*interface-id*] **stats**	インターフェイスのパスごとに入出力パケットを表示します。
show interfaces*interface-id*	（任意）インターフェイスの速度およびデュプレックスを表示します。
show interfaces transceiver dom-supported-list	（任意）接続 SFP モジュールの Digital Optical Monitoring（DOM）ステータスを表示します。
show interfaces transceiver properties	（任意）インターフェイスの温度、電圧、電流量を表示します。
show interfaces [*interface-id*] [{**transceiver properties** | **detail**}] *module number*]	SFP モジュールに関する物理および動作ステータスを表示します。
show running-config interface [*interface-id*]	インターフェイスに対応する RAM 上の実行コンフィギュレーションを表示します。
show version	ハードウェア設定、ソフトウェアバージョン、コンフィギュレーションファイルの名前と送信元、およびブート イメージを表示します。
show controllers ethernet-controller*interface-id***phy**	インターフェイスの Auto-MDIX 動作ステートを表示します。

インターフェイスおよびカウンタのクリアとリセット

表 *8*：インターフェイス用の ***clear*** コマンド

コマンド	目的
clear counters [*interface-id*]	インターフェイス カウンタをクリアします。
clear interface*interface-id*	インターフェイスのハードウェア ロジックをリセットします。
clear line [*number* | **console 0** | **vty***number*]	非同期シリアル回線に関するハードウェア ロジックをリセットします。

（注） **clear counters** 特権 EXEC コマンドは、簡易ネットワーク管理プロトコル（SNMP）を使用して取得されたカウンタをクリアしません。**show interface** 特権 EXEC コマンドで表示されるカウンタのみをクリアします。

インターフェイス特性の設定例

インターフェイスの説明の追加：例

```
スイッチ# configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# description Connects to Marketing
スイッチ(config-if)# end
スイッチ# show interfaces gigabitethernet1/0/2 description
Interface Status         Protocol Description
Gi1/0/2   admin down     down     Connects to Marketing
```

インターフェイス範囲の設定：例

次に、**interface range** グローバル コンフィギュレーション コマンドを使用して、スイッチ 1 上のポート 1 ～ 4 で速度を 100 Mb/s に設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# interface range gigabitethernet1/0/1 - 4
```

```
スイッチ(config-if-range)# speed 100
```

この例では、カンマを使用して範囲に異なるインターフェイスタイプストリングを追加して、ギガビット イーサネット ポート 1 ～ 3 と、10 ギガビット イーサネット ポート 1 および 2 の両方をイネーブルにし、フロー制御ポーズ フレームを受信できるようにします。

```
スイッチ# configure terminal
スイッチ(config)# interface range gigabitethernet1/0/1 - 3 , tengigabitethernet1/0/1 - 2
スイッチ(config-if-range)# flowcontrol receive on
```

インターフェイス レンジ モードで複数のコンフィギュレーション コマンドを入力した場合、各コマンドは入力した時点で実行されます。インターフェイス レンジモードを終了した後で、コマンドがバッチ処理されるわけではありません。コマンドの実行中にインターフェイス レンジコンフィギュレーション モードを終了すると、一部のコマンドが範囲内のすべてのインターフェイスに対して実行されない場合もあります。コマンド プロンプトが再表示されるのを待ってから、インターフェイス範囲コンフィギュレーション モードを終了してください。

インターフェイス レンジ マクロの設定および使用方法：例

次に、*enet_list* という名前のインターフェイス範囲マクロを定義してスイッチ 1 上のポート 1 および 2 を含め、マクロ設定を確認する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# define interface-range enet_list gigabitethernet1/0/1 - 2
スイッチ(config)# end
スイッチ# show running-config | include define
define interface-range enet_list GigabitEthernet1/0/1 - 2
```

次に、複数のタイプのインターフェイスを含む マクロ *macro1* を作成する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# define interface-range macro1 gigabitethernet1/0/1 - 2, gigabitethernet1/0/5
 - 7, tengigabitethernet1/0/1 -2
スイッチ(config)# end
```

次に、インターフェイス レンジ マクロ *enet_list* に対するインターフェイス レンジ コンフィギュレーション モードを開始する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# interface range macro enet_list
スイッチ(config-if-range)#
```

次に、インターフェイス レンジ マクロ *enet_list* を削除し、処理を確認する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# no define interface-range enet_list
スイッチ(config)# end
スイッチ# show run | include define
スイッチ#
```

インターフェイス速度およびデュプレックス モードの設定：例

次に、インターフェイス速度を 100 Mb/s に、10/100/1000 Mbps ポートのデュプレックス モードを半二重に設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# interface gigabitethernet1/0/3
スイッチ(config-if)# speed 10
スイッチ(config-if)# duplex half
```

次に、10/100/1000 Mbps ポートで、インターフェイスの速度を 100 Mbps に設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# speed 100
```

レイヤ 3 インターフェイスの設定：例

```
スイッチ# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# no switchport
スイッチ(config-if)# ip address 192.20.135.21 255.255.255.0
スイッチ(config-if)# no shutdown
```

コンソール メディア タイプの設定：例

次に、USB コンソール メディア タイプをディセーブルにし、RJ-45 コンソール メディア タイプをイネーブルにする例を示します。

```
スイッチ# configure terminal
スイッチ(config)# line console 0
スイッチ(config-line)# media-type rj45
```

この設定は、スタック内のすべてのアクティブなUSBコンソールメディアタイプを終了します。ログにはこの終了の発生が示されます。次に、スイッチ 1 のコンソールが RJ-45 に戻る例を示します。

```
*Mar  1 00:25:36.860: %USB_CONSOLE-6-CONFIG_DISABLE: Console media-type USB disabled by
system configuration, media-type reverted to RJ45.
```

この時点で、スタック内のどのスイッチもUSBコンソールでの入力を受け付けません。ログのエントリには、コンソール ケーブルがいつ接続されたかが示されています。USBコンソール ケーブルが switch 2 に接続されている場合、入力は提供されません。

```
*Mar  1 00:34:27.498: %USB_CONSOLE-6-CONFIG_DISALLOW: Console media-type USB is disallowed
 by system configuration, media-type remains RJ45. (switch-stk-2)
```

次に、前の設定を逆にして、ただちにすべての接続されたUSBコンソールをアクティブにする例を示します。

```
スイッチ# configure terminal
スイッチ(config)# line console 0
スイッチ(config-line)# no media-type rj45
```

USB無活動タイムアウトの設定：例

次に、無活動タイムアウトを30分に設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# line console 0
スイッチ(config-line)# usb-inactivity-timeout 30
```

設定をディセーブルにするには、次のコマンドを使用します。

```
スイッチ# configure terminal
スイッチ(config)# line console 0
スイッチ(config-line)# no usb-inactivity-timeout
```

設定された分数の間にUSBコンソールポートで（入力）アクティビティがなかった場合、無活動タイムアウト設定がRJ-45ポートに適用され、ログにこの発生が示されます。

```
*Mar  1 00:47:25.625: %USB_CONSOLE-6-INACTIVITY_DISABLE: Console media-type USB disabled
due to inactivity, media-type reverted to RJ45.
```

この時点で、USBコンソールポートを再度アクティブ化する唯一の方法は、ケーブルを取り外し、再接続することです。

スイッチのUSBケーブルが取り外され再接続された場合、ログは次のような表示になります。

```
*Mar  1 00:48:28.640: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.
```

インターフェイス特性機能の追加情報

エラーメッセージデコーダ

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

標準および RFC

標準/RFC	タイトル
なし	--

MIB

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

シスコのテクニカル サポート

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

インターフェイス特性の設定の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 4 章

Auto-MDIX の設定

- Auto-MDIX の前提条件，87 ページ
- Auto-MDIX の制約事項，88 ページ
- Auto-MDIX の設定に関する情報，88 ページ
- Auto-MDIX の設定方法，89 ページ
- Auto-MDIX の設定例，90 ページ
- その他の参考資料，91 ページ
- Auto-MDIX の機能履歴と情報，92 ページ

Auto-MDIX の前提条件

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

デフォルトで Automatic Medium-Dependent Interface Crossover（Auto-MDIX）機能がイネーブルに設定されます。Auto-MDIX をイネーブルに設定する場合、Auto-MDIX 機能が正しく動作するようにインターフェイスの速度およびデュプレックスを **auto** に設定する必要があります。

Auto-MDIX は、すべての 10/100/1000 Mbps インターフェイスと、10/100/1000BASE-TX Small Form-Factor Pluggable（SFP）モジュール インターフェイスでサポートされています。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

Auto-MDIX の制約事項

受電デバイスがクロス ケーブルでスイッチに接続されている場合、スイッチは、IEEE 802.3af に完全には準拠していない、Cisco IP Phone やアクセス ポイントなどの準規格の受電をサポートしていない場合があります。これは、スイッチ ポート上で Automatic Medium-Dependent Interface Crossover（Auto-MIDX）がイネーブルかどうかは関係ありません。

Auto-MDIX の設定に関する情報

インターフェイスでの Auto-MDIX

自動メディア依存型インターフェイス クロスオーバー（MDIX）がイネーブルになっているインターフェイスでは、必要なケーブル接続タイプ（ストレートまたはクロス）が自動的に検出され、接続が適切に設定されます。Auto-MDIX 機能を使用せずにスイッチを接続する場合、サーバ、ワークステーション、またはルータなどのデバイスの接続にはストレート ケーブルを使用し、他のスイッチやリピータの接続にはクロス ケーブルを使用する必要があります。Auto-MDIX がイネーブルの場合、他のデバイスとの接続にはどちらのケーブルでも使用でき、ケーブルが正しくない場合はインターフェイスが自動的に修正を行います。ケーブル接続の詳細については、ハードウェア インストレーション ガイドを参照してください。

次の表に、Auto-MDIX の設定およびケーブル接続ごとのリンク ステートを示します。

表 *9*：リンク状態と *Auto-MDIX* の設定

ローカル側の Auto-MDIX	リモート側の Auto-MDIX	ケーブル接続が正しい場合	ケーブル接続が正しくない場合
オン	オン	リンク アップ	リンク アップ
オン	オフ	リンク アップ	リンク アップ
オフ	オン	リンク アップ	リンク アップ
オフ	オフ	リンク アップ	リンク ダウン

Auto-MDIX の設定方法

インターフェイスでの Auto-MDIX の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **speedauto**
5. **duplexauto**
6. **mdix auto**
7. **end**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**speedauto** 例： スイッチ(config-if)# **speed auto**	接続されたデバイスと速度の自動ネゴシエーションを行うようにインターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**duplexauto** 例： スイッチ(config-if)# **duplex auto**	接続されたデバイスとデュプレックス モードの自動ネゴシエーションを行うようにインターフェイスを設定します。
ステップ 6	**mdix auto** 例： スイッチ(config-if)# **mdix auto**	インターフェイスの Auto MDIX をイネーブルにします。
ステップ 7	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Auto-MDIX の設定例

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
スイッチ# configure terminal
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# speed auto
スイッチ(config-if)# duplex auto
スイッチ(config-if)# mdix auto
スイッチ(config-if)# end
```

その他の参考資料

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

Auto-MDIX の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 5 章

イーサネット管理ポートの設定

- 機能情報の確認，93 ページ
- イーサネット管理ポートの前提条件，93 ページ
- イーサネット管理ポートに関する情報，94 ページ
- イーサネット管理ポートの設定方法，96 ページ
- その他の参考資料，97 ページ
- イーサネット管理ポートの機能情報，99 ページ

機能情報の確認

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

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

イーサネット管理ポートの前提条件

PC をイーサネット管理ポートに接続するときに、最初に IP アドレスを割り当てる必要があります。

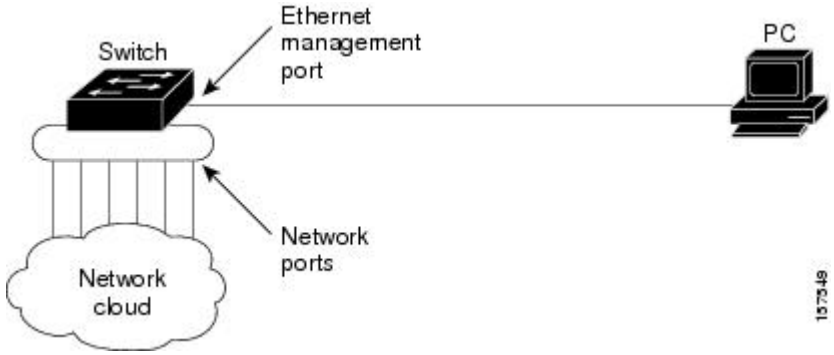
イーサネット管理ポートに関する情報

Gi0/0 または *GigabitEthernet0/0* ポートとも呼ばれるイーサネット管理ポートは、PC を接続する VRF（VPN ルーティング/転送）インターフェイスです。ネットワークの管理に、スイッチ コンソールポートの代わりとしてイーサネット管理ポートを使用できます。スイッチ スタックを管理するときに、PC をスタック メンバ上のイーサネット管理ポートに接続します。

スイッチへのイーサネット管理ポートの直接接続

次の図は、スイッチまたはスタンドアロン スイッチに対して、イーサネット管理ポートを PC に接続する方法を示します。

図 *3*：*PC* とスイッチの接続



ハブを使用したスタック スイッチへのイーサネット管理ポートの接続

スタック スイッチのみのスタックでは、スタック メンバ上のすべてのイーサネット管理ポートが、PC が接続されるハブに接続されます。アクティブ スイッチのイーサネット管理ポートからのアクティブ リンクは、ハブを経由して PC とつながっています。アクティブ スイッチに障害が発生し、新しいアクティブスイッチが選択された場合、アクティブリンクは、新しいアクティブスイッチ上のイーサネット管理ポートから PC までになります。

次の図は、PC がハブを使用してスイッチ スタックに接続する方法を示しています。

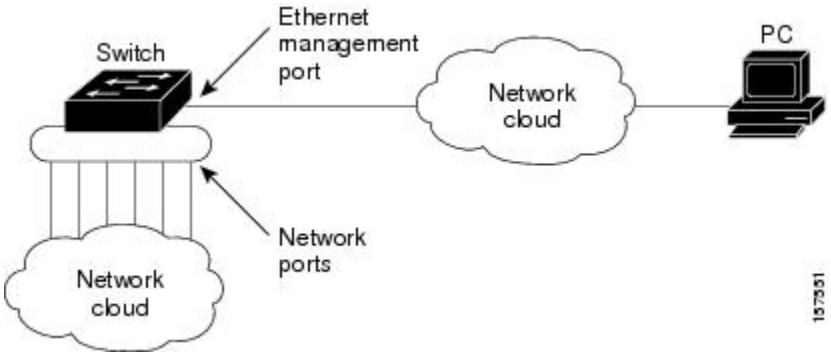
図 *4*：*PC* とスイッチ スタックの接続

イーサネット管理ポートおよびルーティング

デフォルトでは、イーサネット管理ポートはイネーブルです。スイッチは、イーサネット管理ポートからネットワーク ポートにパケットをルーティングできず、その逆もできません。イーサネット管理ポートはルーティングをサポートしていませんが、ポート上でルーティング プロトコルをイネーブルにすることが必要となる場合もあります。

PC とスイッチが複数のホップ分離れていて、パケットが PC に到達するには複数のレイヤ 3 デバイスを経由しなければならない場合に、イーサネット管理ポート上のルーティング プロトコルをイネーブルにします。

図 *5* : ルーティング プロトコルをイネーブルにしたネットワーク例



上記の図では、イーサネット管理ポートとネットワーク ポートが同じルーティングプロセスに関連付けられている場合、ルートは次のように伝播されます。

- イーサネット管理ポートからのルートは、ネットワーク ポートを通してネットワークに伝播されます。
- ネットワーク ポートからのルートは、イーサネット管理ポートを通してネットワークに伝播されます。

イーサネット管理ポートとネットワーク ポートの間ではルーティングはサポートされていないため、これらのポート間のトラフィックの送受信はできません。このような状況になると、これらのポート間にデータ パケット ループが発生し、スイッチおよびネットワークの動作が中断されます。このループを防止するには、イーサネット管理ポートとネットワーク ポートの間のルートを回避するためにルート フィルタを設定してください。

サポートされるイーサネット管理ポートの機能

イーサネット管理ポートは次の機能をサポートします。

- Express Setup（スイッチ スタックでのみ）
- Network Assistant
- パスワード付きの Telnet
- TFTP
- セキュア シェル（SSH）
- Dynamic Host Configuration Protocol（DHCP）ベースの自動設定
- SNMP（ENTITY-MIB および IF-MIB のみ）
- IP ping

- インターフェイス機能
  - 速度：10 Mb/s、100 Mb/s、および自動ネゴシエーション
  - デュプレックス モード：全二重、半二重、自動ネゴシエーション
  - ループバック検出
- Cisco Discovery Protocol（CDP）
- DHCP リレー エージェント
- IPv4 アクセス コントロール リスト（ACL）
- ルーティング プロトコル

注意 イーサネット管理ポートの機能をイネーブルにする前に機能がサポートされていることを確認してください。イーサネット管理ポートのサポートされていない機能を設定しようとすると、機能は正しく動作せず、スイッチに障害が発生するおそれがあります。

イーサネット管理ポートの設定方法

イーサネット管理ポートのディセーブル化およびイネーブル化

手順の概要

1. **configure terminal**
2. **interface gigabitethernet0/0**
3. **shutdown**
4. **no shutdown**
5. **exit**
6. **show interfaces gigabitethernet0/0**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface gigabitethernet0/0** 例： スイッチ(config)# **interface gigabitethernet0/0**	CLI でイーサネット管理ポートを指定します。
ステップ 3	**shutdown** 例： スイッチ(config-if)# **shutdown**	イーサネット管理ポートをディセーブルにします。
ステップ 4	**no shutdown** 例： スイッチ(config-if)# **no shutdown**	イーサネット管理ポートをイネーブルにします。
ステップ 5	**exit** 例： スイッチ(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	**show interfaces gigabitethernet0/0** 例： スイッチ# **show interfaces gigabitethernet0/0**	リンク ステータスを表示します。 PC へのリンク ステータスを調べるには、イーサネット管理ポートの LED をモニタします。リンクがアクティブな場合、LEDはグリーン（オン）であり、リンクが停止中の場合は、LED はオフです。POST エラーがある場合は、LED はオレンジです。

次の作業

イーサネット管理ポートを使用したスイッチの管理または設定に進みます。*Network Management Configuration Guide (Catalyst 3650 Switches)*を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ブートローダ設定	*System Management Configuration Guide*（*Catalyst 3650 Switches*）
ブートローダ コマンド	*System Management Command Reference (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

イーサネット管理ポートの機能情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 6 章

LLDP、LLDP-MED、およびワイヤードロケーション サービスの設定

- 機能情報の確認，101 ページ
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要，102 ページ
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定方法，107 ページ
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定例，120 ページ
- LLDP、LLDP-MED、ワイヤードロケーション サービスのモニタリングとメンテナンス，120 ページ
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの追加情報，122 ページ
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの機能情報，123 ページ

機能情報の確認

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

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

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要

LLDP

Cisco Discovery Protocol（CDP）は、すべてのシスコ製デバイス（ルータ、ブリッジ、アクセス サーバ、スイッチ、およびコントローラ）のレイヤ 2（データ リンク層）上で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションはCDPを使用することにより、ネットワーク接続されている他のシスコ デバイスを自動的に検出し、識別できます。

スイッチでは他社製のデバイスをサポートし他のデバイス間の相互運用性を確保するために、IEEE 802.1AB リンク層検出プロトコル（LLDP）をサポートしています。LLDPは、ネットワーク デバイスがネットワーク上の他のデバイスに自分の情報をアドバタイズするために使用するネイバー探索プロトコルです。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する 2 つのシステムで互いの情報を学習できます。

LLDP でサポートされる TLV

LLDPは一連の属性をサポートし、これらを使用してネイバーデバイスを検出します。属性には、Type、Length、および Value の説明が含まれていて、これらを TLV と呼びます。LLDP をサポートするデバイスは、ネイバーとの情報の送受信に TLV を使用できます。このプロトコルは、設定情報、デバイス機能、およびデバイス ID などの詳細情報をアドバタイズできます。

スイッチは、次の基本管理 TLV をサポートします。これらは必須の LLDP TLV です。

- ポート記述 TLV
- システム名 TLV
- システム記述 TLV
- システム機能 TLV
- 管理アドレス TLV

次の IEEE 固有の LLDP TLV もアドバタイズに使用されて LLDP-MED をサポートします。

- ポート VLAN ID TLV（IEEE 802.1 に固有の TLV）
- MAC/PHY コンフィギュレーション/ステータス TLV（IEEE 802.3 に固有の TLV）

LLDP および Cisco スイッチ のスタック

スイッチ スタックは、ネットワーク内の1つのスイッチとして表示されます。したがって、LLDP は、個々のスタック メンバではなく、スイッチ スタックを検出します。

LLDP-MED

LLDP for Media Endpoint Devices（LLDP-MED）は LLDP の拡張版で、IP 電話などのエンドポイントデバイスとスイッチなどのネットワーク デバイスの間で動作します。特に VoIP アプリケーションをサポートし、検出機能、ネットワーク ポリシー、Power over Ethernet（PoE）、インベントリ管理、およびロケーション情報に関する TLV を提供します。デフォルトで、すべての LLDP-MED TLV がイネーブルです。

LLDP-MED でサポートされる TLV

LLDP-MED では、次の TLV がサポートされます。

- LLDP-MED 機能 TLV

  LLDP-MED エンドポイントは、接続装置がサポートする機能と現在イネーブルになっている機能を識別できます。

- ネットワーク ポリシー TLV

  ネットワーク接続デバイスとエンドポイントはともに、VLAN 設定、および関連するレイヤ 2 とレイヤ 3 属性をポート上の特定アプリケーションにアドバタイズできます。たとえば、スイッチは使用する VLAN 番号を IP 電話に通知できます。IP 電話は任意のスイッチに接続し、VLAN 番号を取得してから、コール制御の通信を開始できます。

  ネットワーク ポリシー プロファイル TLV を定義することによって、VLAN、サービス クラス（CoS）、Diffserv コードポイント（DSCP）、およびタギング モードの値を指定して、音声と音声信号のプロファイルを作成できます。その後、これらのプロファイル属性は、スイッチで中央集約的に保守され、IP 電話に伝播されます。

- 電源管理 TLV

  LLDP-MED エンドポイントとネットワーク接続デバイスの間で拡張電源管理を可能にします。スイッチおよび IP 電話は、デバイスの受電方法、電源プライオリティ、デバイスの消費電力などの電源情報を通知することができます。

  LLDP-MED は拡張電源 TLV もサポートして、きめ細かな電力要件、エンドポイント電源プライオリティ、およびエンドポイントとネットワークの接続デバイスの電源ステータスをアドバタイズします。LLDP がイネーブルでポートに電力が供給されているときは、電力 TLV によってエンドポイントデバイスの実際の電力要件が決定するので、それに応じてシステムの電力バジェットを調整することができます。スイッチは要求を処理し、現在の電力バジェットに基づいて電力を許可または拒否します。要求が許可されると、スイッチは電力バジェットを更新します。要求が拒否された場合、スイッチは、ポートの電力をオフに切り替え、Syslog メッセージを生成して電力バジェットを更新します。LLDP-MED がディセーブルの場合や、エンドポイントが LLDP-MED 電力 TLV をサポートしていない場合は、初期割り当て値が接続終了まで使用されます。

  power inline {**auto** [**max***max-wattage*] | **never** | **static** [**max***max-wattage*]} インターフェイス コンフィギュレーション コマンドを入力して、電力設定を変更できます。PoE インターフェイスはデフォルトで **auto** モードに設定されています。値を指定しない場合は、最大電力（30 W）が供給されます。

- インベントリ管理 TLV

  エンドポイントは、スイッチにエンドポイントの詳細なインベントリ情報を送信することが可能です。インベントリ情報には、ハードウェア リビジョン、ファームウェア バージョン、ソフトウェア バージョン、シリアル番号、メーカー名、モデル名、Asset ID TLV などがあります。

- ロケーション TLV

  スイッチからのロケーション情報をエンドポイント デバイスに提供します。ロケーション TLV はこの情報を送信することができます。

  - 都市ロケーション情報

    都市アドレス情報および郵便番号情報を提供します。都市ロケーション情報の例には、地名、番地、郵便番号などがあります。

  - ELIN ロケーション情報

    発信側のロケーション情報を提供します。ロケーションは、緊急ロケーション識別番号（ELIN）によって決定されます。これは、緊急通報を Public Safety Answering Point（PSAP）にルーティングする電話番号で、PSAP はこれを使用して緊急通報者にコールバックすることができます。

  - 地理的なロケーション情報

    スイッチの緯度、経度、および高度などのスイッチ位置の地理的な詳細を指定します。

  - カスタム ロケーション

    スイッチの位置のカスタマイズされた名前と値を入力します。

ワイヤード ロケーション サービス

スイッチは、接続されているデバイスのロケーション情報およびアタッチメント追跡情報を Cisco Mobility Services Engine（MSE）に送信するのにロケーション サービス機能を使用します。トラッキングされたデバイスは、ワイヤレスエンドポイント、ワイヤードエンドポイント、またはワイヤード スイッチまたはコントローラになります。スイッチは、MSE にネットワーク モビリティ サービス プロトコル（NMSP）のロケーション通知および接続通知を介して、デバイスのリンク アップ イベントおよびリンク ダウン イベントを通知します。

MSE がスイッチに対して NMSP 接続を開始すると、サーバ ポートが開きます。MSE がスイッチに接続する場合は、バージョンの互換性を確保する 1 組のメッセージ交換およびサービス交換情報があり、その後にロケーション情報の同期が続きます。接続後、スイッチは定期的にロケーション通知および接続通知を MSE に送信します。インターバル中に検出されたリンク アップ イベントまたはリンク ダウン イベントは、集約されてインターバルの最後に送信されます。

スイッチがリンク アップ イベントまたはリンク ダウン イベントでデバイスの有無を確認した場合は、スイッチは、MAC アドレス、IP アドレス、およびユーザ名のようなクライアント固有情報を取得します。クライアントが LLDP-MED または CDP に対応している場合は、スイッチは LLDP-MED ロケーション TLV または CDP でシリアル番号および UDI を取得します。

デバイス機能に応じて、スイッチは次のクライアント情報をリンク アップ時に取得します。

- ポート接続で指定されたスロットおよびポート。
- クライアント MAC アドレスで指定された MAC アドレス。
- ポート接続で指定された IP アドレス。
- 802.1X ユーザ名（該当する場合）。
- デバイス カテゴリは、*wired station* として指定されます。
- ステートは *new* として指定されます。
- シリアル番号、UDI。
- モデル番号
- スイッチによる関連付け検出後の時間（秒）

デバイス機能に応じて、スイッチは次のクライアント情報をリンク ダウン時に取得します。

- 切断されたスロットおよびポート。
- MAC アドレス
- IP アドレス
- 802.1X ユーザ名（該当する場合）。
- デバイス カテゴリは、*wired station* として指定されます。
- ステートは *delete* として指定されます
- シリアル番号、UDI。
- スイッチによる関連付け解除検出後の時間（秒）

スイッチがシャットダウンする場合は、スイッチは、MSE との NMSP 接続を終了する前に、ステートの *delete* および IP アドレスとともに接続情報通知を送信します。MSE は、この通知を、スイッチに関連付けられているすべてのワイヤード クライアントに対する関連付け解除として解釈します。

スイッチ上のロケーション アドレスを変更すると、スイッチは、影響を受けるポートを識別する NMSP ロケーション通知メッセージ、および変更されたアドレス情報を送信します。

デフォルトの LLDP 設定

表 *10*：デフォルトの *LLDP* 設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル

機能	デフォルト設定
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	ディセーブル（すべての TLV との送受信）
LLDP インターフェイス ステート	ディセーブル
LLDP 受信	ディセーブル
LLDP 転送	ディセーブル
LLDP med-tlv-select	ディセーブル（すべての LLDP-MED TLV への送信）。LLDP がグローバルにイネーブルにされると、LLDP-MED-TLV もイネーブルになります。

LLDP に関する制約事項

- インターフェイスがトンネル ポートに設定されていると、LLDP は自動的にディセーブルになります。
- 最初にインターフェイス上にネットワークポリシープロファイルを設定した場合、インターフェイス上に **switchport voice vlan** コマンドを適用できません。**switchport voice vlan***vlan-id* がすでに設定されているインターフェイスには、ネットワーク ポリシー プロファイルを適用できます。このように、そのインターフェイスには、音声または音声シグナリング VLAN ネットワーク ポリシー プロファイルが適用されます。
- ネットワーク ポリシー プロファイルを持つインターフェイス上では、スタティック セキュア MAC アドレスを設定できません。

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

LLDP のイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **lldp run**
4. **interface***interface-id*
5. **lldp transmit**
6. **lldp receive**
7. **end**
8. **show lldp**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lldp run** 例： スイッチ (config)# **lldp run**	スイッチで LLDP をグローバルにイネーブルにします。
ステップ 4	**interface***interface-id* 例： スイッチ (config)# **interface**	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	gigabitethernet2/0/1	
ステップ 5	**lldp transmit** 例： スイッチ(config-if)# **lldp transmit**	LLDPパケットを送信するようにインターフェイスをイネーブルにします。
ステップ 6	**lldp receive** 例： スイッチ(config-if)# **lldp receive**	LLDPパケットを受信するようにインターフェイスをイネーブルにします。
ステップ 7	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show lldp** 例： スイッチ# **show lldp**	設定を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

LLDP 特性の設定

LLDP 更新の頻度、情報を廃棄するまでの保持期間、および初期化遅延時間を設定できます。送受信する LLDP および LLDP-MED TLV も選択できます。

（注） ステップ 2 ～ 5 は任意であり、どの順番で実行してもかまいません。

手順の概要

1. **enable**
2. **configureterminal**
3. **lldp holdtime***seconds*
4. **lldp reinit***delay*
5. **lldp timer***rate*
6. **lldp tlv-select**
7. **interface***interface-id*
8. **lldp med-tlv-select**
9. **end**
10. **show lldp**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lldp holdtime***seconds* 例： スイッチ(config)# **lldp holdtime 120**	（任意）デバイスから送信された情報を受信側デバイスが廃棄するまで保持する必要がある期間を指定します。 指定できる範囲は 0 ～ 65535 秒です。デフォルトは 120 秒です。
ステップ 4	**lldp reinit***delay* 例： スイッチ(config)# **lldp reinit 2**	（任意）任意のインターフェイス上で LLDP の初期化の遅延時間（秒）を指定します。 指定できる範囲は 2 ～ 5 秒です。デフォルトは 2 秒です。

	コマンドまたはアクション	目的
ステップ 5	**lldp timer***rate* 例： `スイッチ(config)# lldp timer 30`	（任意）インターフェイス上でLLDPの更新の遅延時間（秒）を指定します。 指定できる範囲は 5 ～ 65534 秒です。デフォルトは 30 秒です。
ステップ 6	**lldp tlv-select** 例： `スイッチ(config)# tlv-select`	（任意）送受信する LLDP TLV を指定します。
ステップ 7	**interface***interface-id* 例： `スイッチ (config)# interface gigabitethernet2/0/1`	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**lldp med-tlv-select** 例： `スイッチ (config-if)# lldp med-tlv-select inventory management`	（任意）送受信する LLDP-MED TLV を指定します。
ステップ 9	**end** 例： `スイッチ (config-if)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show lldp** 例： `スイッチ# show lldp`	設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

LLDP-MED TLV の設定

デフォルトでは、スイッチはエンドデバイスから LLDP-MED パケットを受信するまで、LLDP パケットだけを送信します。スイッチは、MED TLV を持つ LLDP も送信します。LLDP-MED エントリが期限切れになった場合は、スイッチは再び LLDP パケットだけを送信します。

lldp インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスが次の表にリストされている TLV を送信しないように設定できます。

表 *11*：*LLDP-MED TLV*

LLDP-MED TLV	説明
inventory-management	LLDP-MED インベントリ管理 TLV
location	LLDP-MED ロケーション TLV
network-policy	LLDP-MED ネットワーク ポリシー TLV
power-management	LLDP-MED 電源管理 TLV

インターフェイスで TLV をイネーブルにするには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **lldp med-tlv-select**
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ (config)# **interface gigabitethernet2/0/1**	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lldp med-tlv-select** 例： スイッチ(config-if)# **lldp med-tlv-select inventory management**	イネーブルにする TLV を指定します。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Network-Policy TLV の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **network-policy profile***profile number*
4. {**voice** | **voice-signaling**} **vlan** [*vlan-id* {**cos***cvalue* | **dscp***dvalue*}] | [[**dot1p** {**cos***cvalue* | **dscp***dvalue*}] | **none** | **untagged**]
5. **exit**
6. **interface***interface-id*
7. **network-policy***profile number*
8. **lldp med-tlv-select network-policy**
9. **end**
10. **show network-policy profile**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**network-policy profile***profile number* 例： スイッチ(config)# **network-policy profile 1**	ネットワーク ポリシープロファイル番号を指定し、ネットワーク ポリシー コンフィギュレーション モードを開始します。指定できる範囲は 1 ～ 4294967295 です。
ステップ 4	{**voice** | **voice-signaling**} **vlan** [*vlan-id* {**cos***cvalue* | **dscp***dvalue*}] | [[**dot1p** {**cos***cvalue* | **dscp***dvalue*}] | **none** | **untagged**]	ポリシー属性の設定： • **voice**：音声アプリケーション タイプを指定します。 • **voice-signaling**：音声シグナリング アプリケーション タイプを指定します。

	コマンドまたはアクション	目的
	例： スイッチ(config-network-policy)# **voice vlan 100 cos 4**	• **vlan**：音声トラフィックのネイティブ VLAN を指定します。 • *vlan-id*：（任意）音声トラフィックの VLAN を指定します。指定できる範囲は 1 ～ 4094 です。 • **cos***cvalue*：（任意）設定された VLAN のレイヤ 2 プライオリティ サービス クラス（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。 • **dscp***dvalue*：（任意）設定された VLAN の Differentiated Services Code Point（DSCP）値を指定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 46 です。 • **dot1p**：（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話機を設定します。 • **none**：（任意）音声 VLAN に関して IP Phone に指示しません。IP Phone のキーパッドから入力された設定を使用します。 • **untagged**：（任意）タグなしの音声トラフィックを送信するように IP Phone を設定します。これが IP Phone のデフォルト設定になります。 • **untagged**：（任意）タグなしの音声トラフィックを送信するように IP Phone を設定します。これが IP Phone のデフォルト設定になります。
ステップ 5	**exit** 例： スイッチ(config)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface***interface-id* 例： スイッチ (config)# **interface gigabitethernet2/0/1**	ネットワーク ポリシー プロファイルを設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**network-policy***profile number* 例： スイッチ(config-if)# **network-policy**	ネットワーク ポリシー プロファイル番号を指定します。

	コマンドまたはアクション	目的
	`1`	
ステップ 8	**lldp med-tlv-select network-policy** 例： `スイッチ(config-if)# lldp med-tlv-select network-policy`	ネットワーク ポリシー TLV を指定します。
ステップ 9	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show network-policy profile** 例： `スイッチ# show network-policy profile`	設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ロケーション TLV およびワイヤード ロケーション サービスの設定

エンドポイントのロケーション情報を設定し、その設定をインターフェイスに適用するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **location** {**admin-tag** *string* | **civic-location identifier** {*id* | **host**} | **elin-location** *string* **identifier** *id* | **custom-location identifier** {*id* | **host**} | **geo-location identifier** {*id* | **host**}}
3. **exit**
4. **interface** *interface-id*
5. **location** {**additional-location-information** *word* | **civic-location-id** {*id* | **host**} | **elin-location-id** *id* | **custom-location-id** {*id* | **host**} | **geo-location-id** {*id* | **host**} }
6. **end**
7. 次のいずれかを使用します。
   - **show location admin-tag** *string*
   - **show location civic-location identifier** *id*
   - **show location elin-location identifier** *id*
8. **copy running-config startup-config**

手順の詳細

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

ステップ 2	**location** {**admin-tag** *string* | **civic-location identifier** {*id* | **host**} | **elin-location** *string* **identifier** *id* | **custom-location identifier** {*id* | **host**} | **geo-location identifier** {*id* | **host**}}
	
	例：
	
	`スイッチ(config)# location civic-location identifier 1`
	`スイッチ(config-civic)# number 3550`
	`スイッチ(config-civic)# primary-road-name "Cisco Way"`
	`スイッチ(config-civic)# city "San Jose"`
	`スイッチ(config-civic)# state CA`
	`スイッチ(config-civic)# building 19`
	`スイッチ(config-civic)# room C6`
	`スイッチ(config-civic)# county "Santa Clara"`
	`スイッチ(config-civic)# country US`
		エンドポイントにロケーション情報を指定します。
		• **admin-tag**：管理タグまたはサイト情報を指定します。
		• **civic-location**：都市ロケーション情報を指定します。
		• **elin-location**：緊急ロケーション情報（ELIN）を指定します。
		• **custom-location**：カスタム ロケーション情報を指定します。
		• **geo-location**：地理空間のロケーション情報を指定します。
		• **identifier** *id*：都市、ELIN、カスタム、または地理ロケーションの ID を指定します。

	コマンドまたはアクション	目的
		• **host**：ホストの都市、カスタム、または地理ロケーションを指定します。 • *string*：サイト情報またはロケーション情報を英数字形式で指定します。
ステップ 3	**exit** 例： `スイッチ(config-civic)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**interface** *interface-id* 例： `スイッチ (config)# interface gigabitethernet2/0/1`	ロケーション情報を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**location** {**additional-location-information** *word* | **civic-location-id** {*id* | **host**} | **elin-location-id** *id* | **custom-location-id** {*id* | **host**} | **geo-location-id** {*id* | **host**} } 例： `スイッチ(config-if)# location elin-location-id 1`	インターフェイスのロケーション情報を入力します。 • **additional-location-information**：ロケーションまたは場所に関する追加情報を指定します。 • **civic-location-id**：インターフェイスのグローバル都市ロケーション情報を指定します。 • **elin-location-id**：インターフェイスの緊急ロケーション情報を指定します。 • **custom-location-id**：インターフェイスのカスタム ロケーション情報を指定します。 • **geo-location-id**：インターフェイスの地理空間のロケーション情報を指定します。 • **host**：ホストのロケーションの ID を指定します。 • *word*：追加のロケーション情報を指定する語またはフレーズを指定します。 • *id*：都市、ELIN、カスタム、または地理ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

ステップ 7	次のいずれかを使用します。
	• **show location admin-tag** *string*
	• **show location civic-location identifier** *id*
	• **show location elin-location identifier** *id*
	
	例：
	`スイッチ# show location admin-tag`
	または
	`スイッチ# show location civic-location identifier`
	または
	`スイッチ# show location elin-location identifier`
		設定を確認します。

ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ上でのワイヤード ロケーション サービスのイネーブル化

はじめる前に

ワイヤード ロケーションが機能するためには、まず、**ip device tracking** グローバル コンフィギュレーション コマンドを入力する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **nmsp notification interval** {**attachment** | **location**} *interval-seconds*
4. **end**
5. **show network-policy profile**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**nmsp notification interval** {**attachment** | **location**} *interval-seconds* 例： スイッチ(config)# **nmsp notification interval location 10**	NMSP 通知間隔を指定します。 **attachment**：接続通知間隔を指定します。 **location**：位置通知間隔を指定します。 *interval-seconds*：スイッチから MSE にロケーション更新または接続更新が送信されるまでの期間（秒）。指定できる範囲は 1 ～ 30 です。デフォルト値は 30 です。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show network-policy profile** 例： スイッチ# **show network-policy profile**	設定を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

Network-Policy TLV の設定：例

次に、CoS を持つ音声アプリケーションの VLAN 100 を設定して、インターフェイス上のネットワーク ポリシー プロファイルおよびネットワーク ポリシー TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# network-policy 1
Switch(config-network-policy)# voice vlan 100 cos 4
Switch(config-network-policy)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# network-policy profile 1
Switch(config-if)# lldp med-tlv-select network-policy
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
Switchconfig-network-policy)# voice vlan dot1p cos 4
Switchconfig-network-policy)# voice vlan dot1p dscp 34
```

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

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

コマンド	説明
clear lldp counters	トラフィック カウンタを 0 にリセットします。
clear lldp table	LLDP ネイバー情報テーブルを削除します。

コマンド	説明
clear nmsp statistics	NMSP 統計カウンタをクリアします。
show lldp	送信頻度、送信するパケットのホールドタイム、LLDP初期化の遅延時間のような、インターフェイス上のグローバル情報を表示します。
show lldp entry *entry-name*	特定のネイバーに関する情報を表示します。 アスタリスク（*）を入力すると、すべてのネイバーの表示、またはネイバーの名前の入力が可能です。
show lldp interface [*interface-id*]	LLDP がイネーブルに設定されているインターフェイスに関する情報を表示します。 表示対象を特定のインターフェイスに限定できます。
show lldp neighbors [*interface-id*] [**detail**]	デバイスタイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、ポート ID など、ネイバーに関する情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show lldp traffic	送受信パケットの数、廃棄したパケットの数、認識できない TLV の数など、LLDP カウンタを表示します。
show location admin-tag *string*	指定した管理タグまたはサイトのロケーション情報を表示します。
show location civic-location identifier *id*	特定のグローバル都市ロケーションのロケーション情報を表示します。
show location elin-location identifier *id*	緊急ロケーションのロケーション情報を表示します。
show network-policy profile	設定されたネットワークポリシープロファイルを表示します。
show nmsp	NMSP 情報を表示します。

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

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

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

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 7 章

システム MTU の設定

- システム MTU の設定，125 ページ

システム MTU の設定

このモジュールは、Cisco Catalyst 3650 シリーズ スイッチおよび Catalyst 3850 シリーズ スイッチ システムの最大伝送ユニットの設定方法について説明します。

機能情報の確認

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

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

MTU に関する情報

すべてのスイッチ インターフェイスで送受信されるフレームのデフォルト MTU サイズは、1500 バイトです。

システム MTU の制約事項

システム MTU 値を設定する場合、次の注意事項に留意してください。

- スイッチはインターフェイス単位では MTU をサポートしていません。

- **system mtu***bytes* グローバル コンフィギュレーション コマンドを入力すると、スイッチでコマンドが有効になりません。このコマンドが有効になるのは、ファスト イーサネット ポートにおけるシステム MTU サイズに対してだけです。

システム MTU 値の適用

スイッチ スタックでは、スイッチ メンバーに適用される MTU 値は、スタックの設定によって異なります。次のスタック設定がサポートされます。

IP または IPv6 MTU 値の上限は、スイッチスイッチ スタックの設定に基づいており、現在適用されているシステム MTU 値またはシステム ジャンボ MTU 値を参照しています。MTU サイズの設定については、このリリースのコマンドリファレンスの**system mtu** グローバル コンフィギュレーション コマンドを参照してください。

システム MTU の設定

システム MTU の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **systemmtu***bytes*
4. **exit**
5. **showsystemmtu**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**systemmtu***bytes* 例： `Switch(config)# system mtu 1600`	スイッチまたはスイッチ スタックのすべてのイーサネット インターフェイスの最大伝送ユニット（MTU）サイズを適用します。 • MTU の範囲は 1500 ～ 9198 です。デフォルトは 1500 です。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Switch(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**showsystemmtu** 例： `Switch# show system mtu`	設定されたグローバル MTU サイズが表示されます。

Protocol-Specific MTU の設定

システムの MTU が変更されると、インターフェイスの **ip mtu** コマンドの範囲も変更されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **ipmtu***bytes*
5. **ipv6mtu***bytes*
6. **end**
7. **showsystemmtu**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Switch(config)# interface gigabitethernet 0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ipmtu***bytes* 例： `Switch(config-if)# ip mtu 900`	各インターフェイスにおいて送信される IP パケットの最大伝送単位（MTU）サイズを設定します。 • 範囲は 832 ～ 1500 です。
ステップ 5	**ipv6mtu***bytes* 例： `Switch(config-if)# ipv6 mtu 1300`	インターフェイス上で送信する IPv6 パケットの MTU サイズを設定します。 • 範囲は 1280 ～ 1500 です。
ステップ 6	**end** 例： `Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**showsystemmtu** 例： `Switch# show system mtu`	設定されたグローバル MTU サイズを表示します。

システム MTU の設定例

例：システム MTU の設定

```
Switch# configure terminal
Switch(config)# system mtu 1600
Switch(config)# exit
```

例：プロトコル固有の MTU の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/0
Switch(config-if)# ip mtu 900
Switch(config-if)# ipv6 mtu 1286
Switch(config-if)# end
```

システム MTU に関する追加情報

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

システム MTU の機能情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 8 章

内部電源装置の設定

- 内部電源装置に関する情報，131 ページ
- 内部電源装置の設定方法，131 ページ
- 内部電源装置のモニタ，132 ページ
- 内部電源装置の設定例，133 ページ
- その他の参考資料，134 ページ
- 内部電源装置の機能履歴と情報，135 ページ

内部電源装置に関する情報

電源装置に関する情報については、スイッチのインストレーション ガイドを参照してください。

内部電源装置の設定方法

内部電源装置の設定

power supply EXEC コマンドを使用すると、スイッチの内部電源装置の設定および管理ができます。スイッチは、**no power supply** EXEC コマンドをサポートしていません。

ユーザ EXEC モードで開始し、次の手順に従います。

手順の概要

1. **power supply***switch_number***slot**{**A** | **B**} {**off** | **on**}
2. **show environment power**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**power supply***switch_number***slot**{**A** | **B**} {**off** | **on**} 例： スイッチ# **power supply 1 slot A on**	次のいずれかのキーワードを使用して、指定した電源装置を **off** または **on** に設定します。 • **A**：スロット A の電源装置を選択します。 • **B**：スロット B の電源装置を選択します。 （注） 電源装置のスロット B は、スイッチの外側エッジに近いほうです。 • **off**：電源装置をオフに設定します。 • **on**：電源装置をオンに設定します。 デフォルトでは、スイッチの電源装置は **on** です。
ステップ 2	**show environment power** 例： スイッチ# **show environment power**	設定を確認します。

内部電源装置のモニタ

表 *12*：電源装置の ***show*** コマンド

コマンド	目的
show environment power [**all** | **switch***switch_number*]	（任意）スタック内の各スイッチまたは指定したスイッチの内部電源装置のステータスを表示します。指定できる範囲は、スタック内のスイッチ メンバ番号に従って 1 ～ 9 です。 スイッチキーワードは、スタック対応スイッチ上でだけ使用できます。

内部電源装置の設定例

次に、スロット A の電源装置をオフに設定する例を示します。

```
スイッチ# power supply 1 slot A off
Disabling Power supply A may result in a power loss to PoE devices and/or switches ...
Continue? (yes/[no]): yes
スイッチ#
Jun 10 04:52:54.389: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered off
Jun 10 04:52:56.717: %PLATFORM_ENV-1-FAN_NOT_PRESENT: Fan is not present
スイッチ#
```

次に、スロット A の電源装置をオンに設定する例を示します。

```
スイッチ# power supply 1 slot A on
Jun 10 04:54:39.600: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered on
```

次に、**show env power** コマンドの出力例を示します。

```
スイッチ# show env power

SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--- ------------------  ----------  ---------------  -------  -------  -----
1A  PWR-C2-640WAC       DCB1705B05B OK               Good     Good     640
1B  Not Present

スイッチ#
```

表 *13*：*show env power* ステータスの説明

フィールド	説明
OK	電源装置が存在し、電力が良好です。
Not Present	電源装置が未搭載です。
No Input Power	電源装置は存在しますが、入力電力が供給されていません。
Disabled	電源装置が存在し、入力電力は供給されていますが、電源装置が CLI によってオフになっています。
Not Responding	電源装置が認識されていないか、障害が発生しています。
Failure-Fan	電源装置のファンに障害が発生しています。

その他の参考資料

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

内部電源装置の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 9 章

PoE の設定

- 機能情報の確認，137 ページ
- PoE について，137 ページ
- PoE の設定方法，143 ページ
- 電力ステータスのモニタ，150 ページ
- その他の参考資料，150 ページ
- PoE の機能情報，151 ページ

機能情報の確認

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

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

PoE について

Power over Ethernet（PoE）ポート

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

- シスコ先行標準受電デバイス（Cisco IP Phone および Cisco Aironet アクセス ポイントなど）

- IEEE 802.3af 準拠の受電装置

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

サポート対象のプロトコルおよび標準

スイッチは PoE のサポートで次のプロトコルと規格を使用します。

- 電力消費について CDP を使用：受電装置は、消費している電力量をスイッチに通知します。スイッチはこの電力消費に関するメッセージに応答しません。スイッチは、PoE ポートに電力を供給するか、このポートへの電力を取り除くだけです。
- シスコ インテリジェント電力管理：受電装置およびスイッチは、電力ネゴシエーション CDP メッセージによって電力消費レベルについてネゴシエーションを行います。このネゴシエーションにより、7 W より多くを消費する高電力のシスコ受電デバイスは、最も高い電力モードで動作できるようになります。受電デバイスは、最初に低電力モードでブートして 7 W 未満の電力を消費し、ネゴシエーションを行って高電力モードで動作するための十分な電力を取得します。受電装置が高電力モードに切り替わるのは、スイッチから確認を受信した場合に限られます。

  高電力装置は、電力ネゴシエーション CDP をサポートしないスイッチで低電力モードで動作できます。

  シスコのインテリジェントな電力管理の機能には、電力消費に関して CDP との下位互換性があるため、スイッチは、受信する CDP メッセージに従って応答します。CDP はサードパーティの受電デバイスをサポートしません。このため、スイッチは IEEE 分類を使用して装置の消費電力を判断します。
- IEEE 802.3a：この規格の主な機能は、受電装置の検出、電力の管理、切断の検出です。オプションとして受電装置の電力分類があります。詳細については、この規格を参照してください。
- Cisco UPoE 機能は、CDP や LLDP などのレイヤ 2 電力ネゴシエーション プロトコルを使用して、シグナル ペアおよび RJ-45 イーサネット ケーブルのスペア ペアの両方に、最大 60 W の電力（2 X 30 W）を供給します。4 線式 Cisco 独自開発スペ アペア電力 TLV での 30 W 以上の LLDP および CDP 要求により、スペア ペアに電力を供給できます。

関連トピック

Cisco Universal Power Over Ethernet, （143 ページ）

受電装置の検出および初期電力割り当て

スイッチは、PoE 対応ポートがシャットダウンの状態でなく、PoE はイネーブルになっていて（デフォルト）、接続した装置は AC アダプタから電力供給されていない場合、シスコの先行標準受電装置または IEEE 準拠の受電装置を検出します。

装置の検出後、スイッチは、次のように装置のタイプに応じて電力要件を判断します。

- 初期電力割り当ては、受電デバイスが要求する最大電力量です。スイッチは、受電装置を検出および電力供給する場合、この電力を最初に割り当てます。スイッチが受電装置からCDPメッセージを受信し、受電装置がCDP電力ネゴシエーション メッセージを通じてスイッチと電力レベルをネゴシエートしたときに、初期電力割り当てが調整される場合があります。
- スイッチは検出したIEEE装置を消費電力クラス内で分類します。スイッチは、電力バジェットに使用可能な電力量に基づいて、ポートに通電できるかどうかを決定します。表14：IEEE電力分類, （139ページ） に、各種レベルの一覧を示します。

表 *14*：*IEEE* 電力分類

クラス	スイッチから要求される最大電力レベル
0（クラス ステータスは不明）	15.4 W
1	4 W
2	7 W
3	15.4 W
4	30 W（IEEE 802.3at タイプ 2 準拠の受電デバイスの場合）

スイッチは電力要求をモニタリングおよび追跡して必要な場合にだけ電力供給を許可します。スイッチは自身の電力バジェット（PoE のスイッチで使用可能な電力量）を追跡します。電力の供給許可または拒否がポートで行われると、スイッチはパワーアカウンティング計算を実行し、電力バジェットを最新に保ちます。

電力がポートに適用されたあとで、スイッチは CDP を使用して、接続されたシスコ受電装置の *CDP* 固有の電力消費要件を調べます。この要件は、CDPメッセージに基づいて割り当てられる電力量です。これに従って、スイッチは電力バジェットを調整します。これは、サードパーティの PoE 装置には適用されません。スイッチは要件を処理して電力の供給を許可または拒否します。要求が許可されると、スイッチは電力バジェットを更新します。要求が拒否された場合は、スイッチはポートの電力がオフに切り替わっていることを確認し、syslog メッセージを生成して LED を更新します。受電装置はより多くの電力について、スイッチとのネゴシエーションを行うこともできます。

PoE+ では、受電装置が最大 30 W の電力ネゴシエーションのために、Media Dependent Interface（MDI）の Type, Length, and Value description（TLV）、Power-via-MDI TLV で IEEE 802.3at および LLDP 電源を使用します。シスコの先行標準受電装置およびIEEE受電装置では、CDP またはIEEE 802.3at power-via-MDI 電力ネゴシエーション メカニズムにより最大 30 W の電力レベルを要求できます。

（注） クラス 0、クラス 3、およびクラス 4 の受電装置の初期割り当ては 15.4 W です。装置が起動し、CDP または LLDP を使用して 15.4 W を超える要求を送信する場合、最大 30 W を割り当てることができます。

（注） ソフトウェア コンフィギュレーション ガイドおよびコマンド リファレンスでは、CDP 固有の電力消費要件を実際電力消費要件と呼んでいます。

不足電圧、過電圧、オシレータ障害、または短絡状態による障害をスイッチが検出した場合、ポートへの電源をオフにし、syslog メッセージを生成し、電力バジェットと LED を更新します。

PoE 機能は、スイッチがスタック メンバーであるかどうかに関係なく、同じように動作します。電力バジェットはスイッチごとであり、スタックの他のスイッチとは無関係です。新しいアクティブ スイッチの選択は、PoE の動作に影響を与えません。アクティブ スイッチは、スタック内のすべてのスイッチおよびポートの PoE のステータスを追跡し続け、出力表示にそのステータスを含めます。

電力管理モード

スイッチでは、次の PoE モードがサポートされます。

- **auto**：接続されている装置で電力が必要であるかどうか、スイッチが自動的に検出します。ポートに接続されている受電装置をスイッチが検出し、スイッチに十分な電力がある場合、スイッチは電力を供給して電力バジェットを更新し、先着順でポートの電力をオンに切り替えて LED を更新します。LED の詳細については、ハードウェア インストレーション ガイドを参照してください。

  すべての受電装置用としてスイッチに十分な電力がある場合は、すべての受電装置が起動します。スイッチに接続された受電装置すべてに対し十分な電力が利用できる場合、すべての装置に電力を供給します。使用可能な PoE がない場合、または他の装置が電力供給を待機している間に装置の接続が切断されて再接続した場合、どの装置へ電力を供給または拒否されるかが判断できなくなります。

  許可された電力がシステムの電力バジェットを超えている場合、スイッチは電力を拒否し、ポートへの電力がオフになっていることを確認したうえで syslog メッセージを生成し、LED を更新します。電力供給が拒否された後、スイッチは定期的に電力バジェットを再確認し、継続して電力要求の許可を試みます。

  スイッチにより電力を供給されている装置が、さらに壁面コンセントに接続している場合、スイッチは装置に電力を供給し続ける場合があります。このとき、装置がスイッチから受電しているか、AC 電源から受電しているかにかかわらず、スイッチは引き続き装置へ電力を供給していることを報告し続ける場合があります。

  受電装置が取り外された場合、スイッチは切断を自動的に検出し、ポートから電力を取り除きます。非受電装置を接続しても、その装置に障害は発生しません。

ポートで許可される最大ワット数を指定できます。受電装置の IEEE クラス最大ワット数が設定されている最大値より大きい場合、スイッチはそのポートに電力を供給しません。スイッチが受電装置に電力供給したが、受電装置が設定の最大値より多くの電力を CDP メッセージによって後で要求した場合、スイッチはポートの電力を取り除きます。その受電デバイスに割り当てられていた電力は、グローバル電力バジェットに送られます。ワット数を指定しない場合、スイッチは最大値の電力を供給します。任意の PoE ポートで **auto** 設定を使用してください。auto モードがデフォルト設定です。

- **static**：スイッチは、受電装置が接続されていなくてもポートに電力をあらかじめ割り当て、そのポートで電力が使用できるようにします。スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電装置からの CDP メッセージによって調節されることはありません。これは、電力があらかじめ割り当てられていることから、最大ワット数以下の電力を使用するすべての受電デバイスが固定ポートに接続されている場合に電力が保証されるためです。ポートはもう先着順方式ではなくなります。

  ただし、受電装置の IEEE クラスが最大ワット数を超えると、スイッチは装置に電力を供給しません。受電装置が最大ワット数を超える電力を消費していることを CDP メッセージによってスイッチが認識すると、スイッチは受電装置をシャットダウンします。

  ワット数を指定しない場合、スイッチは最大値をあらかじめ割り当てます。スイッチは、受電装置を検出した場合に限り、ポートに電力を供給します。優先順位が高いインターフェイスには、**static** 設定を使用してください。

- **never**：スイッチは受電装置の検出をディセーブルにして、電力が供給されていない装置が接続されても、PoE ポートに電力を供給しません。PoE 対応ポートに電力を絶対に適用せず、そのポートをデータ専用ポートにする場合に限り、このモードを使用してください。

ほとんどの場合、デフォルトの設定（自動モード）の動作は適切に行われ、プラグアンドプレイ動作が提供されます。それ以上の設定は必要ありません。しかし、プライオリティの高いPoEポートを設定したり、PoE ポートをデータ専用にしたり、最大ワット数を指定して高電力受電デバイスをポートで禁止したりする場合は、このタスクを実行します。

電力モニタリングおよび電力ポリシング

リアルタイムの消費電力のポリシングをイネーブルにした場合、受電装置が最大割り当て（カットオフ電力値）を超えて電力を消費すると、スイッチはアクションを開始します。

PoE がイネーブルである場合、スイッチは受電装置のリアルタイムの電力消費を検知します。接続されている受電装置のリアルタイム電力消費をスイッチが監視することを、電力モニタリングまたは電力検知といいます。また、スイッチはパワー ポリシング機能を使用して消費電力をポリシングします。

電力モニタリングは、シスコのインテリジェントな電力管理およびCDPベースの消費電力に対して下位互換性があります。電力モニタリングはこれらの機能とともに動作して、PoE ポートが受電デバイスに電力を供給できるようにします。

スイッチは次のようにして、接続されている装置のリアルタイム電力消費を検知します。

1. スイッチは、個々のポートでリアルタイム消費電力をモニタリングします。
2. スイッチは、ピーク時の電力消費を含め、電力消費を記録します。スイッチは CISCO-POWER-ETHERNET-EXT-MIB を介して情報を報告します。

3 電力ポリシングがイネーブルの場合、スイッチはリアルタイムの消費電力を装置に割り当てられた最大電力と比較して、消費電力をポリシングします。最大消費電力は、PoEポートでカットオフ電力とも呼ばれます。

装置がポートで最大電力割り当てを超える電力を使用すると、スイッチはポートへの電力をオフにしたり、またはスイッチコンフィギュレーションに基づいて受電装置に電力を供給しながらスイッチが syslog メッセージを生成して LED（ポート LED はオレンジ色で点滅）を更新したりすることができます。デフォルトでは、すべての PoE ポートで消費電力のポリシングはディセーブルになっています。

PoE の errdisable ステートからのエラー回復がイネーブルの場合、指定の時間の経過後、スイッチは PoE ポートを errdisable ステートから自動的に回復させます。

エラー回復がディセーブルの場合、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを使用して、手動で PoE ポートをイネーブルにできます。

4 ポリシングがディセーブルである場合、受電装置がPoEポートに割り当てられた最大電力より多くの量を消費しても対処されないため、スイッチに悪影響を与える場合があります。

電力消費値

ポートの初期電力割り当ておよび最大電力割り当てを設定することができます。ただし、これらの値は、スイッチが PoE ポートの電力をオンまたはオフにするときを指定するために設定する値です。最大電力割り当ては、受電デバイスの実際の電力消費と同じではありません。スイッチによって電力ポリシングに使用される実際のカットオフ電力値は、設定済みの電力値と同等ではありません。

電力ポリシングがイネーブルの場合、スイッチは、スイッチ ポートで、受電装置の消費電力を超える消費電力ポリシングを行います。最大電力割り当てを手動で設定する場合、スイッチ ポートと受電デバイス間のケーブルでの電力損失を考慮する必要があります。カットオフ電力とは、受電デバイスの定格消費電力とケーブル上での最悪時の電力損失を合計したものです。

スイッチの PoE がイネーブルの場合、電力ポリシングをイネーブルにすることを推奨します。たとえば、ポリシングがディセーブルで、**power inline auto max6300** インターフェイス コンフィギュレーション コマンドを使用してカットオフ値を設定すると、PoE ポートに設定される最大電力割り当ては 6.3 W（6300 mW）です。装置が最大で 6.3 W の電力を必要とする場合、スイッチはポートに接続されている装置に電力を供給します。CDP によるパワーネゴシエーション実施後の値またはIEEE分類値が設定済みカットオフ値を超えると、スイッチは接続されている装置に電力を供給しなくなります。スイッチが PoE ポートで電力をオンにしたあとは、スイッチは受電装置のリアルタイム電力消費のポリシングを行わないので、受電装置は最大割り当て量を超えて電力を消費できることになり、スイッチと、他の PoE ポートに接続されている受電装置に悪影響を及ぼすことがあります。

スタンドアロン スイッチでは内部電源装置がサポートされるため、受電装置が利用できる総電力量は電源装置の設定によって異なります。

- 電源装置を取り外して、低電力の新しい電源装置に交換すると、スイッチは受電装置に対して十分な電力を供給できなくなり、スイッチは auto モードでポート番号の降順に従って PoE ポートへの電力供給を拒否します。スイッチがこれでも十分な電力を利用できない場合、スイッチは、static モードでポート番号の降順に従ってPoEポートへの電力供給を拒否します。

- 新しい電源装置の電力が前の電源装置より大きく、スイッチが大電力を使用できる場合、スイッチは static モードでポート番号の昇順に従って PoE ポートへの電力供給を許可します。これでもまだ使用可能な電力がある場合、スイッチスイッチは、ポート番号の昇順に従って auto モードで PoE ポートへの電力供給を許可します。

Cisco Universal Power Over Ethernet

Cisco Universal Power Over Ethernet（Cisco UPOE）は、シグナル ペア（導線 1、2、3、6）付きの RJ-45 ケーブルのスペア ペア（導線 4、5、7、8）を使用して、IEEE 802.at PoE 標準を拡張するシスコ独自のテクノロジーで、標準のイーサネット ケーブル配線インフラストラクチャ（クラス D 以上）により最大 60 W の電力を供給する機能を提供します。スペア ペアの電力は、スイッチ ポートとエンドデバイスが Cisco UPOE 対応であることを CDP または LLDP を使用して相互に識別し、エンドデバイスがスペア ペアの電力のイネーブル化を要求したときにイネーブルになります。スペア ペアに給電されると、エンドデバイスは、CDP または LLDP を使用して、スイッチから最大 60 W の電力をネゴシエートできます。

エンド デバイスがシグナル ペアおよびスペア ペアの両方で PoE 対応であるが、Cisco UPOE に必要な CDP または LLDP の拡張をサポートしない場合、4 ペアの強制モード設定により自動的にスイッチ ポートからシグナル ペアおよびスペア ペアの両方の電力がイネーブルになります。

PoE の設定方法

PoE ポートの電力管理モードの設定

（注） PoE 設定を変更するとき、設定中のポートでは電力が低下します。新しい設定、その他の PoE ポートの状態、電力バジェットの状態により、そのポートの電力は再びアップしない場合があります。たとえば、ポート 1 が自動でオンの状態になっていて、そのポートを固定モードに設定するとします。スイッチはポート 1 から電力を取り除き、受電デバイスを検出してポートに電力を再び供給します。ポート 1 が自動でオンの状態になっていて、最大ワット数を 10 W に設定した場合、スイッチはポートから電力を取り除き、受電デバイスを再び検出します。スイッチは、受電デバイスがクラス 1、クラス 2、またはシスコ専用受電デバイスのいずれかの場合に、ポートに電力を再び供給します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **power inline** {**auto** [**max***max-wattage*] | **never** | **static** [**max***max-wattage*]}
5. **end**
6. **show power inline** [*interface-id* | **module***switch-number*]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet2/0/1`	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**power inline** {**auto** [**max***max-wattage*] | **never** | **static** [**max***max-wattage*]} 例： `スイッチ(config-if)# power inline auto`	ポートの PoE モードを設定します。キーワードの意味は次のとおりです。 • **auto**：受電デバイスの検出をイネーブルにします。十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。これがデフォルト設定です。 • **max***max-wattage*：ポートで許可されている電力を制限します。値を指定しない場合は、最大電力が供給されます。 • **max***max-wattage*：ポートで許可されている電力を制限します。Cisco UPoE ポートの範囲は 4000 ~ 60000 mW です。値が指定されていない場合は、最大値が許可されます。 • **never**：装置検出とポートへの電力供給をディセーブルにします。

	コマンドまたはアクション	目的
		（注） ポートにシスコの受電デバイスが接続されている場合は、**power inline never** コマンドでポートを設定しないでください。問題のあるリンクアップが発生し、ポートが errdisable ステートになることがあります。 • **static**：受電デバイスの検出をイネーブルにします。スイッチが受電デバイスを検出する前に、ポートへの電力を事前に割り当てます（確保します）。スイッチは、装置が接続されていなくてもこのポートに電力を予約し、装置の検出時に電力が供給されることを保証します。 スイッチは、自動モードに設定されたポートに電力を割り当てる前に、固定モードに設定されたポートに PoE を割り当てます。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show power inline** [*interface-id* | **module***switch-number*] 例： スイッチ# **show power inline**	スイッチまたはスイッチ スタック、指定したインターフェイス、または指定したスタック メンバに関する PoE ステータスを表示します。 **module***switch-number* キーワードは、スタッキング対応スイッチだけでサポートされます。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

シグナル/スペア ペアの電力のイネーブル化

（注） エンドデバイスがスペア ペアのインライン パワー給電に未対応の場合、またはエンドデバイスが Cisco UPoE に CDP または LLDP 拡張をサポートしている場合は、このコマンドを入力しないでください。

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **power inline four-pair forced**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**power inline four-pair forced** 例： スイッチ(config-if)# **power inline four-pair forced**	スイッチ ポートから信号ペアおよびスペア ペアの両方の電力をイネーブルにします。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

電力ポリシングの設定

デフォルトでは、スイッチは接続されている受電装置の消費電力をリアルタイムでモニタリングします。消費電力に対するポリシングを行うようにスイッチを設定できます。デフォルトではポリシングはディセーブルです。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **power inline police** [**action**{**log** | **errdisable**}]
5. **exit**
6. 次のいずれかを使用します。
   - **errdisable detect cause inline-power**
   - **errdisable recovery cause inline-power**
   - **errdisable recovery interval***interval*
7. **exit**
8. 次のいずれかを使用します。
   - **show power inline police**
   - **show errdisable recovery**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**power inline police** [**action**{**log** | **errdisable**}] 例： スイッチ(config-if)# **power inline police**	ポートでリアルタイム消費電力が最大電力割り当てを超えるときに、次のいずれかのアクションを実行するようにスイッチを設定します。 • **power inline police**：PoE ポートをシャットダウンし、ポートへの電力供給をオフにし、PoE ポートを error-disabled ステートに移行します。 （注） **errdisable detect cause inline-power** グローバル コンフィギュレーション コマンドを使用すると、PoE error-disabled の原因についてエラー検出をイネーブルにできます。**errdisable recovery cause inline-powerinterval***interval* グローバル コンフィギュレーション コマンドを使用すると、PoE error-disabled ステートから回復するためのタイマーをイネーブルにすることもできます。 • **power inline police action errdisable**：リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、ポートへの電力をオフにします。 • **power inline police action log**：ポートに電力を供給しながら syslog メッセージを生成します。 **action log** キーワードを入力しない場合、デフォルトのアクションによってポートがシャットダウンされ、errdisable ステートになります。
ステップ 5	**exit** 例： スイッチ(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	次のいずれかを使用します。 • **errdisable detect cause inline-power** • **errdisable recovery cause inline-power** • **errdisable recovery interval***interval*	（任意）PoE errdisable ステートからのエラー回復をイネーブルにし、PoE 回復メカニズム変数を設定します。 デフォルトでは、回復間隔は 300 秒です。 **interval***interval* では、err-disabled ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。

	コマンドまたはアクション	目的
	例： スイッチ(config)# **errdisable detect cause inline-power** スイッチ(config)# **errdisable recovery cause inline-power** スイッチ(config)# **errdisable recovery interval 100**	
ステップ 7	**exit** 例： スイッチ(config)# **exit**	特権 EXEC モードに戻ります。
ステップ 8	次のいずれかを使用します。 • **show power inline police** • **show errdisable recovery** 例： スイッチ# **show power inline police** スイッチ# **show errdisable recovery**	電力モニタリング ステータスを表示し、エラー回復設定を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

電力ステータスのモニタ

表 *15*：電力ステータスの ***show*** コマンド

コマンド	目的
show env power switch[*switch-number*]	（任意）スタック内の各スイッチまたは指定したスイッチの内部電源装置のステータスを表示します。 指定できる範囲は、スタック内のスイッチ メンバ番号に従って 1 ～ 9 です。次のキーワードは、スタック対応スイッチ上でだけ使用できます。
show power inline[*interface-id* | **module***switch-number*]	スイッチまたはスイッチ スタック、インターフェイス、またはスタック内の特定のスイッチの PoE ステータスを表示します。
show power inline police	電力ポリシングのデータを表示します。

その他の参考資料

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

PoE の機能情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 10 章

EEE の設定

- 機能情報の確認，153 ページ
- EEE について，154 ページ
- EEE の制約事項，154 ページ
- EEE の設定方法，154 ページ
- EEE のモニタリング，156 ページ
- EEE の設定例，156 ページ
- その他の参考資料，157 ページ
- EEE 設定の機能履歴と情報，158 ページ

機能情報の確認

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

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

EEE について

EEE の概要

Energy Efficient Ethernet (EEE) は、アイドル時間にイーサネット ネットワークの消費電力を減らすように設計された IEEE 802.3az の標準です。

低電力アイドル（LPI）モードをサポートするデバイスで EEE をイネーブルにできます。このようなデバイスは、低い使用率のときに LPI モードを開始して、電力を節約できます。LPI モードでは、リンクの両端にあるシステムは、特定のサービスをシャット ダウンして、電力を節約できます。EEE は上位層プロトコルおよびアプリケーションに対して透過的であるように、LPI モードに移行したり、LPI モードから移行する必要があるプロトコルを提供します。

デフォルトの EEE 設定

EEE はデフォルトでディセーブルになっています。

EEE の制約事項

EEE には、次の制約事項があります。

- EEE の設定を変更すると、デバイスがレイヤ 1 の自動ネゴシエーションを再起動しなければならないため、インターフェイスがリセットされます。
- 受信パスでデータを受け入れる前により長いウェイク アップ時間を必要とするデバイスのリンク層検出プロトコル（LLDP）をイネーブルにする必要がある場合があります。これにより、デバイスは送信リンク パートナーから拡張システムのウェイク アップ時間についてネゴシエーションできます。

EEE の設定方法

EEE 対応リンク パートナーに接続されているインターフェイスの EEE をイネーブルまたはディセーブルにできます。

EEE のイネーブル化またはディセーブル化

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **power efficient-ethernet auto**
4. **no power efficient-ethernet auto**
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**power efficient-ethernet auto** 例： スイッチ(config-if)# **power efficient-ethernet auto**	特定のインターフェイスで EEE をイネーブルにします。EEE がイネーブルの場合、デバイスはリンク パートナーに EEE をアドバタイズし、自動ネゴシエートします。
ステップ 4	**no power efficient-ethernet auto** 例： スイッチ(config-if)# **no power efficient-ethernet auto**	指定したインターフェイス上で EEE をディセーブルにします。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

EEE のモニタリング

表 *16*：*EEE* 設定を表示するコマンド

コマンド	目的
show eee capabilities interface *interface-id*	指定インターフェイスの EEE 機能を表示します。
show eee status interface *interface-id*	指定したインターフェイスの EEE ステータス情報を表示します。

EEE の設定例

次に、インターフェイスで EEE をイネーブルにする例を示します。

```
スイッチ# configure terminal
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# power efficient-ethernet auto
```

次に、インターフェイスで EEE をディセーブルにする例を示します。

```
スイッチ# configure terminal
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# no power efficient-ethernet auto
```

その他の参考資料

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

EEE 設定の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 III 部

IPv6

- MLD スヌーピングの設定，161 ページ
- IPv6 ユニキャスト ルーティングの設定，179 ページ
- IPv6 マルチキャストの実装，215 ページ
- IPv6 クライアント IP アドレス ラーニングの設定，249 ページ
- IPv6 WLAN セキュリティの設定，277 ページ
- IPv6 ACL の設定，303 ページ
- IPv6 Web 認証の設定 ，323 ページ
- IPv6 クライアント モビリティの設定，337 ページ
- IPv6 モビリティの設定，347 ページ

第 11 章

MLD スヌーピングの設定

このモジュールには、MLD スヌーピングの設定の詳細が含まれています。

- 機能情報の確認，161 ページ
- IPv6 MLD スヌーピングの設定に関する情報，161 ページ
- IPv6 MLD スヌーピングの設定方法，166 ページ
- MLD スヌーピング情報の表示，175 ページ
- MLD スヌーピングの設定例，177 ページ

機能情報の確認

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

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

IPv6 MLD スヌーピングの設定に関する情報

（注） この IPv6 MLD スヌーピングを使用するには、スイッチが LAN Base イメージを実行している必要があります。

スイッチ上で Multicast Listener Discovery（MLD）スヌーピングを使用して、スイッチド ネットワーク内のクライアントおよびルータに IP Version 6（IPv6）マルチキャスト データを効率的に配

信することができます。特に明記しない限り、スイッチという用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。

（注） スタック構成をサポートしているのは、LAN Base イメージを実行している Catalyst 2960-X スイッチだけです。

（注） IPv6 を使用するには、デュアル IPv4 および IPv6 スイッチング データベース管理（SDM）テンプレートがスイッチに設定されている必要があります。
LAN ベース フィーチャ セットが稼働しているスイッチでは、ルーティング テンプレートはサポートされません。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

MLD スヌーピングの概要

IP Version 4（IPv4）では、レイヤ 2 スイッチはインターネット グループ管理プロトコル（IGMP）スヌーピングを使用して、動的にレイヤ 2 インターフェイスを設定することにより、マルチキャスト トラフィックのフラッディングを抑制します。そのため、マルチキャスト トラフィックは IP マルチキャスト デバイスに対応付けられたインターフェイスにだけ転送されます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピングを使用すると、IPv6 マルチキャスト データは VLAN（仮想 LAN）内のすべてのポートにフラッディングされるのではなく、データを受信するポートのリストに選択的に転送されます。このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャスト ルータで使用されるプロトコルで、ルータに直接接続されたリンク上のマルチキャスト リスナー（IPv6 マルチキャスト パケットを受信するノード）の存在、および隣接ノードを対象とするマルチキャスト パケットを検出します。MLD は IGMP から派生しています。MLD バージョン 1（MLDv1）は IGMPv2 と、MLD バージョン 2（MLDv2）は IGMPv3 とそれぞれ同等です。MLD は Internet Control Message Protocol バージョン 6（ICMPv6）のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の 2 つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピング：MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 基本スヌーピング（MBSS）：MLDv2 制御パケットを使用して、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。

（注） スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 拡張スヌーピングをサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できます。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェアおよびハードウェアで構築されます。その後、スイッチはハードウェアで IPv6 マルチキャストアドレスに基づくブリッジングを実行します。

IPv6 マルチキャスト標準に従い、スイッチは自身の MAC アドレスの下位 4 オクテットと MAC アドレス 33:33:00:00:00:00 の論理 OR を実行して、MAC マルチキャストアドレスを抽出します。たとえば、IPv6 の MAC アドレス FF02:DEAD:BEEF:1:3 は、イーサネットの MAC アドレス 33:33:00:01:00:03 にマッピングされます。

IPv6 宛先アドレスと MAC 宛先アドレスが一致しない場合、マルチキャスト パケットは一致しません。スイッチは、一致しないパケットをハードウェア ベースの MAC アドレス テーブルによって転送します。MAC 宛先アドレスが MAC アドレス テーブルにない場合、スイッチは受信したポートと同じ VLAN 内のすべてのポートにパケットをフラッディングします。

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

- Listener クエリー：IGMPv2 クエリーと同等で、General クエリーまたは Mulicast-Address-Specific クエリー（MASQ）のいずれかになります。
- Multicast Listener レポート：IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージ：IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートします。

メッセージの送受信の結果生じるメッセージ タイマーおよびステート移行は、IGMPv2 メッセージの場合と同じです。リンクに対してローカルで有効な IPv6 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done メッセージに応答します。また、スイッチはレポート抑制、レポート プロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト グループ アドレス設定もサポートします。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングされ、クエリーのコピーは CPU に送信され、処理されます。MLD スヌーピングでは、受信されたクエリーから IPv6 マルチキャスト アドレス データベースを構築します。MLD スヌーピングは、マルチキャストルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、VLAN のクエリア IP 送信元アドレス、VLAN 内のクエリア ポートを学習して、マルチキャストアドレス エージングを維持します。

（注） IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、Catalyst 2960、2960-S、2960-C、2960-X、または 2960-CX スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、グループ固有のクエリーに応答します。このグループが不明の場合、グループ固有のクエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ（IGMP Leave メッセージと同等）を送信できます。スイッチが MLDv1 Done メッセージを受信した際に、即時脱退がイネーブルでなければ、スイッチはメッセージを受信したポートに MASQ を送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポート メンバーシップの削除を設定できます。1 つのアドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対するレポートがない場合のみです。デフォルトの回数は 2 回です。

マルチキャスト ルータ検出

IGMP スヌーピングと同様に、MLD スヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。
- 複数のルータが同じレイヤ 2 インターフェイス上にある場合、MLD スヌーピングではポート上の単一のマルチキャスト ルータ（直前にルータ制御パケットを送信したルータ）を追跡します。

- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの 5 分に基づきます。ポート上で制御パケットが 5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合のみです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出された後は、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポートが受信されると、IPv6 マルチキャスト グループ アドレスが VLAN の MLD データベースに入力されます。その後、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナー メッセージ抑制）は自動的にイネーブルになります。レポート抑制により、スイッチはグループで受信された最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポーティングもサポートします。MLDv1 MASQ が受信されると、スイッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバ ポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ（IGMP Leave メッセージと同等）を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。VLAN で即時脱退をイネーブルにする場合は（IGMP スヌーピングと同様に）、ポートに単一のホストが接続されている VLAN でのみこの機能を使用します。ポートがグループの最後のメンバである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に（1 つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバーシップが削除される時期を MASQ 数の観点から制御で

きます。アドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、**ipv6 mld snooping last-listener-query count** グローバル コンフィギュレーション コマンドにより設定されます。デフォルトの回数は 2 回です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。最大応答時間は、**ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドにより設定します。削除されたポートがマルチキャスト アドレスの最後のメンバである場合は、マルチキャスト アドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

即時脱退がイネーブルでない場合に、ポートが MLD Done メッセージを受信すると、スイッチはポートで MASQ を生成して、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信します。ポートがマルチキャスト グループから削除される前に、送信される MASQ 数およびスイッチが応答を待機する時間を任意で設定できます。

MLDv1 即時脱退をイネーブルにした場合、スイッチはポートで MLD Done メッセージを検出するとただちに、マルチキャスト グループからポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバが 1 つだけ存在する場合に限定してください。同一ポートにマルチキャスト グループのクライアントが複数ある場合は、VLAN で即時脱退をイネーブルにしてはなりません。

トポロジ変更通知処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して、トポロジ変更通知（TCN）送信請求をイネーブルにすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリーによりすべての IPv6 マルチキャスト トラフィックをフラッディングするよう VLAN に設定してから、選択されたポートにのみマルチキャスト データの送信を開始します。この値は、**ipv6 mld snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用して設定します。デフォルトでは、2 つのクエリーが送信されます。スイッチが VLAN 内の STP ルートになる場合、またはスイッチがユーザにより設定された場合は、リンクに対してローカルで有効な IPv6 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。これは IGMP スヌーピングの場合と同じです。

IPv6 MLD スヌーピングの設定方法

MLD スヌーピングのデフォルト設定

表 *17* : ***MLD*** スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング（グローバル）	ディセーブル

機能	デフォルト設定
MLD スヌーピング（VLAN 単位）	イネーブルVLANMLDスヌーピングが実行されるためには、MLDスヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャスト アドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	ディセーブル
MLD スヌーピングの堅牢性変数	グローバル：2、VLAN 単位：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー カウント	グローバル：2、VLAN 単位：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー インターバル	グローバル：1000（1 秒）、VLAN：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバルのインターバルを使用します。
TCN クエリー送信請求	ディセーブル
TCN クエリー カウント	2
MLD リスナー抑制	ディセーブル

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。
- IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標

準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにできます。
- スイッチまたはスイッチ スタックに保持可能なマルチキャスト エントリの最大数は、設定された SDM テンプレートによって決まります。
- スイッチまたはスイッチ スタックに保持可能なアドレス エントリの最大数は 4000 です。

スイッチでの MLD スヌーピングのイネーブル化またはディセーブル化（CLI）

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定はグローバル設定を上書きします。つまり、MLD スヌーピングはデフォルト ステート（イネーブル）の VLAN インターフェイスでのみイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

スイッチで MLD スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping** 例： `スイッチ(config)# ipv6 mld snooping`	スイッチで MLD スヌーピングをイネーブルにします。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： スイッチ(config)# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 5	**reload** 例： スイッチ(config)# **reload**	OS（オペレーティング システム）をリロードします。

VLAN での MLD スヌーピングのイネーブル化またはディセーブル化（CLI）

VLAN で MLD スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping** 例： スイッチ(config)# **ipv6 mld snooping**	スイッチで MLD スヌーピングをイネーブルにします。
ステップ 3	**ipv6 mld snooping vlan***vlan-id* 例： スイッチ(config)# **ipv6 mld snooping vlan 1**	VLAN で MLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 （注） VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **ipv6 mld snooping vlan 1**	特権 EXEC モードに戻ります。

スタティック マルチキャスト グループの設定（CLI）

ホストまたはレイヤ 2 ポートは、通常マルチキャスト グループにダイナミックに加入しますが、VLAN に IPv6 マルチキャスト アドレスおよび メンバ ポートをスタティックに設定することもできます。

マルチキャスト グループのメンバとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan***vlan-id***static***ipv6_multicast_address***interface***interface-id* 例： スイッチ(config)# **ipv6 mld snooping vlan 1 static FF12::3 interface gigabitethernet 0/1**	マルチキャスト グループのメンバとしてレイヤ 2 ポートにマルチキャスト グループを設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • *ipv6_multicast_address* は、128 ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式でなければなりません。 • *interface-id* は、メンバ ポートです。物理インターフェイスまたはポート チャネル（1 ～ 48）に設定できます。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	次のいずれかを使用します。 • **show ipv6 mld snooping address** • **show ipv6 mld snooping address vlan***vlan-id* 例： スイッチ# **show ipv6 mld snooping address** または スイッチ# **show ipv6 mld snooping vlan 1**	スタティック メンバ ポートおよび IPv6 アドレスを確認します。

マルチキャスト ルータ ポートの設定（CLI）

（注） マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

VLAN にマルチキャスト ルータ ポートを追加するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan***vlan-id***mrouter interface***interface-id* 例： スイッチ(config)# **ipv6 mld snooping vlan 1 mrouter interface gigabitethernet**	マルチキャスト ルータの VLAN ID を指定して、マルチキャスト ルータにインターフェイスを指定します。 • 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

	コマンドまたはアクション	目的
	0/2	• このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping mrouter** [**vlan***vlan-id*] 例： スイッチ# **show ipv6 mld snooping mrouter vlan 1**	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。

MLD 即時脱退の有効化（CLI）

MLDv1 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan***vlan-id***immediate-leave** 例： スイッチ(config)# **ipv6 mld snooping vlan 1 immediate-leave**	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**show ipv6 mld snooping vlan***vlan-id* 例： スイッチ# **show ipv6 mld snooping vlan 1**	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。

MLD スヌーピング クエリーの設定（CLI）

スイッチまたは VLAN に MLD スヌーピング クエリーの特性を設定するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping robustness-variable***value* 例： スイッチ(config)# **ipv6 mld snooping robustness-variable 3**	（任意）スイッチが一般クエリーに応答しないリスナー（ポート）を削除する前に、送信されるクエリー数を設定します。指定できる範囲は 1 ～ 3 です。デフォルトは 2 です。
ステップ 3	**ipv6 mld snooping vlan***vlan-id***robustness-variable***value* 例： スイッチ(config)# **ipv6 mld snooping vlan 1 robustness-variable 3**	（任意）VLAN 単位でロバストネス変数を設定します。これにより、MLD レポート応答がない場合にマルチキャスト アドレスがエージング アウトされるまでに、MLD スヌーピングが送信する一般クエリー数が決定されます。指定できる範囲は 1 ～ 3 です。デフォルトは 0 です。0 に設定すると、使用される数はグローバルな堅牢性変数の値になります。
ステップ 4	**ipv6 mld snooping last-listener-query-count***count* 例： スイッチ(config)# **ipv6 mld snooping last-listener-query-count 7**	（任意）MLD クライアントがエージング アウトされる前にスイッチが送信する MASQ 数を設定します。指定できる範囲は 1 ～ 7 です。デフォルトは 2 です。クエリーは 1 秒後に送信されます。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 mld snooping vlan***vlan-id***last-listener-query-count***count** 例： スイッチ(config)# **ipv6 mld snooping vlan 1 last-listener-query-count 7**	（任意）VLAN 単位で last-listener クエリー カウントを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は 1 ～ 7 です。デフォルトは 0 です。0 に設定すると、グローバルなカウント値が使用されます。クエリーは 1秒後に送信されます。
ステップ 6	**ipv6 mld snooping last-listener-query-interval***interval* 例： スイッチ(config)# **ipv6 mld snooping last-listener-query-interval 2000**	（任意）スイッチが MASQ を送信したあと、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。指定できる範囲は、100 ～ 32,768 ミリ秒です。デフォルト値は 1000（1 秒）です。
ステップ 7	**ipv6 mld snooping vlan***vlan-id***last-listener-query-interval***interval* 例： スイッチ(config)# **ipv6 mld snooping vlan 1 last-listener-query-interval 2000**	（任意）VLAN 単位で last-listener クエリー インターバルを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0～32,768 ミリ秒です。デフォルトは 0 です。0 に設定すると、グローバルな最後のリスナー クエリー インターバルが使用されます。
ステップ 8	**ipv6 mld snooping tcn query solicit** 例： スイッチ(config)# **ipv6 mld snooping tcn query solicit**	（任意）トポロジ変更通知（TCN）をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラフィックすべてをフラッディングしてから、マルチキャスト データをマルチキャスト データの受信を要求するポートに対してのみ送信します。デフォルトでは、TCN はディセーブルに設定されています。
ステップ 9	**ipv6 mld snooping tcn flood query count***count* 例： スイッチ(config)# **ipv6 mld snooping tcn flood query count 5**	（任意）TCN がイネーブルの場合、送信される TCN クエリー数を指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ipv6 mld snooping querier** [**vlan***vlan-id*] 例： スイッチ(config)# **show ipv6 mld snooping querier vlan 1**	（任意）スイッチまたは VLAN の MLD スヌーピング クエリア情報を確認します。

MLD リスナー メッセージ抑制の無効化（CLI）

デフォルトでは、MLDスヌーピング リスナー メッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、スイッチはマルチキャスト ルータ クエリーごとに 1 つの MLD レポートのみを転送します。メッセージ抑制がディセーブルの場合は、複数のマルチキャスト ルータに MLD レポートが転送されます。

MLD リスナー メッセージ抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ipv6 mld snooping listener-message-suppression** 例： `スイッチ(config)# no ipv6 mld snooping listener-message-suppression`	MLDメッセージ抑制をディセーブルにします。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping** 例： `スイッチ# show ipv6 mld snooping`	IPv6 MLD スヌーピング レポート抑制がディセーブルであることを確認します。

MLD スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよびVLANインターフェイスの MLD スヌーピング情報を表示できます。また、MLD スヌーピング用に設定された VLAN の IPv6 グループ アドレス マルチキャスト エントリを表示することもできます。

表 *18* : ***MLD*** スヌーピング情報表示用のコマンド

コマンド	目的
show ipv6 mld snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan***vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping mrouter [**vlan***vlan-id*]	ダイナミックに学習され、手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。 （任意）個々の VLAN に関する情報を表示するには、**vlan***vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping querier [**vlan***vlan-id*]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。 （任意）**vlan***vlan-id* を入力して、単一の VLAN 情報を表示します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping address [**vlan***vlan-id*] [**count** | **dynamic** | **user**]	すべての IPv6 マルチキャスト アドレス情報あるいはスイッチまたは VLAN の特定の IPv6 マルチキャスト アドレス情報を表示します。 • **count** を入力して、スイッチまたは VLAN のグループ数を表示します。 • **dynamic** を入力して、スイッチまたは VLAN の MLD スヌーピング学習済みグループ情報を表示します。 • **user** を入力して、スイッチまたは VLAN の MLD スヌーピング ユーザ設定グループ情報を表示します。

コマンド	目的
show ipv6 mld snooping address vlan*vlan-id* [*ipv6-multicast-address*]	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。

MLD スヌーピングの設定例

スタティックなマルチキャスト グループの設定：例

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet
          1/0/1
スイッチ(config)# end
```

マルチキャスト ルータ ポートの設定：例

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet
          0/2
スイッチ(config)# exit
```

MLD 即時脱退のイネーブル化：例

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ipv6 mld snooping vlan 130 immediate-leave
スイッチ(config)# exit
```

MLD スヌーピング クエリーの設定：例

次に、MLD スヌーピングのグローバルな堅牢性変数を 3 に設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ipv6 mld snooping robustness-variable 3
スイッチ(config)# exit
```

次に、VLAN の MLD スヌーピングの最後のリスナー クエリー カウントを 3 に設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
スイッチ(config)# exit
```

次に、MLD スヌーピングの最後のリスナー クエリー インターバル（最大応答時間）を 2000（2 秒）に設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ipv6 mld snooping last-listener-query-interval 2000
スイッチ(config)# exit
```

第 12 章

IPv6 ユニキャスト ルーティングの設定

- 機能情報の確認，179 ページ
- IPv6 ユニキャスト ルーティングの設定について，179 ページ
- DHCP for IPv6 アドレス割り当ての設定，207 ページ
- IPv6 ユニキャスト ルーティングの設定例，212 ページ

機能情報の確認

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

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

IPv6 ユニキャスト ルーティングの設定について

この章では、スイッチに IPv6 ユニキャスト ルーティングを設定する方法について説明します。

（注） この章のすべての IPv6 機能を使用するには、スイッチまたはスタック マスターが IP サービス フィーチャ セットを実行している必要があります。IP ベースのフィーチャ セットを実行しているスイッチは、IPv6 スタティック ルーティング、IPv6 の RIP、および OSPF をサポートします。LAN ベースのフィーチャ セットが稼働しているスイッチは、IPv6 ホスト機能だけをサポートします。

IPv6 の概要

IPv4 ユーザは IPv6 に移行することができ、エンドツーエンドのセキュリティ、Quality of Service（QoS）、およびグローバルに一意なアドレスのようなサービスを利用できます。IPv6 アドレス スペースによって、プライベートアドレスの必要性が低下し、ネットワーク エッジの境界ルータで Network Address Translation（NAT; ネットワーク アドレス変換）処理を行う必要性も低下します。

シスコの IPv6 の実装方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 およびこの章のその他の機能については、

- 『*Cisco IOS IPv6 Configuration Library*』を参照してください。
- Cisco.com の [Search] フィールドを使用して、Cisco IOS ソフトウェア マニュアルを特定します。たとえば、スタティック ルートについての情報が必要な場合は、[Search] フィールドで *Implementing Static Routes for IPv6* と入力すると、スタティック ルートについて調べられます。

IPv6 Addresses

スイッチがサポートするのは、IPv6 ユニキャスト アドレスのみです。サイトローカルなユニキャスト アドレスおよびマルチキャスト アドレスはサポートされません。

IPv6 の 128 ビット アドレスは、コロンで区切られた一連の 8 つの 16 進フィールド（n:n:n:n:n:n:n:n の形式）で表されます。次に、IPv6 アドレスの例を示します。

2031:0000:130F:0000:0000:09C0:080F:130B

実装を容易にするために、各フィールドの先行ゼロは省略可能です。上記アドレスは、先行ゼロを省略した次のアドレスと同じです。

2031:0:130F:0:0:9C0:80F:130B

2 つのコロン（::）を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この短縮形を使用できるのは、各アドレス内で 1 回のみです。

2031:0:130F::09C0:080F:130B

IPv6 アドレス形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Information About Implementing Basic Connectivity for IPv6」の章では、次の項の内容がスイッチに適用されます。

- IPv6 アドレス形式
- IPv6 アドレス タイプ：ユニキャスト
- IPv6 アドレス タイプ：マルチキャスト
- Ipv6 アドレス 出力表示

- 簡易 IPv6 パケット ヘッダー

サポート対象の IPv6 ユニキャスト ルーティング機能

ここでは、スイッチでサポートされている IPv6 プロトコル機能について説明します。

スイッチは、IPv6 の Routing Information Protocol（RIP）、および Open Shortest Path First（OSPF）バージョン 3 プロトコルによる IPv6 ルーティング機能を提供します。等コスト ルートは 16 個までサポートされ、IPv4 および IPv6 フレームを回線レートで同時に転送できます。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクに対してローカルなユニキャストアドレスをサポートします。サイトに対してローカルなユニキャストアドレスはサポートされていません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能グローバル ユニキャスト プレフィックスの付いた IPv6 アドレスです。このアドレス構造を使用すると、ルーティング プレフィックスを厳格に集約することができ、グローバルルーティングテーブル内のルーティング テーブル エントリ数が制限されます。これらのアドレスは、組織を経由して最終的にインターネット サービス プロバイダーに至る集約リンク上で使用されます。

  これらのアドレスはグローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID によって定義されます。現在のグローバル ユニキャスト アドレス割り当てには、バイナリ値 001（2000::/3）で開始するアドレス範囲が使用されます。プレフィックスが 2000::/3（001）～ E000::/3（111）のアドレスには、Extended Unique Identifier（EUI）64 フォーマットの 64 ビット インターフェイス ID を設定する必要があります。

- リンクに対してローカルなユニキャストアドレスをすべてのインターフェイスに自動的に設定するには、修飾EUIフォーマット内で、リンクに対してローカルなプレフィックスFE80::/10（1111 1110 10）およびインターフェイスIDを使用します。ネイバー探索プロトコル（NDP）およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。ローカル リンク上のノードは、リンクに対してローカルなアドレスを使用します。通信する場合に、グローバルに一意なアドレスは不要です。IPv6 ルータは、リンクに対してローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章にある IPv6 ユニキャスト アドレスに関する項を参照してください。

IPv6 の *DNS*

IPv6 は、ドメイン ネーム システム（DNS）のレコード タイプを、DNS 名前/アドレスおよびアドレス/名前の検索プロセスでサポートします。DNS AAAA リソース レコード タイプは IPv6 アドレスをサポートし、IPv4 の A アドレス レコードと同等です。スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス *MTU* ディスカバリ

スイッチはシステム最大伝送単位（MTU）の IPv6 ノードへのアドバタイズおよびパス MTU ディスカバリをサポートします。パス MTU ディスカバリを使用すると、ホストは指定されたデータ

パスを通るすべてのリンクのMTUサイズを動的に検出して、サイズに合せて調整できます。IPv6では、パスを通るリンクの MTU サイズが小さくてパケット サイズに対応できない場合、パケットの送信元がフラグメンテーションを処理します。

ICMPv6

IPv6のインターネット制御メッセージプロトコル（ICMP）は、ICMP宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。IPv6 では、ネイバー探索プロトコルおよびパス MTU ディスカバリに ICMP パケットも使用されます。

ネイバー探索

スイッチは、IPv6 対応の NDP、ICMPv6 の最上部で稼働するプロトコル、および NDP をサポートしない IPv6 ステーション対応のスタティック ネイバー エントリをサポートします。IPv6 ネイバー探索プロセスは ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 未満のルートに対して ICMPv6 リダイレクトをサポートしています。マスク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトがサポートされません。

ネイバー探索スロットリングにより、IPv6 パケットをルーティングするためにネクストホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。IPv6 パケットのネクスト ホップがスイッチによってアクティブに解決しようとしている同じネイバーである場合は、そのようなパケットが追加されると、スイッチはそのパケットをドロップします。このドロップにより、CPU に余分な負荷がかからないようになります。

DRP

スイッチは、ルータのアドバタイズメント メッセージの拡張機能である、IPv6 Default Router Prefernce（DRP）をサポートします。DRP では、特にホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合に、ホストが適切なルータを選択する機能が向上しました。スイッチは、Route Information Option（RFC 4191）をサポートしません。

IPv6 ホストは、オフリンク宛先へのトラフィック用にルータを選択する、デフォルト ルータ リストを維持します。次に、宛先用に選択されたルータは、宛先キャッシュに格納されます。IPv6 NDP では、到達可能であるルータまたは到達可能性の高いルータが、到達可能性が不明または低いルータよりも優先されます。NDP は、到達可能または到達可能の可能性があるルータとして、常に同じルータを選択するか、またはルータ リストから繰り返し使用できます。DRP を使用することにより、IPv6 ホストが、両方ともが到達可能または到達可能の可能性がある 2 台のルータを差別化するように設定できます。

DRP for IPv6 の詳細情報については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチではステートレス自動設定が使用されているため、ホストやモバイル IP アドレスの管理のような、リンク、サブネット、およびサイト アドレス指定の変更を管理することができます。ホストはリンクに対してローカルな独自アドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をアドバタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- Ping、traceroute、Telnet、および TFTP
- IPv6 トランスポートによるセキュア シェル（SSH）
- IPv6 トランスポートによる HTTP サーバ アクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ
- IPv6 アドレスの Cisco Discovery Protocol（CDP）サポート

これらのアプリケーションの管理に関する詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

DHCP for IPv6 アドレスの割り当て

DHCPv6 を使用すると、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。このアドレス割り当て機能により、ホストが接続するネットワークに基づいて、適切なプレフィックス内での重複しないアドレス割り当てが管理されます。アドレスは、1 つまたは複数のプレフィックス プールから割り当てることができます。デフォルトのドメインおよび DNS ネーム サーバ アドレスなど、その他のオプションは、クライアントに戻すことができます。アドレス プールは、特定のインターフェイス、複数のインターフェイス上で使用する場合に割り当てられます。または、サーバが自動的に適切なプールを検出できます。

これらの機能の詳細および設定方法については、『*Cisco IOS IPv6 Configuration Guide*』を参照してください。

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 クライアント、サーバ、またはリレーエージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーキング デバイス間のルートを明示的に定義します。スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

RIP for IPv6

IPv6 の Routing Information Protocol（RIP）は、ルーティング メトリックとしてホップ カウントを使用するディスタンスベクトル プロトコルです。IPv6 アドレスおよびプレフィックスのサポート、すべての RIP ルータを含むマルチキャスト グループ アドレス FF02::9 を RIP アップデート メッセージの宛先アドレスとして使用する機能などがあります。

IPv6 の RIP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

OSPF for IPv6

IP Base フィーチャ セットを実行しているスイッチは、IPv6 の Open Shortest Path First（OSPF）（IP のリンクステート プロトコル）をサポートします。詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 の *HSRP* の設定

HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。IPv6 ホストは、IPv6 ネイバー探索ルータのアドバタイズメント メッセージによって使用可能なルータを学習します。これらのメッセージは定期的にマルチキャストされるか、ホストにより送信請求されます。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカル アドレスがあります。HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

（注） IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2（HSRPv2）をイネーブルにする必要があります。

EIGRP IPv6

スイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol（EIGRP）をサポートしています。IPv6 の EIGRP は稼働するインターフェイス上で設定されるため、グローバルな IPv6 アドレスは不要です。IP Lite を実行しているスイッチは EIGRPv6 スタブ ルーティングをサポートします。

EIGRP IPv6 インスタンスでは、実行する前に暗示的または明示的なルータ ID が必要です。暗示的なルータ ID はローカルの IPv6 アドレスを基にして作成されるため、すべての IPv6 ノードには常に使用可能なルータ ID があります。ただし、EIGRP IPv6 は IPv6 ノードのみが含まれるネットワークで稼働するため、使用可能な IPv6 ルータ ID がない場合があります。

EIGRP for IPv6 の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

EIGRPv6 スタブ ルーティング

EIGRPv6 スタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を低減させます。

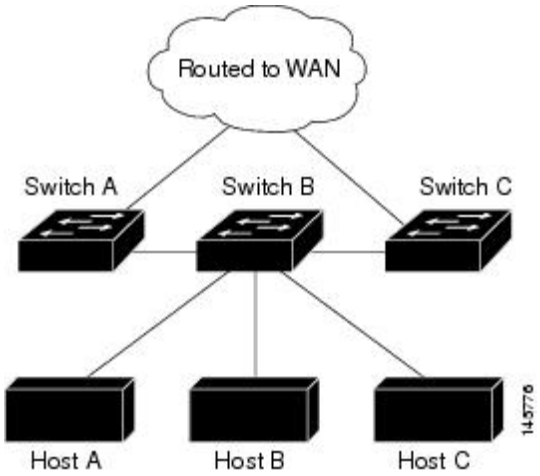
EIGRPv6 スタブ ルーティングを使用するネットワークでは、ユーザに対する IPv6 トラフィックの唯一の許容ルートは、EIGRPv6 スタブ ルーティングを設定しているスイッチ経由です。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRPv6 スタブ ルーティングを使用しているときは、EIGRPv6 を使用してスイッチだけをスタブとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。指定したルートだけがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。スタブルータは、ディストリビューション ルータを使用して適切なアップデートをすべてのピアに送信します。

次の図では、スイッチ B は EIGRPv6 スタブ ルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配信ルート、およびサマリー ルートをスイッチ A と C にアドバタイズします。 スイッチ B は、スイッチ A から学習したルートをアドバタイズしません（逆の場合も同様です）。

図 *6*：*EIGRP* スタブ ルータ設定



EIGRPv6 スタブ ルーティングの詳細については、『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols, Release 12.4*』の「Implementing EIGRP for IPv6」を参照してください。

IPv6 による*SNMP* と *Syslog*

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。IPv6 による Syslog は、このトランスポートのアドレス データ タイプをサポートします。

IPv6 による SNMP および Syslog は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および Syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

IPv6 に関連するサポートでは、SNMP は既存の IP トランスポート マッピングを変更して、IPv4 と IPv6 を同時にサポートします。次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザ データグラム プロトコル（UDP）SNMP ソケットを開く

- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む、IPv6 による SNMP については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、IPv6 による Syslog については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 上の *HTTP*（*S*）

HTTP クライアントは要求を IPv4 HTTP サーバと IPv6 HTTP サーバの両方に送信し、これらのサーバは IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレスを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケット コールは、IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを選択します。受信ソケットは、IPv4 ソケットまたは IPv6 ソケットのいずれかです。リスニング ソケットは、接続を示す IPvv4 と IPv6 の両方の信号を待ち受け続けます。IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされています。

基本 TCP/IP スタックは、デュアル スタック環境をサポートします。HTTP には、TCP/IP スタック、およびネットワーク層相互作用を処理するためのソケットが必要です。

HTTP 接続を確立するには、基本ネットワーク接続（**ping**）がクライアントとサーバ ホストとの間に存在する必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

サポートされていない IPv6 ユニキャスト ルーティング機能

スイッチは、次の IPv6 機能をサポートしません。

- IPv6 ポリシーベース ルーティング
- IPv6 バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）テーブルのサポート
- サイトローカルなアドレス宛ての IPv6 パケット
- IPv4/IPv6 や IPv6/IPv4 などのトンネリング プロトコル
- IPv4/IPv6 または IPv6/IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ
- IPv6 ユニキャスト Reverse-Path Forwarding
- IPv6 Web Cache Communication Protocol（WCCP）

IPv6 機能の制限

スイッチでは IPv6 はハードウェアに実装されるため、ハードウェア メモリ内の IPv6 圧縮アドレスによる制限がいくつか発生します。これらのハードウェア制限により、機能の一部が失われて、制限されます。

機能の制限は次のとおりです。

- スイッチはハードウェアで SNAP カプセル化 IPv6 パケットを転送できません。これらはソフトウェアで転送されます。
- スイッチはソースルート IPv6 パケットに関する QoS 分類をハードウェアで適用できません。

IPv6 とスイッチ スタック

スイッチにより、スタック全体で IPv6 転送がサポートされ、スタック マスターで IPv6 ホスト機能がサポートされます。スタック マスターは IPv6 ユニキャスト ルーティング プロトコルを実行してルーティング テーブルを計算します。スタック メンバー スイッチはテーブルを受信して、転送用にハードウェア IPv6 ルートを作成します。スタック マスターも、すべての IPv6 アプリケーションを実行します。

（注） スタック内で IPv6 パケットをルーティングするには、スタック内のすべてのスイッチで IP Base フィーチャ セットが稼動している必要があります。

新しいスイッチがスタック マスターになる場合、新しいマスターは IPv6 ルーティング テーブルを再計算してこれをメンバー スイッチに配布します。新しいスタック マスターが選択中およびリセット中の間には、スイッチ スタックによる IPv6 パケットの転送は行われません。スタック MAC アドレスが変更され、これによって IPv6 アドレスが変更されます。**ipv6 address***ipv6-prefix/prefixlength***eui-64** インターフェイス コンフィギュレーション コマンドを使用して、拡張固有識別子（EUI）でスタック IPv6 アドレスを指定する場合、アドレスは、インターフェイス MAC アドレスに基づきます。IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化（CLI），（188 ページ）を参照してください。

スタック上で永続的な MAC アドレスを設定し、スタック マスターが変更された場合、スタック MAC アドレスは、約 4 分間、変更されません。

IPv6 スタック マスターおよびメンバーの機能は次のとおりです。

- スタック マスター
  - IPv6 ルーティングプロトコルの実行
  - ルーティング テーブルの生成
  - dCEFv6 を使用するスタック メンバーへのルーティング テーブルの配布
  - IPv6 ホスト機能および IPv6 アプリケーションの実行
- スタック メンバー（IP サービス フィーチャ セットを実行している必要があります）

- スタック マスターからの CEFv6 ルーティング テーブルの受信
- ハードウェアへのルートのプログラミング

（注） IPv6 パケットに例外（IPv6 オプション）がなく、スタック内のスイッチでハードウェア リソースが不足していない場合、IPv6 パケットがスタック全体にわたってハードウェアでルーティングされます。

- マスターの再選択での CEFv6 テーブルのフラッシュ

IPv6 のデフォルト設定

表 *19* : *IPv6* のデフォルト設定

機能	デフォルト設定
SDM テンプレート	アドバンス デスクトップ。デフォルトは拡張テンプレートです
IPv6 ルーティング	すべてのインターフェイスでグローバルにディセーブル
CEFv6 または dCEFv6	ディセーブル（IPv4 CEF および dCEF はデフォルトでイネーブル） （注） IPv6 ルーティングがイネーブルの場合、CEFv6 および dCEF6 は自動的にイネーブル
IPv6 アドレス	未設定

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化（CLI）

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチ上でグローバル転送する方法を説明します。

スイッチ上の IPv6 を設定する前に、次の注意事項に従ってください。

- スイッチでは、この章で説明されたすべての機能がサポートされるわけではありません。サポートされていない IPv6 ユニキャスト ルーティング機能, （186 ページ）を参照してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、16 ビット値を使用したコロン区切りの 16 進形式で指定したアドレスで *ipv6-address* 変数および *ipv6-prefix* 変数を

入力する必要があります。*prefix-length* 変数（スラッシュ（/）で始まる）は、プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバル IPv6 アドレスを設定する必要があります。インターフェイス上で IPv6 アドレスを設定すると、リンクに対してローカルなアドレスの設定、およびそのインターフェイスに対する IPv6 のアクティブ化が自動的に行われます。設定されたインターフェイスは、次に示す、該当リンクの必須マルチキャスト グループに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャスト アドレスの送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:ff00::/104（このアドレスはネイバー探索プロセスで使用される）
- すべてのノードを含む、ルータリンクに対してローカルなマルチキャスト グループ FF02::1
- すべてのルータを含む、リンクに対してローカルなマルチキャスト グループ FF02::2

インターフェイスから IPv6 アドレスを削除するには、**noipv6 address***ipv6-prefix/prefixlength***eui-64** または **no ipv6 address***ipv6-address***link-local** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスで明示的に設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ルーティングをグローバルにディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。

IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

レイヤ 3 インターフェイスに IPv6 アドレスを割り当てて、IPv6 ルーティングをイネーブルにするは、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** **例**： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm preferdual-ipv4-and-ipv6** {**advanced** | **vlan**} **例**： スイッチ(config)# **sdm prefer dual-ipv4-and-ipv6 default**	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 • **advanced**：スイッチをデフォルト テンプレートに設定して、システム リソースを均衡化します。 • **vlan**：ハードウェアでのルーティングをサポートしないスイッチでの VLAN 設定を最大化します。

	コマンドまたはアクション	目的
		（注） advanced はすべてのライセンス レベルで使用できます。VLAN テンプレートは LAN Base ライセンスでのみ使用できます。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	**reload** 例： スイッチ# **reload**	オペレーティング システムをリロードします。
ステップ 5	**configureterminal** 例： スイッチ# **configure terminal**	スイッチのリロード後、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。インターフェイスは物理インターフェイス、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できます。
ステップ 7	**noswitchport** 例： スイッチ(config-if)# **no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 8	次のいずれかを使用します。 • **ipv6 address***ipv6-prefix/prefix length***eui-64** • **ipv6 address***ipv6-address/prefix length* • **ipv6 address***ipv6-address***link-local** • **ipv6 enable** • **ipv6 address***WORD* • **ipv6 address***autoconfig* • **ipv6 address***dhcp*	• IPv6 アドレスの下位 64 ビットの拡張固有識別子（EUI）を使用して、グローバル IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイス上で IPv6 処理がイネーブルになります。 • インターフェイスの IPv6 アドレスを手動で設定します。 • インターフェイスで IPv6 がイネーブルな場合に自動設定されるリンクローカルなアドレスでなく、インターフェイス上の特定のリンクローカルなアドレスを使用

	コマンドまたはアクション	目的
	例： スイッチ(config-if)# **ipv6 address 2001:0DB8:c18:1::/64 eui 64** スイッチ(config-if)# **ipv6 address 2001:0DB8:c18:1::/64** スイッチ(config-if)# **ipv6 address 2001:0DB8:c18:1:: link-local** スイッチ(config-if)# **ipv6 enable**	するように指定します。このコマンドにより、インターフェイス上で IPv6 処理がイネーブルになります。 • インターフェイスに IPv6 リンクローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。
ステップ 9	**exit** 例： スイッチ(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**ip routing** 例： スイッチ(config)# **ip routing**	スイッチ上で IP ルーティングをイネーブルにします。
ステップ 11	**ipv6unicast-routing** 例： スイッチ(config)# **ipv6 unicast-routing**	IPv6 ユニキャスト データ パケットの転送をイネーブルにします。
ステップ 12	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 13	**show ipv6 interface***interface-id* 例： スイッチ# **show ipv6 interface gigabitethernet 1/0/1**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 14	**copyrunning-configstartup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv4 および IPv6 プロトコル スタックの設定（CLI）

IPv4 および IPv6 を両方サポートし、IPv6 ルーティングがイネーブルになるようにレイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

（注） IPv6 アドレスが設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。

手順の概要

1. **configureterminal**
2. **ip routing**
3. **ipv6 unicast-routing**
4. **interface***interface-id*
5. **no switchport**
6. **ip address***ip-address mask* [**secondary**]
7. 次のいずれかを使用します。
   - **ipv6 address***ipv6-prefix/prefix length***eui-64**
   - **ipv6 address***ipv6-address/prefix length*
   - **ipv6 address***ipv6-address***link-local**
   - **ipv6 enable**
   - **ipv6 address***WORD*
   - **ipv6 address***autoconfig*
   - **ipv6 address***dhcp*
8. **end**
9. 次のいずれかを使用します。
   - **show interface***interface-id*
   - **show ip interface***interface-id*
   - **show ipv6 interface***interface-id*
10. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： `Switch(config)# ip routing`	スイッチ上でルーティングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 unicast-routing** 例： `Switch(config)# ipv6 unicast-routing`	スイッチ上で IPv6 データ パケットの転送をイネーブルにします。
ステップ 4	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 5	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ2コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 6	**ip address***ip-address mask* [**secondary**] 例： `Switch(config-if)# ip address 10.1.2.3 255.255.255`	インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを指定します。
ステップ 7	次のいずれかを使用します。 • **ipv6 address***ipv6-prefix/prefix length***eui-64** • **ipv6 address***ipv6-address/prefix length* • **ipv6 address***ipv6-address***link-local** • **ipv6 enable** • **ipv6 address***WORD* • **ipv6 address***autoconfig* • **ipv6 address***dhcp*	• グローバル IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。 • インターフェイスで IPv6 がイネーブルな場合に自動設定されるリンクローカルなアドレスでなく、インターフェイス上のリンクローカルなアドレスを使用するように指定します。 • インターフェイスに IPv6 リンクローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。 （注） インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。 • **show interface***interface-id* • **show ip interface***interface-id* • **show ipv6 interface***interface-id*	入力を確認します。
ステップ 10	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

デフォルト ルータ プリファレンスの設定（CLI）

ルータ アドバタイズメント（RA）メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドによって設定される DRP とともに送信されます。DRP が設定されていない場合は、RA は中小規模のプリファレンスとともに送信されます。

リンク上の 2 つのルータが等価ではあっても、等コストではないルーティングを提供する可能性がある場合、およびポリシーでホストがいずれかのルータを選択するよう指示された場合は、DRP が有効です。

IPv6 の DRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

インターフェイス上のルータに DRP を設定するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始して、DRP を指定するレイヤ 3 インターフェイスを特定します。
ステップ 3	**ipv6 nd router-preference** {**high** | **medium** | **low**} 例： スイッチ(config-if)# **ipv6 nd router-preference medium**	スイッチ インターフェイス上のルータに DRP を指定します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**showipv6interface** 例： スイッチ# **show ipv6 interface**	設定を確認します。
ステップ 6	**copyrunning-configstartup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 ICMP レート制限の設定（CLI）

ICMP レート制限はデフォルトでイネーブルです。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルト バケット サイズ（バケットに格納される最大トークン数）は 10 です。

ICMP レート制限パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 icmp error-interval***interval* [*bucketsize*] 例： スイッチ(config)# **ipv6 icmp error-interval 50 20**	IPv6 ICMP エラー メッセージの間隔とバケット サイズを設定します。 • *interval*：バケットに追加されるトークンの間隔（ミリ秒）。指定できる範囲は 0 ～ 2147483647 ミリ秒です。 • *bucketsize*：（任意）バケットに格納される最大トークン数。指定できる範囲は 1 ～ 200 です。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 interface** [*interface-id*] 例： スイッチ# **show ipv6 interface gigabitethernet 1/0/1**	入力を確認します。
ステップ 5	**copyrunning-configstartup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 の CEF および dCEF の設定

シスコエクスプレスフォワーディング（CEF）は、ネットワーク パフォーマンスを最適化するためのレイヤ 3 IP スイッチング テクノロジーです。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ3スイッチングのパフォーマンスを最大化できます。高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能

力をパケット転送に振り分けることができます。スイッチ スタックでは、ハードウェアによって distributed CEF（dCEF）が使用されます。IPv4 CEF および dCEF はデフォルトでイネーブルです。IPv6 CEF および dCEF はデフォルトでディセーブルですが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ルーティングが設定されていない場合は、IPv6 CEF および dCEF は自動的にディセーブルになります。IPv6 CEF および dCEF は、設定中にディセーブルにできません。IPv6 ステータスを確認するには、**show ipv6 cef** 特権 EXEC コマンドを入力します。

IPv6 ユニキャスト パケットをルーティングするには、最初に **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して、IPv6 ユニキャスト パケットの転送をグローバルに設定してから、**ipv6 address** インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイスに IPv6 アドレスおよび IPv6 処理を設定する必要があります。

CEF および dCEF の設定に関する詳細情報については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のスタティック ルーティングの設定（CLI）

スタティック IPv6 ルートを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、インターフェイスに IPv6 アドレスを設定して少なくとも 1 つのレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

スタティック IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 route***ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*] 例： `スイッチ(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130`	スタティック IPv6 ルートを設定します。 • *ipv6-prefix*：スタティック ルートの宛先となる IPv6 ネットワーク。スタティック ホスト ルートを設定する場合は、ホスト名も設定できます。 • */prefixlength*：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。 • *ipv6-address*：指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。ネクスト ホップの IPv6 アドレスを

	コマンドまたはアクション	目的
		直接接続する必要はありません。再帰処理が実行されて、直接接続されたネクスト ホップの IPv6 アドレスが検出されます。このアドレスは RFC 2373 に記載された形式（16 ビット値を使用したコロン区切りの 16 進表記で指定）で設定する必要があります。 • *interface-id*：Point-To-Point（ポイントツーポイント）インターフェイスおよびブロードキャスト インターフェイスからのダイレクト スタティック ルートを指定します。ポイントツーポイント インターフェイスの場合、ネクスト ホップの IPv6 アドレスを指定する必要はありません。ブロードキャスト インターフェイスの場合は、常にネクスト ホップの IPv6 アドレスを指定するか、または指定したプレフィックスをリンクに割り当てて、リンクに対してローカルなアドレスをネクスト ホップとして指定する必要があります。パケットの送信先となるネクスト ホップの IPv6 アドレスを指定することもできます。 （注） リンクに対してローカルなアドレスをネクスト ホップとして使用する場合は、*interface-id* を指定する必要があります（リンクに対してローカルなネクスト ホップを隣接ルータに設定する必要もあります）。 • *administrative distance*：（任意）アドミニストレーティブ ディスタンス。指定できる範囲は 1 ～ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルート タイプよりも、スタティック ルートが優先します。フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスを使用します。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	次のいずれかを使用します。 • **show ipv6 static**[*ipv6-address* | *ipv6-prefix/prefix length*] [**interface***interface-id*] [**detail**]][**recursive**] [**detail**] • **show ipv6 route static**[*updated*]	IPv6 ルーティング テーブルの内容を表示して、設定を確認します。 • **interface***interface-id*：（任意）出力インターフェイスとして指定されたインターフェイスを含むスタティック ルートのみを表示します。 • **recursive**：（任意）再帰スタティック ルートのみを表示します。**recursive** キーワードは **interface** キーワードと相互に排他的です。ただし、コマンド構文に IPv6 プレフィックスが指定されているかどうかに関係なく、使用することができます。

	コマンドまたはアクション	目的
	例： スイッチ# **show ipv6 static 2001:0DB8::/32 interface gigabitethernet2/0/1** または スイッチ# **show ipv6 route static**	• **detail**：（任意）次に示す追加情報を表示します。 ◦有効な再帰ルートの場合、出力パス セットおよび最大分解深度 ◦無効なルートの場合、ルートが無効な理由
ステップ 5	**copyrunning-configstartup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RIP for IPv6 の設定（CLI）

IPv6 RIP を実行するようにスイッチを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにして、IPv6 RIP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

IPv6 の RIP ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router rip***name* 例： スイッチ(config)# **ipv6 router rip cisco**	IPv6 RIP ルーティング プロセスを設定し、このプロセスに対してルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**maximum-paths***number-paths* 例： スイッチ(config-router)# **maximum-paths 6**	（任意）IPv6 RIP がサポートできる等コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 32 で、デフォルトは 16 ルートです。
ステップ 4	**exit** 例： スイッチ(config-router)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 6	**ipv6 rip***name***enable** 例： スイッチ(config-if)# **ipv6 rip cisco enable**	指定された IPv6 RIP ルーティング プロセスをインターフェイス上でイネーブルにします。
ステップ 7	**ipv6 rip***name***default-information** {**only** | **originate**} 例： スイッチ(config-if)# **ipv6 rip cisco default-information only**	（任意）IPv6 デフォルト ルート（::/0）を RIP ルーティング プロセス アップデートに格納して、指定インターフェイスから送信します。 （注） 任意のインターフェイスから IPv6 デフォルト ルート（::/0）を送信したあとに、ルーティング ループが発生しないようにするために、ルーティング プロセスは任意のインターフェイスで受信したすべてのデフォルト ルートを無視します。 • **only**：デフォルト ルートを送信し、現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを抑制するように選択します。 • **originate**：デフォルト ルート、および現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを送信するように選択します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。 • **show ipv6 rip**[*name*] [**interface***interface-id*] [**database**] [**next-hops**] • **show ipv6 rip** 例： スイッチ# **show ipv6 rip cisco interface gigabitethernet2/0/1** または スイッチ# **show ipv6 rip**	• 現在の IPv6 RIP プロセスに関する情報を表示します。 • IPv6 ルーティング テーブルの現在の内容を表示します。
ステップ 10	**copyrunning-configstartup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF for IPv6 の設定（CLI）

ネットワークでは、IPv6 の OSPF をカスタマイズできます。ただし、IPv6 の OSPF のデフォルト設定は、ほとんどのカスタマーおよび機能の要件を満たします。

次の注意事項に従ってください。

- IPv6 コマンドのデフォルト設定を変更する場合は注意してください。デフォルト設定を変更すると、IPv6 ネットワークの OSPF に悪影響が及ぶことがあります。
- インターフェイスで IPv6 OSPF をイネーブルにする前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 OSPF をイネーブルにするレイヤ 3 インターフェイスで IPv6 をイネーブルにする必要があります。

IPv6 の OSPF ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPF for IPv6」の章を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router ospf***process-id* 例： スイッチ(config)# **ipv6 router ospf 21**	プロセスに対して OSPF ルータ コンフィギュレーション モードをイネーブルにします。プロセス ID は、IPv6 OSPF ルーティング プロセスをイネーブルにする場合に管理上割り当てられる番号です。この ID はローカルに割り当てられ、1 ～ 65535 の正の整数を指定できます。
ステップ 3	**area***area-id***range** {*ipv6-prefix/prefixlength*} [**advertise** | **not-advertise**] [**cost***cost*] 例： スイッチ(config)# **area .3 range 2001:0DB8::/32 not-advertise**	（任意）エリア境界でルートを統合および集約します。 • *area-id*：ルートをサマライズするエリアの ID。10 進数または IPv6 プレフィックスのどちらかを指定できます。 • *ipv6-prefix/prefixlength*：宛先 IPv6 ネットワーク、およびプレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進数。10 進値の前にスラッシュ（/）を付加する必要があります。 • **advertise**：（任意）Type 3 サマリー LSA をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。 • **not-advertise**：（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。Type3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。 • **cost***cost*：（任意）現在のサマリー ルートのメトリックまたはコストを設定します。宛先への最短パスを判別する場合に、OSPF SPF 計算で使用します。指定できる値は 0 ～ 16777215 です。
ステップ 4	**maximum paths***number-paths* 例： スイッチ(config)# **maximum paths 16**	（任意）IPv6 OSPF がルーティング テーブルに入力する必要がある、同じ宛先への等コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 32 で、デフォルトは 16 です。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： スイッチ(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 7	**ipv6 ospf***process-id***area***area-id* [**instance***instance-id*] 例： スイッチ(config-if)# **ipv6 ospf 21 area .3**	インターフェイスで IPv6 の OSPF をイネーブルにします。 • **instance***instance-id*：（任意）インスタンス ID。
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。 • **show ipv6 ospf** [*process-id*] [*area-id*]**interface** [*interface-id*] • **show ipv6 ospf** [*process-id*] [*area-id*] 例： スイッチ# **show ipv6 ospf 21 interface gigabitethernet2/0/1** または スイッチ# **show ipv6 ospf 21**	• OSPF インターフェイスに関する情報を表示します。 • OSPF ルーティング プロセスに関する一般情報を表示します。
ステップ 10	**copyrunning-configstartup-config** 例： スイッチ# **copy running-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

IPv6 の EIGRP の設定

IPv6 EIGRP を実行するようにスイッチを設定する前に、 **ip routing global configuration** グローバル コンフィギュレーション コマンドを入力してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを入力して IPv6 パケットの転送をイネーブルにして、IPv6 EIGRP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにします。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定済みのルータ ID を確認してから、**router-id** コマンドを使用します。

EIGRP IPv4 の場合と同様に、EIGRPv6 を使用して EIGRP IPv6 インターフェイスを指定し、これらのサブセットを受動インターフェイスとして選択できます。**passive-interface** コマンドを使用してインターフェイスをパッシブに設定してから、選択したインターフェイスで **no passive-interface** コマンドを使用してこれらのインターフェイスをアクティブにします。受動インターフェイスでは、EIGRP IPv6 を設定する必要がありません。

設定手順の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 ユニキャスト リバース パス転送の設定

ユニキャスト リバース パス転送（ユニキャスト RPF）機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造（スプーフィングされた）送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。たとえば、Smurf や Tribal Flood Network（TFN）など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタすることを攻撃者が阻止できるようにします。パブリック アクセスを提供するインターネット サービス プロバイダー（ISP）の場合、uRPF が IP ルーティング テーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、そのような攻撃をそらします。この処理により、ISP のネットワーク、その顧客、および残りのインターネットが保護されます。

（注）

- ユニキャスト RPF は、IP サービスでのみでサポートされます。
- スイッチが複数のスイッチ タイプが混在する混合ハードウェア スタック内にある場合は、ユニキャスト RPF を設定しないでください。

IP ユニキャスト RPF 設定の詳細については、『Cisco IOS Security Configuration Guide, Release 12.4』の「Other Security Features」の章を参照してください。

IPv6 の表示

次のコマンドの構文および使用方法の詳細については、Cisco IOS のコマンドリファレンスを参照してください。

表 *20*：*IPv6* をモニタリングするコマンド

コマンド	目的
show ipv6 access-list	アクセス リストのサマリーを表示します。
show ipv6 cef	IPv6 の Cisco エクスプレス フォワーディングを表示します。
show ipv6 interface*interface-id*	IPv6 インターフェイスのステータスと設定を表示します。
show ipv6 mtu	宛先キャッシュごとに IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュ エントリを表示します。
show ipv6 ospf	IPv6 OSPF 情報を表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 protocols	スイッチの IPv6 ルーティング プロトコルのリストを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
show ipv6 routers	ローカル IPv6 ルータを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 *21*：*EIGRP IPv6* 情報を表示するためのコマンド

コマンド	目的
show ipv6 eigrp [*as-number*] *interface*	EIGRP IPv6 用に設定されたインターフェイスの情報を表示します。
show ipv6 eigrp [*as-number*] *neighbor*	EIGRP IPv6 で検出されたネイバーを表示します。
show ipv6 interface[*as-number*] *traffic*	送受信される EIGRP IPv6 パケット数を表示します。
show ipv6 eigrptopology [*as-number* | *ipv6-address*] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors** | **Base**]	IPv6 トポロジ テーブルの EIGRP エントリを表示します。

DHCP for IPv6 アドレス割り当ての設定

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトで、DHCPv6 機能はスイッチに設定されています。

DHCPv6 アドレス割り当ての設定時の注意事項

DHCPv6 アドレス割り当てを設定する場合は、次の注意事項に従ってください。

- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイス上でイネーブルである必要があります。
  - SVI：**interface vlan***vlan_id* コマンドを使用して作成された VLAN インターフェイスです。
  - レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel port-channel-number** コマンドを使用して作成されたポートチャネル論理インターフェイス。
- スイッチは、DHCPv6 クライアント、サーバ、またはリレーエージェントとして動作できます。DHCPv6 クライアント、サーバ、およびリレー機能は、インターフェイスで相互に排他的です。
- DHCPv6 クライアント、サーバ、またはリレーエージェントは、マスタースイッチ上でだけ稼働します。スタック マスターの再選出があった場合、新しいマスタースイッチはDHCPv6

設定を維持します。ただし、DHCP サーバ データベース リース情報のローカルの RAM コピーは、維持されません。

DHCPv6 サーバ機能のイネーブル化（CLI）

DHCPv6 プールの特性を変更するには、**no** 形式の DHCP プール コンフィギュレーション モード コマンドを使用します。インターフェイスに対して DHCPv6 サーバ機能をディセーブルにするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスで DHCPv6 サーバをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 dhcp pool***poolname* 例： スイッチ(config)# **ipv6 dhcp pool 7**	DHCP プール コンフィギュレーション モードを開始して、IPv6 DHCP プールの名前を定義します。プール名は、記号文字列（Engineering など）または整数（0 など）です。
ステップ 3	**address prefix***IPv6-prefix* {**lifetime**} {*t1 t1* | **infinite**} 例： スイッチ(config-dhcpv6)# **address prefix 2001:1000::0/64 lifetime 3600**	（任意）アドレス割り当て用のアドレス プレフィックスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 **lifetime***t1 t1*：IPv6 アドレス プレフィックスが有効ステートを維持するタイム インターバル（秒）を指定します。指定できる範囲は 5 ～ 4294967295 秒です。間隔を指定しない場合は、**infinite** を指定します。
ステップ 4	**link-address***IPv6-prefix* 例： スイッチ(config-dhcpv6)# **link-address 2001:1002::0/64**	（任意）link-address IPv6 プレフィックスを指定します。 着信インターフェイス上のアドレスまたはパケットのリンク アドレスが指定した IPv6 プレフィックスに一致する場合、サーバは設定情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

	コマンドまたはアクション	目的
ステップ 5	**vendor-specific***vendor-id* 例： スイッチ(config-dhcpv6)# **vendor-specific 9**	（任意）ベンダー固有のコンフィギュレーション モードを開始して、ベンダー固有のID番号を指定します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ～ 4294967295 です。
ステップ 6	**suboption***number* {**address***IPv6-address* | **ascii***ASCII-string* | **hex***hex-string*} 例： スイッチ(config-dhcpv6-vs)# **suboption 1 address 1000:235D::**	（任意）ベンダー固有のサブオプション番号を入力します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、または16進文字列をサブオプションパラメータで定義されているように入力します。
ステップ 7	**exit** 例： スイッチ(config-dhcpv6-vs)# **exit**	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 8	**exit** 例： スイッチ(config-dhcpv6)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 10	**ipv6dhcpserver** [*poolname* | **automatic**] [**rapid-commit**] [**preference***value*] [**allow-hint**] 例： スイッチ(config-if)# **ipv6 dhcp server automatic**	インターフェイスに対して DHCPv6 サーバ機能をイネーブルにします。 • *poolname*：（任意）IPv6 DHCP プールのユーザ定義の名前。プール名は、記号文字列（Engineering など）または整数（0 など）です。 • **automatic**：（任意）システムが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。 • **rapid-commit**：（任意）2 つのメッセージの交換方法を許可します。

	コマンドまたはアクション	目的
		• **preference***value*：（任意）サーバによって送信されるアドバタイズメントメッセージ内のプリファレンスオプションで指定されるプリファレンス値を設定します。有効な範囲は0～255です。デフォルトのプリファレンス値は0です。 • **allow-hint**：（任意）サーバが、SOLICITメッセージ内のクライアントからの指示を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントのヒントを無視します。
ステップ11	**end** 例： スイッチ(config)# **end**	特権EXECモードに戻ります。
ステップ12	次のいずれかを実行します。 • **show ipv6 dhcp pool** • **show ipv6 dhcp interface** 例： スイッチ# **show ipv6 dhcp pool** または スイッチ# **show ipv6 dhcp interface**	• DHCPv6プール設定を確認します。 • DHCPv6サーバ機能がインターフェイス上でイネーブルであることを確認します。
ステップ13	**copyrunning-configstartup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

DHCPv6クライアント機能のイネーブル化（CLI）

このタスクでは、インターフェイスに対してDHCPv6クライアントをイネーブルにする方法を説明します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ipv6 address dhcp** [**rapid-commit**] 例： スイッチ(config-if)# **ipv6 address dhcp rapid-commit**	インターフェイスで DHCPv6 サーバから IPv6 アドレスを取得できるようにします。 **rapid-commit**：（任意）アドレス割り当てで、2 つのメッセージの交換方法を許可します。
ステップ 4	**ipv6 dhcp client request** [**vendor-specific**] 例： スイッチ(config-if)# **ipv6 dhcp client request vendor-specific**	（任意）インターフェイスでベンダー固有のオプションを要求できるようにします。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**showipv6dhcpinterface** 例： スイッチ# **show ipv6 dhcp interface**	DHCPv6 クライアントがインターフェイスでイネーブルになっていることを確認します。

IPv6 ユニキャスト ルーティングの設定例

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化：例

次に、IPv6 プレフィックス 2001:0DB8:c18:1::/64 に基づく、リンクに対してローカルなアドレスおよびグローバル アドレスを使用して、IPv6 をイネーブルにする例を示します。EUI-64 インターフェイス ID が、両方のアドレスの下位 64 ビットで使用されます。**show ipv6 interface** EXEC コマンドの出力は、インターフェイスのリンクに対してローカルなプレフィックス FE80::/64 にインターフェイス ID（20B:46FF:FE2F:D940）を付加する方法を示すために追加されています。

```
スイッチ(config)# ipv6 unicast-routing
スイッチ(config)# interface gigabitethernet1/0/11
スイッチ(config-if)# no switchport
スイッチ(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
スイッチ(config-if)# end
スイッチ# show ipv6 interface gigabitethernet1/0/11
GigabitEthernet1/0/11 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

デフォルト ルータ プリファレンスの設定：例

次に、インターフェイス上のルータに高い DRP を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# ipv6 nd router-preference high
スイッチ(config-if)# end
```

IPv4 および IPv6 プロトコル スタックの設定：例

次に、インターフェイス上で IPv4 および IPv6 ルーティングをイネーブルにする例を示します。

```
スイッチ(config)# ip routing
スイッチ(config)# ipv6 unicast-routing
```

```
スイッチ(config)# interface fastethernet1/0/11
スイッチ(config-if)# no switchport
スイッチ(config-if)# ip address 192.168.99.1 255.255.255.0
スイッチ(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
スイッチ(config-if)# end
```

DHCPv6 サーバ機能のイネーブル化：例

次の例では、*engineering* というIPv6アドレス プレフィックスを持つプールを設定する方法を示します。

```
スイッチ# configure terminal
スイッチ(config)# ipv6 dhcp pool engineering
スイッチ(config-dhcpv6)#address prefix 2001:1000::0/64
スイッチ(config-dhcpv6)# end
```

次に、3 リンクアドレスおよびIPv6アドレス プレフィックスを持つ *testgroup* と呼ばれるプールを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ipv6 dhcp pool testgroup
スイッチ(config-dhcpv6)# link-address 2001:1001::0/64
スイッチ(config-dhcpv6)# link-address 2001:1002::0/64
スイッチ(config-dhcpv6)# link-address 2001:2000::0/48
スイッチ(config-dhcpv6)# address prefix 2001:1003::0/64
スイッチ(config-dhcpv6)# end
```

次の例では、*350* というベンダー固有オプションを持つプールを設定する方法を示します。

```
スイッチ# configure terminal
スイッチ(config)# ipv6 dhcp pool 350
スイッチ(config-dhcpv6)# address prefix 2001:1005::0/48
スイッチ(config-dhcpv6)# vendor-specific 9
スイッチ(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
スイッチ(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
スイッチ(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能のイネーブル化：例

次に、IPv6 アドレスを取得して、rapid-commit オプションをイネーブルにする例を示します。

```
スイッチ(config)# interface gigabitethernet2/0/1
スイッチ(config-if)# ipv6 address dhcp rapid-commit
```

IPv6 ICMP レート制限の設定：例

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
スイッチ(config)#ipv6 icmp error-interval 50 20
```

IPv6 のスタティック ルーティングの設定：例

次に、アドミニストレーティブ ディスタンスが 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
スイッチ(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130
```

IPv6 の RIP の設定：例

次に、最大 8 の等コスト ルートにより RIP ルーティング プロセス *cisco* をイネーブルにし、インターフェイス上でこれをイネーブルにする例を示します。

```
スイッチ(config)# ipv6 router rip cisco
スイッチ(config-router)# maximum-paths 8
スイッチ(config)# exit
スイッチ(config)# interface gigabitethernet2/0/11
スイッチ(config-if)# ipv6 rip cisco enable
```

IPv6 の表示：例

次に、**show ipv6 interface** 特権 EXEC コマンドの出力例を示します。

```
スイッチ# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
<output truncated>
```

第 13 章

IPv6 マルチキャストの実装

- 機能情報の確認，215 ページ
- IPv6 マルチキャスト ルーティングの実装に関する情報，215 ページ
- IPv6 マルチキャストの実装，224 ページ

機能情報の確認

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

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

IPv6 マルチキャスト ルーティングの実装に関する情報

この章では、スイッチに IPv6 マルチキャスト ルーティングを実装する方法について説明します。

従来の IP 通信では、ホストはパケットを単一のホスト（ユニキャスト伝送）またはすべてのホスト（ブロードキャスト伝送）に送信できます。IPv6 マルチキャストは、第三の方式を提供するものであり、ホストが単一のデータ ストリームをすべてのホストのサブセット（グループ伝送）に同時に送信できるようにします。

IPv6 マルチキャストの概要

IPv6 マルチキャスト グループは、特定のデータ ストリームを受信する受信側の任意のグループです。このグループには、物理的境界または地理的境界はありません。受信側は、インターネット上または任意のプライベート ネットワーク内の任意の場所に配置できます。特定のグループへの

データ フローの受信に関与する受信側は、ローカル スイッチに対してシグナリングすることによってそのグループに加入する必要があります。このシグナリングは、MLDプロトコルを使用して行われます。

スイッチは、MLDプロトコルを使用して、直接接続されているサブネットにグループのメンバが存在するかどうかを学習します。ホストは、MLD レポート メッセージを送信することによってマルチキャスト グループに加入します。ネットワークでは、各サブネットでマルチキャスト データのコピーを 1 つだけ使用して、潜在的に無制限の受信側にデータが伝送されます。トラフィックの受信を希望する IPv6 ホストはグループ メンバと呼ばれます。

グループ メンバに伝送されるパケットは、単一のマルチキャスト グループ アドレスによって識別されます。マルチキャストパケットは、IPv6ユニキャストパケットと同様に、ベストエフォート型の信頼性を使用してグループに伝送されます。

マルチキャスト環境は、送信側と受信側で構成されます。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージをリッスンして受信できます。

マルチキャスト アドレスがマルチキャスト グループの受信先として選択されます。送信者は、データグラムの宛先アドレスとしてグループのすべてのメンバに到達するためにそのアドレスを使用します。

マルチキャスト グループ内のメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。マルチキャスト グループ内のメンバの場所または数に制約はありません。ホストは、一度に複数のマルチキャスト グループのメンバにすることができます。

マルチキャスト グループがどの程度アクティブであるか、その期間、およびメンバーシップはグループおよび状況によって異なります。メンバを含むグループにアクティビティがない場合もあります。

IPv6 マルチキャスト ルーティングの実装

Cisco IOS ソフトウェアでは、IPv6 マルチキャスト ルーティングを実装するため、次のプロトコルがサポートされています。

- MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャスト アドレスを宛先としたマルチキャストパケットを受信するために使用するノード）を検出するために IPv6 スイッチで使用されます。MLD には 2 つのバージョンがあります。MLD バージョン 1 はバージョン 2 のインターネット グループ管理プロトコル（IGMP）for IPv4 をベースとしています。MLD バージョン 2 はバージョン 3 の IGMP for IPv4 をベースとしています。Cisco IOS ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 と MLD バージョン 1 の両方が使用されます。MLD バージョン 2 は、MLD バージョン 1 と完全な下位互換性があります（RFC 2710 で規定）。MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているスイッチと相互運用します。MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。
- PIM-SM は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。

- PIM in Source Specific Multicast（PIM-SSM）は PIM-SM と類似していますが、IP マルチキャストアドレスを宛先とした特定の送信元アドレス（または特定の送信元アドレスを除くすべてのアドレス）からのパケットを受信する対象をレポートする機能を別途備えています。

IPv6 マルチキャスト リスナー ディスカバリ プロトコル

キャンパス ネットワークでマルチキャストの実装を開始するには、ユーザは最初に、誰がマルチキャストを受信するかを定義する必要があります。MLDプロトコルは、直接接続されているリンク上のマルチキャストリスナー（たとえば、マルチキャストパケットを受信するノード）の存在を検出するため、およびこれらのネイバーノードを対象にしている特定のマルチキャストアドレスを検出するために、IPv6スイッチによって使用されます。これは、ローカル グループおよび送信元固有のグループ メンバーシップの検出に使用されます。

MLD プロトコルは、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャスト トラフィックのフローを自動的に制御および制限する手段を提供します。

マルチキャスト クエリアとマルチキャスト ホスト

マルチキャスト クエリアは、クエリー メッセージを送信して、特定のマルチキャスト グループのメンバーであるネットワーク デバイスを検出するネットワーク デバイス（スイッチなど）です。

マルチキャストホストは、受信側（スイッチを含む）としてレポートメッセージを送信し、クエリアにホスト メンバーシップを通知します。

同じ送信元からのマルチキャストデータ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは、MLD レポートを使用して、マルチキャストグループに対する加入および脱退を行ったり、グループ トラフィックの受信を開始したりします。

MLD では、メッセージの伝送にインターネット制御メッセージ プロトコル（ICMP）が使用されます。すべての MLD メッセージはホップ制限が 1 のリンクローカルであり、すべてにスイッチ アラート オプションが設定されています。スイッチ アラート オプションは、ホップバイホップ オプション ヘッダーの実装を意味します。

MLD アクセス グループ

MLD アクセス グループは、Cisco IOS IPv6 マルチキャスト スイッチでの受信側アクセス コントロールを実現します。この機能では、受信側が加入できるグループのリストを制限し、SSM チャネルへの加入に使用される送信元を許可または拒否します。

受信側の明示的トラッキング

明示的トラッキング機能を使用すると、スイッチがIPv6ネットワーク内のホストの動作を追跡できるようになります。また、この機能により、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

プロトコル独立マルチキャスト

プロトコル独立マルチキャスト（PIM）は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。PIM は、ユニキャスト ルーティング プロトコルとは独立して動作し、他のプロトコルと同様に、マルチキャスト ルート アップデートの送受信を実行します。ユニキャスト ルーティング テーブルに値を入力するために LAN でどのユニキャスト ルーティング プロトコルが使用されているかどうかにかかわらず、Cisco IOS PIM では、独自のルーティング テーブルを構築および管理する代わりに、既存のユニキャスト テーブル コンテンツを使用して、Reverse Path Forwarding（RPF）チェックを実行します。

PIM-SM または PIM-SSM のいずれかを使用するように IPv6 マルチキャストを設定することも、ネットワークで PIM-SM と PIM-SSM の両方を使用することもできます。

PIM スパース モード

IPv6 マルチキャストでは、PIM-SM を使用したドメイン内マルチキャスト ルーティングがサポートされています。PIM-SM は、ユニキャスト ルーティングを使用して、マルチキャスト ツリー構築用のリバースパス情報を提供しますが、特定のユニキャストルーティングプロトコルには依存しません。

PIM-SM は、トラフィックに対して明示的な要求がある場合を除いて、各マルチキャストに関与しているスイッチの数が比較的少なく、これらのスイッチがグループのマルチキャスト パケットを転送しないときに、マルチキャスト ネットワークで使用されます。PIM-SM は、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SM は最初に共有ツリーを使用しますが、これには RP の使用が必要となります。

要求は、ツリーのルート ノードに向けてホップバイホップで送信される PIM join を使用して行われます。PIM-SM のツリーのルート ノードは、共有ツリーの場合は RP、最短パス ツリー（SPT）の場合はマルチキャスト送信元に直接接続されているファーストホップ スイッチになります。RP はマルチキャスト グループを追跡し、マルチキャスト パケットを送信するホストはそのホストのファーストホップ スイッチによって RP に登録されます。

PIM join がツリーの上位方向に送信されると、要求されたマルチキャスト トラフィックがツリーの下位方向に転送されるように、パス上のスイッチがマルチキャスト転送ステートを設定します。マルチキャスト トラフィックが不要になったら、スイッチはルート ノードに向けてツリーの上位方向に PIM prune を送信し、不必要なトラフィックをプルーニング（削除）送信します。この PIM prune がホップごとにツリーを上位方向に移動する際、各スイッチはその転送状態を適切に更新します。最終的に、マルチキャスト グループまたは送信元に関連付けられている転送ステートは削除されます。

マルチキャスト データの送信側は、マルチキャスト グループを宛先としたデータを送信します。送信側の指定スイッチ（DR）は、これらのデータ パケットを受け取り、ユニキャストでカプセル化し、RP に直接送信します。RP は、カプセル化されたこれらのデータ パケットを受信し、カプセル化を解除し、共有ツリー上に転送します。そのあと、パケットは、RP ツリー上のスイッチの（*, G）マルチキャスト ツリー ステートに従って、RP ツリー ブランチの任意の場所に複製され、そのマルチキャスト グループのすべての受信側に最終的に到達します。RP へのデータ パケット

のカプセル化のプロセスは登録と呼ばれ、カプセル化されたパケットはPIM レジスタ パケットと呼ばれます。

IPv6 BSR：RP マッピングの設定

ドメイン内の PIM スイッチは、各マルチキャスト グループを正しい RP アドレスにマッピングできる必要があります。PIM-SM 対応の BSR プロトコルは、グループと RP のマッピング情報をドメイン全体に迅速に配布するためのダイナミック適応メカニズムを備えています。IPv6 BSR 機能を使用すると、到達不能になった RP が検出され、マッピング テーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。

すべての PIM-SM マルチキャスト グループを RP の IP または IPv6 アドレスに関連付ける必要があります。新しいマルチキャスト送信側が送信を開始すると、そのローカル DR がこれらのデータ パケットを PIM register メッセージにカプセル化し、そのマルチキャスト グループの RP に送信します。新しいマルチキャスト受信側が加入すると、そのローカル DR がそのマルチキャスト グループの RP に PIM join メッセージを送信します。PIM スイッチは、（*, G）join メッセージを送信するとき、RP 方向への次のスイッチを認識して、G（グループ）がそのスイッチにメッセージを送信できるようにする必要があります。また、PIM スイッチは、（*, G）ステートを使用してデータ パケットを転送するとき、G を宛先としたパケットの正しい着信インターフェイスを認識する必要があります。これは、他のインターフェイスに着信するパケットを拒否する必要があるためです。

ドメイン内の少数のスイッチが候補ブートストラップ スイッチ（C-BSR）として設定され、単一のBSRがそのドメイン用に選択されます。また、ドメイン内の一連のスイッチが候補RP（C-RP）として設定されます。通常、これらのスイッチは、C-BSRとして設定されているものと同じスイッチです。候補RPは、候補RPアドバタイズメント（C-RP-Adv）メッセージをそのドメインのBSRに定期的にユニキャストし、RP になる意思をアドバタイズします。C-RP-Adv メッセージには、アドバタイズを行っている C-RP のアドレス、およびグループ アドレスとマスク長のフィールドの任意のリストが含まれています。これらのフィールドは、立候補のアドバタイズの対象となるグループ プレフィックスを示します。BSR は、定期的に発信するブートストラップ メッセージ（BSM）にこれらの一連の C-RP とそれに対応するグループ プレフィックスを含めます。BSM は、ドメイン全体にホップバイホップで配布されます。

双方向 BSR がサポートされているため、双方向 RP を C-RP メッセージおよび BSM の双方向範囲でアドバタイズできます。システム内のすべてのスイッチは、BSM で双方向範囲を使用できる必要があります。使用できない場合は、双方向 RP 機能が機能しません。

PIM 送信元固有マルチキャスト

PIM-SSMは、SSMの実装をサポートするルーティング プロトコルであり、PIM-SMから派生したものです。ただし、PIM-SM では PIM join を受けてすべてのマルチキャスト送信元からデータが送信されるのに対し、SSM 機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラム トラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネット ブロードキャスト トラフィックが拒否されます。さらに、SSM では、RPと共有ツリーを使用する代わりに、マルチキャスト グループの送信元アドレスで見つかった情報を使用します。この情報は、MLD メンバーシップ レポートによってラストホップ スイッ

チにリレーされる送信元アドレスを通して受信側から提供されます。その結果として、送信元に直接つながる最短パス ツリーが得られます。

SSM では、データグラムは（S, G）チャネルに基づいて配信されます。1 つの（S, G）チャネルのトラフィックは、IPv6 ユニキャスト送信元アドレス S とマルチキャスト グループ アドレス G を IPv6 宛先アドレスとして使用するデータグラムで構成されます。システムは、（S, G）チャネルのメンバになることによって、このトラフィックを受信します。シグナリングは不要ですが、受信側は特定の送信元からのトラフィックを受信する場合は（S,G）チャネルに加入し、トラフィックを受信しない場合はチャネルから脱退する必要があります。

SSM を動作させるには、MLD バージョン 2 が必要です。MLD を使用すると、ホストが送信元の情報を提供できるようになります。MLD を使用して SSM を動作させるには、Cisco IOS IPv6 スイッチ、アプリケーションが実行されているホスト、およびアプリケーション自体で SSM がサポートされている必要があります。

ルーティング可能アドレスの hello オプション

IPv6 内部ゲートウェイ プロトコルを使用してユニキャスト ルーティング テーブルを構築する場合、アップストリーム スイッチ アドレスを検出するための手順では、PIM ネイバーとネクストホップ スイッチが同じスイッチを表しているかぎり、これらのアドレスは常に同じであるものと想定されます。ただし、スイッチがリンク上に複数のアドレスを持つ場合は、このことが当てはまるとはかぎりません。

この状況は IPv6 において、2 つの一般的な状況で発生することがあります。1 つめの状況は、ユニキャスト ルーティング テーブルが IPv6 内部ゲートウェイ プロトコル（マルチキャスト BGP など）によって構築されない場合に発生します。2 つめの状況は、RP のアドレスがダウンストリーム スイッチとサブネット プレフィックスを共有している場合に発生します（RP スイッチ アドレスはドメインワイドにする必要があるため、リンクローカル アドレスにはできないことに注意してください）。

ルーティング可能アドレスの hello オプションによって、PIM プロトコルでこのような状況を回避できます。このためには、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージ オプションを追加します。PIM スイッチが何らかのアドレスのアップストリーム スイッチを検出すると、RPF 計算の結果は、PIM ネイバーのアドレス自体に加えて、このオプションのアドレスとも比較されます。このオプションにはそのリンク上の PIM スイッチの考えられるアドレスがすべて含まれているため、対象の PIM スイッチがこのオプションをサポートしている場合、常に RPF 計算の結果が含まれます。

PIM メッセージにサイズ制限があることと、ルーティング可能アドレスの hello オプションが単一の PIM hello メッセージ内に収まる必要があるため、インターフェイスで設定できるアドレスの制限は 16 個になっています。

PIM IPv6 スタブ ルーティング

PIM スタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動し、リソースの利用率を軽減します。

PIM スタブ ルーティングを使用するネットワークでは、ユーザに対する IPv6 トラフィックの唯一の許容ルートは、PIM スタブ ルーティングを設定しているスイッチ経由です。PIM 受動インター

フェイスは、VLAN などのレイヤ 2 アクセス ドメイン、または他のレイヤ 2 デバイスに接続されているインターフェイスに接続されます。直接接続されたマルチキャスト レシーバおよび送信元のみが、レイヤ 2 アクセス ドメインで許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

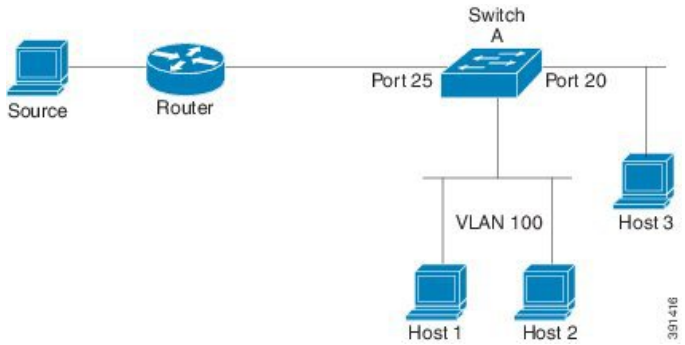
PIM スタブ ルーティングを使用しているときは、IPv6 マルチキャスト ルーティングを使用し、スイッチだけを PIM スタブ ルータとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。スイッチは分散ルータ間の伝送トラフィックをルーティングしません。スイッチのルーテッド アップリンク ポートも設定する必要があります。SVI の場合は、スイッチのアップリンク ポートを使用できません。

また、PIM スタブ ルーティングをスイッチに設定するときは、EIGRP スタブ ルーティングも設定する必要があります。詳細については、EIGRPv6 スタブ ルーティング, （184 ページ）を参照してください。

冗長 PIM スタブ ルータ トポロジーはサポートされません。単一のアクセス ドメインにマルチキャスト トラフィックを転送している複数の PIM ルータがある場合、冗長トポロジーが存在します。PIM メッセージはブロックされ、PIM アサートおよび指定されたルータ選出メカニズムは PIM 受動インターフェイスではサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけがサポートされます。非冗長トポロジーを使用することで、PIM 受動インターフェイスはそのアクセス ドメインで唯一のインターフェイスおよび指定ルータであると想定します。

次に示す図では、スイッチ A ルーテッド アップリンク ポート 25 がルータに接続され、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。この設定により、直接接続されたホストはマルチキャスト発信元からトラフィックを受信できます。詳細については、PIM IPv6 スタブ ルーティングの設定, （236 ページ）を参照してください。

図 *7*：*PIM* スタブ ルータ設定



スタティック mroute

IPv6 スタティック mroute は、RPF チェックを変化させるために使用する IPv4 スタティック mroute とほぼ同様に動作します。IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、RPF チェックに対するスタティック ルート サポートを拡張することによって実装されます。スタティック mroute では、等コスト マルチパス mroute がサポートされています。また、ユニキャスト専用スタティック ルートもサポートされています。

MRIB

マルチキャストルーティング情報ベース（MRIB）は、マルチキャスト ルーティング プロトコル（ルーティング クライアント）によってインスタンス化されるマルチキャスト ルーティング エントリのプロトコル非依存リポジトリです。その主要機能は、ルーティング プロトコルとマルチキャスト転送情報ベース（MFIB）間の非依存性を実現することです。また、クライアント間の調整および通信ポイントとしても機能します。

ルーティング クライアントは、MRIB が提供するサービスを使用して、ルーティング エントリをインスタンス化し、他のクライアントによってルーティング エントリに加えられた変更を取得します。MRIB では、ルーティング クライアント以外に、転送クライアント（MFIB インスタンス）や特別なクライアント（MLD など）も扱われます。MFIB は、MRIB からその転送エントリを取得し、パケットの受信に関連するイベントについて MRIB に通知します。これらの通知は、ルーティング クライアントによって明示的に要求されることも、MFIB によって自発的に生成されることもあります。

MRIB のもう 1 つの重要な機能は、同じマルチキャスト セッション内でマルチキャスト接続を確立する際に、複数のルーティング クライアントの調整を可能にすることです。また、MRIB では、MLD とルーティング プロトコル間の調整も可能です。

MFIB

MFIB は、IPv6 ソフトウェア用のプラットフォーム非依存およびルーティング プロトコル非依存ライブラリです。その主な目的は、転送テーブルが変更されたときに、Cisco IOS プラットフォームに、IPv6 マルチキャスト転送テーブルおよび通知を読み取るインターフェイスを提供することです。MFIB が提供する情報には、明確に定義された転送セマンティクスが含まれています。この情報は、プラットフォームが特定のハードウェアまたはソフトウェア転送メカニズムに容易に変換できる設計になっています。

ネットワーク内でルーティングまたはトポロジが変更されると、IPv6 ルーティング テーブルがアップデートされ、これらの変更が MFIB に反映されます。MFIB は、IPv6 ルーティング テーブル内の情報に基づいて、ネクストホップ アドレス情報を管理します。MFIB エントリとルーティング テーブル エントリの間には 1 対 1 の相互関係があるため、MFIB には既知のすべてのルートが含まれ、高速スイッチングや最適スイッチングなどのスイッチング パスに関連付けられているルート キャッシュ管理の必要がなくなります。

MFIB

（注） 分散 MFIB は、マスターが他のスタック メンバーに MFIB 情報を配布するスタック環境でのみ意味を持ちます。次のセクションでは、ラインカードは単にスタックのメンバー スイッチです。

MFIB（MFIB）は、分散型プラットフォーム上でマルチキャスト IPv6 パケットをスイッチングするために使用されます。また、MFIB には、ラインカード間での複製に関するプラットフォーム固

有の情報も含まれることがあります。転送ロジックのコアを実装する基本 MFIB ルーチンは、すべての転送環境に共通です。

MFIB は、次の機能を実装します。

- ラインカードで生成されたデータ駆動型プロトコル イベントを PIM にリレーします。
- MFIB プラットフォーム アプリケーション プログラム インターフェイス（API）を提供し、ハードウェア アクセラレーション エンジンのプログラミングを担っている、プラットフォーム固有のコードに MFIB の変更を伝播します。また、この API には、ソフトウェアでパケットをスイッチングしたり（パケットがデータ駆動型イベントのトリガーとなっている場合に必要）、ソフトウェアにトラフィックの統計情報をアップロードしたりするエントリ ポイントも含まれています。

また、MFIB および MRIB サブシステムを組み合わせて使用すると、スイッチが各ラインカードで MFIB データベースの「カスタマイズ」コピーを保有したり、MFIB 関連のプラットフォーム固有の情報を RP からラインカードに転送したりできるようになります。

IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング

統合 MFIB は、IPv6 マルチキャストでの PIM-SM および PIM-SSM に対するファスト スイッチングおよびプロセス スイッチングの両サポートを提供するために使用されます。プロセス スイッチングでは、の IOS デーモンが各パケットの調査、書き換え、および転送を行う必要があります。最初にパケットが受信され、システム メモリにコピーされます。次に、スイッチがルーティング テーブル内でレイヤ 3 ネットワーク アドレスを検索します。そのあと、レイヤ 2 フレームがネクストホップの宛先アドレスで書き換えられ、発信インターフェイスに送信されます。また、IOSd は、巡回冗長検査（CRC）も計算します。このスイッチング方式は、IPv6 パケットをスイッチングする方式の中でスケーラビリティが最も低い方式です。

IPv6 マルチキャストの高速スイッチングを使用すると、スイッチは、プロセス スイッチングよりも高いパケット転送パフォーマンスを実現できます。従来ルート キャッシュに格納される情報は、IPv6 マルチキャスト スイッチング用にいくつかのデータ構造に格納されます。これらのデータ構造では、ルックアップが最適化され、パケット転送を効率的に行えるようになっています。

IPv6 マルチキャスト転送では、PIM プロトコル ロジックで許可されていれば、最初のパケットのファスト スイッチングが行われます。IPv6 マルチキャストの高速スイッチングでは、MAC カプセル化ヘッダーが事前に計算されます。IPv6 マルチキャストの高速スイッチングでは、MFIB を使用して、IPv6 送信先プレフィックス ベースのスイッチング判定が行われます。IPv6 マルチキャストの高速スイッチングでは、MFIB に加えて、隣接関係テーブルを使用して、レイヤ 2 アドレッシング情報が付加されます。隣接関係テーブルでは、すべての MFIB エントリのレイヤ 2 ネクストホップ アドレスが管理されます。

隣接が検出されると、隣接関係テーブルにそのデータが入力されます。（ARP などを使用して）隣接エントリが作成されるたびに、その隣接ノードのリンク層ヘッダーが事前に計算され、隣接関係テーブルに格納されます。ルートが決定されると、そのヘッダーはネクスト ホップおよび対応する隣接エントリを指します。そのあと、そのヘッダーはパケット スイッチング時のカプセル化に使用されます。

ロードバランシングと冗長性の両方に対応するようにスイッチが設定されている場合など、ルートには送信先プレフィックスへの複数のパスが存在することがあります。解決されたパスごとに、そのパスのネクストホップ インターフェイスに対応する隣接へのポインタが追加されます。このメカニズムは、複数のパスでのロード バランシングに使用されます。

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 機能では、マルチプロトコル BGP for IPv6 拡張を提供し、IPv4 BGP と同じ機能と機能性をサポートします。マルチキャスト BGP に対する IPv6 拡張には、IPv6 マルチキャスト アドレス ファミリ、ネットワーク層到達可能性情報（NLRI）、およびIPv6アドレスを使用するネクストホップ（宛先へのパス内の次のスイッチ）属性のサポートが含まれています。

マルチキャスト BGP は、ドメイン間 IPv6 マルチキャストの配布を可能にする、拡張された BGP です。マルチプロトコル BGP では、複数のネットワーク層プロトコル アドレス ファミリ（IPv6 アドレス ファミリなど）および IPv6 マルチキャスト ルートに関するルーティング情報を伝送します。IPv6 マルチキャスト アドレス ファミリには、IPv6 PIM プロトコルによる RPF ルックアップに使用される複数のルートが含まれており、マルチキャストBGP IPv6は、同じドメイン間転送を提供します。ユニキャスト BGP が学習したルートは IPv6 マルチキャストには使用されないため、ユーザは、BGP で IPv6 マルチキャストを使用する場合は、マルチプロトコル BGP for IPv6 マルチキャストを使用する必要があります。

マルチキャスト BGP 機能は、個別のアドレス ファミリ コンテキストを介して提供されます。Subsequent Address Family Identifier（SAFI）では、属性で伝送されるネットワーク層到達可能性情報のタイプに関する情報を提供します。マルチプロトコルBGPユニキャストではSAFI 1 メッセージを使用し、マルチプロトコル BGP マルチキャストでは SAFI 2 メッセージを使用します。SAFI 1 メッセージは、ルートは IP ユニキャストだけに使用でき、IP マルチキャストには使用できないことを示します。この機能があるため、IPv6 ユニキャスト RIB 内の BGP ルートは、IPv6 マルチキャスト RPF ルックアップでは無視される必要があります。

IPv6 マルチキャスト RPF ルックアップを使用して、異なるポリシーおよびトポロジ（IPv6 ユニキャストとマルチキャストなど）を設定するよう、個別のBGPルーティングテーブルが維持されています。マルチキャスト RPF ルックアップは、IP ユニキャスト ルート ルックアップと非常によく似ています。

IPv6マルチキャストBGPテーブルと関連付けられているMRIBはありません。ただし、必要な場合、IPv6 マルチキャスト BGP は、ユニキャスト IPv6 RIB で動作します。マルチキャスト BGP では、IPv6 ユニキャスト RIB へのルートの挿入や更新は行いません。

IPv6 マルチキャストの実装

IPv6 マルチキャスト ルーティングのイネーブル化

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 multicast-routing** 例： スイッチ (config)# **ipv6 multicast-routing**	すべての IPv6 対応インターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルになっているすべてのスイッチ インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにします。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD プロトコルのカスタマイズおよび確認

インターフェイスでの MLD のカスタマイズおよび確認

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***type number* 例： Switch(config)# **interface GigabitEthernet 1/0/1**	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 3	**ipv6 mld join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]} 例： Switch (config-if) # **ipv6 mld join-group FF04::10**	指定したグループおよび送信元に対して MLD レポートを設定します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 mld access-group***access-list-name* 例： `Switch (config-if) # ipv6 access-list acc-grp-1`	ユーザに IPv6 マルチキャストの受信側アクセス コントロールの実行を許可します。
ステップ 5	**ipv6 mld static-group** [*group-address*] [**include** | **exclude**] {*source-address* | source-list [*acl*]} 例： `Switch (config-if) # ipv6 mld static-group ff04::10 include 100::1`	指定したインターフェイスにマルチキャスト グループのトラフィックをスタティックに転送し、MLD ジョイナがインターフェイスに存在するかのようにインターフェイスが動作するようにします。
ステップ 6	**ipv6 mld query-max-response-time***seconds* 例： `Switch (config-if) # ipv6 mld query-max-response-time 20`	MLD キューにアドバタイズされる最大応答時間を設定します。
ステップ 7	**ipv6 mld query-timeout***seconds* 例： `Switch (config-if) # ipv6 mld query-timeout 130`	スイッチがインターフェイスのクエリアとして引き継ぐまでのタイムアウト値を設定します。
ステップ 8	**exit** 例： `Switch (config-if) # exit`	このコマンドを2回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 9	**show ipv6 mldgroups [link-local]** [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**] 例： `Switch # show ipv6 mld groups GigabitEthernet 1/0/1`	スイッチに直接接続されており、MLD を介して学習したマルチキャスト グループを表示します。
ステップ 10	**show ipv6 mld groups summary** 例： `Switch # show ipv6 mld groups summary`	MLD キャッシュに存在する (*, G) および (S, G) メンバーシップ レポートの番号を表示します。

	コマンドまたはアクション	目的
ステップ 11	**show ipv6 mldinterface** [*type number*] 例： `Switch # show ipv6 mld interface GigabitEthernet 1/0/1`	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 12	**debug ipv6 mld** [*group-name* | *group-address* | *interface-type*] 例： `Switch # debug ipv6 mld`	MLD プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 13	**debug ipv6 mld explicit** [*group-name* | *group-address* 例： `Switch # debug ipv6 mld explicit`	ホストの明示的トラッキングに関連する情報を表示します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

MLD グループ制限の実装

インターフェイス単位の MLD 制限とグローバル MLD 制限は相互に独立して機能します。インターフェイス単位の MLD 制限とグローバル MLD 制限の両方を同じスイッチで設定できます。MLD制限の数は、グローバルの場合もインターフェイス単位の場合も、デフォルトでは設定されません。ユーザが制限を設定する必要があります。インターフェイス単位のステート制限またはグローバル ステート制限を超えるメンバーシップ レポートは無視されます。

MLD グループ制限のグローバルな実装

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6 mld** [*vrf vrf-name*] **state-limit***number*
4. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ# **enable**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mld** [*vrf vrf-name*] **state-limit***number* 例： スイッチ(config)# **ipv6 mld state-limit 300**	MLD ステートの数をグローバルに制限します。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD グループ制限のインターフェイス単位での実装

手順の概要

1. **enable**
2. **configureterminal**
3. **interface type***number*
4. **ipv6 mld limit***number* [**except**]*access-list*
5. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface type***number* 例： スイッチ(config)# **interface GigabitEthernet 1/0/1**	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 mld limit***number* [**except**]*access-list* 例： スイッチ(config-if)# **ipv6 mld limit 100**	MLD ステートの数をインターフェイス単位で制限します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

受信側の明示的トラッキングによってホストの動作を追跡するための設定

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***type number* 例： Switch(config)# **interface GigabitEthernet 1/0/1**	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 mld explicit-tracking***access-list-name* 例： `Switch(config-if)# ipv6 mld explicit-tracking list1`	ホストの明示的トラッキングをイネーブルにします。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD トラフィック カウンタのリセット

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mldtraffic** 例： `Switch # clear ipv6 mld traffic`	すべての MLD トラフィック カウンタをリセットします。
ステップ 2	**show ipv6 mldtraffic** 例： `Switch # show ipv6 mld traffic`	MLD トラフィック カウンタを表示します。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

MLD インターフェイス カウンタのクリア

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mldcounters***interface-type* 例： `Switch # clear ipv6 mld counters Ethernet1/0`	MLD インターフェイス カウンタをクリアします。
ステップ 2	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM の設定

ここでは、PIM の設定方法について説明します。

PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 pim **rp-address***ipv6-address*[*group-access-list*] 例： `Switch (config) # ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C acc-grp-1`	特定のグループ範囲の PIM RP のアドレスを設定します。
ステップ 3	**exit** 例： `Switch (config) # exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権EXECモードに戻します。
ステップ 4	**show ipv6 piminterface** [state-on] [**state-off**] [*type-number*] 例： `Switch # show ipv6 pim interface`	PIM に対して設定されたインターフェイスに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 5	**show ipv6 pimgroup-map** [*group-name* | group-address] | [*group-range* | *group-mask*] [**info-source {bsr** | **default** | **embedded-rp** | **static**}] 例： `Switch # show ipv6 pim group-map`	IPv6 マルチキャスト グループ マッピング テーブルを表示します。
ステップ 6	**show ipv6 pimneighbor** [**detail**] [*interface-type interface-number* | **count**] 例： `Switch # show ipv6 pim neighbor`	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。
ステップ 7	**show ipv6 pimrange-list** [**config**] [*rp-address* | *rp-name*] 例： `Switch # show ipv6 pim range-list`	IPv6 マルチキャスト範囲リストに関する情報を表示します。
ステップ 8	**show ipv6 pimtunnel** [*interface-type interface-number*] 例： `Switch # show ipv6 pim tunnel`	インターフェイス上の PIM レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示します。
ステップ 9	**debug ipv6 pim** [*group-name* | *group-address* | **interface***interface-type* | **bsr** | **group** | **mvpn** | **neighbor**] 例： `Switch # debug ipv6 pim`	PIM プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM オプションの設定

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pimspt-threshold infinity** [**group-list***access-list-name*] 例： `Switch (config) # ipv6 pim spt-threshold infinity group-list acc-grp-1`	PIM リーフ スイッチが指定したグループの SPT に加入するタイミングを設定します。
ステップ 3	**ipv6 pimaccept-register** {**list***access-list* | **route-map***map-name*} 例： `Switch (config) # ipv6 pim accept-register route-map reg-filter`	RP のレジスタを許可または拒否します。
ステップ 4	**interface***type number* 例： `Switch (config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**ipv6 pim dr-priority***value* 例： `Switch (config-if) # ipv6 pim dr-priority 3`	PIM スイッチの DR プライオリティを設定します。
ステップ 6	**ipv6 pim hello-interval***seconds* 例： `Switch (config-if) # ipv6 pim hello-interval 45`	インターフェイスにおける PIM hello メッセージの頻度を設定します。
ステップ 7	**ipv6 pim join-prune-interval***seconds* 例： `Switch (config-if) # ipv6 pim join-prune-interval 75`	指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。
ステップ 8	**exit** 例： `Switch (config-if) # exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**ipv6 pimjoin-prune statistic** [*interface-type*] 例： `Switch (config-if) # show ipv6 pim join-prune statistic`	各インターフェイスの最後の集約パケットに関する平均 join-prune 集約を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM トラフィック カウンタのリセット

PIM が誤動作する場合、または予想される PIM パケット数が送受信されていることを確認するために、ユーザは PIM トラフィック カウンタをクリアできます。トラフィック カウンタがクリアされたら、ユーザは show ipv6 pim traffic コマンドを入力して、PIM が正しく機能していること、および PIM パケットが正しく送受信されていることを確認できます。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 pimtraffic** 例： `Switch # clear ipv6 pim traffic`	PIM トラフィック カウンタをリセットします。
ステップ 2	**show ipv6 pimtraffic** 例： `Switch # show ipv6 pim traffic`	PIM トラフィック カウンタを表示します。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット

MRIB を使用するのに設定は不要です。ただし、特定の状況においては、ユーザは PIM トポロジ テーブルをクリアして MRIB 接続をリセットし、MRIB 情報を確認する必要がある場合があります。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 pimtopology** [*group-name* | *group-address*] 例： `Switch # clear ipv6 pim topology FF04::10`	PIM トポロジ テーブルをクリアします。
ステップ 2	**show ipv6 mribclient** [**filter**] [**name** {*client-name* | *client-name***: client-id**}] 例： `Switch # show ipv6 mrib client`	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 3	**show ipv6 mribroute** {**link-local** | **summary** | [*sourceaddress-or-name* | *] [*groupname-or-address*[*prefix-length*]]] 例： `Switch # show ipv6 mrib route`	MRIB ルート情報を表示します。
ステップ 4	**show ipv6 pimtopology** [*groupname-or-address* [*sourceaddress-or-name*] | **link-local** | **route-count** [**detail**]] 例： `Switch # show ipv6 pim topology`	特定のグループまたはすべてのグループの PIM トポロジ テーブル情報を表示します。
ステップ 5	**debug ipv6 mribclient** 例： `Switch # debug ipv6 mrib client`	MRIB クライアント管理アクティビティに対するデバッグをイネーブルにします。
ステップ 6	**debug ipv6 mribio** 例： `Switch # debug ipv6 mrib io`	MRIB I/O イベントに対するデバッグをイネーブルにします。
ステップ 7	**debug ipv6 mrib proxy** 例： `Switch # debug ipv6 mrib proxy`	分散型スイッチプラットフォームにおけるスイッチプロセッサとラインカード間の MRIB プロキシ アクティビティに対するデバッグをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 8	**debug ipv6 mribroute** [*group-name* | *group-address*] 例： `Switch # debug ipv6 mrib route`	MRIB ルーティング エントリ関連のアクティビティに関する情報を表示します。
ステップ 9	**debug ipv6 mribtable** 例： `Switch # debug ipv6 mrib table`	MRIBテーブル管理アクティビティに対するデバッグをイネーブルにします。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM IPv6 スタブ ルーティングの設定

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。サポート対象の PIM インターフェイスは、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類です。PIM パッシブ モードに設定されているルーテッド インターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過させたり転送したりするのは MLD トラフィックだけです。

PIM IPv6 スタブ ルーティングの設定時の注意事項

- PIM スタブ ルーティングを設定する前に、スタブ ルータと中央のルータの両方に IPv6 マルチキャスト ルーティングが設定されている必要があります。また、スタブ ルータのアップリンク インターフェイス上に、PIM モード（スパースモード）が設定されている必要があります。
- PIM スタブ ルータは、ディストリビューション ルータ間の伝送トラフィックのルーティングは行いません。ユニキャスト（EIGRP）スタブ ルーティングではこの動作が強制されます。PIM スタブ ルータの動作を支援するためにユニキャスト スタブ ルーティングを設定する必要があります。詳細については、EIGRPv6 スタブ ルーティング，（184 ページ）を参照してください。
- 直接接続されたマルチキャスト（MLD）レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。アクセス ドメインでは、PIM プロトコルはサポートされません。
- 冗長 PIM スタブ ルータ トポロジーはサポートされません。

IPv6 PIM ルーティングのデフォルト設定

この表は、スイッチ用の IPv6 PIM ルーティングのデフォルト設定について示しています。

表 *22* : マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル
PIM マルチキャスト境界	なし。
候補 BSR	ディセーブル
候補 RP	ディセーブル
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

IPv6 PIM スタブ ルーティングのイネーブル化

はじめる前に

PIM スタブ ルーティングは IPv6 ではデフォルトでディセーブルです。インターフェイス上で PIM スタブ ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6 multicast pim-passive-enable**
4. **interface***interface-id*
5. **ipv6 pim**
6. **ipv6 pim**{**bsr**} | {**dr-priority** | *value*} | {**hello-interval** | *seconds*} | {**join-prune-interval** | *seconds*} | {**passive**}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 multicast pim-passive-enable** 例： スイッチ(config-if)# **ipv6 multicast pim-passive-enable**	スイッチでIPv6マルチキャストPIMルーティングをイネーブルにします。
ステップ 4	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 9/0/6**	PIMスタブルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスをMLDスタティック グループに結合する必要があります。 • SVI：**interface vlan***vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN上でIP PIMスパース モードをイネーブルにして、静的に接続されたメンバーとして VLAN をMLDスタティック グループに結合し、VLAN、MLD スタティック グループ、

	コマンドまたはアクション	目的
		および物理インターフェイスで MLD スヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IPv6 アドレスを割り当てる必要があります。
ステップ 5	**ipv6 pim** 例： `スイッチ(config-if)# ipv6 pim`	インターフェイスで PIM をイネーブルにします。
ステップ 6	**ipv6 pim** {**bsr**} | {**dr-priority** | *value*} | {**hello-interval** | *seconds*} | {**join-prune-interval** | *seconds*} | {**passive**} 例： `スイッチ(config-if)# ipv6 pim bsr|dr-priority|hello-interval|join-prune-interval|passive`	インターフェイスでさまざまな PIM スタブ機能を設定します。 **bsr** を入力して PIM スイッチの BSR を設定します。 **dr-priority** を入力して、PIM スイッチの DR プライオリティを設定します。 **hello-interval** を入力して、インターフェイスの PIM hello メッセージの頻度を設定します。 **join-prune-interval** を入力して、指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。 **passive** を入力して、パッシブ モードの PIM を設定します。
ステップ 7	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

IPv6 PIM スタブ ルーティングのモニタ

表 *23* : *PIM* スタブ設定の *show* コマンド

コマンド	目的
show ipv6 pim interface スイッチ# **show ipv6 pim interface**	各インターフェイスで有効になっている PIM スタブを表示します。
show ipv6 mld groups スイッチ# **show ipv6 mld groups**	特定のマルチキャスト グループを結合した対象クライアントを表示します。
show ipv6 mroute スイッチ# **show ipv6 mroute**	ソースから対象クライアントへのマルチキャスト ストリーム転送を確認します。

BSR の設定

ここでの作業について、以下に説明します。

BSR の設定および BSR 情報の確認

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pimbsr candidate bsr***ipv6-address*[*hash-mask-length*] [**priority** *priority-value*] 例： Switch (config) # **ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10**	候補 BSR になるようにスイッチを設定します。
ステップ 3	**interface** *type number* 例： Switch (config) # **interface GigabitEthernet 1/0/1**	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 pim bsr border** 例： `Switch (config-if) # ipv6 pim bsr border`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**exit** 例： `Switch (config-if) # exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 6	**show ipv6 pim** bsr {**election** | **rp-cache** | **candidate-rp**} 例： `Switch (config-if) # show ipv6 pim bsr election`	PIM BSR プロトコル処理に関連する情報を表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BSR への PIM RP アドバタイズメントの送信

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pim bsr candidate rp***ipv6-address* [**group-list***access-list-name*] [**priority***priority-value*] [**interval** seconds] 例： `Switch(config) # ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0`	BSR に PIM RP アドバタイズメントを送信します。

	コマンドまたはアクション	目的
ステップ 3	**interface***type number* 例： `Switch(config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 pim bsr border** 例： `Switch(config-if) # ipv6 pim bsr border`	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

限定スコープ ゾーン内で BSR を使用できるようにするための設定

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pim bsr candidate rp***ipv6-address* [*hash-mask-length*] [**priority** priority-value] 例： `Switch(config) # ipv6 pim bsr candidate bsr 2001:DB8:1:1:4`	候補 BSR になるようにスイッチを設定します。
ステップ 3	**ipv6 pim bsr candidate rp***ipv6-address* [**group-list***access-list-name*] [**priority***priority-value*] [**interval** seconds] 例： `Switch(config) # ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6`	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。

	コマンドまたはアクション	目的
ステップ 4	**interface***type number* 例： `Switch(config-if) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイスコンフィギュレーション モードにします。
ステップ 5	**ipv6 multicast boundary scope***scope-value* 例： `Switch(config-if) # ipv6 multicast boundary scope 6`	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定

IPv6 BSR スイッチは、スコープと RP のマッピングを候補 RP メッセージから学習するのではなく、直接アナウンスするようにスタティックに設定できます。ユーザは、スコープと RP のマッピングをアナウンスするように BSR スイッチを設定して、BSR をサポートしていない RP がその BSR にインポートされるように設定できます。この機能をイネーブルにすると、ローカルの候補 BSR スイッチの既知のリモート RP が、企業の BSR ドメインの外部に配置されている RP を学習できるようになります。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pim bsr announced rp***ipv6-address* [**group-list***access-list-name*] [**priority***priority-value*] 例： `Switch(config)# ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0`	指定した候補 RP の BSR からスコープと RP のマッピングを直接アナウンスします。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピングの設定

SSM マッピング機能をイネーブルにすると、DNS ベースの SSM マッピングが自動的にイネーブルになります。つまり、スイッチは、マルチキャスト MLD バージョン 1 レポートの送信元を DNS サーバから検索するようになります。

スイッチ設定に応じて、DNS ベースのマッピングまたはスタティック SSM マッピングのいずれかを使用できます。スタティック SSM マッピングを使用する場合は、複数のスタティック SSM マッピングを設定できます。複数のスタティック SSM マッピングを設定すると、一致するすべてのアクセス リストの送信元アドレスが使用されるようになります。

（注） DNS ベースの SSM マッピングを使用するには、スイッチは正しく設定されている DNS サーバを少なくとも 1 つ見つける必要があります。スイッチは、その DNS サーバに直接接続される可能性があります。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mldssm-map enable** 例： `Switch(config) # ipv6 mld ssm-map enable`	設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。
ステップ 3	**no ipv6 mldssm-map query dns** 例： `Switch(config) # no ipv6 mld ssm-map query dns`	DNS ベースの SSM マッピングをディセーブルにします。
ステップ 4	**ipv6 mldssm-map static***access-listsource-address* 例： `Switch(config-if) # ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1`	スタティック SSM マッピングを設定します。
ステップ 5	**exit** 例： `Switch(config-if) # exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。

	コマンドまたはアクション	目的
ステップ 6	**show ipv6 mldssm-map** [*source-address*] 例： `Switch(config-if) # show ipv6 mld ssm-map`	SSM マッピング情報を表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スタティック mroute の設定

IPv6 のスタティック マルチキャスト ルート（mroute）は、IPv6 スタティック ルートの拡張として実装できます。スイッチを設定する際には、ユニキャスト ルーティング専用としてスタティック ルートを使用するか、マルチキャスト RPF 選択専用としてスタティック マルチキャスト ルートを使用するか、またはユニキャストルーティングとマルチキャストRPF選択の両方にスタティック ルートを使用するように設定できます。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 route** {*ipv6-prefix / prefix-length ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | *unicast* | *multicast*] [**tag***tag*] 例： `Switch (config) # ipv6 route 2001:DB8::/64 6::6 100`	スタティック IPv6 ルートを確立します。この例は、ユニキャスト ルーティングとマルチキャスト RPF 選択の両方に使用されるスタティック ルートを示しています。
ステップ 3	**exit** 例： `Switch # exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 4	**show ipv6 mroute** [link-local | [*group-name* | *group-address* [*source-address* | *source-name*]] **[summary]** [**count**]	IPv6マルチキャストルーティングテーブルの内容を表示します。

	コマンドまたはアクション	目的
	例： `Switch # show ipv6 mroute ff07::1`	
ステップ 5	**show ipv6 mroute** [**link-local** | *group-name* | *group-address*] **active** [*kbps*] 例： `Switch (config-if) # show ipv6 mroute active`	スイッチ上のアクティブなマルチキャスト ストリームを表示します。
ステップ 6	**show ipv6 rpf** [*ipv6-prefix*] 例： `Switch (config-if) # show ipv6 rpf 2001::1:1:2`	特定のユニキャスト ホスト アドレスおよびプレフィックスの RPF 情報を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 マルチキャストでの MFIB の使用

IPv6 マルチキャスト ルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。

IPv6 マルチキャストでの MFIB の動作の確認

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 mfib** [**linkscope** | **verbose** | *group-address-name* | *ipv6-prefix / prefix-length* | *source-address-name* | **count** | **interface** | **status** | **summary**] 例： `Switch # show ipv6 mfib`	IPv6 MFIB での転送エントリおよびインターフェイスを表示します。

	コマンドまたはアクション	目的
ステップ 2	**show ipv6 mfib** [all | linkscope | group-name | group-address [source-name | source-address]] **count** 例： `Switch # show ipv6 mfib ff07::1`	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 3	**show ipv6 mfib interface** 例： `Switch # show ipv6 mfib interface`	IPv6 マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示します。
ステップ 4	**show ipv6 mfib status** 例： `Switch # show ipv6 mfib status`	一般的な MFIB 設定と動作ステータスを表示します。
ステップ 5	**show ipv6 mfibsummary** 例： `Switch # show ipv6 mfib summary`	IPv6 MFIB エントリおよびインターフェイスの数に関するサマリー情報を表示します。
ステップ 6	**debug ipv6 mfib** [*group-name* | *group-address*] [**adjacency** | **db** | **fs** | **init** | **interface** | **mrib** [**detail**] | **nat** | **pak** | **platform** | **ppr** | **ps** | **signal** | **table**] 例： `Switch # debug ipv6 mfib FF04::10 pak`	IPv6 MFIB に対するデバッグ出力をイネーブルにします。

MFIB トラフィック カウンタのリセット

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mfibcounters** [*group-name* | **group-address** [*source-address* | *source-name*]] 例： `Switch # clear ipv6 mfib counters FF04::10`	アクティブなすべての MFIB トラフィック カウンタをリセットします。

第 14 章

IPv6 クライアント IP アドレス ラーニングの設定

- IPv6 クライアント アドレス ラーニングの前提条件，250 ページ
- IPv6 クライアント アドレス ラーニングについて，250 ページ
- IPv6 ユニキャストの設定（CLI），256 ページ
- RA ガード ポリシーの設定（CLI），257 ページ
- RA ガード ポリシーの適用（CLI），258 ページ
- RA スロットル ポリシーの設定（CLI），259 ページ
- VLAN への RA スロットル ポリシーの適用（CLI），260 ページ
- IPv6 スヌーピングの設定（CLI），261 ページ
- IPv6 ND 抑制ポリシーの設定（CLI），262 ページ
- VLAN/PortChannel での IPv6 スヌーピングの設定，263 ページ
- Switch での IPv6 の設定（CLI），265 ページ
- DHCP プールの設定（CLI），266 ページ
- DHCP を使用しないステートレス自動アドレス設定の設定（CLI），267 ページ
- DHCP によるステートレス自動アドレス設定の設定（CLI），268 ページ
- ステートフル DHCP のローカルな設定（CLI），269 ページ
- ステートフル DHCP の外部的設定（CLI），272 ページ
- IPv6 アドレス ラーニング設定の確認，274 ページ
- その他の参考資料，275 ページ
- IPv6 クライアント アドレス ラーニングの機能情報，276 ページ

IPv6 クライアント アドレス ラーニングの前提条件

IPv6 クライアント アドレス ラーニングを設定する前に、IPv6 をサポートするようにワイヤレス クライアントを設定します。

関連トピック

RA ガード ポリシーの設定（CLI），（257 ページ）

IPv6 クライアント アドレス ラーニングについて

クライアントアドレスラーニングは、アソシエーション、再アソシエーション、非認証、タイムアウト時に、ワイヤレス クライアントの IPv4 および IPv6 アドレス、スイッチによって維持されるクライアント遷移ステートについて学習するために、スイッチで設定されます。

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定（SLACC）
- ステートフル DHCPv6
- 静的設定

これらの方法のいずれの場合も、IPv6 クライアントは常にネイバー送信要求 DAD（重複アドレス検出）要求を送信して、ネットワークに重複する IP アドレスがないようにします。スイッチはクライアントの NDP および DHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習します。

SLAAC アドレス割り当て

IPv6 クライアント アドレス割り当て用の最も一般的な方法は、ステートレス アドレス自動設定（SLAAC）です。SLAAC はクライアントが IPv6 プレフィクスに基づいてアドレスを自己割り当てするシンプルなプラグ アンド プレイ接続を提供します。このプロセスが実現しました。

次のように、ステートレス アドレス自動設定（SLAAC）は設定されています。

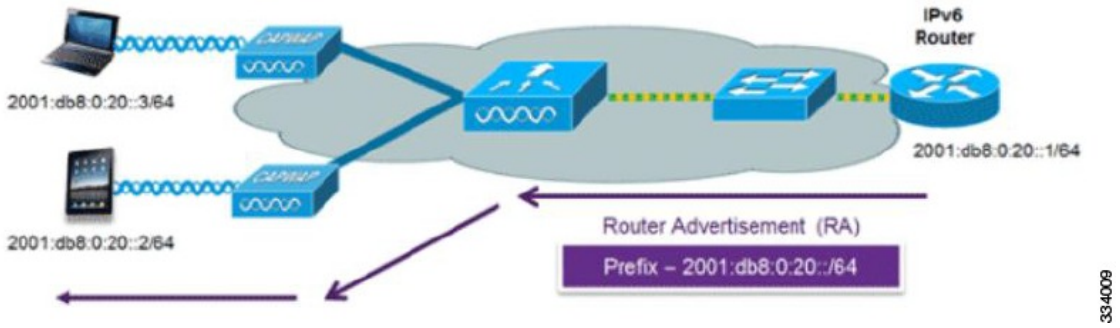
- ホストは、ルータ送信要求メッセージを送信します。
- ホストは、ルータ アドバタイズメント メッセージを待機します。
- ホストは、ルータ アドバタイズメント メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、これを 64 ビット EUI-64 アドレス（イーサネットの場合、MAC アドレスから作成されます）と組み合わせて、グローバル ユニキャスト メッセージを作成します。ホストは、デフォルト ゲートウェイとして、ルータ アドバタイズメント メッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 重複アドレス検出は、選択されるランダム アドレスが他のクライアントと重複しないように、IPv6 クライアントによって実行されます。

- アルゴリズムの選択はクライアントに依存し、多くの場合は設定できます。

次の 2 種類のアルゴリズムに基づいて IPv6 アドレスの最後の 64 ビットが学習可能です。

- インターフェイスの MAC アドレスに基づく EUI-64、または
- ランダムに生成されるプライベート アドレス。

図 *8*：*SLAAC* アドレス割り当て



Cisco 対応 IPv6 ルータからの次の Cisco IOS コンフィギュレーション コマンドを使用して、SLAAC のアドレッシングとルータ アドバタイズメントをイネーブルにします。

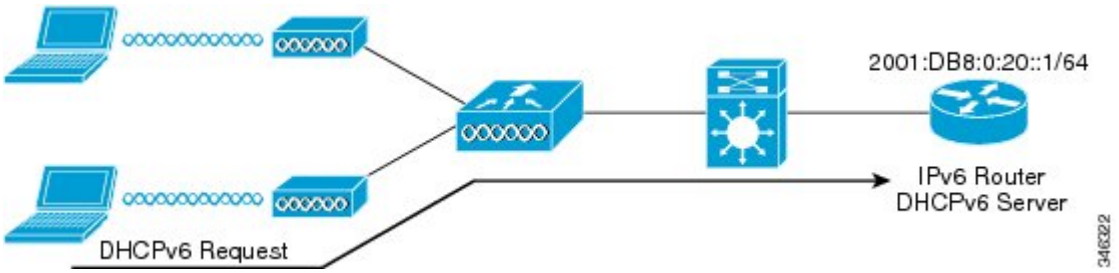
```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

関連トピック

IPv6 スヌーピングの設定（CLI），（261 ページ）
DHCP プールの設定（CLI），（266 ページ）
DHCP を使用しないステートレス自動アドレス設定の設定（CLI），（267 ページ）
DHCP によるステートレス自動アドレス設定の設定（CLI），（268 ページ）
ステートフル DHCP のローカルな設定（CLI），（269 ページ）
ステートフル DHCP の外部的設定（CLI），（272 ページ）

ステートフル DHCPv6 アドレス割り当て

図 *9*：ステートフル *DHCPv6* アドレス割り当て



DHCPv6の使用は、SLAACがすでに導入されている場合は、IPv6クライアント接続で要求されません。DHCPv6 にはステートレスおよびステートフルという 2 種類の動作モードがあります。

DHCPv6 ステートレス モードは、ルータ アドバタイズメントで使用できない追加のネットワーク情報をクライアントに提供するために使用しますが、これはIPv6アドレスではありません。すでにSLAACによって提供されているためです。この情報にはDNS ドメイン名、DNS サーバ、その他の DHCP ベンダー固有オプションを含めることができます。このインターフェイス設定は、SLAAC をイネーブルにしてステートレス DHCPv6 を実装する Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

マネージドモードとも呼ばれるDHCPv6ステートフル オプションは、DHCPv4と同様に動作します。つまり、クライアント SLAAC のとおりにアドレスの最後の 64 ビットを生成するのではなく、固有のアドレスをそれぞれのクライアントに割り当てます。次のインターフェイス設定は、ローカル スイッチのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
end
```

次のインターフェイス設定は、外部 DHCP サーバのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
domain-name cisco.com
```

```
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp_relay destination 2001:DB8:0:20::2
end
```

関連トピック

IPv6 スヌーピングの設定（CLI），（261 ページ）
DHCP プールの設定（CLI），（266 ページ）
DHCP を使用しないステートレス自動アドレス設定の設定（CLI），（267 ページ）
DHCP によるステートレス自動アドレス設定の設定（CLI），（268 ページ）
ステートフル DHCP のローカルな設定（CLI），（269 ページ）
ステートフル DHCP の外部的設定（CLI），（272 ページ）

静的 IP アドレス割り当て

クライアントにスタティックに設定されたアドレス。

ルータ要求

ルータ送信要求メッセージは、ローカル ルーティングに関する情報を入手できる、またはステートレス自動設定を設定できるルータ アドバタイズメントを送信するようにローカル ルータを促進するために、ホスト コントローラによって発行されます。ルータ アドバタイズメントは定期的に送信され、起動時または再起動操作後などに、ホストはルータ送信要求を使用して即時ルータ アドバタイズメントを要求します。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI），（262 ページ）

Router Advertisement

ルータ アドバタイズメント メッセージは、ルータから定期的に送信されるか、ホストからのルータ送信要求メッセージへの応答として送信されます。これらのメッセージに含まれる情報は、ホストでステートレス自動設定を実行し、ルーティング テーブルを変更するために使用されます。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI），（262 ページ）

ネイバー探索

IPv6 ネイバー ディスカバリとは、近隣のノード間の関係を決定するメッセージとプロセスのことです。ネイバー ディスカバリは、IPv4 で使用されていた ARP、ICMP ルータ探索、および ICMP リダイレクトに代わるものです。

信頼できるバインディング テーブル データベースを構築するために、IPv6 ネイバー ディスカバリ検査によってネイバー ディスカバリ メッセージが分析され、準拠しない IPv6 ネイバー ディスカバリ パケットはドロップされます。 スイッチ内のネイバー バインディング テーブルでは、各 IPv6 アドレスと、アソシエートされた MAC アドレスが追跡されます。クライアントは、ネイバー バインディング タイマーに従って、テーブルから消去されます。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI），（262 ページ）

ネイバー探索抑制

ワイヤレス クライアントの IPv6 アドレスは、スイッチによってキャッシュされます。スイッチが IPv6 アドレスを検索する NS マルチキャストを受信して、スイッチによって特定された目的のアドレスがクライアントのいずれかに属している場合、スイッチはクライアントに代わって NA メッセージで応答します。このプロセスによって IPv4 のアドレス解決プロトコル（ARP）テーブルと同等のテーブルが生成されますが、より効率的であり、たいていの場合、使用されるメッセージは少なくなります。

（注） スイッチがプロキシのように動作し NA で応答するのは、**ipv6 nd suppress** コマンドが設定されている場合だけです。

スイッチにワイヤレス クライアントの IPv6 アドレスがない場合、スイッチは NA で応答せず、NS パケットをワイヤレス側に転送します。この問題を解決するために、NS マルチキャスト フォワーディング ノブが用意されています。このノブがイネーブルの場合、スイッチは存在しない（キャッシュ欠落）IPv6 アドレスの NS パケットを取得し、ワイヤレス側に転送します。このパケットは、目的のワイヤレス クライアントに到達し、クライアントは NA で応答します。

このキャッシュ ミス シナリオが発生するのはまれで、完全な IPv6 スタックが実装されていないクライアントが、NDP 時にそれらの IPv6 アドレスをアドバタイズしない可能性はほとんどありません。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI），（262 ページ）

RA Guard

IPv6 クライアントは、IPv6 アドレスを設定し、IPv6 ルータ アドバタイズメント（RA）パケットに基づいてルータ テーブルにデータを入力します。RA ガード機能は、有線ネットワークの RA

ガード機能に類似しています。RA ガードは、ワイヤレス クライアントから発信される不要な、または不正な RA パケットをドロップすることによって、IPv6 ネットワークのセキュリティを強化します。この機能が設定されていないと、悪意のある IPv6 ワイヤレス クライアントが、多くの場合は高い優先順位で、それ自体をネットワークのルータとして通知する可能性があり、そのため、正規の IPv6 ルータよりも優先されることになります。

また、RA ガードは、着信 RA を調べて、メッセージまたはスイッチ設定で検出された情報のみに基づいて、それらをスイッチするかブロックするかを決定します。受信したフレームで使用できる情報は、RA の検証に有用です。

- フレームが受信されるポート
- IPv6 送信元アドレス
- プレフィックス リスト

スイッチで作成された次の設定情報は、受信した RA フレームで検出された情報に対して検証するときに RA ガードで使用できます。

- RA ガード メッセージの受信用に信頼できる/信頼できないポート
- RA 送信者の信頼できる/信頼できない送信元 IPv6 アドレス
- 信頼できる/信頼できないプレフィックス リストおよびプレフィックス範囲
- ルータ プリファレンス

RA ガードはスイッチで行われます。スイッチで RA メッセージをドロップするようにスイッチを設定できます。すべての IPv6 RA メッセージがドロップされ、それによって他のワイヤレス クライアントおよびアップストリーム有線ネットワークが悪意のある IPv6 クライアントから保護されます。

```
//Create a policy for RA Guard//
ipv6 nd raguard policy raguard-router
trusted-port
device-role router
//Applying the RA Guard Policy on port/interface//
interface tengigabitethernet1/0/1 (Katana)
interface gigabitethernet1/0/1 (Edison)

ipv6 nd raguard attach-policy raguard-router
```

関連トピック

RA ガード ポリシーの設定（CLI），（257 ページ）

RA ガード ポリシーの適用（CLI），（258 ページ）

RA スロットル ポリシーの設定（CLI），（259 ページ）

VLAN への RA スロットル ポリシーの適用（CLI），（260 ページ）

RA スロットリング

RA スロットリングは、コントローラがワイヤレス ネットワーク宛ての RA パケットを強制的に制限できるようにします。RA スロットリングを有効にすることにより、多数の RA パケットを送

信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。クライアントが RS パケットを送信すると、RA がクライアントに返送されます。この RA は、コントローラを通過でき、クライアントにユニキャストされます。このプロセスによって、新しいクライアントやローミング クライアントが RA スロットリングの影響を受けないようにすることができます。

関連トピック

RA ガード ポリシーの設定（CLI），（257 ページ）
RA ガード ポリシーの適用（CLI），（258 ページ）
RA スロットル ポリシーの設定（CLI），（259 ページ）
VLAN への RA スロットル ポリシーの適用（CLI），（260 ページ）

IPv6 ユニキャストの設定（CLI）

IPv6 ユニキャストはスイッチとコントローラで常にイネーブルにする必要があります。IPv6 ユニキャスト ルーティングはディセーブルに設定されています。

はじめる前に

IPv6 ユニキャスト データグラムの転送をイネーブルにするには、グローバル コンフィギュレーション モードで **ipv6 unicast-routing** コマンドを使用します。IPv6 ユニキャスト データグラムの転送をディセーブルにするには、このコマンドの **no** 形式を使用します。

手順の概要

1. **configureterminal**
2. **ipv6unicast routing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6unicast routing** 例： `スイッチ (config)# ipv6 unicast routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

RA ガード ポリシーの設定（CLI）

IPv6 クライアント アドレスを追加し、IPv6 ルータ アドバタイズメント パケットに基づいてルータ テーブルに入力するには、スイッチで RA ガード ポリシーを設定します。

はじめる前に

手順の概要

1. **configureterminal**
2. **ipv6nd raguardpolicy**raguard-router
3. **trustedport**
4. **device-rolerouter**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6nd raguardpolicy**raguard-router 例： `スイッチ(config)# ipv6 nd raguard policy raguard-router`	RA ガードポリシー名を定義して、RA ガードポリシー コンフィギュレーション モードを開始します。
ステップ 3	**trustedport** 例： `スイッチ(config-ra-guard)# trustedport`	（任意）このポリシーが信頼できるポートに適用されることを指定します。
ステップ 4	**device-rolerouter** 例： `スイッチ(config-ra-guard)# device-role router`	ポートに接続されているデバイスのロールを指定します。
ステップ 5	**exit** 例： `スイッチ(config-ra-guard)# exit`	RA ガード ポリシー コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。

関連トピック

IPv6 クライアント アドレス ラーニングの前提条件，（250 ページ）
RA Guard，（254 ページ）
RA スロットリング，（255 ページ）
RA ガード ポリシーの適用（CLI），（258 ページ）
RA スロットル ポリシーの設定（CLI），（259 ページ）
VLAN への RA スロットル ポリシーの適用（CLI），（260 ページ）

RA ガード ポリシーの適用（CLI）

スイッチで RA ガード ポリシーを適用すると、すべての信頼できない RA がブロックされます。

はじめる前に

手順の概要

1. **configureterminal**
2. **interfacetengigabitethernet**1/0/1
3. **ipv6ndraguardattach-policy**raguard-router
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interfacetengigabitethernet**1/0/1 例： `スイッチ (config)# interface tengigabitethernet 1/0/1`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 3	**ipv6ndraguardattach-policy**raguard-router 例： `スイッチ(config-if)# ipv6 nd raguard attach-policy raguard-router`	指定したインターフェイスに IPv6 RA ガード機能を適用します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： スイッチ(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。

関連トピック

RA ガード ポリシーの設定（CLI），（257 ページ）
RA Guard，（254 ページ）
RA スロットリング，（255 ページ）
RA スロットル ポリシーの設定（CLI），（259 ページ）
VLAN への RA スロットル ポリシーの適用（CLI），（260 ページ）

RA スロットル ポリシーの設定（CLI）

強制的に制限できるように RA スロットル ポリシーを設定します。

はじめる前に

手順の概要

1. **configureterminal**
2. **ipv6 ndra-throttler policy**ra-throttler1
3. **throttleperiod**500
4. **max-through**10
5. **allow-atleast**5**at-most**10

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ipv6 ndra-throttler policy**ra-throttler1 例： `スイッチ(config)# ipv6 nd ra-throttler policy ra-throttler1`	ルータ アドバタイズメント（RA）スロットラ ポリシー名を定義して、IPv6 RA スロットル ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**throttleperiod**500 例： `スイッチ(config-nd-ra-throttle)# throttleperiod 500`	IPv6 RA スロットラ ポリシーのスロットル期間を設定します。
ステップ 4	**max-through**10 例： `スイッチ(config-nd-ra-throttle)# max-through 500`	スロットル期間ごとに、VLAN あたりのマルチキャスト RA を制限します。
ステップ 5	**allow-atleast5at-most**10 例： `スイッチ(config-nd-ra-throttle)# allow-atleast 5 at-most 10`	RA スロットラ ポリシーのスロットル期間ごとに、デバイスあたりのマルチキャスト RA 数を制限します。

関連トピック

RA ガード ポリシーの設定（CLI），（257 ページ）
RA ガード ポリシーの適用（CLI），（258 ページ）
RA Guard，（254 ページ）
RA スロットリング，（255 ページ）
VLAN への RA スロットル ポリシーの適用（CLI），（260 ページ）

VLAN への RA スロットル ポリシーの適用（CLI）

VLAN に RA スロットル ポリシーを適用します。RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。

はじめる前に

手順の概要

1. **configureterminal**
2. **vlanconfiguration**1
3. **ipv6ndrathrottlerattach-policy**ra-throttler1

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlanconfiguration**1 例： スイッチ(config)# vlan configuration 1	VLAN または VLAN の集合を設定して、VLAN コンフィギュレーション モードを開始します。
ステップ 3	**ipv6ndrathrottlerattach-policy**ra-throttler1 例： スイッチ(config-vlan)# ipv6 nd ra throttler attach-policy ra-throttler1	VLAN または VLAN の集合に IPv6 RA スロットル ポリシーを接続します。

関連トピック

RA ガード ポリシーの設定（CLI），（257 ページ）
RA ガード ポリシーの適用（CLI），（258 ページ）
RA スロットル ポリシーの設定（CLI），（259 ページ）
RA Guard，（254 ページ）
RA スロットリング，（255 ページ）

IPv6 スヌーピングの設定（CLI）

IPv6 スヌーピングはスイッチとコントローラで常にイネーブルにする必要があります。

はじめる前に

クライアント マシンで IPv6 をイネーブルにします。

手順の概要

1. **vlan configuration 1**
2. **ipv6 snooping**
3. **ipv6 nd suppress**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vlan configuration 1** 例： `スイッチ(config)# vlan configuration 1`	VLAN コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 snooping** 例： `スイッチ(config-vlan)# ipv6 snooping`	Vlan で IPv6 スヌーピングをイネーブルにします。
ステップ 3	**ipv6 nd suppress** 例： `スイッチ(config-vlan-config)# ipv6 nd suppress`	Vlan で IPv6 ND 抑制をイネーブルにします。
ステップ 4	**exit** 例： `スイッチ(config-vlan-config)# exit`	設定を保存し、Vlan コンフィギュレーション モードを終了します。

関連トピック

SLAAC アドレス割り当て，（250 ページ）
ステートフル DHCPv6 アドレス割り当て，（252 ページ）

IPv6 ND 抑制ポリシーの設定（CLI）

IPv6 ネイバー探索（ND）マルチキャスト抑制機能では、ドロップする（およびターゲットに代わって送信要求に応答する）、またはユニキャスト トラフィックに変換することで、できるだけ多くの ND マルチキャスト ネイバー送信要求（NS）メッセージを停止します。この機能は、レイヤ 2 スイッチまたはワイヤレス コントローラで実行され、適切なリンクの処理に必要な制御トラフィックの量を減らすために使用されます。

アドレスがバインディングテーブルに挿入されると、マルチキャストアドレスに送信されたアドレス解決要求が代行受信され、デバイスはアドレスの所有者に代わって応答するか、レイヤ 2 で要求をユニキャスト メッセージに変換して宛先に転送します。

はじめる前に

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6ndsuppresspolicy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ(config)# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6ndsuppresspolicy** 例： `スイッチ (config)# ipv6 nd suppress policy`	ND 制御ポリシー名を定義して ND 制御ポリシー コンフィギュレーション モードを開始します。

関連トピック

ルータ要求, （253 ページ）
Router Advertisement, （253 ページ）
ネイバー探索, （254 ページ）
ネイバー探索抑制, （254 ページ）

VLAN/PortChannel での IPv6 スヌーピングの設定

ネイバー探索（ND）抑制は、VLAN またはスイッチ ポートでイネーブルまたはディセーブルにできます。

はじめる前に

手順の概要

1. **vlanconfig901**
2. **ipv6ndsuppress**
3. **end**
4. **interfacegi1/0/1**
5. **ipv6ndsuppress**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vlanconfig901** 例： `スイッチ(config)# vlan config901`	VLAN を作成し、VLAN コンフィギュレーション モードを開始します。
ステップ 2	**ipv6ndsuppress** 例： `スイッチ(config-vlan)# ipv6 nd suppress`	VLAN に IPv6 nd 抑制を適用します。
ステップ 3	**end** 例： `スイッチ(config-vlan)# end`	VLAN コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 4	**interfacegi1/0/1** 例： `スイッチ (config)# interface gi1/0/1`	ギガビット イーサネット ポート インターフェイスを作成します。
ステップ 5	**ipv6ndsuppress** 例： `スイッチ(config-vlan)# ipv6 nd suppress`	インターフェイスに IPv6 nd 抑制を適用します。
ステップ 6	**end** 例： `スイッチ(config-vlan)# end`	VLAN コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

Switch での IPv6 の設定（CLI）

インターフェイス上の IPv6 を設定するには、この設定例を使用します。

はじめる前に

クライアント上の IPv6 および有線インフラストラクチャ上の IPv6 サポートをイネーブルにします。

手順の概要

1. **interfacevlan**1
2. **ipaddress**fe80::1 link-local
3. **ipv6enable**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfacevlan**1 例： `スイッチ(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ipaddress**fe80::1 link-local
	
	例：
	`スイッチ(config-if)# ip address 198.51.100.1 255.255.255.0`
	`スイッチ(config-if)# ipv6 address fe80::1 link-local`
	`スイッチ(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`スイッチ(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 3	**ipv6enable** 例： `スイッチ(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。
ステップ 4	**end** 例： `スイッチ(config)# end`	インターフェイス モードを終了します。

DHCP プールの設定（CLI）

手順の概要

1. **ipv6dhcppool**Vlan21
2. **addressprefix**2001:DB8:0:1:FFFF:1234::/64**lifetime**30010
3. **dns-server**2001:100:0:1::1
4. **domain-name**example.com
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6dhcppool**Vlan21 例： `スイッチ(config)# ipv6 dhcp pool vlan1`	コンフィギュレーション モードを開始し、VLAN の IPv6 DHCP プールを設定します。
ステップ 2	**addressprefix**2001:DB8:0:1:FFFF:1234::/64**lifetime**30010 例： `スイッチ(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10`	コンフィギュレーション DHCP モードを開始し、VLAN のアドレス プールとそのライフタイムを設定します。
ステップ 3	**dns-server**2001:100:0:1::1 例： `スイッチ(config-dhcpv6)# dns-server 2001:20:21::1`	DHCP プールの DNS サーバを設定します。
ステップ 4	**domain-name**example.com 例： `スイッチ(config-dhcpv6)# domain-name example.com`	完全な非修飾ホスト名になるようにドメイン名を設定します。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコンフィギュレーション モードを終了できます。

関連トピック

SLAAC アドレス割り当て，（250 ページ）
ステートフル DHCPv6 アドレス割り当て，（252 ページ）

DHCP を使用しないステートレス自動アドレス設定の設定（CLI）

手順の概要

1. **interfacevlan**1
2. **ipaddress**fe80::1 link-local
3. **ipv6enable**
4. **no ipv6 nd managed-config-flag**
5. **no ipv6 nd other-config-flag**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfacevlan**1 例： `スイッチ(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ipaddress**fe80::1 link-local
	
	例：
	`スイッチ(config-if)# ip address 198.51.100.1 255.255.255.0`
	`スイッチ(config-if)# ipv6 address fe80::1 link-local`
	`スイッチ(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`スイッチ(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 3	**ipv6enable** 例： `スイッチ(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

ステップ 4	**no ipv6 nd managed-config-flag**
	
	例：
	`スイッチ(config)#interface vlan 1`
	`スイッチ(config-if)# no ipv6 nd managed-config-flag`
		接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。

ステップ 5	**no ipv6 nd other-config-flag** 例： `スイッチ(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

SLAAC アドレス割り当て，（250 ページ）
ステートフル DHCPv6 アドレス割り当て，（252 ページ）

DHCP によるステートレス自動アドレス設定の設定（CLI）

手順の概要

1. **interfacevlan**1
2. **ipaddress**fe80::1 link-local
3. **ipv6enable**
4. **no ipv6 nd managed-config-flag**
5. **ipv6 nd other-config-flag**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfacevlan**1 例： スイッチ(config)# interface vlan 1	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	**ipaddress**fe80::1 link-local 例： スイッチ(config-if)# ip address 198.51.100.1 255.255.255.0 スイッチ(config-if)# ipv6 address fe80::1 link-local スイッチ(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64 スイッチ(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64	リンクローカルオプションを使用してインターフェイスで IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6enable** 例： スイッチ(config)# ipv6 enable	（任意）インターフェイス上で IPv6 をイネーブルにします。
ステップ 4	**no ipv6 nd managed-config-flag** 例： スイッチ(config)#interface vlan 1 スイッチ(config-if)# no ipv6 nd managed-config-flag	接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。
ステップ 5	**ipv6 nd other-config-flag** 例： スイッチ(config-if)# no ipv6 nd other-config-flag	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 6	**end** 例： スイッチ(config)# end	インターフェイス モードを終了します。

関連トピック

SLAAC アドレス割り当て，（250 ページ）
ステートフル DHCPv6 アドレス割り当て，（252 ページ）

ステートフル DHCP のローカルな設定（CLI）

このインターフェイス設定は、ローカルスイッチのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

はじめる前に

手順の概要

1. **configureterminal**
2. **ipv6unicast-routing**
3. **ipv6dhcppool**IPv6_DHCPPOOL
4. **addressprefix**2001:DB8:0:1:FFFF:1234::/64
5. **dns-server**2001:100:0:1::1
6. **domain-name**example.com
7. **exit**
8. **interface**vlan1
9. **descriptionIPv6-DHCP-Stateful**
10. **ipv6address**2001:DB8:0:20::1/64
11. **ipaddress**192.168.20.1255.255.255.0
12. **ipv6ndprefix**2001:db8::/64**no-advertise**
13. **ipv6ndmanaged-config-flag**
14. **ipv6ndother-config-flag**
15. **ipv6dhcpserver**IPv6_DHCPPOOL

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6unicast-routing** 例： `スイッチ(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 を設定します。
ステップ 3	**ipv6dhcppool**IPv6_DHCPPOOL 例： `スイッチ (config)# ipv6 dhcp pool IPv6_DHCPPOOL`	コンフィギュレーションモードを開始し、VLAN の IPv6 DHCP プールを設定します。
ステップ 4	**addressprefix**2001:DB8:0:1:FFFF:1234::/64 例： `スイッチ (config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64`	プールに入力するアドレス範囲を指定します。

	コマンドまたはアクション	目的
ステップ 5	**dns-server**2001:100:0:1::1 例： スイッチ (config-dhcpv6)# dns-server 2001:100:0:1::1	DHCP クライアントに DNS サーバのオプションを提供します。
ステップ 6	**domain-name**example.com 例： スイッチ (config-dhcpv6)# domain-name example.com	DHCP クライアントにドメイン名オプションを提供します。
ステップ 7	**exit** 例： スイッチ (config-dhcpv6)# exit	前のモードに戻ります。
ステップ 8	**interface**vlan1 例： スイッチ (config)# interface vlan 1	インターフェイス モードを開始して、ステートフル DHCP を設定します。
ステップ 9	**descriptionIPv6-DHCP-Stateful** 例： スイッチ (config-if)# description IPv6-DHCP-Stateful	ステートフル IPv6 DHCP の説明を入力します。
ステップ 10	**ipv6address**2001:DB8:0:20::1/64 例： スイッチ (config-if)# ipv6 address 2001:DB8:0:20::1/64	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 11	**ipaddress**192.168.20.1255.255.255.0 例： スイッチ (config-if)# ip address 192.168.20.1 255.255.255.0	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 12	**ipv6ndprefix**2001:db8::/64**no-advertise** 例： スイッチ (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise	アドバタイズしてはならない、IPv6 ルーティング プレフィックス アドバタイズメントを設定します。
ステップ 13	**ipv6ndmanaged-config-flag** 例： スイッチ (config-if)# ipv6 nd managed-config-flag	ホストでアドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。

	コマンドまたはアクション	目的
ステップ 14	**ipv6ndother-config-flag** 例： `スイッチ (config-if)# ipv6 nd other-config-flag`	ホストで非アドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 15	**ipv6dhcpserver**IPv6_DHCPPOOL 例： `スイッチ (config-if)# ipv6 dhcp server IPv6_DHCPPOOL`	インターフェイスにDHCPサーバを設定します。

関連トピック

SLAAC アドレス割り当て，（250 ページ）
ステートフル DHCPv6 アドレス割り当て，（252 ページ）

ステートフル DHCP の外部的設定（CLI）

このインターフェイス設定は、外部 DHCP サーバのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

はじめる前に

手順の概要

1. **configureterminal**
2. **ipv6unicast-routing**
3. **dns-server**2001:100:0:1::1
4. **domain-name**example.com
5. **exit**
6. **interface**vlan1
7. **descriptionIPv6-DHCP-Stateful**
8. **ipv6address**2001:DB8:0:20::1/64
9. **ipaddress**192.168.20.1255.255.255.0
10. **ipv6ndprefix**2001:db8::/64**no-advertise**
11. **ipv6ndmanaged-config-flag**
12. **ipv6ndother-config-flag**
13. **ipv6dhcp_relaydestination**2001:DB8:0:20::2

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6unicast-routing** 例： スイッチ(config)# ipv6 unicast-routing	ユニキャスト用に IPv6 を設定します。
ステップ 3	**dns-server**2001:100:0:1::1 例： スイッチ (config-dhcpv6)# dns-server 2001:100:0:1::1	DHCP クライアントに DNS サーバのオプションを提供します。
ステップ 4	**domain-name**example.com 例： スイッチ (config-dhcpv6)# domain-name example.com	DHCP クライアントにドメイン名オプションを提供します。
ステップ 5	**exit** 例： スイッチ (config-dhcpv6)# exit	前のモードに戻ります。
ステップ 6	**interface**vlan1 例： スイッチ (config)# interface vlan 1	インターフェイス モードを開始して、ステートフル DHCP を設定します。
ステップ 7	**descriptionIPv6-DHCP-Stateful** 例： スイッチ (config-if)# description IPv6-DHCP-Stateful	ステートフル IPv6 DHCP の説明を入力します。
ステップ 8	**ipv6address**2001:DB8:0:20::1/64 例： スイッチ (config-if)# ipv6 address 2001:DB8:0:20::1/64	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 9	**ipaddress**192.168.20.1255.255.255.0 例： スイッチ (config-if)# ip address 192.168.20.1 255.255.255.0	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。

	コマンドまたはアクション	目的
ステップ 10	**ipv6ndprefix**2001:db8::/64**no-advertise** 例： `スイッチ (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	アドバタイズしてはならない、IPv6 ルーティング プレフィックス アドバタイズメントを設定します。
ステップ 11	**ipv6ndmanaged-config-flag** 例： `スイッチ (config-if)# ipv6 nd managed-config-flag`	ホストでアドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 12	**ipv6ndother-config-flag** 例： `スイッチ (config-if)# ipv6 nd other-config-flag`	ホストで非アドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 13	**ipv6dhcp_relaydestination**2001:DB8:0:20::2 例： `スイッチ (config-if)# ipv6 dhcp_relay destination 2001:DB8:0:20::2`	インターフェイスにDHCPサーバを設定します。

関連トピック

SLAAC アドレス割り当て，（250 ページ）
ステートフル DHCPv6 アドレス割り当て，（252 ページ）

IPv6 アドレス ラーニング設定の確認

次に、**show ipv6 dhcp pool** コマンドの出力例を示します。このコマンドは、スイッチ上の IPv6 サービス設定を表示します。vlan 21 の設定済みプールの詳細には、プールからアドレスを現在使用している 6 つのクライアントが表示されます。

手順の概要

1. **show ipv6 dhcp pool**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 dhcp pool** 例： スイッチshow ipv6 dhcp pool DHCPv6 pool: vlan21 Address allocation prefix: 2001:DB8:0:1:FFFF:1234::/64 valid 86400 preferred 86400 (6 in use, 0 conflicts) DNS server: 2001:100:0:1::1 Domain name: example.com Active clients: 6	スイッチ上のIPv6サービス設定を表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 Command Reference (Catalyst 3650 Switches)*
IP コマンド リファレンス	*IP Command Reference (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

IPv6 クライアント アドレス ラーニングの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 クライアント アドレス ラーニング機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 15 章

IPv6 WLAN セキュリティの設定

- IPv6 WLAN セキュリティの前提条件，277 ページ
- IPv6 WLAN セキュリティの制限，277 ページ
- IPv6 WLAN セキュリティについて，278 ページ
- IPv6 WLAN セキュリティの設定方法，281 ページ
- その他の参考資料，300 ページ
- IPv6 WLAN セキュリティの機能情報，301 ページ

IPv6 WLAN セキュリティの前提条件

クライアント VLAN をスイッチで設定された WLAN にマッピングする必要があります。

IPv6 WLAN セキュリティの制限

RADIUS サーバのサポート

- 冗長性を保つために複数の RADIUS サーバが設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバでユーザ データベースを同一にする必要があります。

Radius ACS サポート

- Cisco Secure Access Control Server（ACS）とスイッチの両方で、RADIUS を設定する必要があります。
- RADIUS は、Cisco Secure ACS バージョン 3.2 以降のリリースでサポートされます。

IPv6 WLAN セキュリティについて

RADIUS の概要

Remote Authentication Dial-In User Service（RADIUS）とは、ネットワークへの管理アクセス権を取得しようとするユーザに対して中央管理されたセキュリティ機能を提供する、クライアント/サーバプロトコルです。これは、ローカルEAPに類似したバックエンドデータベースとして機能し、認証サービスおよびアカウンティング サービスを提供します。

- 認証：スイッチにログインしようとするユーザを検証するプロセス。

  スイッチで RADIUS サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。複数のデータベースを設定する場合は、バックエンド データベースを試行する順序を指定します。

- アカウンティング：ユーザによる処理と変更を記録するプロセス。

  ユーザによる処理が正常に実行される度に、RADIUSアカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。RADIUSアカウンティング サーバが到達不能の場合、ユーザは中断なく、セッションを続行できます。

ユーザ データグラム プロトコル：RADIUS では、その転送にユーザ データグラム プロトコル（UDP）を使用します。RADIUS では、1 つのデータベースが保持されます。そして、UDP ポート 1812 で受信認証要求がリッスンされ、UDP ポート 1813 で受信アカウンティング要求がリッスンされます。アクセス コントロールを要求するスイッチは、クライアントとして動作し、サーバからAAAサービスを要求します。スイッチとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

複数の RADIUS アカウンティングおよび認証サーバを設定します。たとえば、1 台の RADIUS 認証サーバを中央に配置し、複数の RADIUS アカウンティング サーバを異なる地域に配置できます。同じタイプのサーバを複数設定すると、最初のサーバで障害が発生したり、接続不能になったりしても、コントローラは、必要に応じて 2 台目や 3 台目あるいはそれ以降のサーバへの接続を自動的に試行します。

RADIUS 方式が WLAN に対して設定されている場合、スイッチは WLAN に対して設定されている RADIUS 方式を使用します。ローカル EAP を使用するように WLAN を設定すると、WLAN で設定されているRADIUS方式はローカルをポイントします。WLANには、使用するローカルEAPプロファイルの名前を設定する必要もあります。

RADIUS 方式が WLAN に対して設定されていない場合、スイッチはグローバル モードで定義されているデフォルトの RADIUS 方式を使用します。

ローカル EAP について

ローカルEAPは、ユーザおよびワイヤレスクライアントのローカル認証を可能にする認証方式です。この方式は、バックエンド システムが妨害されたり、外部認証サーバが停止した場合でも、ワイヤレスクライアントへの接続を維持できるように、リモートオフィスで使用する目的で設計

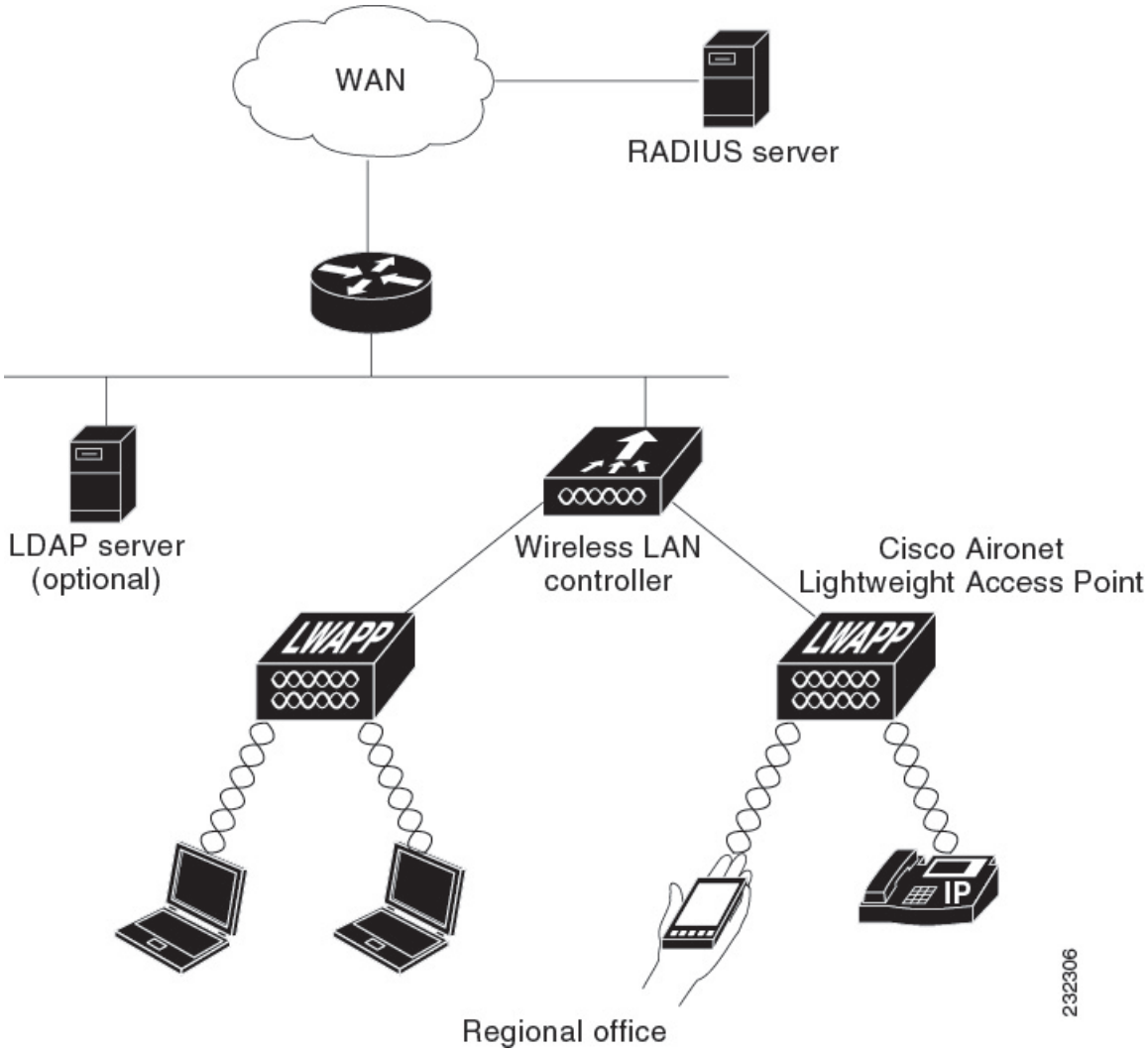
されています。ローカルEAPを有効にすると、スイッチは認証サーバおよびローカルユーザデータベースとして機能するため、外部認証サーバに依存する必要がなくなります。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザのクレデンシャルを取得して、ユーザを認証します。ローカルEAPでは、コントローラとワイヤレスクライアント間で、LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC 認証方式をサポートします。

EAPプロファイル名なしで実施される、または存在しない名前のEAPプロファイルが実施される場合、EAP はデフォルトでローカル認証用の EAP 方式を割り当てません。

（注） LDAPバックエンドデータベースでは、ローカルEAP方式として、EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC がサポートされます。LEAP、EAP-FAST/MSCHAPv2、および PEAPv0。MSCHAPv2は平文のパスワードを返すようにLDAPサーバが設定されている場合にのみサポートされます。

（注） スイッチは、Microsoft Active Directory や Novell の eDirectory などの外部 LDAP データベースに対するローカルEAP認証をサポートしています。Novell の eDirectory に対するローカルEAP認証用にコントローラを設定する方法の詳細については、『Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database』ホワイトペーパーを参照してください。

図 *10*：ローカル *EAP* の例



関連トピック

ローカル ユーザの作成, （281 ページ）
クライアント VLAN とインターフェイスの作成, （282 ページ）
EAP プロファイルの設定, （283 ページ）
クライアント VLAN の作成, （297 ページ）
外部 RADIUS サーバを使用した 802.1x WLAN の作成, （298 ページ）

IPv6 WLAN セキュリティの設定方法

ローカル認証の設定

ローカル ユーザの作成

手順の概要

1. **configure terminal**
2. **username** aaa_test
3. **password 0** aaa_test
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コマンド モードを開始します。
ステップ 2	**username** aaa_test 例： スイッチ(config)# **username aaa_test**	ユーザ名を作成します。
ステップ 3	**password 0** aaa_test 例： スイッチ(config)# **usernameaaa_test password 0 aaa_test**	ユーザ名のパスワードを割り当てます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
スイッチ# configure terminal
スイッチ(config)# username aaa_test password 0 aaa_test
スイッチ(config)# end
```

関連トピック

IPv6 WLAN セキュリティについて，（278 ページ）

クライアント VLAN とインターフェイスの作成

手順の概要

1. **configure terminal**
2. **vlan**
3. **exit**
4. **interface vlan** vlan_ID
5. **ip address**
6. **ipv6 address**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コマンド モードを開始します。
ステップ 2	**vlan** 例： スイッチ(config)# vlan 137	VLAN を作成します。
ステップ 3	**exit** 例： スイッチ (config-vlan)# exit	VLAN コンフィギュレーション モードを終了します。
ステップ 4	**interface vlan** vlan_ID 例： スイッチ (config)# interface vlan 137	インターフェイスに VLAN を関連付けます。
ステップ 5	**ip address** 例： スイッチ(config-if)# ip address 10.7.137.10 255.255.255.0	VLAN インターフェイスに IP アドレスを割り当てます。
ステップ 6	**ipv6 address** 例： スイッチ(config-if)#ipv6 address 2001:db8::20:1/64	VLAN インターフェイスに IPv6 アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
スイッチ# configure terminal
スイッチ(config)# vlan 137
スイッチ(config-vlan)#exit
スイッチ(config)#interface vlan 137
スイッチ(config-if)#ip address 10.7.137.10 255.255.255.0
スイッチ(config-if)#ipv6 address 2001:db8::20:1/64
スイッチ(config-if)#end
```

関連トピック

IPv6 WLAN セキュリティについて，（278 ページ）

EAP プロファイルの設定

手順の概要

1. **eap profile** name
2. **method leap**
3. **method tls**
4. **method peap**
5. **method mschapv2**
6. **method md5**
7. **method gtc**
8. **method fast profile** my-fast
9. **description** my_local**eap profile**
10. **exit**
11. **eap method fast profile**myFast
12. **authority-id** [identity|information]
13. **local-key 0** key-name
14. **pac-password 0** password
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**eap profile** name 例： `スイッチ(config)# eap profile wcm_eap_prof`	EAP プロファイルを作成します。
ステップ 2	**method leap** 例： `スイッチ(config-eap-profile)# method leap`	プロファイルでEAP-LEAP方式を設定します。
ステップ 3	**method tls** 例： `スイッチ(config-eap-profile)# method tls`	プロファイルでEAP-TLS方式を設定します。
ステップ 4	**method peap** 例： `スイッチ(config-eap-profile)# method peap`	プロファイルで PEAP 方式を設定します。
ステップ 5	**method mschapv2** 例： `スイッチ(config-eap-profile)# method mschapv2`	プロファイルで EAP-MSCHAPV2 方式を設定します。
ステップ 6	**method md5** 例： `スイッチ(config-eap-profile)# method md5`	プロファイルでEAP-MD5方式を設定します。
ステップ 7	**method gtc** 例： `スイッチ(config-eap-profile)# method gtc`	プロファイルでEAP-GTC方式を設定します。

ステップ 8	**method fast profile** my-fast
	
	例：
	`スイッチ(config-eap-profile)# eap method fast profile my-fast`
	`スイッチ (config-eap-profile)#description my_local eap profile`
		my-fast という EAP プロファイルを作成します。

ステップ 9	**description** my_local**eap profile** 例： `スイッチ (config-eap-profile)#description my_local eap profile`	ローカル プロファイルの説明を指定します。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `スイッチ (config-eap-profile)# exit`	eapプロファイル コンフィギュレーション モードを終了します。
ステップ 11	**eap method fast profile**myFast 例： `スイッチ (config)# eap method fast profile myFast`	EAP 方式プロファイルを設定します。

ステップ 12	**authority-id** [identity|information]
	
	例：
	`スイッチ(config-eap-method-profile)# authority-id identity my_identity`
	`スイッチ(config-eap-method-profile)#authority-id information my_information`
		EAP方式プロファイルの認証局IDおよび情報を設定します。

ステップ 13	**local-key 0** key-name 例： `スイッチ(config-eap-method-profile)# local-key 0 test`	ローカル サーバ キーを設定します。
ステップ 14	**pac-password 0** password 例： `スイッチ(config-eap-method-profile)# pac-password 0 test`	手動の PAC プロビジョニング用の PAC パスワードを設定します。
ステップ 15	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
スイッチ(config)#eap profile wcm_eap_prof
スイッチ(config-eap-profile)#method leap
スイッチ(config-eap-profile)#method tls
スイッチ(config-eap-profile)#method peap
スイッチ(config-eap-profile)#method mschapv2
スイッチ(config-eap-profile)#method md5
スイッチ(config-eap-profile)#method gtc
スイッチ(config-eap-profile)#eap method fast profile my-fast
スイッチ (config-eap-profile)#description my_local eap profile
スイッチ(config-eap-profile)# exit
スイッチ (config)# eap method fast profile myFast
スイッチ(config-eap-method-profile)#authority-id identity my_identity
スイッチ(config-eap-method-profile)#authority-id information my_information
スイッチ(config-eap-method-profile)#local-key 0 test
スイッチ(config-eap-method-profile)#pac-password 0 test
スイッチ(config-eap-method-profile)# end
```

関連トピック

IPv6 WLAN セキュリティについて，（278 ページ）

ローカル認証モデルの作成

手順の概要

1. **aaa** new-model
2. **authentication dot1x default local**
3. **dot1x** method_list **local**
4. **aaa authentication dot1x** dot1x_name **local**
5. **aaa authorization credential-download** name **local**
6. **aaa local authentication** auth-name **authorization** authorization-name
7. **session ID**
8. **dot1x system-auth-control**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**aaa** new-model 例： `スイッチ(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 2	**authentication dot1x default local** 例： `スイッチ(config)# aaa authentication dot1x default local`	他の方法が見つからない場合、dot1x でデフォルトのローカル RADIUS を使用する必要があることを意味します。
ステップ 3	**dot1x** method_list **local** 例： `スイッチ(config)# aaa authentication dot1x wcm_local local`	wcm_local 方式リスト用のローカル認証を割り当てます。
ステップ 4	**aaa authentication dot1x** dot1x_name **local** 例： `スイッチ(config)# aaa authentication dot1x aaa_auth local`	dot1x 方式用のローカル認証を設定します。
ステップ 5	**aaa authorization credential-download** name **local** 例： `スイッチ(config)# aaa authorization credential-download wcm_author local`	Local/RADIUS/LDAP から EAP クレデンシャルをダウンロードするようにローカル データベースを設定します。

	コマンドまたはアクション	目的
ステップ 6	**aaa local authentication** auth-name **authorization** authorization-name 例： `スイッチ(config)# aaa local authentication wcm_local authorization wcm_author`	ローカル認証および許可を選択します。
ステップ 7	**session ID** 例： `スイッチ(config)# aaa session-id common`	AAA のセッション ID を設定します。
ステップ 8	**dot1x system-auth-control** 例： `スイッチ(config)# dot1x system-auth-control`	dot.1x システム認証制御をイネーブルにします。

```
スイッチ(config)# aaa new-model
スイッチ(config)# aaa authentication dot1x default local
スイッチ(config)# aaa authentication dot1x wcm-local local
スイッチ(config)# aaa authentication dot1x aaa_auth local
スイッチ(config)# aaa authorization credential-download wcm_author local
スイッチ(config)# aaa local authentication wcm_local authorization wcm_author
スイッチ(config)# aaa session-id common
スイッチ(config)# dot1x system-auth-control
```

クライアント WLAN の作成

（注） この例では、ダイナミック WEP の 802.1x を使用しています。ワイヤレス クライアントでサポートされ、スイッチで設定可能な他の任意のセキュリティ メカニズムも使用できます。

手順の概要

1. **configure terminal**
2. **wlan** wlan name **<identifier>** SSID
3. **broadcast-ssid**
4. **no security wpa**
5. **security dot1x**
6. **security** dot1x authentication-list *wcm-local*
7. **local-auth** wcm_eap_prof
8. **client vlan** *137*
9. **no shutdown**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コマンド モードを開始します。
ステップ 2	**wlan** wlan name **<identifier>** SSID 例： スイッチ(config)# wlan wlanProfileName 1 ngwcSSID	WLAN を作成します。
ステップ 3	**broadcast-ssid** 例： スイッチ(config-wlan)# broadcast-ssid	WLAN で SSID をブロードキャストするように設定します。
ステップ 4	**no security wpa** 例： スイッチ(config-wlan)# no security wpa	WLAN の wpa をディセーブルにして、802.1x をイネーブルにします。
ステップ 5	**security dot1x** 例： スイッチ(config-wlan)# security dot1x	WLAN の 802.1x 暗号化セキュリティを設定します。
ステップ 6	**security** dot1x authentication-list *wcm-local* 例： スイッチ(config-wlan)# security dot1x authentication-list wcm-local	dot1x 認証用に WLAN へのサーバ グループ マッピングを設定します。
ステップ 7	**local-auth** wcm_eap_prof 例： スイッチ (config-wlan)# local-auth wcm_eap_profile	ローカル認証用に WLAN に eap プロファイルを設定します。
ステップ 8	**client vlan** *137* 例： スイッチ(config-wlan)# client vlan 137	WLAN に VLAN を関連付けます。
ステップ 9	**no shutdown** 例： スイッチ(config-wlan)# no shutdown	WLAN をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
スイッチ# config terminal
スイッチ(config)#wlan wlanProfileName 1 ngwcSSID
スイッチ(config-wlan)#broadcast-ssid
スイッチ(config-wlan)#no security wpa
スイッチ(config-wlan)#security dot1x
スイッチ(config-wlan)#security dot1x authentication-list wcm-local
スイッチ (config-wlan)# local-auth wcm_eap_prof
スイッチ(config-wlan)#client vlan 137
スイッチ(config-wlan)#no shutdown
スイッチ(config-wlan)#end
スイッチ#
```

関連トピック

WPA2+AES 用クライアント VLAN の作成, （291 ページ）

WPA2+AES でのローカル認証の設定

手順の概要

1. **configure terminal**
2. **aaa** new model
3. **dot1x system-auth-control**
4. **aaa authentication dot1x default local**
5. **aaa local authorization credential-download default local**
6. **aaa local authentication default authorization default**
7. **eap profile** wcm_eap_profile
8. **method leap**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**aaa** new model 例： スイッチ(config)# aaa **new-model**	AAA 認証モデルを作成します。
ステップ 3	**dot1x system-auth-control** 例： スイッチ(config)# dot1x system-auth-control	dot1x システム認証制御をイネーブルにします。
ステップ 4	**aaa authentication dot1x default local** 例： スイッチ(config)# aaa authentication dot1x default local	デフォルト dot1x 方式用のローカル認証を設定します。
ステップ 5	**aaa local authorization credential-download default local** 例： スイッチ(config)# aaa authorization credential-download default local	ローカル サーバから EAP クレデンシャルをダウンロードするようにデフォルトデータベースを設定します。
ステップ 6	**aaa local authentication default authorization default** 例： スイッチ(config)# aaa local authentication default authorization default	デフォルトのローカル認証および許可を選択します。
ステップ 7	**eap profile** wcm_eap_profile 例： スイッチ(config)#eap profile **wcm_eap_profile**	EAP プロファイルを作成します。
ステップ 8	**method leap** 例： スイッチ(config)# method leap	プロファイルで EAP-LEAP 方式を設定します。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
スイッチ# configure terminal
スイッチ(config)# aaa new-model
スイッチ(config)# dot1x system-auth-control
スイッチ(config)# aaa authentication dot1x default local
スイッチ(config)# aaa authorization credential-download default local
```

```
スイッチ(config)# aaa local authentication default authorization default
スイッチ(config)#eap profile wcm_eap_profile
スイッチ(config)# method leap
スイッチ(config)# end
```

WPA2+AES 用クライアント *VLAN* の作成

ローカル認証の WPA2+AES タイプの VLAN を作成します。この VLAN は、後で WLAN にマッピングされます。

手順の概要

1. **configure terminal**
2. **vlan** vlan_ID
3. **exit**
4. **interface** vlan vlan_ID
5. **ip address**
6. **ipv6 address**
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan** vlan_ID 例： `スイッチ (config)# vlan 105`	VLAN を作成します。
ステップ 3	**exit** 例： `スイッチ (config-vlan)# exit`	VLAN モードを終了します。
ステップ 4	**interface** vlan vlan_ID 例： `スイッチ(config)# interface vlan 105`	インターフェイスに VLAN を関連付けます。
ステップ 5	**ip address** 例： `スイッチ(config-if)# ip address 10.8.105.10 255.255.255.0`	VLAN インターフェイスに IP アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 6	**ipv6 address** 例： `スイッチ(config-if)#ipv6 address 2001:db8::10:1/64`	VLAN インターフェイスに IPv6 アドレスを割り当てます。
ステップ 7	**exit** 例： `スイッチ (config-if)# exit`	インターフェイス モードを終了します。

```
スイッチ# configure terminal
スイッチ(config)# vlan105
スイッチ (config-vlan)# exit
スイッチ (config)# interface vlan 105
スイッチ(config-if)#ip address 10.8.105.10 255.255.255.0
スイッチ(config-if)#ipv6 address 2001:db8::10:1/64
スイッチ(config-if)#exit
スイッチ(config)#
```

関連トピック

クライアント WLAN の作成，（287 ページ）

WPA2+AES 用 *WLAN* の作成

WLAN を作成し、WPA2+AES 用に作成されたクライアント VLAN にマッピングします。

手順の概要

1. **configure terminal**
2. **wlan** wpas2-aes-wlan 1 wpas2-aes-wlan
3. **client vlan** 105
4. **local-auth** wcm_eap_profile
5. **security dot1x authentication-list default**
6. **no shutdown**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wlan** wpas2-aes-wlan 1 wpas2-aes-wlan 例： スイッチ(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan スイッチ(config-wlan)#	WLAN を作成します。
ステップ 3	**client vlan** 105 例： スイッチ(config-wlan)#client vlan 105 スイッチ(config-wlan)#	クライアント VLAN に WLAN をマッピングします。
ステップ 4	**local-auth** wcm_eap_profile 例： スイッチ(config-wlan)#local-auth wcm_eap_profile	WLAN に EAP プロファイルを作成し、設定します。
ステップ 5	**security dot1x authentication-list default** 例： スイッチ(config-wlan)#security dot1x authentication-list default	デフォルトの dot1x 認証リストを使用します。
ステップ 6	**no shutdown** 例： スイッチ(config-wlan)#no shutdown スイッチ(config-wlan)#	WLAN をイネーブルにします。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
スイッチ# configure terminal
スイッチ(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan
スイッチ(config-wlan)#client vlan 105
スイッチ(config-wlan)#local-auth wcm_eap_profile
スイッチ(config-wlan)#security dot1x authentication-list default
スイッチ(config-wlan)#no shutdown
スイッチ(config-wlan)# exit
```

外部 RADIUS サーバの設定

RADIUS 認証サーバ ホストの設定

手順の概要

1. **configure terminal**
2. **radius server One**
3. **address ipv4** address **auth-port**auth_port_number **acct-port** acct_port_number
4. **address ipv6** address **auth-port**auth_port_number **acct-port** acct_port_number
5. **key** 0cisco
6.

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**radius server One** 例： `スイッチ (config)# radius server One`	RADIUS サーバを作成します。
ステップ 3	**address ipv4** address **auth-port**auth_port_number **acct-port** acct_port_number 例： `スイッチ (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813`	RADIUS サーバの IPv4 アドレスを設定します。
ステップ 4	**address ipv6** address **auth-port**auth_port_number **acct-port** acct_port_number 例： `スイッチ (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813`	RADIUS サーバの IPv6 アドレスを設定します。
ステップ 5	**key** 0cisco 例： `スイッチ (config-radius-server)# key 0 cisco`	**exit**
ステップ 6	 例： `スイッチ (config-radius-server)# exit`	RADIUS サーバ モードを終了します。

```
スイッチ# configure terminal
スイッチ (config)# radius server One
スイッチ (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813
スイッチ (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813
スイッチ (config-radius-server)# key 0 cisco
スイッチ (config-radius-server)#exit
```

関連トピック

RADIUS 認証サーバ グループの設定 , （295 ページ）

RADIUS 認証サーバ グループの設定

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa group server radius** wcm_rad
4. **server** <ip address>**auth-port**1812**acct-port**1813
5. **aaa authentication dot1x** method_list **group** wcm_rad
6. **dot1x system-auth-control**
7. **aaa session-idcommon**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**aaa new-model** 例： `スイッチ(config)#aaa new-model`	AAA 認証モデルを作成します。

ステップ 3	**aaa group server radius** wcm_rad
	
	例：
	`スイッチ(config)# aaa group server radius wcm_rad`
	
	`スイッチ(config-sg-radius)#`
		RADIUS サーバ グループを作成します。

	コマンドまたはアクション	目的

ステップ 4	**server** <ip address>**auth-port**1812**acct-port**1813
	
	例：
	`スイッチ(config-sg-radius)# server One auth-port 1812 acct-port 1813`
	`スイッチ(config-sg-radius)# server Two auth-port 1812 acct-port 1813`
	`スイッチ(config-sg-radius)# server Three auth-port 1812 acct-port 1813`
		手順 3 で作成した RADIUS グループにサーバを追加します。RADIUS アカウンティング サーバおよび認証サーバの UDP ポートを設定します。

ステップ 5	**aaa authentication dot1x** method_list **group** wcm_rad 例： `スイッチ(config)# aaa authentication dot1x method_list group wcm_rad`	RADIUS グループに方式リストをマッピングします。
ステップ 6	**dot1x system-auth-control** 例： `スイッチ(config)# dot1x system-auth-control`	RADIUS グループのシステム認証制御をイネーブルにします。
ステップ 7	**aaa session-idcommon** 例： `スイッチ(config)# aaa session-id common`	RADIUS グループから、特定のコールに対して送信されるすべてのセッション ID 情報が同じであることを確認します。

```
スイッチ# configure terminal
スイッチ(config)# aaa new-model
スイッチ(config)# aaa group server radius wcm_rad
スイッチ(config-sg-radius)# server One auth-port 1812 acct-port 1813
スイッチ(config-sg-radius)# server Two auth-port 1812 acct-port 1813
スイッチ(config-sg-radius)# server Three auth-port 1812 acct-port 1813
スイッチ(config)# aaa authentication dot1x method_list group wcm_rad
スイッチ(config)# dot1x system-auth-control
スイッチ(config)# aaa session-id common
スイッチ(config)#
```

関連トピック

RADIUS 認証サーバ ホストの設定 , （294 ページ）

クライアント VLAN の作成

手順の概要

1. **configure terminal**
2. **vlan** 137
3. **exit**
4. **interface vlan** 137
5. **ip address** 10.7.137.10 255.255.255.0
6. **ipv6 address** 2001:db8::30:1/64
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コマンド モードを開始します。
ステップ 2	**vlan** 137 例： スイッチ(config)# vlan 137	VLAN を作成してインターフェイスに関連付けます。
ステップ 3	**exit** 例： スイッチ (config-vlan)# exit	VLAN モードを終了します。
ステップ 4	**interface vlan** 137 例： スイッチ (config)# interface vlan 137	インターフェイスに VLAN を割り当てます。
ステップ 5	**ip address** 10.7.137.10 255.255.255.0 例： スイッチ(config-if)# ip address **10.7.137.10 255.255.255.0**	VLAN インターフェイスに IPv4 アドレスを割り当てます。
ステップ 6	**ipv6 address** 2001:db8::30:1/64 例： スイッチ(config-if)# ipv6 address **2001:db8::30:1/64**	VLAN インターフェイスに IPv6 アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
スイッチ# configure terminal
スイッチ(config)# vlan137
スイッチ(config-vlan)# exit
スイッチ(config)# interface vlan137
スイッチ(config-if)# ip address 10.7.137.10 255.255.255.0
スイッチ(config-if)# ipv6 address 2001:db8::30:1/64
スイッチ(config-if)# end
```

関連トピック

IPv6 WLAN セキュリティについて, （278 ページ）
外部 RADIUS サーバを使用した 802.1x WLAN の作成, （298 ページ）

外部 RADIUS サーバを使用した 802.1x WLAN の作成

手順の概要

1. **configure terminal**
2. **wlan** ngwc-1x<**ssid**>ngwc-1x
3. **broadcast-ssid**
4. **no security wpa**
5. **security dot1x**
6. **security dot1x authentication-list** wcm-rad
7. **client vlan** 137
8. **no shutdown**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wlan** ngwc-1x**<ssid>**ngwc-1x 例： スイッチ(config)# wlan ngwc_8021x 2 ngwc_8021x	802.1x 認証用の新しい WLAN を作成します。
ステップ 3	**broadcast-ssid** 例： スイッチ(config-wlan)# broadcast-ssid	WLAN で SSID をブロードキャストするように設定します。
ステップ 4	**no security wpa** 例： スイッチ(config-wlan)# no security wpa	WLAN の WPA をディセーブルにして、802.1x をイネーブルにします。
ステップ 5	**security dot1x** 例： スイッチ(config-wlan)# security dot1x	WLAN の 802.1x 暗号化セキュリティを設定します。
ステップ 6	**security dot1x authentication-list** wcm-rad 例： スイッチ(config-wlan)# security dot1x authentication-list wcm-rad	dot1x 認証用に WLAN へのサーバ グループ マッピングを設定します。
ステップ 7	**client vlan** 137 例： スイッチ(config-wlan)# client vlan 137	WLAN に VLAN を関連付けます。
ステップ 8	**no shutdown** 例： スイッチ(config-wlan)# no shutdown	WLAN をイネーブルにします。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
スイッチ# configure terminal
スイッチ(config)#wlan ngwc_8021x 2 ngwc_8021x
スイッチ(config-wlan)# broadcast-ssid
スイッチ(config-wlan)# no security wpa
スイッチ(config-wlan)# security dot1x
スイッチ(config-wlan)# security dot1x authentication-list wcm-rad
スイッチ(config-wlan)# client vlan 137
```

```
スイッチ(config-wlan)# no shutdown
スイッチ(config-wlan)# end
```

関連トピック

クライアント VLAN の作成，（297 ページ）
IPv6 WLAN セキュリティについて，（278 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 Command Reference (Catalyst 3650 Switches)*
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
WLAN の設定	*WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

IPv6 WLAN セキュリティの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 WLAN セキュリティ機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 16 章

IPv6 ACL の設定

- IPv6 ACL の前提条件，303 ページ
- IPv6 ACL の制限，303 ページ
- IPv6 ACL について，304 ページ
- IPv6 ACL の設定 ，307 ページ
- IPv6 ACL の設定方法，308 ページ
- IPv6 ACL の確認，315 ページ
- IPv6 ACL の設定例，316 ページ
- その他の参考資料，321 ページ
- IPv6 ACL の機能情報，322 ページ

IPv6 ACL の前提条件

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。また、スイッチで IP ベース フィーチャ セットが稼働している場合、入力ルータ ACL を作成しそれを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

関連トピック

IPv6 ACL の作成，（308 ページ）

IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは再帰 ACL（**reflect** キーワード）をサポートしません。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポートまたはSVI）にACLを適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうかを判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ（ACE）を追加しようとする場合、スイッチは現在インターフェイスに適用されている ACL に ACE が追加されることを許可しません。

IPv6 ACL について

アクセスコントロールリスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます）。スイッチで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、またはワイヤレス クライアントとやり取りするデータ トラフィックの制御用の WLAN、あるいは中央処理装置（CPU）宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

Web 認証用に事前認証 ACL を作成することもできます。このような ACL は、認証が完了するまでに特定のタイプのトラフィックを許可するために使用されます。

IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

（注） ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

IPv6 ACL の概要

スイッチは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンド トラフィッ

クまたはインバウンド トラフィックでサポートされます。IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。

- IPv6 ポート ACL は、レイヤ 2 インターフェイスのインバウンド トラフィックでだけサポートされます。IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。

IP ベース フィーチャ セットが稼働しているスイッチは、入力ルータ IPv6 ACL だけをサポートします。ポート ACL または出力ルータ IPv6 ACL はサポートされません。

（注） サポートされない IPv6 ACL を設定した場合、エラー メッセージが表示され、その設定は有効になりません。

スイッチは、IPv6 トラフィックの Virtual LAN（VLAN）ACL（VLAN マップ）をサポートしません。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

- SVI に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド IP パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに

  着信したパケットはポート ACL によってフィルタリングされます。発信ルーテッド IPv6 パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。

（注） いずれかのポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

関連トピック

IPv6 ACL の作成，（308 ページ）
インターフェイスへの IPv6 の適用，（313 ページ）
WLAN IPv6 ACL の作成，（314 ページ）
IPv6 ACL の表示，（315 ページ）

ACL のタイプ

ユーザあたりの IPv6 ACL

ユーザあたりのACLの場合、テキスト文字列として、完全アクセス制御エントリ（ACE）がACSで設定されます。

ACE はコントローラで設定されません。ACE は `ACCESS-Accept` 属性でスイッチに送信され、クライアントに直接適用されます。ワイヤレス クライアントが外部スイッチにローミングするときに、ACEが、AAA属性としてモビリティ ハンドオフ メッセージで外部スイッチに送信されます。ユーザあたりの ACL を使用した出力方向はサポートされていません。

フィルタ ID IPv6 ACL

filter-Id ACL の場合、完全な ACE および `acl name(filter-id)` がスイッチで設定され、`filter-id` のみが ACS で設定されます。`filter-id` は ACCESS-Accept 属性でスイッチに送信され、スイッチは ACE の filter-id をルックアップしてから、クライアントに ACE を適用します。クライアント L2 が外部スイッチにローミングするときに、filter-id だけがモビリティ ハンドオフ メッセージで外部スイッチに送信されます。ユーザあたりの ACL を使用した出力フィルタ ACL はサポートされていません。外部スイッチは filter-id と ACE を事前に設定する必要があります。

ダウンロード可能 IPv6 ACL

ダウンロード可能 ACL（dACL）の場合、完全な ACE および `dacl` 名はすべて ACS だけで設定されます。

（注） コントローラは ACL を設定しません。

ACS は `dacl` 名をスイッチに対しその `ACCESS-Accept` 属性で送信します。さらに `dacl` 名を使用して、ACE のために `dACL` 名が ACS に、`access-request` 属性によって戻されます。

ACS は `access-accept` 属性でスイッチの対応する ACE に応答します。ワイヤレス クライアントが外部スイッチにローミングするときに、`dacl` 名だけがモビリティ ハンドオフ メッセージで外部スイッチに送信されます。外部スイッチは、`dacl` 名の ACS サーバにアクセスして ACE を取得します。

IPv6 ACL とスイッチ スタック

スタック マスターは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバーに配信します。

（注） スイッチ スタック内で IPv6 を完全に機能させるには、すべてのスタック メンバーで拡張 IP サービス フィーチャ セットが稼働している必要があります。

新しいスイッチがスタック マスターを引き継ぐと、ACL 設定がすべてのスタック メンバーに配信されます。メンバスイッチは、新しいスタック マスターによって配信された設定との同期をとり、不要なエントリを一掃します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、スタック マスターは変更内容をすべてのスタック メンバーに配信します。

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します

はじめる前に

IPv6 ACL を設定する場合は、事前にデュアル IPv4 および IPv6 SDM テンプレートのいずれかを選択する必要があります。

手順の概要

1. IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
2. IPv6 ACL が、トラフィックをブロックする（拒否）または通過させる（許可）よう設定します。
3. トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。
4. インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。	
ステップ 2	IPv6 ACL が、トラフィックをブロックする（拒否）または通過させる（許可）よう設定します。	
ステップ 3	トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。	
ステップ 4	インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。	

IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージプロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリが満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはインターフェイスでドロップされます。

（注） 追加できなかった ACL と同じタイプのパケットのみ（ipv4、ipv6、MAC）がインターフェイスでドロップされます。

IPv6 ACL の設定方法

IPv6 ACL の作成

IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **ipv6access-list***acl_name*
3. **{deny|permit}protocol**
4. **{deny|permit}tcp**
5. **{deny|permit}udp**
6. **{deny|permit}icmp**
7. **end**
8. **showipv6access-list**
9. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6access-list***acl_name* 例： ipv6 access-list access-list-name	名前を使用して IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 3	**{deny|permit}protocol** 例： {deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • source-ipv6-prefix/prefix-length または destination-ipv6-prefix/ prefix-length は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 • host source-ipv6-address または destination-ipv6-address には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト

	コマンドまたはアクション	目的
		アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （任意）operatorには、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、lt（より小さい）、gt（より大きい）、eq（等しい）、neq（等しくない）、range（包含範囲）があります。 source-ipv6-prefix/prefix-length 引数のあとの operator は、送信元ポートに一致する必要があります。destination-ipv6- prefix/prefix-length 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）port-number は、0 ～ 65535 の 10 進数またはTCP あるいはUDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）dscp value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）fragments を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • （任意）log を指定すると、エントリと一致するパケットに関するログ メッセージがコンソールに送信されます。log-input を指定すると、ログ エントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 • （任意）routing を入力して、IPv6 パケットのルーティングを指定します。 • （任意）sequence value を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。

	コマンドまたはアクション	目的
		• （任意）time-range name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 4	**{deny|permit}tcp** 例： `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。パラメータはステップ 3 で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 • ack：確認応答（ACK）ビット セット • established：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • fin：終了ビット セット。送信元からのデータはそれ以上ありません。 • neq {port | protocol}：所定のポート番号上にないパケットだけを照合します。 • psh：プッシュ機能ビット セット • range {port | protocol}：ポート番号の範囲内のパケットだけを照合します。 • rst：リセット ビット セット • syn：同期ビット セット • urg：緊急ポインタ ビット セット
ステップ 5	**{deny|permit}udp** 例： `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port |protocol}] [range {port |protocol}] [routing][sequence value][time-range name]`	（任意）UDP アクセス リストおよびアクセス条件を定義します。 ユーザ データグラム プロトコルの場合は、udp を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [port]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。
ステップ 6	**{deny|permit}icmp** 例： `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any |`	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージプロトコルの場合は、icmp を入力します。ICMP パラメータはステップ 3a

	コマンドまたはアクション	目的
	hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]	の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • icmp-type：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-code：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-message：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、?キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**showipv6access-list** 例： show ipv6 access-list	アクセス リストの設定を確認します。
ステップ 9	**copyrunning-configstartup-config** 例： copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv6 ACL の前提条件，（303 ページ）
IPv6 ACL の概要，（304 ページ）
インターフェイスへの IPv6 の適用，（313 ページ）
WLAN IPv6 ACL の作成，（314 ページ）
IPv6 ACL の表示，（315 ページ）

インターフェイスへの IPv6 の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する手順について説明します。レイヤ 2 およびレイヤ 3 インターフェイスの発信または着信トラフィックに IPv6 ACL を適用できます。IPv6 ACL はレイヤ 3 インターフェイスの着信管理トラフィックにだけ適用できます。

インターフェイスへのアクセスを制御する管理には、特権EXECモードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface**interface_id
3. **noswitchport**
4. **ipv6address***ipv6_address*
5. **ipv6traffic-filter***acl_name*
6. **end**
7. **showrunning-configinterfacetenGigabitEthernet1/0/3**
8. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface**interface_id 例： スイッチ# interface interface-id	アクセス リストを適用するレイヤ 2 インターフェイス（ポート ACL 用）またはレイヤ 3 スイッチ仮想インターフェイス（ルータ ACL 用）を特定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**noswitchport** 例： スイッチ# no switchport	レイヤ 2 モード（デフォルト）からレイヤ 3 モードにインターフェイスを変更します（ルータ ACL を適用する場合のみ）。
ステップ 4	**ipv6address***ipv6_address* 例： スイッチ# ipv6 address ipv6-address	レイヤ 3 インターフェイス（ルータ ACL 用）で Ipv6 アドレスを設定します。 （注） このコマンドは、レイヤ2インターフェイスでは、またはインターフェイスに明示的な IPv6 アドレスが設定されている場合には、必要ありません。

	コマンドまたはアクション	目的
ステップ 5	**ipv6traffic-filter***acl_name* 例： スイッチ# ipv6 traffic-filter access-list-name {in | out}	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 7	**showrunning-configinterfacetenGigabitEthernet1/0/3** 例： スイッチ# show running-config interface tenGigabitEthernet 1/0/3 .... Building configuration .... Current configuration : 98 bytes ! interface TenGigabitEthernet1/0/3 switchport mode trunk ipv6 traffic-filter MyFilter out end	設定の概要を示します。
ステップ 8	**copyrunning-configstartup-config** 例： copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv6 ACL の作成，（308 ページ）
IPv6 ACL の概要，（304 ページ）
WLAN IPv6 ACL の作成，（314 ページ）
IPv6 ACL の表示，（315 ページ）

WLAN IPv6 ACL の作成

手順の概要

1. **ipv6traffic-filter acl***acl_name*
2. **ipv6traffic-filteraclweb**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6traffic-filter acl***acl_name* 例： `スイッチ(config-wlan)# ipv6 traffic-filter acl <acl_name>`	名前付き WLAN ACL を作成します。
ステップ 2	**ipv6traffic-filteraclweb** 例： `スイッチ(config-wlan)# ipv6 traffic-filter acl web <acl_name-preauth>`	WLAN ACL の事前認証を作成します。

```
スイッチ(config-wlan)# ipv6 traffic-filter acl <acl_name>
スイッチ(config-wlan)#ipv6 traffic-filter acl web <acl_name-preauth>
```

関連トピック

IPv6 ACL の作成，（308 ページ）
インターフェイスへの IPv6 の適用，（313 ページ）
IPv6 ACL の概要，（304 ページ）
IPv6 ACL の表示，（315 ページ）

IPv6 ACL の確認

IPv6 ACL の表示

1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show access-list** 例： `スイッチ# show access-lists`	スイッチに設定されたすべてのアクセスリストを表示します。

	コマンドまたはアクション	目的
ステップ 2	**show ipv6 access-list** *acl_name* 例： `スイッチ# show ipv6 access-list [access-list-name]`	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

関連トピック

IPv6 ACL の作成，（308 ページ）
インターフェイスへの IPv6 の適用，（313 ページ）
WLAN IPv6 ACL の作成，（314 ページ）
IPv6 ACL の概要，（304 ページ）

IPv6 ACL の設定例

例：IPv6 ACL の作成

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番めの拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番めの許可エントリは、その他のすべてのトラフィックを許可します。暗黙の全否定の条件が各 IPv6 アクセス リストの末尾にあるため、2 番めの許可エントリは必要です。

（注） ロギングは、レイヤ 3 インターフェイスでのみサポートされます。

```
スイッチ(config)# ipv6 access-list CISCO
スイッチ(config-ipv6-acl)# deny tcp any any gt 5000
スイッチ (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
スイッチ(config-ipv6-acl)# permit icmp any any
スイッチ(config-ipv6-acl)# permit any any
```

例：IPv6 ACL の適用

次に、レイヤ 3 インターフェイスの発信トラフィックに対して、アクセス リスト Cisco を適用する例を示します。

```
スイッチ(config)# interface TenGigabitEthernet 1/0/3

スイッチ(config-if)# no switchport
スイッチ(config-if)# ipv6 address 2001::/64 eui-64
スイッチ(config-if)# ipv6 traffic-filter CISCO out
```

例：IPv6 ACL の表示

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
スイッチ #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

次に、show ipv6 access-lists 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
スイッチ# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

例：RA スロットリングと NS 抑制の設定

このタスクでは、省電力のワイヤレス クライアントが頻繁な非請求の定期的 RA に影響されないように、RA スロットル ポリシーを作成する方法について説明します。非請求タイプのマルチキャスト RA は、コントローラによってスロットルされます。

はじめる前に

クライアント マシンで IPv6 をイネーブルにします。

手順の概要

1. **configure terminal**
2. **ipv6 nd ra-throttler policy** Mythrottle
3. **throttle-period** 20
4. **max-through** 5
5. **allow at-least** 3 **at-most** 5
6. **switch (config)# vlan configuration 100**
7. **ipv6 nd suppress**
8. **ipv6 nd ra-th attach-policy** attach-policy_name
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd ra-throttler policy** Mythrottle 例： スイッチ (config)# ipv6 nd ra-throttler policy Mythrottle	Mythrottle という RA スロットラ ポリシーを作成します。
ステップ 3	**throttle-period** 20 例： スイッチ (config-nd-ra-throttle)# throttle-period 20	スロットリングを適用する時間間隔セグメントを特定します。
ステップ 4	**max-through** 5 例： スイッチ (config-nd-ra-throttle)# max-through 5	許容する初期 RA の数を特定します。
ステップ 5	**allow at-least** 3 **at-most** 5 例： スイッチ (config-nd-ra-throttle)# allow at-least 3 at-most 5	初期RAが送信された後に、間隔セグメントの終了まで許容される RA の数を特定します。
ステップ 6	**switch (config)# vlan configuration 100** 例： スイッチ (config)# vlan configuration 100	vlan あたりの設定を作成します。
ステップ 7	**ipv6 nd suppress** 例： スイッチ (config)# ipv6 nd suppress	Vlan でネイバー探索をディセーブルにします。
ステップ 8	**ipv6 nd ra-th attach-policy** attach-policy_name 例： スイッチ (config)# ipv6 nd ra-throttle attach-policy attach-policy_name	ルータ アドバタイズメント スロットリングをイネーブルにします。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権EXECモードに戻ります。また、Ctrl+Zキーを押しても、グローバル コンフィギュレーション モードを終了できます。

例：RA ガード ポリシーの設定

手順の概要

1. **ipv6 nd raguard policy** MyPloicy
2. **trusted-port**
3. **device-role router**
4. **interface tenGigabitEthernet** 1/0/1
5. **ipv6 nd raguard attach-policy**MyPolicy
6. **vlan configuration** 19-21,23
7. **ipv6 nd suppress**
8. **ipv6 snooping**
9. **ipv6 nd raguard attach-policy** MyPolicy
10. **ipv6 nd ra-throttler attach-policy** Mythrottle

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6 nd raguard policy** MyPloicy 例： `スイッチ (config)# ipv6 nd raguard policy MyPolicy`	
ステップ 2	**trusted-port** 例： `スイッチ (config-nd-raguard)# trusted-port`	上記で作成したポリシーの信頼できるポートを設定します。

ステップ 3	**device-role router**
	
	例：
	`スイッチ (config-nd-raguard)# device-role [host|monitor|router|switch]`
	`スイッチ (config-nd-raguard)# device-role router`
		上記で作成した信頼できるポートに RA を送信可能な信頼できるデバイスを定義します。

ステップ 4	**interface tenGigabitEthernet** 1/0/1 例： `スイッチ (config)# interface tenGigabitEthernet 1/0/1`	信頼できるデバイスにインターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 nd raguard attach-policy**MyPolicy 例： `スイッチ (config-if)# ipv6 nd raguard attach-policy Mypolicy`	ポートから受信した RA を信頼するようにポリシーを設定し、接続します。
ステップ 6	**vlan configuration** 19-21,23 例： `スイッチ (config)# vlan configuration 19-21,23`	ワイヤレス クライアントの vlan を設定します。
ステップ 7	**ipv6 nd suppress** 例： `スイッチ (config-vlan-config)# ipv6 nd suppress`	無線上で ND メッセージを抑制します。
ステップ 8	**ipv6 snooping** 例： `スイッチ (config-vlan-config)# ipv6 snooping`	IPv6 トラフィックをキャプチャします。
ステップ 9	**ipv6 nd raguard attach-policy** MyPolicy 例： `スイッチ (config-vlan-config)# ipv6 nd raguard attach-policy Mypolicy`	ワイヤレス クライアントの vlan に RA ガード ポリシーを接続します。
ステップ 10	**ipv6 nd ra-throttler attach-policy** Mythrottle 例： `スイッチ (config-vlan-config)#ipv6 nd ra-throttler attach-policy Mythrottle`	ワイヤレス クライアントの vlan に RA スロットリング ポリシーを接続します。

例：IPv6 ネイバー バインディングの設定

手順の概要

1. **ipv6 neighbor binding** [vlan]19 2001:db8::25:4 **interface tenGigabitEthernet** 1/0/3 aaa.bbb.ccc

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6 neighbor binding** [vlan]19 2001:db8::25:4 **interface tenGigabitEthernet** 1/0/3 aaa.bbb.ccc 例： `スイッチ (config)# ipv6 neighbor binding vlan 19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc`	送信元 MAC アドレスとして aaa.bbb.ccc が設定されたインターフェイス te1/0/3 を介して VLAN 19 で送信する場合にのみ有効なネイバー 2001:db8::25:4 を設定して検証します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 Command Reference (Catalyst 3650 Switches)*
ACL 設定	*Security Configuration Guide (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

IPv6 ACL の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 ACL 機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 17 章

IPv6 Web 認証の設定

- IPv6 Web 認証の前提条件，323 ページ
- IPv6 Web 認証の制限，323 ページ
- IPv6 Web 認証について，324 ページ
- IPv6 Web 認証の設定方法，325 ページ
- IPv6 Web 認証の確認，332 ページ
- その他の参考資料，333 ページ
- IPv6 Web 認証の機能情報，334 ページ

IPv6 Web 認証の前提条件

次の設定を、IPv6 Web 認証を開始する前に行う必要があります。

- IPv6 デバイス トラッキング
- IPv6 DHCP スヌーピング
- wlan 上の 802.1x タイプのセキュリティをディセーブルにします。
- 各 WLAN には、vlan が関連付けられている必要があります。
- デフォルトの wlan 設定を **shutdown** から **no shutdown**に変更します。

関連トピック

WLAN のセキュリティのイネーブル化，（327 ページ）

IPv6 Web 認証の制限

次の制限は、IPv6 Web 認証の使用時に適用されます。

関連トピック

WLAN のセキュリティのイネーブル化，（327 ページ）

IPv6 Web 認証について

Web 認証は、レイヤ 3 セキュリティ機能です。スイッチでは、有効なユーザー名とパスワードを入力するまで、特定のクライアントからの IP トラフィック（DHCP および DNS 関連パケットを除く）を拒否します。これはサプリカントまたはクライアント ユーティリティを必要としないシンプルな認証方式です。一般に Web 認証は、ゲスト アクセス ネットワークを展開する顧客が使用します。HTTP と HTTPS の両方からのトラフィックで、ページがログイン ページを表示できるようにします。

（注） Web 認証は、データ暗号化を提供せず、通常は、接続が常に重要になるホット スポットまたはキャンパス環境用のシンプルなゲスト アクセスとして使用されます。

WLAN は、Web ベース認証の**security webauth** として設定されます。スイッチは次のタイプの Web ベース認証をサポートしています。

- Web 認証：クライアントが Web ページにクレデンシャルを入力し、次に Wlan コントローラによって検証されます。
- Web 同意：Wlan コントローラは、[Accept/Deny] ボタンが用意されたポリシー ページを提供します。ネットワークにアクセスするには、[Accept] ボタンをクリックします。

一般に Wlan はオープン認証用に設定されます。つまり、レイヤ 2 認証なしで、Web ベースの認証メカニズムが使用されるときに設定されます。

Web 認証プロセス

次のイベントは、WLAN が Web 認証用に設定されている場合に発生します。

- ユーザは、Web ブラウザを開き、URL アドレスとして、たとえば、*http://www.example.com* を入力します。クライアントは、この URL の DNS 要求を送信して、宛先の IP アドレスを取得します。スイッチは DNS 要求を DNS サーバにバイパスし、サーバは宛先 *www.example.com* の IP アドレスが含まれている DNS 応答で応答します。次にこれがワイヤレス クライアントに転送されます。
- クライアントは、宛先 IP アドレスで TCP 接続を開こうとします。*www.example.com* の IP アドレス宛ての TCP SYN パケットを送信します。
- スイッチにはクライアントに設定されたルールがあり、*www.example.com* のプロキシとして機能できません。*www.example.com* の IP アドレスとしての送信元とともにクライアントに TCP SYN-ACK パケットを戻します。クライアントは、スリーウェイ TCP ハンドシェイクを完了するために TCP ACK パケットを戻し、TCP 接続が完全に確立されます。

- クライアントは、*www.example.com* 宛ての HTTP GET パケットを送信します。スイッチはこのパケットをインターセプトし、リダイレクト処理用に送信します。HTTP アプリケーション ゲートウェイは、クライアントによって要求された HTTP GET への応答として、HTML 本文を準備し送信します。この HTML では、クライアントはスイッチのデフォルトの Web ページ（たとえば、*http://<Virtual-Server-IP>/login.html*）に転送されます。
- クライアントは、たとえば、*www.example.com* などの IP アドレスとの TCP 接続を閉じます。
- クライアントは仮想 IP に移動する場合に、スイッチの仮想 IP アドレスで TCP 接続を開こうとします。スイッチに、仮想 IP 用の TCP SYN パケットを送信します。
- スイッチは TCP SYN-ACK で返答し、クライアントはハンドシェイクを完了するために、TCP ACK をスイッチに戻します。
- クライアントは、ログイン ページの要求のために、仮想 IP 宛ての */login.html* 用に HTTP GET を送信します。
- この要求は、スイッチの Web サーバで許可され、サーバはデフォルト ログイン ページで応答します。クライアントは、ユーザがログインできるブラウザ ウィンドウでログイン ページを受信します。

関連トピック

WPA のディセーブル化, （325 ページ）
WLAN のセキュリティのイネーブル化, （327 ページ）
WLAN のパラメータ マップのイネーブル化, （327 ページ）
WLAN の認証リストのイネーブル化, （328 ページ）
グローバル Web 認証 WLAN パラメータ マップの設定, （328 ページ）
WLAN の設定, （329 ページ）
グローバル コンフィギュレーション モードの IPv6 のイネーブル化, （331 ページ）
パラメータ マップの確認, （332 ページ）
認証リストの確認, （332 ページ）

IPv6 Web 認証の設定方法

WPA のディセーブル化

はじめる前に

802.1x をディセーブルにします。一般的な Web 認証では、レイヤ 2 セキュリティを使用しません。レイヤ 2 セキュリティを削除するには、この設定を使用します。

手順の概要

1. **configureterminal**
2. **wlan** test1 2 test1
3. **no security** wpa

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** test1 2 test1 例： `スイッチ(config)# wlan test1 2 test1`	WLAN を作成し、SSID を割り当てます。
ステップ 3	**no security** wpa 例： `スイッチ(config-wlan)# no security wpa`	Wlan に対して WPA のサポートをディセーブルにします。

次の作業

次をイネーブルにします。

- セキュリティ Web 認証
- パラメータ ローカル
- 認証リスト

関連トピック

Web 認証プロセス，（324 ページ）

WLAN のセキュリティのイネーブル化

手順の概要

1. **parameter-map type web-auth global**
2. **virtual-ip ipv4** 192.0.2.1
3. **virtual-ip ipv6** 2001:db8::24:2

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**parameter-map type web-auth global** 例： `スイッチ(config)# parameter-map type web-auth global`	すべての Web 認証 wlan にパラメータ マップを適用します。
ステップ 2	**virtual-ip ipv4** 192.0.2.1 例： `スイッチ(config-params-parameter-map)# virtual-ip ipv4 192.0.2.1`	仮想ゲートウェイの IPv4 アドレスを定義します。
ステップ 3	**virtual-ip ipv6** 2001:db8::24:2 例： `スイッチ(config-params-parameter-map)# virtual-ip ipv6 2001:db8::24:2`	仮想ゲートウェイの IPv6 アドレスを定義します。

関連トピック

IPv6 Web 認証の前提条件，（323 ページ）
IPv6 Web 認証の制限，（323 ページ）
Web 認証プロセス，（324 ページ）

WLAN のパラメータ マップのイネーブル化

手順の概要

1. **security web-auth parameter-map** <mapname>

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**security web-auth parameter-map** <mapname> 例： `スイッチ(config-wlan)# security web-auth parameter-map webparalocal`	wlan 用の Web 認証をイネーブルにし、パラメータ マップを作成します。

関連トピック

Web 認証プロセス，（324 ページ）

WLAN の認証リストのイネーブル化

手順の概要

1. **security web-auth authentication-list** webauthlistlocal

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**security web-auth authentication-list** webauthlistlocal 例： `スイッチ(config-wlan)# security web-auth`	wlan 用の Web 認証をイネーブルにし、ローカル Web 認証リストを作成します。

関連トピック

Web 認証プロセス，（324 ページ）

グローバル Web 認証 WLAN パラメータ マップの設定

この例を使用して、グローバル Web 認証 WLAN を設定し、パラメータ マップを追加します。

手順の概要

1. **parameter-map type webauth global**
2. **virtual-ip ipv6** 2001:db8:4::1
3. **ratelimit init-state-sessions** 120
4. **max-https-conns** 70

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**parameter-map type webauth global** 例： `スイッチ (config)# parameter-map type webauth global`	グローバル Web 認証を設定し、パラメータ マップを追加します。
ステップ 2	**virtual-ip ipv6** 2001:db8:4::1 例： `スイッチ (config-params-parameter-map)# virtual-ip ipv6 2001:db8:4::1`	認証用のワイヤレス クライアントに表示される仮想ゲートウェイ IP アドレスを定義します。
ステップ 3	**ratelimit init-state-sessions** 120 例： `スイッチ (config-params-parameter-map)# ratelimit init-state-sessions 120`	グローバル レート制限を設定して、スイッチで Web クライアントが使用できる帯域幅を制限し、オーバーフラッディング攻撃を防止します。
ステップ 4	**max-https-conns** 70 例： `スイッチ (config-params-parameter-map)# max-http-conns 70`	オーバーフラッディング攻撃を防止するため、スイッチで試行される http 接続の最大数を設定します。

関連トピック

Web 認証プロセス，（324 ページ）
WLAN の設定，（329 ページ）

WLAN の設定

はじめる前に

- WLAN は、Vlan が関連付けられている必要があります。デフォルトでは、新しい Wlan は常に設定要件に応じて変更できる Vlan 1 に関連付けられます。

- WLAN を *no shutdown* に設定して、イネーブルにします。デフォルトでは、Wlan は *shutdown* パラメータで設定され、ディセーブルです。

手順の概要

1. **wlan** *1*
2. **client vlan** *interface ID*
3. **security web-auth authentication list** webauthlistlocal
4. **security web-auth parameter-map** global
5. **no security wpa**
6. **no shutdown**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wlan** *1* 例： `スイッチ(config-wlan)# wlan 1 name vicweb ssid vicweb`	wlan を作成し、SSID を割り当てます。
ステップ 2	**client vlan** *interface ID* 例： `スイッチ(config-wlan)# client vlan VLAN0136`	クライアントを vlan インターフェイスに割り当てます。
ステップ 3	**security web-auth authentication list** webauthlistlocal 例： `スイッチ(config-wlan)# security web-auth authentication-list webauthlistlocal`	wlan 用の Web 認証を設定します。
ステップ 4	**security web-auth parameter-map** global 例： `スイッチ(config-wlan)# security web-auth parameter-map global`	wlan にパラメータ マップを設定します。
ステップ 5	**no security wpa** 例： `スイッチ(config-wlan)# no security wpa`	wlan のセキュリティ ポリシーを設定します。これにより wlan がイネーブルになります。
ステップ 6	**no shutdown** 例： `スイッチ(config-wlan)# no shutdown`	Wlan を設定して、イネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： スイッチ(config)# **end**	特権EXECモードに戻ります。また、Ctrl+Zキーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

グローバル Web 認証 WLAN パラメータ マップの設定，（328 ページ）
Web 認証プロセス，（324 ページ）
グローバル コンフィギュレーション モードの IPv6 のイネーブル化，（331 ページ）

グローバル コンフィギュレーション モードの IPv6 のイネーブル化

Web 認証用にグローバル コンフィギュレーションの IPv6 をイネーブルにします。

手順の概要

1. **configure terminal**
2. **web-auth global**
3. **virtual IPv6**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**web-auth global** 例： スイッチ(config)# parameter-map type webauth global	パラメータ マップのタイプを Web 認証としてグローバルに設定します。
ステップ 3	**virtual IPv6** 例： スイッチ(config-params-parameter-map)# virtual-ip ipv6	Web 認証用の仮想 IP として IPv6 を選択します。 （注） Web 認証用の優先 IP として IPv4 を選択することもできます。

関連トピック

WLAN の設定，（329 ページ）
Web 認証プロセス，（324 ページ）
パラメータ マップの確認，（332 ページ）

IPv6 Web 認証の確認

パラメータ マップの確認

Wlan に対して設定したパラメータ マップを確認するには、**show running configuration** コマンドを使用します。

手順の概要

1. **show running config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show running config** 例： スイッチshow running config	スイッチの実行コンフィギュレーション全体を表示します。パラメータマップのグレップを行い結果を表示します。

```
wlan alpha 2 alpha
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list webauthlistlocal
 security web-auth parameter-map webparalocal
```

関連トピック

グローバル コンフィギュレーション モードの IPv6 のイネーブル化，（331 ページ）
Web 認証プロセス，（324 ページ）
認証リストの確認，（332 ページ）

認証リストの確認

Wlan に対して設定した認証リストを確認するには、**show running configuration** コマンドを使用します。

手順の概要

1. **show running configuration**
2. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show running configuration** 例： スイッチ#show running-config	Wlan の設定を表示します。 スイッチ# show running-config
ステップ 2	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
スイッチ#show running-config
 ..................................
 ..................................
 ..................................
 wlan alpha 2 alpha
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list webauthlistlocal
 security web-auth parameter-map webparalocal
 ..................................
 ..................................
 ..................................
```

関連トピック

パラメータ マップの確認，（332 ページ）
Web 認証プロセス，（324 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 Command Reference (Catalyst 3650 Switches)*
Web 認証設定	*Security Configuration Guide (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

IPv6 Web 認証の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 Web 認証機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 18 章

IPv6 クライアント モビリティの設定

- IPv6 クライアント モビリティの前提条件，337 ページ
- IPv6 クライアント モビリティの制限，337 ページ
- IPv6 クライアント モビリティについて，338 ページ
- IPv6 クライアント モビリティの確認，342 ページ
- IPv6 クライアント モビリティのモニタリング，343 ページ
- その他の参考資料，343 ページ
- IPv6 クライアント モビリティの機能情報，344 ページ

IPv6 クライアント モビリティの前提条件

ワイヤレス IPv6 クライアント接続をイネーブルにするには、基礎となる有線ネットワークで、SLAAC または DHCPv6 などの IPv6 ルーティングおよびアドレス割り当て機能をサポートしている必要があります。スイッチは IPv6 ルータに対する L2 隣接関係が必要です。また、VLAN はパケットがスイッチに着信するときにタグを付ける必要があります。AP は、IPv6 ネットワーク上で接続を必要としません。すべてのトラフィックが AP とスイッチ間の IPv4 CAPWAP トンネル内でカプセル化されるためです。

IPv6 クライアント モビリティの制限

- IPv6 クライアント モビリティを使用する場合、クライアントはスタティック ステートレス自動設定（Windows XP クライアントなど）またはステートフル DHCPv6 IP アドレッシング（Windows 7 クライアントなど）とともに IPv6 をサポートする必要があります。

- ステートフル DHCPv6 IP アドレッシングが円滑に動作できるようにするには、DHCPv6 サーバとして動作するように設定された DHCP for IPv6 機能をサポートするスイッチまたはルータ（スイッチなど）、または組み込み DHCPv6 サーバを備えた Windows 2008 サーバなどの

専用サーバが必要です。Cisco Catalyst 3850 スイッチおよび Cisco Catalyst 5700 スイッチは、（内部的に）DHCPv6 サーバとして機能できます。

（注） Cisco Catalyst 3850 スイッチに SDM IPv6 テンプレートをロードするには、**sdm prefer dual-ipv4** および **v6** デフォルト コマンドを入力し、スイッチをリセットします。

IPv6 クライアント モビリティについて

スイッチは、IPv6 専用ノードまたはデュアル スタック ノードに対し IPv6 モビリティをサポートします。IPv6 クライアント モビリティは次のレイヤに分かれます。

- リンク層および
- ネットワーク層

リンク層は、リンク層接続を失うことなく、同じ SSID で識別される同一 BSS（基本サービス セット）の任意の AP にクライアントがローミングできるようにする 802.11 プロトコルによって処理されます。

ただし、リンク層モビリティは、ローミング中にワイヤレス クライアントのレイヤ 3 アプリケーションがシームレスに動作を継続するには十分ではありません。Cisco IOSd のワイヤレス モビリティ モジュールは、モビリティ トンネリングを使用して、クライアントが異なるスイッチ上の異なるサブネット間をローミングするときに、クライアントのレイヤ 3 PoP（Point of Presence）用のシームレスな接続を維持します。

IPv6 は、プロトコルの TCP/IP スイートの IPv4 に代わることを目的とした次世代ネットワーク層インターネットプロトコルです。この新しいバージョンでは、一意のグローバル IP アドレスを必要とするユーザとアプリケーションに対応するためのインターネット グローバルアドレス空間を増大させます。IPv6 は、128 ビットの送信元アドレスおよび宛先アドレスを組み込むことにより、32 ビットの IPv4 アドレスよりも格段に多くのアドレスを提供します。

コントローラをまたいだ IPv6 クライアントをサポートするには、IPv6 クライアントが同じレイヤ 3 ネットワーク上にとどまるように、ICMPv6 メッセージを特別に処理する必要があります。スイッチは、ICMPv6 メッセージを代行受信することで IPv6 クライアントを追跡し、シームレスなモビリティを提供して、ネットワーク攻撃からネットワークを保護します。NDP（ネイバー ディスカバリ パケット）パケットは、マルチキャストからユニキャストに変換され、クライアントごとに個別に配信されます。この固有なソリューションによって、ネイバーディスカバリ パケットとルータ アドバタイズメント パケットの VLAN 間でのリークを防止できます。クライアントは、特定のネイバー ディスカバリ パケットおよびルータ アドバタイズメント パケットを受信することで IPv6 アドレス指定が適切であることを確認し、不要なマルチキャスト トラフィックを回避します。

IPv6 モビリティの設定は、IPv4 モビリティと同一であり、シームレスなローミングを実現するためにクライアント側で別個のソフトウェアを使用する必要はありません。スイッチは、同じモビリティ グループに属している必要があります。IPv4 と IPv6 の両クライアント モビリティが、デフォルトで有効になります。

IPv6 クライアント モビリティは次のことに使用されます。

- レイヤ 2 およびレイヤ 3 ローミングでのクライアント IPv6 複数アドレスの維持
- IPv6 ネイバー探索プロトコル（NDP）パケットの管理
- クライアントの IPv6 アドレスの学習

ルータ アドバタイズメントの使用

ネイバー探索プロトコル（NDP）はリンク層で動作し、リンク上の他のノードの検出を行います。他のノードのリンク層アドレスを特定し、使用可能なルータを検索し、他のアクティブなネイバーノードのパスに関する到達可能性情報を維持します。

ルータ アドバタイズメント（RA）は、使用可能なルータを検出し、IPv6 アドレス、リンク MTU などを生成するネットワーク プレフィクスを取得するためにホストで使用される IPv6 ネイバー探索プロトコル（NDP）パケットの 1 つです。ルータは、定期的またはホスト ルータ送信要求メッセージへの応答として RA を送信します。

IPv6 ワイヤレス クライアント モビリティは IPv6 RA パケットを管理します。集約アクセススイッチは、リンクローカル全ノード マルチキャスト RA パケットをローカルおよび RA が受信される同じ VLAN にマップされたローミング ワイヤレス ノードに転送します。

図 1 では、ワイヤレス ノード モビリティでのリンクローカル全ノード マルチキャスト RA の転送の問題について説明します。

図 *11*：ルータ *2* から無効な *RA* を受け取るローミング クライアント

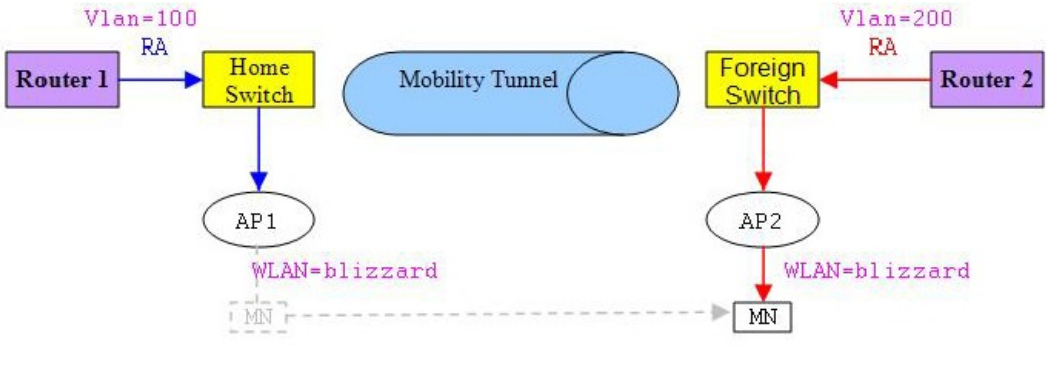
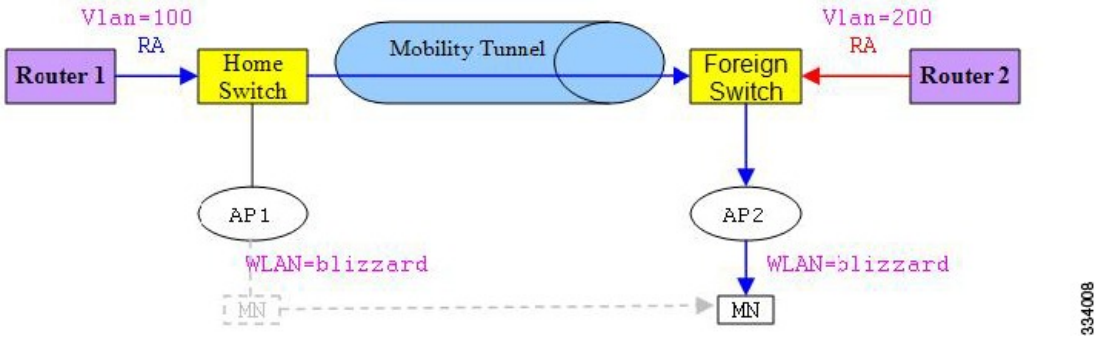


図 2 では、ローミング クライアント「MN」が外部スイッチで VLAN 200 から RA をどのように受信するか、および新しい IP アドレスを取得してどのように L3 モビリティの PoP（Point of Presence）に入るかを示しています。

図 *12*：ルータ *1* から有効な *RA* を受け取るローミング クライアント



関連トピック

IPv6 クライアント モビリティの確認，（342 ページ）
IPv6 クライアント モビリティのモニタリング，（343 ページ）

RA スロットリングと NS 抑制

頻繁な非請求タイプの定期的 RA による制約を受けないように省電力ワイヤレス クライアントを保護するため、コントローラで非請求タイプのマルチキャスト RA をスロットルできます。

関連トピック

IPv6 クライアント モビリティの確認，（342 ページ）
IPv6 クライアント モビリティのモニタリング，（343 ページ）

IPv6 アドレス ラーニング

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定（SLAAC）
- ステートフル DHCPv6
- 静的設定

これらの方法の場合、IPv6 クライアントは常に NS DAD（重複アドレス検出）要求を送信して、ネットワークに重複する IP アドレスがないようにします。スイッチはクライアントの NDP および DHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習し、コントローラ データベースを更新します。データベースは、クライアントの新しい IP アドレスについて通知します。

関連トピック

IPv6 クライアント モビリティの確認, （342 ページ）
IPv6 クライアント モビリティのモニタリング, （343 ページ）

複数の IP アドレスの処理

RUN 状態後に新しい IP アドレスが受信されると、追加の場合も削除の場合も、コントローラは表示目的でそのローカル データベース上の新しい IP アドレスを更新します。基本的に、IPv6 は既存または IPv4 の場合と同じ PEM ステート マシン コード フローを使用します。IP アドレスが、たとえば、外部エンティティによって Prime Infrastructure から要求されると、コントローラは、すべての使用可能な IP アドレス、IPv4 および IPv6 を外部エンティティへの API/SPI インターフェイスに含めます。

IPv6 クライアントは、様々な目的でスタックから複数の IP アドレスを取得できます。たとえば、リンクローカル トラフィックのリンクローカル アドレスおよびルーティング可能な固有のローカル アドレスまたはグローバル アドレスがあります。

クライアントが DHCP 要求状態にあり、コントローラが IPv4 または IPv6 アドレス用にデータベースから最初の IP アドレスの通知を受信すると、PEM はクライアントを RUN 状態に移行させます。

RUN 状態後に新しい IP アドレスが受信されるときは、追加の場合も削除の場合も、コントローラは表示目的でそのローカル データベース上の新しい IP アドレスを更新します。

IP アドレスが、たとえば、外部エンティティによって Prime Infrastructure から要求されると、コントローラは、使用可能な IP アドレス、IPv4 および IPv6 を外部エンティティに提供します。

関連トピック

IPv6 クライアント モビリティの確認, （342 ページ）
IPv6 クライアント モビリティのモニタリング, （343 ページ）

IPv6 Configuration

スイッチは IPv4 クライアントと同様にシームレスに IPv6 クライアントをサポートします。管理者は、IPV6、IPv6 スヌーピングおよびスロットリング機能を有効にするには、Vlan を手動で設定する必要があります。これにより、スイッチとそのさまざまなクライアント間でのスロットリングを NDP パケットで行えます。

関連トピック

IPv6 クライアント モビリティの確認, （342 ページ）
IPv6 クライアント モビリティのモニタリング, （343 ページ）

ハイ アベイラビリティ

スイッチはクライアント IP アドレスが学習しにくいときにワイヤレス クライアントと同期します。スイッチオーバーが発生すると、IPv6 ネイバー バインディング テーブルがスタンバイ ステー

トに同期されます。ただし、スイッチオーバーが完了し、ネイバーバインディングテーブルがそのクライアントの最新情報で更新されると、ワイヤレス クライアント自体はアソシエート解除され、新しいアクティブ ステートに再アソシエートされます。

再アソシエーション時に、クライアントが他の AP に移動すると、バインディング テーブル内の元のエントリがしばらくの間ダウンとマークされ、期限切れになります。

別の AP からスイッチを結合する新しいエントリの場合は、新しい IP アドレスが学習されて、コントローラのデータベースに通知されます。

（注） この機能は、Cisco Catalyst 3850 スイッチでのみ使用できます。

関連トピック

IPv6 クライアント モビリティの確認, （342 ページ）
IPv6 クライアント モビリティのモニタリング, （343 ページ）

IPv6 クライアント モビリティの確認

表 9 に示すコマンドは、IPv6 クライアント モビリティに適用されます。

表 *24*：*Cisco 5760 WLC* の *IPv6* クライアント モビリティを確認するためのコマンド

コマンド	説明
debug mobility ipv6	すべてのワイヤレス クライアント IPv6 モビリティのデバッグをイネーブルにします。
debug **client** **mac-address** (mac-addr)	ワイヤレスクライアントのデバッグを表示します。デバッグ情報の MAC アドレスを入力します。

関連トピック

ルータ アドバタイズメントの使用, （339 ページ）
RA スロットリングと NS 抑制, （340 ページ）
IPv6 アドレス ラーニング, （340 ページ）
複数の IP アドレスの処理, （341 ページ）
IPv6 Configuration, （341 ページ）
ハイ アベイラビリティ, （341 ページ）
IPv6 クライアント モビリティのモニタリング, （343 ページ）

IPv6 クライアント モビリティのモニタリング

表 10 のコマンドは、スイッチスイッチで IPv6 クライアント モビリティをモニタリングするために使用されます。

表 *25* : *IPv6* クライアント モビリティ コマンドのモニタリング

コマンド	説明
show wireless client summary	アクティブなクライアントのワイヤレス固有設定を表示します。
show wireless client mac-address (mac-addr)	アクティブなクライアントのワイヤレス固有設定をそのMACアドレスに基づいて表示します。

関連トピック

IPv6 クライアント モビリティの確認, （342 ページ）
ルータ アドバタイズメントの使用, （339 ページ）
RA スロットリングと NS 抑制, （340 ページ）
IPv6 アドレス ラーニング, （340 ページ）
複数の IP アドレスの処理, （341 ページ）
IPv6 Configuration, （341 ページ）
ハイ アベイラビリティ, （341 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 Command Reference (Catalyst 3650 Switches)*
モビリティ設定	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

IPv6 クライアント モビリティの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 クライアント モビリティ機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 19 章

IPv6 モビリティの設定

- IPv6 モビリティの前提条件，347 ページ
- IPv6 モビリティについて，347 ページ
- IPv6 モビリティの設定方法，348 ページ
- IPv6 モビリティのモニタリング，348 ページ
- その他の参考資料，350 ページ
- IPv6 モビリティの機能情報，352 ページ

IPv6 モビリティの前提条件

モビリティとその関連のインフラストラクチャを設定して使用できるようにする必要があります。

IPv6 モビリティについて

モビリティ（ローミング）は、できるだけ低遅延で、確実かつスムーズに、あるアクセス ポイントから別のアクセス ポイントへのアソシエーションを維持する無線 LAN クライアントの機能です。この項では、スイッチが無線ネットワークに存在する場合のモビリティの動作について説明します。

あるワイヤレス クライアントがアクセス ポイントにアソシエートして認証すると、アクセス ポイントのスイッチは、クライアント データベースにそのクライアントに対するエントリを設定します。このエントリには、クライアントの MAC アドレス、IP アドレス、セキュリティ コンテキストおよびアソシエーション、Quality of Service（QoS）コンテキスト、WLAN、およびアソシエートされたアクセス ポイントが含まれます。スイッチはこの情報を使用してフレームを転送し、ワイヤレス クライアントで送受信されるトラフィックを管理します。

ワイヤレス クライアントがそのアソシエーションをあるアクセス ポイントから別のアクセス ポイントへ移動する場合、スイッチは新たにアソシエートするアクセス ポイントでクライアントのデータベースをアップデートするだけです。必要に応じて、新たなセキュリティ コンテキストと

アソシエーションも確立されます。しかし、クライアントが 1 つのスイッチに接続されたアクセスポイントから別のスイッチに接続されたアクセスポイントにローミングする際には、プロセスはより複雑になります。また、同一のサブネット上でこれらのスイッチが動作しているかどうかによっても異なります。

コントローラ間ローミング

クライアントが新たなスイッチに接続されたアクセス ポイントへアソシエートする場合、新たなスイッチはモビリティ メッセージを元のスイッチと交換し、スティッキアンカリングがディセーブルの場合に、クライアントのデータベース エントリは新たなスイッチに移動されます。

関連トピック

IPv6 モビリティのモニタリング, （348 ページ）

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

サブネット間ローミングは、スイッチがクライアントのローミングに関するモビリティ メッセージを交換する点でコントローラ間ローミングと似ています。ただし、クライアントのデータベース エントリを新しいスイッチに移動するのではなく、元のスイッチのクライアント データベース内で該当クライアントに「アンカー」エントリのマークが付けられます。このデータベース エントリが新しいスイッチのクライアント データベースにコピーされ、新しいスイッチ内で「外部」エントリのマークが付けられます。ローミングはワイヤレス クライアントには透過的なまま行われ、クライアントは元の IP アドレスを保持します。

サブネット間ローミングでは、アンカーと外部の両スイッチの WLAN に、ソースベースのルーティングやソースベースのファイアウォールは設定せずに同一のネットワーク アクセス権限を設定する必要があります。そのようにしない場合、ハンドオフ後クライアントにネットワーク接続上の問題が発生することがあります。

モビリティの設定の詳細については、『Cisco 5700 Wireless LAN Controller Mobility Configuration Guide, Cisco IOS XE, Release 3.2SE』を参照してください。

関連トピック

IPv6 モビリティのモニタリング, （348 ページ）

IPv6 モビリティの設定方法

IPv6 モビリティのモニタリング

この章では、モビリティ関連 IPv6 設定を表示します。モビリティ関連の設定を確認するには、『Cisco 5700 Wireless LAN Controller Mobility Configuration Guide, Cisco IOS XE 3.2SE』を参照してください。

手順の概要

1. **show ipv6 neighbors binding mac** C0C1.C06B.C4E2

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 neighbors binding mac** C0C1.C06B.C4E2 例： スイッチ# show ipv6 neighbors binding mac C0C1.C06B.C4E2	IPv6 関連のモビリティ設定を表示します。

```
スイッチ# show ipv6 neighbors binding mac C0C1.C06B.C4E2
Binding Table has 45 entries, 37 dynamic (limit 100)
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other Packet, API
- API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned

    IPv6 address                            Link-Layer addr Interface vlan prlvl  age
state    Time left
L   FE80:20:25::16                          2037.064C.BA71  Vl25        25  0100 3137mn
REACHABLE
L   FE80:20:24::16                          2037.064C.BA41  Vl24        24  0100 3137mn
REACHABLE
L   FE80:20:23::16                          2037.064C.BA44  Vl23        23  0100 3137mn
REACHABLE
ND  FE80:20:23::13                          2037.0653.6BC4  Te1/0/1     23  0005   85s
REACHABLE  223 s try 0
ND  FE80:20:22::17                          2037.064D.06F6  Te1/0/1     22  0005    3mn
REACHABLE  92 s try 0
L   FE80:20:22::16                          2037.064C.BA76  Vl22        22  0100 3137mn
REACHABLE
ND  FE80:20:22::13                          2037.0653.6BF6  Te1/0/1     22  0005  165s
REACHABLE  136 s try 0
ND  FE80:20:22::12                          2037.064C.94F6  Te1/0/1     22  0005   23s
REACHABLE  281 s try 0
ND  FE80:20:22::2                           0022.550E.8FC3  Te1/0/1     22  0005   18s
REACHABLE  295 s try 0
ND  FE80:20:21::17                          2037.064D.06E8  Te1/0/1     21  0005    4mn
REACHABLE  60 s try 0
L   FE80:20:21::16                          2037.064C.BA68  Vl21        21  0100 3137mn
REACHABLE
ND  FE80:20:21::13                          2037.0653.6BE8  Te1/0/1     21  0005   57s
REACHABLE  252 s try 0
ND  FE80:20:21::12                          2037.064C.94E8  Te1/0/1     21  0005    4s
REACHABLE  297 s
ND  FE80:20:21::2                           0022.550E.8FC2  Te1/0/1     21  0005    2s
REACHABLE  307 s try 0
ND  FE80::F866:8BE0:12E4:39CF               C0C1.C06B.C4E2  Ca4         21  0005    3mn
REACHABLE  89 s try 0
ND  FE80::6D0A:DB33:D69E:91C7               0050.B606.A6CE  Te1/0/1     22  0005  135s
REACHABLE  171 s try 0
ND  FE80::985:8189:9937:BB05                8CA9.8295.09CC  Ca0         21  0005   15s
REACHABLE  287 s
ND  FE80::20:24:13                          2037.0653.6BC1  Te1/0/1     24  0005  155s
REACHABLE  145 s try 0
L   2001:20:23::16                          2037.064C.BA44  Vl23        23  0100 3137mn
```

```
REACHABLE
DH  2001:20:22:0:C96C:AF29:5DDC:2689        0050.B606.A6CE  Te1/0/1     22  0024   19s
REACHABLE  286 s try 0(16574
DH  2001:20:22:0:A46B:90B2:F0DB:F952        0050.B606.A6CE  Te1/0/1     22  0024 2339mn
STALE      32401 s
DH  2001:20:22:0:7DFD:14EC:B1E4:1172        0050.B606.A6CE  Te1/0/1     22  0024 2339mn
STALE      24394 s
DH  2001:20:22:0:7CB3:D6DD:FD6A:50F         0050.B606.A6CE  Te1/0/1     22  0024 2333mn
STALE      29195 s
DH  2001:20:22:0:6D32:AF24:FDE1:2504        0050.B606.A6CE  Te1/0/1     22  0024  509mn
STALE      118821 s
DH  2001:20:22:0:5106:5AD:FE98:A2F0         0050.B606.A6CE  Te1/0/1     22  0024 2328mn
STALE      31362 s
ND  2001:20:22::201:13                      0050.B606.A6CE  Te1/0/1     22  0005   49s
REACHABLE  264 s try 0
L   2001:20:22::16                          2037.064C.BA76  Vl22        22  0100 3137mn
REACHABLE
ND  2001:20:22::13                          2037.0653.6BF6  Te1/0/1     22  0005  175s
REACHABLE  131 s try 0
ND  2001:20:22::2                           0022.550E.8FC3  Te1/0/1     22  0005   28s
REACHABLE  274 s try 0
ND  2001:20:21:0:F866:8BE0:12E4:39CF        C0C1.C06B.C4E2  Ca4         21  0005    4mn
REACHABLE  21 s try 0
ND  2001:20:21:0:C085:9D4C:4521:B777        0021.CC73.AA17  Te1/0/1     21  0005   11s
REACHABLE  290 s try 0
ND  2001:20:21:0:6233:4BFF:FE1A:744C        6033.4B1A.744C  Ca4         21  0005    3mn
REACHABLE  108 s try 0
ND  2001:20:21:0:447E:745D:2F48:1C68        8CA9.8295.09CC  Ca0         21  0005   34s
REACHABLE  276 s
ND  2001:20:21:0:3920:DDE8:B29:AD51         C0C1.C06B.C4E2  Ca4         21  0005    3mn
REACHABLE  87 s try 0
ND  2001:20:21:0:1016:A333:FAD5:6E66        0021.CC73.AA17  Te1/0/1     21  0005    4mn
REACHABLE  18 s try 0
ND  2001:20:21:0:C42:E317:BA9B:EB17         6033.4B1A.744C  Ca4         21  0005    4mn
REACHABLE  61 s try 0
ND  2001:20:21:0:985:8189:9937:BB05         8CA9.8295.09CC  Ca0         21  0005  135s
REACHABLE  173 s try 0
ND  2001:20:21::201:20                      0021.CC73.AA17  Te1/0/1     21  0005    4mn
REACHABLE  43 s try 0
ND  2001:20:21::17                          2037.064D.06E8  Te1/0/1     21  0005    4mn
REACHABLE  50 s try 0
L   2001:20:21::16                          2037.064C.BA68  Vl21        21  0100 3137mn
REACHABLE
ND  2001:20:21::13                          2037.0653.6BE8  Te1/0/1     21  0005   67s
REACHABLE  237 s try 0
ND  2001:20:21::12                          2037.064C.94E8  Te1/0/1     21  0005    5mn
REACHABLE  512 ms try 0
ND  2001:20:21::2                           0022.550E.8FC2  Te1/0/1     21  0005   12s
REACHABLE  294 s try 0
```

関連トピック

コントローラ間ローミング，（348 ページ）

スティッキ アンカリングでのサブネット内ローミング、およびサブネット間ローミング，（348 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 Command Reference (Catalyst 3650 Switches)*

関連項目	マニュアル タイトル
モビリティ設定	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

IPv6 モビリティの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 モビリティ機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 IV 部

IP

- HSRP の設定，355 ページ

第 20 章

HSRP の設定

- HSRP の設定，355 ページ

HSRP の設定

この章では、ホット スタンバイ ルータ プロトコル（HSRP）を使用する方法について説明します。これによって、IP トラフィック ルーティングに冗長性を提供し、個々のルータのアベイラビリティに依存しないルーティングを実現します。

レイヤ 2 モードの HSRP のバージョンを使用すると、クラスタ コマンド スイッチが故障した場合、クラスタ管理を引き継ぐ冗長コマンド スイッチを設定することもできます。

機能情報の確認

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

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

HSRP の設定に関する情報

HSRP の概要

HSRP は、デフォルト ゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファースト ホップ冗長性を確保することでネットワークのアベイラビリティを高めるシスコの標準方式です。HSRP を使用すると、特定のルータのアベイラビリティに依存せず IP トラフィックをルーティングできます。また、一連のルータ インターフェイスを組み合わせることで、1 台の仮想ルー

タ、または LAN 上のホストへのデフォルト ゲートウェイのように機能させることができます。ネットワークまたはセグメント上に HSRP を設定すると、仮想 MAC（メディア アクセス コントロール）アドレス、および設定されたルータ グループ間で共有されるIPアドレスを使用できるようになりHSRP が設定された複数のルータは、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスを使用できるようになります。仮想ルータは、実際には存在しません。仮想ルータは、相互にバックアップ機能を提供するように設定されている複数のルータの共通のターゲットを表します。1 台のルータがアクティブなルータとして、もう 1 台のルータがスタンバイ ルータとして選択されます。スタンバイ ルータは、指定されたアクティブ ルータが故障した場合に、グループの MAC アドレスおよび IP アドレスを制御するルータです。

（注） HSRP グループ内のルータには、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）など、HSRP をサポートする任意のルータ インターフェイスを指定できます。

HSRPは、ネットワーク上のホストからのIPトラフィックに冗長性を提供することで、ネットワークのアベイラビリティを高めます。アクティブ ルータは、ルータ インターフェイスのグループ内でパケットのルーティングを実行するために選択されたルータです。スタンバイ ルータは、アクティブ ルータが故障した場合、または事前に設定した条件が満たされた場合に、ルーティング作業を引き継ぐルータです。

HSRP は、ホストがルータ ディスカバリ プロトコルをサポートしておらず、選択されたルータのリロードや電源故障時に新しいルータに切り替えることができない場合に有効です。HSRPをネットワーク セグメントに設定すると、HSRP は仮想 MAC アドレスと IP アドレスを 1 つずつ提供します。このアドレスは、HSRP が動作するルータ インターフェイス グループ内のルータ インターフェイス間で共有できます。プロトコルによってアクティブ ルータとして選択されたルータは、グループの MAC アドレス宛てのパケットを受信し、ルーティングします。n 台のルータで HSRP が稼働している場合、n +1 個の IP アドレスおよび MAC アドレスが割り当てられます。

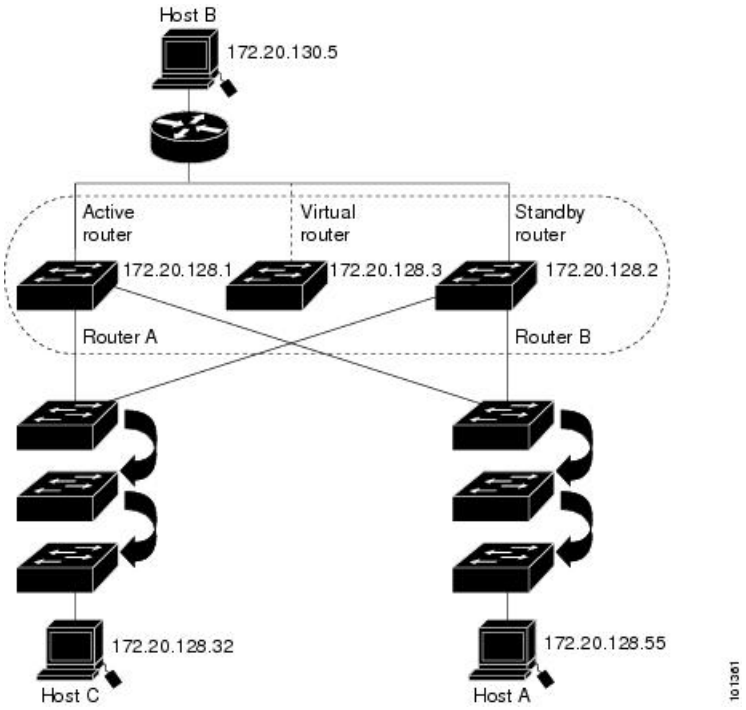
指定されたアクティブ ルータの故障を HSRP が検出すると、選択されているスタンバイ ルータがホットスタンバイ グループの MAC アドレスおよび IP アドレスの制御を引き継ぎます。この時点で新しいスタンバイ ルータも選択されます。HSRP が稼働しているデバイスは、マルチキャスト UDP ベースの hello パケットを送受信することにより、ルータ障害の検出、アクティブ ルータおよびスタンバイ ルータの指定を行います。インターフェイスに HSRP が設定されている場合、そのインターフェイスではインターネット制御メッセージプロトコル（ICMP）のリダイレクト メッセージが自動的にイネーブルになっています。

レイヤ 3 で動作するスイッチおよびスイッチ スタック間で複数のホット スタンバイ グループを設定すると、冗長ルータをさらに活用できます。そのためには、インターフェイスに設定するホットスタンバイ コマンド グループごとにグループ番号を指定します。たとえば、スイッチ 1 のインターフェイスをアクティブ ルータ、スイッチ 2 のインターフェイスをスタンバイ ルータとして設定できます。また、スイッチ 2 の別のインターフェイスをアクティブ ルータ、スイッチ 1 の別のインターフェイスをスタンバイ ルータとして設定することもできます。

次の図に、HSRP用に設定されたネットワークのセグメントを示します。各ルータには、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスが設定されています。ルータ A の IP アドレスをネットワーク上のホストに設定する代わりに、デフォルトルータとして仮想ルータのIPアドレスを設定します。ホスト C からホスト B にパケットが送信される場合、ホスト C は仮想ルータの MAC アドレスにパケットを送信します。何らかの理由により、ルータ A がパケットの転送を

停止すると、ルータ B が仮想 IP アドレスおよび仮想 MAC アドレスに応答してアクティブ ルータとなり、アクティブ ルータの作業を行います。ホスト C は引き続き仮想ルータの IP アドレスを使用し、ホスト B 宛のパケットをアドレッシングします。ルータ B はそのパケットを受信し、ホスト B に送信します。ルータ B は HSRP の機能を使用し、ルータ A が動作を再開するまで、ホスト B のセグメント上のユーザと通信する必要があるホスト C のセグメント上のユーザに連続的にサービスを提供します。また、ホスト A セグメントとホスト B の間で、引き続き通常のパケット処理機能を実行します。

図 *13*：*HSRP* の一般的な構成



レイヤ 3 で動作するスイッチおよびスイッチ スタック間で複数のホット スタンバイ グループを設定すると、冗長ルータをさらに活用できます。そのためには、インターフェイスに設定するホットスタンバイ コマンド グループごとにグループ番号を指定します。たとえば、スイッチ 1 のインターフェイスをアクティブ ルータ、スイッチ 2 のインターフェイスをスタンバイ ルータとして設定できます。また、スイッチ 2 の別のインターフェイスをアクティブ ルータ、スイッチ 1 の別のインターフェイスをスタンバイ ルータとして設定することもできます。

HSRP のバージョン

Cisco IOS XE Release 3.3SE 以降の製品は、下記のホットスタンバイ ルータ プロトコル（HSRP）バージョンをサポートしています。

スイッチでは、次の HSRP バージョンがサポートされます。

- HSRPv1：HSRP のバージョン 1（デフォルトのバージョン）。次の機能があります。
  - HSRP グループ番号は 0 ～ 255 まで使用できます。

- HSRPv1 は 224.0.0.2 のマルチキャスト アドレスを使用して hello パケットを送信しますが、これは Cisco Group Management Protocol（CGMP）の脱退処理と競合します。HSRPv1 と CGMP は相互に排他的なため、同時には使用できません。

- HSRPv2：HSRP のバージョン 2。このバージョンには次の機能があります。
  - HSRPv2 は 224.0.0.102 のマルチキャスト アドレスを使用して hello パケットを送信します。HSRPv2 と CGMP 脱退処理は相互に排他的ではありません。同時に使用できます。
  - HSRPv2 のパケット形式は、HSRPv1 とは異なります。

HSRPv1 を実行しているスイッチは、ルータの送信元 MAC アドレスが仮想 MAC アドレスのため、hello パケットを送信した物理的なルータを特定できません。

HSRPv2 のパケット形式は、HSRPv1 とは異なります。HSRPv2 パケットは、パケットを送信した物理ルータの MAC アドレスを格納できる 6 バイトの識別子フィールドを持った、Type Length Value（TLV）形式を使用します。

HSRPv1 を実行しているインターフェイスが HSRPv2 パケットを取得した場合、このタイプ フィールドは無視されます。

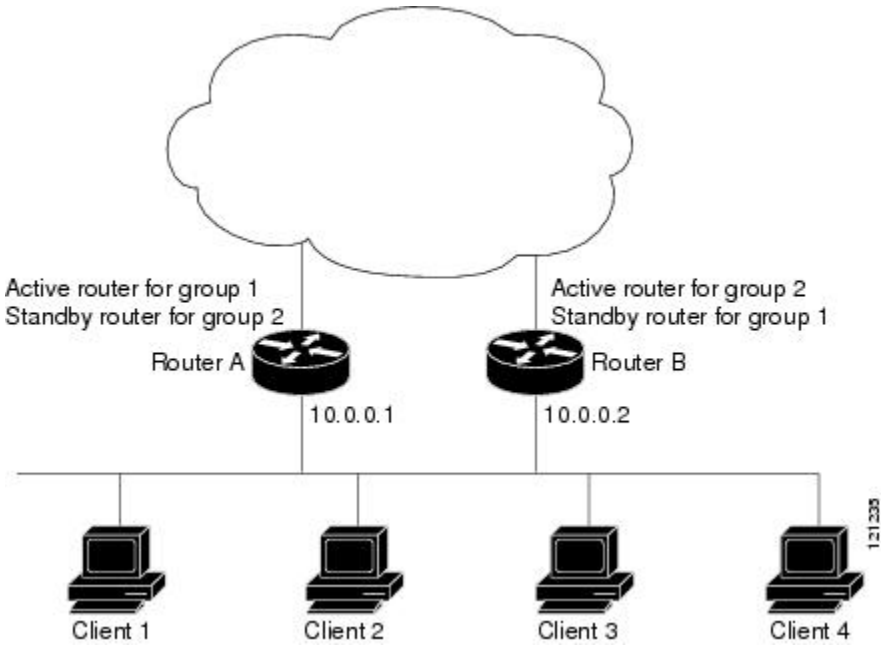
MHSRP

スイッチは、Multiple HSRP（MHSRP）をサポートします。MHSRP は HSRP の拡張版で、複数の HSRP グループ間でのロード シェアリングが可能です。ホスト ネットワークからサーバ ネットワークまで、ロードバランシングを実現して複数のスタンバイ グループ（およびパス）を使用するために、MHSRP を設定できます。

下の図では、半分のクライアントがルータ A に設定されており、もう半分はルータ B に設定されています。ルータ A およびルータ B の設定により、合計 2 つの HSRP グループが確立されています。グループ 1 では、ルータ A に最高のプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブ ルータになり、ルータ B がスタンバイ ルータとなります。グループ 2 では、ルータ B に最も高いプライオリティが割り当てられているため、ルータ B がデフォルトのアクティブ ルータであり、ルータ A がスタンバイ ルータです。通常の運用では、2 つのルータが IP トラフィック負荷を分散します。いずれかのルータが使用できなくなると、もう一方のルータがアクティブになり、使用できないルータのパケット転送機能を引き継ぎます。

（注） MHSRP では、ルータに障害が発生して正常に戻った場合にプリエンプションによりロード シェアリングを復元するために、**standby preempt** インターフェイス コンフィギュレーション コマンドを HSRP インターフェイスで入力する必要があります。

図 *14*：*MSHRP* ロード シェアリング



SSO HSRP

SSO HSRP は、冗長なルート プロセッサ（RP）を装備したデバイスがステートフル スイッチオーバー（SSO）冗長モード用に設定されているときの HSRP の動作を変更します。ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。

この機能を使用すると、HSRP の SSO 情報がスタンバイ RP に同期されるため、HSRP 仮想 IP アドレスを使用して送信されるトラフィックをスイッチオーバー中も引き続き転送できるほか、データの損失やパスの変更も発生しません。さらに、HSRP アクティブ デバイスの両方の RP に障害が発生しても、スタンバイ状態の HSRP デバイスが HSRP アクティブ デバイスとして処理を引き継ぎます。

この機能は、動作の冗長モードが SSO に設定されている場合にデフォルトでイネーブルになっています。

HSRP およびスイッチ スタック

HSRP の hello メッセージは、スタック マスターで生成されます。HSRP がアクティブであるスタック マスターに障害が発生すると、HSRP アクティブ ステートのフラッピングが生じることが

あります。これは、新規スタック マスターが選択および初期化されている間に HSRP hello メッセージが生成されず、スタック マスターが故障したあとでないとスタンバイ ルータがアクティブにならない可能性があるためです。

IPv6 の HSRP の設定

IPServices および IPBase フィーチャ セットを実行中のスイッチは、IPv6 のホットスタンバイ ルータ プロトコル（HSRP）をサポートします。HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。IPv6 ホストは、IPv6 ネイバー探索ルータのアドバタイズメント メッセージによって使用可能なルータを学習します。これらのメッセージは定期的にマルチキャストされるか、ホストにより送信請求されます。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカル アドレスがあります。

HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

（注） IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2（HSRPv2）をイネーブルにする必要があります。

HSRP の設定方法

HSRP のデフォルト設定

表 *26*：*HSRP* のデフォルト設定

機能	デフォルト設定
HSRP バージョン	バージョン 1
HSRP グループ	未設定
スタンバイ グループ番号	0
スタンバイ MAC アドレス	0000.0c07.acXX に指定されたシステム。XX は、HSRP グループ番号
スタンバイ プライオリティ	100
スタンバイ遅延	0（遅延なし）
スタンバイでのインターフェイスプライオリティの追跡	10

機能	デフォルト設定
スタンバイ hello 時間	3 秒
スタンバイ ホールドタイム	10 秒

HSRP HSRP 設定時の注意事項

- HSRPv2 および HSRPv1 は相互に排他的です。HSRPv2 は、同じインターフェイス上で HSRPv1 と一緒には動作しません（その逆も同様）。
- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - ルーテッド ポート：インターフェイス コンフィギュレーション モードで **no switchport** コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。
  - SVI：グローバル コンフィギュレーション モードで **interface vlan***vlan_id* によって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
  - レイヤ 3 モードの Etherchannel ポート チャネル：グローバル コンフィギュレーション モードで **interface port-channel***port-channel-number* を使用し、イーサネット インターフェイスをチャネル グループにバインドして作成されたポートチャネル論理インターフェイスです。
- すべてのレイヤ 3 インターフェイスに IP アドレスを割り当てる必要があります。
-
- インターフェイスの HSRP バージョンを変更する場合、HSRP グループは新しい MAC アドレスを持つことになるため、リセットされます。
- 有効なグループ番号、無効なグループ番号の例：
- 2、150、225 の番号でグループを設定する場合、3850 の番号を持つ他のグループは設定できません。これは、0 ～ 255 の範囲内ではありません。
- 520、600、700 の番号でグループを設定する場合、900 の番号を持つ他のグループは設定できません。これは、512 ～ 767 の範囲内ではありません。

HSRP のイネーブル化

インターフェイス コンフィギュレーション コマンド **standby ip** は、設定されているインターフェイスで HSRP をアクティブ化します。IP アドレスを指定した場合は、IP アドレスがホットスタンバイ グループの指定アドレスとして使用されます。IP アドレスを指定しなかった場合は、スタンバイ機能によってアドレスが学習されます。指定アドレスを使用し、LAN 上に少なくとも 1 つのレイヤ 3 ポートを設定する必要があります。IP アドレスを設定すると、常に、現在使用されている別の指定アドレスが、設定した IP アドレスに変更されます。

standby ip コマンドがインターフェイス上でイネーブルに設定され、プロキシ ARP がイネーブルの場合、インターフェイスのホットスタンバイ ステートがアクティブになると、プロキシ ARP 要

求に対する応答は、ホットスタンバイ グループの MAC アドレスを使用して実行されます。インターフェイスが別のステートの場合、プロキシ ARP の応答は抑制されます。

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **standby version**{**1**| **2**}
4. **standby**[*group-number*] **ip**[*ip-address* [**secondary**]]
5. **end**
6. **show standby**[*interface-id*[*group*]]
7. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	インターフェイス コンフィギュレーション モードを開始し、HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	**standby version**{**1**| **2**} 例： `Switch(config-if)# standby version 1`	（任意）インターフェイスに HSRP バージョンを設定します。 • 1：HSRPv1 を選択します。 • 2：HSRPv2 を選択します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、インターフェイスはデフォルトの HSRP バージョンである HSRPv1 を実行します。
ステップ 4	**standby**[*group-number*] **ip**[*ip-address* [**secondary**]] 例： `Switch(config-if)# standby 1 ip`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）group-number：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）ip-address：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮

	コマンドまたはアクション	目的
		想IPアドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります
ステップ 6	**show standby**[*interface-id*[*group*]] 例： `Switch # show standby`	スタンバイ グループの設定を確認します。
ステップ 7	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

HSRP のプライオリティの設定

standby priority, **standby preempt**、および **standby track** インターフェイス コンフィギュレーション コマンドはいずれも、アクティブ ルータとスタンバイ ルータを検索するための特性、および新しいアクティブ ルータが処理を引き継いだ場合の動作を設定するために使用できます。

HSRP プライオリティを設定する場合の注意事項は、次のとおりです。

- プライオリティを割り当てておくと、アクティブ ルータおよびスタンバイ ルータを選択できます。プリエンプションがイネーブルの場合は、プライオリティが最高のルータがアクティブルータになります。プライオリティが等しい場合は、現在アクティブなルータに変更はありません。
- 最大の値（1～255）が、最高のプライオリティ（アクティブルータになる確率が最も高い）を表します。

- プライオリティ、プリエンプト、またはその両方を設定するときは、少なくとも 1 つのキーワード（**priority**、**preempt**、または両方）を指定する必要があります。
- インターフェイスが **standby track** コマンドによって設定されている場合、ルータ上の別のインターフェイスがダウンすると、デバイスのプライオリティが動的に変更されることもあります。
- **standby track** インターフェイス コンフィギュレーション コマンドを実行すると、ルータのホットスタンバイ プライオリティとインターフェイスのアベイラビリティが関連付けられます。この機能は、HSRP用に設定されていないインターフェイスを追跡する場合に有効です。追跡対象のインターフェイスが故障すると、トラッキングが設定されているデバイスのホットスタンバイ プライオリティが10減少します。追跡対象でないインターフェイスの場合は、そのステートが変わっても、設定済みデバイスのホットスタンバイ プライオリティは変わりません。ホットスタンバイ用に設定されたインターフェイスごとに、追跡するインターフェイスのリストを個別に設定できます。
- **standby track***interface-priority* インターフェイス コンフィギュレーション コマンドを実行すると、追跡対象のインターフェイスがダウンした場合のホットスタンバイ プライオリティの減少幅を指定できます。インターフェイスが稼働状態に戻ると、プライオリティは同じ分だけ増加します。
- *interface-priority* 値が設定されている場合に、複数の追跡対象インターフェイスがダウンすると、設定済みプライオリティの減少幅が累積されます。プライオリティ値が設定されていない追跡対象インターフェイスが故障した場合、デフォルトの減少幅は 10 です。この値は累積されません。
- インターフェイスに対してルーティングを最初にイネーブルにした時点で、完全なルーティング テーブルは存在しません。このインターフェイスがプリエンプトに設定されている場合はアクティブ ルータになりますが、十分なルーティング処理はできません。この問題を解決するには、ルータがルーティング テーブルを更新できるように遅延時間を設定します。

インターフェイスに HSRP プライオリティ特性を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **standby** [*group-number*] **priority***priority*
4. **standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
5. **standby** [*group-number*] **track** *type number*[*interface-priority*]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	インターフェイス コンフィギュレーション モードを開始し、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3	**standby** [*group-number*] **priority***priority* 例： `Switch(config-if)# standby 120 priority 50`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）group-number：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 4	**standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デ

	コマンドまたはアクション	目的
		フォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	**standby** [*group-number*] **track** *type number*[*interface-priority*] 例： `Switch(config-if)# standby track interface gigabitethernet1/1/1`	他のインターフェイスを追跡するようにインターフェイスを設定します。この設定により、他のインターフェイスの 1 つがダウンした場合は、そのデバイスのホットスタンバイ プライオリティが減少します。 • （任意）group-number：コマンドが適用されるグループ番号です。 • type：追跡対象のインターフェイスタイプを（インターフェイス番号とともに）入力します。 • number：追跡対象のインターフェイス番号を（インターフェイスタイプとともに）入力します。 • （任意）interface-priority：インターフェイスがダウンした場合、または稼働状態に戻った場合に、ルータのホットスタンバイ プライオリティを減少または増加させる幅を入力します。デフォルト値は 10 です。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MHSRP の設定

MHSRP およびロードバランシングをイネーブルにするには、MHSRP の項の *MHSRP* ロードシェアリングの図に示したように、グループのアクティブ ルータとして 2 つのルータを設定し、スタンバイ ルータとして仮想ルータを設定します。ルータに障害が発生して正常に戻った場合、プリエンプションを発生させてロードバランシングを復元するために、**standby preempt** インターフェ

イス コンフィギュレーション コマンドをそれぞれの HSRP インターフェイスで入力する必要があります。

ルータ A はグループ 1 のアクティブ ルータとして、ルータ B はグループ 2 のアクティブ ルータとして設定されています。ルータ A の HSRP インターフェイスの IP アドレスは 10.0.0.1、グループ 1 のスタンバイ プライオリティは 110（デフォルトは 100）です。ルータ B の HSRP インターフェイスの IP アドレスは 10.0.0.2、グループ 2 のスタンバイ プライオリティは 110 です。

グループ 1 は仮想 IP アドレス 10.0.0.3 を使用し、グループ 2 は仮想 IP アドレス 10.0.0.4 を使用します。

ルータ *A* の設定

手順の概要

1. **configure terminal**
2. **interface***type number*
3. **no switchport**
4. **ip address***ip-address mask*
5. **standby**[*group-number*]**ip**[*ip-address*[**secondary**]]
6. **standby** [*group-number*] **priority***priority*
7. **standby**[*group-number*] **preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
8. **standby**[*group-number*]**ip**[*ip-address*[**secondary**]]
9. **standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***type number* 例： `Switch (config)# interface gigabitethernet1/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** 例： `Switch (config)# no switchport`	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。

	コマンドまたはアクション	目的
ステップ 4	**ip address***ip-address mask* 例： `Switch (config-if)# 10.0.0.1 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby**[*group-number*]**ip**[*ip-address*[**secondary**]] 例： `Switch (config-if)# standby 1 ip 10.0.0.3`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 6	**standby** [*group-number*] **priority***priority* 例： `Switch(config-if)# standby 1 priority 110`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
ステップ 7	**standby**[*group-number*] **preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 8	**standby**[*group-number*]**ip**[*ip-address*[**secondary**]] 例： `Switch (config-if)# standby 2 ip 10.0.0.4`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のイ

	コマンドまたはアクション	目的
		ンターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 9	**standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] 例： `Switch(config-if)# standby 2 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルータ *B* の設定

手順の概要

1. **configure terminal**
2. **interface***type number*
3. **no switchport**
4. **ip address***ip-address mask*
5. **standby**[*group-number*]**ip**[*ip-address*[**secondary**]]
6. **standby** [*group-number*] **priority***priority*
7. **standby**[*group-number*] **preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
8. **standby**[*group-number*]**ip**[*ip-address*[**secondary**]]
9. **standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***type number* 例： `Switch (config)# interface gigabitethernet1/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**no switchport** 例： `Switch (config)# no switchport`	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 4	**ip address***ip-address mask* 例： `Switch (config-if)# 10.0.0.2 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby**[*group-number*]**ip**[*ip-address*[**secondary**]] 例： `Switch (config-if)# standby 1 ip 10.0.0.3`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 6	**standby** [*group-number*] **priority***priority* 例： `Switch(config-if)# standby 1 priority 110`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルトプライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。

	コマンドまたはアクション	目的
		デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 7	**standby**[*group-number*] **preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 8	**standby**[*group-number*]**ip**[*ip-address*[**secondary**]] 例： `Switch (config-if)# standby 2 ip 10.0.0.4`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。

	コマンドまたはアクション	目的
		少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 9	**standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] 例： `Switch(config-if)# standby 2 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

HSRP 認証およびタイマーの設定

HSRP 認証ストリングを設定したり、hello タイム インターバルやホールドタイムを変更することもできます。

これらの属性を設定する場合の注意事項は次のとおりです。

- 認証ストリングはすべての HSRP メッセージで暗号化されずに送信されます。相互運用できるように、接続されたすべてのルータおよびアクセス サーバに同じ認証ストリングを設定する必要があります。認証ストリングが一致しないと、HSRP によって設定された他のルータから、指定されたホットスタンバイ IP アドレスおよびタイマー値を学習できません。
- スタンバイ タイマー値が設定されていないルータまたはアクセス サーバは、アクティブ ルータまたはスタンバイ ルータからタイマー値を学習できます。アクティブ ルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。
- ホットスタンバイ グループのすべてのルータで、同じタイマー値を使用する必要があります。通常、*holdtime* は *hellotime* の 3 倍以上です。

インターフェイスに HSRP の認証とタイマーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **standby**[*group-number*] **authentication***string*
4. **standby**[*group-number*]**timers***hellotimeholdtime*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config) # interface gigabitethernet1/0/1`	インターフェイス コンフィギュレーション モードを開始し、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3	**standby**[*group-number*] **authentication***string* 例： `Switch(config-if) # standby 1 authentication word`	（任意）**authentication***string*：すべての HSRP メッセージで伝達されるストリングを入力します。認証ストリングには 8 文字までを指定できます。デフォルトのストリングは **cisco** です。 （任意）*group-number*：コマンドが適用されるグループ番号です。
ステップ 4	**standby**[*group-number*]**timers***hellotimeholdtime* 例： `Switch(config-if) # standby 1 timers 5 15`	（任意）hello パケット間隔、およびアクティブ ルータのダウンを他のルータが宣言するまでの時間を設定します。 • *group-number*：コマンドが適用されるグループ番号です。 • （任意）*hellotime*：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • *holdtime*：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。
ステップ 5	**end** 例： `Switch(config-if) # end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ICMP リダイレクト メッセージの HSRP サポートのイネーブル化

HSRP が設定されたインターフェイスでは、ICMP リダイレクト メッセージが自動的にイネーブルになります。ICMP は、エラーをレポートするためのメッセージ パケットや IP 処理に関連する他の情報を提供する、ネットワーク層インターネット プロトコルです。ICMP には、ホストへのエラー パケットの方向付けや送信などの診断機能があります。この機能は、HSRP を介した発信 ICMP リダイレクト メッセージをフィルタリングします。HSRP では、ネクスト ホップ IP アドレスが HSRP 仮想 IP アドレスに変更される可能性があります。詳細については、『Cisco IOS IP Configuration Guide, Release 12.4』を参照してください。

HSRP グループおよびクラスタリングの設定

デバイスが HSRP スタンバイ ルーティングに参加し、クラスタリングがイネーブルの場合は、同じスタンバイ グループを使用して、コマンド スイッチの冗長性および HSRP の冗長性を確保できます。同じ HSRP スタンバイ グループをイネーブルにし、コマンド スイッチおよびルーティングの冗長性を確保するには、**cluster standby-group***HSRP-group-name* [**routing-redundancy**] グローバル コンフィギュレーション コマンドを使用します。**routing-redundancy** キーワードを指定せずに同じ HSRP スタンバイ グループ名でクラスタを作成すると、そのグループに対する HSRP スタンバイ ルーティングはディセーブルになります。

HSRP の確認

HSRP コンフィギュレーションの確認

HSRP 設定を表示するには、次の特権 EXEC モードで次のコマンドを使用します。

show standby[*interface-id*[*group*]][**brief**][**detail**]

スイッチ全体、特定のインターフェイス、HSRP グループ、またはインターフェイスの HSRP グループに関する HSRP 情報を表示できます。HSRP 情報の概要または詳細のいずれを表示するかを指定することもできます。デフォルト表示は **detail** です。多数の HSRP グループがある場合に、修飾子を指定しないで **show standby** コマンドを使用すると、正確に表示されないことがあります。

```
Switch #show standby
VLAN1 - Group 1
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.182
Hot standby IP address is 172.20.128.3 configured
Active router is 172.20.128.1 expires in 00:00:09
Standby router is local
Standby virtual mac address is 0000.0c07.ac01
Name is bbb

VLAN1 - Group 100
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.262
Hot standby IP address is 172.20.138.51 configured
```

```
Active router is 172.20.128.1 expires in 00:00:09
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac64
Name is test
```

HSRP の設定例

HSRP のイネーブル化：例

次に、インターフェイスのグループ 1 で HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、HSRP を使用して学習されます。

（注） これは、HSRP をイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch # show standby
```

HSRP のプライオリティの設定：例

次に、ポートをアクティブにして、IP アドレスおよびプライオリティ 120（デフォルト値よりも高いプライオリティ）を設定して、アクティブ ルータになるまで 300 秒（5 分間）待機する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
Switch # show standby
```

MHSRP の設定：例

次に、*MHSRP* ロードシェアリングの図で示したMHSRP設定をイネーブルにする例を示します。

ルータ A の設定

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

ルータ B の設定

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 1 priority 110
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

HSRP 認証およびタイマーの設定：例

次に、グループ 1 のホットスタンバイ ルータを相互運用させるために必要な認証ストリングとして、word を設定する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

次に、hello パケット間隔が 5 秒、ルータがダウンしたと見なされるまでの時間が 15 秒となるように、スタンバイ グループ 1 のタイマーを設定する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

HSRP グループおよびクラスタリングの設定：例

次に、スタンバイ グループ my_hsrp をクラスタにバインドし、同じ HSRP グループをイネーブルにしてコマンド スイッチおよびルータの冗長性に使用する例を示します。このコマンドを実行できるのは、コマンドスイッチに対してだけです。スタンバイ グループの名前または番号が存在しない場合、またはスイッチがクラスタ メンバー スイッチである場合は、エラー メッセージが表示されます。

```
Switch # configure terminal
Switch(config) # cluster standby-group my_hsrp routing-redundancy
Switch(config-if)# end
```

HSRP の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
RFC 2281	『Cisco Hot Standby Router Protocol』

MIB

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

シスコのテクニカル サポート

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

HSRP の設定に関する機能情報

表 *27* : *HSRP* の設定に関する機能情報

リリース	機能情報
3SE	この機能が導入されました

第 V 部

レイヤ 2/3

- スパニングツリー プロトコルの設定，385 ページ
- 複数のスパニング ツリー プロトコルの設定，419 ページ
- オプションのスパニングツリー機能の設定，463 ページ
- EtherChannel の設定，493 ページ
- 単方向リンク検出の設定，535 ページ

第 21 章

スパニングツリー プロトコルの設定

- 機能情報の確認，385 ページ
- STP の制約事項，385 ページ
- スパニング ツリー プロトコルに関する情報，386 ページ
- スパニングツリー機能の設定方法，401 ページ
- スパニングツリー ステータスのモニタリング，415 ページ
- スパニング ツリー プロトコルに関する追加情報，416 ページ
- STP の機能情報，417 ページ

機能情報の確認

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

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

STP の制約事項

- ルート スイッチとしてスイッチを設定しようとする場合、ルート スイッチにするために必要な値が 1 未満だと、失敗します。
- ネットワークが、拡張システム ID をサポートするスイッチとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするスイッチがルート スイッチになる可能性は低くなります。古いソフトウェアを実行している接続スイッチのプライオリティより

VLAN 番号が大きい場合は常に、拡張システム ID によってスイッチ プライオリティ値が増加します。

- 各スパニングツリー インスタンスのルート スイッチは、バックボーンまたはディストリビューション スイッチでなければなりません。アクセス スイッチをスパニングツリー プライマリ ルートとして設定しないでください。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

関連トピック

ルート スイッチの設定（CLI），（403 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID，（389 ページ）
スパニングツリー トポロジと BPDU，（387 ページ）
接続を維持するためのエージング タイムの短縮，（396 ページ）

スパニング ツリー プロトコルに関する情報

スパニングツリー プロトコル

スパニングツリー プロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークが正常に動作するには、任意の 2 つのステーション間で存在できるアクティブ パスは 1 つだけです。エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンド ステーションにメッセージが重複して到着する可能性があります。スイッチは、複数のレイヤ 2 インターフェイスのエンド ステーション MAC アドレスを学習する可能性もあります。このような状況によって、ネットワークが不安定になります。スパニングツリーの動作は透過的であり、エンド ステーション側で、単一 LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STP は、スパニングツリー アルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のスイッチを 1 つ選択します。アルゴリズムは、次に基づき、各ポートにロールを割り当て、スイッチド レイヤ 2 ネットワークを介して最良のループフリー パスを算出します。アクティブ トポロジでのポートの役割：

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているスイッチ、またはバックアップの役割が指定されているスイッチはルート スイッチです。 少なくとも *1* つのポートに役割が指定されているスイッチは、指定スイッチを意味します。

冗長データ パスはスパニングツリーによって、強制的にスタンバイ（ブロックされた）ステートにされます。スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリーアルゴリズムがスパニングツリートポロジを再計算し、スタンバイ パスをアクティブにします。スイッチは、スパニングツリー フレーム （ブリッジ プロトコル データ ユニット（BPDU）と呼ばれる）を定期間隔で送受信します。スイッチはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。 BPDU には、スイッチおよび MAC アドレス、スイッチの優先順位、ポートの優先順位、およびパス コストを含む、送信側スイッチとそのポートに関する情報が含まれます。スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート スイッチおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

スイッチの 2 つのポートがループの一部である場合、 spanning-tree および、パス コスト設定は、どのポートがフォワーディング ステートになるか、およびどのポートがブロッキング ステートになるかを制御します。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。The コスト値は、メディア速度を表します。

（注） デフォルトではスイッチは、Small Form-Factor Pluggable（SFP）モジュールを備えていないインターフェイスにだけ、（接続が稼働していることを確認するために）キープアライブ メッセージを送信します。[**no**] **keepalive** インターフェイス コンフィギュレーション コマンドをキーワードなしで入力すると、インターフェイスのデフォルトを変更できます。

スパニングツリー トポロジと BPDU

スイッチドネットワーク内の安定したアクティブ スパニングツリートポロジは、次の要素によって制御されます。

- スイッチ上の各 VLAN に関連付けられた一意のブリッジ ID（スイッチ プライオリティおよびMACアドレス）。スイッチ スタックでは、ある特定のスパニングツリー インスタンスに対して、すべてのスイッチが同一のブリッジ ID を使用します。
- ルート スイッチに対するスパニングツリー パス コスト。
- 各レイヤ2インターフェイスに対応付けられたポートID（ポートプライオリティおよびMACアドレス）。

ネットワーク内のスイッチに電源が入ると、各機能はルート スイッチとして機能します。各スイッチは、そのすべてのポートからコンフィギュレーション BPDU を送信します。BPDU によって通信が行われ、スパニングツリー トポロジが計算されます。各設定BPDU には、次の情報が含まれています。

- 送信スイッチがルート スイッチとして識別するスイッチの一意のブリッジ ID
- ルートまでのスパニングツリー パス コスト
- 送信スイッチのブリッジ ID

- メッセージ エージ
- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

スイッチは、優位な情報（より小さいブリッジID、より低いパス コストなど）が含まれているコンフィギュレーション BPDU を受信すると、そのポートに対する情報を保存します。この BPDU をスイッチのルート ポート上で受信した場合、そのスイッチが指定スイッチとなっているすべての接続 LAN に、更新したメッセージを付けて BPDU を転送します。

スイッチは、そのポートに現在保存されている情報よりも下位の情報を含むコンフィギュレーション BPDU を受信した場合は、その BPDU を廃棄します。スイッチが下位 BPDU を受信した LAN の指定スイッチである場合、そのポートに保存されている最新情報を含む BPDU をその LAN に送信します。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- ネットワーク内の1つのスイッチがとして選択されます。ルート スイッチ（スイッチドネットワークのスパニングツリートポロジーの論理的な中心）。箇条書きの項目の下の図を参照してください。

  VLAN ごとに、スイッチ プライオリティが最も高い（最も小さい数字の優先順位の値）スイッチがルート スイッチとして選択されます。すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合、VLAN 内で MAC アドレスの最も小さいスイッチがルート スイッチになります。スイッチのプライオリティ値は、次の図のようにブリッジ ID の最上位ビットを占めます。

- スイッチごとに（ルート スイッチを除く）、ルート ポートが 1 つ選択されます。このポートは、スイッチからルート スイッチにパケットを転送するときに最適パス（最小コスト）を提供します。

  スイッチ スタックのルート ポートを選択する場合には、スパニング ツリーは次の順序に従います。

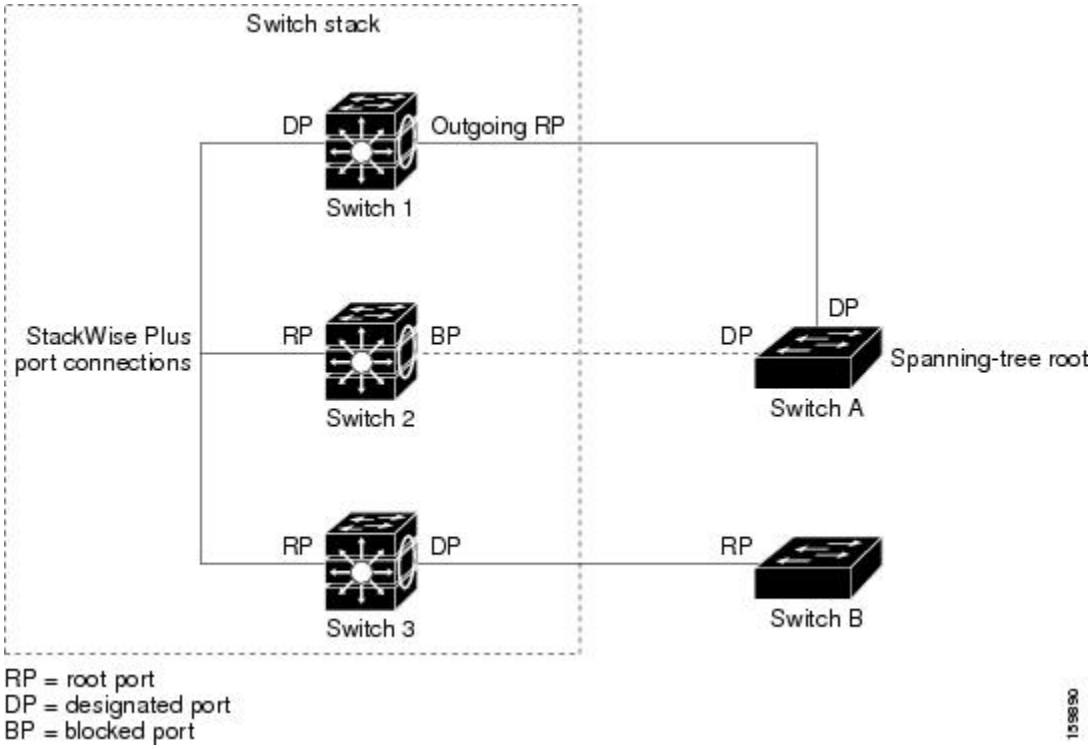
  - 最も低いルート ブリッジ ID を選択
  - ルート スイッチへの最も低いパス コストを選択
  - 最も低い代表ブリッジ ID を選択
  - 最も低い代表パス コストを選択
  - 最も低いポート ID を選択

- スタック ルート スイッチ上の1つの発信ポートだけが、ルート ポートとして選択されます。スタック内の残りのスイッチは、次の図に示すように指定スイッチになります（スイッチ 2 およびスイッチ 3）。
- ルート スイッチへの最短距離は、パス コストに基づいてスイッチごとに計算されます。

- LAN セグメントごとに指定スイッチが選択されます。指定スイッチは、その LAN からルート スイッチにパケットを転送するときの最小パス コストを提供します。DP は、指定スイッチが LAN に接続されているポートです。

1 つのスタック メンバーがスタック ルート スイッチとして選択されます。スタック ルート スイッチには出力ルート ポート（スイッチ 1）が含まれます。

図 *15*：スイッチ スタックのスパニング ツリー ポート ステート



スイッチドネットワーク上のいずれの地点からもルート スイッチに到達する場合に必要のないパスはすべて、スパニングツリー ブロッキング モードになります。

関連トピック

ルート スイッチの設定（CLI），（403 ページ）
STP の制約事項，（385 ページ）

ブリッジ ID、デバイス プライオリティ、および拡張システム ID

IEEE 802.1D 標準では、それぞれのスイッチに固有のルート スイッチの選択を制御するブリッジ識別子（ブリッジ ID）が必要です。各 VLAN は PVST+ と Rapid PVST+ によって異なる論理ブリッジと見なされるので、同一のスイッチは設定された各 VLAN とは異なるブリッジ ID を保有している必要があります。スイッチ上の各 VLAN には一意の 8 バイト ブリッジ ID が設定されます。上位の 2 バイトはスイッチ プライオリティに使用され、残りの 6 バイトがスイッチの MAC アドレスから取得されます。

スイッチではIEEE 802.1tスパニングツリー拡張機能がサポートされ、従来はスイッチプライオリティに使用されていたビットの一部がVLAN IDとして使用されるようになりました。その結果、スイッチに割り当てられるMACアドレスが少なくなり、より広い範囲のVLAN IDをサポートできるようになり、しかもブリッジIDの一意性を損なうこともありません。

従来はスイッチ プライオリティに使用されていた2バイトが、4ビットのプライオリティ値と12ビットの拡張システムID値（VLAN IDと同じ）に割り当てられています。

表 *28*：デバイス プライオリティ値および拡張システム *ID*

プライオリティ値				拡張システム ID（VLAN ID と同設定）										
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニングツリーは、ブリッジIDをVLANごとに一意にするために、拡張システムID、スイッチプライオリティ、および割り当てられたスパニングツリーMACアドレスを使用します。スイッチ スタックは他のネットワークからは単一のスイッチとして認識されるため、スタック内のすべてのスイッチは、指定のスパニングツリーに対して同一のブリッジIDを使用します。スタック マスターに障害が発生した場合、スタック メンバは新しいスタック マスターの新しいMACアドレスに基づいて、実行中のすべてのスパニングツリーのブリッジIDを再計算します。

拡張システムIDのサポートにより、ルートスイッチ、セカンダリルートスイッチ、およびVLANのスイッチ プライオリティの手動での設定方法に影響が生じます。たとえば、スイッチのプライオリティ値を変更すると、スイッチがルート スイッチとして選定される可能性も変更されることになります。大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。

指定されたVLANのルート スイッチに24576に満たないスイッチ プライオリティが設定されている場合は、スイッチはそのVLANについて、自身のプライオリティを最小のスイッチプライオリティより4096だけ小さい値に設定します4096は、表に示すように4ビット スイッチ スイッチ プライオリティ値の最下位ビットの値です。

関連トピック

ルート スイッチの設定（CLI），（403 ページ）
STP の制約事項，（385 ページ）
ルート スイッチの設定（CLI），（443 ページ）
ルート スイッチ，（423 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

ポート プライオリティとパス コスト

ループが発生した場合、スパニングツリーはポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプラ

イオリティ値（高い数値）を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

スパニングツリー パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、スパニングツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスに同じコスト値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

スイッチがスイッチ スタックのメンバーの場合は、最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには（ポート プライオリティを調整せずに）大きいコスト値を与えます。詳細については、関連項目を参照してください。

関連トピック

ポート プライオリティの設定（CLI），（407 ページ）
パス コストの設定（CLI），（408 ページ）

スパニングツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジーの変化が発生します。インターフェイスがスパニングツリートポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成されることがあります。インターフェイスは新しいトポロジ情報がスイッチドLAN上で伝播されるまで待機し、フレーム転送を開始する必要があります。インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

スパニングツリーを使用しているスイッチの各レイヤ 2 インターフェイスは、次のいずれかのステートになります。

- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：インターフェイスをフレーム転送に関与させることをスパニングツリーが決定した場合、ブロッキング ステートから最初に移行するステートです。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニングツリーに含まれません。シャットダウンポートであるか、ポート上にリンクがないか、またはポート上でスパニングツリーインスタンスが稼働していないためです。

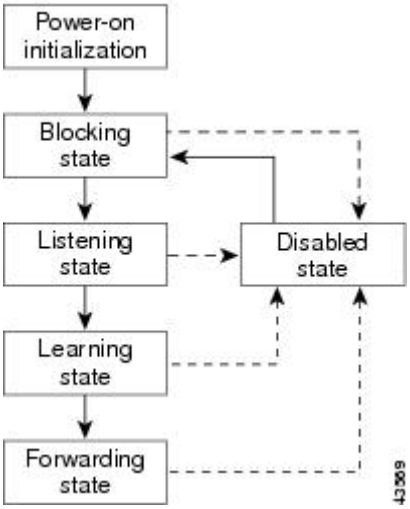
インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング

- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

インターフェイスはこれらのステート間を移動します。

図 *16*：スパニングツリー インターフェイス ステート



デフォルト設定では、スイッチを起動するとスパニングツリーがイネーブルになります。その後、スイッチの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。スパニングツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. スパニングツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニング ステートになります。
2. スパニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートの間、スイッチが転送データベースのエンド ステーションの位置情報を学習しているとき、インターフェイスはフレーム転送をブロックし続けます。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 インターフェイスはフレームの転送に関与しません。初期化後、スイッチの各インターフェイスに BPDU が送信されます。スイッチは最初、他のスイッチと BPDUを交換するまで、ルートとして動作します。この交換により、ネットワーク内でどのスイッチがルートまたはルート スイッチになるかが確立されます。ネットワーク内にスイッチが 1 つしかない場合は交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニング ステートになります。インターフェイスはスイッチの初期化後、必ずブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、ブロッキング ステートを経て、レイヤ2インターフェイスが最初に移行するステートです。インターフェイスがリスニング ステートになるのは、スパニングツリーによってそのインターフェイスのフレーム転送への関与が決定された場合です。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ 2 インターフェイスは、フレームの転送に関与できるように準備します。インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 インターフェイスは、フレームを転送します。インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ブロッキング ステートのレイヤ 2 インターフェイスは、フレームの転送やスパニングツリーに関与しません。ディセーブル ステートのインターフェイスは動作不能です。

ディセーブル インターフェイスは、次の機能を実行します。

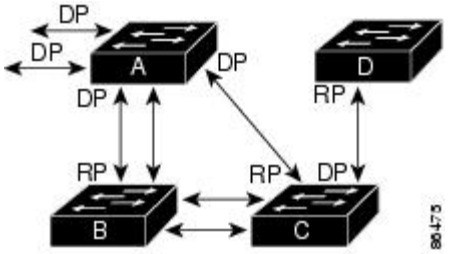
- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

スイッチ またはポートがルート スイッチまたはルート ポートになる仕組み

ネットワーク上のすべてのスイッチがデフォルトのスパニングツリー設定でイネーブルになっている場合、最小の MAC アドレスを持つスイッチがルート スイッチになります。

スイッチ A はルート スイッチとして選択されます。すべてのスイッチのスイッチのプライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最も小さいためです。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、スイッチ A が最適なルート スイッチとは限りません。ルート スイッチになるように、最適なスイッチのプライオリティを引き上げる（数値を引き下げる）と、スパニングツリーの再計算が強制的に行われ、最適なスイッチをルートとした新しいトポロジが形成されます。

図 *17*：スパニングツリー トポロジ



RP = Root Port
DP = Designated Port

スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチドネットワークの送信元エンドステーションから宛先エンドステーションまでのパスが最適にならない場合があります。たとえば、ルート ポートよりプライオリティの高いインターフェイスに高

速リンクを接続すると、ルート ポートが変更される可能性があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチBのあるポートがギガビット イーサネット リンクで、スイッチ上の別のポート（10/100 リンク）がルート ポートであると仮定します。ネットワーク トラフィックはギガビット イーサネット リンクに流す方が効率的です。ギガビット イーサネット ポートのスパニングツリー ポート プライオリティをルート ポートより高くする（数値を小さくする）と、ギガビット イーサネット ポートが新しいルート ポートになります。

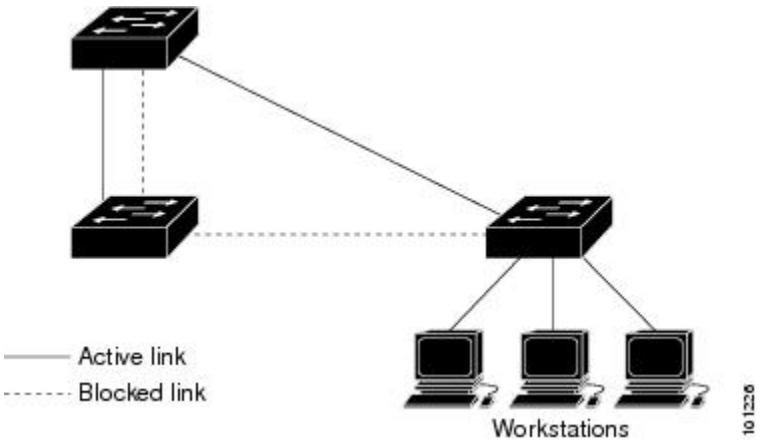
関連トピック

ポート プライオリティの設定（CLI），（407 ページ）

スパニングツリーおよび冗長接続

2 つのスイッチ インターフェイスを別の 1 台のデバイス、または 2 台の異なるデバイスに接続することにより、スパニングツリーを使用して冗長バックボーンを作成できます。スパニングツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合にはそのディセーブルにしていた方をイネーブルにします。一方のリンクが高速で、他方が低速の場合、必ず、低速の方のリンクがディセーブルになります。速度が同じ場合、ポート プライオリティとポート ID が加算され、最大値を持つリンクがスパニングツリーによってディセーブルにされます。

図 *18*：スパニングツリーおよび冗長接続



EtherChannel グループを使用して、スイッチ間に冗長リンクを設定することもできます。

スパニングツリー アドレスの管理

IEEE 802.1D では、各種ブリッジ プロトコルに使用させるために、0x00180C2000000 ～ 0x0180C2000010 の範囲で 17 のマルチキャスト アドレスが規定されています。これらのアドレスは削除できないスタティック アドレスです。

スパニングツリー ステートに関係なく、スタック内の各スイッチは 0x0180C2000000 ～ 0x0180C2000000 のアドレス宛てのパケットを受信しますが、転送は行いません。

スパニングツリーがイネーブルの場合、スイッチまたはスタック内の各スイッチの CPU は 0x0180C2000000 および 0x0180C2000010 宛てのパケットを受信します。スパニングツリーがディセーブルの場合は、スイッチまたはスタック内の各スイッチは、それらのパケットを不明のマルチキャスト アドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミック アドレスのエージング タイムはデフォルトで 5 分です。これは、**mac-address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルトの設定です。ただし、スパニングツリーの再構成により、多数のステーションの位置が変更されることがあります。このようなステーションは、再構成中、5分以上にわたって到達できないことがあるので、アドレステーブルからステーション アドレスを削除し、改めて学習できるように、アドレス エージング タイムが短縮されます。スパニングツリー再構成時に短縮されるエージング タイムは、転送遅延パラメータ値（**spanning-tree vlan** *vlan-id* **forward-time** *seconds* グローバル コンフィギュレーション コマンド）と同じです。

各 VLAN はそれぞれ独立したスパニングツリー インスタンスであるため、スイッチは VLAN 単位でエージング タイムを短縮します。ある VLAN でスパニングツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスがエージング タイム短縮の対象になります。他の VLAN のダイナミック アドレスは影響を受けず、スイッチで設定されたエージング間隔がそのまま保持されます。

関連トピック

ルート スイッチの設定（CLI），（403 ページ）
STP の制約事項，（385 ページ）

スパニングツリー モードおよびプロトコル

このスイッチでサポートされるモードおよびプロトコルは、次のとおりです。

- PVST+：このスパニングツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。PVST+ はスイッチ上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリー パスを提供します。

  PVST+ は、対象となる VLAN にレイヤ 2 ロード バランシングを提供します。ネットワーク上の VLAN を使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリンクを使用できるようにします。VLAN 上の PVST+ インスタンスごとに、それぞれ 1 つのルート スイッチがあります。このルート スイッチは、その VLAN に対応するスパニングツリー情報を、ネットワーク上の他のすべてのスイッチに伝送します。このプロセスにより、各スイッチがネットワークに関する共通の情報を持つため、ネットワーク トポロジが確実に維持されます。

- Rapid PVST+：このスパニングツリー モードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。15.2(4) E リリース以降、STP のデフォルト モードは Rapid PVST+ です。高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変

更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージング タイムが使用されます。

Rapid PVST+ は PVST+ と同じ設定を使用しているので（特に明記する場合を除く）、スイッチで必要なことは最小限の追加設定のみです。Rapid PVST+ の利点は、大規模な PVST+ のインストール ベースを Rapid PVST+ に移行する際に、複雑なマルチ スパニングツリー プロトコル（MSTP）設定の学習やネットワーク再設定の必要がないことです。Rapid PVST+ モードでは、各 VLAN は独自のスパニングツリー インスタンスを最大数実行します。

- MSTP：このスパニングツリー モードは IEEE 802.1s 標準に準拠しています。複数の VLAN を同一のスパニングツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要となるスパニングツリーインスタンスの数を減らすことができます。MSTP は Rapid Spanning-Tree Protocol（RSTP）（IEEE 802.1w 準拠）上で実行され、転送遅延を解消し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行することにより、スパニングツリーの高速コンバージェンスを可能にします。スイッチ スタックでは、クロス スタック高速移行（CSRT）機能が RSTP と同じ機能を実行します。RSTP または CSRT を使用しなければ、MSTP は稼働できません。

関連トピック

スパニングツリー モードの変更（CLI），（401 ページ）

サポートされるスパニングツリー インスタンス

PVST+ または Rapid PVST+ モードでは、スイッチまたはスイッチ スタックは最大 128 のスパニングツリー インスタンスをサポートします。

MSTP モードでは、スイッチまたはスイッチ スタックは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

関連トピック

スパニング ツリーのディセーブル化（CLI），（402 ページ）
スパニングツリー機能のデフォルト設定，（400 ページ）
MSTP のデフォルト設定，（439 ページ）

スパニングツリーの相互運用性と下位互換性

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree（CST）のルートは MST バックボーンの内側に配置する必要があり、PVST+ スイッチを複数の MST リージョンに接続することはできません。

ネットワーク内に Rapid PVST+ を実行しているスイッチと PVST+ を実行しているスイッチが存在する場合、Rapid PVST+ スイッチと PVST+ スイッチを別のスパニングツリー インスタンスに設定することを推奨します。Rapid PVST+ スパニングツリー インスタンスでは、ルート スイッチは Rapid PVST+ スイッチでなければなりません。PVST+ インスタンスでは、ルート スイッチは PVST+

スイッチでなければなりません。PVST+ スイッチはネットワークのエッジに配置する必要があります。

すべてのスタック メンバーが、同じバージョンのスパニングツリーを実行します（すべてPVST+、すべて Rapid PVST+、またはすべて MSTP）。

表 *29*：*PVST+*、*MSTP*、*Rapid PVST+* の相互運用性と互換性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり（制限あり）	あり（PVST+ に戻る）
MSTP	あり（制限あり）	あり	あり（PVST+ に戻る）
Rapid PVST+	あり（PVST+ に戻る）	あり（PVST+ に戻る）	あり

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）
MSTP 設定時の注意事項，（422 ページ）
MST リージョン，（424 ページ）

STP および IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニングツリー ストラテジに一定の制限を設けています。この規格では、トランク上で使用できるすべての VLAN に対して、1 つのスパニングツリー インスタンスしか認められません。ただし、IEEE 802.1Q トランクを介して接続される Cisco スイッチのネットワークにおいて、スイッチはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。

IEEE 802.1Q トランクを介して Cisco スイッチを他社製のデバイスに接続する場合、Cisco スイッチは PVST+ を使用してスパニングツリーの相互運用性を実現します。Rapid PVST+ がイネーブルの場合、スイッチは PVST+ ではなく Rapid PVST+ を使用します。スイッチは、トランクの IEEE 802.1Q VLAN のスパニングツリー インスタンスと他社の IEEE 802.1Q スイッチのスパニングツリー インスタンスを結合します。

ただし、PVST+ または Rapid PVST+ の情報はすべて、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離された Cisco スイッチによって維持されます。Cisco スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

PVST+ は IEEE 802.1Q トランクで自動的に有効になるので、ユーザ側で設定する必要はありません。アクセス ポートおよび ISL（スイッチ間リンク）トランク ポートでの外部スパニングツリーの動作は、PVST+ の影響を受けません。

VLAN ブリッジ スパニングツリー

シスコ VLANブリッジ スパニングツリーは、フォールバック ブリッジング機能（ブリッジ グループ）で使用し、DECnet などの IP 以外のプロトコルを 2 つ以上の VLAN ブリッジ ドメインまたはルーテッド ポート間で伝送します。VLAN ブリッジ スパニングツリーにより、ブリッジ グループは個々の VLAN スパニングツリーの上部にスパニングツリーを形成できるので、VLAN 間で複数の接続がある場合に、ループが形成されないようにします。また、ブリッジングされている VLAN からの個々のスパニングツリーが単一のスパニングツリーに縮小しないようにする働きもします。

VLANブリッジ スパニングツリーをサポートするには、一部のスパニングツリー タイマーを増やします。フォールバック ブリッジング機能を使用するには、スイッチで IP サービス フィーチャ セットをイネーブルにする必要があります。

スパニング ツリーとスイッチ スタック

スイッチ スタックが PVST+ または Rapid PVST+ モードで動作している場合：

- スイッチ スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが与えられたスパニングツリーに同一のブリッジ ID を使用します。ブリッジ ID は、アクティブ スイッチの MAC アドレスから取得されます。
- 新しいスイッチがスタックに加わると、そのスイッチは、アクティブ スイッチのブリッジ ID を自分のブリッジ ID として設定します。新しく追加されたスイッチの ID が最も小さく、ルート パス コストがすべてのスタック メンバー間で同じ場合は、新しく追加されたスイッチがスタック ルートになります。
- スタック メンバがスタックから除外されると、スタック内でスパニングツリーの再コンバージェンスが発生します（スタック外で発生する場合もあります）。残っているスタック メンバのうち最も低いスタック ポート ID を持つスタック メンバが、スタック ルートになります。
- スイッチ スタック外にあるネイバー スイッチに障害が発生したか、またはその電源が停止した場合、通常のスパニングツリー処理が発生します。スパニングツリーの再コンバージェンスは、アクティブなトポロジ内のスイッチが失われたことにより発生する場合もあります。
- スイッチ スタック外にある新しい スイッチがネットワークに追加された場合、通常のスパニングツリー処理が発生します。スパニングツリーの再コンバージェンスは、ネットワークにスイッチが追加されたことにより発生する場合もあります。

スパニングツリー機能のデフォルト設定

表 *30*：スパニングツリー機能のデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル
スパニングツリー モード	Rapid PVST+（PVST+ と MSTP はディセーブル）
スイッチ プライオリティ	32768
スパニングツリーポートプライオリティ（インターフェイス単位で設定可能）	128
スパニングツリーポートコスト（インターフェイス単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリーVLANポートプライオリティ（VLAN単位で設定可能）	128
スパニングツリーVLANポートコスト（VLAN単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー タイマー	hello タイム：2 秒 転送遅延時間：15 秒 最大エージング タイム：20 秒 転送保留カウント：6 BPDU

（注） リリース 15.2(4) E 以降では、STP のデフォルト モードは Rapid PVST+ です。

関連トピック

スパニング ツリーのディセーブル化（CLI），（402 ページ）
サポートされるスパニングツリー インスタンス，（397 ページ）

スパニングツリー機能の設定方法

スパニングツリー モードの変更（CLI）

スイッチは次の 3 つのスパニングツリー モードをサポートします。Per-VLAN Spanning-Tree Plus（PVST+）、Rapid PVST+、またはマルチ スパニングツリー プロトコル（MSTP）。デフォルトでは、スイッチは Rapid PVST+ プロトコルを実行します。

デフォルト モード以外のモードをイネーブルにする場合、この手順は必須です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**}
4. **interface***interface-id*
5. **spanning-tree link-type point-to-point**
6. **end**
7. **clear spanning-tree detected-protocols**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mode** {**pvst**	**mst**	**rapid-pvst**} 例： スイッチ(config)# **spanning-tree mode pvst**	スパニングツリー モードを設定します。すべてのスタック メンバーは、同じバージョンのスパニング ツリーを実行します。 • PVST+ をイネーブルにするには、**pvst** を選択します。 • MSTP をイネーブルにするには、**mst** を選択します。 • **rapid-pvst** を選択して、Rapid PVST+ をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**interface***interface-id* 例： スイッチ(config)# **interface GigabitEthernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。VLAN ID の範囲は 1 ～ 4094 です。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 5	**spanning-tree link-type point-to-point** 例： スイッチ(config-if)# **spanning-tree link-type point-to-point**	このポートのリンク タイプがポイントツーポイントであることを指定します。 このポート（ローカル ポート）をポイントツーポイント リンクでリモート ポートと接続し、ローカル ポートが指定ポートになると、スイッチはリモート ポートとネゴシエーションし、ローカル ポートをフォワーディング ステートにすばやく変更します。
ステップ 6	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**clear spanning-tree detected-protocols** 例： スイッチ# **clear spanning-tree detected-protocols**	スイッチ上のいずれかのポートが IEEE 802.1D レガシー スイッチ上のポートに接続されている場合は、このコマンドによりスイッチ全体のプロトコル移行プロセスを再開します。 このステップは、このスイッチで Rapid PVST+ が稼働していることを指定スイッチが検出する場合のオプションです。

関連トピック

スパニングツリー モードおよびプロトコル，（396 ページ）

スパニング ツリーのディセーブル化（CLI）

スパニングツリーはデフォルトで、VLAN 1 およびスパニングツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。スパニングツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。

注意 スパニングツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **no spanning-tree vlan***vlan-id*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree vlan***vlan-id* 例： `スイッチ(config)# no spanning-tree vlan 300`	*vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

関連トピック

サポートされるスパニングツリー インスタンス，（397 ページ）
スパニングツリー機能のデフォルト設定，（400 ページ）

ルート スイッチの設定（CLI）

特定の VLAN でスイッチをルートとして設定するには、**spanning-tree vlan***vlan-id***root** グローバル コンフィギュレーション コマンドを使用して、スイッチプライオリティをデフォルト値（32768）から、それより大幅に小さい値に変更します。このコマンドを入力すると、ソフトウェアが各

VLAN について、ルート スイッチのスイッチ プライオリティを確認します。拡張システム ID をサポートするため、スイッチは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、このスイッチを指定された VLAN のルートに設定できます。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大スイッチ ホップ カウント）を指定するには、**diameter** キーワードを使用します。ネットワーク直径を指定すると、スイッチはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree vlan***vlan-id***root primary** [**diameter***net-diameter*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan***vlan-id***root primary** [**diameter***net-diameter* 例： `スイッチ(config)# spanning-tree vlan 20-24 root primary diameter 4`	指定された VLAN のルートになるように、スイッチを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 •（任意）**diameter***net-diameter* には、任意の 2 つのエンド ステーション間の最大スイッチ数を指定します。範囲は 2 ～ 7 です。

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

次の作業

ルート スイッチとしてスイッチを設定した後で、**spanning-tree vlan***vlan-id***hello-time**、**spanning-tree vlan***vlan-id***forward-time**、および **spanning-tree vlan***vlan-id***max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、および最大エージング タイムを手動で設定することは推奨できません。

関連トピック

ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （389 ページ）
スパニングツリー トポロジと BPDU, （387 ページ）
接続を維持するためのエージング タイムの短縮, （396 ページ）
STP の制約事項, （385 ページ）

セカンダリ ルート デバイスの設定（CLI）

スイッチをセカンダリ ルートとして設定すると、スイッチプライオリティがデフォルト値（32768）から 28672 に変更されます。このプライオリティでは、スイッチがプライマリ ルート スイッチが失敗した場合の、指定された VLAN のルートスイッチになる可能性があります。ここでは、その他のネットワーク スイッチが、デフォルトのスイッチ プライオリティの 32768 を使用しているためにルート スイッチになる可能性が低いことが前提となっています。

このコマンドを複数のスイッチに対して実行すると、複数のバックアップルート スイッチを設定できます。**spanning-tree vlan***vlan-id***root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree vlan***vlan-id***root secondary** [**diameter***net-diameter*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan***vlan-id***root secondary** [**diameter***net-diameter* 例： スイッチ(config)# **spanning-tree vlan 20-24 root secondary diameter 4**	指定された VLAN のセカンダリ ルートになるように、スイッチを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）**diameter***net-diameter* には、任意の 2 つのエンド ステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。 プライマリ ルート スイッチを設定したときと同じネットワーク直径を使用してください。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

ポート プライオリティの設定（CLI）

（注） スイッチがスイッチ スタックのメンバである場合、**spanning-tree** [**vlan** *vlan-id*] **port-priority***priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree** [**vlan** *vlan-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させるインターフェイスには、低いコスト値を割り当て、最後に選択させるインターフェイスには高いコスト値を割り当てます。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree port-priority***priority*
5. **spanning-treevlan***vlan-id***port-priority***priority*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）です。

	コマンドまたはアクション	目的
ステップ 4	**spanning-tree port-priority***priority* 例： スイッチ(config-if)# **spanning-tree port-priority 0**	インターフェイスのポート プライオリティを設定します。 *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 5	**spanning-treevlan***vlan-id***port-priority***priority* 例： スイッチ(config-if)# **spanning-tree vlan 20-25 port-priority 0**	VLAN のポート プライオリティを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 6	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

関連トピック

ポート プライオリティとパス コスト，（390 ページ）

スイッチ またはポートがルート スイッチまたはルート ポートになる仕組み，（394 ページ）

パス コストの設定（CLI）

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree cost***cost*
5. **spanning-tree vlan***vlan-id***cost***cost*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）です。
ステップ 4	**spanning-tree cost***cost* 例： スイッチ(config-if)# **spanning-tree cost 250**	インターフェイスのコストを設定します。 ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**spanning-tree vlan***vlan-id***cost***cost* 例： スイッチ(config-if)# **spanning-tree vlan 10,12-15,20 cost 300**	VLAN のコストを設定します。 ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一

	コマンドまたはアクション	目的
		連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 6	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-treeinterface*interface-id* 特権 EXEC コマンドで情報が表示されるのは、リンクアップ動作可能の状態にあるポートに限られます。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティとパス コスト，（390 ページ）

VLAN のデバイス プライオリティの設定（CLI）

スイッチプライオリティを設定して、スタンドアロンスイッチまたはスタックにあるスイッチがルート スイッチとして選択される可能性を高めることができます。

（注） このコマンドの使用には注意してください。スイッチのプライオリティを変更する場合は通常、**spanning-tree vlan***vlan-id***root primary** および **spanning-tree vlan***vlan-id***root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree vlan***vlan-id***priority***priority*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan***vlan-id***priority***priority* 例： スイッチ(config)# **spanning-tree vlan 20 priority 8192**	VLAN のスイッチ プライオリティの設定 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。この値が低いほど、スイッチがルート スイッチとして選択される可能性が高くなります。 有効なプライオリティ値は4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。その他の値はすべて拒否されます。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

hello タイムの設定（CLI）

helloタイムはルートスイッチによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

手順の概要

1. **enable**
2. **spanning-tree vlan***vlan-id***hello-time***seconds*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**spanning-tree vlan***vlan-id***hello-time***seconds* 例： スイッチ(config)# **spanning-tree vlan 20-24 hello-time 3**	VLAN の hello タイムを設定します。hello タイムはルート スイッチによって設定メッセージが生成されて送信される時間の間隔です。このメッセージは、スイッチが活動中であることを表します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

VLAN の転送遅延時間の設定（CLI）

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree vlan***vlan-id***forward-time***seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan***vlan-id***forward-time***seconds* 例： スイッチ(config)# **spanning-tree vlan 20,25 forward-time 18**	VLAN の転送時間を設定します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

VLAN の最大エージング タイムの設定（CLI）

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree vlan***vlan-id***max-age***seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan***vlan-id***max-age***seconds* 例： スイッチ(config)# **spanning-tree vlan 20 max-age 30**	VLAN の最大エージング タイムを設定します。最大エージング タイムは、スイッチが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

転送保留カウントの設定（CLI）

転送保留カウント値を変更することで、BPDU のバースト サイズを設定できます。

（注） このパラメータをより高い値に変更すると、（特に Rapid PVST+ モードで）CPU の使用率に大きく影響します。逆に、この値を低く設定すると、セッションによってはコンバージェンスを抑えることができます。この値は、デフォルト設定で使用することを推奨します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree transmit hold-count***value*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree transmit hold-count***value* 例： スイッチ(config)# **spanning-tree transmit hold-count 6**	1 秒間停止する前に送信できる BPDU 数を設定します。 *value* に指定できる範囲は 1 ～ 20 です。デフォルト値は 6 です。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

スパニングツリー ステータスのモニタリング

表 *31*：スパニングツリー ステータス表示用のコマンド

show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。

show spanning-tree vlan *vlan-id*	指定した VLAN のスパニング ツリー情報を表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree interface *interface-id* **portfast**	指定したインターフェイスのスパニングツリー portfast 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。またはSTP ステートセクションのすべての行を表示します。

スパニングツリー カウンタをクリアするには、**clear spanning-tree** [**interface** i*nterface-id*] 特権 EXEC コマンドを使用します。

スパニング ツリー プロトコルに関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	*LAN Switching Command Reference, Cisco IOS XE Release 3SE（Catalyst 3650 Switches）*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

STP の機能情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 22 章

複数のスパニングツリープロトコルの設定

- 機能情報の確認，419 ページ
- MSTP の前提条件，419 ページ
- MSTP の制約事項，420 ページ
- MSTP について，421 ページ
- MSTP 機能の設定方法，440 ページ
- MSTP に関する追加情報，460 ページ
- MSTP の機能情報，461 ページ

機能情報の確認

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

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

MSTP の前提条件

- 2 つ以上のスイッチを同じマルチ スパニングツリー（MST）リージョンに設定するには、その 2 つに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

- 2 つ以上のスタックされたスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。
- ネットワーク内の冗長パスでロード バランシングを機能させるには、すべての VLAN/インスタンスマッピングの割り当てが一致している必要があります。一致していないと、すべてのトラフィックが 1 つのリンク上で伝送されます。パス コストを手動で設定することで、スイッチ スタック全体にわたりロード バランシングを実現できます。
- Per-VLAN Spanning-Tree Plus（PVST+）と MST クラウドの間、または Rapid- PVST+ と MST クラウドの間でロード バランシングが機能するためには、すべての MST 境界ポートがフォワーディングでなければなりません。MST クラウドの内部スパニング ツリー（IST）マスターが共通スパニング ツリー（CST）のルートである場合、MST境界ポートはフォワーディングです。MST クラウドが複数の MST リージョンから構成されている場合、いずれかの MST リージョンに CST ルートを含める必要があり、その他すべての MST リージョンに、PVST+ クラウドまたは高速 PVST+ クラウドを通るパスよりも、MST クラウド内に含まれるルートへのパスが良くする必要があります。クラウド内のスイッチを手動で設定しなければならない場合もあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）
MSTP 設定時の注意事項，（422 ページ）
MST リージョン，（424 ページ）

MSTP の制約事項

- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。
- スイッチ スタックは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。
- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは 1 つのバージョンだけです（たとえば、すべての VLAN で PVST+ を実行する、すべての VLAN で Rapid PVST+ を実行する、またはすべての VLAN で MSTP を実行します）。
- MST コンフィギュレーションの VLAN トランキング プロトコル（VTP）伝搬はサポートされません。ただし、コマンドライン インターフェイス（CLI）または簡易ネットワーク管理プロトコル（SNMP）サポートを通じて、MST リージョン内の各スイッチで MST コンフィギュレーション（リージョン名、リビジョン番号、およびVLANとインスタンスのマッピング）を手動で設定することは可能です。
- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。

- リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバーで構成されます。リージョンの各メンバーは高速スパニングツリー プロトコル（RSTP）ブリッジ プロトコル データ ユニット（BPDU）を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリー インスタンスの数は 65 までです。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。
- スイッチをルート スイッチとして設定した後に、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定することは推奨できません。

表 *32*：*PVST+*、*MSTP*、*Rapid PVST+* の相互運用性と互換性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり（制限あり）	あり（PVST+ に戻る）
MSTP	あり（制限あり）	あり	あり（PVST+ に戻る）
Rapid PVST+	あり（PVST+ に戻る）	あり（PVST+ に戻る）	あり

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）
MSTP 設定時の注意事項，（422 ページ）
MST リージョン，（424 ページ）
ルート スイッチの設定（CLI），（443 ページ）
ルート スイッチ，（423 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

MSTP について

MSTP の設定

高速コンバージェンスのために RSTP を使用する MSTP では、複数の VLAN をグループ化して同じスパニングツリーインスタンスにマッピングすることが可能で、多くの VLAN をサポートするのに必要なスパニングツリー インスタンスの数を軽減できます。MSTP は、データ トラフィックに複数の転送パスを提供し、ロードバランシングを実現して、多数の VLAN をサポートするのに必要なスパニングツリー インスタンスの数を減らすことができます。MSTP を使用すると、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）は影響を受けないので、ネットワークのフォールトトレランスが向上します。

（注） マルチ スパニングツリー（MST）実装は IEEE 802.1s 標準に準拠しています。

MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの導入です。MSTP の導入により、サービス プロバイダー環境に求められる高可用性ネットワークを実現できます。

スイッチが MST モードの場合、IEEE 802.1w 準拠の RSTP が自動的にイネーブルになります。RSTP は、IEEE 802.1D の転送遅延を軽減し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行する明示的なハンドシェイクによって、スパニングツリーの高速コンバージェンスを実現します。

MSTP と RSTP は、既存のシスコ独自の Multiple Instance STP（MISTP）、および既存の Cisco PVST+ と Rapid Per-VLAN Spanning-Tree plux（Rapid PVST+）を使用して、スパニングツリーの動作を改善し、（オリジナルの）IEEE 802.1D スパニング ツリーに準拠した機器との下位互換性を保持しています。

スイッチスタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが同一のスイッチ ID を使用します。

MSTP 設定時の注意事項

- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して、MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- UplinkFast、BackboneFast、クロススタック UplinkFast の設定のガイドラインについては、関連項目のセクションの該当するセクションを参照してください。
- スイッチが MST モードの場合は、パス コスト値の計算に、ロング パス コスト計算方式（32 ビット）が使用されます。ロング パス コスト計算方式では、次のパス コスト値がサポートされます。

速度	パス コスト値
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

MSTP の前提条件, （419 ページ）
MSTP の制約事項, （420 ページ）
スパニングツリーの相互運用性と下位互換性, （397 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast, （471 ページ）
UplinkFast, （465 ページ）

ルート スイッチ

スイッチは、マッピングされている VLAN グループのスパニングツリー インスタンスを保持しています。スイッチ ID は、スイッチのプライオリティおよびスイッチの MAC アドレスで構成されており、各インスタンスに関連付けられます。VLAN のグループでは、最小のスイッチ ID をもつスイッチがルート スイッチになります。

スイッチをルートとして設定する場合は、スイッチ プライオリティをデフォルト値（32768）からそれより大幅に低い値に変更し、スイッチが、指定したスパニングツリー インスタンスのルート スイッチになるようにします。このコマンドを入力すると、スイッチはルート スイッチのスイッチ プライオリティをチェックします。拡張システム ID をサポートしているため、24576 という値でスイッチが指定したスパニングツリー インスタンスのルートとなる場合、そのスイッチは指定したインスタンスに対する自身のプライオリティを 24576 に設定します。

指定されたインスタンスのルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です）。詳細については、関連項目の「Bridge ID, スイッチ Priority, and Extended System ID」リンクを参照してください。

ネットワークが、拡張システム ID をサポートするスイッチとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするスイッチがルート スイッチになる可能性は低くなります。古いソフトウェアを実行している接続スイッチのプライオリティより VLAN 番号が大きい場合は常に、拡張システム ID によってスイッチ プライオリティ値が増加します。

各スパニングツリー インスタンスのルート スイッチは、バックボーンまたはディストリビューション スイッチでなければなりません。アクセス スイッチをスパニングツリー プライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大スイッチ ホップ カウント）を指定するには、**diameter** キーワード（MST インスタンスが 0 の場合のみ使用できる）を指定します。ネットワーク直径を指定すると、スイッチはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

関連トピック

ルート スイッチの設定（CLI）, （443 ページ）
MSTP の制約事項, （420 ページ）

ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （389 ページ）

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して矛盾のないようにスイッチを設定する必要があります。同じ MST 設定の相互接続スイッチの集まりによって MST リージョンが構成されます。

MST 設定では、それぞれのスイッチが属する MST リージョンが制御されます。この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。その中で MST リージョンの設定を指定することにより、リージョンのスイッチを設定します。MST インスタンスに VLAN をマッピングし、リージョン名を指定して、リビジョン番号を設定できます。手順と例については、関連項目の「MST リージョンの設定の指定と MSTP のイネーブル化」リンクをクリックします。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。さらに、各メンバは、RSTP ブリッジ プロトコル データ ユニット（BPDU）を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリー インスタンスの数は 65 までです。インスタンスは、0 ～ 4094 の範囲の任意の番号で識別できます。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

関連トピック

MST リージョンの図, （427 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI）, （440 ページ）
MSTP の前提条件, （419 ページ）
MSTP の制約事項, （420 ページ）
スパニングツリーの相互運用性と下位互換性, （397 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast, （471 ページ）
UplinkFast, （465 ページ）

IST、CIST、CST

すべてのスパニングツリーインスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の 2 つのタイプのスパニングツリーを確立して保持しています。

- Internal Spanning-Tree（IST）は、1 つの MST リージョン内で稼働するスパニングツリーです。

  各 MST リージョン内の MSTP は複数のスパニングツリー インスタンスを維持しています。インスタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。その他すべての MSTI には、1 ～ 4094 の番号が付きます。

  IST は、BPDU を送受信する唯一のスパニングツリー インスタンスです。他のスパニングツリーの情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されていま

す。MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニングツリーインスタンスをサポートする処理が必要な BPDU の数を大幅に減少できます。

同一リージョン内の すべての MST インスタンスは同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポロジ パラメータ（ルート スイッチ ID、ルート パス コストなど）を持っています。デフォルトでは、すべての VLAN が IST に割り当てられます。

MSTI はリージョンにローカルです。たとえばリージョン A およびリージョン B が相互接続されていても、リージョン A の MSTI 1 は、リージョン B の MSTI 1 に依存しません。

- Common and Internal Spanning-Tree（CIST）は、各 MST リージョン内の IST と、MST リージョンおよびシングル スパニングツリーを相互接続する Common Spanning-Tree（CST）の集合です。

  1 つのリージョン内で計算されたスパニングツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーと見なされます。CIST は、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 標準をサポートするスイッチ間で実行されるスパニングツリー アルゴリズムによって形成されます。MST リージョン内の CIST は、リージョン外の CST と同じです。

MST リージョン内の動作

IST は 1 つのリージョン内のすべての MSTP スイッチを接続します。IST が収束すると、IST のルートは、CIST リージョナル ルート（IEEE 802.1s 標準が実装される以前は *IST* マスターと呼ばれた）になります。これは、リージョン内で最も小さいスイッチ ID、および CIST ルートに対するパス コストをもつスイッチです。ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートがリージョンの外部にある場合、リージョンの境界に位置する MSTP スイッチの 1 つが CIST リージョナル ルートとして選択されます。

MSTP スイッチは初期化時に、自身が CIST のルートおよび CIST リージョナル ルートであることを主張するために CIST ルートと CIST リージョナル ルートへのパス コストがいずれもゼロに設定された BPDU を送信します。スイッチはすべての MSTI を初期化し、そのすべてのルートであることを主張します。スイッチは、ポート用に現在保存されているものより上位の MST ルート情報（低いスイッチ ID、低いパス コストなど）を受信した場合、CIST リージョナル ルートとしての主張を放棄します。

リージョンには、初期化中に多くのサブ リージョンが含まれて、それぞれに独自の CIST リージョナル ルートが含まれることがあります。スイッチは、優位の IST 情報を受信すると、古いサブ リージョンを脱退して、真の CIST リージョナル ルートが含まれている新しいサブリージョンに加入します。真の CIST リージョナル ルートが含まれている以外のサブリージョンは、すべて縮小します。

正常な動作のためには、MST リージョン内のすべてのスイッチが同じ CIST リージョナル ルートを承認する必要があります。共通の CIST リージョナル ルートに収束する場合、そのリージョン内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

関連トピック

MST リージョンの図, （427 ページ）

MST リージョン間の動作

ネットワーク内に複数のリージョンまたはレガシー IEEE 802.1D スイッチが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP スイッチから構成される CST を構築して保持します。MSTI は、リージョンの境界にある IST と組み合わさり、CST になります。

IST はリージョン内のすべての MSTP スイッチを接続し、スイッチド ドメイン全体を囲む CIST のサブツリーとして認識されます。サブツリーのルートは CIST リージョナル ルートです。MST リージョンは、隣接する STP スイッチおよび MST リージョンへの仮想スイッチとして認識されます。

CST インスタンスのみが BPDU を送受信し、MST インスタンスはスパニングツリー情報を BPDU に追加して隣接するスイッチと相互作用し、最終的なスパニングツリー トポロジを算出します。したがって、BPDU 伝送に関連するスパニングツリー パラメータ（hello タイム、転送時間、最大エージング タイム、最大ホップ カウントなど）は、CST インスタンスだけで設定されますが、その影響はすべての MST インスタンスに及びます。スパニングツリー トポロジに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンスと MST インスタンスの両方で設定できます。

MSTP スイッチは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、レガシー IEEE 802.1D スイッチと通信します。MSTP スイッチは、MSTP BPDU を使用して MSTP スイッチと通信します。

関連トピック

MST リージョンの図, （427 ページ）

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部の MST 命名規則は、一部の内部パラメータまたはリージョン パラメータを識別するように変更されました。これらのパラメータは、ネットワーク全体に関連している外部パラメータと違い、MST リージョン内でのみ影響があります。CIST はネットワーク全体を網羅するスパニングツリー インスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル修飾子ではなく外部修飾子が必要です。

- CIST ルートは、ネットワーク全体を網羅する一意のインスタンスのためのルート スイッチです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。MST リージョンは、CIST への単一スイッチと見なすことに注意してください。CIST 外部ルート パス コストは、これらの仮想スイッチ、およびどのリージョンにも属さないスイッチの間で算出されるルート パス コストです。
- CIST リージョナル ルートは、準規格の実装で IST マスターと呼ばれていました。CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。CIST ルートがリージョン内にない場合、CIST リージョナル ルートは、リージョン内の CIST ルートに最も近いスイッチです。CIST リージョナル ルートは、IST のルート スイッチとして動作します。

- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。このコストは、IST つまりインスタンス 0 だけに関連します。

表 *33*：準規格と規格の用語

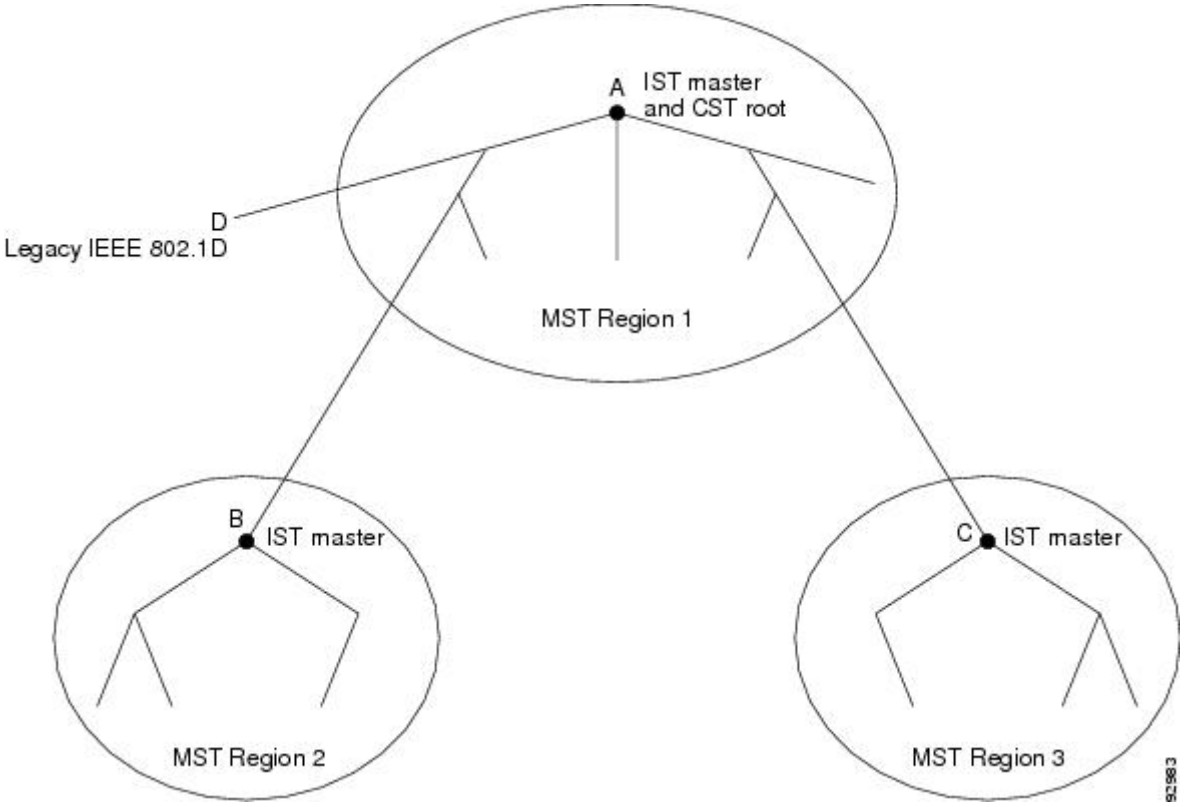
IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

MST リージョンの図

この図は、3 個の MST リージョンとレガシー IEEE 802.1D スイッチ（D）を示しています。リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。リージョン 2 の CIST

リージョナル ルート（B）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。RSTP はすべてのリージョンで稼働しています。

図 *19*：***MST*** リージョン、***CIST*** マスター、および ***CST*** ルート



関連トピック

MST リージョン，（424 ページ）
MST リージョン内の動作，（425 ページ）
MST リージョン間の動作，（426 ページ）

ホップ カウント

IST および MST インスタンスは、スパニングツリー トポロジの計算に、コンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報を使用しません。その代わりに、IP Time To Live（TTL）メカニズムに似た、ルートまでのパス コストおよびホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することにより、リージョン内の最大ホップを設定し、その値をリージョン内の IST インスタンスとすべての MST インスタンスに適用できます。ホップ カウントは、メッセージエージ情報と同じ結果になります（再設定を開始）。インスタンスのルート スイッチは、コストが 0 でホップ カウントが最大値に設定されている BPDU（M レコード）を常に送信します。スイッチは、この BPDU を受信する

と、受信した残りのホップ カウントから 1 を引き、生成する BPDU で残りのホップ カウントとしてこの値を伝播します。カウントがゼロに達すると、スイッチは BPDU を廃棄し、ポート用に維持されている情報を期限切れにします。

BPDU の RSTP 部分に格納されているメッセージ有効期間と最大エージング タイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTP が稼働する単一のスパニングツリー リージョン、PVST+ または Rapid PVST+ が稼働する単一のスパニングツリー リージョン、または異なる MST コンフィギュレーションを持つ別の MST リージョンに MST リージョンを接続します。境界ポートは、LAN、単一のスパニングツリー スイッチまたは MST 設定が異なるスイッチの指定スイッチにも接続します。

IEEE 802.1s 標準では、境界ポートの定義はなくなりました。IEEE 802.1Q-2002 標準では、ポートが受信できる 2 種類のメッセージを識別します。

- 内部（同一リージョンから）
- 外部（別のリージョンから）

メッセージが内部の場合、CIST の部分は CIST によって受信されるので、各 MST インスタンスは個々の M レコードだけを受信します。

メッセージが外部である場合、CIST だけが受信します。CIST の役割がルートや代替ルートの場合、または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。

MST リージョンには、スイッチおよび LAN の両方が含まれます。セグメントは、DP のリージョンに属します。そのため、セグメントの指定ポートではなく異なるリージョンにあるポートは境界ポートになります。この定義では、リージョン内部の 2 つのポートが、別のリージョンに属するポートとセグメントを共有し、内部メッセージおよび外部メッセージの両方を 1 つのポートで受信できるようになります。

シスコ先行標準の実装との主な違いは、STP 互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。

（注） レガシー STP スイッチがセグメントに存在する場合、メッセージは常に外部と見なされます。

シスコ先行標準の実装から他に変更された点は、送信スイッチ ID を持つ RSTP またはレガシー IEEE 802.1Q スイッチの部分に、CIST リージョナル ルート スイッチ ID フィールドが加えられたことです。リージョン全体は、一貫した送信者スイッチ ID をネイバー スイッチに送信し、単一仮想スイッチのように動作します。この例では、A または B がセグメントに指定されているかどうかに関係なく、ルートの一貫した送信者スイッチ ID が同じである BPDU をスイッチ C が受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標準には含まれていない一部の（要望されている）先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的に MST 標準に含まれませんでしたが、境界の概念自体はシスコの実装に投影されています。ただし、リージョン境界にある MST インスタンスのポートは、対応する CIST ポートのステートに必ずしも従うわけではありません。現在、2 つの境界の役割が存在しています。

- 境界ポートが CIST リージョナル ルートのルート ポートである場合：CIST インスタンス ポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わった後であれば（その後フォワーディングします）、その場合のみ合意を返信してフォワーディング ステートに移行できます。MSTI ポートには、特別なマスターの役割があります。
- 境界ポートが CIST リージョナル ルートのルート ポートでない：MSTI ポートは、CIST ポートのステートおよび役割に従います。標準では提供される情報が少ないため、MSTI ポートが BPDU（M レコード）を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかりにくい場合があります。この場合、境界の役割自体は存在していませんが、**show** コマンドで見ると、出力される *type* カラムで、ポートが境界ポートとして認識されていることがわかります。

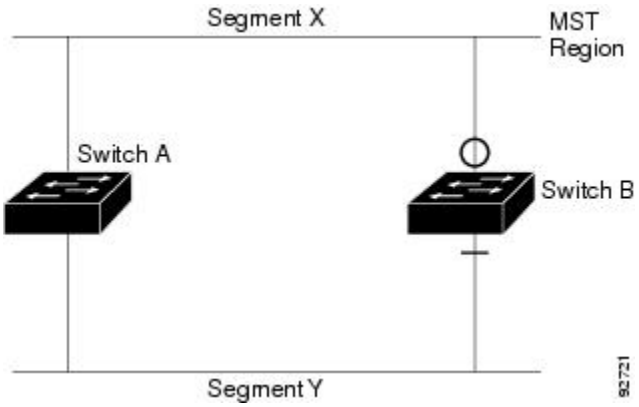
レガシーおよび規格スイッチの相互運用

準規格スイッチの自動検出はエラーになることがあるので、インターフェイス コンフィギュレーション コマンドを使用して準規格ポートを識別できます。スイッチの規格と準規格の間にリージョンを形成することはできませんが、CIST を使用して相互運用することができます。このような特別な方法を採用しても、失われる機能は、異なるインスタンス上のロード バランシングだけです。ポートが先行標準の BPDU を受信すると、CLI（コマンドライン インターフェイス）にはポートの設定に応じて異なるフラグが表示されます。スイッチが準規格 BPDU 送信用に設定されていないポートで準規格 BPDU を初めて受信したときは、Syslog メッセージも表示されます。

A が規格のスイッチで、B が準規格のスイッチとして、両方とも同じリージョンに設定されているとします。A は CIST のルート スイッチです。B のセグメント X にはルート ポート（BX）、セグメント Y には代替ポート（BY）があります。セグメント Y がフラップして BY のポートが代替になってから準規格 BPDU を 1 つ送信すると、AY は準規格スイッチが Y に接続されていることを検出できず、規格 BPDU の送信を続けます。ポート BY は境界に固定され、A と B との間で

のロード ランシングは不可能になります。セグメント X にも同じ問題がありますが、B はトポロジの変更であれば送信する場合があります。

図 *20*：規格および準規格のスイッチの相互運用



（注） 規格 MST 実装と準規格 MST 実装間の相互作用を最低限に抑えることを推奨します。

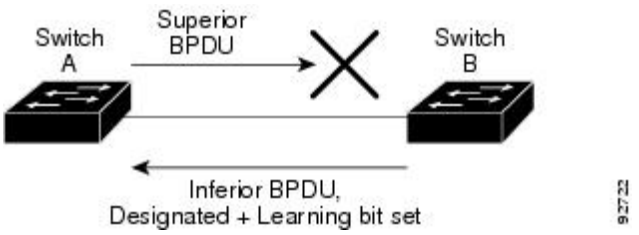
単一方向リンク障害の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

指定ポートは、矛盾を検出すると、そのロールを維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジング ループを解決できるからです。

次の図に、ブリッジング ループの一般的な原因となる単方向リンク障害を示します。スイッチ A はルート スイッチであり、スイッチ B へのリンクで BPDU は失われます。RSTP および MST BPDU には、送信側ポートの役割とステートが含まれます。スイッチ A はこの情報を使用し、ルータ A が送信する上位 BPDU にスイッチ B が反応しないこと、およびスイッチ B がルート スイッチではなく指定ブリッジであることを検出できます。この結果、スイッチ A は、そのポートをブロックし（またはブロックし続け）、ブリッジング ループが防止されます。

図 *21*：単一方向リンク障害の検出



MSTP およびスイッチ スタック

スイッチスタックは、ネットワークのその他の部分に対しては単一のスパニングツリーノードに見え、すべてのスタック メンバーが与えられたスパニングツリーに同一のブリッジ ID を使用します。ブリッジ ID は、アクティブ スイッチの MAC アドレスから取得されます。

MSTP をサポートしていないスイッチが、MSTP またはリバースをサポートしているスイッチ スタックに追加されると、スイッチはバージョンが不一致の状態になります。可能な場合、スイッチは、スイッチ スタックで実行中のソフトウェアと同じバージョンに自動的にアップグレードまたはダウングレードされます。

IEEE 802.1D STP との相互運用性

MSTP が稼働しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このスイッチは、レガシーIEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上ではIEEE 802.1D BPDU のみを送信します。また、MSTP スイッチは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、スイッチが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシースイッチが指定スイッチでない限り、レガシースイッチがリンクから削除されたかどうか検出できないためです。このスイッチが接続するスイッチがリージョンに加入していると、スイッチはポートに境界の役割を割り当て続ける場合があります。プロトコル移行プロセスを再開するには（強制的にネイバースイッチと再びネゴシエーションするには）、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシー スイッチが RSTP スイッチであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。したがって、MSTP スイッチは、バージョン 0 コンフィギュレーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで送信します。境界ポートは、LAN、単一スパニングツリースイッチまたはMST設定が異なるスイッチのいずれかの指定のスイッチに接続します。

RSTP 概要

RSTPは、ポイントツーポイントの配線を利用して、スパニングツリーの高速コンバージェンスを実現します。また、1 秒未満の間に、スパニングツリーを再構成できます（IEEE 802.1D スパニングツリーのデフォルトに設定されている 50 秒とは異なります）。

ポートの役割およびアクティブ トポロジ

RSTPは、ポートに役割を割り当てて、アクティブトポロジを学習することによって高速コンバージェンスを実現します。RSTPはスイッチをルートスイッチとして最も高いスイッチプライオリティ（プライオリティの数値が一番小さい）に選択するために、IEEE802.1DSTP上に構築されます。RSTP は、次のうちいずれかのポートの役割をそれぞれのポートに割り当てます。

- ルート ポート：スイッチ がルートスイッチ にパケットを転送するとき、最適なパス（最低コスト）を提供します。
- 指定ポート：指定スイッチに接続し、その LAN からルート スイッチにパケットを転送するとき、パス コストを最低にします。DP は、指定スイッチが LAN に接続されているポートです。
- 代替ポート：現在のルート ポートが提供したパスに代わるルート スイッチへの代替パスを提供します。
- バックアップ ポート：指定ポートが提供した、スパニングツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートは、2 つのポートがループバック内でポイントツーポイント リンクによって接続されるか、共有 LAN セグメントとの複数の接続がスイッチにある場合に限って存在できます。
- ディセーブル ポート：スパニングツリーの動作において何も役割が与えられていません。

ルート ポートまたは指定ポートのロールを持つポートは、アクティブなトポロジに含まれます。代替ポートまたはバックアップ ポートのロールがあるポートは、アクティブ トポロジから除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTP は、すべてのルート ポートおよび指定ポートがただちにフォワーディング ステートに移行し、代替ポートとバックアップ ポートが必ず廃棄ステート（IEEE 802.1D のブロッキング ステートと同じ）になるように保証します。ポートのステートにより、転送処理および学習処理の動作が制御されます。

表 *34*：ポート ステートの比較

Operational Status	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	ブロッキング	廃棄	いいえ
イネーブル	リスニング	廃棄	いいえ
イネーブル	ラーニング	ラーニング	はい
イネーブル	フォワーディング	フォワーディング	はい
ディセーブル	ディセーブル	廃棄	いいえ

Cisco STP の実装との一貫性を保つため、このマニュアルでは、ポート ステートを廃棄ではなくブロッキングとして定義します。DP はリスニング ステートから開始します。

高速コンバージェンス

RSTP は、スイッチ、スイッチ ポート、LAN のうちいずれかの障害のあと、接続の高速回復を提供します。エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- エッジ ポート：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して RSTP スイッチでエッジ ポートとしてポートを設定した場合、エッジ ポートはフォワーディング ステートにすぐに移行します。エッジ ポートは Port Fast 対応ポートと同じであり、単一エンド ステーションに接続しているポートだけでイネーブルにする必要があります。
- ルート ポート：RSTP は、新しいルート ポートを選択した場合、古いルート ポートをブロックし、新しいルート ポートをフォワーディング ステートにすぐに移行します。
- ポイントツーポイント リンク：ポイントツーポイント リンクによってあるポートと別のポートを接続することでローカル ポートが指定ポートになると、提案合意ハンドシェイクを使用して他のポートと急速な移行がネゴシエートされ、トポロジにループがなくなります。

  スイッチ A がスイッチ B にポイントツーポイント リンクで接続され、すべてのポートはブロッキング ステートになっています。スイッチ A のプライオリティがスイッチ B のプライオリティよりも数値的に小さいとします。スイッチ A は提案メッセージ（提案フラグを設定した設定 BPDU）をスイッチ B に送信し、指定スイッチとしてそれ自体を提案します。

  スイッチ B は、提案メッセージの受信後、提案メッセージを受信したポートを新しいルート ポートとして選択し、エッジ以外のすべてのポートを強制的にブロッキング ステートにして、新しいルート ポートを介して合意メッセージ（合意フラグを設定した BPDU）を送信します。

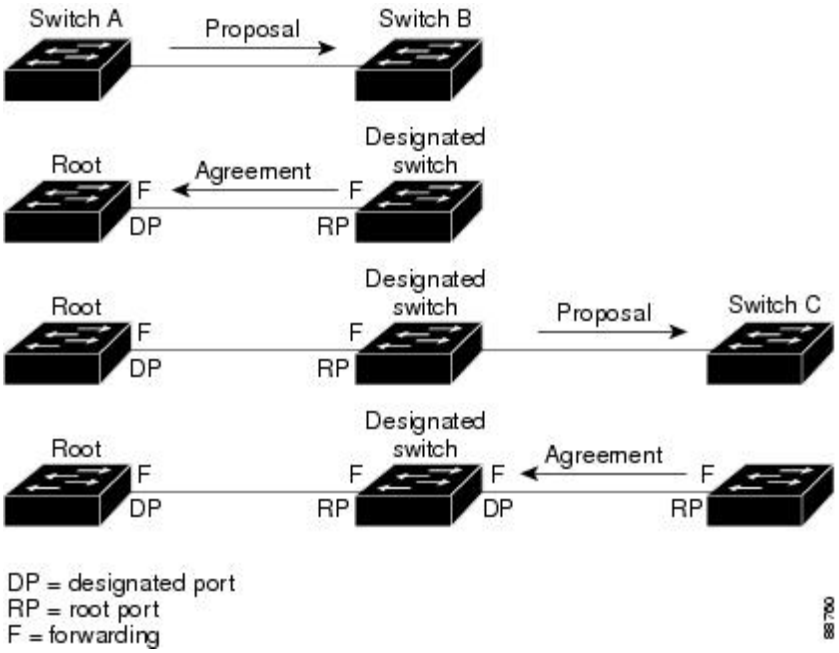
  スイッチ A も、スイッチ B の合意メッセージの受信後、指定ポートをフォワーディング ステートにすぐに移行します。スイッチ B はすべてのエッジ以外のポートをブロックし、スイッチ A およびルータ B の間にポイントツーポイント リンクがあるので、ネットワークにループは形成されません。

  スイッチ C がスイッチ B に接続すると、同様のセットのハンドシェーク メッセージが交換されます。スイッチ C はスイッチ B に接続されているポートをルート ポートとして選択し、両端がフォワーディング ステートにすぐに移行します。このハンドシェーク処理を繰り返して、もう 1 つのスイッチがアクティブ トポロジーに加わります。ネットワークが収束すると、この提案/合意ハンドシェイクがルートからスパニングツリーのリーフへと進みます。

  スイッチ スタックでは、Cross-Stack Rapid Transition（CSRT）機能を使用すると、ポートがフォワーディング ステートに移行する前に、スタック メンバで、提案/合意ハンドシェイク中にすべてのスタック メンバーから確認メッセージを受信できます。スイッチが MST モードの場合、CSRT は自動的にイネーブルにされます。

  スイッチはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用すると、デュプレックス設定によって制御されるデフォルト設定を無効にすることができます。

図 *22*：高速コンバージェンスの提案と合意のハンドシェイク



ポート ロールの同期

スイッチがそのルータのポートの 1 つで提案メッセージを受信し、そのポートが新しいルート ポートとして選択されると、RSTP によってその他すべてのポートが新しいルートの情報と強制的に同期化します。

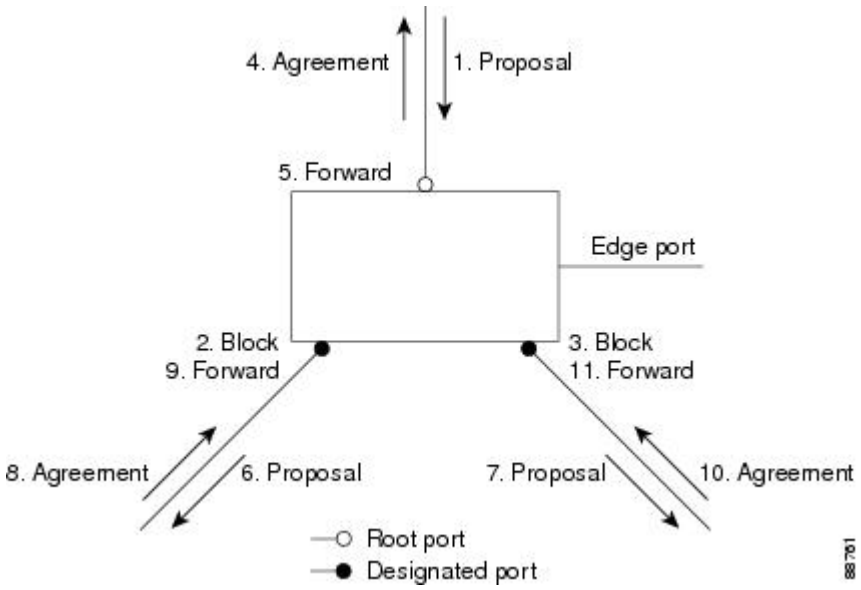
その他すべてのポートが同期化されている場合、スイッチはルート ポートで受信した上位ルート情報で同期化されます。スイッチのそれぞれのポートは、次のような場合に同期化します。

- ポートがブロッキング ステートである。
- エッジ ポートである（ネットワークのエッジに存在するように設定されたポート）。

指定ポートがフォワーディング ステートでエッジ ポートとして設定されていない場合、RSTP によって新しいルート情報と強制的に同期されると、その指定ポートはブロッキング ステートに移行します。一般的に RSTP がルート情報でポートを強制的に同期化し、ポートが上の条件を満たしていない場合、そのポート ステートはブロッキングに設定されます。

スイッチは、すべてのポートが同期化されたことを確認した後で、ルート ポートに対応する指定スイッチに合意メッセージを送信します。ポイントツーポイント リンクで接続されたスイッチがポートの役割で合意すると、RSTP はポート ステートをフォワーディングにすぐに移行します。

図 *23*：高速コンバージェンス中のイベントのシーケンス



ブリッジ プロトコル データ ユニットの形式および処理

RSTP BPDU のフォーマットは、プロトコル バージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報がないことを示しています。

表 *35*：*RSTP BPDU* フラグ

ビット	機能
0	トポロジーの変化（TC）
1	提案
2 ～ 3: 00 01 10 11	ポートの役割： 不明 代替ポート ルート ポート 指定ポート
4	ラーニング

ビット	機能
5	フォワーディング
6	合意
7	トポロジー変更確認応答（TCA）

送信側スイッチは RSTP BPDU の提案フラグを設定し、そのLAN の指定スイッチとして自分自身を提案します。提案メッセージのポートの役割は、常に DP に設定されます。

送信側スイッチは、RSTP BPDU の合意フラグを設定して以前の提案を受け入れます。合意メッセージ内のポート ロールは、常にルート ポートに設定されます。

RSTP には個別のトポロジ変更通知（TCN）BPDU はありません。TC フラグが使用されて、TC が示されます。ただし、IEEE 802.1D スイッチとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニング フラグおよびフォワーディング フラグは、送信側ポートのステートに従って設定されます。

優位 *BPDU* 情報の処理

ポートに現在保存されているルート情報よりも優位のルート情報（小さいスイッチ ID、低いパス コストなど）をポートが受け取ると、RSTP は再構成を開始します。ポートが新しいルート ポートとして提案されて選択されると、RSTP は強制的にその他すべてのポートを同期化します。

受信した BPDU が、提案フラグが設定されている RSTP BPDU である場合、スイッチはその他すべてのポートが同期化されてから合意メッセージを送信します。BPDU が IEEE 802.1D BPDU の場合、スイッチは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。新しいルート ポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

ポートで優位の情報が受信されたために、そのポートがバックアップ ポートまたは代替ポートになる場合、RSTP はそのポートをブロッキング ステートに設定し、合意メッセージは送信しません。DP は、転送遅延タイマーが失効するまで、提案フラグを設定して BPDU を送信し続け、転送遅延タイマーの失効時に、ポートはフォワーディング ステートに移行します。

下位 *BPDU* 情報の処理

指定ポートの役割を持つ下位 BPDU（そのポートに現在保存されている値より大きいスイッチ ID、高いパス コストなど）を指定ポートが受信した場合、その指定ポートはただちに現在の自身の情報で応答します。

トポロジの変更

ここでは、スパニングツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出：IEEE 802.1D では、どのようなブロッキング ステートとフォワーディング ステートとの間の移行でもトポロジの変更が発生しますが、RSTP でトポロジの変更が発生するのは、ブロッキング ステートからフォワーディング ステートに移行する場合だけです（トポロジの変更と見なされるのは、接続数が増加する場合だけです）。エッジポートにおけるステート変更は、TC の原因になりません。RSTP スイッチは、TC を検出すると、TCN を受信したポートを除く、エッジ以外のすべてのポートで学習した情報を削除します。
- 通知：IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。ただし、IEEE 802.1D との相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。
- 確認：RSTP スイッチは、指定ポートで IEEE 802.1D スイッチから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D スイッチに接続されたルート ポートで TC 時間タイマー（IEEE 802.1D のトポロジ変更タイマーと同じ）がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

  この処理は、IEEE 802.1D スイッチをサポートする目的でのみ必要とされます。RSTP BPDU は TCA ビットが設定されていません。
- 伝播：RSTP スイッチは、DP またはルート ポートを介して別のスイッチから TC メッセージを受信すると、エッジ以外のすべての DP、およびルート ポート（TC メッセージを受信したポートを除く）に変更を伝播します。スイッチはこのようなすべてのポートで TC-while タイマーを開始し、そのポートで学習した情報を消去します。
- プロトコルの移行：IEEE 802.1D スイッチとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU が送信される最低時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブである間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコル タイプを無視します。

  スイッチはポートの移行遅延タイマーが満了した後に IEEE 802.1D BPDU を受信した場合、IEEE 802.1D スイッチに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。ただし、RSTP スイッチが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了した後に RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用が開始されます。

プロトコル移行プロセス

MSTP が稼働しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MST スイッチは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RST BPDU（バージョン2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、スイッチが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシースイッチが指定スイッチでない限り、レガシースイッチがリンクから削除されたかどうか検出できないためです。また、接続するスイッチがリージョンに加入していると、スイッチはポートに境界の役割を割り当て続ける場合があります。

関連トピック

プロトコルの移行プロセスの再開（CLI），（459 ページ）

MSTP のデフォルト設定

表 *36*：*MSTP* のデフォルト設定

機能	デフォルト設定
スパニングツリー モード	MSTP
スイッチプライオリティ（CIST ポートごとに設定可能）	32768
スパニングツリー ポート プライオリティ（CIST ポート単位で設定可能）	128
スパニングツリー ポート コスト（CIST ポート単位で設定可能）	1000 Mb/s：20000 100 Mb/s：20000 10 Mb/s：20000 1000 Mb/s：20000 100 Mb/s：20000 10 Mb/s：20000
hello タイム	3 秒
転送遅延時間	20 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

関連トピック

サポートされるスパニングツリー インスタンス，（397 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

MSTP 機能の設定方法

MST リージョン設定の指定と MSTP のイネーブル化（CLI）

2 つ以上のスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/インスタンスマッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

リージョンには、MST 設定が同一である、1 つ以上のメンバーを含めることができます。各メンバーでは、RSTP BPDU を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は65までです。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst configuration**
4. **instance***instance-id* **vlan***vlan-range*
5. **name***name*
6. **revision***version*
7. **show pending**
8. **exit**
9. **spanning-tree mode mst**
10. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree mst configuration** 例： `スイッチ(config)# spanning-tree mst configuration`	MST コンフィギュレーション モードを開始します。
ステップ 4	**instance***instance-id* **vlan***vlan-range* 例： `スイッチ(config-mst)# instance 1 vlan 10-20`	VLAN を MSTI にマップします。 • *instance-id* に指定できる範囲は、0 ～ 4094 です。 • **vlan***vlan-range* に指定できる範囲は、1 ～ 4094 です。 VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN の範囲を指定するには、ハイフンを使用します。たとえば **instance 1 vlan 1-63** では、VLAN 1 ～ 63 が MST インスタンス 1 にマップされます。 一連の VLAN を指定するには、カンマを使用します。たとえば **instance 1 vlan 10, 20, 30** と指定すると、VLAN 10、20、30 が MST インスタンス 1 にマップされます。
ステップ 5	**name***name* 例： `スイッチ(config-mst)# name region1`	コンフィギュレーション名を指定します。*name* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。
ステップ 6	**revision***version* 例： `スイッチ(config-mst)# revision 1`	設定リビジョン番号を指定します。指定できる範囲は 0 ～ 65535 です。
ステップ 7	**show pending** 例： `スイッチ(config-mst)# show pending`	保留中の設定を表示し、設定を確認します。
ステップ 8	**exit** 例： `スイッチ(config-mst)# exit`	すべての変更を適用し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**spanning-tree mode mst** 例： スイッチ(config)# **spanning-tree mode mst**	MSTP をイネーブルにします。RSTP もイネーブルになります。 スパニングツリー モードを変更すると、すべてのスパニングツリーインスタンスは以前のモードであるため停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。 MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 10	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

MSTP 設定時の注意事項，（422 ページ）
MST リージョン，（424 ページ）
MSTP の前提条件，（419 ページ）
MSTP の制約事項，（420 ページ）
スパニングツリーの相互運用性と下位互換性，（397 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast，（471 ページ）
UplinkFast，（465 ページ）
MSTP のデフォルト設定，（439 ページ）
ルート スイッチの設定（CLI），（443 ページ）
MSTP の制約事項，（420 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID，（389 ページ）
セカンダリ ルート スイッチの設定（CLI），（444 ページ）
ポート プライオリティの設定（CLI），（446 ページ）
パス コストの設定（CLI），（448 ページ）
スイッチ プライオリティの設定（CLI），（449 ページ）
hello タイムの設定（CLI），（451 ページ）
転送遅延時間の設定（CLI），（452 ページ）
最大エージング タイムの設定（CLI），（454 ページ）
最大ホップ カウントの設定（CLI），（455 ページ）
高速移行を確実にするためのリンク タイプの指定（CLI），（456 ページ）

ネイバー タイプの設定（CLI），（457 ページ）
プロトコルの移行プロセスの再開（CLI），（459 ページ）

ルート スイッチの設定（CLI）

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。この例のステップ 2 では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst***instance-id***root primary**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst***instance-id***root primary** 例： `スイッチ(config)# spanning-tree mst 0 root primary`	ルート スイッチとしてスイッチを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。

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

関連トピック

ルート スイッチ, （423 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI）, （440 ページ）
MSTP の制約事項, （420 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （389 ページ）
セカンダリ ルート スイッチの設定（CLI）, （444 ページ）

セカンダリ ルート スイッチの設定（CLI）

拡張システム ID をサポートするスイッチをセカンダリ ルートとして設定する場合、スイッチ プライオリティはデフォルト値（32768）から 28672 に修正されます。プライマリ ルート スイッチで障害が発生した場合は、このスイッチが指定インスタンスのルート スイッチになる可能性があります。ここでは、その他のネットワーク スイッチが、デフォルトのスイッチプライオリティの 32768 を使用しているためにルート スイッチになる可能性が低いことが前提となっています。

このコマンドを複数のスイッチに対して実行すると、複数のバックアップルートスイッチを設定できます。**spanning-tree mst***instance-id***root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst***instance-id***root secondary**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst***instance-id***root secondary** 例： `スイッチ(config)# spanning-tree mst 0 root secondary`	セカンダリ ルート スイッチとしてスイッチを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）
ルート スイッチの設定（CLI），（443 ページ）

ポート プライオリティの設定（CLI）

ループが発生した場合、MSTP はポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

（注） スイッチがスイッチ スタックのメンバーの場合、**spanning-tree mst** [*instance-id*] **port-priority***priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree mst** [*instance-id*] **cost***cost* インターフェイス コンフィギュレーション コマンドを使用し、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させたいポートには、より小さいコスト値を割り当て、最後に選択させたいポートには、より大きいコスト値を割り当てることができます。詳細については、関連項目の下に表示されるパス コストのトピックを参照してください。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree mst***instance-id***port-priority***priority*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface GigabitEthernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree mst***instance-id***port-priority***priority* 例： スイッチ(config-if)# **spanning-tree mst 0 port-priority 64**	ポート プライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *priority* 値の範囲は 0 ～ 240 で、16 ずつ増加します。デフォルト値は 128 です。値が小さいほど、プライオリティが高くなります。 使用可能な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 だけです。その他の値はすべて拒否されます。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

show spanning-tree mstinterface*interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。ポートがリンクアップ動作状態になっていない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認できます。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）
パス コストの設定（CLI），（448 ページ）

パス コストの設定（CLI）

MSTP パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスに同じコスト値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree mst***instance-id***cost***cost*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポートとポート チャネル論理インターフェイスがあります。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**spanning-tree mst***instance-id***cost***cost* 例： スイッチ(config-if)# **spanning-tree mst 0 cost 17031970**	コストを設定します。 ループが発生した場合、MSTP はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

show spanning-tree mst interface*interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティの設定（CLI），（446 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

スイッチ プライオリティの設定（CLI）

スイッチのプライオリティを変更すると、スタンドアロン スイッチまたはスタック内のスイッチであるかに関係なく、ルートスイッチとして選択される可能性が高くなります。

（注） このコマンドの使用には注意してください。通常のネットワーク設定では、**spanning-tree mst** *instance-id***root primary** および **spanning-tree mst***instance-id***root secondary** グローバル コンフィギュレーション コマンドを使用して、スイッチをルートまたはセカンダリ ルート スイッチとして指定することをお勧めします。これらのコマンドが動作しない場合にのみスイッチプライオリティを変更する必要があります。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

使用する指定された MST インスタンス ID も把握する必要があります。この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst***instance-id***priority***priority*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst***instance-id***priority***priority* 例： `スイッチ(config)# spanning-tree mst 0 priority 40960`	スイッチのプライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。

	コマンドまたはアクション	目的
		• *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。この値が低いほど、スイッチがルート スイッチとして選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。これらは唯一の許容値です。
ステップ 4	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

hello タイムの設定（CLI）

hello タイムはルート スイッチによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst hello-time***seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst hello-time***seconds* 例： スイッチ(config)# **spanning-tree mst hello-time 4**	すべての MST インスタンスについて、hello タイムを設定します。hello タイムはルート スイッチによって設定メッセージが生成されて送信される時間の間隔です。このメッセージは、スイッチが活動中であることを表します。 *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 3 です。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

転送遅延時間の設定（CLI）

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst forward-time***seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst forward-time***seconds* 例： スイッチ(config)# **spanning-tree mst forward-time 25**	すべての MST インスタンスについて、転送時間を設定します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、ポートが待機する秒数です。 *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 20 です。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

最大エージング タイムの設定（CLI）

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst max-age***seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst max-age***seconds* 例： `スイッチ(config)# spanning-tree mst max-age 40`	すべての MST インスタンスについて、最大経過時間を設定します。最大エージング タイムは、スイッチが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

最大ホップ カウントの設定（CLI）

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst max-hops***hop-count*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst max-hops***hop-count* 例： `スイッチ(config)# spanning-tree mst max-hops 25`	BPDU を廃棄してポート用に保持していた情報を期限切れにするまでの、リージョンでのホップ数を設定します。 *hop-count* に指定できる範囲は 1 ～ 255 です。デフォルト値は 20 です。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

高速移行を確実にするためのリンク タイプの指定（CLI）

ポイントツーポイント リンクでポート間を接続し、ローカル ポートが DP になると、RSTP は提案と合意のハンドシェークを使用して別のポートと高速移行をネゴシエーションし、ループがないトポロジを保証します。

デフォルトの場合、リンク タイプはインターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続、半二重ポートは共有接続と見なされます。MSTP を実行しているリモート スイッチの単一ポートに、半二重リンクを物理的にポイントツーポイントで接続した場合は、リンク タイプのデフォルト設定を無効にして、フォワーディング ステートへの高速移行をイネーブルにすることができます。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree link-type point-to-point**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface GigabitEthernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポート、VLAN、およびポート チャネル論理インターフェイスがあります。VLAN ID の範囲は 1 ～ 4094 です。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**spanning-tree link-type point-to-point** 例： スイッチ(config-if)# **spanning-tree link-type point-to-point**	ポートのリンク タイプがポイントツーポイントであることを指定します。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

ネイバー タイプの設定（CLI）

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることができます。デフォルトの場合、ポートは準規格デバイスを自動的に検出できますが、規格 BPDU および準規格 BPDU の両方を受信できます。デバイスとそのネイバーの間に不一致がある場合は、CIST だけがインターフェイスで動作します。

準規格 BPDU だけを送信するようにポートを設定できます。ポートが STP 互換モードになっていても、すべての **show** コマンドで準規格フラグが表示されます。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree mst pre-standard**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface GigabitEthernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**spanning-tree mst pre-standard** 例： スイッチ(config-if)# **spanning-tree mst pre-standard**	ポートが準規格 BPDU だけを送信できることを指定します。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）

プロトコルの移行プロセスの再開（CLI）

この手順では、プロトコル移行プロセスを再開し、ネイバー スイッチとの再ネゴシエーションを強制します。また、スイッチを MST モードに戻します。これは、IEEE 802.1D BPDU の受信後にスイッチがそれらを受信しない場合に必要です。

スイッチでプロトコルの移行プロセスを再開する（隣接するスイッチで再ネゴシエーションを強制的に行う）手順については、これらの手順に従ってください。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

コマンドのインターフェイス バージョンを使用する場合は、使用する MST インターフェイスが分かっている必要があります。この例では、インターフェイスとして GigabitEthernet1/0/1 を使用します。それが「関連項目」で示されている手順によって設定されたインターフェイスであるからです。

手順の概要

1. **enable**
2. 次のいずれかのコマンドを入力します。
   - **clear spanning-tree detected-protocols**
   - **clear spanning-tree detected-protocolsinterface***interface-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかのコマンドを入力します。 • **clear spanning-tree detected-protocols** • **clear spanning-tree detected-protocolsinterface***interface-id* 例： `スイッチ# clear spanning-tree detected-protocols`	スイッチが MSTP モードに戻り、プロトコルの移行プロセスが再開されます。

	コマンドまたはアクション	目的
	または スイッチ# **clear spanning-tree detected-protocols interface GigabitEthernet1/0/1**	

次の作業

この手順は、スイッチでさらにレガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定された BPDU）を受信する場合に、繰り返しが必要なことがあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）
プロトコル移行プロセス，（438 ページ）

MSTP に関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	*LAN Switching Command Reference, Cisco IOS XE Release 3SE（Catalyst 3650 Switches）*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

MSTP の機能情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 23 章

オプションのスパニングツリー機能の設定

- オプションのスパニングツリー機能について，463 ページ
- オプションのスパニングツリー機能の設定方法，475 ページ
- スパニングツリー ステータスのモニタリング，490 ページ
- オプションのスパニング ツリー機能に関する追加情報，490 ページ
- オプションのスパニングツリー機能の機能情報，491 ページ

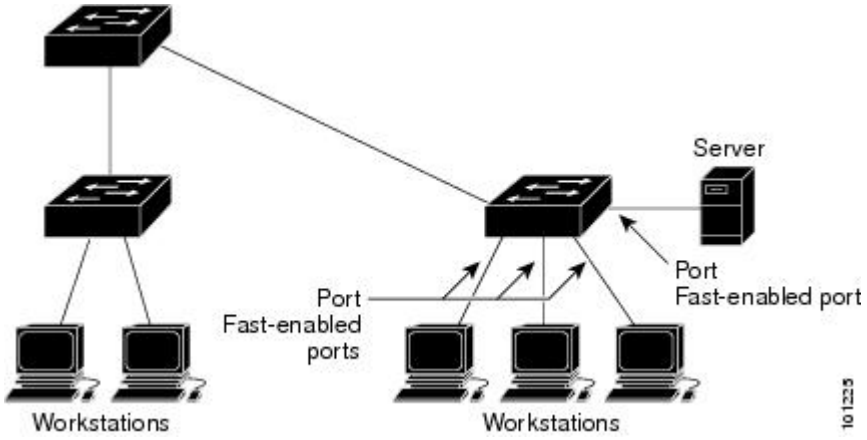
オプションのスパニングツリー機能について

PortFast

PortFast機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートから直接フォワーディング ステートに移行します。

1 台のワークステーションまたはサーバに接続されているインターフェイス上で PortFast を使用すると、スパニングツリーが収束するのを待たずにデバイスをすぐにネットワークに接続できます。

図 *24*：*PortFast* がイネーブルなインターフェイス



1 台のワークステーションまたはサーバに接続されたインターフェイスがブリッジ プロトコル データ ユニット（BPDU）を受信しないようにする必要があります。スイッチを再起動すると、PortFast がイネーブルに設定されているインターフェイスは通常のスパニングツリー ステータスの遷移をたどります。

インターフェイスまたはすべての非トランク ポートでイネーブルにして、この機能をイネーブルにできます。

関連トピック

PortFast のイネーブル化（CLI），（475 ページ）

オプションのスパニング ツリー機能の制約事項

BPDU ガード

ブリッジ プロトコル データ ユニット（BPDU）ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

PortFast エッジ対応ポート上でグローバル レベルで BPDU ガードをイネーブルにすると、スパニング ツリーは、BPDU が受信されると、PortFast エッジ動作ステートのポートをシャット ダウンします。有効な設定では、PortFast エッジ対応ポートは BPDU を受信しません。PortFast エッジ対応ポートが BPDU を受信した場合は、許可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは error-disabled ステートになります。この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

PortFast エッジ機能をイネーブルにせずにインターフェイス レベルでポート上の BPDU ガードをイネーブルにした場合、ポートが BPDU を受信すると、error-disabled ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダーネットワーク内でアクセスポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

関連トピック

BPDU ガードのイネーブル化（CLI），（477 ページ）

BPDU フィルタリング

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルでは、PortFast エッジ対応インターフェイスで BPDU フィルタリングをイネーブルにすると、PortFast エッジ動作ステートにあるインターフェイスでの BPDU の送受信が防止されます。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。PortFast エッジ対応インターフェイスでは、BPDU を受信すると、PortFast エッジ動作ステートが解除され、BPDU フィルタリングがディセーブルになります。

PortFast エッジ機能をイネーブルにせずに、インターフェイスで BPDU フィルタリングをイネーブルにすると、インターフェイスでの BPDU の送受信が防止されます。

注意 BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチ全体または 1 つのインターフェイスで BPDU フィルタリング機能をイネーブルにできます。

関連トピック

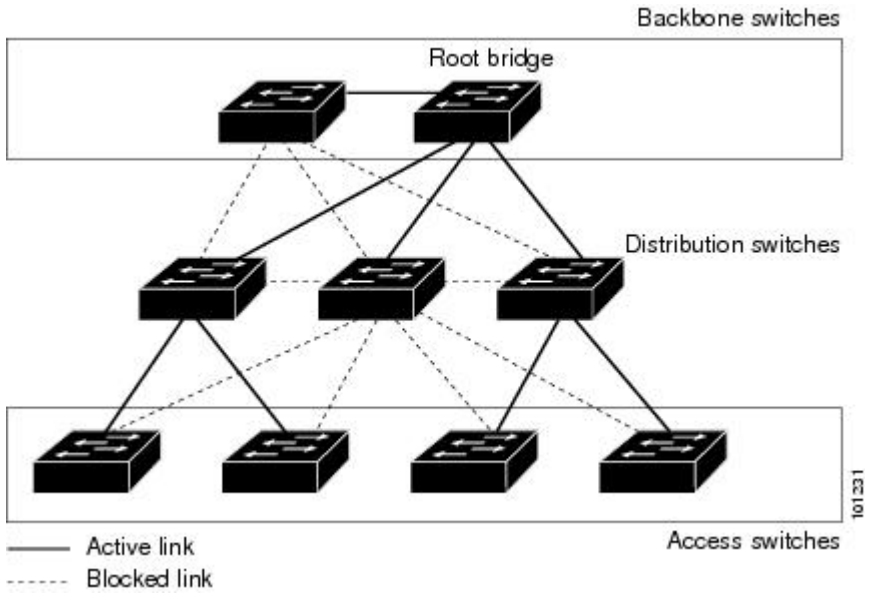
BPDU フィルタリングのイネーブル化（CLI），（479 ページ）

UplinkFast

階層型ネットワークに配置されたスイッチは、バックボーン スイッチ、ディストリビューション スイッチ、およびアクセス スイッチに分類できます。この複雑なネットワークには、ディストリ

ビューション スイッチとアクセス スイッチがあり、ループを防止するために、スパニング ツリーがブロックする冗長リンクが少なくとも 1 つあります。

図 *25*：階層型ネットワークのスイッチ



スイッチの接続が切断されると、スイッチはスパニングツリーが新しいルート ポートを選択すると同時に代替パスの使用を開始します。リンクやスイッチに障害が発生した場合、またはスパニングツリーが UplinkFast のイネーブル化によって自動的に再設定された場合に、新しいルート ポートを短時間で選択できます。ルート ポートは、通常のスパニングツリー手順とは異なり、リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

スパニングツリーが新規ルート ポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッディングし、インターフェイス上で学習した各アドレスにパケットを送信します。max-update-rate パラメータの値を小さくすることで、これらのマルチキャスト トラフィックのバーストを制限できます（このパラメータはデフォルトで毎秒 150 パケットです）。ただし、0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。

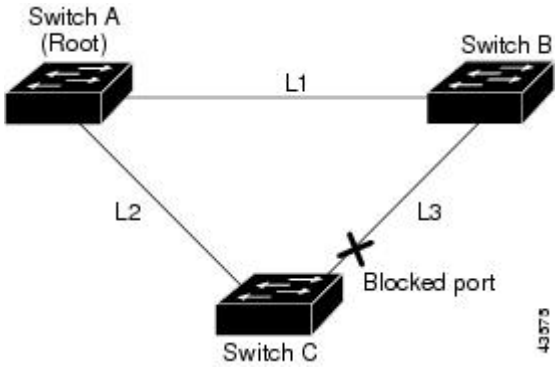
（注） UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのスイッチで非常に有効です。バックボーン デバイスには適していません。他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロード バランシングを実行します。アップリンク グループは、（VLAN ごとの）レイヤ 2 インターフェイスの集合であり、いかなるときも、その中の 1 つのインターフェイスだけが転送を行います。つまり、アップリンク グループは、（転送を行う）

ルート ポートと、（セルフループを行うポートを除く）ブロックされたポートの集合で構成されます。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

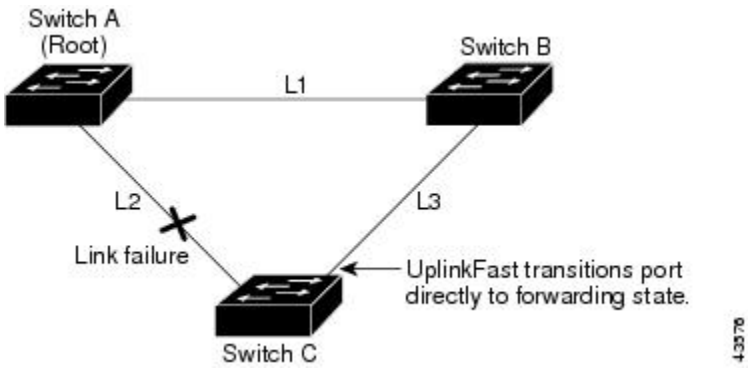
このトポロジにはリンク障害がありません。ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 *26*：直接リンク障害が発生する前の *UplinkFast* の例



スイッチ C が、ルート ポートの現在のアクティブ リンクである L2 でリンク障害（直接リンク障害）を検出すると、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、直接フォワーディング ステートに移行させます。この切り替えに必要な時間は、約 1 ～ 5 秒です。

図 *27*：直接リンク障害が発生したあとの *UplinkFast* の例



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）
MSTP 設定時の注意事項，（422 ページ）
MST リージョン，（424 ページ）
冗長リンクで使用するための UplinkFast のイネーブル化（CLI），（481 ページ）
高速コンバージェンスを発生させるイベント，（470 ページ）

クロススタック UplinkFast

クロススタック UplinkFast（CSUF）は、スイッチ スタック全体にスパニングツリー高速移行（通常のネットワーク状態の下では 1 秒未満の高速コンバージェンス）を提供します。高速移行の間は、スタック上の代替冗長リンクがフォワーディング ステートになり、一時的なスパニングツリー ループもバックボーンへの接続の損失も発生させません。一部の設定では、この機能により、冗長性と復元力を備えたネットワークが得られます。CSUF は UplinkFast 機能をイネーブルにすると、自動的にイネーブルになります。

CSUF で高速移行が得られない場合もあります。この場合は、通常のスパニングツリー移行が発生し、30 ～ 40 秒以内に完了します。詳細については、「関連項目」を参照してください。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化（CLI），（481 ページ）
高速コンバージェンスを発生させるイベント，（470 ページ）

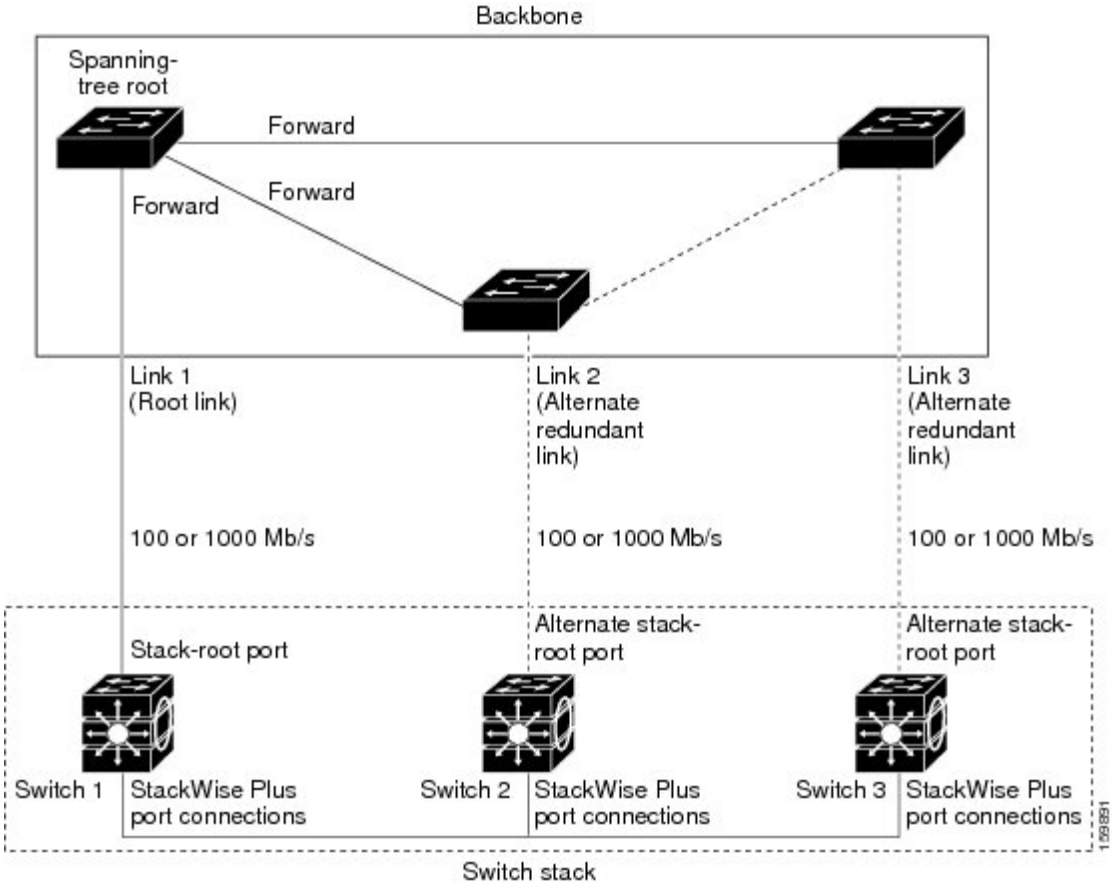
クロススタック UplinkFast の動作

クロススタック UplinkFast（CSUF）によって、ルートへのパスとしてスタック内で 1 つのリンクが確実に選択されます。

スイッチ 1 のスタックルート ポートは、スパニングツリーのルートへパスを提供しています。スイッチ 2 およびスイッチ 3 の代替スタックルート ポートは、現在のスタックルート スイッチに障害が発生したか、またはそのスパニングツリー ルートへのリンクに障害が発生した場合に、スパニングツリー ルートへの代替パスを提供できます。

ルート リンクである Link 1 は、スパニングツリー フォワーディング ステートになっています。Link 2 と Link 3 は、スパニングツリー ブロッキング ステートになっている代替冗長リンクです。スイッチ 1 に障害が発生したか、そのスタック ルート ポートに障害が発生したか、または Link 1 に障害が発生した場合には、CSUF が、1 秒未満でスイッチ 2 またはスイッチ 3 のいずれかにある代替スタックルート ポートを選択して、それをフォワーディング ステートにします。

図 *28*：クロススタック *UplinkFast* トポロジ



特定のリンク損失またはスパニングツリーイベントが発生した場合（次のトピックを参照）、Fast Uplink Transition Protocol は、ネイバー リストを使用して、高速移行要求をスタック メンバーに送信します。

高速移行要求を送信するスイッチは、ルート ポートとして選択されたポートをフォワーディング ステートへ高速移行する必要があります。また、高速移行を実行するには、事前に各スタックから確認応答を取得しておく必要があります。

スタック内の各スイッチが、ルート、コスト、およびブリッジ ID を比較することにより、このスパニングツリーインスタンスのスタック ルートとなるよりも送信スイッチの方がよりよい選択肢であるかどうかを判断します。スタック ルートとして送信スイッチが最も良い選択である場合は、スタック内の各スイッチが確認応答を返します。それ以外の場合は、高速移行要求を送信します。この時点では、送信スイッチは、すべてのスタック スイッチから確認応答を受け取っていません。

すべてのスタック スイッチから確認応答を受け取ると、送信スイッチの Fast Uplink Transition Protocol は代替スタック ルート ポートをすぐにフォワーディング ステートに移行させます。送信スイッチがすべてのスタック スイッチからの確認応答を取得しなかった場合、通常のスパニングツリー移行（ブロッキング、リスニング、ラーニング、およびフォワーディング）が行われ、ス

パニングツリー トポロジが通常のレート（2 × 転送遅延時間 + 最大エージング タイム）で収束します。

Fast Uplink Transition Protocol は、VLAN ごとに実装されており、一度に 1 つのスパニングツリー インスタンスにしか影響しません。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化（CLI），（481 ページ）
高速コンバージェンスを発生させるイベント，（470 ページ）

高速コンバージェンスを発生させるイベント

CSUF 高速コンバージェンスは、ネットワーク イベントまたはネットワーク障害に応じて、発生する場合もあれば発生しない場合もあります。

高速コンバージェンス（通常のネットワーク状態で1秒未満）は、次のような状況で発生します。

- スタック ルート ポート リンクに障害が発生した。

  スタック内の 2 つのスイッチがルートへの代替パスを持つ場合、それらのスイッチの片方だけが高速移行を行います。

- スタック ルートをスパニングツリー ルートに接続するリンクに障害が発生し、回復した。
- ネットワークの再設定により、新しいスタックルート スイッチが選択された。
- ネットワークの再設定により、現在のスタックルート スイッチ上で新しいポートがスタック ルート ポートとして選択された。

（注） 複数のイベントが同時に発生すると、高速移行が行われなくなる場合もあります。たとえば、スタック メンバの電源がオフになり、それと同時にスタック ルートをスパニングツリー ルートに接続しているリンクが回復した場合、通常のスパニングツリー コンバージェンスが発生します。

通常のスパニングツリー コンバージェンス（30 ～ 40 秒）は、次のような状況で発生します。

- スタック ルート スイッチの電源がオフになったか、またはソフトウェアに障害が発生した。
- 電源がオフになっていたか、または障害が発生していたスタック ルート スイッチの電源が入った。
- スタック ルートになる可能性のある新しいスイッチがスタックに追加された。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化（CLI），（481 ページ）
UplinkFast，（465 ページ）
クロススタック UplinkFast，（468 ページ）

クロススタック UplinkFast の動作, （468 ページ）

BackboneFast

BackboneFastは、バックボーンのコアにおける間接障害を検出します。BackboneFastは、UplinkFast機能を補完するテクノロジーです。UplinkFast は、アクセス スイッチに直接接続されたリンクの障害に対応します。BackboneFast は、最大エージング タイマーを最適化します。最大エージングタイマーによって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御されます。スイッチが別のスイッチの指定ポートから下位 BPDU を受信した場合、BPDUは他のスイッチでルートまでのパスが失われた可能性を示すシグナルとなり、BackboneFastはルートまでの別のパスを見つけようとします。

スイッチのルートポートまたはブロックされたインターフェイスが、指定スイッチから下位BPDUを受け取ると、BackboneFast が開始します。下位 BPDU は、ルート ブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位 BPDU を受信した場合、そのスイッチが直接接続されていないリンク（間接リンク）で障害が発生したことを意味します（指定スイッチとルート スイッチ間の接続が切断されています）。スパニングツリーのルールに従い、スイッチは最大エージング タイム（デフォルトは 20 秒）の間、下位 BPDU を無視します。

スイッチは、ルート スイッチへの代替パスの有無を判別します。下位BPDUがブロック インターフェイスに到達した場合、スイッチ上のルート ポートおよび他のブロック インターフェイスがルート スイッチへの代替パスになります（セルフループ ポートはルート スイッチの代替パスとは見なされません）。下位 BPDU がルート ポートに到達した場合には、すべてのブロック インターフェイスがルートスイッチへの代替パスになります。下位BPDUがルートポートに到達し、しかもブロックインターフェイスがない場合、スイッチはルートスイッチへの接続が切断されたものと見なし、ルートポートの最大エージングタイムが経過するまで待ち、通常のスパニングツリー ルールに従ってルート スイッチになります。

スイッチが代替パスでルート スイッチに到達できる場合、スイッチはその代替パスを使用して、Root Link Query（RLQ）要求を送信します。スイッチは、スタック メンバーがルート スイッチへの代替ルートを持つかどうかを学習するために、すべての代替パスにRLQ要求を送信し、ネットワーク内およびスタック内の他のスイッチからのRLQ応答を待機します。スイッチは、すべての代替パスに RLQ 要求を送信し、ネットワーク内の他のスイッチからの RLQ 応答を待機します。

スタック メンバが、ブロック インターフェイス上の非スタック メンバから RLQ 応答を受信し、その応答が他の非スタック スイッチ宛てのものであった場合、そのスタック メンバは、スパニングツリー インターフェイス ステートに関係なく、その応答パケットを転送します。

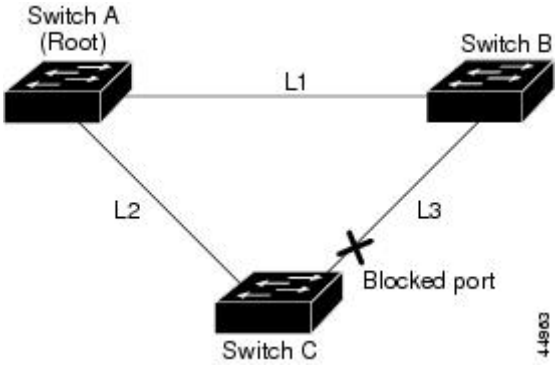
スタック メンバが非スタック メンバから RLQ 応答を受信し、その応答がスタック宛てのものであった場合、そのスタック メンバは、他のすべてのスタック メンバがその応答を受信するようにその応答を転送します。

ルートへの代替パスがまだ存在していると判断したスイッチは、下位 BPDU を受信したインターフェイスの最大エージングタイムが経過するまで待ちます。ルートスイッチへのすべての代替パスが、スイッチとルート スイッチ間の接続が切断されていることを示している場合、スイッチは RLQ 応答を受信したインターフェイスの最大エージング タイムを満了させます。1 つまたは複数の代替パスからルート スイッチへ引き続き接続できる場合、スイッチは下位BPDUを受信したすべてのインターフェイスを指定ポートにして、（ブロッキング ステートになっていた場合）ブ

ロッキング ステートを解除し、リスニング ステート、ラーニング ステートを経てフォワーディング ステートに移行させます。

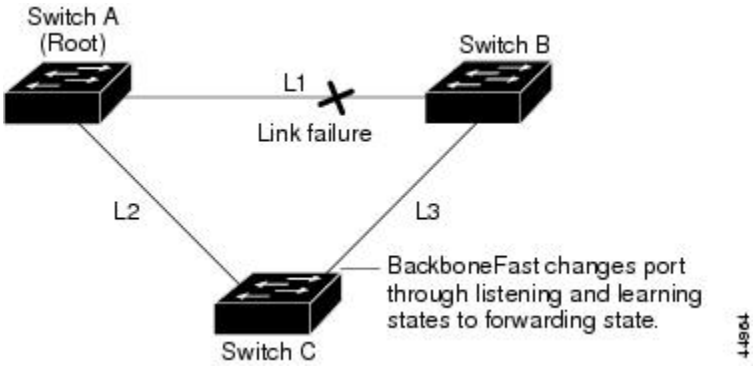
これは、リンク障害が発生していないトポロジ例です。ルート スイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 *29*：間接リンク障害が発生する前の *BackboneFast* の例



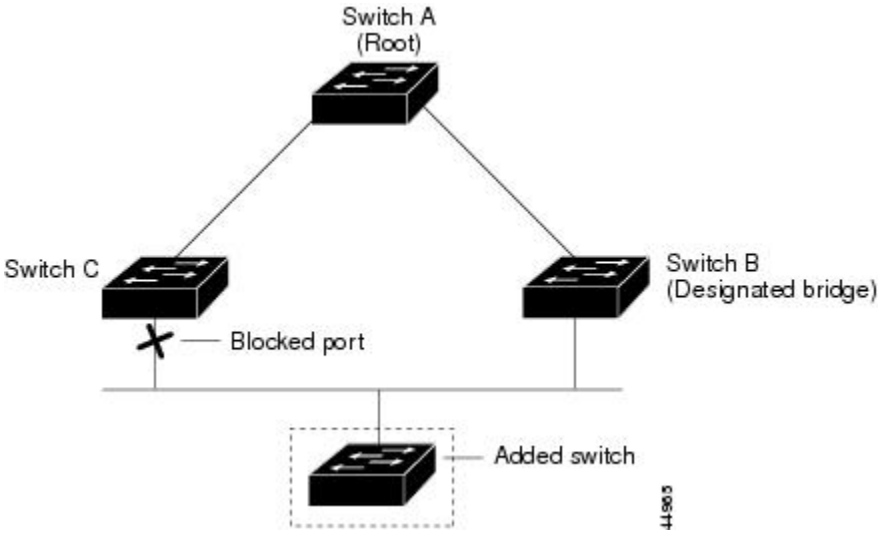
リンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、この障害を検出できません。一方スイッチ B は、L1 によってルート スイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。BackboneFast は、次に、スイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを提供します。ルートスイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に設定されていればその倍の時間です。BackboneFast がリンク L1 で発生した障害に応じてトポロジを再設定します。

図 *30*：間接リンク障害が発生したあとの *BackboneFast* の例



新しいスイッチがメディア共有型トポロジに組み込まれた場合、認識された指定スイッチ（スイッチ B）から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。新しいスイッチは、自身がルート スイッチであることを伝える下位 BPDU の送信を開始します。ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定スイッチであることを学習します。

図 *31*：メディア共有型トポロジにおけるスイッチの追加



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI），（440 ページ）
MSTP 設定時の注意事項，（422 ページ）
MST リージョン，（424 ページ）
BackboneFast をイネーブル化（CLI），（484 ページ）

EtherChannel ガード

EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾が発生します。また、EtherChannel の両端でチャネルのパラメータが異なる場合にも、設定の矛盾が発生します。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのインターフェイスを errdisable ステートにし、エラー メッセージを表示します。

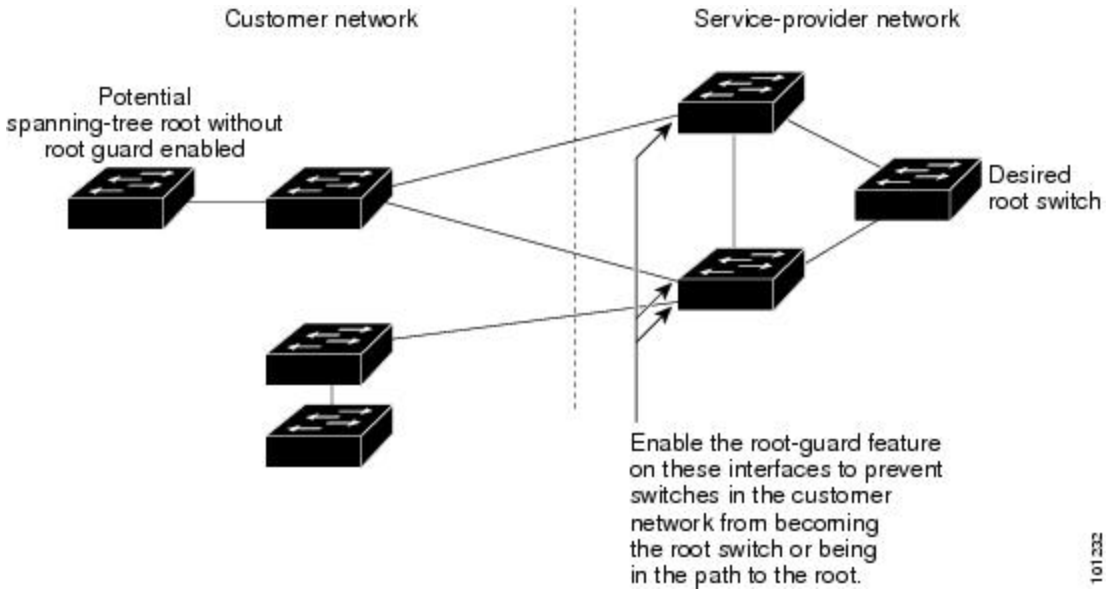
関連トピック

EtherChannel ガードのイネーブル化（CLI），（485 ページ）

ルート ガード

サービス プロバイダー（SP）のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多く含まれている場合があります。このようなトポロジでは、スパニングツリーが再構成され、カスタマースイッチをルート スイッチとして選択する可能性があります。この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルート ガード機能をイネーブルに設定します。スパニングツリーの計算によってカスタマー ネットワーク内のインターフェイスがルート ポートとして選択されると、ルート ガードがそのインターフェイスを root-inconsistent（ブロッキング）ステートにして、カスタマーのスイッチがルート スイッチにならないようにするか、ルートへのパスに組み込まれないようにします。

図 *32*：サービス プロバイダー ネットワークのルート ガード



SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ（root-inconsistent ステートになり）、スパニングツリーが新しいルート スイッチを選択します。カスタマーのスイッチがルート スイッチになることはありません。ルートへのパスに組み込まれることもありません。

スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定ポートにします。また、境界ポートがルート ガードによって Internal Spanning-Tree（IST）インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インスタンスでもブロックされます。境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。VLAN は、MST インスタンスに対してグループ化された後、マッピングされます。

注意 ルート ガード機能を誤って使用すると、接続が切断されることがあります。

関連トピック

ルート ガードのイネーブル化（CLI），（486 ページ）

ループ ガード

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチド ネットワーク全体でイネーブルにした場合に最も効果があります。ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされている場合でのみ、非境界ポートで BPDU を送信しません。境界ポートでは、ループ ガードがすべての MST インスタンスでインターフェイスをブロックします。

関連トピック

ループ ガードのイネーブル化（CLI），（488 ページ）

オプションのスパニングツリー機能の設定方法

PortFast のイネーブル化（CLI）

PortFast機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、すぐにスパニングツリー フォワーディング ステートに移行されます。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

注意 PortFastを使用するのは、1つのエンドステーションがアクセスポートまたはトランクポートに接続されている場合に限定されます。スイッチまたはハブに接続するインターフェイス上でこの機能をイネーブルにすると、スパニングツリーがネットワークループを検出または阻止できなくなり、その結果、ブロードキャストストームおよびアドレスラーニングの障害が起きる可能性があります。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree portfast** [**trunk**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ2	**configureterminal** 例： スイッチ# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ4	**spanning-tree portfast** [**trunk**] 例： スイッチ(config-if)#	単一ワークステーションまたはサーバに接続されたアクセスポート上でPortFastをイネーブルにします。**trunk**キーワードを指定すると、トランクポート上でPortFastをイネーブルにできます。

	コマンドまたはアクション	目的
	spanning-tree portfast trunk	（注） トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランク ポート上では機能しないためです。 トランク ポート上で PortFast をイネーブルにする場合は、事前に、トランク ポートとワークステーションまたはサーバの間にループがないことを確認してください。 デフォルトでは、PortFast はすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

次の作業

spanning-tree portfast default グローバル コンフィギュレーション コマンドを使用すると、すべての非トランク ポート上で PortFast 機能をグローバルにイネーブルにできます。

関連トピック

PortFast, （463 ページ）
オプションのスパニング ツリー機能の制約事項

BPDU ガードのイネーブル化（CLI）

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU ガード機能をイネーブルにできます。

注意 PortFast エッジは、エンド ステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree portfast edge bpduguard default**
4. **interface***interface-id*
5. **spanning-tree portfast edge**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree portfast edge bpduguard default** 例： スイッチ(config)# **spanning-tree portfast edge bpduguard default**	BPDU ガードをグローバルにイネーブルにします。 BPDU ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	エンド ステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**spanning-tree portfast edge** 例： スイッチ(config-if)# **spanning-tree portfast edge**	PortFast エッジ機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

次の作業

ポートのシャットダウンを防ぐには、**errdisable detect cause bpduguard shutdown vlan** グローバル コンフィギュレーション コマンドを使用すると、違反の発生時にポートで問題になっている VLAN のみをシャットダウンできます。

PortFast エッジ機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにすることもできます。BPDU を受信したポートは、errdisable ステートになります。

関連トピック

BPDU ガード, （464 ページ）

BPDU フィルタリングのイネーブル化（CLI）

PortFast エッジ機能をイネーブルにしなくても、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイスで BPDU フィルタリングをイネーブルにすることもできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。

注意 BPDUフィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU フィルタリング機能をイネーブルにできます。

注意 PortFast エッジは、エンド ステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree portfast edge bpdufilter default**
4. **interface***interface-id*
5. **spanning-tree portfast edge**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**spanning-tree portfast edge bpdufilter default** 例： スイッチ(config)# **spanning-tree portfast edge bpdufilter default**	BPDU フィルタリングをグローバルにイネーブルにします。 BPDU フィルタリングは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	エンドステーションに接続するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 5	**spanning-tree portfast edge** 例： スイッチ(config-if)# **spanning-tree portfast edge**	指定したインターフェイスで PortFast エッジ機能をイネーブルにします。
ステップ 6	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

関連トピック

BPDU フィルタリング，（465 ページ）

冗長リンクで使用するための UplinkFast のイネーブル化（CLI）

（注） UplinkFast をイネーブルにすると、スイッチまたはスイッチ スタックのすべての VLAN に影響します。個々の VLAN について UplinkFast を設定することはできません。

Rapid PVST+ または MSTP に対して UplinkFast または Cross-Stack UplinkFast（CSUF）機能を設定できますが、この機能は、スパニングツリーのモードを PVST+ に変更するまではディセーブル（非アクティブ）になったままです。

この手順は任意です。UplinkFast および CSUF をイネーブルにするには、次の手順に従います。

はじめる前に

スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにすることはできません。スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにする場合は、最初に **no spanning-tree vlan***vlan-id***priority** グローバル コンフィギュレーション コマンドを使用することによって、VLAN のスイッチ プライオリティをデフォルト値に戻す必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree uplinkfast** [**max-update-rate***pkts-per-second*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree uplinkfast** [**max-update-rate***pkts-per-second*] 例： スイッチ(config)# **spanning-tree uplinkfast max-update-rate 200**	UplinkFast をイネーブルにします。 （任意）*pkts-per-second* に指定できる範囲は毎秒 0 ～ 32000 パケットです。デフォルト値は 150 です。 0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。 このコマンドを入力すると、すべての非スタック ポート インターフェイス上で CSUF もイネーブルになります。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティは 49152 に設定されます。UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します（パス コストを 3000 以上の値に変更した場合、パス コストは変更されません）。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をイネーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにイネーブルになります。

関連トピック

UplinkFast, （465 ページ）
クロススタック UplinkFast, （468 ページ）
クロススタック UplinkFast の動作, （468 ページ）
高速コンバージェンスを発生させるイベント, （470 ページ）

UplinkFast のディセーブル化（CLI）

この手順は任意です。

UplinkFast および Cross-Stack UplinkFast（SUF）をディセーブルにするには、次の手順に従います。

はじめる前に

UplinkFast を有効にする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **no spanning-tree uplinkfast**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree uplinkfast** 例： スイッチ(config)# **no spanning-tree uplinkfast**	スイッチおよびそのスイッチのすべての VLAN で UplinkFast および CSUF をディセーブルにします。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をディセーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにディセーブルになります。

BackboneFast をイネーブル化（CLI）

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニングツリーの再構成をより早く開始できます。

Rapid PVST+ または MSTP に対して BackboneFast 機能を設定できます。ただし、スパニングツリーモードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

この手順は任意です。スイッチ上で BackboneFast をイネーブルにするには、次の手順に従います。

はじめる前に

BackboneFast を使用する場合は、ネットワーク上のすべてのスイッチでイネーブルする必要があります。BackboneFast は、トークンリング VLAN ではサポートされません。この機能は他社製スイッチでの使用にサポートされています。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree backbonefast**
4. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree backbonefast** 例： `スイッチ(config)# spanning-tree backbonefast`	BackboneFast をイネーブルにします。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

関連トピック

BackboneFast, （471 ページ）

EtherChannel ガードのイネーブル化（CLI）

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、EtherChannel の設定の矛盾を検出する EtherChannel ガード機能をイネーブルにできます。

この手順は任意です。

スイッチで EtherChannel ガードをイネーブルにするには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree etherchannel guard misconfig**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree etherchannel guard misconfig** 例： スイッチ(config)# **spanning-tree etherchannel guard misconfig**	EtherChannel ガードをイネーブルにします。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

次の作業

show interfaces status err-disabled 特権 EXEC コマンドを使用することで、EtherChannel の設定矛盾が原因でディセーブルになっているスイッチ ポートを表示できます。リモート デバイス上では、**show etherchannel summary** 特権 EXEC コマンドを使用して、EtherChannel の設定を確認できます。

設定を修正した後、誤って設定していたポート チャネル インターフェイス上で、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してください。

関連トピック

EtherChannel ガード, （473 ページ）

ルート ガードのイネーブル化（CLI）

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロック ステートの）バックアップ インターフェイスがルート ポートになります。ただし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。

（注） ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。

スイッチ上でルート ガードをイネーブルにするには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree guard root**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree guard root** 例： `スイッチ(config-if)# spanning-tree guard root`	インターフェイス上でルート ガードをイネーブルにします。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセーブルです。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

関連トピック

ルート ガード, （474 ページ）

ループ ガードのイネーブル化（CLI）

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。ループ ガードは、スパニングツリーがポイントツーポイントと見なすインターフェイス上でのみ動作します。

（注） ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。スイッチでループ ガードをイネーブルにするには、次の手順に従います。

手順の概要

1. 次のいずれかのコマンドを入力します。
   - **show spanning-tree active**
   - **show spanning-tree mst**
2. **configure terminal**
3. **spanning-tree loopguard default**
4. **end**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	次のいずれかのコマンドを入力します。
	• **show spanning-tree active**
	• **show spanning-tree mst**
	
	例：
	`スイッチ# show spanning-tree active`
	または
	`スイッチ# show spanning-tree mst`
		どのインターフェイスが代替ポートまたはルート ポートであるかを確認します。

ステップ 2	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree loopguard default** 例： `スイッチ(config)# spanning-tree loopguard default`	ループ ガードをイネーブルにします。 ループ ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ループ ガード, （475 ページ）

スパニングツリー ステータスのモニタリング

表 *37* : スパニングツリー ステータスをモニタリングするコマンド

コマンド	目的
show spanning-tree active	アクティブインターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface*interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree mst interface*interface-id*	指定インターフェイスの MST 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。またはスパニングツリー ステート セクションのすべての行を表示します。
show spanning-tree mst interface*interface-id***portfast edge**	指定したインターフェイスのスパニングツリー portfast 情報を表示します。

オプションのスパニング ツリー機能に関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	LAN Switching Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches).

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

オプションのスパニングツリー機能の機能情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 24 章

EtherChannel の設定

- 機能情報の確認，493 ページ
- EtherChannel の制約事項，493 ページ
- EtherChannel について，494 ページ
- EtherChannel の設定方法，513 ページ
- EtherChannel、PAgP、および LACP ステータスのモニタ，529 ページ
- EtherChannel の設定例，530 ページ
- EtherChannels の追加リファレンス，532 ページ
- EtherChannels の機能情報，533 ページ

機能情報の確認

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

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

EtherChannel の制約事項

次に、EtherChannels の制約事項を示します。

- EtherChannel のすべてのポートは同じ VLAN に割り当てるか、またはトランク ポートとして設定する必要があります。

- LAN Base ライセンス フィーチャ セットを実行している場合は、レイヤ 3 EtherChannels はサポートされません。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

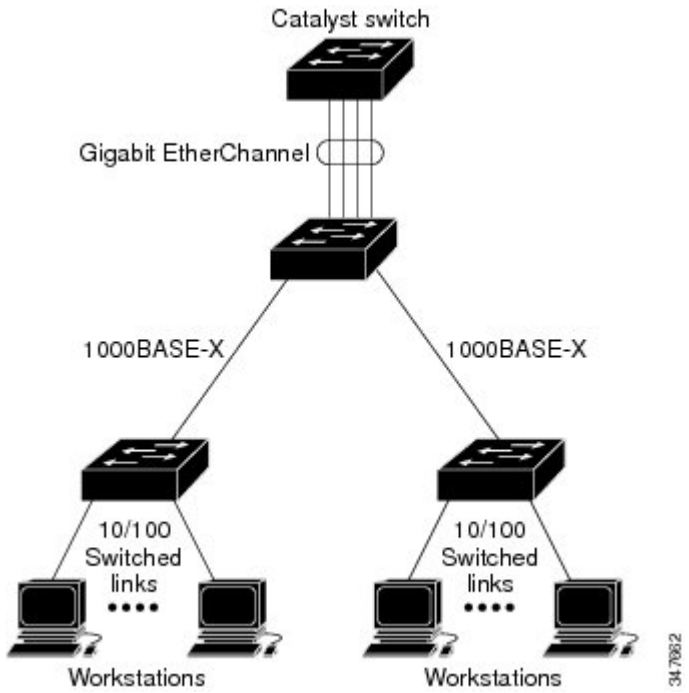
EtherChannel について

EtherChannel の概要

EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用して、ワイヤリング クローゼットとデータセンター間の帯域幅を増やすことができます。さらに、ボトルネックが発生しやすいネットワーク上のあらゆる場所に EtherChannel を配置できます。EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャネル内の他のリンクにトラフィックをリダイレクトします。

EtherChannel は、単一の論理リンクにバンドルする個別のイーサネット リンクで構成されます。

図 *33*：一般的な *EtherChannel* 構成



EtherChannel は、スイッチ間またはスイッチとホスト間に、最大 8 Gb/s（ギガビット EtherChannel）または 80 Gb/s（10 ギガビット EtherChannel）の全二重帯域幅を提供します。

各 EtherChannel は、互換性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

EtherChannel の最大数は 128 に制限されています。

LAN Base フィーチャ セットでは、最大 24 個の EtherChannel をサポートします。

各 EtherChannel 内のすべてのポートは、レイヤ 2 またはレイヤ 3 ポートのいずれかとして設定する必要があります。EtherChannel レイヤ 3 ポートは、ルーテッドポートで構成されます。ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ 3 モードに設定された物理ポートです。詳細については、「Configuring Interface Characteristics」を参照してください。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI）, （513 ページ）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）

EtherChannel のモード

EtherChannel は、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、または On のいずれかのモードに設定できます。EtherChannel の両端は同じモードで設定します。

- EtherChannel の一方の端を PAgP または LACP モードに設定すると、システムはもう一方の端とネゴシエーションし、アクティブにするポートを決定します。リモート ポートが EtherChannel とネゴシエーションができない場合、ローカル ポートは独立ステートになり、他の単一リンクと同様にデータ トラフィックを引き続き伝送します。ポート設定は変更されませんが、ポートは EtherChannel に参加しません。
- EtherChannel を **on** モードに設定すると、ネゴシエーションは実行されません。スイッチは EtherChannel 内で互換性のあるすべてのポートを強制的にアクティブにします。EtherChannel のもう一方の端（他のスイッチ上）も、同じように **on** モードに設定する必要があります。それ以外を設定した場合、パケットの損失が発生する可能性があります。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI）, （513 ページ）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）

スイッチ上の EtherChannel

スイッチ上、スタックの単一スイッチ上、またはスタックの複数スイッチ上（クロススタック EtherChannel とも呼ぶ）で EtherChannel を作成できます。

図 *34*：単一スイッチ *EtherChannel*

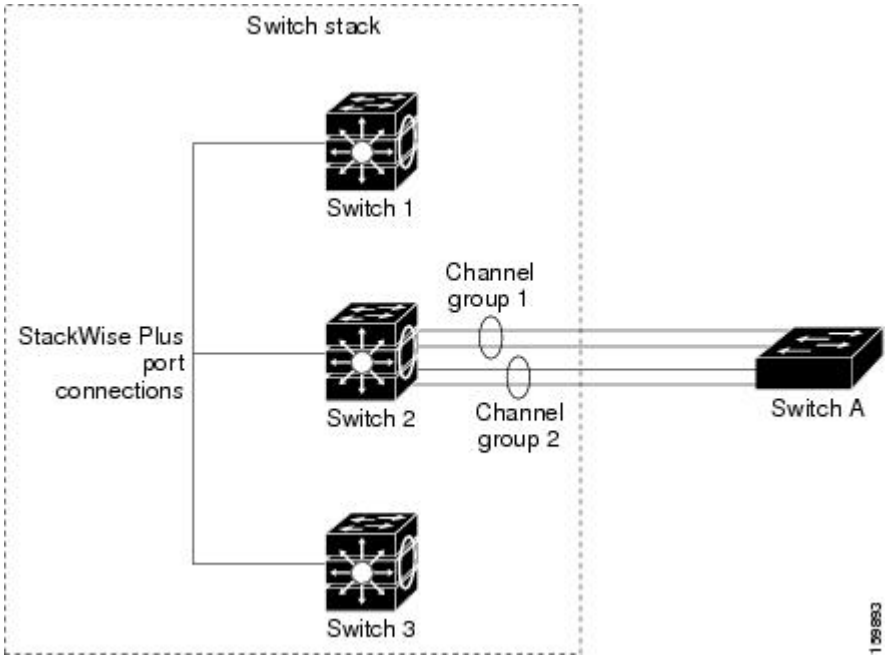
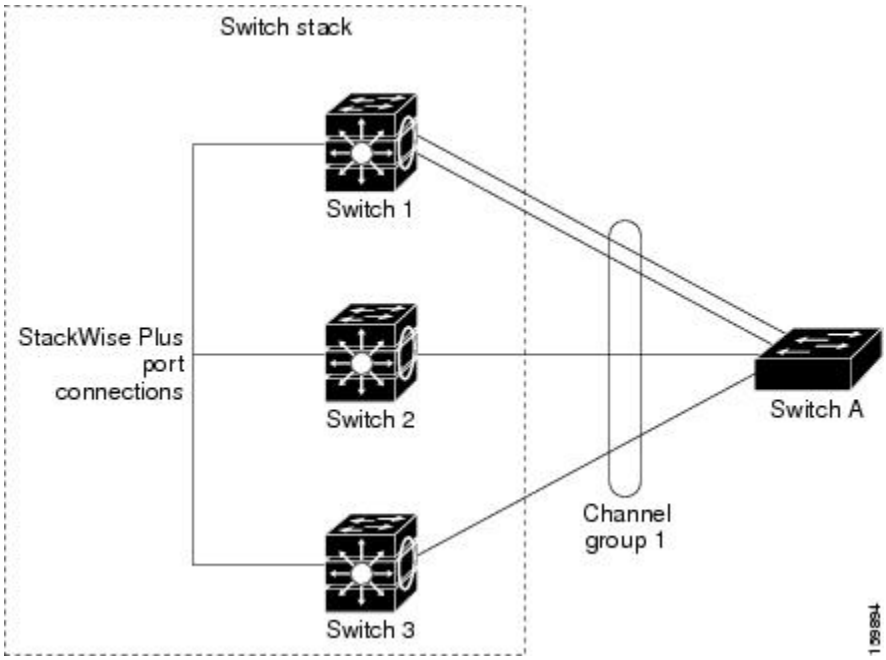


図 *35*：クロススタック *EtherChannel*



関連トピック

レイヤ 2 EtherChannel の設定 （CLI），（513 ページ）
EtherChannel 設定時の注意事項，（510 ページ）
EtherChannel のデフォルト設定，（508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）

EtherChannel リンクのフェールオーバー

EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが EtherChannel 内の残りのリンクに切り替えられます。スイッチでトラップがイネーブルになっている場合、スイッチ、EtherChannel、および失敗したリンクを区別したトラップが送信されます。EtherChannel の 1 つのリンク上の着信ブロードキャストおよびマルチキャスト パケットは、EtherChannel の他のリンクに戻らないようにブロックされます。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI），（513 ページ）
EtherChannel 設定時の注意事項，（510 ページ）
EtherChannel のデフォルト設定，（508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）

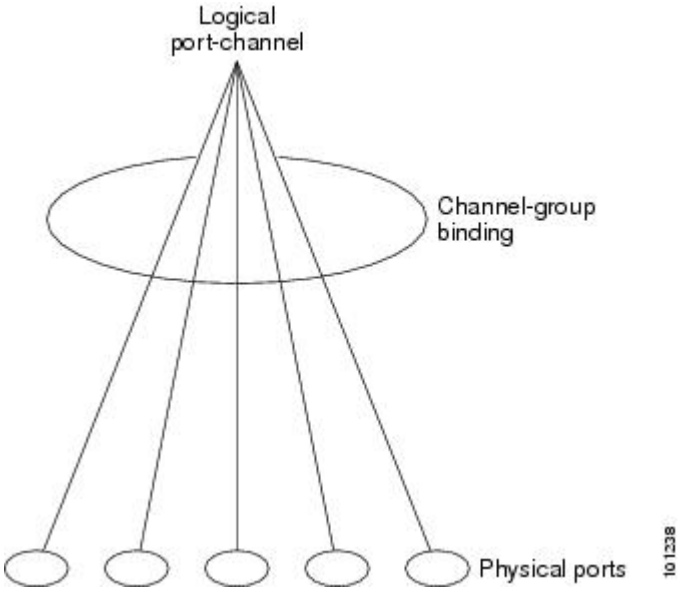
チャネル グループおよびポートチャネル インターフェイス

EtherChannel は、チャネル グループとポートチャネル インターフェイスから構成されます。チャネル グループはポートチャネルインターフェイスに物理ポートをバインドします。ポートチャネ

ルインターフェイスに適用した設定変更は、チャネル グループにまとめてバインドされるすべての物理ポートに適用されます。

channel-group コマンドは、物理ポートおよびポートチャネル インターフェイスをまとめてバインドします。各 EtherChannel には 1 ～ 128 までの番号が付いたポートチャネル論理インターフェイスがあります。このポートチャネル インターフェイス番号は、**channel-group** インターフェイス コンフィギュレーション コマンドで指定した番号に対応しています。

図 *36*：物理ポート、チャネル グループおよびポートチャネル インターフェイスの関係



- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル インターフェイスを動的に作成します。

  また、**interface port-channel***port-channel-number* グローバル コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group** *channel-group-number* コマンドを使用する必要があります。*channel-group-number* は *port-channel-number* と同じ値に設定することも、違う値を使用することもできます。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポートチャネルを作成します。

- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。その後、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

- レイヤ 3 ポートでレイヤ 3 インターフェイスとしてインターフェイスを設定するには、**no switchport** インターフェイス コマンドを使用した上で **channel-group** インターフェイス コンフィギュレーション コマンドを使用して動的にポートチャネル インターフェイスを作成します。

関連トピック

ポートチャネル論理インターフェイスの作成 （CLI）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）
物理インターフェイスの設定（CLI）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）

Port Aggregation Protocol; ポート集約プロトコル

ポート集約プロトコル（PAgP）はシスコ独自のプロトコルで、Cisco スイッチおよび PAgP をサポートするベンダーによってライセンス供与されたスイッチでのみ稼働します。PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチまたはスイッチ スタックは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似している（スタック内の単一スイッチ上の）ポートを、単一の論理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、PAgP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクを EtherChannel にグループ化した後で、PAgP は単一スイッチ ポートとして、スパニングツリーにそのグループを追加します。

PAgP モード

PAgP モードは、PAgP ネゴシエーションを開始する PAgP パケットをポートが送信できるか、または受信した PAgP パケットに応答できるかを指定します。

表 *38* : *EtherChannel PAgP* モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。これにより、PAgP パケットの送信は最小限に抑えられます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。EtherChannel メンバが、スイッチ スタックにある異なるスイッチから（クロススタック EtherChannel）の場合、このモードはサポートされません。

スイッチ ポートは、**auto** モードまたは **desirable** モードに設定された相手ポートとだけ PAgP パケットを交換します。**on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

PAgP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **desirable** モードのポートは、**desirable** モードまたは **auto** モードの別のポートとともに EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートとともに EtherChannel を形成できます。

どのポートも PAgP ネゴシエーションを開始しないため、**auto** モードのポートは、**auto** モードの別のポートとは EtherChannel を形成できません。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI）, （513 ページ）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）
物理インターフェイスの設定（CLI）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）

サイレント モード

PAgP 対応のデバイスにスイッチを接続する場合、**non-silent** キーワードを使用すると、非サイレント動作としてスイッチ ポートを設定できます。**auto** モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレント モードが指定されていると見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにスイッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼働させると、このスイッチ ポートが動作しなくなります。ただし、サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI）, （513 ページ）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）

ポートチャネル論理インターフェイスの作成 （CLI）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）

物理インターフェイスの設定（CLI）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）

PAgP 学習方式およびプライオリティ

ネットワーク デバイスは、PAgP 物理ラーナーまたは集約ポート ラーナーに分類されます。物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。集約（論理）ポートによってアドレスを学習するデバイスは、集約ポート ラーナーです。学習方式は、リンクの両端で同一の設定にする必要があります。

デバイスとそのパートナーが両方とも集約ポート ラーナーの場合、論理ポートチャネル上のアドレスを学習します。デバイスは EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポート ラーナーの場合には自動検出できません。したがって、物理ポートでアドレスを学習するには、ローカル デバイスに手動で学習方式を設定する必要があります。また、負荷の分散方式を送信元ベース分散に設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要もあります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホット スタンバイに使用することもできます。選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。パケット伝送用に常に選択されるようにポートを設定するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。

（注） CLI で **physical-port** キーワードを指定した場合でも、スイッチがサポートするのは、集約ポート上でのアドレス ラーニングのみです。**pagp learn-method** コマンドおよび **pagp port-priority** コマンドは、スイッチのハードウェアには作用しませんが、Catalyst 1900 スイッチなどの物理ポートによるアドレス ラーニングだけをサポートするデバイスと PAgP の相互運用性を確保するために必要です。

スイッチのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポート ラーナーとしてスイッチを設定することを推奨します。送信元 MAC アドレスに基づいて負荷の分散方式を設定するには、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用します。すると、スイッチは送信元アドレスを学習した EtherChannel 内の同じポートを使用して、物理ラーナーにパケットを送信します。**pagp learn-method** コマンドは、このような場合のみ使用してください。

関連トピック

PAgP 学習方式およびプライオリティの設定 （CLI），（521 ページ）
EtherChannel 設定時の注意事項，（510 ページ）
EtherChannel のデフォルト設定，（508 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ，（529 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）

PAgP と他の機能との相互作用

ダイナミック トランキング プロトコル（DTP）および Cisco Discovery Protocol（CDP）は、EtherChannel の物理ポートを使用してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で PAgP プロトコル データ ユニット（PDU）を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。レイヤ 3 EtherChannel の場合は、（**interface port-channel** グローバル コンフィギュレーション コマンドを使用して）ポートが作成された直後に、アクティブなスイッチによって MAC アドレスが割り当てられます。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼働状態のポート上だけです。

Link Aggregation Control Protocol

LACP は IEEE 802.3ad で定義されており、Cisco スイッチが IEEE 802.3ad プロトコルに適合したスイッチ間のイーサネット チャネルを管理できるようにします。LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチまたはスイッチ スタックは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単

一の倫理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、LACP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成した後で、LACP は単一スイッチ ポートとして、スパニングツリーにそのグループを追加します。

LACP モード

LACP モードでは、ポートが LACP パケットを送信できるか、LACP パケットの受信のみができるかどうかを指定します。

表 *39*：*EtherChannel LACP* モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。これにより、LACP パケットの送信を最小限に抑えます。

active モードおよび **passive LACP** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

LACP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** モードまたは **passive** モードの別のポートとともに EtherChannel を形成できます。
- 両ポートとも LACP ネゴシエーションを開始しないため、**passive** モードのポートは、**passive** モードの別のポートと EtherChannel を形成することはできません。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI），（513 ページ）
EtherChannel 設定時の注意事項，（510 ページ）
EtherChannel のデフォルト設定，（508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）

LACP とリンクの冗長性

LACP ポートチャネルの最小リンクおよびLACP の最大バンドルの機能を使用して、LACP ポートチャネル動作、帯域幅の可用性およびリンク冗長性をさらに高めることができます。

LACP ポートチャネルの最小リンク機能：

- LACP ポート チャネルでリンクし、バンドルする必要があるポートの最小数を設定します。
- 低帯域幅の LACP ポート チャネルがアクティブにならないようにします。
- 必要な最低帯域幅を提供する十分なアクティブ メンバ ポートがない場合、LACP ポートチャネルが非アクティブになるようにします。

LACP の最大バンドル機能：

- LACP ポート チャネルのバンドル ポートの上限数を定義します。
- バンドル ポートがより少ない場合のホット スタンバイ ポートを可能にします。たとえば、5 個のポートがある LACP ポート チャネルで、3 個の最大バンドルを指定し、残りの 2 個のポートをホット スタンバイ ポートとして指定できます。

関連トピック

LACP 最大バンドル機能の設定（CLI），（523 ページ）
LACP ホット スタンバイ ポートの設定：例，（531 ページ）
LACP ポート チャネルの最小リンク機能の設定（CLI），（524 ページ）
LACP ホット スタンバイ ポートの設定：例，（531 ページ）

LACP と他の機能との相互作用

DTP および CDP は、EtherChannel の物理ポートを介してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。レイヤ 3 EtherChannel の場合は、**interface port-channel** グローバル コンフィギュレーション コマンドでインターフェイスが作成された直後に、アクティブなスイッチによって MAC アドレスが割り当てられます。

LACP が LACP PDU を送受信するのは、LACP が active モードまたは passive モードでイネーブルになっている稼働状態のポートとの間だけです。

EtherChannel の On モード

EtherChannel の **on** モードは、EtherChannel の手動設定に使用します。**on** モードを使用すると、ポートはネゴシエーションせずに強制的に EtherChannel に参加します。リモート デバイスが PAgP や LACP をサポートしていない場合にこの **on** モードが役立ちます。**on** モードでは、リンクの両端のスイッチが **on** モードに設定されている場合のみ EtherChannel を使用できます。

同じチャネル グループの **on** モードで設定されたポートは、速度やデュプレックスのようなポート特性に互換性を持たせる必要があります。**on** モードで設定されている場合でも、互換性のないポートは suspended ステートになります。

注意 **on** モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパニングツリー ループが発生することがあります。

ロードバランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル内の 1 つのリンクを選択する数値に縮小することによって、チャネル内のリンク間でトラフィックのロード バランシングを行います。MAC アドレス、IP アドレス、送信元アドレス、宛先アドレス、または送信元と宛先両方のアドレスに基づいた負荷分散など、複数の異なるロード バランシング モードから 1 つを指定できます。選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。

グローバル コンフィギュレーション コマンド **port-channel load-balance** および **port-channel load-balance extended** を使用して、ロードバランシングおよび転送方式を設定します。

関連トピック

EtherChannel ロードバランシングの設定（CLI），（518 ページ）
EtherChannel 設定時の注意事項，（510 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）
EtherChannel のデフォルト設定，（508 ページ）
レイヤ 3 EtherChannel 設定時の注意事項，（513 ページ）

MAC アドレス転送

送信元MACアドレス転送の場合、EtherChannelに転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、ロード バランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャネル ポートを使用しますが、送信元ホストが同じパケットは同じチャネル ポートを使用します。

宛先MACアドレス転送の場合、EtherChannelに転送されたパケットは、着信パケットの宛先ホストのMACアドレスに基づいてチャネルポート間で分配されます。したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネル ポートに転送されます。

送信元および宛先MACアドレス転送の場合、EtherChannelに転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャネル ポート間で分配されます。この転送方式は、負荷分散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のスイッチに対して送信元MACアドレス転送と宛先MACアドレス転送のどちらが適切であるかが不明な場合に使用できます。送信元および宛先 MAC アドレス転送の場合、ホスト A

からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

EtherChannel ロードバランシングの設定（CLI），（518 ページ）
EtherChannel 設定時の注意事項，（510 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）
EtherChannel のデフォルト設定，（508 ページ）
レイヤ 3 EtherChannel 設定時の注意事項，（513 ページ）

IP アドレス転送

送信元 IP アドレスベース転送の場合、パケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。ロードバランシングを行うために、IP アドレスが異なるパケットはチャネルでそれぞれ異なるポートを使用しますが、IP アドレスが同じパケットはチャネルで同じポートを使用します。

宛先 IP アドレスベース転送の場合、パケットは着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。ロードバランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、チャネルの異なるチャネルポートに送信できます。異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常にチャネルの同じポートに送信されます。

送信元と宛先 IP アドレスベース転送の場合、パケットは着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたもので、特定のスイッチに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切であるか不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

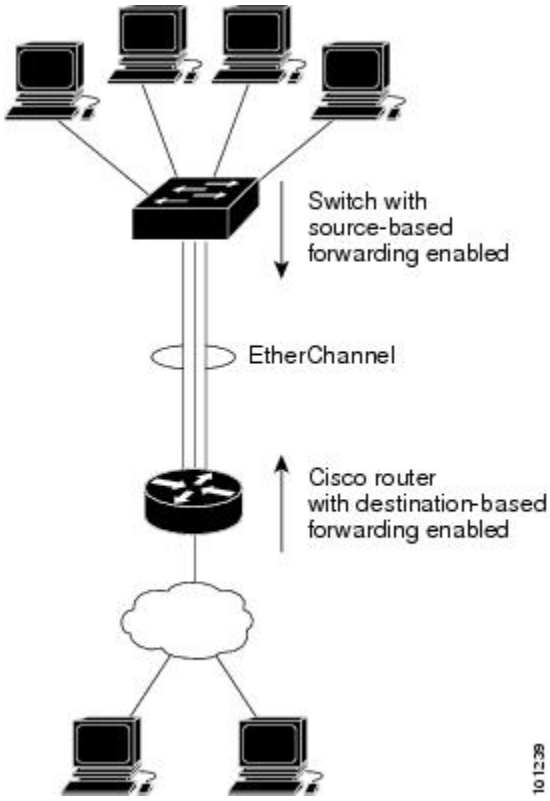
EtherChannel ロードバランシングの設定（CLI），（518 ページ）
EtherChannel 設定時の注意事項，（510 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）
EtherChannel のデフォルト設定，（508 ページ）
レイヤ 3 EtherChannel 設定時の注意事項，（513 ページ）

ロードバランシングの利点

ロードバランシング方式には異なる利点があるため、ネットワーク内のスイッチの位置、および負荷分散が必要なトラフィックの種類に基づいて特定のロードバランシング方式を選択する必要があります。

次の図では、4 台のワーク ステーションの EtherChannel がルータと通信します。ルータは単一 MAC アドレス デバイスであるため、スイッチ EtherChannel で送信元ベース転送を行うことにより、スイッチが、ルータで使用可能なすべての帯域幅を使用することが保証されます。ルータは、宛先アドレスベース転送を行うように設定されます。これは、多数のワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっているためです。

図 *37*：負荷の分散および転送方式



設定で一番種類が多くなるオプションを使用してください。たとえば、チャネル上のトラフィックが単一 MAC アドレスを宛先とする場合、宛先 MAC アドレスを使用すると、チャネル内の同じリンクが常に選択されます。ただし、送信元アドレスまたは IP アドレスを使用した方が、ロードバランシングの効率がよくなる場合があります。

関連トピック

EtherChannel ロードバランシングの設定（CLI），（518 ページ）
EtherChannel 設定時の注意事項，（510 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）
EtherChannel のデフォルト設定，（508 ページ）
レイヤ 3 EtherChannel 設定時の注意事項，（513 ページ）

EtherChannel およびスイッチ スタック

EtherChannel に加入しているポートが含まれているスタック メンバに障害が発生したり、スタックを離れると、アクティブなスイッチにより、障害が発生したスタック スイッチ メンバ ポートが削除されます。EtherChannel に残っているポートがある場合、接続は引き続き確保されます。

スイッチが既存のスタックに追加されると、新しいスイッチがアクティブなスイッチから実行コンフィギュレーションを受信し、EtherChannel 関連のスタック コンフィギュレーションで更新されます。スタック メンバでは、動作情報（動作中で、チャネルのメンバであるポートのリスト）も受信します。

2 つのスタック間で設定されている EtherChannel がマージされた場合、セルフループ ポートになります。スパニングツリーにより、この状況が検出され、必要な動作が発生します。権利を獲得したスイッチ スタックにある PAgP 設定または LACP 設定は影響を受けませんが、権利を失ったスイッチ スタックの PAgP 設定または LACP 設定は、スタックのリブート後に失われます。

スイッチ スタックおよび PAgP

PAgP では、アクティブ スイッチに障害が発生するか、スタックを離れた場合、スタンバイ スイッチが新しいアクティブ スイッチになります。EtherChannel 帯域幅に変更がない場合、スパニングツリーの再コンバージェンスはトリガーされません。新しいアクティブ スイッチはアクティブ スイッチの該当項目にスタック メンバの設定を同期します。PAgP 設定は、EtherChannel に古いアクティブ スイッチ上にあるポートがない限り、アクティブ スイッチの変更後も影響を受けません。

スイッチ スタックおよび LACP

LACP の場合、システム ID は、アクティブ スイッチから取得したスタック MAC アドレスが使用されます。アクティブ スイッチに障害が発生したり、スタックを離れ、スタンバイ スイッチが新しいアクティブ スイッチが変更になっても、LACP システム ID は変更されません。デフォルトでは、LACP 設定はアクティブ スイッチの変更後も影響を受けません。

EtherChannel のデフォルト設定

EtherChannel のデフォルト設定を、次の表に示します。

表 *40*：*EtherChannel* のデフォルト設定

機能	デフォルト設定
チャネル グループ	割り当てなし
ポートチャネル論理インターフェイス	未定義
PAgP モード	デフォルトなし。
PAgP 学習方式	すべてのポートで集約ポート ラーニング

機能	デフォルト設定
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし。
LACP 学習方式	すべてのポートで集約ポート ラーニング
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768
LACP システム ID	LACP システムのプライオリティ、スイッチまたはスタックの MAC アドレス。
ロード バランシング	スイッチ上での負荷分散は着信パケットの送信元 MAC アドレスに基づきます。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI），（513 ページ）
EtherChannel の概要，（494 ページ）
EtherChannel のモード，（495 ページ）
スイッチ上の EtherChannel，（496 ページ）
EtherChannel リンクのフェールオーバー，（497 ページ）
LACP モード，（503 ページ）
PAgP モード，（499 ページ）
サイレント モード，（500 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
チャネル グループおよびポートチャネル インターフェイス，（497 ページ）
PAgP モード，（499 ページ）
サイレント モード，（500 ページ）
物理インターフェイスの設定（CLI）
チャネル グループおよびポートチャネル インターフェイス，（497 ページ）
PAgP モード，（499 ページ）
サイレント モード，（500 ページ）
EtherChannel ロードバランシングの設定（CLI），（518 ページ）
ロードバランシングおよび転送方式，（505 ページ）
MAC アドレス転送，（505 ページ）
IP アドレス転送，（506 ページ）

ロードバランシングの利点，（506 ページ）
PAgP 学習方式およびプライオリティの設定（CLI），（521 ページ）
PAgP 学習方式およびプライオリティ，（501 ページ）
LACP システム プライオリティの設定（CLI），（526 ページ）
LACP ポート プライオリティの設定（CLI），（527 ページ）

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワーク ループおよびその他の問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。設定上の問題を回避するために、次の注意事項に従ってください。

- スイッチまたはスイッチ スタック上では、128 を超える EtherChannel を設定しないでください。
- PAgP EtherChannel は、同じタイプのイーサネット ポートを 8 つまで使用して設定します。
- 同じタイプのイーサネット ポートを最大で 16 個備えた LACP EtherChannel を設定してください。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックス モードで動作するように設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。**shutdown** インターフェイス コンフィギュレーション コマンドによってディセーブルにされた EtherChannel 内のポートは、リンク障害として扱われます。そのポートのトラフィックは、EtherChannel 内の他のポートの 1 つに転送されます。
- グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかで設定を変更した場合は、グループ内のすべてのポートでも変更する必要があります。
  - 許可 VLAN リスト
  - 各 VLAN のスパニングツリー パス コスト
  - 各 VLAN のスパニングツリー ポート プライオリティ
  - スパニングツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバになるように設定しないでください。
- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP を実行している EtherChannel グループはスタックの同一スイッチ、または異なるスイッチで共存できます。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。
- EtherChannel の一部としてセキュア ポートを設定したり、セキュア ポートの一部として EtherChannel を設定したりしないでください。

- アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。
- EtherChannel がスイッチインターフェイス上に設定されている場合、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、IEEE 802.1x をスイッチ上でグローバルにイネーブルにする前に、EtherChannel の設定をインターフェイスから削除します。
- クロススタック EtherChannel が設定されていると、スイッチ スタック パーティション、ループおよび転送の問題が発生する可能性があります。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI），（513 ページ）
EtherChannel の概要，（494 ページ）
EtherChannel のモード，（495 ページ）
スイッチ上の EtherChannel，（496 ページ）
EtherChannel リンクのフェールオーバー，（497 ページ）
LACP モード，（503 ページ）
PAgP モード，（499 ページ）
サイレント モード，（500 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
チャネル グループおよびポートチャネル インターフェイス，（497 ページ）
PAgP モード，（499 ページ）
サイレント モード，（500 ページ）
物理インターフェイスの設定（CLI）
チャネル グループおよびポートチャネル インターフェイス，（497 ページ）
PAgP モード，（499 ページ）
サイレント モード，（500 ページ）
EtherChannel ロードバランシングの設定（CLI），（518 ページ）
ロードバランシングおよび転送方式，（505 ページ）
MAC アドレス転送，（505 ページ）
IP アドレス転送，（506 ページ）
ロードバランシングの利点，（506 ページ）
PAgP 学習方式およびプライオリティの設定 （CLI），（521 ページ）
PAgP 学習方式およびプライオリティ，（501 ページ）
LACP システム プライオリティの設定（CLI），（526 ページ）
LACP ポート プライオリティの設定（CLI），（527 ページ）

レイヤ 2 EtherChannel 設定時の注意事項

レイヤ 2 EtherChannels を設定する場合は、次の注意事項に従ってください。

- EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。
- EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。VLAN 許容範囲が一致していないと、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
- スパニングツリー パス コストが異なるポートは、設定上の矛盾がない限り、EtherChannel を形成できます。異なるスパニングツリー パス コストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI）, （513 ページ）
EtherChannel の概要, （494 ページ）
EtherChannel のモード, （495 ページ）
スイッチ上の EtherChannel, （496 ページ）
EtherChannel リンクのフェールオーバー, （497 ページ）
LACP モード, （503 ページ）
PAgP モード , （499 ページ）
サイレント モード, （500 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
チャネル グループおよびポートチャネル インターフェイス, （497 ページ）
PAgP モード , （499 ページ）
サイレント モード, （500 ページ）
物理インターフェイスの設定（CLI）
チャネル グループおよびポートチャネル インターフェイス, （497 ページ）
PAgP モード , （499 ページ）
サイレント モード, （500 ページ）
EtherChannel ロードバランシングの設定（CLI）, （518 ページ）
ロードバランシングおよび転送方式, （505 ページ）
MAC アドレス転送, （505 ページ）
IP アドレス転送, （506 ページ）
ロードバランシングの利点, （506 ページ）
PAgP 学習方式およびプライオリティの設定 （CLI）, （521 ページ）
PAgP 学習方式およびプライオリティ, （501 ページ）

LACP システム プライオリティの設定（CLI），（526 ページ）
LACP ポート プライオリティの設定（CLI），（527 ページ）

レイヤ 3 EtherChannel 設定時の注意事項

- レイヤ 3 EtherChannel の場合は、レイヤ 3 アドレスをチャネル内の物理ポートでなく、ポートチャネル論理インターフェイスに割り当ててください。

関連トピック

EtherChannel ロードバランシングの設定（CLI），（518 ページ）
ロードバランシングおよび転送方式，（505 ページ）
MAC アドレス転送，（505 ページ）
IP アドレス転送，（506 ページ）
ロードバランシングの利点，（506 ページ）

EtherChannel の設定方法

EtherChannelの設定後、ポートチャネルインターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。

レイヤ 2 EtherChannel の設定 （CLI）

レイヤ 2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャネル グループにポートを割り当てます。このコマンドにより、ポートチャネル論理インターフェイスが自動的に作成されます。

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. **switchport mode** {**access** | **trunk**}
4. **switchport access vlan***vlan-id*
5. **channel-group***channel-group-number***mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive**}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet2/0/1`	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスは、物理ポートです。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 3	**switchport mode** {**access** | **trunk**} 例： `スイッチ(config-if)# switchport mode access`	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセスポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。指定できる範囲は 1 ～ 4094 です。
ステップ 4	**switchport access vlan***vlan-id* 例： `スイッチ(config-if)# switchport access vlan 22`	ポートをスタティックアクセスポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。指定できる範囲は 1 ～ 4094 です。
ステップ 5	**channel-group***channel-group-number***mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive**} 例： `スイッチ(config-if)# channel-group 5 mode auto`	チャネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 **mode** には、次のキーワードのいずれか 1 つを選択します。 • **auto**：PAgP デバイスが検出された場合にのみ、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。このキーワードは、EtherChannel メンバがスイッチ スタックの異なるスイッチのものである場合にはサポートされません。 • **desirable**：PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、

	コマンドまたはアクション	目的
		ポートはPAgPパケットを送信することによって、相手ポートとのネゴシエーションを開始します。このキーワードは、EtherChannel メンバがスイッチ スタックの異なるスイッチのものである場合にはサポートされません。 • **on**：PAgP またはLACP を使用せずにポートが強制的にチャネル化されます。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**：（任意）スイッチ が PAgP 対応のパートナーに接続されている場合、ポートが **auto** または **desirable** モードになると非サイレント動作を行うようにスイッチ ポートを設定します。**non-silent** を指定しないと、サイレントが想定されます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。 • **active**：LACP デバイスが検出された場合にのみ、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive**：ポート上でLACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 6	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel の概要，（494 ページ）
EtherChannel のモード，（495 ページ）
スイッチ上の EtherChannel，（496 ページ）
EtherChannel リンクのフェールオーバー，（497 ページ）

LACP モード, （503 ページ）
PAgP モード , （499 ページ）
サイレント モード, （500 ページ）
EtherChannel 設定時の注意事項, （510 ページ）
EtherChannel のデフォルト設定, （508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （512 ページ）

レイヤ 3 EtherChannel の設定 （CLI）

レイヤ 3 EtherChannel にイーサネット ポートを割り当てるには、この手順を実行します。この手順は必須です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **no ip address**
5. **noswitchport**
6. **channel-group***channel-group-number***mode**{**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/2**	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。

	コマンドまたはアクション	目的
		LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 4	**no ip address** 例： スイッチ(config-if)# **no ip address**	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 5	**noswitchport** 例： スイッチ(config-if)# **no switchport**	ポートをレイヤ 3 モードにします。
ステップ 6	**channel-group***channel-group-number***mode**{**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**} 例： スイッチ(config-if)# **channel-group 5 mode auto**	チャネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 **mode** には、次のキーワードのいずれか 1 つを選択します。 • **auto**：PAgP デバイスが検出された場合にのみ、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。このキーワードは、EtherChannel メンバがスイッチ スタックの異なるスイッチのものである場合にはサポートされません。 • **desirable**：PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。このキーワードは、EtherChannel メンバがスイッチ スタックの異なるスイッチのものである場合にはサポートされません。 • **on**：PAgP または LACP を使用せずにポートが強制的にチャネル化されます。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**：（任意）スイッチが PAgP 対応のパートナーに接続されている場合、ポートが **auto** または **desirable** モードになると非サイレント動作を行うようにスイッチ ポートを設定します。**non-silent** を指定しないと、サイ

	コマンドまたはアクション	目的
		レントが想定されます。サイレント設定は、ファイルサーバまたはパケットアナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャネルグループにポートを結合し、このポートが伝送に使用されます。 • **active**：LACP デバイスが検出された場合にのみ、LACP をイネーブルにします。ポートをアクティブネゴシエーション ステートにします。この場合、ポートはLACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive**：ポート上でLACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 7	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

EtherChannel ロードバランシングの設定（CLI）

複数の異なる転送方式の 1 つを使用するようにEtherChannel ロードバランシングを設定できます。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **port-channel load-balance** {**dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **extended** [**dst-ip** | **dst-mac** | **dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] | **src-dst-ip** | **src-dst-mac** **src-dst-mixed-ip-port src-dst-portsrc-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**}
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance** {**dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **extended** [**dst-ip** | **dst-mac** | **dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] | **src-dst-ip** | **src-dst-mac** **src-dst-mixed-ip-port** **src-dst-portsrc-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**} 例： スイッチ(config)# **port-channel load-balance src-mac**	EtherChannel のロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **dst-mixed-ip-port**：ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **dst-port**：宛先 TCP/UDP ポートを指定します。 • **extended**：標準コマンドで使用可能なもの以外に、送信元および宛先の方式を組み合わせた、拡張ロードバランシング方式を指定します。 • **ipv6-label**：IPv6 フロー ラベルを指定します。 • **l3-proto**：レイヤ 3 プロトコルを指定します。 • **src-dst-ip**：送信元および宛先ホストの IP アドレスを指定します。 • **src-dst-mac**：送信元および宛先ホストの MAC アドレスを指定します。 • **src-dst-mixed-ip-port**：送信先および宛先ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **src-dst-port**：送信元および宛先 TCP/UDP ポートを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。 • **src-mac**：着信パケットの送信元 MAC アドレスを指定します。 • **src-mixed-ip-port**：送信元ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **src-port**：送信元 TCP/UDP ポートを指定します。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ロードバランシングおよび転送方式，（505 ページ）
MAC アドレス転送，（505 ページ）
IP アドレス転送，（506 ページ）
ロードバランシングの利点，（506 ページ）
EtherChannel 設定時の注意事項，（510 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）
EtherChannel のデフォルト設定，（508 ページ）
レイヤ 3 EtherChannel 設定時の注意事項，（513 ページ）

EtherChannel 拡張ロードバランシングの設定（CLI）

ロードバランシング方式を組み合わせて使用する場合には、拡張ロードバランシングを設定します。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **port-channel load-balance extended** [**dst-ip** | **dst-macdst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**]
3. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**port-channel load-balance extended** [**dst-ip** | **dst-macdst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] 例： スイッチ(config)# **port-channel load-balance extended dst-ip dst-mac src-ip**	EtherChannel 拡張ロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **dst-port**：宛先 TCP/UDP ポートを指定します。 • **ipv6-label**：IPv6 フロー ラベルを指定します。 • **l3-proto**：レイヤ 3 プロトコルを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。 • **src-mac**：着信パケットの送信元 MAC アドレスを指定します。 • **src-port**：送信元 TCP/UDP ポートを指定します。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

PAgP 学習方式およびプライオリティの設定 （CLI）

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **pagp learn-methodphysical-port**
4. **pagp port-priority***priority*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/2**	伝送ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**pagp learn-methodphysical-port** 例： スイッチ(config-if)# **pagp learn-method physical port**	PAgP 学習方式を選択します。 デフォルトでは、**aggregation-port learning** が選択されています。つまり、EtherChannel 内のポートのいずれかを使用して、スイッチがパケットを送信元に送信します。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。 物理ポート ラーナーである別のスイッチに接続する**物理ポート**を選択します。**port-channel load-balance** グローバル コンフィギュレーション コマンドを **src-mac** に設定してください。 学習方式はリンクの両端で同じ方式に設定する必要があります。
ステップ 4	**pagp port-priority***priority* 例： スイッチ(config-if)# **pagp port-priority 200**	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 *priority* に指定できる範囲は 0 ～ 255 です。デフォルト値は 128 です。プライオリティが高いほど、ポートが PAgP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

関連トピック

PAgP 学習方式およびプライオリティ，（501 ページ）
EtherChannel 設定時の注意事項，（510 ページ）
EtherChannel のデフォルト設定，（508 ページ）

EtherChannel、PAgP、および LACP ステータスのモニタ，（529 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）

LACP ホット スタンバイ ポートの設定

LACP がイネーブルの場合、ソフトウェアはデフォルトで、チャネルにおける LACP 互換ポートの最大数（最大 16 個のポート）の設定を試みます。一度にアクティブにできる LACP リンクは 8 つだけです。残りの 8 個のリンクがホット スタンバイ モードになります。アクティブ リンクの 1 つが非アクティブになると、ホット スタンバイ モードのリンクが代わりにアクティブになります。

チャネルでアクティブ ポートの最大数を指定することでデフォルト動作を上書きできます。この場合、残りのポートがホット スタンバイ ポートになります。たとえばチャネルで最大 5 個のポートを指定した場合、11 個までのポートがホット スタンバイ ポートになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリティに基づいてアクティブにするホット スタンバイ ポートを決定します。ソフトウェアは、LACP を操作するシステム間のすべてのリンクに、次の要素（プライオリティ順）で構成された一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID（スイッチ MAC アドレス）
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。プライオリティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバイ モードにするポートを決定します。

アクティブ ポートかホット スタンバイ ポートかを判別するには、次の（2 つの）手順を使用します。まず、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。次に、ポート プライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートとホット スタンバイ ポートを決定します。他のシステムのポート プライオリティとポート番号の値は使用されません。

ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響を与えるように、LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更できます。

LACP 最大バンドル機能の設定（CLI）

ポート チャネルで許可されるバンドル化された LACP ポートの最大数を指定すると、ポート チャネル内の残りのポートがホット スタンバイ ポートとして指定されます。

ポート チャネルの LACP ポートの最大数を設定するには、特権 EXEC モードで開始して、次の手順に従います。この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface port-channel***channel-number*
3. **lacp max-bundle** *max-bundle-number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel***channel-number* 例： `スイッチ(config)# interface port-channel 2`	ポート チャネルのインターフェイス コンフィギュレーション モードを開始します。 指定できる範囲は 1 ～ 128 です。
ステップ 3	**lacp max-bundle** *max-bundle-number* 例： `スイッチ(config-if)# lacp max-bundle 3`	ポートチャネル バンドルで LACP ポートの最大数を指定します。 指定できる範囲は 1 ～ 8 です。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

関連トピック

LACP とリンクの冗長性 , （504 ページ）
LACP ホット スタンバイ ポートの設定：例, （531 ページ）

LACP ポート チャネルの最小リンク機能の設定（CLI）

リンク アップ状態で、リンク アップ ステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるアクティブ ポートの最小数を指定できます。EtherChannel

の最小リンクを使用して、低帯域幅 LACP EtherChannel がアクティブになることを防止できます。また、LACP EtherChannel にアクティブ メンバー ポートが少なすぎて、必要な最低帯域幅を提供できない場合、この機能により LACP EtherChannel が非アクティブになります。

ポート チャネルに必要なリンクの最小数を設定する。次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel***channel-number*
4. **port-channel min-links***min-links-number*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel***channel-number* 例： スイッチ(config)# **interface port-channel 2**	ポートチャネルのインターフェイス コンフィギュレーション モードを開始します。 *channel-number* の範囲は 1 ～ 63 です。
ステップ 4	**port-channel min-links***min-links-number* 例： スイッチ(config-if)# **port-channel min-links 3**	リンク アップ状態で、リンク アップ ステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるメンバ ポートの最小数を指定できます。 *min-links-number* の範囲は 2 ～ 8 です。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

LACP とリンクの冗長性，（504 ページ）
LACP ホット スタンバイ ポートの設定：例，（531 ページ）

LACP システム プライオリティの設定（CLI）

lacp system-priority グローバル コンフィギュレーション コマンドを使用して、LACP をイネーブルにしているすべての EtherChannel に対してシステム プライオリティを設定できます。LACP を設定済みの各チャネルに対しては、システム プライオリティを設定できません。デフォルト値を変更すると、ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響します。

show etherchannel summary 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが H になっています）。

LACP システム プライオリティを設定するには、次の手順に従います。この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **lacp system-priority***priority*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lacp system-priority***priority* 例： スイッチ(config)# **lacp system-priority**	LACP システム プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。デフォルトは 32768 です。

	コマンドまたはアクション	目的
	32000	値が小さいほど、システム プライオリティは高くなります。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項，（510 ページ）
EtherChannel のデフォルト設定，（508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ，（529 ページ）

LACP ポート プライオリティの設定（CLI）

デフォルトでは、すべてのポートは同じポートプライオリティです。ローカルシステムのシステム プライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さな値に変更して、最初にアクティブになるホットスタンバイ リンクを変更できます。ホット スタンバイ ポートは、番号が小さい方が先にチャネルでアクティブになります。**show etherchannel summary** 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが H になっています）。

（注） LACP がすべての互換ポートを集約できない場合（たとえば、ハードウェアの制約が大きいリモート システム）、EtherChannel 中でアクティブにならないポートはすべてホット スタンバイ ステートになり、チャネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP ポート プライオリティを設定するには、次の手順に従います。この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **lacp port-priority***priority*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/2**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lacp port-priority***priority* 例： スイッチ(config-if)# **lacp port-priority 32000**	LACP ポート プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。デフォルトは 32768 です。値が小さいほど、ポートが LACP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項，（510 ページ）
EtherChannel のデフォルト設定，（508 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（512 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ，（529 ページ）

EtherChannel、PAgP、および LACP ステータスのモニタ

この表に記載されているコマンドを使用して EtherChannel、PAgP、および LACP ステータスを表示できます。

表 *41*：*EtherChannel*、*PAgP*、および *LACP* ステータスのモニタ用コマンド

コマンド	説明
clear lacp{*channel-group-number* **counters** | **counters**}	LACP チャネル グループ情報およびトラフィック カウンタをクリアします。
clear pagp{*channel-group-number* **counters** | **counters**}	PAgP チャネル グループ情報およびトラフィック カウンタをクリアします。
show etherchannel[*channel-group-number* {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}] [**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **auto** | **summary**]	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。負荷分散方式またはフレーム配布方式、ポート、ポート チャネル、プロトコル、および Auto-LAG 情報も表示されます。
show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 PAgP 設定、ネイバー情報などの PAgP 情報が表示されます。
show pagp [*channel-group-number*] **dual-active**	デュアルアクティブ検出ステータスが表示されます。
show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**}	トラフィック情報、内部 LACP 設定、ネイバー情報などの LACP 情報が表示されます。
show running-config	設定エントリを確認します。
show etherchannel load-balance	ポート チャネル内のポート間のロード バランシング、またはフレーム配布方式を表示します。

関連トピック

PAgP 学習方式およびプライオリティの設定 （CLI），（521 ページ）
PAgP 学習方式およびプライオリティ，（501 ページ）
LACP システム プライオリティの設定（CLI），（526 ページ）
LACP ポート プライオリティの設定（CLI），（527 ページ）

EtherChannel の設定例

レイヤ 2 EtherChannel の設定：例

この例では、スタック内の 1 つのスイッチに EtherChannel を設定する例を示します。2 つのポートを VLAN 10 のスタティック アクセス ポートとして、PAgP モードが **desirable** であるチャネル 5 に割り当てます。

```
スイッチ# configure terminal
スイッチ(config)# interface range gigabitethernet2/0/1 -2
スイッチ(config-if-range)# switchport mode access
スイッチ(config-if-range)# switchport access vlan 10
スイッチ(config-if-range)# channel-group 5 mode desirable non-silent
スイッチ(config-if-range)# end
```

この例では、スタック内の 1 つのスイッチに EtherChannel を設定する例を示します。2 つのポートは VLAN 10 のスタティックアクセス ポートとして、LACP モードが **active** であるチャネル 5 に割り当てられます。

```
スイッチ# configure terminal
スイッチ(config)# interface range gigabitethernet2/0/1 -2
スイッチ(config-if-range)# switchport mode access
スイッチ(config-if-range)# switchport access vlan 10
スイッチ(config-if-range)# channel-group 5 mode active
スイッチ(config-if-range)# end
```

次の例では、クロススタック EtherChannel を設定する方法を示します。LACP パッシブ モードを使用して、VLAN 10 内のスタティックアクセス ポートとしてスタック メンバ 1 のポートを 2 つ、スタック メンバ 2 のポートを 1 つチャネル 5 に割り当てます。

```
スイッチ# configure terminal
スイッチ(config)# interface range gigabitethernet2/0/4 -5
スイッチ(config-if-range)# switchport mode access
スイッチ(config-if-range)# switchport access vlan 10
スイッチ(config-if-range)# channel-group 5 mode passive
スイッチ(config-if-range)# exit
スイッチ(config)# interface gigabitethernet3/0/3
スイッチ(config-if)# switchport mode access
スイッチ(config-if)# switchport access vlan 10
スイッチ(config-if)# channel-group 5 mode passive
スイッチ(config-if)# exit
```

PoE または LACP ネゴシエーションのエラーは、スイッチからアクセスポイント（AP）に 2 つのポートを設定した場合に発生する可能性があります。このシナリオは、ポート チャネルの設定をスイッチ側で行うと回避できます。詳細については、次の例を参照してください。

```
interface Port-channel1
  switchport access vlan 20
 switchport mode access
  switchport nonegotiate
```

```
no port-channel standalone-disable   <--this one
spanning-tree portfast
```

（注） ポートがポートのフラッピングに関するLACPエラーを検出した場合は、次のコマンドも含める必要があります。**no errdisable detect cause pagp-flap**

レイヤ 3 EtherChannel の設定：例

この例では、レイヤ3インターフェイスの設定方法を示します。2つのポートは、LACPモードが **active** であるチャネル 5 に割り当てられます。

```
スイッチ# configure terminal
スイッチ(config)# interface range gigabitethernet2/0/1 -2
スイッチ(config-if-range)# no ip address
スイッチ(config-if-range)# no switchport
スイッチ(config-if-range)# channel-group 5 mode active
スイッチ(config-if-range)# end
```

この例では、クロススタック レイヤ 3 EtherChannel の設定方法を示します。スタック メンバー 2 の 2 つのポートとスタック メンバー 3 の 1 つのポートは、LACP active モードでチャネル 7 に割り当てられます。

```
スイッチ# configure terminal
スイッチ(config)# interface range gigabitethernet2/0/4 -5
スイッチ(config-if-range)# no ip address
スイッチ(config-if-range)# no switchport
スイッチ(config-if-range)# channel-group 7 mode active
スイッチ(config-if-range)# exit
スイッチ(config)# interface gigabitethernet3/0/3
スイッチ(config-if)# no ip address
スイッチ(config-if)# no switchport
スイッチ(config-if)# channel-group 7 mode active
スイッチ(config-if)# exit
```

LACP ホット スタンバイ ポートの設定：例

この例では、少なくとも 3 個のアクティブ ポートがある場合にアクティブ化される EtherChannel を設定する例を示します（ポート チャネル 2）。これは、7 個のアクティブ ポートとホット スタンバイ ポートとしての最大 9 個の残りのポートから構成されます。

```
スイッチ# configure terminal
スイッチ(config)# interface port-channel 2
スイッチ(config-if)# port-channel min-links 3
スイッチ(config-if)# lacp max-bundle 7
```

関連トピック

LACP 最大バンドル機能の設定（CLI），（523 ページ）
LACP とリンクの冗長性，（504 ページ）
LACP ポート チャネルの最小リンク機能の設定（CLI），（524 ページ）
LACP とリンクの冗長性，（504 ページ）

EtherChannels の追加リファレンス

関連資料

関連項目	マニュアル タイトル
レイヤ 2 コマンド リファレンス	*Layer 2/3 Command Reference (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

EtherChannels の機能情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。
Cisco IOS 15.2(3)E2、Cisco IOS XE 3.7.2E	Auto-LAG 機能が導入されました。

第 25 章

単方向リンク検出の設定

- 機能情報の確認，535 ページ
- UDLD 設定の制約事項，535 ページ
- UDLD について，536 ページ
- UDLD の設定方法，540 ページ
- UDLD のモニタおよびメンテナンス，543 ページ
- UDLD の追加リファレンス，543 ページ
- UDLD の機能情報，544 ページ

機能情報の確認

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

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

UDLD 設定の制約事項

次に、単方向リンク検出（UDLD）設定の制約事項を示します。

- UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。

- モード（通常またはアグレッシブ）を設定する場合、リンクの両側に同じモードを設定します。

注意 ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

UDLD について

UniDirectional Link Detection（UDLD）は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニタリングしたり、単一方向リンクの存在を検出できるようにするためのレイヤ 2 プロトコルです。このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。UDLD は単一方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。単一方向リンクは、スパニングツリートポロジループをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。通常モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できます。アグレッシブ モードの UDLD は、光ファイバ リンクおよびツイストペア リンク上の片方向トラフィックと、光ファイバ リンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ 1 のメカニズムを使用して、リンクの物理ステータスを学習します。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバー ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合に、単一方向リンクが発生します。

通常モード

通常モードの UDLD は、光ファイバ ポートの光ファイバが誤って接続されている場合に単一方向リンクを検出しますが、レイヤ 1 メカニズムは、この誤った接続を検出しません。ポートが正しく接続されていてもトラフィックが片方向である場合、単一方向リンクを検出するはずのレイヤ 1 メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。この場合、論理リンクは不確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ 1 メカニズムがリンクの物理的な問題を検出するため、リンクは稼働状態でなくなります。この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされます。

関連トピック

UDLD のグローバルなイネーブル化（CLI），（540 ページ）
インターフェイスでの UDLD のイネーブル化（CLI），（541 ページ）

アグレッシブ モード

アグレッシブ モードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイント リンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがトラフィックを送受信できない。
- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがダウンし、残りのインターフェイスが稼働している。
- ケーブルのうち 1 本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイント リンクでは、UDLD hello パケットをハートビートと見なすことができ、ハートビートがあればリンクは正常です。逆に、ハートビートがないということは、双方向リンクを再確立できない限り、リンクをシャットダウンする必要があることを意味しています。

レイヤ 1 の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブ モードの UDLD はそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは自動ネゴシエーションでは実行できません。

関連トピック

UDLD のグローバルなイネーブル化（CLI），（540 ページ）
インターフェイスでの UDLD のイネーブル化（CLI），（541 ページ）

単一方向の検出方法

UDLD は、2 つの方法で動作します。

- ネイバー データベース メンテナンス
- イベントドリブン検出およびエコー

関連トピック

UDLD のグローバルなイネーブル化（CLI），（540 ページ）
インターフェイスでの UDLD のイネーブル化（CLI），（541 ページ）

ネイバー データベース メンテナンス

UDLDは、アクティブな各ポート上でhelloパケット（別名アドバタイズまたはプローブ）を定期的に送信して、他の UDLD 対応ネイバーに関して学習し、各デバイスがネイバーに関する情報を常に維持できるようにします。

スイッチが hello メッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、情報をキャッシュします。古いキャッシュ エントリの期限が切れる前に、スイッチが新しいhelloメッセージを受信すると、スイッチが古いエントリを新しいエントリで置き換えます。

UDLD の実行中にポートがディセーブルになったり、ポート上で UDLD がディセーブルになったり、またはスイッチをリセットした場合、UDLDは設定変更の影響を受けるポートの既存のキャッシュ エントリをすべてクリアします。UDLD は、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを1つまたは複数送信します。このメッセージは、キャッシュを継続的に同期するためのものです。

イベントドリブン検出およびエコー

UDLD は検出動作としてエコーを利用します。UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続の UDLD デバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。この動作はすべての UDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLDモードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブ モードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

関連トピック

UDLD のグローバルなイネーブル化（CLI），（540 ページ）
インターフェイスでの UDLD のイネーブル化（CLI），（541 ページ）

UDLD リセット オプション

インターフェイスがUDLD でディセーブル化された場合、次のオプションの1つを使用してUDLDをリセットできます。

- **udld reset** インターフェイス コンフィギュレーション コマンド。
- **shutdown** インターフェイス コンフィギュレーション コマンドに続いて **no shutdown** インターフェイス コンフィギュレーション コマンドを入力すると、ディセーブル化されたポートを再起動できます。

- **no udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドの後に **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを実行すると、ディセーブル化されたポートが再びイネーブルになります。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** [**aggressive**] インターフェイス コンフィギュレーション コマンドを実行すると、ディセーブル化された光ファイバ ポートが再びイネーブルになります。
- **errdisable recovery cause udld** グローバル コンフィギュレーション コマンドを入力すると、UDLD の errdisable ステートから自動回復するタイマーをイネーブルにできます。さらに、**errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンドを入力すると、UDLD の errdisable ステートから回復する時間を指定できます。

関連トピック

UDLD のグローバルなイネーブル化（CLI），（540 ページ）
インターフェイスでの UDLD のイネーブル化（CLI），（541 ページ）

UDLD のデフォルト設定

表 *42*：*UDLD* のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ ポート上でディセーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX ポート上でディセーブル
UDLD アグレッシブ モード	ディセーブル

関連トピック

UDLD のグローバルなイネーブル化（CLI），（540 ページ）
インターフェイスでの UDLD のイネーブル化（CLI），（541 ページ）

UDLD の設定方法

UDLD のグローバルなイネーブル化（CLI）

アグレッシブ モードまたは通常モードでUDLDをイネーブルにし、スイッチ上のすべての光ファイバ ポートに設定可能なメッセージ タイマーを設定するには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **udld**{**aggressive** | **enable** | **message time***message-timer-interval*}
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**udld**{**aggressive** | **enable** | **message time***message-timer-interval*} 例： スイッチ(config)# **udld enable** **message time 10**	UDLD モードの動作を指定します。 • **aggressive**：すべての光ファイバ ポート上で、UDLD をアグレッシブ モードでイネーブルにします。 • **enable**：スイッチ上のすべての光ファイバ ポート上で、UDLD を通常モードでイネーブルにします。UDLD はデフォルトでディセーブルです。 個々のインターフェイスの設定は、**udld enable** グローバル コンフィギュレーション コマンドの設定を上書きします。 • **message time***message-timer-interval*：アドバタイズ フェーズに存在し、双方向と検出されたポートにおける UDLD プローブ メッセージ間の時間間隔を設定します。有効な範囲は 1 ～ 90 秒です。デフォルト値は 15 です。 （注） このコマンドが作用するのは、光ファイバ ポートだけです。他のポート タイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
		UDLD をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

UDLD のモニタおよびメンテナンス
アグレッシブ モード，（537 ページ）
通常モード，（536 ページ）
単一方向の検出方法，（537 ページ）
イベントドリブン検出およびエコー，（538 ページ）
UDLD リセット オプション，（538 ページ）
UDLD のデフォルト設定，（539 ページ）

インターフェイスでの UDLD のイネーブル化（CLI）

アグレッシブ モードまたは通常モードをイネーブルにする、またはポート上で UDLD をディセーブルにするには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **udld port** [**aggressive**]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	UDLD用にイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**udld port** [**aggressive**] 例： スイッチ(config-if)# **udld port aggressive**	UDLD はデフォルトでディセーブルです。 • **udld port**：指定されたポート上で、UDLD を通常モードでイネーブルにします。 • **udld port aggressive**：（任意）指定されたポート上でアグレッシブ モードで UDLD をイネーブルにします。 （注） 特定の光ファイバ ポート上でUDLDをディセーブルにする場合は、**no udld port** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

関連トピック

UDLD のモニタおよびメンテナンス
アグレッシブ モード，（537 ページ）
通常モード，（536 ページ）
単一方向の検出方法，（537 ページ）
イベントドリブン検出およびエコー，（538 ページ）
UDLD リセット オプション，（538 ページ）
UDLD のデフォルト設定，（539 ページ）

UDLD のモニタおよびメンテナンス

コマンド	目的
show udld [*interface-id* | **neighbors**]	指定されたポートまたはすべてのポートの UDLD ステータスを表示します。

UDLD の追加リファレンス

関連資料

関連項目	マニュアル タイトル
レイヤ 2 コマンド リファレンス	*Layer 2/3 Command Reference (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

UDLD の機能情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 VI 部

Lightweight アクセス ポイント

- アクセス ポイント ディスカバリ用のスイッチの設定，547 ページ
- データ暗号化の設定，557 ページ
- 再送信間隔および再試行回数の設定，561 ページ
- 適応型ワイヤレス侵入防御システムの設定，565 ページ
- アクセス ポイントの認証の設定，571 ページ
- 自律アクセス ポイントの Lightweight モードへの変換，581 ページ
- Cisco ワークグループ ブリッジの使用，593 ページ
- プローブ要求フォワーディングの設定，599 ページ
- RFID トラッキングの最適化，601 ページ
- 国番号の設定，605 ページ
- リンク遅延の設定，611 ページ
- Power over Ethernet の設定，621 ページ

第 26 章

アクセスポイントディスカバリ用のスイッチの設定

- 機能情報の確認，547 ページ
- アクセス ポイント ディスカバリ用のスイッチの設定の前提条件，547 ページ
- アクセス ポイント ディスカバリ用のスイッチの設定の制約事項，548 ページ
- アクセス ポイント ディスカバリ用のスイッチの設定に関する情報，549 ページ
- アクセス ポイント ディスカバリの設定方法，551 ページ
- アクセス ポイント ディスカバリ用のスイッチの設定例，553 ページ
- AP パス スルーの設定方法，554 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

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

アクセス ポイント ディスカバリ用のスイッチの設定の前提条件

- Control and Provisioning of Wireless Access Points（CAPWAP）UDP ポート 5246 および 5247（Lightweight Access Point Protocol（LWAPP）UDP ポート 12222 および 12223 と同等のポー

ト）が有効になっており、アクセス ポイントがスイッチに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。

- アクセス コントロール リスト（ACL）がスイッチとアクセス ポイントの間の制御パスにある場合は、新しいプロトコル ポートを開いてアクセス ポイントが孤立しないようにする必要があります。
- アクセス ポイントが UP 状態であり、IP アドレスが変更される場合は、既存の CAPWAP トンネルを解除してスイッチに再 join します。
- アクセス ポイントをネットワークでアクティブにするには、スイッチがそのアクセス ポイントを検出する必要があります。Lightweight アクセス ポイントでは、次のスイッチ ディスカバリのプロセスがサポートされています。
  - レイヤ 3 CAPWAP ディスカバリ：アクセス ポイントから複数のサブネットでこの機能をイネーブルにできます。この機能は、レイヤ 2 ディスカバリで使用される MAC アドレスではなく IP アドレスと UDP パケットを使用します。
  - ローカルに保存されているスイッチの IP アドレス ディスカバリ：アクセス ポイントがすでにスイッチにアソシエートされている場合、プライマリ、セカンダリ、およびターシャリ スイッチの IP アドレスはアクセス ポイントの不揮発性メモリに保存されます。今後の展開用にアクセスポイントにスイッチの IP アドレスを保存するこのプロセスは、「アクセス ポイントのプライミング」と呼ばれます。
  - DHCP サーバの検出：この機能では、スイッチDHCP オプション 43 を使用してアクセス ポイントにの IP アドレスを割り当てます。Cisco スイッチでは、通常この機能に使用される DHCP サーバ オプションをサポートしています。
  - DNS の検出：アクセス ポイントでは、ドメイン ネーム サーバ（DNS）を介してスイッチを検出できます。CISCO-CAPWAP-CONTROLLER.*localdomain* に応答してスイッチ IP アドレスを返すように DNS を設定する必要があります。ここで *localdomain* はアクセス ポイントのドメイン名です。アクセス ポイントは、DHCP サーバから IP アドレスと DNS の情報を受信すると、DNS に接続して CISCO-CAPWAP-CONTROLLER.*localdomain* を解決します。DNS からスイッチの IP アドレスのリストを受信すると、アクセス ポイントはスイッチにディスカバリ要求を送信します。

アクセス ポイント ディスカバリ用のスイッチの設定の制約事項

- スイッチが適切な日時で設定されていることを確認してください。スイッチに設定されている日時がアクセス ポイントの証明書の作成日とインストール日に先行すると、アクセス ポイントはスイッチに join しません。
- ディスカバリ プロセス中は、1140、1260、3500、1040、1600、2600、または 3600 などの、シスコ スイッチによってサポートされるアクセス ポイントはシスコ スイッチに対してのみクエリを行います。

アクセス ポイント ディスカバリ用のスイッチの設定に関する情報

CAPWAP 環境では、Lightweight アクセス ポイントは CAPWAP 検出メカニズムを用いてスイッチを検出し、スイッチに CAPWAP 接続要求を送信します。スイッチはスイッチに接続するためのアクセス ポイントを許可するため、アクセス ポイントに CAPWAP 接続応答を送信します。アクセスポイントがスイッチに接続されると、スイッチはその構成、ファームウェア、コントロール トランザクション、データ トランザクションを管理します。

アクセス ポイント通信プロトコル

Cisco Lightweight アクセス ポイントは、IETF 標準 CAPWAP を使用してネットワーク上のスイッチおよび他の Lightweight アクセス ポイントと通信します。

CAPWAP は LWAPP に基づく標準の互換プロトコルであり、スイッチによる無線アクセス ポイントの集合の管理を可能にします。CAPWAP は、次の理由によりスイッチに実装されます。

- LWAPP を使用するシスコ製品に、CAPWAP を使用する次世代シスコ製品へのアップグレード パスを提供するため。
- RFID リーダーおよび類似のデバイスを管理するため。
- スイッチにサードパーティのアクセス ポイントとの将来的な互換性を持たせるため。

アクセス ポイントの join 情報の表示

CAPWAP discovery 要求をスイッチに少なくとも 1 回送信するアクセス ポイントの接続に関する統計情報は、アクセス ポイントがリブートまたは切断されても、スイッチ上に維持されます。これらの統計情報が削除されるのは、スイッチがリブートされた場合、または統計情報のクリアを選択した場合のみです。

アクセス ポイント接続プロセスのトラブルシューティング

アクセス ポイントがスイッチへの接続に失敗するのには、RADIUS 認証が保留になっている、スイッチで自己署名証明書が有効になっていない、アクセス ポイントとスイッチとで規制ドメインが一致しないなど、多くの原因が考えられます。

アクセス ポイントには、CAPWAP 関連のすべてのエラーを syslog サーバに送信するよう設定できます。すべての CAPWAP エラー メッセージが syslog サーバでそのまま表示できるので、スイッチでデバッグ コマンドを有効にする必要はありません。

スイッチがアクセス ポイントからの CAPWAP join 要求を受信するまで、アクセス ポイントの状態は保持されません。そのため、特定のアクセス ポイントからの CAPWAP discovery 要求が拒否された理由を判断することは難しい場合があります。そのような接続の問題を、スイッチで CAPWAP のデバッグ コマンドを有効にせずトラブルシューティングするため、スイッチはこのスイッチにディスカバリ メッセージを送信するすべてのアクセスポイントの情報を収集し、このスイッチに正常に接続したアクセス ポイントがあればその情報を保持します。

スイッチは、CAPWAP discovery 要求をスイッチに送信する各アクセス ポイントについて、接続関連のすべての情報を収集します。収集は、最初のディスカバリ メッセージがアクセスポイントから受信されたときに開始し、最後の設定ペイロードがスイッチからアクセス ポイントに送信されたときに終了します。

スイッチが接続関連情報を保持しているアクセス ポイントが最大数に達すると、それ以外のアクセス ポイントの情報は収集されなくなります。

DHCP サーバで syslog サーバの IP アドレスをアクセス ポイントに返すよう設定することもできます。サーバ上でオプション 7 を使用します。それにより、アクセス ポイントではすべての syslog メッセージがこの IP アドレスへ送信されるようになります。

アクセス ポイントがスイッチに接続していない場合、syslog サーバの IP アドレスは、アクセス ポイントの CLI を介して設定します。**capwap ap log-server***syslog_server_IP_address* コマンドを入力します。

アクセス ポイントが最初にスイッチに接続する際、スイッチはグローバル syslog サーバの IP アドレス（デフォルトは 255.255.255.255）をアクセス ポイントにプッシュします。その後、IP アドレスが次のいずれかのシナリオで上書きされるまで、アクセス ポイントはすべての syslog メッセージをこの IP アドレスに送信します。

- アクセス ポイントが接続されているスイッチは同じだが、**ap syslog host** *Syslog_Server_IP_Address* コマンドを使用して、スイッチのグローバル syslog サーバの IP アドレス設定を変更した。この場合、スイッチはグローバル syslog サーバの新しい IP アドレスをアクセス ポイントにプッシュします。
- アクセス ポイントが接続されているスイッチは同じだが、スイッチのアクセス ポイントについて、**ap name** *Cisco_AP* **syslog host** *Syslog_Host_IP_Address* コマンドを使用して、特定の syslog サーバの IP アドレスを設定した。この場合、スイッチは特定の syslog サーバの新しい IP アドレスをアクセス ポイントにプッシュします。
- アクセス ポイントがスイッチから切断され、**capwap ap log-server** *syslog_server_IP_address* コマンドを使用して、アクセス ポイントの CLI から syslog サーバの IP アドレスを設定した。このコマンドは、アクセスポイントがどのスイッチにも接続されていない場合に限り機能します。
- アクセス ポイントがスイッチから切断され、別のスイッチに接続した。この場合、新しいスイッチはそのグローバル syslog サーバの IP アドレスをアクセス ポイントへプッシュします。

新しい syslog サーバの IP アドレスが既存の syslog サーバの IP アドレスを上書きするたびに、古いアドレスは固定記憶域から消去され、新しいアドレスがそこに保存される。アクセス ポイントも、その syslog サーバの IP アドレスに到達できるのであれば、すべての syslog メッセージを新しい IP アドレスに送信するようになります。

アクセス ポイント ディスカバリの設定方法

アクセス ポイントの Syslog サーバの設定（GUI）

ステップ 1 [Configuration] > [Wireless] > [Access Points] > [All Aps] の順に選択します。
[All Aps] ページが開き、スイッチと関連付けられたアクセス ポイントのリストおよびそれらの現在の設定が表示されます。

ステップ 2 [Show] ドロップダウン リストで、[Quick Filter] を選択します。
フィルタ オプション（テキスト ボックス）は、テーブルのそれぞれの列のヘッダーに表示されます。

ステップ 3 対応するテキスト ボックスにキーワードを入力して、検索のためのフィルタ基準を指定し、[Filter] アイコンをクリックします。

アクセス ポイントの Syslog サーバの設定（CLI）

手順の概要

1. **show ap config global**
2. **show ap name** *Cisco_AP* **config general**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ap config global** 例： `スイッチ# show ap config global`	スイッチを join するすべてのアクセス ポイントのグローバル Syslog サーバ設定を表示します。
ステップ 2	**show ap name** *Cisco_AP* **config general** 例： `スイッチ# show ap name AP03 config general`	特定のアクセス ポイントの Syslog サーバ設定を表示します。

アクセス ポイントの join 情報のモニタリング（CLI）

（注） スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **enable**
2. **show ap join stats summary**
3. **show ap mac-address** *mac_address* **join stats summary**
4. **show ap mac-address** *mac_address* **join stats detailed**
5. **clear ap join statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 2	**show ap join stats summary** 例： `スイッチ# show ap join stats summary`	スイッチに join しているまたは join を試行したすべてのアクセス ポイントの MAC アドレスを表示します。
ステップ 3	**show ap mac-address** *mac_address* **join stats summary** 例： `スイッチ# show ap mac-address 000.2000.0400 join stats summary`	最後の join エラーの詳細を含む AP のすべての統計情報を表示します。
ステップ 4	**show ap mac-address** *mac_address* **join stats detailed** 例： `スイッチ# show ap mac-address 000.2000.0400 join stats detailed`	特定のアクセス ポイントについて収集された join 関連の統計情報を表示します。

	コマンドまたはアクション	目的
ステップ 5	**clear ap join statistics** 例： `スイッチ# clear ap join statistics`	すべてのアクセスポイントのjoin統計情報をクリアします。 （注） 特定のアクセスポイントに対応する join 統計情報をクリアするには、**clear ap mac-address** *mac_address* **join statistics** コマンドを入力します。

関連トピック

すべてのアクセス ポイントの MAC アドレスの表示：例, （553 ページ）

Lightweight Cisco Aironet アクセス ポイントの DHCP オプション 43 の設定例, （554 ページ）

アクセス ポイント ディスカバリ用のスイッチの設定例

すべてのアクセス ポイントの MAC アドレスの表示：例

次に、スイッチに join しているすべてのアクセス ポイントの MAC アドレスを表示する例を示します。

```
スイッチ# show ap join stats summary
Number of APs.......................................... 4

Base Mac           EthernetMac       AP Name IP Address    Status
------------------ ----------------- ------- ------------- ----------
00:0b:85:57:bc:c0 00:0b:85:57:bc:c0 AP1130  10.10.163.217 Joined
00:1c:0f:81:db:80 00:1c:63:23:ac:a0 AP1140  10.10.163.216 Not joined
00:1c:0f:81:fc:20 00:1b:d5:9f:7d:b2 AP1     10.10.163.215 Joined
00:21:1b:ea:36:60 00:0c:d4:8a:6b:c1 AP2     10.10.163.214 Not joined
```

次に、特定のアクセス ポイントに関する最後の join エラーの詳細を表示する例を示します。

```
スイッチ# show ap mac-address 000.2000.0400 join stats summary
Is the AP currently connected to controller..... Yes
Time at which the AP joined this
controller last time.................................. Aug 21 12:50:36.061
Type of error
that occurred last.................. AP got or has been disconnected
Reason for error
that occurred last........... The AP has been reset by the controller
Time at which the last join error occurred......... Aug 21 12:50:34.374
```

次に、特定のアクセス ポイントに関して収集されたすべての join 関連の統計情報を表示する例を示します。

```
スイッチ# show ap mac-address 000.2000.0400 join stats detailed
Discovery phase statistics
- Discovery requests received.......................... 2
- Successful discovery responses sent.................. 2
- Unsuccessful discovery request processing.......... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt.......... Aug 21 12:50:23.335
```

```
- Time at last unsuccessful discovery attempt........ Not applicable

Join phase statistics
- Join requests received............................. 1
- Successful join responses sent..................... 1
- Unsuccessful join request processing............... 1
- Reason for last unsuccessful join attempt.....      RADIUS authorization
                                                      is pending
                                                      for the AP
- Time at last successful join attempt............... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt............. Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received.................... 1
- Successful configuration responses sent............ 1
- Unsuccessful configuration request processing...... 0
- Reason for last unsuccessful configuration attempt.. Not applicable
- Time at last successful configuration attempt...... Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt..... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure.......... Not applicable

Last AP disconnect details
- Reason for last AP connection failure.............. The AP has been reset by
                                                      the controller
Last join error summary
- Type of error that occurred last................... AP got or has been
                                                      disconnected
- Reason for error that occurred last................ The AP has been reset
                                                      by the controller
- Time at which the last join error occurred.......... Aug 21 12:50:34.374
```

Lightweight Cisco Aironet アクセス ポイントの DHCP オプション 43 の設定例

AP join プロセスの詳細については、「*DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example*」を参照してください。

AP パス スルーの設定方法

AP パススルーについて

AP パススルーでは、 Cisco Catalyst 3850 シリーズ スイッチおよび Cisco Catalyst 3650 シリーズ スイッチに接続されているすべてのアクセス ポイントをネットワーク上の別のコントローラに接続します。

このリリースに先立ち、Cisco Catalyst 3850 シリーズ スイッチおよび Cisco Catalyst 3650 シリーズ スイッチに接続されているすべてのアクセス ポイントは 、ワイヤレス マネジメント VLAN がオンのときにスイッチ上で終端します。スイッチに接続したサポート対象外のアクセス ポイントは、異なる VLAN 上のコントローラに接続できません。AP パススルーでは、異なる VLAN を割り当てることで、接続された AP を VLAN ネットワーク上の別のワイヤレス コントローラに接続します。

AP パスの利点は次のとおりです。

- 一部の AP が、Cisco Catalyst 3850 シリーズ スイッチおよび Cisco Catalyst 3650 シリーズ スイッチに接続され、他のAPがネットワーク上の他のコントローラに接続し続けているとき、新世代の Cisco Wireless Controller の部分的な展開を許可します。
- Cisco Catalyst 3850 シリーズ スイッチおよび Cisco Catalyst 3650 シリーズ スイッチでサポート対象外の AP がネットワーク内の他のコントローラに接続するのを許可します。
- ワイヤレス LAN コントローラは、有線およびワイヤレス ゲストへのアクセスを提供するために使用されます。APパススルーにより、APは有線ゲストアクセスがオンになると、Cisco Catalyst 3850 シリーズ スイッチおよび Cisco Catalyst 3650 シリーズ スイッチを他の任意のコントローラに接続します。

APのパススルーの設定

サポートされるアクセス ポイントのもの以外の VLAN のすべてのアクセス ポイントは、AP のパススルー モードになり、スイッチでは終了しません。

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ2	**wireless management interface vlan** *vlan_id* 例： `スイッチ(config)# wireless management interface vlan10`	ワイヤレス管理の VLAN でサポートされるアクセス ポイントに接続されているポートを設定します。
ステップ3	**interface GigabitEthernet1/0/1** 例： `スイッチ(config)# interface TenGigabitEthernet1/0/1`	10 ギガビット イーサネット インターフェイスを設定します。 コマンド プロンプトが (config)# から (config-if)# に変わります。
ステップ4	**description Supported AP switchport access***vlan_id* 例： `スイッチ(config-if)# switchport access vlan10`	このアクセスポートがトラフィックを伝送するVLANを指定します。
ステップ5	**description Unsupported AP switchport access***vlan_id* 例： `スイッチ(config-if)# switchport access vlan20`	ワイヤレス管理のVLAN以外のVLANでサポートされていないアクセス ポイントに接続されているポートを設定します。

第 27 章

データ暗号化の設定

- 機能情報の確認，557 ページ
- データ暗号化を設定するための前提条件，557 ページ
- データ暗号化の設定に関する制約事項，558 ページ
- データの暗号化について，558 ページ
- データ暗号化の設定方法，558 ページ
- データ暗号化の設定例，559 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

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

データ暗号化を設定するための前提条件

- Cisco 1260、3500、3600、801、1140、1310、および 1520 シリーズのアクセス ポイントは、Datagram Transport Layer Security（DTLS）のデータ暗号化をサポートします。
- スイッチを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効化または無効化できます。
- シスコ スイッチを使用するロシア人以外のお客様はデータ DTLS ライセンスは必要ありません。

データ暗号化の設定に関する制約事項

- 暗号化はスイッチおよびアクセス ポイントの両方においてスループットを制限するため、多くのエンタープライズ ネットワークにおいて最大スループットが必要です。
- スイッチにデータ DTLS のライセンスがなく、スイッチに関連付けられているアクセス ポイントで DTLS が有効になっている場合、データ パスは暗号化されません。
- DTLS ライセンスがないイメージでは DTLS コマンドは使用できません。

データの暗号化について

スイッチにより、DTLSを使用してアクセスポイントとスイッチのCAPWAPコントロールパケット（および、オプションとしてCAPWAPデータ パケット）の暗号化が可能です。DTLSは、標準化過程にあるTLSに基づくインターネット技術特別調査委員会（IETF）プロトコルです。CAPWAPコントロールパケットとは、スイッチとコントローラとアクセスポイントの間で交換される管理パケットであり、CAPWAP データ パケットは転送された無線フレームをカプセル化します。CAPWAP コントロールおよびデータ パケットはそれぞれ異なる UDP ポートである 5246（コントロール）および 5247（データ）で送信されます。アクセス ポイントが DTLS データ暗号化をサポートしない場合、DTLS はコントロール プレーンにのみ有効となり、データ プレーンの DTLS セッションは確立されません。

データ暗号化の設定方法

データ暗号化の設定（CLI）

手順の概要

1. **configure terminal**
2. **ap link-encryption**
3. **end**
4. **show ap link-encryption**
5. **show wireless dtls connections**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap link-encryption** 例： スイッチ(config)# ap link-encryption	このコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセスポイントのデータ暗号化をイネーブルにします。デフォルト値は [disabled] です。 データ暗号化モードに変更するには、アクセス ポイントをスイッチに再 join する必要があります。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 4	**show ap link-encryption** 例： スイッチ# show ap link-encryption	すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化の状態を表示します。このコマンドはまた、整合性チェックの失敗およびリプレイエラーの数を追跡する認証エラーを表示します。リレー エラーは、アクセス ポイントが同じパケットを受信する回数の追跡に役立ちます。
ステップ 5	**show wireless dtls connections** 例： スイッチ# show wireless dtls connections	すべてのアクティブな DTLS 接続の概要を表示します。 （注） DTLS データの暗号化に問題が生じた場合は、**debug dtls ap {all|event|trace}** コマンドを入力して、すべての DTLS メッセージ、イベント、またはトレースをデバッグします。

関連トピック

すべてのアクセス ポイントのデータ暗号化の状態の表示：例, （559 ページ）

データ暗号化の設定例

すべてのアクセス ポイントのデータ暗号化の状態の表示：例

次に、すべてのアクセスポイントまたは特定のアクセスポイントの暗号化の状態を表示する例を示します。このコマンドはまた、整合性チェックの失敗およびリプレイ エラーの数を追跡する認

証エラーを表示します。リレーエラーは、アクセスポイントが同じパケットを受信する回数の追跡に役立ちます。

```
スイッチ# show ap link-encryption
                  Encryption  Dnstream  Upstream    Last
AP Name                State     Count     Count  Update
------------------  ----------  --------  --------  ------
3602a                  Enabled         0         0   Never
```

次に、すべてのアクティブな DTLS 接続のサマリーを表示する例を示します。

```
スイッチ# show wireless dtls connections
AP Name         Local Port   Peer IP       Peer Port  Ciphersuite
--------------- ------------ ------------- ---------- --------------------
3602a           Capwap_Ctrl  10.10.21.213  46075      TLS_RSA_WITH_AES_128_CBC_SHA
3602a           Capwap_Data  10.10.21.213  46075      TLS_RSA_WITH_AES_128_CBC_SHA
```

第 28 章

再送信間隔および再試行回数の設定

- 機能情報の確認，561 ページ
- アクセス ポイントの再送信間隔と再試行回数の設定の前提条件，561 ページ
- 再送信間隔および再試行回数について，562 ページ
- アクセス ポイントの再送信間隔と再試行回数の設定方法，562 ページ
- CAPWAP の最大伝送単位情報の表示（CLI），563 ページ
- アクセス ポイントの再送信間隔と再試行回数の設定例，564 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

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

アクセス ポイントの再送信間隔と再試行回数の設定の前提条件

- 再送信間隔と再試行回数の両方とも、グローバルと特定のアクセス ポイント レベルで設定できます。グローバル設定では、これらの設定パラメータがすべてのアクセスポイントに適用されます。また、特定のアクセス ポイント レベルで再送信間隔と再試行回数を設定すると、値はその特定のアクセス ポイントに適用されます。アクセス ポイント固有の設定は、グローバル設定よりも優先されます。

再送信間隔および再試行回数について

スイッチとアクセス ポイントは、Control And Provisioning of Wireless Access Points（CAPWAP）の信頼性の高いトランスポート プロトコルを使用してパケットを交換します。各要求に対して、応答が定義されています。この応答を使用して、要求メッセージの受信を確認します。応答メッセージは明示的に確認されません。したがって、応答メッセージが受信されない場合は、再送信間隔後に元の要求メッセージが再送信されます。最大再送信回数に達しても要求が確認されないと、セッションが終了し、アクセス ポイントは再度別のスイッチに関連付けられます。

アクセス ポイントの再送信間隔と再試行回数の設定方法

アクセス ポイントの再送信間隔と再試行回数の設定（CLI）

手順の概要

1. **enable**
2. **configure terminal**
3. **ap capwap retransmit interval** *interval_time*
4. **ap capwap retransmit count** *count_value*
5. **end**
6. **ap name** *Cisco_AP* **capwap retransmit interval** *interval_time*
7. **ap name** *Cisco_AP* **capwap retransmit count** *count_value*
8. **show ap capwap retransmit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ# **enable**	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap capwap retransmit interval** *interval_time* 例： スイッチ(config)# ap capwap retransmit interval 2	すべてのアクセスポイントに対してコントロールパケットの再送信間隔をグローバルに設定します。 （注） 間隔パラメータの範囲は 2 ～ 5 です。

	コマンドまたはアクション	目的
ステップ 4	**ap capwap retransmit count** *count_value* 例： スイッチ(config)# ap capwap retransmit count 3	すべてのアクセスポイントに対してコントロールパケットの再試行回数をグローバルに設定します。 （注） 回数の範囲は 3 ～ 8 です。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコンフィギュレーションモードを終了できます。
ステップ 6	**ap name** *Cisco_AP* **capwap retransmit interval** *interval_time* 例： スイッチ# ap name AP02 capwap retransmit interval 2	ユーザが指定した個々のアクセス ポイントに対してコントロール パケットの再送信間隔を設定します。 （注） 間隔の範囲は 2 ～ 5 です。 （注） **ap name** コマンドを使用するには、特権 EXEC モードを開始しておく必要があります。
ステップ 7	**ap name** *Cisco_AP* **capwap retransmit count** *count_value* 例： スイッチ# ap name AP02 capwap retransmit count 3	ユーザが指定した個々のアクセス ポイントに対してコントロール パケットの再試行回数を設定します。 （注） 再試行回数の範囲は 3 ～ 8 です。
ステップ 8	**show ap capwap retransmit** 例： スイッチ# show ap capwap retransmit	CAPWAP の再送信の詳細を表示します。

CAPWAP の最大伝送単位情報の表示（CLI）

手順の概要

1. **enable**
2. **show ap name** *Cisco_AP* **config general**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ# enable	特権 EXEC モードを開始します。
ステップ 2	**show ap name** *Cisco_AP* **config general** 例： スイッチ# show ap name Maria-1250 config general | include MTU	スイッチ上の CAPWAP パスの最大伝送単位（MTU）を表示します。MTU は、送信されるパケットの最大サイズ（バイト）を指定します。

関連トピック

CAPWAP 再送信の詳細の表示：例, （564 ページ）
最大伝送単位情報の表示：例, （564 ページ）

アクセス ポイントの再送信間隔と再試行回数の設定例

CAPWAP 再送信の詳細の表示：例

次のコマンドを入力します。

```
スイッチ# show ap capwap retransmit
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval             Retransmit Count

-------------------------------- -------------------------------
--------------------------------
3602a                            5                               3
```

最大伝送単位情報の表示：例

次に、スイッチの CAPWAP パスの最大伝送単位（MTU）を表示する例を示します。MTU は、送信されるパケットの最大サイズ（バイト）を指定します。

```
スイッチ# show ap name cisco-ap-name config general | include MTU
CAPWAP Path MTU.................................. 1500
```

第 29 章

適応型ワイヤレス侵入防御システムの設定

- 機能情報の確認，565 ページ
- wIPS 設定の前提条件，565 ページ
- アクセス ポイントでの wIPS の設定方法，566 ページ
- wIPS 情報のモニタリング，567 ページ
- アクセス ポイントでの wIPS の設定例，569 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

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

wIPS 設定の前提条件

- 通常のローカル モードのアクセス ポイントは、ワイヤレス侵入防御システム（wIPS）機能のサブセットによって拡張されています。この機能を使用すると、分離されたオーバーレイ ネットワークがなくても、アクセス ポイントを展開して保護機能を提供できます。

アクセス ポイントでの wIPS の設定方法

アクセス ポイントでの wIPS の設定（CLI）

手順の概要

1. **ap name** *Cisco_AP* **mode local**
2. **ap name** *Cisco_AP* **dot11 5ghz shutdown**
3. **ap name** *Cisco_AP* **dot11 24ghz shutdown**
4. **ap name** *Cisco_AP* **mode monitor submode wips**
5. **ap name** *Cisco_AP* **monitor-mode wips-optimized**
6. **show ap dot11 24ghz monitor**
7. **ap name** *Cisco_AP* **no dot11 5ghz shutdown**
8. **ap name** *Cisco_AP* **no dot11 24ghz shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ap name** *Cisco_AP* **mode local** 例： `スイッチ# ap name AP01 mode local`	モニタ モードのアクセス ポイントを設定します。 APのモードを変更するとアクセスポイントがリブートされることを示すメッセージが表示されます。このメッセージは、APモードの変更を続行するかどうかを指定できるプロンプトも表示します。続行するには、プロンプトで**y**を入力します。
ステップ 2	**ap name** *Cisco_AP* **dot11 5ghz shutdown** 例： `スイッチ# ap name AP01 dot11 5ghz shutdown`	アクセス ポイントの 802.11a 無線を無効にします。
ステップ 3	**ap name** *Cisco_AP* **dot11 24ghz shutdown** 例： `スイッチ# ap name AP02 dot11 24ghz shutdown`	アクセス ポイントの 802.11b 無線を無効にします。
ステップ 4	**ap name** *Cisco_AP* **mode monitor submode wips** 例： `スイッチ# ap name AP01 mode monitor submode wips`	アクセス ポイントで wIPS サブモードを設定します。 （注） アクセス ポイントで wIPS を無効にするには、**ap name** *Cisco_AP* **modemonitor submode none** コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 5	**ap name** *Cisco_AP* **monitor-mode wips-optimized** 例： `スイッチ# ap name AP01 monitor-mode wips-optimized`	アクセス ポイントに対して wIPS が最適化されたチャネル スキャンを有効にします。 アクセス ポイントは、250 ミリ秒の間、各チャネルをスキャンします。監視設定に基づいてスキャンされるチャネルの一覧が取得されます。次のオプションから選択できます。 • **All**：アクセス ポイントの無線でサポートされているすべてのチャネル。 • **Country**：アクセス ポイントの使用国でサポートされているチャネルのみ。 • **Country**：動的チャネル割り当て（DCA）アルゴリズムによって使用されるチャネルセットのみ（デフォルトでは、アクセスポイントの使用国で許可された、オーバーラップしないすべてのチャネルを含む）。
ステップ 6	**show ap dot11 24ghz monitor** 例： `スイッチ# show ap dot11 24ghz monitor`	監視設定チャネル セットを表示します。 （注） コマンド出力の 802.11b 監視チャネル値は監視設定チャネル セットを示します。
ステップ 7	**ap name** *Cisco_AP* **no dot11 5ghz shutdown** 例： `スイッチ# ap name AP01 no dot11 5ghz shutdown`	アクセス ポイントの 802.11a 無線を有効にします。
ステップ 8	**ap name** *Cisco_AP* **no dot11 24ghz shutdown** 例： `スイッチ# ap name AP01 no dot11 24ghz shutdown`	アクセス ポイントの 802.11b 無線を有効にします。

wIPS 情報のモニタリング

（注） スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **show ap name** *Cisco_AP* **config general**
2. **show ap monitor-mode summary**
3. **show wireless wps wips summary**
4. **show wireless wps wips statistics**
5. **clear wireless wips statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ap name** *Cisco_AP* **config general** 例： `スイッチ# show ap name AP01 config general`	アクセス ポイントの wIPS サブモードで情報を表示します。
ステップ 2	**show ap monitor-mode summary** 例： `スイッチ# show ap monitor-mode summary`	アクセス ポイントで wIPS 最適化チャネル スキャン コンフィギュレーションを表示します。
ステップ 3	**show wireless wps wips summary** 例： `スイッチ# show wireless wps wips summary`	NCS または Prime によって転送した wIPS コンフィギュレーションをスイッチに表示します。
ステップ 4	**show wireless wps wips statistics** 例： `スイッチ# show wireless wps wips statistics`	現在の wIPS オペレーションをスイッチに表示します。
ステップ 5	**clear wireless wips statistics** 例： `スイッチ# clear wireless wips statistics`	スイッチで wIPS 統計をクリアします。

関連トピック

モニタ設定チャネル セットの表示：例, （569 ページ）

wIPS 情報の表示：例, （569 ページ）

アクセス ポイントでの wIPS の設定例

モニタ設定チャネル セットの表示：例

次に、モニタ設定チャネル セットを表示する例を示します。

```
スイッチ# show ap dot11 24ghz monitor
Default 802.11b AP monitoring
802.11b Monitor Mode.......................... enable
802.11b Monitor Channels...................... Country channels
802.11b AP Coverage Interval.................. 180 seconds
802.11b AP Load Interval...................... 60 seconds
802.11b AP Noise Interval..................... 180 seconds
802.11b AP Signal Strength Interval........... 60 seconds
```

wIPS 情報の表示：例

次に、アクセス ポイントの wIPS サブモードの情報を表示する例を示します。

```
スイッチ# show ap name AP01 config general
Cisco AP Identifier.............. 3
Cisco AP Name.................... AP1131:46f2.98ac
...
AP Mode ......................... Monitor
Public Safety ................... Disabled Disabled
AP SubMode ...................... WIPS
```

次に、アクセス ポイントの wIPS が最適化されたチャネル スキャンの設定を表示する例を示します。

```
スイッチ# show ap monitor-mode summary
AP Name       Ethernet MAC   Status   Scanning
                                      Channel
                                      List
------------- -------------- -------- ---------
AP1131:4f2.9a 00:16:4:f2:9:a WIPS     1,6,NA,NA
```

次に、WCS によってスイッチに転送される wIPS 設定を表示する例を示します。

```
スイッチ# show wireless wps wips summary
Policy Name.............. Default
Policy Version........... 3
```

次に、スイッチでの wIPS 動作の現在の状態を表示する例を示します。

```
スイッチ# show wireless wps wips statistics
Policy Assignment Requests............ 1
Policy Assignment Responses........... 1
Policy Update Requests................ 0
Policy Update Responses............... 0
Policy Delete Requests................ 0
Policy Delete Responses............... 0
Alarm Updates......................... 13572
Device Updates........................ 8376
Device Update Requests................ 0
Device Update Responses............... 0
Forensic Updates...................... 1001
Invalid WIPS Payloads................. 0
Invalid Messages Received............. 0
CAPWAP Enqueue Failed................. 0
NMSP Enqueue Failed................... 0
NMSP Transmitted Packets.............. 22950
```

```
NMSP Transmit Packets Dropped..... 0
NMSP Largest Packet.................. 1377
```

第 30 章

アクセス ポイントの認証の設定

- 機能情報の確認，571 ページ
- アクセス ポイントの認証を設定するための前提条件，571 ページ
- アクセス ポイントの認証を設定する際の制限，572 ページ
- アクセス ポイントに対する認証の設定について，572 ページ
- アクセス ポイントの認証の設定方法，573 ページ
- アクセス ポイントの認証の設定例，580 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

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

アクセス ポイントの認証を設定するための前提条件

- スイッチに現在 join しているすべてのアクセス ポイント、また今後 join するアクセスポイントがスイッチに join するときに継承するグローバル ユーザ名、パスワード、およびイネーブル パスワードを設定することができます。必要に応じて、このグローバル資格情報よりも優先される、独自のユーザ名、パスワード、およびイネーブル パスワードを特定のアクセス ポイントに割り当てることができます。

- アクセス ポイントをスイッチに join すると、そのアクセス ポイントのコンソール ポート セキュリティが有効になり、コンソール ポートへログインするたびにユーザ名とパスワードの入力を要求されます。ログインした時点では非特権モードのため、特権モードを使用するには、イネーブル パスワードを入力する必要があります。
- スイッチで設定したグローバル資格情報はスイッチやアクセス ポイントをリブートした後も保持されます。この情報が上書きされるのは、アクセス ポイントを、グローバル ユーザ名およびパスワードが設定された新しいスイッチに join した場合のみです。グローバル資格情報を使って新しいスイッチを設定しなかった場合、このアクセス ポイントは最初のスイッチに設定されているグローバル ユーザ名とパスワードをそのまま保持します。
- アクセス ポイントにより使用される資格情報を追跡する必要があります。そうしないと、アクセス ポイントのコンソール ポートにログインできなくなることがあります。アクセス ポイントをデフォルトの *Cisco/Cisco* ユーザ名およびパスワードに戻す必要がある場合は、スイッチの設定をクリアする必要があります。これにより、アクセス ポイントの設定は工場出荷時のデフォルト設定に戻ります。デフォルトのアクセス ポイント設定をリセットするには、**ap name** *Cisco_AP* **mgmtuser username** *Cisco* **password** *Cisco* コマンドを入力します。コマンドを入力しても、アクセス ポイントの固定 IP アドレスはクリアされません。アクセス ポイントがスイッチに再 join すると、デフォルトの *Cisco/Cisco* のユーザ名およびパスワードを適用します。
- 現在スイッチに join している、また、今後 join するすべてのアクセス ポイントにグローバル認証を設定できます。必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセス ポイントに割り当てることができます。
- この機能は、次のハードウェアによりサポートされます。
  - 認証をサポートするすべての Cisco スイッチ。
  - Cisco Aironet 1140、1260、1310、1520、1600、2600、3500、および 3600 アクセス ポイント

アクセス ポイントの認証を設定する際の制限

- AP 設定におけるスイッチ名は、大文字と小文字が区別されます。したがって、AP 設定には、必ず正確なシステム名を設定してください。正確に設定しないと、AP フォールバックが機能しません。

アクセス ポイントに対する認証の設定について

Cisco IOS アクセス ポイントには、工場出荷時にデフォルトの enable パスワード *Cisco* が設定されています。このパスワードを使用して、非特権モードでログインすると、ネットワークのセキュリティに対する脅威となる **show** および **debug** コマンドの入力が許可されます。不正アクセスを防止し、ユーザがアクセス ポイントのコンソール ポートからコンフィギュレーション コマンドを入力できるようにするには、デフォルトのイネーブル パスワードを変更する必要があります。

Lightweight アクセス ポイントとシスコのスイッチの間で 802.1X 認証を設定できます。アクセス ポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用するスイッチにより認証されます。

アクセス ポイントの認証の設定方法

アクセス ポイントのグローバル資格情報の設定（CLI）

手順の概要

1. **enable**
2. **configure terminal**
3. **ap mgmtuser username** *user_name* **password 0** *passsword* **secret 0** *secret_value*
4. **end**
5. **ap name** *Cisco_AP* **mgmtuser username** *user_name* **password** *password* **secret** *secret*
6. **show ap summary**
7. **show ap name** *Cisco_AP* **config general**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap mgmtuser username** *user_name* **password 0** *passsword* **secret 0** *secret_value* 例： `スイッチ(config)# ap mgmtuser apusr1 password appass 0 secret 0 appass1`	スイッチに現在 join しているすべてのアクセス ポイント、および今後スイッチに join するアクセス ポイントに対し、グローバル ユーザ名とパスワードを設定し、パスワードをイネーブルにします。このコマンドでは、パラメータ 0 は暗号化されていないパスワードが続くことを指定し、8 は AES 暗号化パスワードが続くことを指定します。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

	コマンドまたはアクション	目的
ステップ 5	**ap name** *Cisco_AP* **mgmtuser username** *user_name* **password** *password* **secret** *secret* 例： `スイッチ(config)# ap name TSIM_AP-2 mgmtuser apusr1 password appass secret secret`	特定のアクセス ポイントのグローバル資格情報を上書きし、固有のユーザ名とパスワードを割り当て、このアクセス ポイントに対しパスワードをイネーブルにします。 このコマンドに入力した資格情報は、スイッチやアクセス ポイントをリブートした後や、アクセス ポイントが新しいスイッチに join された場合でも保持されます。 （注） このアクセスポイントでスイッチのグローバル資格情報を強制的に使用する必要がある場合は、**ap name** *Cisco_AP* **no mgmtuser** コマンドを入力します。このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。
ステップ 6	**show ap summary** 例： `スイッチ# show ap summary`	接続されたすべての Cisco AP のサマリーを表示します。
ステップ 7	**show ap name** *Cisco_AP* **config general** 例： `スイッチ# show ap name AP02 config general`	特定のアクセス ポイントのグローバル資格情報の設定を表示します。 （注） このアクセス ポイントがグローバル クレデンシャル用に設定されている場合は、[AP User Mode] テキスト ボックスに [Automatic] と表示されます。このアクセス ポイントのグローバル クレデンシャルが上書きされている場合は、[AP User Mode] テキスト ボックスに [Customized] と表示されます。

アクセス ポイントのグローバル資格情報の設定（GUI）

ステップ 1 [Configuration] > [Wireless] > [Access Points] > [Global AP Configuration] の順に選択します。[Global Configuration] ページが表示されます。

ステップ 2 [Login Credentials] 領域で、次のパラメータを入力します。

- User Name
- Password
- Confirm Password
- Secret Password

- シークレット パスワードの確認

パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。パスワードには、管理ユーザ名やユーザ名を逆にした文字列を含めることはできません。パスワードに使用しないほうがよい文字には、Cisco、oscic、admin、nimda のような語のほか、大文字の代わりに 1 や |、！を、o の代わりに 0 を、s の代わりに $ を使用して置き換えた文字などがあります。

ステップ 3 [Apply] をクリックします。
グローバル ユーザ名とパスワードは、スイッチと関連付けられたすべてのアクセス ポイントに適用されます。

ステップ 4 [Save Configuration] をクリックします。

ステップ 5 （任意）次の手順に従って、特定のアクセス ポイントのグローバル資格情報を上書きし、固有のユーザ名とパスワードを割り当てることができます。

a) [Configuration] > [Wireless] > [Access Points] > [All Aps] の順に選択します。
[All APs] ページが表示されます。

b) アクセス ポイントの名前をクリックします。
[AP] > [Edit] ページが表示されます。

c) [Credentials] タブをクリックします。

d) [Login Credentials] 領域で、[Over-ride Global Credentials] チェックボックスをオンにします。

e) 次のパラメータの値を入力します。

- Username
- Password
- Enable Password

f) [Apply] をクリックします。

g) [Save Configuration] をクリックします。

アクセス ポイントの認証の設定（CLI）

手順の概要

1. **enable**
2. **configure terminal**
3. **ap dot1x username** *user_name_value* **password 0** *password_value*
4. **end**
5. **ap name** *Cisco_AP* **dot1x-user username** *username_value* **password** *password_value*
6. **configure terminal**
7. **no ap dot1x username** *user_name_value* **password 0** *password_value*
8. **end**
9. **show ap summary**
10. **show ap name** *Cisco_AP* **config general**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ# **enable**	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap dot1x username** *user_name_value* **password 0** *password_value* 例： スイッチ(config)# ap dot1x username AP3 password 0 password	にスイッチ現在 join しているすべてのアクセス ポイント、または今後 join するスイッチアクセス ポイントにグローバル認証のユーザ名とパスワードを設定します。このコマンドには、次のキーワードと引数が含まれます。 • **username**：すべてのアクセス ポイントの 802.1X ユーザ名を指定します。 • *user-id*：ユーザ名。 • **password**：すべてのアクセス ポイントの 802.1X パスワードを指定します。 • **0**：暗号化されないパスワードを指定します。 • **8**：AES 暗号化パスワードを指定します。 • *passwd*：パスワード。

	コマンドまたはアクション	目的
		（注） passwordパラメータには強力なパスワードを入力する必要があります。強力なパスワードの長さは少なくとも8文字で、大文字と小文字、数字、および記号の組み合わせを含み、いずれの言語の単語でもありません。
ステップ4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ5	**ap name** *Cisco_AP* **dot1x-user username** *username_value* **password** *password_value* 例： `スイッチ# ap name AP03 dot1x-user username apuser1 password appass`	グローバル認証設定を無効にし、独自のユーザ名およびパスワードを特定のアクセス ポイントに割り当てます。このコマンドには、次のキーワードと引数が含まれます。 • **username**：ユーザ名を追加するように指定します。 • *user-id*：ユーザ名。 • **password**：パスワードを追加するように指定します。 • **0**：暗号化されないパスワードを指定します。 • **8**：AES 暗号化パスワードを指定します。 • *passwd*：パスワード。 （注） passwordパラメータには強力なパスワードを入力する必要があります。強力なパスワードの特徴については、ステップ2の注記を参照してください。 このコマンドに入力した認証設定は、スイッチやアクセスポイントをリブートした後や、アクセス ポイントが新しいスイッチに join された場合でも保持されます。
ステップ6	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ7	**no ap dot1x username** *user_name_value* **password 0** *password_value* 例： `スイッチ(config)# no ap dot1x username dot1xusr password 0 dot1xpass`	すべてのアクセス ポイントまたは特定のアクセス ポイントに対して802.1X 認証をディセーブルにします。 このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。 （注） 特定のアクセスポイントの802.1X認証は、グローバル802.1X認証が有効でない場合にだけ無効にできます。グローバル802.1X 認証が有効な場合は、すべてのアクセス ポイントに対してだけ 802.1X を無効にできます。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 9	**show ap summary** 例： スイッチ# show ap summary	スイッチに join するすべてのアクセス ポイントの認証設定を表示します。 （注） グローバルな認証が設定されていない場合、[Global AP Dot1x User Name] テキスト ボックスには「Not Configured」と表示されます。
ステップ 10	**show ap name** *Cisco_AP* **config general** 例： スイッチ# show ap name AP02 config general	特定のアクセス ポイントの認証設定を表示します。 （注） このアクセス ポイントがグローバル認証用に設定されている場合は、[AP Dot1x User Mode] テキスト ボックスに「Automatic」と表示されます。このアクセス ポイントのグローバル認証設定が上書きされている場合は、[AP Dot1x User Mode] テキスト ボックスに「Customized」と表示されます。

関連トピック

アクセス ポイントの認証設定の表示：例，（580 ページ）

認証のスイッチの設定（CLI）

（注） スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **dot1x system-auth-control**
4. **aaa new-model**
5. **aaa authentication dot1x default group radius**
6. **radius-server host** *host_ip_adress* **acct-port** *port_number* **auth-port** *port_number* **key 0** *unencryptied_server_key*
7. **interface TenGigabitEthernet1/0/1**
8. **switch mode access**
9. **dot1x pae authenticator**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**dot1x system-auth-control** 例： `スイッチ(config)# dot1x system-auth-control`	システム認証制御をイネーブルにします。
ステップ 4	**aaa new-model** 例： `スイッチ(config)# aaa new-model`	新しいアクセス コントロール コマンドと機能をイネーブルにします
ステップ 5	**aaa authentication dot1x default group radius** 例： `スイッチ(config)# aaa authentication dot1x default group radius`	サーバ グループ内のすべての RADIUS ホストを使用して、IEEE 802.1X のデフォルトの認証リストを設定します。
ステップ 6	**radius-server host** *host_ip_adress* **acct-port** *port_number* **auth-port** *port_number* **key 0** *unencryptied_server_key* 例： `スイッチ(config)# radius-server host 10.1.1.1 acct-port 1813 auth-port 6225 key 0 encryptkey`	RADIUS認証サーバのクリアテキストの暗号キーを設定します。
ステップ 7	**interface TenGigabitEthernet1/0/1** 例： `スイッチ(config)# interface TenGigabitEthernet1/0/1`	10 ギガビット イーサネット インターフェイスを設定します。 コマンド プロンプトが Controller(config)# から Controller(config-if)# に変更します。
ステップ 8	**switch mode access** 例： `スイッチ(config-if)# switch mode access`	インターフェイスへの無条件の truncking モード アクセスを設定します。

	コマンドまたはアクション	目的
ステップ 9	**dot1x pae authenticator** 例： `スイッチ(config-if)# dot1x pae authenticator`	オーセンティケータとして 802.1X インターフェイスの PAE タイプを設定します。
ステップ 10	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

アクセス ポイントの認証設定の表示：例, （580 ページ）

アクセス ポイントの認証の設定例

アクセス ポイントの認証設定の表示：例

次に、スイッチに接続するすべてのアクセス ポイントの認証設定を表示する例を示します。

```
スイッチ# show ap summary
Number of APs.................................... 1
Global AP User Name.............................. globalap
Global AP Dot1x User Name........................ globalDot1x
```

次に、特定のアクセス ポイントの認証設定を表示する例を示します。

```
スイッチ# show ap name AP02 config dot11 24ghz general
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... TSIM_AP2
...
AP Dot1x User Mode............................... AUTOMATIC
AP Dot1x User Name............................... globalDot1x
```

第 31 章

自律アクセス ポイントの Lightweight モードへの変換

- 機能情報の確認，581 ページ
- Lightweight モードに自律アクセス ポイントを変換するための前提条件，582 ページ
- Lightweight モードに変換される Autonomous アクセス ポイントについて，582 ページ
- Lightweight アクセス ポイントの Autonomous アクセス ポイントへの再変換方法，584 ページ
- アクセス ポイントの認可（CLI），585 ページ
- 変換したアクセス ポイントでの Reset ボタンのディセーブル化（CLI），587 ページ
- AP クラッシュ ログ情報のモニタリング，588 ページ
- アクセス ポイントでの固定 IP アドレスの設定方法，589 ページ
- TFTP リカバリ手順を使用したアクセス ポイントのリカバリ，591 ページ
- Autonomous アクセス ポイントを Lightweight モードに変換する場合の設定例，591 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

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

Lightweightモードに自律アクセスポイントを変換するための前提条件

- Lightweightモードに変換したアクセスポイントは、無線ドメインサービス（WDS）をサポートしません。変換したアクセス ポイントは、Cisco ワイヤレス LAN スイッチとのみ通信し、WDSデバイスとは通信できません。ただし、アクセスポイントがコントローラにアソシエートする際、スイッチが WDS に相当する機能を提供します。
- すべての Cisco Lightweight アクセス ポイントでは、無線ごとに 16 の Basic Service Set Identifier（BSSID）およびアクセス ポイントごとに合計 16 のワイヤレス LAN をサポートします。変換されたアクセス ポイントがスイッチにアソシエートすると、アクセス ポイントがアクセス ポイント グループのメンバーでない限り、ID 1～16 のワイヤレス LAN のみがアクセス ポイントにプッシュされます。
- Lightweight モードに変換したアクセス ポイントは、DHCP、DNS、または IP サブネット ブロードキャストを使用して IP アドレスを取得し、スイッチを検出する必要があります。

Lightweight モードに変換される Autonomous アクセス ポイントについて

Autonomous Cisco Aironet アクセス ポイントを Lightweight モードに変換できます。アクセス ポイントをLightweightモードにアップグレードしようとすると、アクセスポイントはスイッチと通信し、スイッチから構成およびソフトウェア イメージを受信します。

Lightweight モードから Autonomous モードへの復帰

Autonomous アクセス ポイントを Lightweight モードに変換してから、Autonomous モードをサポートする Cisco IOS リリース（Cisco IOS リリース 12.3(7)JA 以前のリリース）をロードして、そのアクセス ポイントを Lightweight 装置から Autonomous 装置に戻すことができます。アクセス ポイントがスイッチに関連付けられている場合、スイッチを使用して Cisco IOS リリースをロードします。アクセス ポイントがスイッチに関連付けられていない場合、TFTP を使用して Cisco IOS リリースをロードします。いずれの方法でも、ロードする Cisco IOS Release を含む TFTP サーバにアクセス ポイントがアクセスできる必要があります。

DHCP オプション 43 および DHCP オプション 60 の使用

Cisco Aironet アクセス ポイントは、DHCP オプション 43 に Type-Length-Value（TLV）形式を使用します。DHCP サーバは、アクセス ポイントの DHCP ベンダー クラス ID（VCI）文字列に基づいてオプションを返すよう、プログラムする必要があります（DHCP オプション 60）。

DHCP オプション 43 の設定方法については、ご使用の DHCP サーバの製品ドキュメンテーションを参照してください。『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*』には、DHCP サーバのオプション 43 の設定手順の例が記載されています。

アクセス ポイントが、サービス プロバイダー オプション AIR-OPT60-DHCP を選択して注文された場合、そのアクセス ポイントの VCI 文字列は、前の表にある VCI 文字列と異なります。VCI 文字列の末尾には「ServiceProvider」が付きます。たとえば、このオプションが付いた 1260 は、VCI 文字列「Cisco AP c1260-ServiceProvider」を返します。

（注） DHCP サーバから取得するスイッチの IP アドレスは、ユニキャスト IP アドレスになります。DHCP オプション 43 を設定する場合は、スイッチの IP アドレスをマルチキャスト アドレスとして設定しないでください。

変換したアクセス ポイントがクラッシュ情報をスイッチに送信する方法

変換したアクセスポイントが予期せずリブートした場合、アクセスポイントではクラッシュ発生時にローカル フラッシュ メモリ上にクラッシュ ファイルが保存されます。装置がリブートしたら、アクセス ポイントはリブートの理由をスイッチに送信します。クラッシュにより装置がリブートした場合、スイッチは既存の CAPWAP メッセージを使用してクラッシュ ファイルを取得し、スイッチのフラッシュ メモリに保存します。クラッシュ情報のコピーは、スイッチがアクセス ポイントから取得した時点で、アクセス ポイントのフラッシュ メモリから削除されます。

変換したアクセス ポイントからのメモリ コア ダンプのアップロード

デフォルトでは、Lightweight モードに変換したアクセス ポイントは、スイッチにメモリ コア ダンプを送信しません。このセクションでは、スイッチ GUI または CLI を使用してアクセス ポイント コア ダンプをアップロードする手順について説明します。

変換されたアクセス ポイントの MAC アドレスの表示

コントローラが変換されたアクセス ポイントの MAC アドレスをコントローラ GUI の情報ページに表示する方法には、いくつか異なる点があります。

- [AP Summary] ページには、コントローラにより変換されたアクセス ポイントのイーサネット MAC アドレスのリストが表示されます。
- [AP Detail] ページには、変換されたアクセス ポイントの BSS MAC アドレスとイーサネット MAC アドレスのリストが、コントローラにより表示されます。
- [Radio Summary] ページには、変換されたアクセス ポイントのリストがスイッチにより無線 MAC アドレス順に表示されます。

Lightweight アクセス ポイントの静的 IP アドレスの設定

DHCP サーバに IP アドレスを自動的に割り当てさせるのではなく、アクセス ポイントに IP アドレスを指定する場合は、コントローラ GUI または CLI を使用してアクセス ポイントに固定 IP アドレスを設定できます。静的 IP アドレスは、通常、AP 数の限られた導入でのみ使用されます。

静的 IP アドレスがアクセス ポイントに設定されている場合は、DNS サーバと、アクセス ポイントが属するドメインとを指定しない限り、アクセスポイントはドメイン ネーム システム（DNS）解決を使用してスイッチを検出できません。これらのパラメータは、スイッチ CLI または GUI のいずれかを使用して設定できます。

（注） アクセス ポイントを設定して、アクセスポイントの以前の DHCP アドレスが存在したサブネット上にない固定 IP アドレスを使用すると、そのアクセス ポイントはリブート後に DHCP アドレスにフォール バックします。アクセス ポイントが DHCP アドレスにフォール バックした場合は、**show ap config general***Cisco_AP* CLI コマンドを入力すると、アクセス ポイントがフォールバック IP アドレスを使用していることが表示されます。ただし、GUI は固定 IP アドレスと DHCP アドレスの両方を表示しますが、DHCP アドレスをフォールバック アドレスであるとは識別しません。

Lightweight アクセス ポイントの Autonomous アクセス ポイントへの再変換方法

Lightweight アクセス ポイントを Autonomous モードに戻す方法（CLI）

手順の概要

1. **enable**
2. **ap name** *Cisco_AP* **tftp-downgrade** *tftp_server_ip_address tftp_server_image_filename*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *Cisco_AP* **tftp-downgrade** *tftp_server_ip_address tftp_server_image_filename* 例： `スイッチ# ap name AP02 tftp-downgrade 10.0.0.1 tsrvname`	Lightweight アクセス ポイントを Autonomous モードに戻します。 （注） このコマンドを入力したら、アクセスポイントが再起動するまで待機し、CLI または GUI を使用してアクセス ポイントを再設定します。

モード ボタンと TFTP サーバを使用して Lightweight アクセス ポイントを Autonomous モードに戻す方法

ステップ 1 TFTP サーバ ソフトウェアを実行している PC に、10.0.0.2 ～ 10.0.0.30 の範囲に含まれる固定 IP アドレスを設定します。

ステップ 2 コンピュータの TFTP サーバ フォルダにアクセス ポイントのイメージ ファイル（たとえば、1140 シリーズ アクセス ポイントの場合は *c1140-k9w7-tar.123-7.JA.tar* ）が存在すること、およびその TFTP サーバがアクティブであることを確認します。

ステップ 3 TFTP サーバ フォルダ内の 1140 シリーズ アクセス ポイントのイメージ ファイルの名前を **c1140-k9w7-tar.default**に変更します。

ステップ 4 カテゴリ 5（CAT5）のイーサネット ケーブルを使用して、PC をアクセス ポイントに接続します。

ステップ 5 アクセス ポイントの電源を切ります。

ステップ 6 MODE ボタンを押しながら、アクセス ポイントに電源を再接続します。

（注） アクセス ポイントの**MODE** ボタンがイネーブルになります。

ステップ 7 **MODE** ボタンを押し続けて、ステータス LED が赤色に変わったら（約 20 ～ 30 秒かかります）、MODE ボタンを放します。

ステップ 8 アクセス ポイントがリブートしてすべての LED が緑色に変わった後、ステータス LED が緑色に点滅するまで待ちます。

ステップ 9 アクセス ポイントがリブートしたら、GUI または CLI を使用してアクセス ポイントを再設定します。

アクセス ポイントの認可（CLI）

手順の概要

1. **enable**
2. **configure terminal**
3. **ap auth-list ap-policy authorize-ap**
4. **username** *user_name* **mac aaa attribute list** *list_name*
5. **aaa new-model**
6. **aaa authorization credential-download** *auth_list* **local**
7. **aaa attribute list** *list*
8. **aaa session-id common**
9. **aaa local authentication default authorization default**
10. **show ap name** *Cisco_AP* **config general**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ# **enable**	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap auth-list ap-policy authorize-ap** 例： スイッチ(config)# ap auth-list ap-policy authorize-ap	アクセス ポイントの許可ポリシーを設定します。
ステップ 4	**username** *user_name* **mac aaa attribute list** *list_name* 例： スイッチ(config)# username aaa.bbb.ccc mac aaa attribute list attrlist	アクセス ポイントの MAC アドレスをローカルで設定します。
ステップ 5	**aaa new-model** 例： スイッチ(config)# aaa new-model	新しいアクセス コントロール コマンドと機能をイネーブルにします
ステップ 6	**aaa authorization credential-download** *auth_list* **local** 例： スイッチ(config)# aaa authorization credential-download auth_download local	ローカル サーバから EAP 資格情報をダウンロードします。
ステップ 7	**aaa attribute list** *list* 例： スイッチ(config)# aaa attribute list alist	AAA 属性リストの定義を設定します。
ステップ 8	**aaa session-id common** 例： スイッチ(config)# aaa session-id common	AAA の共通セッション ID を設定します。
ステップ 9	**aaa local authentication default authorization default** 例： スイッチ(config)# aaa local authentication default authorization default	ローカル認証方式リストを設定します。

	コマンドまたはアクション	目的
ステップ 10	**show ap name** *Cisco_AP* **config general** 例： スイッチ(config)# show ap name AP01 config general	特定のアクセス ポイントに対応する設定情報を表示します。

変換したアクセス ポイントでの Reset ボタンのディセーブル化（CLI）

Lightweight モードに変換したアクセス ポイントの Reset ボタンをイネーブルまたはディセーブルにできます。Reset ボタンには、アクセス ポイントの外面に MODE と書かれたラベルが付けられています。

（注） コントローラ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ap reset-button**
4. **end**
5. **ap name** *Cisco_AP* **reset-button**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ# enable	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**no ap reset-button** 例： `スイッチ(config)# no ap reset-button`	スイッチに関連付けられ、変換したすべてのアクセス ポイントの Reset ボタンをディセーブルにします。 （注） スイッチに関連付けられ、変換したすべてのアクセス ポイントの Reset ボタンをイネーブルにするには、**ap reset-button** コマンドを入力します。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**ap name** *Cisco_AP* **reset-button** 例： `スイッチ# ap name AP02 reset-button`	指定した変換済みアクセスポイントのResetボタンをイネーブルにします。

AP クラッシュ ログ情報のモニタリング

（注） スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **enable**
2. **show ap crash-file**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 2	**show ap crash-file** 例： `スイッチ# show ap crash-file`	クラッシュ ファイルがスイッチにダウンロードされているかどうかを確認します。

アクセス ポイントでの固定 IP アドレスの設定方法

アクセス ポイントでの固定 IP アドレスの設定（CLI）

手順の概要

1. **enable**
2. **ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway*
3. **enable**
4. **configure terminal**
5. **ap static-ip name-server** *nameserver_ip_address*
6. **ap static-ip domain** *static_ip_domain*
7. **end**
8. **show ap name** *Cisco_AP* **config general**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway* 例： `スイッチ# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2`	アクセス ポイントの固定 IP アドレスを設定します。このコマンドには、次のキーワードと引数が含まれます。 • **ip-address**：Cisco アクセス ポイントの固定 IP アドレスを指定します。 • *ip-address*：Cisco アクセス ポイントの固定 IP アドレス。 • **netmask**：Cisco アクセス ポイントの固定 IP ネットマスクを指定します。 • *netmask*：Cisco アクセス ポイントの固定 IP ネットマスク。 • **gateway**：Cisco アクセス ポイント ゲートウェイを指定します。 • *gateway*：Cisco アクセス ポイント ゲートウェイの IP アドレス。 アクセス ポイントがリブートしてスイッチに再 join し、指定した固定 IP アドレスがアクセス ポイントにプッシュされます。固

	コマンドまたはアクション	目的
		定IPアドレスがアクセス ポイントに送信された後、DNSサーバのIPアドレスおよびドメイン名を設定できます。アクセス ポイントのリブート後にステップ 3 と 4 を実行します。
ステップ 3	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 4	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 5	**ap static-ip name-server** *nameserver_ip_address* 例： `スイッチ(config)# ap static-ip name-server 10.10.10.205`	特定のアクセス ポイントまたはすべてのアクセス ポイントがDNS解決を使用してスイッチを検出できるようDNSサーバを設定します。 （注） DNS サーバ設定を元に戻すには、**no ap static-ip name-server** *nameserver_ip_address* コマンドを入力します。
ステップ 6	**ap static-ip domain** *static_ip_domain* 例： `スイッチ(config)# ap static-ip domain domain1`	特定のアクセス ポイントまたはすべてのアクセス ポイントが属するドメインを設定します。 （注） ドメイン名の設定を元に戻すには、**no ap static-ip domain** *static_ip_domain* コマンドを入力します。
ステップ 7	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show ap name** *Cisco_AP* **config general** 例： `スイッチ# show ap name AP03 config general`	アクセス ポイントの IP アドレス設定を表示します。

TFTP リカバリ手順を使用したアクセス ポイントのリカバリ

ステップ 1 必要なリカバリ イメージを Cisco.com（ap3g2-k9w8-tar.152-2.JA.tar）からダウンロードし、ご利用の TFTP サーバのルート ディレクトリにインストールします。

ステップ 2 TFTP サーバをターゲットのアクセス ポイントと同じサブネットに接続して、アクセス ポイントをパワーサイクリングします。アクセス ポイントは TFTP イメージから起動し、スイッチ に接続してサイズの大きなアクセス ポイントのイメージをダウンロードし、アップグレード手順を完了します。

ステップ 3 アクセス ポイントが回復したら、TFTP サーバを削除できます。

Autonomous アクセス ポイントを Lightweight モードに変換する場合の設定例

アクセス ポイントの IP アドレス設定の表示：例

次に、アクセス ポイントの IP アドレス設定を表示する例を示します。

```
スイッチ# show ap name AP03 dot11 24ghz config general
Cisco AP Identifier.............. 4
Cisco AP Name............................ AP6
IP Address Configuration................. Static IP assigned
IP Address............................... 10.10.10.118
IP NetMask............................... 255.255.255.0
Gateway IP Addr.......................... 10.10.10.1
Domain................................... Domain1
Name Server.............................. 10.10.10.205
...
```

アクセス ポイントのクラッシュ ファイル情報の表示：例

次の例は、アクセスポイントのクラッシュファイル情報を表示する方法を示しています。このコマンドを使用して、ファイルがスイッチにダウンロードされたかどうかを確認できます。

```
スイッチ# show ap crash-file
Local Core Files:
lrad_AP1130.rdump0 (156)

The number in parentheses indicates the size of the file. The size should
be greater than zero if a core dump file is available.
```

第 32 章

Cisco ワークグループ ブリッジの使用

- 機能情報の確認，593 ページ
- Cisco ワークグループ ブリッジと Cisco 以外のワークグループ ブリッジについて，593 ページ
- ワークグループ ブリッジ状態のモニタリング，594 ページ
- WGB の問題のデバッグ（CLI），595 ページ
- ワークグループ ブリッジの設定例，596 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

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

Cisco ワークグループ ブリッジと Cisco 以外のワークグループ ブリッジについて

WGB とは、Autonomous IOS アクセス ポイント上で設定でき、イーサネットで WGB アクセス ポイントに接続されたクライアントの代わりに Lightweight アクセス ポイントに無線で接続を提供するモードです。イーサネット インターフェイス上の有線クライアントの MAC アドレスを記憶し、それを Internet Access Point Protocol（IAPP）メッセージングを使用して Lightweight アクセス ポイントに報告することで、WGB は単一の無線セグメントを介して有線ネットワークに接続します。

WGB は、単一の無線接続を Lightweight アクセス ポイントに確立して、有線クライアントに無線で接続できるようになります。

Cisco WGB が使用されている場合、WGB は、アソシエートされているすべてのクライアントをアクセスポイントに通知します。スイッチアクセスポイントにアソシエートされたクライアントを認識します。シスコ以外の WGB が使用されている場合、スイッチには、WGB の後方にある有線セグメントのクライアントの IP アドレスに関する情報は伝わりません。この情報がないと、スイッチは以下の種類のメッセージをドロップします。

- WGB クライアントに対するディストリビューション システムからの ARP REQ
- WGB クライアントからの ARP RPLY
- WGB クライアントからの DHCP REQ
- WGB クライアントに対する DHCP RPLY

ワークグループ ブリッジ状態のモニタリング

（注） スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **enable**
2. **show wireless wgb summary**
3. **show wireless wgb mac-address** *wgb_mac_address* **detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 2	**show wireless wgb summary** 例： `スイッチ# show wireless wgb summary`	ネットワーク上のワークグループ ブリッジ（WGB）を表示します。
ステップ 3	**show wireless wgb mac-address** *wgb_mac_address* **detail** 例： `スイッチ# show wireless wgb mac-address 00:0d:ed:dd:25:82 detail`	特定の WGB に接続されている有線クライアントの詳細を表示します。

WGB の問題のデバッグ（CLI）

（注） スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **enable**
2. **debug iapp all**
3. **debug iapp error**
4. **debug iapp packet**
5. **debug mobility handoff** [**switch** *switch_number*]
6. **debug dhcp**
7. **debug dot11 mobile**
8. **debug dot11 state**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 2	**debug iapp all** 例： `スイッチ# debug iapp all`	IAPP メッセージのデバッグをイネーブルにします。
ステップ 3	**debug iapp error** 例： `スイッチ# debug iapp error`	IAPP エラー イベントのデバッグをイネーブルにします。
ステップ 4	**debug iapp packet** 例： `スイッチ# debug iapp packet`	IAPP パケットのデバッグをイネーブルにします。
ステップ 5	**debug mobility handoff** [**switch** *switch_number*]	ローミング問題のデバッグをイネーブルにします。

	コマンドまたはアクション	目的
	例： スイッチ# debug mobility handoff	
ステップ 6	**debug dhcp** 例： スイッチ# debug dhcp	DHCP を使用する場合の IP 割り当ての問題をデバッグします。
ステップ 7	**debug dot11 mobile** 例： スイッチ# debug dot11 mobile	dot11/モバイルデバッグをイネーブルにします。スタティック IP を使用する場合の IP 割り当ての問題をデバッグします。
ステップ 8	**debug dot11 state** 例： スイッチ# debug dot11 state	dot11/ステートデバッグをイネーブルにします。スタティック IP を使用する場合の IP 割り当ての問題をデバッグします。

ワークグループ ブリッジの設定例

WGB の設定：例

次に、40 ビットの WEP キーでスタティック WEP を使用して WGB アクセス ポイントを設定する例を示します。

```
スイッチ# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチ(config)# dot11 ssid WGB_with_static_WEP
スイッチ(config-ssid)# authentication open
スイッチ(config-ssid)# guest-mode
スイッチ(config-ssid)# exit
スイッチ(config)# interface  dot11Radio 0
スイッチ(config)# station-role workgroup-bridge
スイッチ(config-if)# encry mode wep 40
スイッチ(config-if)# encry key 1 size 40 0 1234567890
スイッチ(config-if)# ssid WGB_with_static_WEP
スイッチ(config-if)# end
```

この WGB がアクセス ポイントにアソシエートしていることを確認するには、WGB に次のコマンドを入力します。

show dot11 association

以下に類似した情報が表示されます。

```
スイッチ# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address    IP address      Device        Name            Parent         State
000b.8581.6aee 10.11.12.1      WGB-client    map1            -              Assoc
ap#
```

第 33 章

プローブ要求フォワーディングの設定

- 機能情報の確認，599 ページ
- プローブ要求フォワーディングの設定について，599 ページ
- プローブ要求フォワーディングの設定方法（CLI），599 ページ

機能情報の確認

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

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

プローブ要求フォワーディングの設定について

プローブ要求とはクライアントが送信する 802.11 管理フレームであり、SSID の機能についての情報を要求します。デフォルトでは、アクセス ポイントは応答済みのプローブ要求をスイッチが処理できるよう送信します。応答済みのプローブ要求とは、アクセス ポイントがサポートする SSID のプローブ要求です。必要に応じて、応答済みのプローブ要求および未応答のプローブ要求の両方をスイッチにフォワードするようアクセス ポイントを設定できます。スイッチは応答済みのプローブ要求からの情報を使用してロケーションの精度を向上できます。

プローブ要求フォワーディングの設定方法（CLI）

（注） スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **configure terminal**
2. **wireless probe filter**
3. **wireless probe filter** *num_probes interval*
4. **end**
5. **show wireless probe**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless probe filter** 例： `スイッチ(config)# wireless probe filter`	アクセス ポイントからスイッチに転送されたプローブ要求のフィルタリングをイネーブルまたはディセーブルにします。 （注） デフォルトのフィルタ設定であるプローブ フィルタリングを有効にすると、アクセス ポイントは応答済みのプローブ要求のみをスイッチに転送します。プローブ フィルタリングを無効にすると、アクセス ポイントは応答済みのプローブ要求と未応答のプローブ要求の両方をスイッチに転送します。
ステップ 3	**wireless probe filter** *num_probes interval* 例： `スイッチ(config)# wireless probe filter 5 5`	指定された間隔のアクセス ポイント無線ごとにクライアント単位でスイッチに送信されるプローブ要求の数を制限します。このコマンドで次の引数を指定する必要があります。 • *num_probes*：指定された間隔での、1 つのアクセス ポイント無線および 1 つのクライアントあたりのスイッチへ送られたプローブ要求数。範囲は 1 ～ 100 です。 • *interval*：ミリ秒単位でのプローブ制限間隔。範囲は 100 ～ 10000 です。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**show wireless probe** 例： `スイッチ# show wireless probe`	詳細なプローブ要求の設定を表示します。

第 34 章

RFID トラッキングの最適化

- 機能情報の確認，601 ページ
- アクセス ポイントでの RFID トラッキングの最適化，601 ページ
- アクセス ポイントでの RFID トラッキングの最適化方法，602 ページ
- RFID トラッキングの最適化の設定例，603 ページ

機能情報の確認

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

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

アクセス ポイントでの RFID トラッキングの最適化

RFID タグの監視とロケーション計算を最適化するには、802.11b/g アクセス ポイント無線用の 2.4GHz 帯域内で最高 4 つのチャネルでトラッキングの最適化を有効化できます。この機能を使用して、通常、タグが動作するようにプログラムされているチャネル（チャネル 1、6、11 など）のみをスキャンすることができます。

アクセス ポイントでの RFID トラッキングの最適化方法

アクセス ポイントでの RFID トラッキングの最適化（CLI）

手順の概要

1. **ap name** *Cisco_AP* **mode monitor submode none**
2. **ap name** *Cisco_AP* **dot11 24ghz shutdown**
3. **ap name** *Cisco_AP* **monitor-mode tracking-opt**
4. **ap name** *Cisco_AP* **monitor-mode dot11b** {**fast-channel** [*first_channel second_channel third_channel fourth_channel*]}
5. **ap name** *Cisco_AP* **no dot11 24ghz shutdown**
6. **show ap monitor-mode summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ap name** *Cisco_AP* **mode monitor submode none** 例： `スイッチ# ap name 3602a mode monitor submode none`	アクセス ポイントの監視サブモードを none として指定します。 （注） アクセスポイントのモードを変更するとアクセスポイントがリブートすることを示す警告メッセージが表示され、**Y** を入力することで続行するかどうかを指定するプロンプトが表示されます。 **Y**を入力すると、アクセス ポイントがリブートします。
ステップ 2	**ap name** *Cisco_AP* **dot11 24ghz shutdown** 例： `スイッチ# ap name AP01 dot11 24ghz shutdown`	アクセス ポイント無線をディセーブルにします。
ステップ 3	**ap name** *Cisco_AP* **monitor-mode tracking-opt** 例： `スイッチ# ap name TSIM_AP1 monitor-mode tracking-opt`	使用する国でサポートされる動的チャネル割り当て（DCA）チャネルのみをスキャンするようにアクセス ポイントを設定します。 （注） アクセスポイントのトラッキングの最適化をディセーブルにするには、**ap name** *Cisco_AP* **monitor-mode tracking-opt no-optimization** コマンドを入力します。

	コマンドまたはアクション	目的

ステップ 4	**ap name** *Cisco_AP* **monitor-mode dot11b** {**fast-channel** [*first_channel second_channel third_channel fourth_channel*]}
	
	例：
	`スイッチ# ap name AP01 monitor-mode dot11b`
	`fast-channel 1 2 3 4`
		アクセス ポイントによりスキャンされる特定の 802.11b チャネルを最大 4 つ選択します。
		（注） 米国では、チャネル変数に 1 ～ 11 の値（両端の値を含む）を割り当てることができます。その他の国ではさらに多くのチャネルがサポートされています。少なくともチャネルを 1 つ割り当てる必要があります。

ステップ 5	**ap name** *Cisco_AP* **no dot11 24ghz shutdown** 例： `スイッチ# ap name AP01 no dot11 24ghz shutdown`	アクセス ポイント無線をイネーブルにします。
ステップ 6	**show ap monitor-mode summary** 例： `スイッチ# show ap monitor-mode summary`	モニタ モードですべてのアクセス ポイントを表示します。

RFID トラッキングの最適化の設定例

モニタ モードでのすべてのアクセス ポイントの表示：例

次に、モニタ モードですべてのアクセス ポイントを表示する例を示します。

```
スイッチ# show ap monitor-mode summary

AP Name       Ethernet MAC   Status   Scanning
                                      Channel
                                      List
------------- -------------- -------- ----------
AP1131:4f2.9a 00:16:4:f2:9:a Tracking 1,6,NA,NA
```

第 35 章

国番号の設定

- 機能情報の確認，605 ページ
- 国番号の設定に関する前提条件，605 ページ
- 国番号の設定について，606 ページ
- 国番号の設定方法（CLI），607 ページ
- 国番号の設定例，609 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD>を参照してください。

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

国番号の設定に関する前提条件

- 通常、スイッチごとに 1 つの国番号を設定します。そのスイッチの物理的な場所とそのアクセス ポイントが一致しているコードを 1 つ設定します。スイッチごとに最大 20 の国番号を設定できます。これによって、複数の国がサポートされ、1 つのスイッチからさまざまな国にあるアクセス ポイントを管理できます。
- multiple-country 機能を使用している場合、同じ RF グループに join する予定のすべてのスイッチは、同じ国のセットを同じ順序で設定する必要があります。

- アクセス ポイントは、使用可能なすべての法定周波数を使用できます。ただし、アクセス ポイントは関連するドメインでサポートされる周波数に割り当てられます。
- RF グループ リーダーに設定されている国リストによって、メンバーが動作するチャネルが決定します。このリストは、RF グループ メンバーに設定されている国とは無関係です。
- 日本の規制ドメインにあるスイッチの場合は、最後にスイッチをブートしたときにスイッチで設定した 1 つ以上の日本の国番号（JP、J2、または J3）を持っている必要があります。
- 日本の規制ドメインにあるスイッチの場合は、スイッチに join された - J 規制ドメインのアクセス ポイントを少なくとも 1 つ持っている必要があります。

国番号の設定について

コントローラおよびアクセス ポイントは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。アクセス ポイント内の無線は、製造時に特定の規制区域に割り当てられています（ヨーロッパの場合には E など）。しかし、国番号を使用すると、稼働する特定の国を指定できます（フランスの場合には FR、スペインの場合には ES など）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

日本の国番号について

国番号は、各国で合法的に使用できるチャネルを定義します。日本で使用できる国番号は、次のとおりです。

- JP：コントローラに join できるのは、-J 無線のみです。
- J2：コントローラに join できるのは、-P 無線のみです。
- J3：WLC に join できるのは、-U、-P、および -Q（1550/1600/2600/3600 以外）無線ですが、-U の周波数を使用します。
- J4：コントローラに join できるのは、2.4G JPQU および 5G PQU です。

（注） 1550、1600、2600、および 3600 AP には J4 が必要です。

日本の規制区域のアクセス ポイントでサポートされているチャネルと電力レベルの一覧については、『*Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points*』を参照してください。

国番号の設定方法（CLI）

（注） スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **enable**
2. **show wireless country supported**
3. **configure terminal**
4. **ap dot11 24ghz shutdown**
5. **ap dot11 5ghz shutdown**
6. **ap country** *country_code*
7. **end**
8. **show wireless country channels**
9. **configure terminal**
10. **no ap dot11 5ghz shutdown**
11. **no ap dot11 24ghz shutdown**
12. **end**
13. **ap name** *Cisco_AP* **shutdown**
14. **configure terminal**
15. **ap country** *country_code*
16. **end**
17. **ap name** *Cisco_AP* **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 2	**show wireless country supported** 例： `スイッチ# show wireless country supported`	すべての使用可能な国番号のリストを表示します。
ステップ 3	**configure terminal** 例： `スイッチ# configure terminal`	グローバルコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ap dot11 24ghz shutdown** 例： スイッチ(config)# ap dot11 5ghz shutdown	802.11a ネットワークをディセーブルにします。
ステップ 5	**ap dot11 5ghz shutdown** 例： スイッチ(config)# ap dot11 24ghz shutdown	802.11b/g ネットワークをディセーブルにします。
ステップ 6	**ap country** *country_code* 例： スイッチ(config)# ap country IN	特定の国にアクセス ポイントを割り当てます。 （注） 選択した Country Code が、アクセス ポイントの無線のうち少なくとも 1 つの無線の規制ドメインに適合していることを確認します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show wireless country channels** 例： スイッチ# show wireless country channels	スイッチに設定された国番号の使用可能なチャネルのリストを表示します。 （注） ステップ 6 で複数の国番号を設定した場合にのみ、ステップ 9 ～ 17 を実行します。
ステップ 9	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 10	**no ap dot11 5ghz shutdown** 例： スイッチ(config)# no ap dot11 5ghz shutdown	802.11a ネットワークをイネーブルにします。
ステップ 11	**no ap dot11 24ghz shutdown** 例： スイッチ(config)# no ap dot11 24ghz shutdown	802.11b/g ネットワークをイネーブルにします。
ステップ 12	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

	コマンドまたはアクション	目的
ステップ 13	**ap name** *Cisco_AP* **shutdown** 例： スイッチ# ap name AP02 shutdown	アクセス ポイントをディセーブルにします。 （注） 国番号を設定しているアクセス ポイントのみをディセーブルにすることを確認します。
ステップ 14	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 15	**ap country** *country_code* 例： スイッチ# ap country IN	アクセス ポイントを特定の国に割り当てます。 （注） 選択した国番号が、アクセス ポイントの無線のうち少なくとも 1 つの無線の規制ドメインに適合していることを確認します。 （注） ネットワークをイネーブルにし、いくつかのアクセス ポイントをディセーブルにして、**ap country** *country_code* コマンドを入力した場合、指定された国番号は、ディセーブルにされたアクセス ポイントでのみ設定されます。他のアクセス ポイントは、すべて無視されます。
ステップ 16	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 17	**ap name** *Cisco_AP* **no shutdown** 例： スイッチ# ap name AP02 no shutdown	アクセス ポイントを有効にします。

国番号の設定例

国番号のチャネル リストの表示：例

次に、スイッチに設定されている国番号に使用可能なチャネルの一覧を表示する例を示します。

```
スイッチ# show wireless country channels

Configured Country.....................: US - United States
KEY: * = Channel is legal in this country and may be configured manually.
A = Channel is the Auto-RF default in this country.
. = Channel is not legal in this country.
C = Channel has been configured for use by Auto-RF.
x = Channel is available to be configured for use by Auto-RF.
(-,-) = (indoor, outdoor) regulatory domain allowed by this country.
```

```
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11bg :
Channels : 1 1 1 1 1
: 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US : A * * * * A * * * * A . . .
Auto-RF : . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11a : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
: 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US : . A . A . A . A A A A A * * * * * . . . * * * A A A A
*
Auto-RF : . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
4.9GHz 802.11a :
Channels : 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
: 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
US (-A ,-AB ): * * * * * * * * * * * * * * * * * * A * * * * * A
Auto-RF : . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

第 36 章

リンク遅延の設定

- 機能情報の確認，611 ページ
- リンク遅延を設定するための前提条件，611 ページ
- リンク遅延を設定する際の制限，612 ページ
- リンク遅延の設定について，612 ページ
- リンク遅延の設定方法，614 ページ
- TCP MSS の設定方法，616 ページ
- リンク テストの実行（CLI），617 ページ
- リンク遅延の設定例，618 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

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

リンク遅延を設定するための前提条件

- スイッチにより、現在のラウンドトリップ時間および継続的な最短および最長ラウンドトリップ時間が表示されます。最短および最長時間はスイッチが動作している限り維持され、クリアして再開することもできます。

- スイッチ GUI または CLI を使用して特定のアクセス ポイントのリンク遅延を設定することも、CLI を使用してスイッチに join されたすべてのアクセス ポイントのリンク遅延を設定することもできます。

リンク遅延を設定する際の制限

- リンク遅延は、アクセス ポイントとスイッチ間の Control and Provisioning of Wireless Access Points（CAPWAP）の応答所要時間を計算します。ネットワーク遅延や ping 応答は計測しません。

リンク遅延の設定について

スイッチでリンク遅延を設定して、アクセス ポイントとスイッチとの間のリンクを計測できます。この機能は、リンクが低速または信頼できない WAN 接続の可能性があるスイッチに接続されたすべてのアクセス ポイントで使用できます。

TCP MSS

トランスミッションコントロールプロトコル（TCP）スリーウェイ ハンドシェイクにおけるクライアントの最大セグメント サイズ（MSS）が、最大伝送単位で処理できるサイズよりも大きい場合、スループットの低下およびパケットのフラグメンテーションが発生する場合があります。この問題を回避するには、スイッチに接続されているすべてのアクセス ポイント、または特定のアクセス ポイントに対して、MSS を指定します。

この機能を有効にすると、アクセス ポイントがデータ パスのワイヤレス クライアントと送受信する TCP パケットの MSS を選択します。これらのパケットの MSS が設定した値または CAPWAP トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、設定された新しい値に変更します。

リンク テスト

リンク テストを使用して、2 つのデバイス間の無線リンクの質を決定します。リンク テストの際には、要求と応答の 2 種類のリンク テスト パケットを送信します。リンク テストの要求パケットを受信した無線は、適切なテキストボックスを記入して、応答タイプセットを使用して送信者にパケットを返信します。

クライアントからアクセスポイント方向への無線リンクの質は、アクセスポイントからクライアント方向へのものと異なることがあり、それは双方の送信電力と受信感度が非対称であることによるものです。2 種類のリンク テスト（ping テストおよび CCX リンク テスト）を実行できます。

ping リンク テストでは、コントローラはクライアントからアクセス ポイント方向でのみリンクの質をテストできます。アクセス ポイントで受信された ping パケットの RF パラメータは、クライアントからアクセス ポイント方向のリンクの質を決定するためにコントローラによりポーリングされます。

*CCX*リンク テストでは、スイッチはアクセス ポイントからクライアントの方向でもリンクの質をテストできます。スイッチはクライアントにリンク テスト要求を発行し、クライアントは、応答パケットで受信した要求パケットの RF パラメータ（受信信号強度インジケータ [RSSI]、信号対雑音比 [SNR] など）を記録します。リンク テストの要求と応答の両方のロールを、アクセス ポイントとスイッチに実装します。アクセス ポイントまたはスイッチから CCX v4 クライアントまたは v5 クライアントに対してリンク テストを開始できるのと同様に、CCX v4 クライアントまたは v5 クライアントからもアクセス ポイントまたはスイッチに対してリンク テストを開始できます。

スイッチでは、CCX リンク テストでのリンクの質のメトリックが両方向（アウト：アクセス ポイントからクライアント、イン：クライアントからアクセス ポイント）で表示されます。

- RSSI の形式の信号強度（最小、最大、および平均）
- SNR の形式の信号の質（最小、最大、および平均）
- 再試行されたパケットの合計数
- 単一パケットの最大再試行回数
- 消失パケット数
- 正常に送信されたパケットのデータ レート

コントローラにより、方向とは無関係に次のメトリックが表示されます。

- リンク テストの要求/応答の往復時間（最小、最大、および平均）

コントローラ ソフトウェアは、CCX バージョン 1 ～ 5 をサポートします。CCX サポートは、コントローラ上の各WLANについて自動的に有効となり、無効にできません。コントローラでは、クライアント データベースにクライアントの CCX バージョンが格納されます。このクライアントの機能を制限するには、これを使用します。クライアントが CCX v4 または v5 をサポートしていない場合、コントローラはクライアント上でpingリンク テストを実行します。クライアントが CCX v4 または v5 をサポートしている場合、コントローラはクライアント上で CCX リンク テストを実行します。クライアントが CCX リンク テストの間にタイムアウトになった場合、コントローラは ping リンク テストに自動的に切り替わります。

リンク遅延の設定方法

リンク遅延の設定（CLI）

手順の概要

1. **enable**
2. **configure terminal**
3. **ap link-latency**
4. **ap tcp-adjust-mss size** *size*
5. **show ap name** *Cisco_AP* **config general**
6. **ap name** *Cisco_AP* **link-latency** [**reset**]
7. **show ap name** *Cisco_AP* **config general**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap link-latency** 例： `スイッチ(config)# ap link-latency`	現在スイッチに関連付けられているすべてのアクセス ポイントのリンク遅延をイネーブルにします。 （注） スイッチと関連付けられているすべてのアクセス ポイントのリンク遅延をディセーブルにするには、**no ap link-latency** コマンドを使用します。 （注） これらのコマンドは、現在スイッチにジョインされているアクセス ポイントのリンク遅延のみをイネーブルまたはディセーブルにします。将来ジョインするアクセス ポイントのリンク遅延をイネーブルまたはディセーブルにする必要があります。

	コマンドまたはアクション	目的
		（注） このスイッチに関連付けられている特定のアクセス ポイントのリンク遅延をイネーブルまたはディセーブルにするには、特権 EXEC モードで次のコマンドを入力します。 • **ap name** *Cisco_AP* **link-latency**：リンク遅延をイネーブルにします。 • **ap name** *Cisco_AP* **no link-latency**：リンク遅延をディセーブルにします。
ステップ 4	**ap tcp-adjust-mss size** *size* 例： `スイッチ(config)# ap tcp-adjust-mss size 537`	すべてのアクセス ポイントの TCP MSS 調整サイズを設定します。範囲は 536 ～ 1363 です。
ステップ 5	**show ap name** *Cisco_AP* **config general** 例： `スイッチ(config)# show ap name AP02 config general`	アクセス ポイントの一般的な設定の詳細を表示します。これらの設定の詳細には、コマンドで指定したアクセス ポイントに対応するリンク遅延の結果が含まれます。 このコマンドの出力には、次のリンク遅延結果が含まれます。 • [Current Delay]：アクセス ポイントからスイッチ、およびその逆の方向の CAPWAP ハートビート パケットの現在のラウンドトリップ時間（ミリ秒）。 • [Maximum Delay]：リンク遅延がイネーブルになったか、またはリセットされてからのアクセス ポイントからスイッチ、およびその逆の方向の CAPWAP ハートビート パケットの最長のラウンドトリップ時間（ミリ秒）。 • [Minimum Delay]：リンク遅延がイネーブルになったか、またはリセットされてからのアクセス ポイントからスイッチ、およびその逆の方向の CAPWAP ハートビート パケットの最長のラウンドトリップ時間（ミリ秒）。
ステップ 6	**ap name** *Cisco_AP* **link-latency** [**reset**] 例： `スイッチ(config)# ap name AP02 link-latency reset`	特定のアクセス ポイントのスイッチの現在、最短、および最長リンク遅延統計情報をクリアします。

	コマンドまたはアクション	目的
ステップ 7	**show ap name** *Cisco_AP* **config general** 例： `スイッチ(config)# show ap name AP02 config general`	アクセス ポイントの一般的な設定の詳細を表示します。リセット操作の結果を表示するには、このコマンドを使用します。

TCP MSS の設定方法

TCP MSS の設定（CLI）

手順の概要

1. **configure terminal**
2. **ap tcp-adjust-mss size** *size_value*
3. **reload**
4. **show ap tcp-adjust-mss**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap tcp-adjust-mss size** *size_value* 例： `スイッチ(config)# ap tcp-adjust-mss size 537`	ユーザが指定した特定のアクセス ポイントで TCP MSS をイネーブルにします。 （注） スイッチに関連付けられているすべてのアクセス ポイントで TCP MSS をイネーブルにするには、**ap tcp-adjust-mss size** *size_value* コマンドを入力します。ここで、サイズ パラメータの範囲は 536～1363 バイトです。デフォルト値はクライアントにより異なります。
ステップ 3	**reload** 例： `スイッチ# reload`	変更をイネーブルにするには、スイッチをリブートします。

	コマンドまたはアクション	目的
ステップ 4	**show ap tcp-adjust-mss** 例： `スイッチ# show ap tcp-adjust-mss`	このスイッチに関連付けられているすべてのアクセス ポイントの現在の TCP MSS 設定を表示します。 （注） 特定のアクセス ポイントに対応する TCP MSS 設定を表示するには、**show ap name** *Cisco_AP* **tcp-adjust-mss** コマンドを入力します。

リンク テストの実行（CLI）

（注） スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

手順の概要

1. **test wireless linktest** *mac_address*
2. **configure terminal**
3. **wireless linktest frame-size** *frame_size*
4. **wireless linktest number-of-frames** *number_of_frames*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**test wireless linktest** *mac_address* 例： `スイッチ# test wireless linktest 00:0d:88:c5:8a:d1`	リンク テストを実行します。
ステップ 2	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**wireless linktest frame-size** *frame_size* 例： `スイッチ(config)# wireless linktest frame-size 41`	各パケットのリンク テスト フレームのサイズを設定します。

	コマンドまたはアクション	目的
ステップ 4	**wireless linktest number-of-frames** *number_of_frames* 例： スイッチ(config)# wireless linktest number-of-frames 50	リンク テスト用に送信するフレームの数を設定します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

リンク遅延の設定例

リンク テストの実行：例

次に、リンク テストを実行する例を示します。

```
スイッチ# test wireless linktest 6470.0227.ca55
スイッチ# show wireless linktest statistic

Link Test to 64700227CA55 with 500 frame-size.
Client MAC Address                            : 6470.0227.ca55
AP Mac Address                                : 44e4.d901.19c0
Link Test Packets Sent                        : 20
Link Test Packets Received                    : 20
Link Test Pkts Lost(Total/AP->Clnt/Clnt->AP)  : 0/0/0
Link Test Pkts round trip time (min/max/avg)  : 9ms/31ms/14ms
RSSI at AP (min/max/average)                  : -53dBm/-51dBm/-52dBm
RSSI at Client (min/max/average)              : -48dBm/-40dBm/-44dBm
```

リンク遅延情報の表示：例

この例は、アクセス ポイントの一般的な設定の詳細を表示する方法を示しています。これらの設定の詳細には、コマンドで指定したアクセス ポイントに対応するリンク遅延の結果が含まれます。

```
スイッチ# show ap name AP01 config general

Cisco AP Name                                  : AP01
Cisco AP Identifier                            : 55
Country Code                                   : US  - United States
Regulatory Domain Allowed by Country           : 802.11bg:-A     802.11a:-A
AP Country Code                                : US  - United States
AP Regulatory Domain                           : Unconfigured
Switch Port Number                             : Te1/0/1
MAC Address                                    : 0000.2000.03f0
IP Address Configuration                       : Static IP assigned
IP Address                                     : 9.9.9.16
IP Netmask                                     : 255.255.0.0
```

```
Gateway IP Address                              : 9.9.9.2
Fallback IP Address Being Used                  : 9.9.9.16
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
Cisco AP Location                               : default-location
Cisco AP Group Name                             : default-group
Primary Cisco Controller Name                   : CAPWAP Controller
Primary Cisco Controller IP Address             : 9.9.9.2
Secondary Cisco Controller Name                 :
Secondary Cisco Controller IP Address           : Not Configured
Tertiary Cisco Controller Name                  :
Tertiary Cisco Controller IP Address            : Not Configured
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 3502E
AP Image                                        : C3500-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K002
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : Not Configured
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 16 days 3 hours 14 minutes 1 s
econd
AP CAPWAP Up Time                               : 33 minutes 15 seconds
Join Date and Time                              : 01/02/2013 22:41:47
Join Taken Time                                 : 16 days 2 hours 40 minutes 45
seconds
Join Priority                                   : 1
Ethernet Port Duplex                            : Auto
Ethernet Port Speed                             : Auto
AP Link Latency                                 : Enabled
Current Delay                                   : 0
Maximum Delay                                   : 0
Minimum Delay                                   : 0
Last Updated (based on AP up time)              : 0 seconds
Rogue Detection                                 : Disabled
AP TCP MSS Adjust                               : Disabled
AP TCP MSS Size                                 : 536
```

TCP MSS 設定の表示：例

次に、スイッチに関連付けられているすべてのアクセス ポイントの現在の TCP MSS 設定を表示する例を示します。

```
スイッチ# show ap tcp-adjust-mss

AP Name                    TCP State        MSS Size
-----------------------------------------------------
AP01                       Disabled         6146
```

```
AP02                    Disabled        536
AP03                    Disabled        6146
AP04                    Disabled        6146
AP05                    Disabled        6146
```

第 37 章

Power over Ethernet の設定

- 機能情報の確認，621 ページ
- Power over Ethernet の設定について，621 ページ
- Power over Ethernet の設定方法，622 ページ
- Power over Ethernet の設定例，623 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD>を参照してください。

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

Power over Ethernet の設定について

Lightweight モードに変換されたアクセス ポイント（AP1262 など）アクセス ポイントが Cisco pre-Intelligent Power Management（pre-IPM）スイッチに接続されたパワーインジェクタで電源を供給されている場合、インライン パワーとも呼ばれる Power over Ethernet（PoE）を設定する必要があります。

Power over Ethernet の設定方法

Power over Ethernet の設定（CLI）

手順の概要

1. **ap name** *Cisco_AP* **power injector installed**
2. **ap name** *Cisco_AP* **power injector override**
3. **ap name** *Cisco_AP* **power injector switch-mac-address** *switch_mac_address*
4. **show ap name** *Cisco_AP* **config general**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ap name** *Cisco_AP* **power injector installed** 例： `スイッチ# ap name AP02 power injector installed`	PoE パワー インジェクタ状態をイネーブルにします。アクセス ポイントは、パワー インジェクタがこの特定のスイッチ ポートに接続されていることを記憶します。アクセス ポイントを再配置する場合、新しいパワー インジェクタの存在を検証した後で、このコマンドを再度入力する必要があります。 （注） ネットワークに、12 W アクセス ポイントへ直接接続すると過負荷を発生する可能性のある、従来のシスコ 6 W スイッチが装備されている場合には、このコマンドを入力します。このコマンドを入力する前に Cisco Discovery Protocol（CDP）がイネーブルになっていることを確認します。有効になっていない場合、このコマンドは失敗します。
ステップ 2	**ap name** *Cisco_AP* **power injector override** 例： `スイッチ# ap name AP02 power injector override`	セーフティ チェックを解除し、アクセス ポイントが他のスイッチ ポートに接続できるようにします。ネットワークに、12 W アクセス ポイントに直接接続すると過負荷を発生する可能性のある従来のシスコ 6 W スイッチが装備されていない場合は、このコマンドを使用できます。アクセス ポイントは、パワー インジェクタが常に接続されていることを前提としています。アクセス ポイントを再配置した場合も、パワー インジェクタの存在を前提とします。
ステップ 3	**ap name** *Cisco_AP* **power injector switch-mac-address** *switch_mac_address* 例： `スイッチ# ap name AP02 power injector switch-mac-address 10a.2d.5c.3d`	パワー インジェクタが設置されたスイッチ ポートの MAC アドレスを設定します。 （注） 接続スイッチ ポートの MAC アドレスがわかっていて、[Installed] オプションを使用して自動的に検出しない場合は、このコマンドを入力します。

	コマンドまたはアクション	目的
ステップ 4	**show ap name** *Cisco_AP* **config general** 例： `スイッチ# show ap name AP02 config general`	特定のアクセス ポイントの PoE 設定を含む共通の情報を表示します。 （注） アクセスポイントが最大電力で動作していない場合、[Power Type/Mode] テキスト ボックスには、「degraded mode」と表示されます。

Power over Ethernet の設定例

Power over Ethernet 情報の表示：例

次に、特定のアクセス ポイントの PoE 設定を含む共通の情報を表示する例を示します。

```
スイッチ# show ap name AP01 config general

Cisco AP Identifier.............. 1
Cisco AP Name.................... AP1
...
PoE Pre-Standard Switch.......... Enabled
PoE Power Injector MAC Addr...... Disabled
Power Type/Mode.................. PoE/Low Power (degraded mode)
...
```

第 VII 部

Mobility

- モビリティについて，627 ページ
- モビリティ ネットワーク要素，633 ページ
- モビリティ制御プロトコル，637 ページ
- モビリティの設定，645 ページ

第 38 章

モビリティについて

- 概要，627 ページ
- 有線およびワイヤレス モビリティ，628 ページ
- モビリティの機能，628 ページ
- 低遅延ローミングを実現するスティッキ アンカリング，630 ページ
- ブリッジ ドメイン ID および L2/L3 ローミング，631 ページ
- リンク ダウンの動作，631 ページ
- モビリティ コントローラのプラットフォーム固有のスケール要件，631 ページ

概要

スイッチは、単に速度やフィードの増加をもたらすだけではなく、アクセス レイヤでより多くのサービスを提供します。ワイヤレス サービスはスイッチと統合され、アクセス レイヤ スイッチがワイヤレス ユーザのデータ プレーンの終端となります。これにより、シスコのユニファイド アーキテクチャを実現できます。統合とは、モビリティ サービスがワイヤレスと有線の両方のステーションに提供されることを意味します。

スイッチは、シームレスなローミングを提供します。これには、クライアントに対するネットワーク構成と展開オプションの透過性が必要です。

エンド ユーザの観点からすれば、どのモビリティ イベントも IP アドレス、デフォルト ルータ、または DHCP サーバを変更することはできません。これは、ステーションがローミングするときに、次のことができるようにする必要があることを意味します。

- デフォルト ルータに ARP を送信します。
- 以前にアドレスを割り当てているサーバに DHCP 要求を送信します。

インフラストラクチャの観点からすれば、モビリティ イベントが発生した場合、ステーションのトラフィックは現在の接続ポイントに従う必要があります。これは、モビリティ エージェント（MA）またはモビリティ コントローラ（MC）のどちらかです。これは、ステーションが異なる

サブネットに設定されたネットワークに移動したかどうかに関係なく当てはまります。ステーションがモビリティ イベント後にトラフィックを受信しない期間は、可能な限り短くする必要があります（できれば 40 ms 以下）。これには、必要な認証手順も含まれます。

インフラストラクチャの観点からすれば、モビリティ管理ソリューションには 4 つの主要なコンポーネントが必要です。これらの機能はすべて、ローミングの制約の範囲内で実行する必要があります。

- 最初のアソシエーション：この機能は、ネットワーク内でユーザの新しい接続ポイントを識別するために使用されます。
- コンテキストの転送：この機能は、ステーションに関連するステート情報を転送するために使用されます。これにより、セキュリティおよびアプリケーション ACL やサービスなど、ステーションの静的なリアルタイム ポリシーがハンドオフ全体にわたって等しく保たれるようにします。
- ハンドオフ：この機能は、ステーションの接続ポイントが変更され、以前のアクセス スイッチによってステーションの制御が放棄される必要があることを示すために使用されます。
- データ プレーン：通常、この機能はハンドオフ プロセスに関連しており、パフォーマンスを著しく低下させずにステーションのトラフィックがステーションから引き続き提供および受信されるようにします。

注意 ワイヤレス管理インターフェイス VLAN において Virtual Routing and Forwarding（VRF）を設定した場合は、モビリティ機能は正常に動作しない可能性があります。

有線およびワイヤレス モビリティ

統合アクセス ソリューションの主な機能の 1 つ（Cisco Catalyst 3850 スイッチと Cisco WLC 5700 シリーズ コントローラの両方に適用）は、イーサネット接続からワイヤレスへ（逆も同様）のモビリティ イベント全体にわたり、デバイスにIPアドレスを設定し、セッションの持続性を維持する機能です。この機能により、ユーザはイーサネット ネットワークに可能な限りとどまり、必要に応じてワイヤレス モビリティを自由に使用できます。

この機能は、クライアントとインフラストラクチャの両方のサポートを活用し、2 要素認証（デバイスとユーザ）を使用します。デバイス認証クレデンシャルは、モビリティ コントローラ（MC）でキャッシュされます。デバイスがリンク層間を移行し、デバイス クレデンシャルの検証で一致が見つかった場合、MC は同じ IP アドレスが新しいインターフェイスに割り当てられるようにします。

モビリティの機能

- モビリティ コントローラ（MC）：コントローラは、ピア グループ間のローミング イベントに対するモビリティ管理サービスを提供します。MCは、RADIUSなどの管理およびポリシー

ベースの制御プロトコルに単一の窓口を提供します。これにより、ネットワーク全体にわたって移行するユーザの位置をインフラストラクチャ サーバが維持する必要性がなくなります。MC は、サブドメイン内のすべてのモビリティ エージェントに、モビリティ設定、ピア グループ メンバーシップ、およびメンバーのリストを送信します。サブドメインは、それを形成する MC と同義です。各サブ ドメインは、MC、および AP が関連付けられたアクセス スイッチ（0 台以上）で構成されます。

- モビリティ エージェント（MA）：モビリティ エージェントは、ワイヤレス モジュールを実行しているアクセス スイッチ、または内部 MA を実行している MC です。モビリティ エージェントは、MA を実行しているデバイスに AP を介して接続されたモバイル クライアント用のクライアント モビリティ ステート マシンを維持するワイヤレス コンポーネントです。
- モビリティ サブドメイン：モビリティ ドメイン ネットワークの自律部分です。モビリティ サブドメインは、単一のモビリティ コントローラおよび関連するモビリティ エージェント（MA）で構成されます。

（注） 複数のモビリティ コントローラが存在する場合でも、1 台の MC だけを常にアクティブにできます。

モビリティ サブドメインは、アクティブなモビリティ コントローラにより管理されるデバイスのセットです。モビリティ サブドメインは、一連のモビリティ エージェントおよび関連するアクセス ポイントで構成されます。

- モビリティ グループ：高速ローミングがサポートされるモビリティ コントローラ（MC）の集まりです。モビリティ グループの概念は、頻繁な移動が必要なキャンパス内の建物の集まりと同じです。
- モビリティ ドメイン：モビリティがサポートされるモビリティ サブドメインの集まりです。モビリティ ドメインという用語は、キャンパス ネットワークと同じ意味合いがあります。
- Mobility Oracle （MO）：Mobility Oracle は、モビリティ サブドメインで発生するモビリティ イベントの窓口として機能します。また、モビリティ ドメイン全体、ホーム、および現在のサブドメインにある各ステーションのローカル データベースを維持します。モビリティ ドメインには 1 つ以上の Mobility Oracle が含まれますが、常にアクティブなのは 1 つだけです。
- モビリティ トンネル エンドポイント（MTE）：モビリティ トンネル エンドポイント（MTE）は、トンネリングを使用してモバイル デバイスにデータ プレーン サービスを提供します。これにより、ネットワーク上のユーザの Point of Presence を一定に保ち、ローミング イベントのネットワークへの影響を最小化します。
- 接続ポイント：ステーションの接続ポイントは、ネットワークへの接続時にデータ パスが最初に処理される場所です。これは、現在サービスを提供しているアクセス スイッチ、またはワイヤレス LAN コントローラになります。
- Point of Presence：ステーションの Point of Presence は、ステーションがアドバタイズされているネットワーク内の場所です。たとえば、アクセス スイッチがルーティング プロトコルを介してステーションへ到達可能性をアドバタイズしている場合、ルートがアドバタイズされているインターフェイスはステーションの Point of Presence と見なされます。

- スイッチ ピア グループ（SPG）：ピア グループは、高速モビリティ サービスが提供される隣接アクセス スイッチの静的に作成されたリストです。ピア グループは、ハンドオフ中のスイッチ間のインタラクションの範囲を地理的に近いものだけに限定します。
- ステーション：ネットワークに接続し、ネットワークからサービスを要求するユーザデバイス。デバイスには、有線、ワイヤレス、またはその両方のインターフェイスがあります。
- 同じ SPG 内のスイッチ：ローカル スイッチのピア グループに属するピア スイッチ。
- SPG 外のスイッチ：ローカル スイッチのピア グループに属さないピア アクセス スイッチ。
- 外部モビリティ コントローラ：外部モビリティ サブドメインのステーションにモビリティ管理サービスを提供するモビリティ コントローラ。外部モビリティ コントローラは、外部サブドメインのアクセス スイッチとホーム ドメインのモビリティ コントローラ間の連絡窓口として機能します。
- 外部モビリティ サブドメイン：モビリティ コントローラで制御され、別のモビリティ サブドメインに固定されたステーションをサポートするモビリティ サブドメイン
- 外部スイッチ：現在ステーションにサービスを提供している外部モビリティ サブドメインのアクセス スイッチ。
- アンカー モビリティ コントローラ：ホーム モビリティ サブドメインでステーションの制御およびモビリティ管理サービスを一元化するモビリティ コントローラ。
- アンカー モビリティ サブドメイン：モビリティ コントローラによって制御される、IP アドレスが割り当てられたステーションのモビリティ サブドメイン。
- アンカー スイッチ：ステーションに最後にサービスを提供したホーム モビリティ サブドメインのスイッチ。

低遅延ローミングを実現するスティッキ アンカリング

スティッキ アンカリングにより、クライアントが最初にネットワークに参加するスイッチにおいて、クライアントの Point of Presence からのローミングの遅延を低く保つことができます。クライアントをローミングするためにクライアントのポリシーをスイッチに適用するのはコストがかかります。ダウンロード可能な ACL を AAA サーバに問い合わせる必要があるため、大幅な遅延が生じる可能性があります。これは、時間的制約のあるクライアント トラフィックを復元するのにはふさわしくありません。

この遅延を管理するため、異なるスイッチに接続された AP 間でクライアントがローミングを行うときに、クライアント トラフィックはクライアントが最初にアソシエートするスイッチに常にトンネル経由で送信されます。サブドメイン内のローミングであるか、サブドメイン間のローミングであるかは関係ありません。クライアントは、ネットワークの初期接続ポイントにずっと固定されます。

この動作はデフォルトでイネーブルにされています。サブネット間のローミングにのみクライアント アンカリングを許可するには、この動作をディセーブルにできます。これは、WLAN コンフィギュレーションごとに設定され、WLANコンフィギュレーションモードで使用できます。お

客様は、時間的制約のあるアプリケーションとそうでないアプリーションそれぞれに、異なる SSID を設定できます。

ブリッジ ドメイン ID および L2/L3 ローミング

ブリッジ ドメイン ID は、特定のローミング タイプ（L2 または L3）を選択するための情報をモビリティ ノードに提供します。また、ネットワーク管理者はネットワーク配信全体で VLAN ID を再使用できるようになります。VLAN ID に関連付けられたサブネット設定がない場合、VLAN ID と共に追加パラメータの使用が必要になる可能性があります。ネットワーク管理者は、同じブリッジ ドメイン ID の特定の VLAN が一意のサブネットに関連付けられていることを確認します。まず、モバイル ノードは、そのノードのブリッジ ドメイン ID およびクライアントに関連付けられた VLAN ID を確認して、ローミング タイプを特定します。L2 ローミングとして処理するには、ブリッジ ドメイン ID と VLAN ID が同じである必要があります。

SPG とその後の MC の作成時に、各 SPG にブリッジ ドメイン ID が設定されます。複数の SPG で同じブリッジ ドメイン ID を使用できます。また、SPG 内のすべての MA は同じブリッジ ドメイン ID を共有します。この情報は、設定のダウンロードの一部として MA が最初に起動したときに MA へプッシュされます。システムの起動時にブリッジ ドメイン ID が変更された場合、変更された SPG 内のすべての MA にプッシュされ、次のローミングですぐに有効になります。

リンク ダウンの動作

ここでは、冗長マネージャがなく、MC や MO でダウンタイムが発生した場合の MA-MC および MC-MO 間のデータ同期に関する情報を提供します。MA-MC または MC-MO 間でキープアライブが設定されている場合、クライアントのデータベースは MO とその MC および MC とその MA の間で同期されます。

モビリティ コントローラのプラットフォーム固有のスケール要件

モビリティ コントローラ（MC）のロールは、Cisco WLC 5700 シリーズ、CUWN および Catalyst 3850 スイッチなど、さまざまなプラットフォームでサポートされています。次の表に、これら 3 つのプラットフォームのスケール要件の概要を示します。

拡張性	MC としての Catalyst 3850	MC としての Catalyst 3650	MC としての Cisco WLC 5700	MC としての CUWN 5508	MC としての WiSM2
モビリティ ドメイン内の MC の最大数	8	8	72	72	72
モビリティ グループ内の MC の最大数	8	8	24	24	24

拡張性	MC としての Catalyst 3850	MC としての Catalyst 3650	MC としての Cisco WLC 5700	MC としての CUWN 5508	MC としての WiSM2
サブドメイン内の MA の最大数（MC ごと）	16	16	350	350	350
サブドメイン内の SPG の最大数（MC ごと）	8	8	24	24	24
SPG 内の MA の最大数	16	16	64	64	64

第 39 章

モビリティ ネットワーク要素

- Mobility Agent，633 ページ
- モビリティ コントローラ，634 ページ
- Mobility Oracle，635 ページ
- ゲスト コントローラ，636 ページ

Mobility Agent

モビリティコントローラはスイッチに配置されます。モビリティコントローラは、制御パスおよびデータ パスのエンティティであり、次の処理を実行します。

- スイッチ上でのモビリティ イベントの処理
- モビリティ用スイッチのデータ パス要素の設定
- モビリティ コントローラとの通信

スイッチは、ワイヤレス ステーションで 802.11 トラフィックをカプセル化する CAPWAP トンネルを終端することにより、MA としてデータ パス機能を実行します。

これにより、スイッチは有線およびワイヤレス トラフィックに機能を均等に適用できます。スイッチに関する限り、802.11 は単なる別のアクセス メディアです。

MA では次の機能が実行されます。

- モビリティ プロトコルのサポート：MA のタイムリーな対応により、スイッチがローミング バジェットを達成できるようにします。
- Point of Presence：ワイヤレス サブネットが MC で使用できず、ワイヤレス クライアント VLAN が新しい接続ポイントで使用できない場合、MA が Point of Presence を引き継ぎ、クライアント トラフィックをトンネル経由で送信します。
- ARP サーバ：ネットワークがレイヤ 2 モードで設定されている場合、MA が接続されているステーションの到達可能性をアドバタイズします。トンネリングを使用する場合、ステー

ションのために ARP 要求がトンネル経由で送信されます。ここで、Point of Presence（アンカー スイッチ）がアップリンク インターフェイスへブリッジします。

- プロキシ IGMP：スイッチ上の MA が、ローミング イベントの発生後、ステーションのためにマルチキャスト グループへの登録を行います。この情報は、新しいスイッチへコンテキストの一部として渡されます。これにより、ローミング時にマルチキャスト フローがユーザを追跡します。
- ルーティング：スイッチがレイヤ 3 アクセス ネットワークに接続されている場合、MA はトンネリングが提供されていない関連付けられたステーションのルートをインジェクトします。
- 802.1X オーセンティケータ：オーセンティケータ機能は MA に含まれており、有線およびワイヤレスのステーションを処理します。
- セキュアな PMK の共有：ステーションがネットワークに正常に認証されると、MA は PMK を MC に転送します。MC は、サブドメインに属するすべての MA、およびモビリティ グループのピア MC へ PMK をフラッディングします。

MA では次のデータ パス機能も実行されます。

- モビリティ トンネル：トンネリングの使用時に、アクセス スイッチが Point of Presence として機能している場合、MA はモビリティ トンネルから MC へのパケット、さらにピア グループ内の他の MA へのパケットをカプセル化および非カプセル化します。MA は、接続ポイント間のクライアント データ トラフィックのトンネリングをサポートします。他のスイッチに使用するパケット形式は CAPWAP（802.3 ペイロードと併用）です。MA は、モビリティ トンネルの再構成およびフラグメンテーションもサポートします。
- 暗号化：モビリティ ノード間のモビリティ制御トラフィックは暗号化された DTLS です。MA は、接続ポイントで CAPWAP 制御とデータ（任意）も暗号化します。
- CAPWAP：スイッチは、CAPWAP 制御とデータ プレーンをサポートします。スイッチ転送ロジックは、CAPWAP トンネルを 802.11 および 802.3 のペイロードと終端させます。大きなフレーム（1500 バイト以上）のサポートは一般的に使用できないため、スイッチが CAPWAP フラグメンテーションと再構成をサポートします。

モビリティ コントローラ

モビリティ コントローラの主な機能は、スイッチ ピア グループの範囲外のクライアント ローミングを調整することです。モビリティ コントローラのその他の機能は次のとおりです。

- ステーション データベース：モビリティ コントローラはローカル モビリティ サブドメイン内で接続されたすべてのクライアントのデータベースを維持します。
- モビリティ プロトコル：MC はモビリティ プロトコルをサポートします。これにより、対象ローミング ポイントが迅速に応答し、150 ms というローミング バジェットを達成できます。
- Mobility Oracle へのインターフェイス：モビリティ コントローラは、スイッチと Mobility Oracle 間のゲートウェイとして機能します。モビリティ コントローラがローカル データベー

スで一致を見つけられない場合、ワイヤレス クライアント エントリの一致（データベース内）を提案し、モビリティ ドメインを管理する Mobility Oracle に要求を転送します。

（注） Mobility Oracle の機能は、プラットフォームでサポートされている場合にのみ MC でイネーブルにできます。

- ARP サーバ：ステーションに対してトンネリングを使用する場合、ネットワーク上の Point of Presence はモビリティ トンネル エンドポイント（MTE）です。モビリティ コントローラは、担当するステーションで受信する ARP 要求に応答します。
- ルーティング：モビリティ コントローラがレイヤ 3 ネットワークに接続されている場合、モビリティ コントローラはサポートするステーションのルートをネットワークへインジェクトする必要があります。
- MTE の設定：モビリティ コントローラは、すべてのモビリティ管理関連の要求においてスイッチのコントロール ポイントです。ステーションの接続ポイントで変更が発生すると、モビリティ コントローラは MTE の転送ポリシーを設定します。
- NTP サーバ：モビリティ コントローラは、スイッチに対して NTP サーバとして機能し、クロックを同期化するようにすべてのノードをサポートします。

（注） デフォルトでイネーブルにされたモビリティ コントローラ機能を持つ Cisco 5700 シリーズ WLC および他のコントローラ プラットフォームは、スイッチ ピア グループ（SPG）に追加できません。

Mobility Oracle

Mobility Oracle は必要に応じてサブドメインを越えたクライアントのローミングを調整します。次の機能で構成されます。

- ステーション データベース：Mobility Oracle はモビリティ ドメイン内でサービスが提供されているすべてのステーションのデータベースを維持します。このデータベースは、サポートするモビリティ サブドメインすべてにおいて、Mobility Oracle とすべてのモビリティ コントローラとのインタラクション時に入力されます。
- モビリティ コントローラへのインターフェイス：Mobility Oracle がモビリティ コントローラから要求を受信すると、ステーションの検索を実行し、必要に応じてモビリティ コントローラへ要求を転送します。
- NTP サーバ：Mobility Oracle はモビリティ コントローラに対する NTP サーバとして機能し、モビリティ ドメイン内のすべてのスイッチのクロックを同期します。

ゲスト コントローラ

ゲスト アクセス機能により、ワイヤレス クライアントへのゲスト アクセスが可能になります。ゲスト トンネルはモビリティ トンネルと同じ形式を使用します。ゲスト アクセス機能を使用すれば、アクセス スイッチ上でゲストVLANを設定する必要はありません。有線およびワイヤレス クライアントからのトラフィックは、ゲストコントローラで終端します。ゲストVLANがアクセス スイッチに存在しないため、トラフィックは既存のモビリティトンネルを介して、さらにゲスト コントローラへのゲスト トンネルを介して、MTE に送信されます。

このアプローチの利点は、ゲスト コントローラにトンネル経由で送信される前に、すべてのゲスト トラフィックが MTE を通過することです。ゲスト コントローラは、自身とすべての MTE 間のトンネルだけをサポートする必要があります。

このアプローチの欠点は、ゲスト クライアントからのトラフィックが 2 回トンネル経由で送信されることです。最初は MTE に、さらにゲスト コントローラにトンネル経由で送信されます。

ゲストコントローラではローミングがサポートされていないため、クライアントはゲストコントローラへローミングできません。この制限は、IOS-XEのゲストアンカーのみに適用され、AireOSへは適用されません。

第 40 章

モビリティ制御プロトコル

- モビリティ制御プロトコルについて，637 ページ
- 最初のアソシエーションとローミング，637 ページ
- 最初のアソシエーション，638 ページ
- スイッチ内のハンドオフ，640 ページ
- スイッチ ピア グループ内のハンドオフ，640 ページ
- スイッチ ピア グループ間のハンドオフ，641 ページ
- サブ ドメイン間のハンドオフ，642 ページ
- モビリティ グループ間のハンドオフ，643 ページ

モビリティ制御プロトコルについて

モビリティ制御プロトコルは、トンネル型とルーティング型のどちらでも使用されます。モビリティ制御プロトコルは、MO、MC、および MA 間のモビリティ イベントに使用されます。

モビリティ アーキテクチャは、次の両方のアプローチを使用します。

- 各 SPG 内のスイッチとの直接通信を使用した分散型アプローチ
- MC と MO を使用した集中型アプローチ

この目的は、スイッチ間のインタラクションを制限してシステム全体を拡張しつつ、集中化された MC 上でオーバーヘッドを削減することです。

最初のアソシエーションとローミング

次のシナリオは、モビリティ管理プロトコルに適用されます。

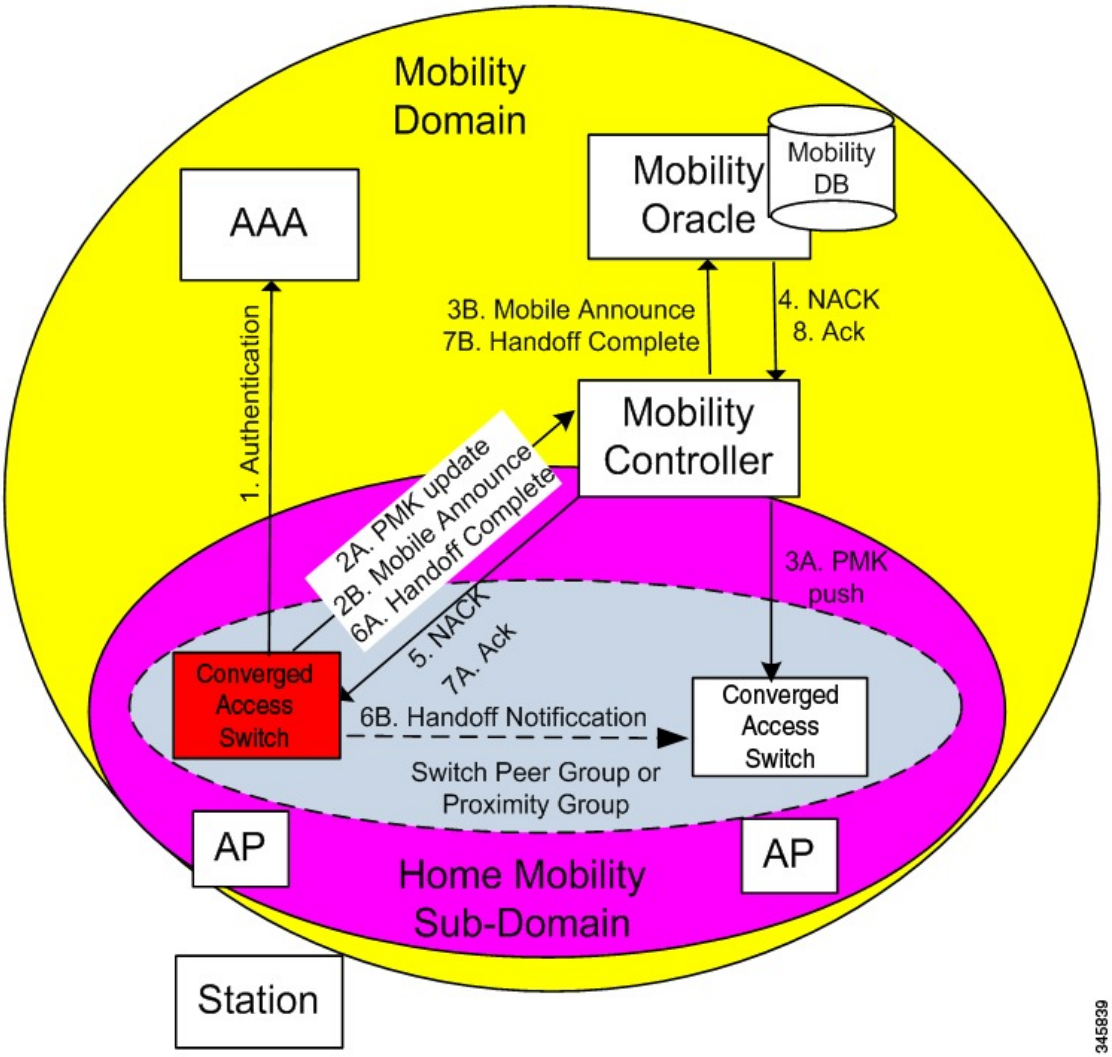
- 最初のアソシエーション

- スイッチ内のローミング
- スイッチ ピア グループ内のローミング
- スイッチ ピア グループ間のローミング
- サブドメイン間のローミング
- グループ間のローミング

最初のアソシエーション

次の図では、最初のアソシエーション プロセスとそれに続くスイッチについて説明します。

図 *38*：最初のアソシエーション



1 ステーションがモビリティ エージェントに最初に関連付けられると、MA は検索を実行して、キー キャッシングのキーイング情報を MA でローカルに入手できるかどうか判断します。キーイング情報が入手できない場合、つまりステーションがネットワークに最初に表示される場合、スイッチはデバイスに自身を認証して、Pairwise Master Key（PMK）を生成するように求めます。PMK はクライアントと RADIUS サーバ側で生成され、RADIUS サーバはオーセンティケータである MA に PMK を転送します。

2 MA は MC に PMK を送信します。

3 MA から PMK を受け取ると、MC はサブドメイン内のすべての MA、およびモビリティ グループ内の他のすべての MC に PMK を送信します。

4 モビリティ グループは、単一キー ドメインです。これにより、802.11r に対応するステーションはキー ドメインを認識し、802.11r で定義された高速移行手順の使用を試みます。

（注） 802.11r プロトコルは、キーイング情報を共有するアクセス ポイントの集まりであるキー ドメインを定義します。

5 （図のステップ 2B を参照）PMK が MA のローカル キー キャッシュ内に存在しないという事実が示すように、ステーションはモビリティ サブドメインにとって新しいため、MA は MC にモバイル通知メッセージを送信します。

6 MC は、クライアントがデータベース内に存在するかどうかを確認します。クライアントが検出されない場合、MC は MO に転送します（可能な場合）。

7 （図のステップ 5 を参照）ステーションがネットワークにとって新しいため、MO は否定応答（NACK）を返します。これは、MC によりスイッチへ転送されます。Mobility Oracle が使用できない場合、モバイル通知への応答がない原因は MC にあります。

8 スイッチの MA は、Handoff Complete メッセージにより、ステーションの新しい接続ポイントについて MC に通知します。

9 MA は、Handoff Notification メッセージによって、ステーションの新しい接続ポイントについてスイッチ ピア グループ（SPG）内の他の MA に通知します。MC とやり取りすることなくローカル ハンドオフを可能にするには、SPG 内の MA にこの通知を送信する必要があります。SPG 内の MA に送信された Handoff Notification メッセージで、MC に送信された Handoff Complete メッセージ内のすべての情報を伝える必要はありません。

10 （図のステップ 7B を参照）MC はデータベースを更新し、Mobility Oracle に Handoff Complete メッセージを転送します。これにより、Mobility Oracle のデータベースが更新され、ステーションの現在のホーム モビリティ サブドメインが記録されます。

スイッチ全体にわたり迅速に移動するデバイスにより発生する競合状態を解消するため、モビリティ サブドメイン内に存在するかどうかに関係なく、MA と MC/MO 間のメッセージは時間同期されます。これにより、受信した要求に異常があったとしても、MC と MO はそれらの要求を適切に処理できます。

SPG 内の MA に送信された Handoff Notification は認識されません。

スイッチ内のハンドオフ

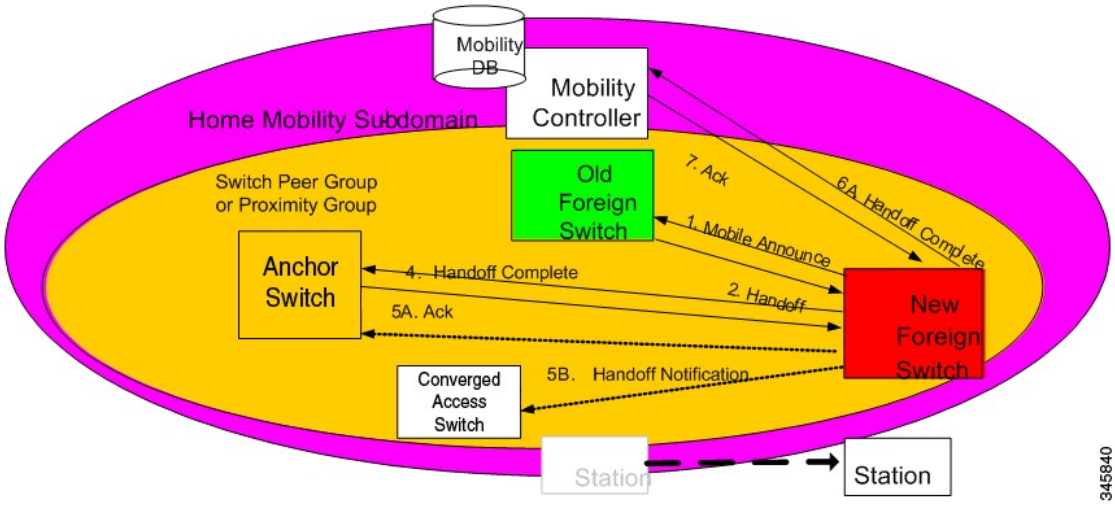
MA 内のモビリティ イベントは SPG と MC に対して完全に透過的です。ステーションが同じ MA の AP 間を移動して、迅速なハンドオフの実行を試みる場合、PMK は MA 上にあります。MA はその他の信号を呼び出すことなく迅速なハンドオフを完了します。

スイッチ ピア グループ内のハンドオフ

スイッチ ピア グループ（SPG）とは、ユーザがローミングを行う MA のグループのことで、高速ローミング サービスを提供します。SPG 内で MA が直接ハンドオフを実行することにより、必要な交換メッセージの数が少なくなり、MC のオーバーヘッドが減少します。

最初のアソシエーションが完了すると、ステーションはその SPG に属する別の MA に移動します。スイッチ ピア グループ内のローミングでは、最初のアソシエーション、ステーション PMK はモビリティ サブドメイン内のすべての MA に転送されています。

図 *39*：スイッチ ピア グループ内のハンドオフ



次のプロセスでは、スイッチ ピア グループ内のハンドオフについて説明します。

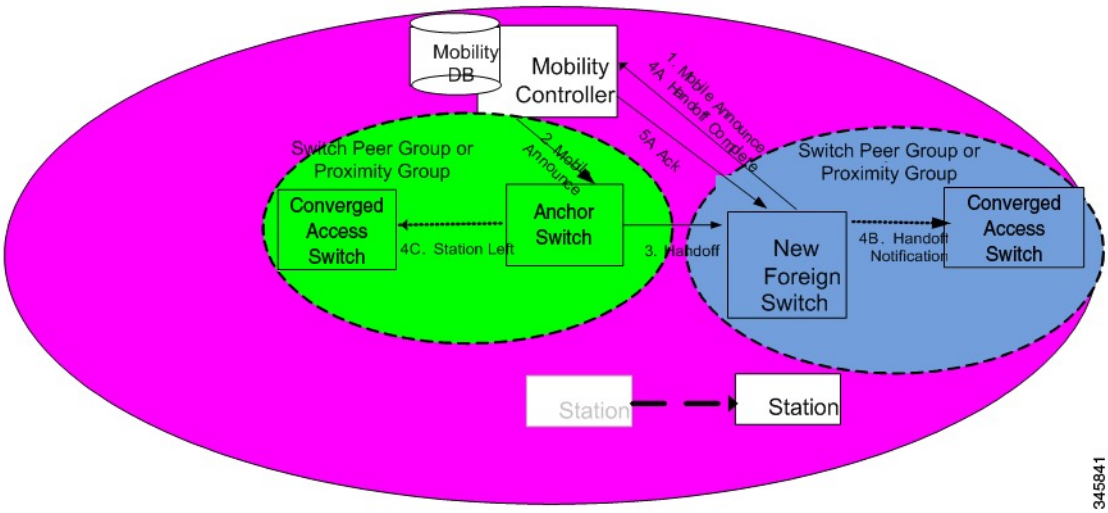
1. 最初のアソシエーションの例では、ステーションの現在の接続ポイントを確認するために、Handoff Notification メッセージがすべての MA に送信されます。
2. 新しい MA は、クライアントが関連付けられた以前の MA にユニキャスト モバイル通知メッセージを送信します。
3. ハンドオフが完了したら、新しい MA は MC へ Handoff Complete メッセージを送信します。
4. 新しいスイッチは、同じ SPG 内のすべての MA に Handoff Notification を送信して、クライアントの新しい Point of Presence について通知します。

スイッチ ピア グループ間のハンドオフ

SPG 内ローミングは、考えられるすべてのシナリオをカバーしているわけではありません。同じ SPG に存在しない 2 つの MA 間でモビリティ イベントが発生する可能性があります。

ネットワーク内での Handoff Notification メッセージの紛失や新しい SPG に存在しない MA へのステーションのローミングなどの理由により、MA にステーションの現在の接続ポイントに関する情報がない場合、MA は MC を参照します。MC は、モビリティ サブドメイン内のクライアントの Point of Presence に関する情報を提供します。これにより、モビリティ サブドメイン内の他の MC すべてを参照せずに済みます。

図 *40*：スイッチ ピア グループ間のハンドオフ



上記の図は、同じ SPG ではなく、同じモビリティ サブドメインに存在する MA で発生するモビリティ イベントの例を示します。

（注） MA の色は SPG を表す円と一致します。

1. 新しい MA には、クライアントの初期認証時にモビリティ サブドメインの各 MA に転送されたステーションの PMK があります。
2. MA は内部の隣接する MA にあるステーションの存在を前もって通知されていなかったため、別の SPG がサブドメインの MC へモバイル通知を送信します。
3. （図のステップ 2 を参照）モバイル通知メッセージを受信すると、MC はデータベース内で検索を実行し、以前にステーションにサービスを提供していた MA へ要求を転送します。この情報は、信頼性の高い方法で古い MA から送信された Handoff Complete メッセージにより、MC に通知されます。
4. （図のステップ 3 を参照）上の緑色で示されている古い MA は、新しい MA へハンドオフ メッセージを直接送信します。

5 古い MA は、Station Left メッセージを使用して、ステーションがグループを離れたことを SPG 内の他の MA に通知する必要があります。これにより、ステーションが MA の 1 つに戻ったとしても、古い MA はもはやサービスをステーションに提供しないことを MA は認識できます。

6 ハンドオフが完了すると、新しい MA は信頼性の高い方法で MC に Handoff Complete メッセージを送信します。

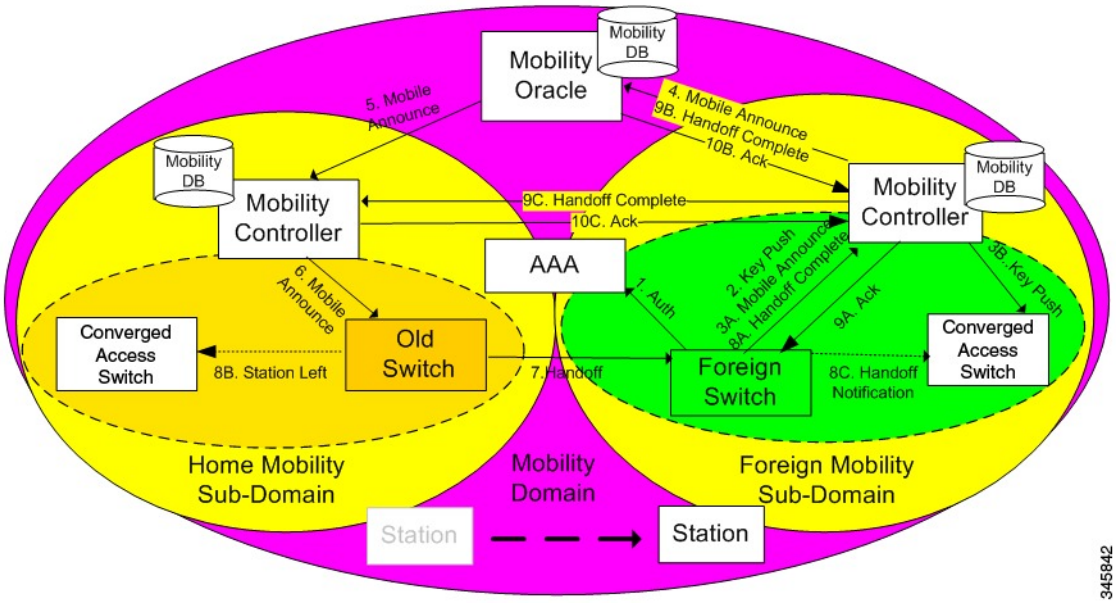
7 新しい MA は SPG 内の他の MA に Handoff Notification を送信します。

サブ ドメイン間のハンドオフ

サブドメインは、モビリティ コントローラとそのモビリティ コントローラが直接管理するモビリティ エージェントによって形成される集合体です。サブドメイン間のモビリティ イベントは、2 台のモビリティ コントローラ間の通信を意味しています。これら 2 台のモビリティ コントローラは、同じモビリティ グループ値で設定され、相互に認識できます。これらは互いのモビリティ リストに表示されます。また、異なるモビリティ グループ値で設定しても、相互に認識できます。

同じモビリティ グループの MC 間のサブドメインでローミング イベントが発生した場合、新しい AP によりアドバタイズされる 802.11r キー ドメインは同じです。また、クライアントの初期認証時には、クライアントの PMK もすべての MC へ送信されます。新しい MC はクライアントに再認証を強制する必要がありません。また、新しい MC は、以前の MC のうちどれがワイヤレス クライアント モビリティを管理しているかも認識します。

図 *41*：サブ ドメイン間のハンドオフ



次の手順は、モビリティ コントローラが同じモビリティ グループに属している場合のサブ ドメイン間のハンドオフに関するものです。

1. 最初の MA によりクライアントの PMK がモビリティ グループのすべての MC へ送信されたときに、新しい MA は MC からクライアントの PMK をすでに受信したため、再認証は必要ではありません。
2. 新しい MA は、サブドメインの MC へモバイル通知を送信する別の SPG 内で、隣接する MA にあるステーションの存在を前もって通知されていませんでした。
3. モバイル通知メッセージを受信すると、MC はモバイル通知を MO へ転送します。MO はデータベース内で検索を実行して、以前にステーションにサービスを提供していた MC へ要求を転送します。
4. 以前の MC は、ステーションにサービスを提供していた MA へその要求を転送します。
5. 黄色で示されている古い MA は、新しい MA へハンドオフ メッセージを直接送信します。
6. 古い MA は、Station Left メッセージを使用して、ステーションが SPG を離れたことを、SPG 内の他の MA に通知する必要があります。これにより、ステーションが MA の 1 つに戻った場合に、古い MA はもはやサービスをステーションに提供しないことを MA は認識できます。
7. ハンドオフが完了すると、新しい MA は信頼性の高い方法で新しいモビリティ コントローラに Handoff Complete メッセージを送信します。
8. 新しい MA は他のすべての MA に Handoff Notification を送信します。
9. 新しい MC は、古い MC に Handoff Complete を送信します。

モビリティ グループ間のハンドオフ

モビリティ グループは、同じモビリティ グループ名を共有し、相互に認識する MC により形成されます。

ローミング イベントはモビリティ グループ全体で発生するため、新しい AP によってアドバタイズされる 802.11r キー ドメインは異なります。結果として、クライアントは再認証を行う必要があります。MC はモビリティ グループ内でのみ伝搬されます。また、モビリティ グループ間のローミングでは、ステーションがモビリティ グループの境界を越える際に、ステーションの再認証が必要です。認証が完了すると、生成される PMK は同じモビリティ グループ内の MA および MC にプッシュされます。各 PMK は特定のサブドメイン（802.11y キー ドメイン）に関連付けられているため、ステーションは以前のサブドメインから PMK をキャッシュします。これにより、PMK キャッシュ タイムアウト インターバル内に PMK が以前のサブドメインへローミングで戻る場合、再認証を行う必要がなくなります。残りの手順は、サブドメイン間のハンドオフのステップと同じです（ただし、これらのステップはモビリティ グループ間のローミングに関連しています）。

第 41 章

モビリティの設定

- モビリティ コントローラの設定，645 ページ
- モビリティ エージェントの設定，653 ページ
- モビリティ エージェントを管理するモビリティ コントローラ，656 ページ

モビリティ コントローラの設定

統合アクセス コントローラの設定

ピア グループ、ピア グループ メンバー、ブリッジ ドメイン ID の作成（CLI）

はじめる前に

- モビリティ エージェントでは、モビリティ コントローラの IP アドレスだけを設定できます。
- モビリティ コントローラでは、各ピア グループ メンバーのピア グループおよび IP アドレスを定義できます。

手順の概要

1. **wireless mobility controller**
2. **wireless mobility controller peer-group***SPG1*
3. **wireless mobility controller peer-group***SPG1***member ip***member-ip-addr***public-ip***public-ip-addr*
4. **wireless mobility controller peer-group***SPG1***member ip***member-ip-addr***public-ip***public-ip-addr*
5. **wireless mobility controller peer-group***SPG2*
6. **wireless mobility controller peer-group***SPG2***member ip***member-ip-addr***public-ip***public-ip-addr*
7. **wireless mobility controller peer-group***SPG1***bridge-domain-id***id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility controller** 例： スイッチ(config)# **wireless mobility controller**	デバイスのモビリティ コントローラ機能をイネーブルにします。このコマンドはスイッチだけに適用されます。デフォルトのコントローラはモビリティ コントローラです。
ステップ 2	**wireless mobility controller peer-group***SPG1* 例： スイッチ(config)# **wireless mobility controller peer-group SPG1**	SPG1 という名前のピア グループが作成されます。
ステップ 3	**wireless mobility controller peer-group***SPG1***member ip***member-ip-addr***public-ip***public-ip-addr* 例： スイッチ(config)# **wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip 10.10.20.2**	ピア グループにモビリティ エージェントを追加します。 （注） 10.10.20.2 は、モビリティ エージェントの直接 IP アドレスです。NAT を使用する場合、任意のパブリック IP アドレスを使用して、モビリティ エージェントの NATed アドレスを入力します。NAT を使用しない場合、パブリック IP アドレスは使用されず、デバイスはモビリティ エージェントの直接 IP アドレスを表示します。
ステップ 4	**wireless mobility controller peer-group***SPG1***member ip***member-ip-addr***public-ip***public-ip-addr* 例： スイッチ(config)# **wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip 10.10.20.6**	ピア グループ SPG1 に別のメンバーを追加します。
ステップ 5	**wireless mobility controller peer-group***SPG2* 例： スイッチ(config)# **wireless mobility controller peer-group SPG2**	別のピア グループ SPG2 を作成します。
ステップ 6	**wireless mobility controller peer-group***SPG2***member ip***member-ip-addr***public-ip***public-ip-addr* 例： スイッチ(config)# **wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip 10.10.10.20**	ピア グループ SPG2 にメンバーを追加します。

	コマンドまたはアクション	目的
ステップ 7	**wireless mobility controller peer-group***SPG1***bridge-domain-id***id* 例： スイッチ(config)# **wireless mobility controller peer-group SPG1 bridge-domain-id 54**	（任意）他の SPG でサブネット VLAN マッピングを定義するために使用される SPG1 にブリッジ ドメインを追加します。

次に、ピア グループを作成し、メンバーを追加する例を示します。

```
スイッチ(config)# wireless mobility controller
スイッチ(config)# wireless mobility controller peer-group SPG1
スイッチ(config)# wireless mobility controller peer-group SPG1
スイッチ(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip
 10.10.20.2
スイッチ(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip
 10.10.20.6
スイッチ(config)# wireless mobility controller peer-group SPG2
スイッチ(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip
 10.10.10.20
スイッチ(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54
```

ローカル モビリティ グループの設定（CLI）

モビリティ グループが MC のグループである場合の、ワイヤレス モビリティ グループとモビリティ グループ メンバーの設定。

はじめる前に

MC は 1 つのグループだけに所属できますが、複数のモビリティ グループ内の MC を認識できます。

手順の概要

1. **wireless mobility group name***group-name*
2. **wireless mobility group member ip***member-ip-addr***public-ip***public-ip-addr*
3. **wireless mobility group keepalive interval***time-in-seconds*
4. **wireless mobility group keepalive count***count*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility group name***group-name* 例： スイッチ(config)# **wireless mobility group name Mygroup**	Mygroup という名前のモビリティ グループを作成します。
ステップ 2	**wireless mobility group member ip***member-ip-addr***public-ip***public-ip-addr* 例： スイッチ(config)# **wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28**	Mygroup モビリティ グループにモビリティ コントローラを追加します。 （注） NAT を使用する場合、任意のパブリック IP アドレスを使用して、モビリティ コントローラの NATed IP アドレスを入力します。
ステップ 3	**wireless mobility group keepalive interval***time-in-seconds* 例： スイッチ(config)# **wireless mobility group keepalive interval 5**	モビリティ メンバーに送信される 2 つのキープアライブの間隔を設定します。
ステップ 4	**wireless mobility group keepalive count***count* 例： スイッチ(config)# **wireless mobility group keepalive count 3**	メンバー ステータスがダウン状態に移行するまでのキープアライブ再試行回数を入力します。

```
スイッチ(config)# wireless mobility group name Mygroup
スイッチ(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28
スイッチ(config)# wireless mobility group keepalive interval 5
スイッチ(config)# wireless mobility group keepalive count 3
```

ピア モビリティ グループの追加（CLI）

はじめる前に

MC は 1 つのグループだけに所属しますが、複数のグループ内の MC を認識できます。

手順の概要

1. **wireless mobility group member ip***member-ip-addr***public-ip***public-ip-addr***group***group-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility group member ip***member-ip-addr***public-ip***public-ip-addr***group***group-name* 例： スイッチ(config)# **wireless mobility group member ip 10.10.10.24 public-ip 10.10.10.25 group Group2**	Mygroup 以外のグループにメンバーをピア MC として追加します。

ローミング動作のオプション パラメータの設定

この設定により、スティッキ アンカーをディセーブルにします。必要に応じ、このコマンドは、ターゲット SSID にローミングが必要なすべての MA と MC との間で使用できます。

手順の概要

1. **wlan** open21
2. **no mobility anchor sticky**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wlan** open21 例： スイッチ(config)# wlan open20	WLAN を設定します。
ステップ 2	**no mobility anchor sticky** 例： スイッチ(config-wlan)# no mobility anchor sticky	デフォルトのスティッキモビリティアンカーをディセーブルにします。

```
スイッチ(config)# wlan open20
スイッチ(config-wlan)# no mobility anchor sticky
```

モビリティ コントローラの Mobility Oracle への指定（CLI）

はじめる前に

既知のモビリティ コントローラ上で Mobility Oracle を設定できます。

手順の概要

1. **wireless mobility group member ip***member-ip-addr***group***group-name*
2. **wireless mobility oracle ip***oracle-ip-addr*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility group member ip***member-ip-addr***group***group-name* 例： スイッチ(config)# **wireless mobility group member ip 10.10.10.10 group Group3**	MC を作成してモビリティ グループに追加します。
ステップ 2	**wireless mobility oracle ip***oracle-ip-addr* 例： スイッチ(config)# **wireless mobility oracle ip 10.10.10.10**	Mobility Oracle としてモビリティ コントローラを設定します。

```
スイッチ(config)# wireless mobility group member ip 10.10.10.10 group Group3
スイッチ(config)# wireless mobility oracle ip 10.10.10.10
```

ゲスト コントローラの設定

ゲスト コントローラは、クライアント トラフィックを非武装地帯（DMZ）のゲスト アンカー コントローラへトンネル経由で送信する場合に使用されます。ゲスト クライアントはWeb認証プロセスを通過します。Web 認証プロセスは任意です。ゲストは認証なしでトラフィックを渡すこともできます。

ゲスト クライアントがゲスト コントローラのモビリティ アンカー アドレスと接続するモビリティ エージェントの WLAN をイネーブルにします。

Cisco 5500 シリーズ WLC、Cisco WiSM2、Cisco 5700 シリーズ WLC などのゲスト コントローラ WAN で、独自の IP アドレスとしてモビリティ アンカーの IP アドレスを設定します。これにより、トラフィックはモビリティ エージェントからゲスト コントローラへトンネル経由で送信されます。

（注） Cisco 5700 シリーズ WLC をゲスト アンカー コントローラとして、また Cisco 5500 シリーズ WLC または Cisco WiSM2 をエクスポートまたは外部コントローラとした場合、Cisco 5700 シリーズ WLC ではユーザごとのゲスト ユーザ ロールはサポートされていません。

手順の概要

1. **wlan***wlan-id*
2. **mobility anchor***guest-anchor-ip-addr*
3. **client vlan***vlan-name*
4. **security open**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wlan***wlan-id* 例： `スイッチ(config)# wlan Mywlan1`	クライアントの WLAN を作成します。
ステップ 2	**mobility anchor***guest-anchor-ip-addr* 例： `スイッチ(config-wlan)# mobility anchor 10.10.10.2`	MA でゲストアンカー（GA）の IP アドレスをイネーブルにします。 （注） モビリティ コントローラでゲストアンカーをイネーブルにする場合、IP アドレスを入力する必要はありません。WLAN コンフィギュレーション モードで **mobility anchor** コマンドを入力して、モビリティ コントローラの GA をイネーブルにします。
ステップ 3	**client vlan***vlan-name* 例： `スイッチ(config-wlan)# client vlan gc_ga_vlan1`	クライアントの WLAN に VLAN を割り当てます。
ステップ 4	**security open** 例： `スイッチ(config-wlan)# security open`	WLAN にセキュリティ タイプを割り当てます。

```
スイッチ(config)# wlan Mywlan1
スイッチ(config-wlan)# mobility anchor 10.10.10.2
スイッチ(config-wlan)# client vlan gc_ga_vlan1
スイッチ(config-wlan)# security open
```

ゲスト アンカーの設定

手順の概要

1. **wlan** Mywlan1
2. **mobility anchor** <guest-anchors-own-ip-address>
3. **client vlan**<vlan-name>
4. **security open**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wlan** Mywlan1 例： `スイッチ(config)# wlan Mywlan1`	クライアントの WLAN を作成します。
ステップ 2	**mobility anchor** <guest-anchors-own-ip-address> 例： `スイッチ(config-wlan)# mobility anchor 10.10.10.2`	ゲスト アンカー（GA）のゲスト アンカー IP アドレスをイネーブルにします。GA は自身のアドレスを割り当てます。
ステップ 3	**client vlan**<vlan-name> 例： `スイッチ(config-wlan)# client vlan gc_ga_vlan1`	クライアントの WLAN に VLAN を割り当てます。
ステップ 4	**security open** 例： `スイッチ(config-wlan)# security open`	WLAN にセキュリティ タイプを割り当てます。

```
スイッチ(config)# wlan Mywlan1
スイッチ(config-wlan)# mobility anchor 10.10.10.2
スイッチ(config-wlan)# client vlan gc_ga_vlan1
スイッチ(config-wlan)# security open
```

モビリティ エージェントの設定

モビリティ コントローラの指定によるモビリティ エージェントの設定（CLI）

はじめる前に

- デフォルトでは、スイッチはモバイル エージェントとして設定されます。
- ネットワークには少なくとも1台のモビリティ コントローラがあり、モビリティ コントローラとのネットワーク接続が動作している必要があります。
- モビリティ エージェントからはモビリティを設定できません。モビリティ エージェントでは、SPG コンフィギュレーションをダウンロードするモビリティ コントローラの IP アドレスだけを設定できます。
- モビリティ エージェントでは、外部モビリティ エージェントを指定するようにモビリティ コントローラ アドレスを設定するか、モビリティ コントローラ機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **wirelessmanagementinterface**vlan 21

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wirelessmanagementinterface**vlan 21 例： `スイッチ (config)# wireless management interface vlan 21`	デバイスのワイヤレス機能をイネーブルにし、モビリティ エージェント機能をアクティブ化します。これにより、APがCAPWAPトンネルを終端する場所を確保できます。

次に、モビリティ コントローラを指定して、モビリティ グループにモビリティ エージェントを追加する例を示します。

```
スイッチ(config)# wireless management interface vlan 21
```

モビリティ エージェントのモビリティ コントローラの設定（CLI）

手順の概要

1. **wireless mobility controller**
2. **wireless mobility controller ip***ip-addr*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility controller** 例： スイッチ (config)# **wireless mobility controller** Mobility role changed to Mobility Controller. Please save config and reboot the whole stack.	スイッチでモビリティ機能をイネーブルにします。 （注） このコマンドの入力後、設定を保存してスイッチをリブートし、モビリティ コントローラ機能を有効にします。
ステップ 2	**wireless mobility controller ip***ip-addr* 例： スイッチ (config)# **wireless mobility controller ip 10.10.21.3**	モバイル エージェントに関連するモビリティ コントローラを指定します。 （注） モバイルエージェントが設定され、モビリティ コントローラが別のデバイスにある場合、モビリティ コントローラの SPG を設定して、モビリティ エージェントが正しく機能するようにします。

次の作業

モビリティ エージェントにモビリティ コントローラのロールを追加したら、モビリティ エージェントに任意のパラメータを設定できます。

モビリティ エージェントへのモビリティ コントローラ ロールの追加

手順の概要

1. **wireless mobility controller ip** 10.10.21.3

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility controller ip** 10.10.21.3 例： スイッチ(config)# wireless mobility controller ip 10.10.21.3	モビリティ エージェントをモビリティ コントローラに変換します。

次に、モビリティ エージェントにモビリティ コントローラ ロールを追加する例を示します。

```
スイッチ(config)# wireless mobility controller ip 10.10.21.3
Mobility role changed to Mobility Controller.
Please save config and reboot the whole stack.
```

モビリティ エージェントのオプション パラメータの設定（CLI）

ここでは、スイッチのロード バランシングを設定する方法を示します。

- デフォルトでは、ロード バランシングはイネーブルにされており、ディセーブルにはできません。
- スイッチは最大 2000 のクライアントをサポートし、デフォルト値はクライアントの最大負荷の 50 % です。
- スイッチがしきい値に達すると、同じ SPG 内のより負荷が低いモビリティ エージェントに新しいクライアントの負荷を再配信します。

手順の概要

1. **wireless mobility load-balance threshold***threshold-value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility load-balance threshold***threshold-value* 例： スイッチ(config)# **wireless mobility load-balance threshold 150**	ロード バランシングをトリガーするしきい値を設定します。

モビリティ エージェントを管理するモビリティ コントローラ

概要

モビリティ コントローラ（MC）は最大16のMAをサポートできます。ワイヤレスおよびAAA、ACL などの一般的なコンフィギュレーションは、通常、すべてのスイッチで同じです。ただし、以前の Cisco IOS XE では、これらの構成を分散モードを設定したすべての MA で明示的に実行する必要がありました。モビリティコントローラが制御するモビリティエージェント機能を使用して、このようなワイヤレスおよびMAとMCの共通設定をプッシュできるこの問題に対応します。このことにより、MC からすべての MA を設定、監視、トラブルシューティングするのに役立ちます。これは一元化モードを設定します。

MCでは、同時に一元管理することも、一元管理しないことも可能です。一元管理されるMAは、MC で設定した一連の設定を受信します。一元管理されない MA では、MC の設定を受信しません。MA が一元管理されている間は、MC から MA にプッシュされている設定の変更はできません。

モビリティ コントローラ（MC）はすべての一元化 MA に既存の CAPWAP トンネルを介して、すべての関連する設定をプッシュします。また、MCは、MCからMAに追加できる設定をプッシュします。

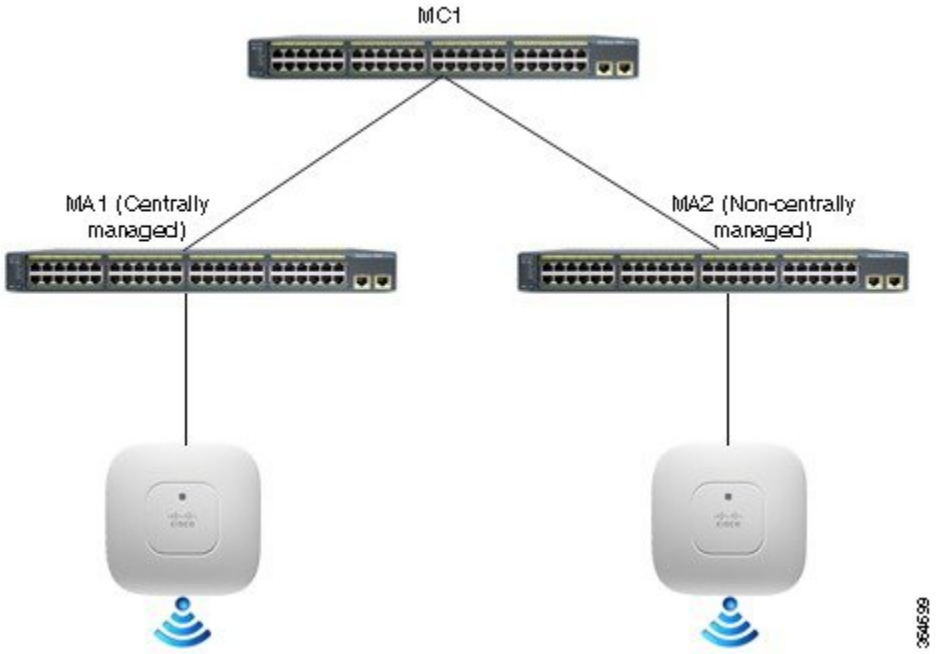
（注） この機能を使用するには、最初に MA と MC の間の CAPWAP トンネルを起動する設定を行う必要があります。

MA に送信される構成については、以下の項で説明します。

- 共通設定：セキュリティ設定、いわゆる認証、許可、アカウンティングなど、有線とワイヤレスの間で共有される設定。
- ワイヤレス設定：すべてのワイヤレス設定。

MA と MC の間で同期したコマンドの一覧については、*MC Managing MA - List of Commands Synchronized Between MC and MA*（http://www.cisco.com/c/en/us/td/docs/wireless/controller/mc-ma/mc-ma-sync.html）を参照してください。

図 *42*：*MC* が一元管理する *MA*



分散モードと一元化モードの違い

分散モード	一元化モード
MC で設定するには： • MA から MC へのモビリティ ピアリング設定 • Wireless LAN（ワイヤレス LAN） • ワイヤレス QoS ポリシー • ワイヤレス Flexible NetFlow/AVC • ワイヤレス セキュリティ ACL • AAA グローバル コンフィギュレーション • ロケーション • CleanAir、RRM、クライアント リンク • グローバルおよび AP ごとの設定	MC で設定するには： • MA から MC へのモビリティ ピアリング設定 • Wireless LAN（ワイヤレス LAN） • ワイヤレス セキュリティ ACL • AAA グローバル コンフィギュレーション • ロケーション • CleanAir、RRM、クライアント リンク • グローバルおよび AP ごとの設定

分散モード	一元化モード
MA で設定するには： • MA から MC へのモビリティ ピアリング設定 • Wireless LAN（ワイヤレス LAN） • ワイヤレス QoS ポリシー • ワイヤレス Flexible NetFlow/AVC • ワイヤレス セキュリティ ACL • AAA グローバル コンフィギュレーション • ロケーション • CleanAir、RRM、クライアント リンク • グローバルおよび AP ごとの設定	MA で設定するには： • MA から MC へのモビリティ ピアリング設定 • ワイヤレス QoS ポリシー • ワイヤレス Flexible NetFlow/AVC

機能の履歴

リリース	Remarks
Cisco IOS XE リリース 3.7.0E	この機能は、Catalyst 3850 および Catalyst 3650 シリーズのスイッチに導入されています。
Cisco IOS XE リリース 3.7.1E	Catalyst 4500E Supervisor Engine 8-E に本機能のサポートが追加されました。

機能制限

- 一元化モードは、総合アクセス ソリューション プラットフォームのみに適用され、Cisco 5500 または 8500 シリーズ ワイヤレス コントローラなどの Cisco AireOS ワイヤレス プラットフォームではサポートされません。
- MA が一元化モードになると、グローバルな設定が無効になり、残りの設定およびモニタリングは Web GUI で使用可能です。
- この機能は、Cisco Prime Infrastructure ではサポートされていません。
- Out-of-Sync リロード：MC が同期していない MA を検出すると、MA は強制的にリロードされ、リロード後に MC から全体のコンフィギュレーションを再同期します。
- MA と MC が同期しない場合のシナリオには、次のようなものがあります。

- 新しい MA は MC と結合して、MA は一元的に管理されます。
- MA がある MC から別の MC へ移動された場合

- QoS の設定は、MC から MC へプッシュされません。
- MC は、すべての構成を一元管理された MA へすべてプッシュします。設定のサブセットを選択し、すべての MA ではなく特定の MA グループへプッシュすることはできません。
- WLAN 設定は MC からプッシュされるため、L3 ローミングはできません。

MA を管理する MC の設定（GUI）

ステップ 1 モビリティ コントローラで、[Configuration] > [Controller] > [Mobility Management] > [Switch Peer Group] の順に選択します。

ステップ 2 新しいスイッチ ピア グループ メンバーを作成またはスイッチ グループ メンバーを編集します。

ステップ 3 [Switch Peer Group] > [New/Switch Peer Group] > [Modify] の順に選択して表示されるページで、[Centralized mode] チェックボックスを選択して、メンバー MA を MC から一元管理されるように設定します。

ステップ 4 設定を保存します。

ステップ 5 モビリティ エージェントの GUI ホーム ページで、ステータスが [Centrally Managed] と表示されていることを確認できます。

例

この例では、MC で WLAN を作成して、一元管理される MC と WLAN 設定を同期する方法を示しています。

ステップ 1 MC で、MCMA_Demo という名前の WLAN を作成します。

ステップ 2 [Apply] をクリックします。
WLAN が作成されますが、デフォルトでは無効にされています。

ステップ 3 WLAN を有効にする：[WLAN] > [Edit] ページで、[Status] チェックボックスのチェックを外します。

ステップ 4 [Interface/Interface Group（G）] を [VLAN0022] に変更します。

ステップ 5 [Security] タブで、[Layer 2 Security] を [None] に設定します。

ステップ 6 [Apply] をクリックし、[Save Configuration] をクリックします。
これにより、一元管理される MA と設定を同期します。

ステップ 7 MA で、[WLANs] ページに移動します。
MC で作成し、MA と同期した MCMA_Demo WLAN が表示されます。

MA を管理する MC の設定（CLI）

ステップ 1 MC で次のようにします。

a) 次のコマンドを入力して、ワイヤレス管理インターフェイスを設定します。
```
スイッチ(config)# wireless management interface vlan vlan-id
```
b) 次のコマンドを入力して、スイッチ ピア グループ（SPG）を設定します。
```
スイッチ(config)# wireless mobility controller peer-group spg-name
```
c) 次のコマンドを入力して、MA を SPG に追加し、一元管理されるように設定します（一元化オプションのみ使用）。
```
スイッチ# wireless mobility controller peer-group spg-name member ip ip-addr mode centralized
```

ステップ 2 MA で次のようにします。

a) 次のコマンドを入力して、MC の IP アドレスを指定します。
```
スイッチ(config)# wireless mobility controller ip mc-ip-addr
```
b) 次のコマンドを入力して、ワイヤレス管理インターフェイスを設定します。
```
スイッチ(config)# wireless management interface vlan vlan-id
```

ステップ 3 一元的モニタリング：

a) MC から、次のコマンドを入力して MA の状態を確認できます。
```
スイッチ# show wireless mobility summary

Mobility Controller Summary:

Mobility Role                               : Mobility Controller
Mobility Protocol Port                      : 16666
Mobility Group Name                         : default
Mobility Oracle IP Address                  : 0.0.0.0
DTLS Mode                                   : Enabled
Mobility Domain ID for 802.11r              : 0xac34
Mobility Keepalive Interval                 : 10
Mobility Keepalive Count                    : 3
Mobility Control Message DSCP Value         : 48
Mobility Domain Member Count                : 1

IP         Public IP        Link   Status     Centralized(Cfgd : Running)
-------------------------------------------------------------------------------
1.1.1.1     1.1.1.1          UP   : UP         Enabled        Enabled
3.3.3.1     3.3.3.1          DOWN : DOWN       Enabled        Enabled
```

設定された一元化モード	実行中の一元化モード	説明
ディセーブル	ディセーブル	MA は、MC で一元管理されるように設定されていません。

設定された一元化モード	実行中の一元化モード	説明
イネーブル	ディセーブル	MAは、MCで一元管理されるように設定されていますが、MAへのトンネルはまだダウン状態である、またはMAはまだMCから一元管理されていることを通知するメッセージを確認していません。
イネーブル	イネーブル	MAは、MCで一元管理されるように設定されており、MAは一元管理モードで実行中です。
ディセーブル	イネーブル	なし。

b) このコマンドを入力すると、SPG に関係なく、および一元管理されているかどうかに関わらず、MC 上で設定されているすべての MA を確認できます。

```
スイッチ# show cmm member-table

CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 16

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.155
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 16
Last rcvd cfg rev on MA = 16
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 16
Last sent cfg timestamp = 1427826323 sec 936009397 nsec
----------------


Members: No. of MAs configured on the MC
System Rev No on MC: What version number the MC is at

Entry
```

上記の出力例は、MA が作動しており、MC から設定を受け取ったことを示します。

c) MC で実行され、CMM エージェントに格納された設定を、同期のために確認するには、次のコマンドを入力します。

```
スイッチ# show cmm config

Current version number: 17
To sync and save configuration to Mobility Agents execute: "wr memory"

Config commands present in the buffer:
access-list 1 permit any
wlan MCMA_Demo 4 MCMA_Demo
client vlan 22
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

（注） MC からの設定は、「wr memory」コマンドが MC で実行された後にのみ MA と同期されます。

ステップ 4 リモート コマンド：MC から MA でコマンドをリモート実行できます。例えば、次のコマンドを MC で入力して、クライアントが稼働時間に達したかどうかを確認できます。

```
スイッチ# remote command 1.1.1.1 sh wcdb da all

Total Number of Wireless Clients = 1
                Clients Waiting to Join   = 0
                Local Clients             = 0
                Anchor Clients            = 1
                Foreign Clients           = 0
                MTE Clients               = 0


Mac Address       VlanId   IP Address     Src If             Auth     Mob
----------      ---------  -------------  --------          -----   -------
ec55.f9c6.35c3     22        53.1.1.2    0x00D19B00000001C5  RUN    ANCHOR
```

また、次のコマンドを入力して、MC から MA にリモートでログインできます。

```
スイッチ# remote login 1.1.1.1

Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session


User Access Verification

Password:
MA1>en
Password:
MA1#
```

例

この例では、MC で WLAN を作成して、一元管理される MC と WLAN 設定を同期する方法を示しています。

ステップ 1 MC では、次のコマンドを入力して、MCMA_Demo という名前の WLAN を作成します。

```
スイッチ(config)# wlan MCMA_Demo 1 MCMA_Demo
スイッチ(config-wlan)# exit
スイッチ(config)# exit
```

ステップ 2 設定を確認するには、次のコマンドを入力します。

```
スイッチ# sh cmm config

Current version number: 3
To sync and save configuration to Mobility Agents execute: "wr memory"

Config commands present in the buffer:
wlan MCMA_Demo 1 MCMA_Demo
exit
```

ステップ 3 一元管理されるように設定されている MA の数を調べるには、次のコマンドを入力します。

```
スイッチ# sh cmm member-table

CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 2

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 2
Last rcvd cfg rev on MA = 2
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 2
Last sent cfg timestamp = 1432843797 sec 57656031 nsec
----------------
```

ステップ 4 次のコマンドを入力して、WLAN の詳細を確認します。

```
スイッチ# sh wlan summary

Number of WLANs: 1

WLAN  Profile Name    SSID          VLAN Status
-------------------------------------------------
```

```
1        MCMA_Demo    MCMA_Demo       1    DOWN
```

ステップ 5 次のコマンドを入力して、設定を保存します。

```
スイッチ# wr memory

Building configuration...
Compressed configuration from 7612 bytes to 3409 bytes[OK]
```

ステップ 6 次のコマンドを入力して、MA の同期ステータスを確認します。

```
スイッチ# sh cmm member-table

CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 3

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 2
Last rcvd cfg rev on MA = 2
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_STALE
Last sent cfg rev to MA = 3
Last sent cfg timestamp = 1432847325 sec 107200589 nsec
----------------
```

ステップ 7 MA で、次のコマンドを入力して、MC で作成された WLAN が MA と同期していることを確認します。

```
スイッチ# sh wlan summary

Number of WLANs: 1

WLAN  Profile Name    SSID           VLAN Status
-------------------------------------------------
1    MCMA_Demo     MCMA_Demo          1    DOWN
```

複数の設定が同期されているログの例

```
MC -

MC#sh cmm config
Current version number: 4
To sync and save configuration to Mobility Agents execute: "wr memory"

Config commands present in the buffer:
wlan open 2 open
assisted-roaming dual-list
assisted-roaming neighbor-list
```

```
broadcast-ssid
ccx aironet-iesupport
channel-scan defer-priority 4
client association limit ap 0
client association limit radio 0
client vlan default
exclusionlist
exclusionlist timeout 60
ip access-group web none
mac-filtering test
mobility anchor sticky
radio all
security wpa
security wpa akm dot1x
security wpa wpa2
security wpa wpa2 ciphers aes
security dot1x authentication-list test
security dot1x encryption 104
security ft over-the-ds
security ft reassociation-timeout 20
security static-wep-key authentication open
security tkip hold-down 60
security web-auth authentication-list test2
security web-auth parameter-map test3
service-policy client input un
service-policy client output un
service-policy input unk
service-policy output unk
session-timeout 1800
no shutdown
exit


MC#sh cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 3

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 3
Last rcvd cfg rev on MA = 3
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 3
Last sent cfg timestamp = 1433441315 sec 669464681 nsec
----------------


MC#sh wlan summary

Number of WLANs: 2

WLAN Profile Name                     SSID                            VLAN Status
-------------------------------------------------------------------------------
1    test                             test                            1    DOWN
2    open                             open                            1    UP

MC#wr mem
Building configuration...
Compressed configuration from 7972 bytes to 3619 bytes[OK]
MC#
MC#
MC#
MC#
MC#sh wlan summary

Number of WLANs: 2
```

```
WLAN Profile Name                    SSID                              VLAN Status
-------------------------------------------------------------------------------
1    test                            test                              1    DOWN
2    open                            open                              1    UP

MC#sh cmm config
Current version number: 4
To sync and save configuration to Mobility Agents execute: "wr memory"

Config commands present in the buffer:


MC#sh cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 4

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 3
Last rcvd cfg rev on MA = 3
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_STALE
Last sent cfg rev to MA = 4
Last sent cfg timestamp = 1433488804 sec 349065646 nsec
----------------


MC#sh cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 4

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 3
Last rcvd cfg rev on MA = 3
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_STALE
Last sent cfg rev to MA = 4
Last sent cfg timestamp = 1433488812 sec 349323943 nsec
----------------


MC#sh cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 4

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 4
Last rcvd cfg rev on MA = 4
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 4
Last sent cfg timestamp = 1433488820 sec 349544632 nsec
```

```
----------------
MC#



MA -



MA21#sh cmm config
Current version number: 3
Centrally Managed: True
MA21#sh wlan sum
MA21#sh wlan summary

Number of WLANs: 1

WLAN Profile Name                     SSID                            VLAN Status
-------------------------------------------------------------------------------
1    test                             test                            1    DOWN

MA21#
Building configuration...

*Jun  5 07:21:18.295: %SYS-5-CONFIG_I: Configured from console by vty1
*Jun  5 07:21:18.314: %CMM-6-CONFIG_SYNC_SAVE_MSG: Saving config rev#4 received
from Mobility Controller.Compressed configuration from 13033 bytes to 4340 bytes[OK]

MA21#sh cmm config
Current version number: 4
Centrally Managed: True
MA21#sh wlan summary

Number of WLANs: 2

WLAN Profile Name                     SSID                            VLAN Status
-------------------------------------------------------------------------------
1    test                             test                            1    DOWN
2    open                             open                            1    UP


MA21#sh run wlan
wlan test 1 test
 shutdown
wlan open 2 open
 assisted-roaming dual-list
 assisted-roaming neighbor-list
 ip access-group web none
 mac-filtering test
 security dot1x authentication-list test
 security web-auth authentication-list test2
 security web-auth parameter-map test3
 service-policy client input un
 service-policy client output un
 service-policy input unk
 service-policy output unk
 no shutdown
MA21#
MA21#sh run wlan ?
  WORD  Wlan profile name to display
  |     Output modifiers
  <cr>

MA21#sh run wlan open
wlan open 2 open
 assisted-roaming dual-list
 assisted-roaming neighbor-list
 ip access-group web none
 mac-filtering test
 security dot1x authentication-list test
 security web-auth authentication-list test2
 security web-auth parameter-map test3
```

```
 service-policy client input un
 service-policy client output un
 service-policy input unk
 service-policy output unk
 no shutdown
MA21#
MA21#
```

第 VIII 部

Network Management

- Cisco IOS Configuration Engine の設定，671 ページ
- Cisco Discovery Protocol の設定，697 ページ
- 簡易ネットワーク管理プロトコルの設定，711 ページ
- サービス レベル契約の設定，749 ページ
- ローカル ポリシーの設定，775 ページ
- SPAN および RSPAN の設定，789 ページ
- パケット キャプチャの設定，839 ページ

第 42 章

Cisco IOS Configuration Engine の設定

- 機能情報の確認，671 ページ
- Configuration Engine を設定するための前提条件，671 ページ
- Configuration Engine の設定に関する制約事項，672 ページ
- Configuration Engine の設定について，672 ページ
- Configuration Engine の設定方法，679 ページ
- CNS 設定のモニタリング，693 ページ
- その他の参考資料，694 ページ

機能情報の確認

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

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

Configuration Engine を設定するための前提条件

- ユーザが接続している設定エンジン インスタンスの名前を取得します。
- CNS は、イベント バスとコンフィギュレーション サーバの両方を使用してデバイスに設定を提供するので、設定済みのスイッチごとに ConfigID と DeviceID の両方を定義する必要があります。

- **cns config partial** グローバル コンフィギュレーション コマンドを使用して設定したすべてのスイッチがイベント バスにアクセスする必要があります。スイッチを起源とする DeviceID は、Cisco Configuration Engine 内の対応するスイッチ定義の DeviceID と一致する必要があります。ユーザが接続しているイベント バスのホスト名を把握する必要があります。

関連トピック

Cisco Networking Service ID およびデバイスのホスト名，（674 ページ）
DeviceID，（675 ページ）

Configuration Engine の設定に関する制約事項

- コンフィギュレーション サーバの 1 つのインスタンスでは、設定済みの 2 つのスイッチが同じ ConfigID 値を共有できません。
- イベント バスの 1 つのインスタンスでは、設定済みの 2 つのスイッチが同じ DeviceID 値を共有できません。

関連トピック

Cisco Networking Service ID およびデバイスのホスト名，（674 ページ）

Configuration Engine の設定について

Cisco Configuration Engine ソフトウェア

Cisco Configuration Engine は、ネットワーク管理ユーティリティ ソフトウェアで、ネットワーク デバイスおよびサービスの配置と管理を自動化するためのコンフィギュレーション サービスとして機能します。各 Cisco Configuration Engine は、シスコ デバイス（スイッチとルータ）のグループとデバイスが提供するサービスを管理し設定を保存して、必要に応じて配信します。Cisco Configuration Engine は、デバイス固有のコンフィギュレーション変更を生成してデバイスに送信し、コンフィギュレーション変更を実行して結果をログに記録することにより、初期設定とコンフィギュレーションの更新を自動化します。

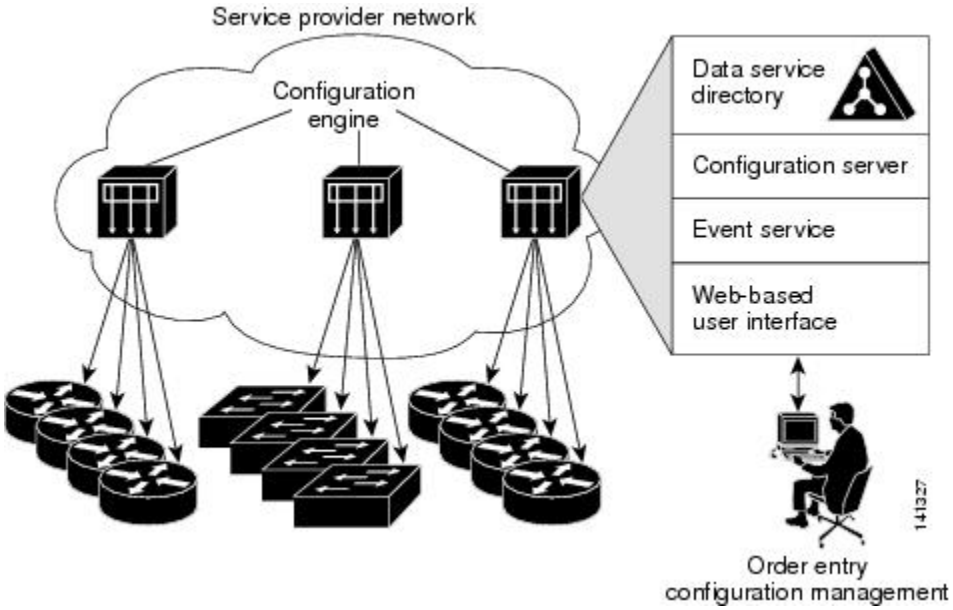
Cisco Configuration Engine は、スタンドアロン モードとサーバ モードをサポートし、次の Cisco Networking Service（CNS）コンポーネントがあります。

- コンフィギュレーション サービス
  - Web サーバ
  - ファイル マネージャ
  - ネームスペース マッピング サーバ
- イベント サービス（イベント ゲートウェイ）

- データ サービス ディレクトリ（データ モデルおよびスキーマ）

スタンドアロンモードでは、内部に組み込まれたディレクトリ サービスがサポートされます。このモードでは、外部ディレクトリまたはその他のデータ ストアは必要ありません。サーバモードでは、ユーザが定義した外部ディレクトリの使用がサポートされます。

図 *43*：*Cisco Configuration Engine* のアーキテクチャの概要



コンフィギュレーション サービス

コンフィギュレーション サービスは、Cisco Configuration Engine の中核コンポーネントです。スイッチ上にある Cisco IOS CNS エージェントと連携して動作するコンフィギュレーション サーバで構成されています。コンフィギュレーション サービスは、初期設定と論理グループによる大規模な再設定のために、デバイスとサービスの設定をスイッチに配信します。スイッチはネットワーク上で初めて起動するときに、コンフィギュレーション サービスから初期設定を受信します。

コンフィギュレーション サービスは CNS イベント サービスを使用して設定変更イベントを送受信し、成功および失敗の通知を送信します。

コンフィギュレーション サーバは Web サーバであり、コンフィギュレーション テンプレートと組み込み型ディレクトリ（スタンドアロン モード）またはリモート ディレクトリ（サーバ モード）に保存されているデバイス固有の設定情報を使用します。

コンフィギュレーション テンプレートは、CLI（コマンドライン インターフェイス）コマンド形式で静的な設定情報を含んだテキスト ファイルです。テンプレートでは、変数は、Lightweight Directory Access Protocol（LDAP）URL を使用して指定します。この URL はディレクトリに保存されているデバイス固有の設定情報を参照します。

Cisco IOS エージェントは受信したコンフィギュレーション ファイルの構文をチェックし、イベントを発行して構文チェックが成功または失敗したかを表示します。コンフィギュレーション エー

ジェントは設定をただちに適用することも、あるいは同期化イベントをコンフィギュレーション サーバから受信するまで適用を遅らせることもできます。

イベント サービス

Cisco Configuration Engine は、設定イベントの受信および生成にイベント サービスを使用します。イベント サービスはイベント エージェント、イベント ゲートウェイから構成されます。イベント エージェントはスイッチ上にあり、スイッチと Cisco Configuration Engine のイベント ゲートウェイ間の通信を容易にします。

イベント サービスは、非常に有効なパブリッシュ サブスクライブ通信方式です。イベント サービスは、サブジェクトベースのアドレス指定を使用して、メッセージを宛先に送信します。サブジェクトベースのアドレス表記法では、メッセージおよび宛先には簡単で均一なネームスペースを定義します。

関連トピック

CNS イベント エージェントのイネーブル化, （679 ページ）

ネームスペース マッパー

Cisco Configuration Engine はネームスペース マッパー（NSM）を備えています。これは、アプリケーション、デバイスまたはグループ ID、およびイベントに基づいてデバイスの論理グループを管理するための検索サービスを提供します。

Cisco IOS デバイスは、たとえば cisco.cns.config.load といった、Cisco IOS ソフトウェアで設定されたサブジェクト名と一致するイベント サブジェクト名のみを認識します。ネームスペース マッピング サービスを使用すると、希望する命名規則を使用することでイベントを指定できます。サブジェクト名でデータ ストアにデータを入力した場合、NSM はイベント サブジェクト名ストリングを、Cisco IOS が認識するものに変更します。

サブスクライバの場合、一意のデバイス ID とイベントが指定されると、ネームスペース マッピング サービスは、サブスクライブ対象のイベント セットを返します。同様にパブリッシャの場合、一意のグループ ID、デバイス ID、およびイベントが指定されると、マッピング サービスは、パブリッシュ対象のイベント セットを返します。

Cisco Networking Service ID およびデバイスのホスト名

Cisco Configuration Engine は、設定対象の各スイッチに一意の識別子が関連付けられていることを前提としています。一意の識別子は複数の同義語を持つことができますが、各同義語は特定のネームスペース内で一意です。イベント サービスは、ネームスペースの内容を使用してメッセージのサブジェクトベース アドレス指定を行います。

Cisco Configuration Engine は、イベント バス用とコンフィギュレーション サーバ用の 2 つの名前空間を交差します。コンフィギュレーション サーバのネームスペースでは、*ConfigID* という用語がデバイスの一意な識別子です。イベント バスのネームスペースでは、*DeviceID* という用語がデバイスの CNS 一意識別子です。

関連トピック

Configuration Engine を設定するための前提条件, （671 ページ）

Configuration Engine の設定に関する制約事項, （672 ページ）

ConfigID

設定対象のスイッチはそれぞれ固有の ConfigID を持ちます。これは Cisco Configuration Engine ディレクトリからスイッチ CLI 属性の対応するセットを取得するためのキーとなります。スイッチで定義された ConfigID は、Cisco Configuration Engine 上の対応するスイッチ定義の ConfigID と一致する必要があります。

ConfigID は起動時に固定され、スイッチ ホスト名を再設定した場合でもデバイスを再起動するまで変更できません。

DeviceID

イベント バスに参加している設定済みのスイッチごとに一意の DeviceID があります。これはスイッチの送信元アドレスに似ているので、スイッチをバス上の特定の宛先として指定できます。

DeviceID の発信元は、スイッチの Cisco IOS ホスト名によって定義されます。ただし、DeviceID 変数およびその使用は、スイッチに隣接するイベント ゲートウェイ内にあります。

イベント バス上の Cisco IOS の論理上の終点は、イベント ゲートウェイに組み込まれ、それがスイッチの代わりにプロキシとして動作します。イベント ゲートウェイはイベント バスに対して、スイッチおよび対応する DeviceID を表示します。

スイッチは、イベント ゲートウェイとの接続が成功するとすぐに、そのホスト名をイベント ゲートウェイに宣言します。接続が確立されるたびに、イベント ゲートウェイは DeviceID 値を Cisco IOS ホスト名に組み合わせます。イベント ゲートウェイは、スイッチと接続している間、この DeviceID 値を保持します。

関連トピック

Configuration Engine を設定するための前提条件, （671 ページ）

ホスト名および DeviceID

DeviceID は、イベント ゲートウェイと接続したときに固定され、スイッチ ホスト名を再設定した場合でも変更されません。

スイッチでスイッチ ホスト名を変更するとき、DeviceID を更新する唯一の方法は、スイッチとイベント ゲートウェイ間の接続を切断することです。DeviceID 更新の手順については、以下の「関連項目」を参照してください。

接続が再確立されると、スイッチは変更したホスト名をイベント ゲートウェイに送信します。イベント ゲートウェイは DeviceID を新しい値に再定義します。

注意 Cisco Configuration Engine ユーザ インターフェイスを使用するときは、最初に DeviceID フィールドを、スイッチが前ではなく後に取得するホスト名値に設定する必要があります。Cisco IOS CNS エージェント用に設定を再初期化する必要があります。そのようにしないと、後続の部分的なコンフィギュレーション コマンド操作で誤動作が発生する可能性があります。

関連トピック

DeviceID の更新, （689 ページ）

ホスト名、DeviceID、および ConfigID

スタンドアロン モードでは、ホスト名の値をスイッチに設定すると、コンフィギュレーション サーバはイベントをホスト名に送信する場合、そのホスト名を DeviceID として使用します。ホスト名が設定されていない場合、イベントはデバイスの cn=<*value*>で送信されます。

サーバ モードでは、ホスト名は使用されません。このモードでは、バス上のイベント送信には常に一意の DeviceID 属性が使用されます。この属性が設定されていない場合はスイッチを更新できません。

Cisco Configuration Engine で **Setup** を実行する場合、これらの属性および関連する属性（タグ値のペア）を設定します。

Cisco IOS CNS エージェント

CNS イベント エージェント機能によって、スイッチはイベント バス上でイベントにパブリッシュおよびサブスクライブを行い、Cisco IOS CNS エージェントと連携できます。スイッチ Cisco IOS ソフトウェアに組み込まれているこれらのエージェントでは、スイッチを接続して、自動的に設定できます。

関連トピック

Cisco IOS CNS エージェントのイネーブル化, （681 ページ）

初期設定

スイッチが最初に起動すると、ネットワークで Dynamic Host Configuration Protocol（DHCP）要求をブロードキャストすることで IP アドレスを取得しようとします。サブネット上には DHCP サーバがないものと想定し、ディストリビューション スイッチは DHCP リレー エージェントとして動作し、要求を DHCP サーバに転送します。DHCP サーバは要求を受信すると、新しいスイッチに IP アドレスを割り当て、Trivial File Transfer Protocol（TFTP）サーバのインターネット プロトコル（IP）アドレス、ブートストラップ コンフィギュレーション ファイルへのパス、デフォルト ゲートウェイの IP アドレスを、DHCP リレー エージェントに対するユニキャスト応答に組み入れます。DHCP リレー エージェントは、この応答をスイッチに転送します。

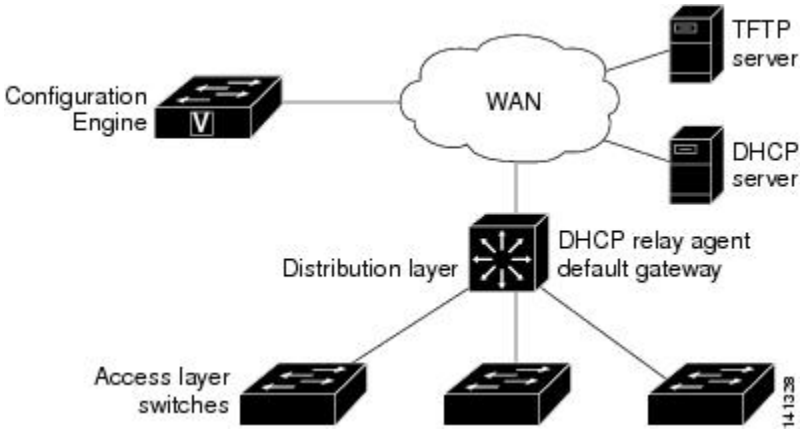
スイッチは、割り当てられた IP アドレスを自動的にインターフェイス VLAN 1（デフォルト）に設定し、TFTP サーバからブートストラップ コンフィギュレーション ファイルをダウンロードし

ます。ブートストラップ コンフィギュレーション ファイルが正常にダウンロードされると、スイッチはそのファイルを実行コンフィギュレーションにロードします。

Cisco IOS CNS エージェントは、該当する ConfigID および EventID を使用して Configuration Engine との通信を開始します。Configuration Engine はこの ConfigID をテンプレートにマッピングして、スイッチに完全なコンフィギュレーション ファイルをダウンロードします。

次の図に、DHCP ベースの自動設定を使用して初期ブートストラップ コンフィギュレーション ファイルを取得するためのネットワーク構成例を示します。

図 *44*：初期設定



関連トピック

Cisco IOS CNS エージェントの初期設定のイネーブル化，（683 ページ）
CNS 設定のモニタリング，（693 ページ）

差分（部分的）設定

ネットワークが稼働すると、Cisco IOS CNS エージェントを使用して新しいサービスを追加できます。差分（部分）設定は、スイッチに送信できます。実際の設定を、イベント ペイロードとしてイベント ゲートウェイを介して（プッシュ処理）送信するか、スイッチにプル オペレーションを開始させる信号イベントとして送信できます。

スイッチは、適用する前に設定の構文をチェックできます。構文が正しい場合は、スイッチは差分設定を適用し、コンフィギュレーション サーバに成功を信号で伝えるイベントを発行します。スイッチが差分設定を適用しない場合、エラー ステータスを示すイベントを発行します。スイッチが差分設定を適用した場合、不揮発性 RAM（NVRAM）に書き込むか、または書き込むように指示されるまで待つことができます。

関連トピック

Cisco IOS CNS エージェントの部分的設定のイネーブル化，（691 ページ）
CNS 設定のモニタリング，（693 ページ）

コンフィギュレーションの同期

スイッチは、設定を受信した場合、書き込み信号イベントの受信時に設定の適用を遅らせることができます。書き込み信号イベントは、更新された設定を NVRAM に保存しないようにスイッチに指示します。スイッチは更新された設定を実行コンフィギュレーションとして使用します。これによりスイッチの設定は、次のリブート時の使用のために NVRAM に設定を保存する前に、他のネットワーク アクティビティと同期化されます。

自動 CNS 設定

スイッチの自動CNS設定をイネーブルにするには、まずこのトピックに示す前提条件を完了する必要があります。条件設定を完了したらスイッチの電源を入れます。**setup** プロンプトでは何も入力しません。スイッチが初期設定を開始します。コンフィギュレーション ファイル全体がスイッチにロードされると作業は完了です。

初期設定中の動作については、「関連項目」を参照してください。

表 *43*：自動設定イネーブル化の条件

デバイス	必要な設定
アクセス スイッチ	出荷時の設定（コンフィギュレーション ファイルなし）
ディストリビューション スイッチ	• IP ヘルパー アドレス • DHCP リレー エージェントをイネーブルにする[1] • IP ルーティング（デフォルト ゲートウェイとして使用する場合）
DHCP サーバ	• IP アドレスの割り当て • TFTP サーバの IP アドレス • TFTP サーバのブートストラップ コンフィギュレーション ファイルへのパス • デフォルト ゲートウェイの IP アドレス

デバイス	必要な設定
TFTP サーバ	• スイッチと Configuration Engine との通信を可能にする CNS コンフィギュレーション コマンドを含むブートストラップ コンフィギュレーション ファイル • （デフォルトのホスト名の代わりに）スイッチ MAC アドレスまたはシリアル番号のいずれかを使用して ConfigID および EventID を生成するように設定されたスイッチ • スイッチにコンフィギュレーション ファイルをプッシュするように設定された CNS イベント エージェント
CNS Configuration Engine	デバイス タイプ別の 1 つまたは複数のテンプレートで、テンプレートにデバイスの ConfigID がマッピングされています。

[1] DHCP リレーは、DHCP サーバがクライアントとは異なるサブネット上にある場合にのみ必要です。

Configuration Engine の設定方法

CNS イベント エージェントのイネーブル化

（注） スイッチ上で CNS イベント エージェントをイネーブルにしてから、CNS 設定エージェントをイネーブルにする必要があります。

スイッチ上で CNS イベント エージェントをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cns event** {*hostname* | *ip-address*} [*port-number*] [[**keepalive***secondsretry-count*] [**failover-time***seconds*] [**reconnect-time***time*] | **backup**]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cns event** {*hostname* | *ip-address*} [*port-number*] [[**keepalive***secondsretry-count*] [**failover-time***seconds*] [**reconnect-time***time*] | **backup**] 例： スイッチ(config)# **cns event 10.180.1.27 keepalive 120 10**	イベントエージェントをイネーブルにして、ゲートウェイパラメータを入力します。 • {*hostname* | *ip-address*} に、イベント ゲートウェイのホスト名または IP アドレスを入力します。 • （任意）*port number* に、イベント ゲートウェイのポート番号を入力します。デフォルトのポート番号は 11011 です。 • （任意）**keepalive***seconds* に、スイッチがキープアライブ メッセージを送信する間隔を入力します。*retry-count* に、キープアライブ メッセージへの応答がない場合に接続を終了するまでのスイッチのメッセージ送信回数を入力します。デフォルト値はいずれも 0 です。 • （任意）**failover-time***seconds* に、バックアップ ゲートウェイが確立された後にスイッチがプライマリ ゲートウェイ ルートを待つ時間を入力します。 • （任意）**reconnect-time***time* に、スイッチがイベント ゲートウェイに再接続しようとする前の最大時間間隔を入力します。 • （任意）バックアップ ゲートウェイであることを示す場合は、**backup** を入力します（省略した場合は、プライマリ ゲートウェイになります）。 （注） **encrypt** キーワードおよび **clock-timeout***time* キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

イベント エージェントに関する情報を確認するには、**show cns event connections** コマンドを特権 EXEC モードで使用します。

CNS イベント エージェントをディセーブルにするには、**no cns event** { *ip-address* | *hostname* } グローバル コンフィギュレーション コマンドを使用します。

関連トピック

イベント サービス，（674 ページ）

Cisco IOS CNS エージェントのイネーブル化

スイッチ上で Cisco IOS CNS エージェントをイネーブルにするには、次の手順を実行します。

はじめる前に

このエージェントをイネーブルにする前に、スイッチで CNS イベント エージェントをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **cns config initial** {*hostname* | *ip-address*} [*port-number*]
4. **cns config partial** {*hostname* | *ip-address*} [*port-number*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**
8. Cisco IOS CNS エージェントを、スイッチで開始します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cns config initial** {*hostname* | *ip-address*} [*port-number*] 例： スイッチ(config)# **cns config initial 10.180.1.27 10**	Cisco IOS CNS エージェントをイネーブルにし、コンフィギュレーション サーバ パラメータを入力します。 • {*hostname*|*ip-address*} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。 このコマンドが Cisco IOS CNS エージェントをイネーブルにして、スイッチで初期設定を開始します。
ステップ 4	**cns config partial** {*hostname* | *ip-address*} [*port-number*] 例： スイッチ(config)# **cns config partial 10.180.1.27 10**	Cisco IOS CNS エージェントをイネーブルにし、コンフィギュレーション サーバ パラメータを入力します。 • {*hostname*|*ip-address*} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。

	コマンドまたはアクション	目的
		Cisco IOS CNS エージェントをイネーブルにして、スイッチで部分的設定を開始します。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 8	Cisco IOS CNS エージェントを、スイッチで開始します。	

次の作業

リモートで差分設定をスイッチに送信するために、Cisco Configuration Engine を使用できるようになりました。

関連トピック

Cisco IOS CNS エージェント，（676 ページ）

Cisco IOS CNS エージェントの初期設定のイネーブル化

スイッチ上で、CNS コンフィギュレーション エージェントをイネーブルにして初期設定を開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cns template connect***name*
4. **cli***config-text*
5. 別の CNS 接続テンプレートを設定する場合は、ステップ 3 ～ 4 を繰り返します。
6. **exit**
7. **cns connect***name* [**retries***number*] [**retry-interval***seconds*] [**sleep***seconds*] [**timeout***seconds*]
8. **discover** {**controller***controller-type* | **dlci** [**subinterface***subinterface-number*] | **interface** [*interface-type*] | **line***line-type*}
9. **template***name* [*... name*]
10. ステップ 8 ～ 9 を繰り返し、CNS 接続プロファイルにさらに多くのインターフェイスパラメータと CNS 接続テンプレートを指定します。
11. **exit**
12. **hostname***name*
13. **ip route***network-number*
14. **cns id***interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]
15. **cns id** {**hardware-serial** | **hostname** | **string***string* | **udi**} [**event**] [**image**]
16. **cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page***page*] [**source***ip-address*] [**syntax-check**]
17. **end**
18. **show running-config**
19. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**cns template connect***name* 例： スイッチ(config)# **cns template connect template-dhcp**	CNSテンプレート接続コンフィギュレーションモードを開始して、CNS 接続テンプレートの名前を指定します。
ステップ 4	**cli***config-text* 例： スイッチ(config-tmpl-conn)# **cli ip address dhcp**	CNS接続テンプレートにコマンドラインを入力します。テンプレート内の各コマンドラインにこの手順を繰り返します。
ステップ 5	別の CNS 接続テンプレートを設定する場合は、ステップ 3 ～ 4 を繰り返します。	
ステップ 6	**exit** 例： スイッチ(config)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**cns connect***name* [**retries***number*] [**retry-interval***seconds*] [**sleep***seconds*] [**timeout***seconds*] 例： スイッチ(config)# **cns connect dhcp**	CNS 接続コンフィギュレーション モードを開始し、CNS 接続プロファイルの名前を指定し、プロファイルパラメータを定義します。スイッチは CNS 接続プロファイルを使用して Configuration Engine に接続します。 • CNS 接続プロファイルの *name* を入力します。 • （任意）**retries***number* に、接続のリトライ回数を入力します。指定できる範囲は 1 ～ 30 です。デフォルト値は 3 です。 • （任意）**retry-interval***seconds* に、Configuration Engine への連続する接続の試行間隔を入力します。指定できる範囲は 1 ～ 40 秒です。デフォルトは 10 秒です。 • （任意）**sleep***seconds* に、最初の接続試行を実行するまで待機する時間を入力します。指定できる範囲は 0 ～ 250 秒です。デフォルト値は 0 です。 • （任意）**timeout***seconds* に、接続試行が終了するまでの時間を入力します。値の範囲は 10 ～ 2000 秒です。デフォルト値は 120 です。
ステップ 8	**discover** {**controller***controller-type* | **dlci** [**subinterface***subinterface-number*] | **interface** [*interface-type*] | **line***line-type*}	CNS 接続プロファイル内のインターフェイス パラメータを入力します。

	コマンドまたはアクション	目的
	例： スイッチ(config-cns-conn)# **discover interface gigabitethernet**	• **controller***controller-type* に、コントローラ タイプを入力します。 • **dlci** に、アクティブなデータリンク接続識別子（DLCI）を入力します。 （任意）**subinterface***subinterface-number* に、アクティブな DLCI の検索に使用するポイントツーポイント サブインターフェイス番号を指定します。 • **interface** [*interface-type*] に、インターフェイスのタイプを入力します。 • **line***line-type* に、回線タイプを入力します。
ステップ 9	**template***name* [*... name*] 例： スイッチ(config-cns-conn)# **template template-dhcp**	スイッチの設定に適用する CNS 接続プロファイル内の CNS 接続テンプレートのリストを指定します。複数のテンプレートを指定できます。
ステップ 10	ステップ 8 ～ 9 を繰り返し、CNS 接続プロファイルにさらに多くのインターフェイス パラメータと CNS 接続テンプレートを指定します。	
ステップ 11	**exit** 例： スイッチ(config-cns-conn)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**hostname***name* 例： スイッチ(config)# **hostname device1**	スイッチのホスト名を入力します。
ステップ 13	**ip route***network-number* 例： Remoteスイッチ(config)# **ip route 172.28.129.22 255.255.255.255 11.11.11.1**	（任意）IP アドレスが *network-number* の Configuration Engine へのスタティック ルートを確立します。
ステップ 14	**cns id***interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]	（任意）Configuration Engine が使用する一意の EventID または ConfigID を設定します。このコマンドを入力する場合は、**cns id**

	コマンドまたはアクション	目的
	例： `Remoteスイッチ(config)# cns id GigabitEthernet1/0/1 ipaddress`	{**hardware-serial** | **hostname** | **string***string* | **udi**} [**event**] [**image**] コマンドを入力しないでください。 • *interface num* に、インターフェイスのタイプを入力します。たとえば、ethernet、group-async、loopback、virtual-template を入力します。この設定では、一意の ID を定義するためにどのインターフェイスから IP アドレスまたは MAC アドレスを取得するかを指定します。 • {**dns-reverse** | **ipaddress** | **mac-address**} では、ホスト名を取得してそのホスト名を一意の ID として割り当てるには **dns-reverse** を入力し、IP アドレスを使用するには **ipaddress** を入力し、MAC アドレスを一意の ID として使用するには **mac-address** を入力します。 • （任意）ID をスイッチの識別に使用する event-id 値になるように設定するには、**event** を入力します。 • （任意）ID をスイッチの識別に使用する image-id 値になるように設定するには、**image** を入力します。 （注） **event** と **image** キーワードの両方を省略した場合は、スイッチの識別には image-id 値が使用されます。
ステップ 15	**cns id** {**hardware-serial** | **hostname** | **string***string* | **udi**} [**event**] [**image**] 例： `Remoteスイッチ(config)# cns id hostname`	（任意）Configuration Engine が使用する一意の EventID または ConfigID を設定します。このコマンドを入力する場合は、**cns id***interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] コマンドを入力しないでください。 • {**hardware-serial** | **hostname** | **string** *string*| **udi**} で、**hardware-serial** を入力してスイッチのシリアル番号を一意の ID として設定するか、**hostname**（デフォルト）を入力してスイッチのホスト名を一意の ID として選択するか、**string***string* に任意のテキストストリングを一意の ID として入力するか、または **udi** を入力して Unique Device Identifier（UDI）を一意の ID として設定します。
ステップ 16	**cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page***page*] [**source***ip-address*] [**syntax-check**] 例： `Remoteスイッチ(config)# cns config initial 10.1.1.1 no-persist`	Cisco IOS エージェントをイネーブルにして、初期設定を開始します。 • {*hostname* | *ip-address*} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は 80 です。

	コマンドまたはアクション	目的
		• （任意）設定が完了したときの設定の成功、失敗、または警告のメッセージ用に **event** をイネーブルにします。 • （任意）**cns config initial** グローバル コンフィギュレーション コマンドの入力結果によってプルされた設定の NVRAM への自動書き込みを抑制するには、**no-persist** を入力します。**no-persist** キーワードを入力しない場合、**cns config initial** コマンドを使用すると、その結果の設定が自動的に NVRAM に書き込まれます。 • （任意）**page***page* に、初期設定の Web ページを入力します。デフォルトは /Config/config/asp です。 • （任意）送信元 IP アドレスに使用するには、**source***ip-address* を入力します。 • （任意）このパラメータを使用したときの構文をチェックするには、**syntax-check** をイネーブルにします。 （注） コマンドラインのヘルプ ストリングに表示されますが、**encrypt**、**status***url*、**inventory** キーワードはサポートされていません。
ステップ 17	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 18	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 19	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

コンフィギュレーション エージェントに関する情報を確認するには、**show cns config connections** コマンドを特権 EXEC モードで使用します。

CNS Cisco IOS エージェントをディセーブルにするには、**no cns config initial** { *ip-address* | *hostname* } グローバル コンフィギュレーション コマンドを使用します。

関連トピック

初期設定, （676 ページ）
CNS 設定のモニタリング, （693 ページ）

DeviceID の更新

スイッチ上でホスト名を変更するときに DeviceID を更新するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show cns config connections**
3. CNS イベント エージェントがイベント ゲートウェイに正しく接続されていることを確認します。
4. **show cns event connections**
5. ステップ 4 の出力に基づいて、次に示す現在接続されている接続に関する情報を記録します。この手順の以降のステップで IP アドレスとポート番号を使用します。
6. **configure terminal**
7. **no cns event***ip-addressport-number*
8. **cns event***ip-addressport-number*
9. **end**
10. **show cns event connections** からの出力を調べて、スイッチとイベント接続間の接続が再確立されていることを確認します。
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**show cns config connections** 例： `スイッチ# show cns config connections`	CNS イベント エージェントがゲートウェイに接続しているか、接続されているか、またはアクティブか、およびイベント エージェントに使用されているゲートウェイ、その IP アドレス、およびポート番号を表示します。

	コマンドまたはアクション	目的
ステップ 3	CNS イベント エージェントがイベント ゲートウェイに正しく接続されていることを確認します。	次のように **show cns config connections** の出力を確認します。 • 接続がアクティブになっている。 • 接続で現在設定されているスイッチ ホスト名を使用している。DeviceID はこれらの手順を使用して、新しいホスト名の設定に対応するように更新されます。
ステップ 4	**show cns event connections** 例： `スイッチ# show cns event connections`	スイッチのイベント接続情報を表示します。
ステップ 5	ステップ 4 の出力に基づいて、次に示す現在接続されている接続に関する情報を記録します。この手順の以降のステップで IP アドレスとポート番号を使用します。	
ステップ 6	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 7	**no cns event***ip-addressport-number* 例： `スイッチ(config)# no cns event 172.28.129.22 2012`	このコマンドで、ステップ 5 で記録した IP アドレスとポート番号を指定します。 このコマンドで、スイッチとイベント ゲートウェイ間の接続が解除されます。最初に接続を解除し、次にこの接続を再確立して、DeviceID を更新する必要があります。
ステップ 8	**cns event***ip-addressport-number* 例： `スイッチ(config)# cns event 172.28.129.22 2012`	このコマンドで、ステップ 5 で記録した IP アドレスとポート番号を指定します。 このコマンドで、スイッチとイベント ゲートウェイ間の接続が再確立されます。
ステップ 9	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show cns event connections** からの出力を調べて、スイッチとイベント接続間の接続が再確立されていることを確認します。	
ステップ 11	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ホスト名および DeviceID, （675 ページ）

Cisco IOS CNS エージェントの部分的設定のイネーブル化

スイッチ上で Cisco IOS CNS エージェントをイネーブルにして部分設定を開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source***ip-address*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source***ip-address*] 例： スイッチ(config)# **cns config partial 172.28.129.22 2013**	コンフィギュレーション エージェントをイネーブルにし、部分設定を開始します。 • {*ip-address* | *hostname*} に、コンフィギュレーション サーバの IP アドレスまたはホスト名を入力します。 • （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は 80 です。 • （任意）送信元 IP アドレスに使用するには、**source***ip-address* を入力します。 （注） **encrypt** キーワードは、コマンドラインのヘルプストリングに表示されますが、サポートされていません。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

次の作業

コンフィギュレーション エージェントに関する情報を確認するには、**show cns config stats** または **show cns config outstanding** コマンドのいずれかを特権 EXEC モードで使用します。

Cisco IOS エージェントをディセーブルにするには、**no cns config partial** { *ip-address* | *hostname* } グローバル コンフィギュレーション コマンドを使用します。部分設定を取り消すには、**cns config cancel** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

差分（部分的）設定，（677 ページ）
CNS 設定のモニタリング，（693 ページ）

CNS 設定のモニタリング

表 *44* : ***CNS show*** コマンド

コマンド	目的
show cns config connections スイッチ# `show cns config connections`	CNS Cisco IOS CNS エージェントの接続のステータスを表示します。
show cns config outstanding スイッチ# `show cns config outstanding`	開始されたがまだ終了していない差分（部分）CNS 設定に関する情報を表示します。
show cns config stats スイッチ# `show cns config stats`	Cisco IOS CNS エージェントに関する統計情報を表示します。
show cns event connections スイッチ# `show cns event connections`	CNS イベント エージェントの接続のステータスを表示します。
show cns event gateway スイッチ# `show cns event gateway`	スイッチのイベント ゲートウェイ情報を表示します。
show cns event stats スイッチ# `show cns event stats`	CNS イベント エージェントに関する統計情報を表示します。

コマンド	目的
show cns event subject スイッチ# **show cns event subject**	アプリケーションによってサブスクライブされたイベントエージェントのサブジェクト一覧を表示します。

関連トピック

Cisco IOS CNS エージェントの部分的設定のイネーブル化，（691 ページ）
差分（部分的）設定，（677 ページ）
Cisco IOS CNS エージェントの初期設定のイネーブル化，（683 ページ）
初期設定，（676 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Configuration Engine のセットアップ	*Cisco Configuration Engine Installation and Setup Guide, 1.5 for Linux*http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/1.5/installation_linux/guide/setup_1.html

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	-

MIB

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

シスコのテクニカル サポート

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

第 43 章

Cisco Discovery Protocol の設定

- 機能情報の確認，697 ページ
- CDP に関する情報，697 ページ
- CDP の設定方法，699 ページ
- CDP のモニタおよびメンテナンス，707 ページ
- その他の参考資料，708 ページ

機能情報の確認

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

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

CDP に関する情報

CDP の概要

CDP はすべてのシスコ デバイス（ルータ、ブリッジ、アクセス サーバ、コントローラ、およびスイッチ）のレイヤ 2（データリンク層）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスにネイバー シスコ デバイスを検出できます。また、下位レイヤのトランスペアレント プロトコルが稼働しているネイバー デバイスのデバイス タイプや、簡易ネットワーク管理プロトコル（SNMP）エージェント アドレ

スを学習することもできます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDP は、サブネットワーク アクセス プロトコル（SNAP）をサポートしているすべてのメディアで動作します。CDP はデータリンク層でのみ動作するため、異なるネットワーク層プロトコルをサポートする 2 つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャストアドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。このアドバタイズには、受信側デバイスで CDP 情報を廃棄せずに保持する時間を表す存続可能時間、つまりホールドタイム情報も含まれます。各デバイスは他のデバイスから送信されたメッセージも待ち受けて、ネイバー デバイスについて学習します。

CDP はスイッチ上で Network Assistant をイネーブルにすることで、ネットワークをグラフィカルに表示できます。スイッチは CDP を使用してクラスタ候補を検出し、クラスタ メンバ、およびコマンド スイッチから最大 3 台（デフォルト）離れたクラスタ対応の他のデバイスについての情報を維持します。

関連トピック

CDP 特性の設定，（699 ページ）

CDP のモニタおよびメンテナンス，（707 ページ）

CDP のデフォルト設定

この表は、CDP のデフォルト設定を示します。

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP タイマー（パケット更新頻度）	60 秒
CDP ホールドタイム（廃棄までの時間）	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

関連トピック

Enabling CDP，（702 ページ）

CDP のディセーブル化，（701 ページ）

インターフェイス上での CDP のイネーブル化，（705 ページ）

インターフェイス上での CDP のディセーブル化，（704 ページ）

CDP の設定方法

CDP 特性の設定

次の CDP 特性を設定できます。

- CDP 更新の頻度
- 破棄するまで情報を保持する時間の長さ
- バージョン 2 アドバタイズを送信するかどうか

（注） ステップ 3 ～ 5 はすべて任意であり、どの順番で実行してもかまいません。

CDP 特性を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cdp timer***seconds*
4. **cdp holdtime***seconds*
5. **cdp advertise-v2**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**cdp timer***seconds* 例： スイッチ(config)# **cdp timer 20**	（任意）CDP 更新の送信頻度を秒単位で設定します。 指定できる範囲は 5 ～ 254 です。デフォルトは 60 秒です。
ステップ 4	**cdp holdtime***seconds* 例： スイッチ(config)# **cdp holdtime 60**	（任意）受信デバイスがこのデバイスから送信された情報を破棄せずに保持する時間を指定します。 指定できる範囲は 10 ～ 255 秒です。デフォルトは 180 秒です。
ステップ 5	**cdp advertise-v2** 例： スイッチ(config)# **cdp advertise-v2**	（任意）バージョン 2 アドバタイズを送信するように CDP を設定します。 これは、デフォルトの状態です。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

デフォルト設定に戻すには、CDP コマンドの **no** 形式を使用します。

関連トピック

CDP の概要，（697 ページ）
CDP のモニタおよびメンテナンス，（707 ページ）

CDP のディセーブル化

CDP はデフォルトで有効になっています。

（注） スイッチ クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

CDP デバイス検出機能をディセーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no cdp run**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no cdp run** 例： `スイッチ(config)# no cdp run`	CDP をディセーブルにします。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

CDP を使用するには、再びイネーブルにする必要があります。

関連トピック

Enabling CDP, （702 ページ）
CDP のデフォルト設定, （698 ページ）

Enabling CDP

CDP はデフォルトで有効になっています。

（注） スイッチ クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

無効になっている CDP を有効にするには、次の手順を実行します。

はじめる前に

CDP を無効にする必要があります。そのようにしないと有効にできません。

手順の概要

1. **enable**
2. **configureterminal**
3. **cdp run**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cdp run** 例： スイッチ(config)# **cdp run**	無効にされている場合は、CDP を有効にします。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

CDP が有効になっていることを示すには、**showrunall** コマンドを使用します。**showrun** だけを入力した場合、CDP の有効化が表示されないことがあります。

関連トピック

CDP のデフォルト設定, （698 ページ）

CDP のディセーブル化, （701 ページ）

インターフェイス上での CDP のディセーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。

（注） スイッチ クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

ポート上で CDP をディセーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **no cdp enable**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	CDP をディセーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no cdp enable** 例： スイッチ(config-if)# **no cdp enable**	ステップ 3 で指定したインターフェイスで CDP をディセーブルにします。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

インターフェイス上での CDP のイネーブル化，（705 ページ）
CDP のデフォルト設定，（698 ページ）

インターフェイス上での CDP のイネーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。

（注） スイッチ クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

ポート上でディセーブルになっている CDP をイネーブルにするには、次の手順を実行します。

はじめる前に

CDP をイネーブルにしようとしているポートで、CDP をディセーブルになっている必要があります。そうでない場合は、イネーブルにできません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **cdp enable**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet1/0/1`	CDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cdp enable** 例： `スイッチ(config-if)# cdp enable`	ディセーブルにされているインターフェイスで CDP をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

CDP のデフォルト設定，（698 ページ）
インターフェイス上での CDP のディセーブル化，（704 ページ）

CDP のモニタおよびメンテナンス

表 *45*：*CDP* 情報を表示するためのコマンド

コマンド	説明
clear cdp counters	トラフィック カウンタを 0 にリセットします。
clear cdp table	ネイバー デバイスに関する情報を収めた CDP テーブルを削除します。
show cdp	送信間隔、送信したパケットの保持時間などのグローバル情報を表示します。

コマンド	説明
show cdp entry *entry-name* [**version**] [**protocol**]	特定のネイバーに関する情報を表示します。 アスタリスク（*）を入力してすべてのCDPネイバーを表示することも、情報が必要なネイバーの名前を入力することもできます。 また、指定されたネイバー上でイネーブルになっているプロトコルの情報や、デバイス上で稼働しているソフトウェアのバージョン情報が表示されるように、表示内容を制限することもできます。
show cdp interface [*interface-id*]	CDP がイネーブルに設定されているインターフェイスの情報を表示します。 必要なインターフェイスの情報だけを表示できます。
show cdp neighbors [*interface-id*] [*detail*]	装置タイプ、インターフェイス タイプ、インターフェイス番号、保持時間の設定値、機能、プラットフォーム、ポート ID を含めたネイバー情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show cdp traffic	CDP カウンタ（送受信されたパケット数およびチェックサム エラーを含む）を表示します。

関連トピック

CDP 特性の設定，（699 ページ）

CDP の概要，（697 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*Network Management Command Reference, Cisco IOS XE Release 3E*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	-

MIB

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

シスコのテクニカル サポート

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

第 44 章

簡易ネットワーク管理プロトコルの設定

- 機能情報の確認，711 ページ
- SNMP の前提条件，712 ページ
- SNMP の制約事項，714 ページ
- SNMP に関する情報，715 ページ
- SNMP の設定方法，719 ページ
- SNMP ステータスのモニタリング，744 ページ
- SNMP の例，745 ページ
- その他の参考資料，746 ページ
- 簡易ネットワーク管理プロトコルの機能の履歴と情報，747 ページ

機能情報の確認

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

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

SNMP の前提条件

サポートされている SNMP バージョン

このソフトウェア リリースは、次の SNMP バージョンをサポートしています。

- SNMPv1：RFC1157 に規定された SNMP（完全インターネット標準）。
- SNMPv2C は、SNMPv2Classic のバルク検索機能を残し、エラー処理を改善したうえで、SNMPv2Classic のパーティ ベースの管理およびセキュリティ フレームワークをコミュニティ ストリング ベースの管理フレームワークに置き換えたものです。次の機能があります。
  - SNMPv2：RFC 1902 ～ 1907 に規定された SNMP バージョン 2（ドラフト版インターネット標準）
  - SNMPv2C：RFC 1901 に規定された SNMPv2 のコミュニティ ストリング ベースの管理フレームワーク（試験版インターネット プロトコル）
- SNMPv3：SNMP のバージョン 3 は、RFC 2273 ～ 2275 に規定されている相互運用可能な標準ベース プロトコルです。SNMPv3 は、ネットワーク上のパケットを認証、暗号化することでデバイスへのアクセスに対するセキュリティを提供します。SNMPv3 は、次のセキュリティ機能を備えています。
  - メッセージの完全性：パケットが伝送中に改ざんされないようにします。
  - 認証：有効な送信元からのメッセージであるかどうかを判別します。
  - 暗号化：パッケージの内容をミキシングし、許可されていない送信元に内容が読まれることを防止します。

（注） 暗号化を選択するには、**priv** キーワードを入力します。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティが、IP アドレス アクセス コントロール リストおよびパスワードによって定義されます。

SNMPv2C にはバルク検索機能が組み込まれ、より詳細なエラー メッセージを管理ステーションに報告します。バルク検索機能は、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラー コードが使用されています。これらのエラーは、SNMPv1 では単一のエラー コードで報告されます。SNMPv2 では、エラー リターン コードでエラー タイプが報告されるようになりました。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ レベルとセキュリティ モデルの組み合わせにより、SNMP パケットを扱うときに使用するセキュ

リティ方式が決まります。使用可能なセキュリティ モデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

次の表では、この特性を識別し、セキュリティモデルとセキュリティレベルの異なる組み合わせを比較します。

表 *46*：*SNMP* セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	いいえ	コミュニティ ストリングの照合を使用して認証します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	いいえ	コミュニティ ストリングの照合を使用して認証します。
SNMPv3	noAuthNoPriv	ユーザ名	いいえ	ユーザ名の照合を使用して認証します。
SNMPv3	authNoPriv	Message Digest 5（MD5）または Secure Hash Algorithm（SHA）	いいえ	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。

モデル	レベル	認証	暗号化	結果
SNMPv3	authPriv	MD5 または SHA	データ暗号規格（DES）または Advanced Encryption Standard（AES）	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。 次の暗号化アルゴリズムで、User-based Security Model（USM）を指定できます。 • CBC-DES（DES-56）規格に基づく認証に加えた DES 56 ビット暗号化 • 3DES 168 ビット暗号化 • AES 128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化

管理ステーションでサポートされている SNMP バージョンを使用するには、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、およびSNMPv3 を使用する通信をサポートするようにソフトウェアを設定できます。

SNMP の制約事項

バージョンの制約事項

- SNMPv1 は informs をサポートしていません。

SNMP に関する情報

SNMP の概要

SNMP は、マネージャとエージェント間の通信のメッセージ フォーマットを提供するアプリケーション レイヤ プロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および管理情報ベース（MIB）で構成されます。SNMP マネージャは、Cisco Prime Infrastructure などのネットワーク管理システム（NMS）に統合できます。エージェントおよびMIBは、スイッチに常駐します。スイッチ上でSNMPを設定するには、マネージャとエージェント間の関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイス パラメータやネットワーク データの保存場所である MIB から値を収集します。また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MACアドレス追跡、TCP接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、次の表に示す動作を実行します。

表 *47*：*SNMP* の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。[2]
get-bulk-request[3]	テーブルの複数の行など、通常はサイズの小さい多数のデータ ブロックに分割して送信する必要がある巨大なデータ ブロックを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

2 この動作を使用した場合、SNMP マネージャは厳密な変数名を知る必要はありません。テーブル内を順に検索して、必要な変数を検出します。

3 get-bulk コマンドを使用できるのは、SNMPv2 以上に限られます。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニングツリー トポロジが変更された場合、認証に失敗した場合などがあります。

関連トピック

SNMP エージェントのディセーブル化, （719 ページ）

SNMP ステータスのモニタリング, （744 ページ）

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。NMS がスイッチにアクセスするには、NMS 上のコミュニティ ストリング定義が スイッチ 上の 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致しなければなりません。

コミュニティ ストリングの属性は、次のいずれかです。

- 読み取り専用（RO）：コミュニティ ストリングを除き MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りアクセス権を与えますが、書き込みアクセスは許可しません。
- 読み取り-書き込み（RW）：MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りおよび書き込みアクセス権を与えますが、コミュニティ ストリングへのアクセスは許可しません。
- クラスタを作成すると、コマンド スイッチがメンバ スイッチと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンド スイッチ上で最初に設定された RW および RO コミュニティ ストリングにメンバ スイッチ番号（@esN、N はスイッチ番号）を追加し、これらのストリングをメンバ スイッチに伝播します。

関連トピック

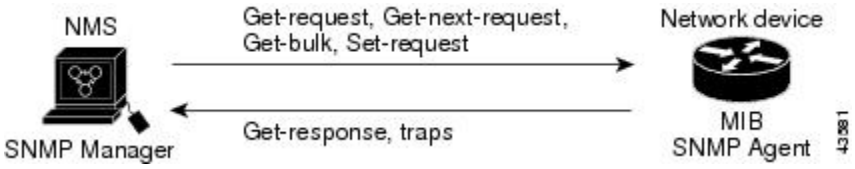
コミュニティ ストリングの設定, （721 ページ）

SNMP MIB 変数アクセス

NMS の例として、Cisco Prime Infrastructure ネットワーク管理ソフトウェアがあります。Cisco Prime Infrastructure 2.0 ソフトウェアは、スイッチ MIB 変数を使用して装置変数を設定し、ネットワーク上の装置をポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

次の図に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対し、トラップ（特定イベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス トラッキングなどの状況を SNMP マネージャに通知します。SNMP エージェントはさらに、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送信される MIB 関連のクエリに応答します。

図 *45* : *SNMP* ネットワーク



SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、スイッチから SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、トラップまたは情報を選択するオプションがコマンドにない限り、キーワード traps はトラップ、情報、またはその両方を表します。**snmp-server host** コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

（注） SNMPv1 は informs をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうかが送信側にわからないからです。情報要求の場合、受信した SNMP マネージャは SNMP 応答プロトコル データ ユニット（PDU）でメッセージを確認します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。再送信できるので、情報の方がトラップより意図した宛先に届く可能性が高くなります。

情報の方がトラップより信頼性が高いのは、スイッチおよびネットワークのリソースを多く消費するという特性にも理由があります。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は 1 回限りですが、情報は数回にわたって再送信つまり再試行が可能です。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。

したがって、トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。SNMP マネージャですべての通知を受信することが重要な場合は、情報要求を使用してください。ネットワークまたはスイッチのメモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

関連トピック

SNMP 通知の設定，（730 ページ）

SNMP ステータスのモニタリング，（744 ページ）

SNMP ifIndex MIB オブジェクト値

SNMP エージェントの IF-MIB モジュールがリブート後すぐに起動されます。さまざまな物理インターフェイス ドライバが IF-MIB モジュールの登録を初期化されているように、「インデックス番号をください」と示します。IF-MIB モジュールが先着順で使用可能な次の ifIndex 番号を割り当てます。つまり、1 つのリブートから他のリブートへのドライバの初期化順序のマイナーな違いが、同じ物理インターフェイスにリブートを行う以前のものとは別のインデックス番号を取得する可能性があるということです（インデックス持続が有効化されていない限り）。

SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル[4]
SNMP トラップ レシーバ	未設定
SNMP トラップ	TCP 接続のトラップ（tty）以外は、イネーブルではありません。
SNMP バージョン	バージョン キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで **noauth**（noAuthNoPriv）になります。
SNMP 通知タイプ	タイプが指定されていない場合、すべての通知が送信されます。

4 これは、スイッチが起動し、スタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが設定されていない場合のデフォルトです。

SNMP 設定時の注意事項

スイッチが起動し、スイッチのスタートアップ コンフィギュレーションに少なくとも 1 つの **snmp-server** グローバル コンフィギュレーション コマンドが設定されている場合、SNMP エージェントはイネーブルになります。

SNMP グループは、SNMP ユーザを SNMP ビューに対応付けるテーブルです。SNMP ユーザは、SNMP グループのメンバです。SNMP ホストは、SNMP トラップ動作の受信側です。SNMP エンジン *ID* は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP グループを設定するときには、次の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しません。**snmp-server host** グローバル コンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザを対応するグループに追加します。グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。
- リモートユーザを設定する場合は、ユーザが存在するデバイスのリモートSNMPエージェントに対応する IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモート ユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドを **remote** オプションとともに使用して、SNMP エンジン ID を設定してください。リモート エージェントの SNMP エンジン ID およびユーザ パスワードを使用して認証およびプライバシー ダイジェストが算出されます。先にリモート エンジン ID を設定しておかないと、コンフィギュレーション コマンドがエラーになります。
- SNMP情報を設定するときには、プロキシ要求または情報の送信先となるリモートエージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。
- ローカル ユーザがリモート ホストと関連付けられていない場合、スイッチは **auth**（authNoPriv）および **priv**（authPriv）の認証レベルの情報を送信しません。
- SNMP エンジン ID の値を変更すると、重大な影響が生じます。（コマンド ラインで入力された）ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて、MD5 またはSHA セキュリティ ダイジェストに変換されます。コマンドラインのパスワードは、RFC 2274 の規定に従って廃棄されます。このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合はSNMPv3ユーザのセキュリティ ダイジェストが無効となり、**snmp-server user***username* グローバル コンフィギュレーション コマンドを使用して、SNMPユーザを再設定する必要があります。エンジン ID を変更した場合は、同様の制限によってコミュニティ ストリングも再設定する必要があります。

関連トピック

SNMP グループおよびユーザの設定, （724 ページ）

SNMP ステータスのモニタリング, （744 ページ）

SNMP の設定方法

SNMP エージェントのディセーブル化

no snmp-server グローバル コンフィギュレーション コマンドは、デバイス上で実行している SNMP エージェントのすべてのバージョン（バージョン 1、バージョン 2C、バージョン 3）をディセーブルにします。入力した最初の **snmp-server** グローバル コンフィギュレーション コマンドによっ

て、SNMP エージェントのすべてのバージョンを再度イネーブルにします。特に SNMP をイネーブルにするために指定された Cisco IOS コマンドはありません。

SNMP エージェントをディセーブルにするには、次の手順を実行します。

はじめる前に

SNMP エージェントをディセーブルにする前にイネーブルにする必要があります。デバイス上で入力した最初の **snmp-server** グローバル コンフィギュレーション コマンドによって SNMP エージェントがイネーブルになります。

手順の概要

1. **enable**
2. **configureterminal**
3. **no snmp-server**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no snmp-server** 例： `スイッチ(config)# no snmp-server`	SNMP エージェント動作をディセーブルにします。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

SNMP エージェント機能，（716 ページ）
SNMP ステータスのモニタリング，（744 ページ）

コミュニティ ストリングの設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングは、スイッチ上のエージェントへのアクセスを許可する、パスワードと同様の役割を果たします。ストリングに対応する次の特性を 1 つまたは複数指定することもできます。

- コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限

スイッチ上でコミュニティ ストリングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server community***string*[**view***view-name*][**ro**|**rw**][*access-list-number*]
4. **access-list***access-list-number*{**deny**|**permit**}*source*[*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server community***string*[**view***view-name*][**ro**|**rw**][*access-list-number*] 例： `スイッチ(config)# snmp-server community comaccess ro 4`	コミュニティ ストリングを設定します。 （注） コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。 • *string* には、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。任意の長さのコミュニティ ストリングを 1 つまたは複数設定できます。 • （任意）**view** には、コミュニティがアクセスできるビュー レコードを指定します。 • （任意）許可された管理ステーションで MIB オブジェクトを取得する場合は読み取り専用（**ro**）、許可された管理ステーションで MIB オブジェクトを取得およ

	コマンドまたはアクション	目的
		び変更する場合は読み書き（**rw**）を指定します。デフォルトでは、コミュニティストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 • （任意）*access-list-number* には、1 ～ 99 および 1300 ～ 1999 の標準 IP アクセスリスト番号を入力します。
ステップ 4	**access-list***access-list-number*{**deny**|**permit**}*source*[*source-wildcard*] 例： `スイッチ(config)# access-list 4 deny any`	（任意）ステップ 3 で標準 IP アクセス リスト番号を指定してリストを作成した場合は、必要に応じてコマンドを繰り返します。 • *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、コミュニティストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します（コミュニティ ストリングに値を入力しないでください）。

特定のコミュニティ ストリングを削除するには、**no snmp-server** コミュニティ ストリング グローバル コンフィギュレーション コマンドを使用します。

スイッチのローカルまたはリモート SNMP サーバ エンジンを表す識別名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

関連トピック

SNMP コミュニティ ストリング，（716 ページ）

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモート SNMP サーバ エンジンを表す識別名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

スイッチ上の SNMP グループとユーザを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server engineID** {**local***engineid-string*|**remote***ip-address*[**udp-port***port-number*]*engineid-string*}
4. **snmp-server group***group-name*{**v1**|**v2c**|**v3**{**auth**|**noauth**|**priv**}}[**read***readview*][**write***writeview*][**notify***notifyview*][**access***access-list*]
5. **snmp-server user***username groupname*{**remote***host*[**udp-port***port*]}{**v1**[**access***acl*]|**v2c**[**access***acl*]|**v3**[**encrypted**][**access***acl*][**auth**{**md5**|**sha**}*auth-password*][**priv**{**des**|**3des**|**aes**{**128**|**192**|**256**}}*priv-password*]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション
ステップ 1	**enable** 例： スイッチ> **enable**
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**
ステップ 3	**snmp-server engineID** {**local***engineid-string*|**remote***ip-address*[**udp-port***port-number*]*engineid-string*} 例： スイッチ(config)# **snmp-server engineID local 1234**

	コマンドまたはアクション
ステップ 4	**snmp-server group***group-name*{**v1**|**v2c**|**v3**{**auth**|**noauth**|**priv**}}[**read***readview*][**write***writeview*][**notify***notifyview*][**access***access-list*] 例： スイッチ(config)# **snmp-server group public v2c access lmnop**

	コマンドまたはアクション
ステップ 5	**snmp-server user***username group-name* {**remote***host* [**udp-port***port*]} {**v1** [**access***access-list*]|**v2c** [**access***access-list*]|**v3** [**encrypted**] [**access***access-list* 例： スイッチ(config)# **snmp-server user Pat public v2c**

	コマンドまたはアクション

	コマンドまたはアクション
ステップ 6	**end** 例： スイッチ(config)# **end**
ステップ 7	**show running-config** 例： スイッチ# **show running-config**
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**

関連トピック

SNMP 設定時の注意事項，（718 ページ）
SNMP ステータスのモニタリング，（744 ページ）

SNMP 通知の設定

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生したときにスイッチが生成するシステム アラートです。デフォルトでは、トラップ マネージャは定義されず、トラップは送信されません。この Cisco IOS Release が稼働しているスイッチでは、トラップ マネージャを無制限に設定できます。

（注） コマンド構文で **traps** というワードを使用するコマンドは多数あります。トラップまたは情報を選択するオプションがコマンドにない限り、キーワード **traps** はトラップ、情報のいずれか、またはその両方を表します。**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

snmp-server enable traps グローバル コンフィギュレーション コマンドを **snmp-server host** グローバル コンフィギュレーション コマンドと組み合わせて使用すると、次の表に示す通知タイプを特定のホストで受信できます。これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定できます。

（注） **snmp-server enable traps** コマンドは、デバイスのローカル認証のためのトラップをサポートしていません。

表 *48*：デバイスの通知タイプ

通知タイプのキーワード	説明
bridge	STP ブリッジ MIB トラップを生成します。
クラスタ	クラスタ設定が変更された場合に、トラップを生成します。
config	SNMP 設定が変更された場合に、トラップを生成します。
copy-config	SNMP コピー設定が変更された場合に、トラップを生成します。
cpu threshold	CPU に関連したトラップをイネーブルにします。
entity	SNMP エンティティが変更された場合に、トラップを生成します。

通知タイプのキーワード	説明
envmon	環境モニタ トラップを生成します。ファン、シャットダウン、ステータス、電源、温度の環境トラップのいずれかまたはすべてをイネーブルにできます。
flash	SNMP FLASH 通知を生成します。スイッチ スタックでは、オプションとして、フラッシュの追加または削除に関する通知をイネーブルにできます。このようにすると、スタックからスイッチを削除するか、またはスタックにスイッチを追加した場合に（物理的な取り外し、電源の再投入、またはリロードの場合に）、トラップが発行されます。
fru-ctrl	エンティティ現場交換可能ユニット（FRU）制御トラップを生成します。スイッチスタックでは、このトラップはスタックにおけるスイッチの挿入/取り外しを意味します。
hsrp	ホットスタンバイ ルータ プロトコル（HSRP）が変更された場合に、トラップを生成します。
ipmulticast	IP マルチキャスト ルーティングが変更された場合に、トラップを生成します。
mac-notification	MAC アドレス通知のトラップを生成します。
ospf	Open Shortest Path First（OSPF）が変更された場合に、トラップを生成します。シスコ固有、エラー、リンクステート アドバタイズ、レート制限、再送信、ステート変更に関するトラップを任意にイネーブルにできます。
pim	Protocol-Independent Multicast（PIM）が変更された場合に、トラップを生成します。無効な PIM メッセージ、ネイバー変更、およびランデブー ポイント（RP）マッピングの変更に関するトラップを任意にイネーブルにできます。
port-security	SNMP ポート セキュリティ トラップを生成します。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。 （注） 通知タイプ **port-security** を使用してトラップを設定する際に、まずポートセキュリティ トラップを設定して、次に以下のポートセキュリティ トラップ レートを設定します。 **1 snmp-server enable trapsport-security** **2 snmp-server enable trapsport-securitytrap-rate***rate*

通知タイプのキーワード	説明
snmp	認証、コールド スタート、ウォーム スタート、リンク アップ、またはリンク ダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 1000 です。デフォルトは 0 に設定されています（制限なしの状態では、発生ごとにトラップが送信されます）。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP の Syslog トラップを生成します。
tty	TCP 接続のトラップを生成します。このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバーシップが変更された場合に、トラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN トランキング プロトコル（VTP）が変更された場合に、トラップを生成します。

ホストにトラップまたは情報を送信するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server engineID remote***ip-addressengineid-string*
4. **snmp-server user***usernamegroup-name*{**remote***host*[**udp-port***port*]}{**v1**[**access***access-list*]|**v2c**[**access***access-list*]|**v3**[**encrypted**][**access***access-list*][**auth**{**md5**|**sha**}*auth-password*}
5. **snmp-server group***group-name*{**v1**|**v2c**|**v3**{**auth**|**noauth**|**priv**}}[**read***readview*][**write***writeview*][**notify***notifyview*][**access***access-list*]
6. **snmp-server host***host-addr*[**informs**|**traps**][**version**{**1**|**2c**|**3**{**auth**|**noauth**|**priv**}}]*community-string*[*notification-type*]
7. **snmp-server enable traps***notification-types*
8. **snmp-server trap-source***interface-id*
9. **snmp-server queue-length***length*
10. **snmp-server trap-timeout***seconds*
11. **end**
12. **show running-config**
13. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション
ステップ 1	**enable** 例： スイッチ> **enable**
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**
ステップ 3	**snmp-server engineID remote***ip-addressengineid-string* 例： スイッチ(config)# **snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b**
ステップ 4	**snmp-server user***usernamegroup-name*{**remote***host*[**udp-port***port*]}{**v1**[**access***access-list*]|**v2c**[**access***access-list*]|**v3**[**encrypted**][**access***access-lis* 例： スイッチ(config)# **snmp-server user Pat public v2c**

	コマンドまたはアクション
ステップ 5	**snmp-server group***group-name*{**v1**|**v2c**|**v3**{**auth**|**noauth**|**priv**}}[**read***readview*][**write***writeview*][**notify***notifyview*][**access***access-list*] 例： スイッチ(config)# **snmp-server group public v2c access lmnop**
ステップ 6	**snmp-server host***host-addr*[**informs**|**traps**][**version**{**1**|**2c**|**3**{**auth**|**noauth**|**priv**}}]*community-string*[*notification-type*] 例： スイッチ(config)# **snmp-server host 203.0.113.1 comaccess snmp**

	コマンドまたはアクション
ステップ 7	**snmp-server enable traps***notification-types* 例： スイッチ(config)# **snmp-server enable traps snmp**
ステップ 8	**snmp-server trap-source***interface-id* 例： スイッチ(config)# **snmp-server trap-source GigabitEthernet1/0/1**

	コマンドまたはアクション
ステップ 9	**snmp-server queue-length***length* 例： スイッチ(config)# **snmp-server queue-length 20**
ステップ 10	**snmp-server trap-timeout***seconds* 例： スイッチ(config)# **snmp-server trap-timeout 60**
ステップ 11	**end** 例： スイッチ(config)# **end**
ステップ 12	**show running-config** 例： スイッチ# **show running-config**
ステップ 13	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**

次の作業

snmp-server host コマンドでは、通知を受信するホストを指定します。**snmp-server enable trap** コマンドによって、指定された通知方式（トラップおよび情報）がグローバルでイネーブルになります。ホストが情報を受信できるようにするには、そのホストに対応する **snmp-server host informs** コマンドを設定し**snmp-server enable traps** コマンドを使用して情報をグローバルにイネーブルにする必要があります。

指定したホストがトラップを受信しないようにするには、**no snmp-server host***host* グローバル コンフィギュレーション コマンドを使用します。キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** グローバル コンフィギュレーション コマンドを使用してください。特定のトラップ タイプをディセーブルにするには、**no snmp-server enable traps***notification-types* グローバル コンフィギュレーション コマンドを使用します。

関連トピック

SNMP 通知, （717 ページ）

SNMP ステータスのモニタリング, （744 ページ）

エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム接点およびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server contact***text*
4. **snmp-server location***text*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server contact***text* 例： スイッチ(config)# **snmp-server contact Dial System Operator at beeper 21555**	システムの連絡先文字列を設定します。
ステップ 4	**snmp-server location***text* 例： スイッチ(config)# **snmp-server location Building 3/Room 222**	システムの場所を表す文字列を設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP を通して使用する TFTP サーバの制限

SNMP を介したコンフィギュレーション ファイルの保存とロードに使用する TFTP サーバを、アクセス リストで指定されたサーバに限定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server tftp-server-list***access-list-number*
4. **access-list***access-list-number*{**deny**|**permit**}*source*[*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server tftp-server-list***access-list-number* 例： スイッチ(config)# **snmp-server tftp-server-list 44**	SNMP を介したコンフィギュレーション ファイルのコピーに使用する TFTP サーバを、アクセス リストのサーバに限定します。 *access-list-number* には、1 ～ 99 および 1300 ～ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 4	**access-list***access-list-number* {**deny**|**permit**} *source* [*source-wildcard*] 例： スイッチ(config)# **access-list 44 permit 10.1.1.2**	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 *source* には、スイッチにアクセスできる TFTP サーバの IP アドレスを入力します。 （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP のトラップフラグの設定

手順の概要

1. **configureterminal**
2. **trapflags ap** { **interfaceup | register**}
3. **trapflags client** {**dot11 | excluded**}
4. **trapflags dot11-security** {**ids-sig-attack | wep-decrypt-error**}
5. **trapflags mesh**
6. **trapflags rogueap**
7. **trapflags rrm-params** {**channels | tx-power**}
8. **trapflags rrm-profile** {**coverage | interference | load | noise**}
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**trapflags ap** { **interfaceup** | **register**} 例： スイッチ(config)# **trapflags ap interfaceup**	AP 関連トラップの送信をイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの **no** 形式を使用します。 • interfaceup：Cisco AP インターフェイス（A または B）が起動したときにトラップをイネーブルにします。 • register：Cisco AP が Cisco スイッチ に登録するときにトラップをイネーブルにします。
ステップ 3	**trapflags client** {**dot11** | **excluded**} 例： スイッチ(config)# **trapflags client excluded**	クライアント関連 DOT11 トラップの送信をイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの **no** 形式を使用します。 • dot11：クライアントの DOT11 トラップをイネーブルにします。 • excluded：クライアント用の除外されたトラップをイネーブルにします。
ステップ 4	**trapflags dot11-security** {**ids-sig-attack** | **wep-decrypt-error**} 例： スイッチ(config)# **trapflags dot11-security wep-decrypt-error**	802.11 セキュリティ関連トラップの送信をイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの **no** 形式を使用します。 • ids-sig-attack：IDS シグニチャ攻撃トラップをイネーブルにします。 • wep-decrypt-error：クライアントの WEP 復号化エラーのトラップをイネーブルにします。
ステップ 5	**trapflags mesh** 例： スイッチ(config)# **trapflags mesh**	メッシュのトラップをイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 6	**trapflags rogueap** 例： スイッチ(config)# **trapflags rogueap**	不正 AP 検出のトラップをイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
ステップ 7	**trapflags rrm-params** {**channels** | **tx-power**} 例： スイッチ(config)# **trapflags rrm-params tx-power**	RRM-parameter 更新関連トラップの送信をイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの **no** 形式を使用します。 • channels：RF マネージャが自動的に Cisco AP インターフェイスのチャネル番号を変更するときにトラップをイネーブルにします。 • tx-power：RF マネージャが自動的に Cisco AP インターフェイスの Tx-Power レベルを変更するときにトラップをイネーブルにします。
ステップ 8	**trapflags rrm-profile** {**coverage** | **interference** | **load** | **noise**} 例： スイッチ(config)# **trapflags rrm-profile interference**	RRM-Profile 関連トラップの送信をイネーブルにします。トラップ フラグをディセーブルにするには、このコマンドの **no** 形式を使用します。 • coverage：RF マネージャによって保持されるカバレッジ プロファイルでエラーが発生したときにトラップをイネーブルにします。 • interference：RF マネージャによって保持される干渉プロファイルでエラーが発生したときにトラップをイネーブルにします。 • load：RF マネージャによって保持される負荷プロファイルでエラーが発生したときにトラップをイネーブルにします。 • noise：RF マネージャによって保持されるノイズ プロファイルでエラーが発生したときにトラップをイネーブルにします。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

SNMP ワイヤレス トラップ通知のイネーブル化

手順の概要

1. **configureterminal**
2. **snmp-server enable traps wireless** [**AP** | **RRM** | **bsn80211SecurityTrap** | **bsnAPParamUpdate** | **bsnAPProfile** | **bsnAccessPoint** | **bsnMobileStation** | **bsnRogue** | **client** | **mfp** | **rogue**]
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server enable traps wireless** [**AP** | **RRM** | **bsn80211SecurityTrap** | **bsnAPParamUpdate** | **bsnAPProfile** | **bsnAccessPoint** | **bsnMobileStation** | **bsnRogue** | **client** | **mfp** | **rogue**] 例： スイッチ(config)# **snmp-server enable traps wireless AP**	SNMP ワイヤレス トラップ通知をイネーブルにします。 • AP：アクセス ポイント トラップをイネーブルにします。 • RRM：RRM トラップをイネーブルにします。 • bsn80211SecurityTrap：セキュリティ関連のトラップをイネーブルにします。 • bsnAPParamUpdate：更新される AP パラメータのトラップをイネーブルにします。 • bsnAPProfile：BSN AP プロファイル トラップをイネーブルにします。 • bsnAccessPoint：BSN アクセス ポイント トラップをイネーブルにします。 • bsnMobileStation：ワイヤレス クライアント トラップを制御します。 • bsnRogue：BSN 不正関連トラップをイネーブルにします。 • client：クライアント トラップをイネーブルにします。 • mfp：MFP トラップをイネーブルにします。 • rogue：不正関連トラップをイネーブルにします。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

SNMP ステータスのモニタリング

不正なコミュニティ ストリング エントリ、エラー、要求変数の数など、SNMP の入出力統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。また、次の表にリストされたその他の特権 EXEC コマンドを使用して、SNMP 情報を表示することもできます。

表 *49* : ***SNMP*** 情報を表示するためのコマンド

コマンド	目的
show snmp	SNMP 統計情報を表示します。
	デバイスに設定されているローカル SNMP エンジンおよびすべてのリモートエンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求の情報を表示します。
show snmp sessions	現在の SNMP セッションの情報を表示します。
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。 （注） このコマンドは、**auth** | **noauth** | **priv** モードの SNMPv3 設定情報を表示するときに使用する必要があります。この情報は、**show running-config** の出力には表示されません。

関連トピック

SNMP エージェントのディセーブル化, （719 ページ）
SNMP エージェント機能, （716 ページ）
SNMP グループおよびユーザの設定, （724 ページ）
SNMP 設定時の注意事項, （718 ページ）
SNMP 通知の設定, （730 ページ）
SNMP 通知, （717 ページ）

SNMP の例

次に、SNMP のすべてのバージョンをイネーブルにする例を示します。この設定では、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定では、スイッチ はトラップを送信しません。

```
スイッチ(config)# snmp-server community public
```

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。スイッチはさらに、SNMPv1 を使用してホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に VTP トラップを送信します。コミュニティ ストリング *public* は、トラップとともに送信されます。

```
スイッチ(config)# snmp-server community public
スイッチ(config)# snmp-server enable traps vtp
スイッチ(config)# snmp-server host 192.180.1.27 version 2c public
スイッチ(config)# snmp-server host 192.180.1.111 version 1 public
スイッチ(config)# snmp-server host 192.180.1.33 public
```

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証障害トラップは、SNMPv2C がコミュニティ ストリング *public* を使用してホスト *cisco.com* に送信します。

```
スイッチ(config)# snmp-server community comaccess ro 4
スイッチ(config)# snmp-server enable traps snmp authentication
スイッチ(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは制限されます。1行めで、スイッチはすでにイネーブルになっているトラップ以外に、エンティティ MIB トラップを送信できるようになります。2 行目はこれらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の **snmp-server** ホスト コマンドを無効にします。

```
スイッチ(config)# snmp-server enable traps entity
スイッチ(config)# snmp-server host cisco.com restricted entity
```

次に、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする例を示します。

```
スイッチ(config)# snmp-server enable traps
スイッチ(config)# snmp-server host myhost.cisco.com public
```

次に、ユーザとリモート ホストを関連付けて、ユーザがグローバル コンフィギュレーション モードのときに **auth**（authNoPriv）認証レベルで情報を送信する例を示します。

```
スイッチ(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
スイッチ(config)# snmp-server group authgroup v3 auth
スイッチ(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
スイッチ(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
スイッチ(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
スイッチ(config)# snmp-server enable traps
スイッチ(config)# snmp-server inform retries 0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
SNMP コマンド	*Network Management Command Reference, Cisco IOS XE Release 3E*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	-

MIB

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

シスコのテクニカル サポート

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

簡易ネットワーク管理プロトコルの機能の履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 45 章

サービス レベル契約の設定

この章では、スイッチで Cisco IOS IP サービス レベル契約（SLA）を使用する方法について説明します。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチまたはスイッチ スタックを意味します。

- 機能情報の確認，749 ページ
- SLA の制約事項，750 ページ
- SLA について，750 ページ
- IP SLA 動作の設定方法，756 ページ
- IP SLA 動作のモニタリング，770 ページ
- IP SLA 動作のモニタリングの例，771 ページ
- その他の参考資料，772 ページ

機能情報の確認

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

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

SLA の制約事項

ここでは、SLA の制約事項を示します。

次に示すのは、IP SLA ネットワーク パフォーマンス測定の制約事項です。

- スイッチは、ゲートキーパー登録遅延動作測定を使用した Voice over IP（VoIP）サービス レベルはサポートしていません。
- Cisco IOS デバイスだけが宛先 IP SLA Responder の送信元になります。
- 他社製のデバイスに IP SLA Responder を設定することはできません。また、Cisco IOS IP SLA はこれらのデバイス固有のサービスに対してだけ動作パケットを送信できます。

関連トピック

IP SLA ネットワーク パフォーマンス測定の実装, （759 ページ）

Cisco IOS IP SLA でのネットワーク パフォーマンスの測定, （751 ページ）

IP SLA レスポンダおよび IP SLA 制御プロトコル, （752 ページ）

SLA について

Cisco IOS IP サービス レベル契約（SLA）

Cisco IOS IP SLA はネットワークにデータを送信し、複数のネットワーク ロケーション間あるいは複数のネットワーク パス内のパフォーマンスを測定します。Cisco IOS IP SLA は、ネットワーク データおよび IP サービスをシミュレーションし、ネットワーク パフォーマンス情報をリアルタイムで収集します。Cisco IOS IP SLA は、Cisco IOS デバイス間のトラフィックまたは Cisco IOS デバイスからネットワーク アプリケーション サーバのようなリモート IP デバイスへのトラフィックを生成し、分析します。さまざまな Cisco IOS IP SLA 動作で評価を実行し、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用します。

Cisco IOS IP SLA 動作に応じてシスコ デバイスのネットワーク パフォーマンス統計情報がモニタリングされ、コマンドライン インターフェイス（CLI）MIB および簡易ネットワーク管理プロトコル（SNMP）MIB に格納されます。IP SLA パケットには設定可能な IP レイヤおよびアプリケーション層のオプションがあります。たとえば、発信元および宛先 IP アドレス、ユーザ データグラム プロトコル（UDP）/TCP ポート番号、タイプ オブ サービス（ToS）バイト（DiffServ コード ポイント（DSCP）および IP プレフィックス ビットを含む）、VPN ルーティング/転送インスタンス（VRF）、URL Web アドレスなどが設定できます。

Cisco IP SLA はレイヤ 2 転送に依存していないので、異なるネットワーク間にエンドツーエンド動作を設定してエンド ユーザが経験しそうなメトリックを最大限に反映させることができます。IP SLA は、次のパフォーマンス メトリックを収集して分析するために、。

- 遅延（往復および一方向）
- ジッタ（方向性あり）

- パケット損失（方向性あり）
- パケット シーケンス（パケット順序）
- パス（ホップ単位）
- 接続（方向性あり）
- サーバまたは Web サイトのダウンロード時間

Cisco IP SLA は SNMP によるアクセスが可能なので、Cisco Prime Internetwork Performance Monitor（IPM）やサードパーティ製パフォーマンス管理製品などのパフォーマンス モニタリング アプリケーションでも使用できます。

IP SLA を使用すると、次の利点が得られます。

- SLA モニタリング、評価、検証。
- ネットワーク パフォーマンス モニタリング。
  - ネットワークのジッター、遅延、パケット損失の測定。
  - 連続的で信頼性のある予測可能な測定。
- IP サービス ネットワーク ヘルス アセスメントにより、既存の QoS が新しい IP サービスに適していることを確認できる。
- 端末間のネットワーク アベイラビリティをモニタリングして、ネットワーク リソースをあらかじめ検証し接続をテストできる（たとえば、ビジネス上の重要なデータを保存する NFS サーバのネットワーク アベイラビリティをリモート サイトから確認できる）。
- 問題をすぐに認識し、トラブルシューティングにかかる時間を短縮できる一貫性のある信頼性の高い測定によるネットワーク動作のトラブルシューティング。
- マルチプロトコル ラベル スイッチング（MPLS）パフォーマンス モニタリングとネットワークの検証を行う（スイッチが MPLS をサポートする場合）。

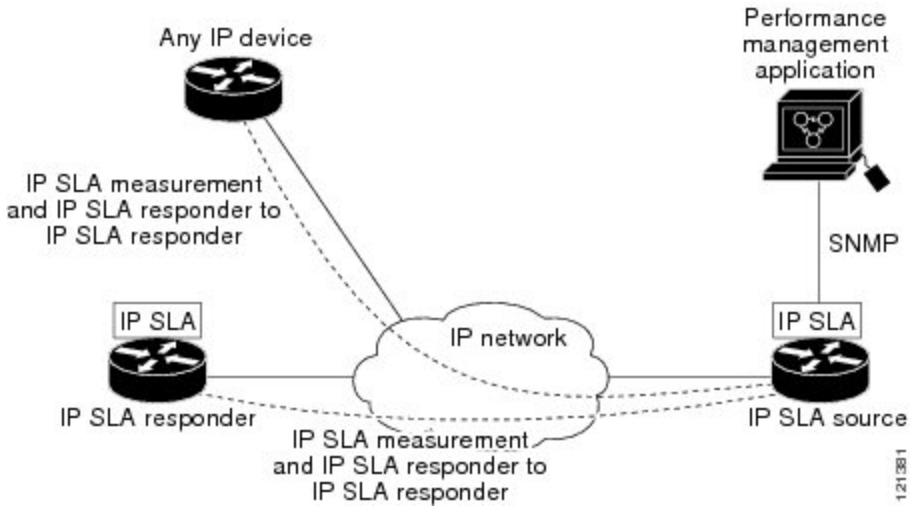
Cisco IOS IP SLA でのネットワーク パフォーマンスの測定

IP SLA を使用して、プローブを物理的に配置せずに、コア、分散、エッジといったネットワーク内の任意のエリア間のパフォーマンスをモニタリングすることができます。2 つのネットワーク デバイス間のネットワーク パフォーマンスは、生成トラフィックで測定します。

次の図に、送信元デバイスが宛先デバイスに生成パケットを送信するときに IP SLA が開始される手順を示します。宛先デバイスがパケットを受信すると、IP SLA 動作の種類によって、送信元のタイム スタンプ情報に応じてパフォーマンス メトリックを算出します。IP SLA 動作は、特定の

プロトコル（UDP など）を使用してネットワークの送信元から宛先へのネットワーク測定を行います。

図 *46*：*Cisco IOS IP SLA* 動作



関連トピック

IP SLA ネットワーク パフォーマンス測定の実装，（759 ページ）

SLA の制約事項，（750 ページ）

IP SLA レスポンダおよび IP SLA 制御プロトコル

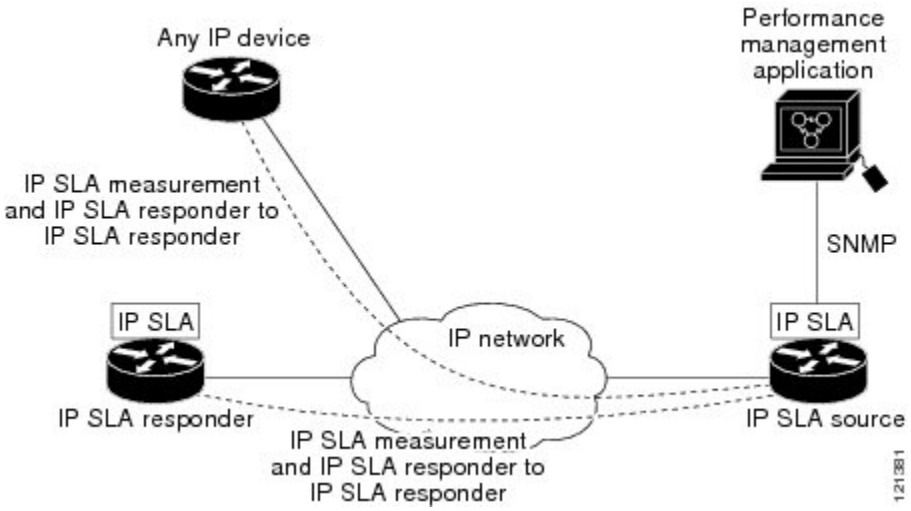
IP SLA レスポンダは宛先 Cisco デバイスに組み込まれたコンポーネントで、システムが IP SLA 要求パケットを予想して応答します。Responderは専用プローブなしで正確な測定を行います。レスポンダは、受信および応答するポートが通知されるメカニズムを Cisco IOS IP SLA コントロールプロトコルを通じて実現します。

（注） IP SLA レスポンダはレスポンダ設定可能なスイッチである Cisco IOS レイヤ 2 にすることもできます。レスポンダは、IP SLA 機能を全面的にサポートする必要はありません。

次の図は、IP ネットワーク内での Cisco IOS IP SLA レスポンダの配置場所を示します。レスポンダは、IP SLA 動作から送信されたコントロール プロトコル メッセージを指定されたポートで受信します。コントロール メッセージを受信したら、指定された UDP または TCP ポートを指定された時間だけイネーブルにします。この間に、レスポンダは要求を受け付け、応答します。レス

ポンダは、IP SLA パケットに応答した後または指定の時間が経過したら ポートをディセーブルにします。セキュリティの向上のために、コントロール メッセージではMD5 認証が利用できます。

図 *47*：*Cisco IOS IP SLA* 動作



すべての IP SLA 動作に対して宛先デバイスのレスポンダをイネーブルにする必要はありません。たとえば、宛先ルータが提供しているサービス（Telnet や HTTP など）は Responder では必要ありません。

関連トピック

SLA の制約事項, （750 ページ）

IP SLA の応答時間の計算

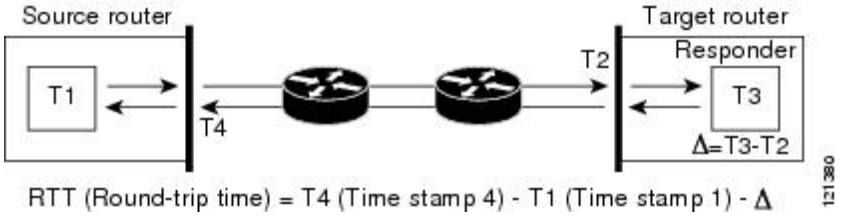
スイッチ、コントローラ、ルータは、他のハイ プライオリティ プロセスがあるために、着信パケットの処理に数十ミリ秒かかることがあります。この遅延により応答時間が影響を受けます。テストパケットの応答が処理待ちのキューに入っていることもあるからです。この場合、応答時間は正しいネットワーク遅延を反映しません。IP SLA はソース デバイスとターゲット デバイス（レスポンダが使用されている場合）の処理遅延を最小化し、正しいラウンドトリップ時間（RTT）を識別します。IP SLA テスト パケットは、タイム スタンプによって処理遅延を最小化します。

IP SLA レスポンダがイネーブルの場合、パケットが割り込みレベルでインターフェイスに着信したときおよびパケットが出て行くときにターゲットデバイスでタイム スタンプを付け、処理時間は含めません。タイム スタンプはサブミリ秒単位で構成されます。

次の図は、レスポンダの動作を示します。RTT を算出するためのタイム スタンプが 4 つ付けられます。ターゲット ルータでレスポンダ機能がイネーブルの場合、タイム スタンプ 3（TS3）からタイム スタンプ 2（TS2）を引いてテストパケットの処理にかかった時間を求め、デルタ（Δ）で表します。次に全体の RTT からこのデルタの値を引きます。IP SLA により、この方法はソース

ルータにも適用されます。その場合、着信タイム スタンプ 4（TS4）が割り込みレベルで付けられ、より正確な結果を得ることができます。

図 *48*：*Cisco IOS IP SLA* レスポンダ タイム スタンプ



この他にも、ターゲット デバイスに 2 つのタイム スタンプがあれば一方向遅延、ジッタ、方向性を持つパケット損失がトラッキングできるという利点があります。大半のネットワーク動作は非同期なので、このような統計情報があるのは問題です。ただし一方向遅延測定を取り込むには、ソース ルータとターゲット ルータの両方にネットワーク タイム プロトコル（NTP）を設定し、両方のルータを同じくロック ソースに同期させる必要があります。一方向ジッタ測定にはクロック同期は不要です。

IP SLA 動作のスケジューリング

IP SLA 動作を設定する場合、統計情報の取り込みとエラー情報の収集から開始するように動作をスケジューリングする必要があります。スケジューリングは、すぐに動作を開始する、または特定の月、日、時刻に開始するように設定できます。また、*pending* オプションを使用して、あとで動作を開始するように設定することもできます。pending オプションは動作の内部状態に関するもので、SNMP で表示できます。トリガーを待機する反応（しきい値）動作の場合も pending オプションを使用します。1 度に 1 つの IP SLA 動作をスケジューリングしたり、グループの動作をスケジューリングすることもできます。

Cisco IOS CLI または CISCO RTTMON-MIB で 1 つのコマンドを使用して、複数の IP SLA 動作をスケジューリングできます。等間隔で動作を実行するようにスケジューリングすると、IP SLA モニタリング トラフィックの数を制御できます。IP SLA 動作をこのように分散させると CPU 使用率を最小限に抑え、ネットワーク スケーラビリティを向上させることができます。

IP SLA 複数動作のスケジューリング機能の詳細については、『*Cisco IOS IP SLA Configuration Guide*』の「IP SLAs—Multiple Operation Scheduling」の章を参照してください。

IP SLA 動作のしきい値のモニタリング

サービス レベル契約モニタリングを正しくサポートするには、違反が発生した場合にすぐに通知されるメカニズムにする必要があります。IP SLA は次のような場合にイベントによってトリガーされる SNMP トラップを送信できます。

- 接続の損失
- タイムアウト
- RTT しきい値

- 平均ジッタしきい値
- 一方向パケット損失
- 一方向ジッタ
- 一方向平均オピニオン評点（MOS）
- 一方向遅延

IP SLA しきい値違反が発生した場合も、あとで分析するために別の IP SLA 動作がトリガーされます。たとえば、回数を増やしたり、Internet Control Message Protocol（ICMP）パス エコーや ICMP パス ジッター動作を開始してトラブルシューティングを行うことができます。

ICMP エコー

ICMP エコー動作は、シスコ デバイスと IP を使用するその他のデバイス間のエンドツーエンド応答時間を測定します。応答時間は、ICMP エコー要求メッセージを宛先に送信し、ICMP エコー応答を受信するのにかかる時間を測定して算出されます。多くのお客様は、IP SLA ICMP ベース動作、社内 ping テスト、またはこの応答所要時間を測定するために ping ベース専用プローブを使用します。IP SLA ICMP エコー動作は、ICMP ping テストと同じ仕様に準拠しており、どちらの方法でも同じ応答所要時間になります。

関連トピック

ICMP エコー動作を使用した IP サービス レベルの分析, （767 ページ）

UDP ジッター

ジッターとは、パケット間遅延の差異を説明する簡単な用語です。複数のパケットが送信元から宛先まで 10 ミリ秒の間隔で継続的に送信される場合、宛先は 10 ミリ秒間隔で受信します（ネットワークが正常に動作している場合）。しかし、ネットワークに遅延がある場合（キューイングや代替ルートを通じた到着など）、パケットの着信の間隔が 10 ミリ秒を超える場合や 10 ミリ秒未満になる場合があります。正のジッター値は、パケットが 10 ミリ秒を超える間隔で到着することを示します。負のジッター値は、パケットが 10 ミリ秒未満の間隔で到着することを示します。パケットの到着が 12 ミリ秒間隔の場合、正のジッター値は 2 ミリ秒です。8 ミリ秒間隔で到着する場合、負のジッター値は 2 ミリ秒です。遅延による影響を受けやすいネットワークの場合、正のジッタ値は望ましくありません。ジッタ値 0 が理想的です。

ジッターのモニタリング以外にも、IP SLA UDP ジッター動作を多目的データ収集動作に使用できます。IP SLA によって生成されるパケットは、データを送受信するパケットを含めて、送信元および動作ターゲットからシーケンス情報とタイム スタンプを伝送します。このデータに基づいて、UDP ジッター動作は次を測定します。

- 方向別ジッター（送信元から宛先へ、宛先から送信元へ）
- 方向別パケット損失
- 方向別遅延（一方向遅延）
- ラウンドトリップ遅延（平均 RTT）

データを送受信するパスが異なる場合もあるので（非同期）、方向別データを使用すればネットワークで発生している輻輳や他の問題の場所を簡単に突き止めることができます。

UDP ジッタ動作では合成（シミュレーション）UDP トラフィックを生成し、送信元ルータからターゲット ルータに多数の UDP パケットを送信します。その際の各パケットのサイズ、パケット同士の間隔、送信間隔は決められています。デフォルトでは、10バイトのペイロードサイズのパケット フレームを 10 ミリ秒で 10 個生成し、60 秒間隔で送信します。これらのパラメータは、提供する IP サービスを最適にシミュレートするように設定できます。

一方向遅延を正確に測定する場合、（NTP によって提供される）送信元デバイスとターゲット デバイス間のクロック同期が必要です。一方向ジッタおよびパケット損失を測定する場合は、クロック同期は不要です。送信元デバイスとターゲット デバイスの間でクロックが同期していない場合、一方向ジッターとパケット損失のデータは戻されますが、UDP ジッター動作による一方向遅延測定は 0 の値が戻ります。

関連トピック

UDP ジッター動作を使用した IP サービス レベルの分析, （763 ページ）

IP SLA 動作の設定方法

ここでは、利用可能なすべての動作の設定情報について説明されているわけではありません。設定情報の詳細については『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。ここでは、応答側の設定、UDP ジッター動作の設定（応答側が必要）、ICMP エコー動作の設定（応答側が不要）などの動作例を説明します。他の動作の設定の詳細については、次の URL の『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。

デフォルト設定

IP SLA 動作は設定されていません。

設定時の注意事項

IP SLA のコマンドについては、『*Cisco IOS IP SLA Command Reference, Release 12.4T*』のコマンド リファレンスを参照してください。

説明と設定手順の詳細については、『*Cisco IOS IP SLAs Configuration Guide, Release 12.4TL*』を参照してください。

ガイドに記載されている IP SLA コマンドまたは動作の中にはスイッチでサポートされないものもあります。スイッチでは、UDP ジッター、UDP エコー、HTTP、TCP 接続、ICMP エコー、ICMP パス エコー、ICMP パス ジッター、FTP、DNS、DHCP を使用する IP サービス レベル分析がサポートされます。また、複数動作スケジューリングおよび事前に設定されたしきい値のモニタリングもサポートされます。ゲートキーパー登録遅延動作測定を使用した Voice over IP（VoIP）サービス レベルはサポートしていません。

IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用してソフトウェア イメージで動作タイプがサポートされていることを確認してください。コマンド出力例は次のとおりです。

```
スイッチ# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

IP SLA レスポンダの設定

IP SLA レスポンダは、Cisco IOS ソフトウェアベース デバイスだけで利用可能です。これには、IP SLA 機能をフルにサポートしていない一部のレイヤ 2 スイッチも含まれます。

ターゲット デバイス（動作ターゲット）上の IP SLA 応答側を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sla responder** {**tcp-connect** |**udp-echo**}**ipaddress***ip-address***port***port-number*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sla responder** {**tcp-connect** |**udp-echo**}**ipaddress***ip-address***port***port-number* 例： スイッチ(config)# **ip sla responder udp-echo 172.29.139.134 5000**	スイッチを IP SLA レスポンダとして設定します。 キーワードの意味は次のとおりです。 • **tcp-connect**：レスポンダの TCP 接続動作をイネーブルにします。 • **udp-echo**：レスポンダの User Datagram Protocol（UDP）エコー動作またはジッター動作をイネーブルにします。 • **ipaddress***ip-address*：宛先 IP アドレスを入力します。 • **port***port-number*：宛先ポート番号を入力します。 （注） IP アドレスとポート番号は、IP SLA 動作のソース デバイスに設定した IP アドレスおよびポート番号と一致している必要があります。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA ネットワーク パフォーマンス測定の実装

スイッチ上でIP SLAネットワーク パフォーマンス測定を実施するには、次の手順を実行します。

はじめる前に

show ip sla application 特権 EXEC コマンドを使用して、ソフトウェア イメージで目的の動作タイプがサポートされていることを確認してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sla***operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port***port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval***interpacket-interval*]
5. **frequency***seconds*
6. **threshold***milliseconds*
7. **exit**
8. **ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**]
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip sla***operation-number* 例： スイッチ(config)# **ip sla 10**	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port***port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval***interpacket-interval*] 例： スイッチ(config-ip-sla)# **udp-jitter 172.29.139.134 5000**	IP SLA 動作を目的の動作タイプとして設定して（例では UDP ジッター動作が使用されています）、そのコンフィギュレーションモードを開始します（例では UDP ジッター コンフィギュレーション モードが使用されています）。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • *destination-port*：宛先ポート番号を 1 ～ 65535 の範囲で指定します。 •（任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 •（任意）**source-port***port-number*：送信元ポート番号を 1 ～ 65535 の範囲で指定します。ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 •（任意）**control**：IP SLA 制御メッセージの IP SLA レスポンダへの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA 制御メッセージは宛先デバイスに送信され、IP SLA レスポンダとの接続が確立されます。 •（任意）**num-packets***number-of-packets*：生成するパケット数を入力します。指定できる範囲は 1 ～ 6000 です。デフォルトは 10 です。 •（任意）**interval***inter-packet-interval*：パケットの送信間隔をミリ秒で入力します。指定できる範囲は 1 ～ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 5	**frequency***seconds* 例： スイッチ(config-ip-sla-jitter)# **frequency 45**	（任意）SLA 動作のオプションを設定します。次の例では、指定された IP SLA 動作が繰り返されるレートを設定します。指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。

	コマンドまたはアクション	目的
ステップ 6	**threshold***milliseconds* 例： スイッチ(config-ip-sla-jitter)# **threshold 200**	（任意）しきい値条件を設定します。次の例では、指定された IP SLA 動作のしきい値が 200 に設定されます。有効な範囲は 0 ～ 60000 ミリ秒です。
ステップ 7	**exit** 例： スイッチ(config-ip-sla-jitter)# **exit**	SLA 動作コンフィギュレーション モード（この例では UDP ジッター コンフィギュレーション モード）を終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**] 例： スイッチ(config)# **ip sla schedule 10 start-time now life forever**	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 •（任意）**life**：動作の実行を無制限（**forever**）に指定するか、特定の秒数（*seconds*）を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 •（任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24 時間表記）、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すると、開始時刻を指定するまでは情報を収集しません。 **now** と入力すると、ただちに動作を開始します。 **after***hh:mm:ss* と入力すると、指定した時刻の経過後に動作を開始します。 •（任意）**ageout***seconds*：情報を収集していないときのメモリの動作を保存する秒数を指定します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 •（任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

UDP ジッター コンフィギュレーション

次に、UDP ジッター IP SLA 動作の設定例を示します。

```
スイッチ(config)# ip sla 10
スイッチ(config-ip-sla)# udp-jitter 172.29.139.134 5000
スイッチ(config-ip-sla-jitter)# frequency 30
スイッチ(config-ip-sla-jitter)# exit
スイッチ(config)# ip sla schedule 5 start-time now life forever
スイッチ(config)# end
スイッチ# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

関連トピック

Cisco IOS IP SLA でのネットワーク パフォーマンスの測定, （751 ページ）

SLA の制約事項, （750 ページ）

UDP ジッター動作を使用した IP サービス レベルの分析

送信元デバイス上の UDP ジッタ動作を設定するには、次の手順を実行します。

はじめる前に

送信元デバイス上でUDPジッター動作を設定するには、ターゲットデバイス（動作ターゲット）で、IP SLA レスポンダをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sla***operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port***port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval***interpacket-interval*]
5. **frequency***seconds*
6. **exit**
7. **ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**]
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip sla***operation-number* 例： スイッチ(config)# **ip sla 10**	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port***port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval***interpacket-interval*] 例： スイッチ(config-ip-sla)# **udp-jitter 172.29.139.134 5000**	IP SLA 動作を UDP ジッター動作として設定し、UDP ジッター コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • *destination-port*：宛先ポート番号を 1 ～ 65535 の範囲で指定します。 •（任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 •（任意）**source-port***port-number*：送信元ポート番号を 1 ～ 65535 の範囲で指定します。ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 •（任意）**control**：IP SLA 制御メッセージの IP SLA レスポンダへの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA 制御メッセージは宛先デバイスに送信され、IP SLA レスポンダとの接続が確立されます。 •（任意）**num-packets***number-of-packets*：生成するパケット数を入力します。指定できる範囲は 1 ～ 6000 です。デフォルトは 10 です。 •（任意）**interval***inter-packet-interval*：パケットの送信間隔をミリ秒で入力します。指定できる範囲は 1 ～ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 5	**frequency***seconds* 例： スイッチ(config-ip-sla-jitter)# **frequency 45**	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： スイッチ(config-ip-sla-jitter)# **exit**	UDP ジッター コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**] 例： スイッチ(config)# **ip sla schedule 10 start-time now life forever**	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 •（任意）**life**：動作の実行を無制限（**forever**）に指定するか、特定の秒数（*seconds*）を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 •（任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24 時間表記）、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すると、開始時刻を指定するまでは情報を収集しません。 **now** と入力すると、ただちに動作を開始します。 **after***hh:mm:ss* と入力すると、指定した時刻の経過後に動作を開始します。 •（任意）**ageout***seconds*：情報を収集していないときのメモリの動作を保存する秒数を指定します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 •（任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 10	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

UDP ジッター IP SLA 動作の設定

次に、UDP ジッター IP SLA 動作の設定例を示します。

```
スイッチ(config)# ip sla 10
スイッチ(config-ip-sla)# udp-jitter 172.29.139.134 5000
スイッチ(config-ip-sla-jitter)# frequency 30
スイッチ(config-ip-sla-jitter)# exit
スイッチ(config)# ip sla schedule 5 start-time now life forever
スイッチ(config)# end
スイッチ# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

関連トピック

UDP ジッター，（755 ページ）

ICMP エコー動作を使用した IP サービス レベルの分析

送信元デバイス上の ICMP エコー動作を設定するには、次の手順を実行します。

はじめる前に

この動作では、IP SLA レスポンダ側を有効にしておく必要はありません。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sla***operation-number*
4. **icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface***interface-id*]
5. **frequency***seconds*
6. **exit**
7. **ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**]
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sla***operation-number* 例： スイッチ(config)# **ip sla 10**	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface***interface-id*] 例： `スイッチ(config-ip-sla)# icmp-echo 172.29.139.134`	IP SLA 動作を ICMP エコー動作として設定し、ICMP エコー コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 •（任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 •（任意）**source-interface***interface-id*：動作に対する送信元インターフェイスを指定します。
ステップ 5	**frequency***seconds* 例： `スイッチ(config-ip-sla-echo)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 6	**exit** 例： `スイッチ(config-ip-sla-echo)# exit`	UDP エコー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**] 例： `スイッチ(config)# ip sla schedule 5 start-time now life forever`	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 •（任意）**life**：動作の実行を無制限（**forever**）に指定するか、特定の秒数（*seconds*）を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 3600 秒（1 時間）です。 •（任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24時間表記）、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すると、開始時刻を指定するまでは情報を収集しません。 **now** と入力すると、ただちに動作を開始します。

	コマンドまたはアクション	目的
		after *hh:mm:ss* と入力すると、指定した時刻の経過後に動作を開始します。 • （任意）**ageout***seconds*：情報を収集していないときのメモリの動作を保存する秒数を指定します。指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 8	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ICMP エコー IP SLA 動作の設定

次に、ICMP エコー IP SLA 動作の設定例を示します。

```
スイッチ(config)# ip sla 12
スイッチ(config-ip-sla)# icmp-echo 172.29.139.134
スイッチ(config-ip-sla-echo)# frequency 30
スイッチ(config-ip-sla-echo)# exit
スイッチ(config)# ip sla schedule 5 start-time now life forever
スイッチ(config)# end
スイッチ# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
```

```
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

関連トピック

IP SLA 動作のしきい値のモニタリング, （754 ページ）

IP SLA 動作のモニタリング

次の表で、IP SLA 動作の設定と結果を表示するために使用するコマンドについて説明します。

表 *50*：*IP SLA* 動作のモニタリング

show ip sla application	Cisco IOS IP SLA のグローバル情報を表示します。
show ip sla authentication	IP SLA 認証情報を表示します。
show ip sla configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA動作に関する、デフォルト値をすべて含めた設定値を表示します。
show ip sla enhanced-history {**collection-statistics** | **distribution statistics**} [*entry-number*]	収集した履歴バケットの拡張履歴統計情報、あるいはすべての IP SLA 動作または特定の IP SLA 動作に関する分散統計情報を表示します。
show ip sla ethernet-monitor configuration [*entry-number*]	IP SLA 自動イーサネット設定を表示します。
show ip sla group schedule [*schedule-entry-number*]	IP SLA グループ スケジューリング設定と個別情報を表示します。

show ip sla history [*entry-number* | **full** | **tabular**]	すべての IP SLA 動作について収集した履歴を表示します。
show ip sla mpls-lsp-monitor {**collection-statistics** | **configuration** | **ldp operational-state** | **scan-queue** | **summary** [*entry-number*] | **neighbors**}	MPLS ラベル スイッチド パス（LSP）ヘルス モニタ動作を表示します。
show ip sla reaction-configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する、予防的しきい値のモニタリングの設定を表示します。
show ip sla reaction-trigger [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する反応トリガー情報を表示します。
show ip sla responder	IP SLA レスポンダ側の情報を表示します。
show ip sla statistics [*entry-number* | **aggregated** | **details**]	動作ステータスおよび統計情報の現在値または合計値を表示します。

IP SLA 動作のモニタリングの例

次の例は、アプリケーションごとのすべての IP SLA を示しています。

```
スイッチ# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

次の例は、すべての IP SLA ディストリビューション統計情報を示しています。

```
スイッチ# show ip sla enhanced-history distribution-statistics

Point by point Enhanced History
Entry    = Entry Number
Int      = Aggregation Interval
BucI     = Bucket Index
```

```
StartT   = Aggregation Start Time
Pth      = Path index
Hop      = Hop in path index
Comps    = Operations completed
OvrTh    = Operations completed over thresholds
SumCmp   = Sum of RTT (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry Int BucI StartT     Pth Hop Comps OvrTh SumCmp     SumCmp2L   SumCmp2H   T
Max    TMin
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco Medianet Metadata Guide	http://www.cisco.com/en/US/docs/ios-xml/ios/mdata/configuration/15-sy/mdata-15-sy-book.html#mdata_new.pdf
Cisco Media Services Proxy Configuration Guide	http://www.cisco.com/en/US/docs/ios-xml/ios/msp/configuration/15-mt/msp-15-mt-book.pdf
Cisco Mediatrace and Cisco Performance Monitor Configuration Guide	http://www.cisco.com/en/US/docs/ios-xml/ios/mcl_mmon/configuration/15-mt/mm-15-mt-book/mm-mediatrace.pdf

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	-

MIB

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

シスコのテクニカル サポート

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

第 46 章

ローカル ポリシーの設定

- 機能情報の確認，775 ページ
- ローカル ポリシーの設定に関する制限，775 ページ
- ローカル ポリシーの設定に関する情報，776 ページ
- ローカル ポリシーの設定方法，778 ページ
- ローカル ポリシーの監視，784 ページ
- 例：ローカル ポリシーの設定，785 ページ
- ローカル ポリシーの設定に関する追加情報，786 ページ
- ローカル ポリシーの設定の実行に関する機能履歴，787 ページ

機能情報の確認

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

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

ローカル ポリシーの設定に関する制限

スイッチ上でサポートされるポリシー マップ属性は、QoS、VLAN、セッション タイムアウト、および ACL です。

関連トピック

インターフェイス テンプレートの作成（CLI），（778 ページ）
パラメータ マップの作成（CLI），（779 ページ）
クラス マップの作成（CLI），（780 ページ）
ポリシー マップの作成（CLI），（781 ページ）
WLAN 上のデバイスのローカル ポリシーの適用（CLI），（782 ページ）
ローカル ポリシーの設定に関する情報，（776 ページ）

ローカル ポリシーの設定に関する情報

ローカルポリシーは、HTTP と DHCP に基づいてデバイスをプロファイルすることで、ネットワーク上のエンドデバイスを識別できるようにします。ユーザは、デバイスベースのポリシーを設定して、それをネットワーク上でユーザ単位またはデバイス ポリシー単位に適用できます。

ローカルポリシーを使用すれば、モバイルデバイスのプロファイリングと、プロファイルしたデバイスの特定の VLAN への基本オンボーディングが可能になります。また、ACL と QoS を割り当てたり、セッション タイムアウトを設定したりできます。

ローカル ポリシーは次の 2 種類のコンポーネントとして設定できます。

- ネットワークに参加しているクライアントに固有のサービステンプレートとしてのポリシー属性の定義とポリシー一致基準の適用。
- ポリシーへの一致基準の適用。

次のポリシー一致属性がローカル ポリシーの設定に使用されます。

- デバイス：デバイスのタイプを定義します。Windows ベースのコンピュータ、スマートフォン、iPad や iPhone などの Apple デバイス。
- ユーザ名：ユーザのユーザ名を定義します。
- ユーザ ロール：学生や従業員などのユーザ タイプまたはユーザが属しているユーザ グループを定義します。
- MAC：エンド ポイントの MAC アドレスを定義します。
- MAC OUI：MAC アドレス OUI を定義します。

スイッチでエンドポイントごとにこれらのパラメータに対応する一致が検出されたら、ポリシーを追加できます。ポリシー強制は、次のセッション属性に基づくモバイル デバイスの基本デバイス オンボーディングを可能にします。

- VLAN
- QoS
- ACL
- Session timeout

これらのポリシーを設定して、エンドポイントに指定したポリシーを強制できます。ワイヤレス クライアントは、に基づいてプロファイルされます。スイッチは、これらの属性と事前定義の分類プロファイルを使用してデバイスを識別します。

デフォルト プロファイル テキスト ファイルの置き換え

新しいデバイスが未分類の場合は、デバイスの MAC アドレスをシスコ サポート チームまでご連絡ください。シスコ サポート チームがその MAC アドレスを含む新しい **dc_default_profile.txt** ファイルを提供します。**dc_default_profile.txt** ファイルを以前のファイルと置き換える必要があります。**dc_default_profile.txt** ファイルを変更するには、次の手順に従ってください。

1. 次のコマンドを入力して、デバイス分類子を停止します。
   スイッチ**(config)#no device classifier**
2. 次のコマンドを入力して、ファイルをコピーします。
   スイッチ**#device classifier profile location***filepath*
3. 次のコマンドを入力して、デバイス分類子を開始します。
   スイッチ**(config)# device classifier**

トランク ポート上のセッション モニタの無効化

アップリンク トランク ポート上では、セッション モニタリングを作成しないでください。デフォルトで、セッション モニタリングは有効になっています。セッション モニタリングを無効にする必要があります。

1. 次のコマンドを入力して、グローバル コンフィギュレーション モードを開始します。
   スイッチ**#configure terminal**
2. 次のコマンドを入力して、インターフェイス コンフィギュレーション モードを開始します。
   スイッチ**(config)#interface***interface-id*
3. 次のコマンドを入力して、セッション モニタリングを無効にします。
   スイッチ**(config-if)#no access-session monitor**

関連トピック

インターフェイス テンプレートの作成（CLI），（778 ページ）
パラメータ マップの作成（CLI），（779 ページ）
クラス マップの作成（CLI），（780 ページ）
ポリシー マップの作成（CLI），（781 ページ）
WLAN 上のデバイスのローカル ポリシーの適用（CLI），（782 ページ）
ローカル ポリシーの設定に関する制限，（775 ページ）
ローカル ポリシーの監視，（784 ページ）
例：ローカル ポリシーの設定，（785 ページ）

ローカル ポリシーの設定方法

ローカル ポリシーの設定（CLI）

ローカル ポリシーを設定するには、次の手順を実行します。

1. サービス テンプレートを作成します。
2. インターフェイス テンプレートを作成します。
3. パラメータ マップを作成します。
4. ポリシー マップを作成します。
5. WLAN 上でローカル ポリシーを適用します。

インターフェイス テンプレートの作成（CLI）

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**template***interface-template-name* 例： スイッチ(config)# **template cisco-phone-template** スイッチ(config-template)#	インターフェイス テンプレート コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： スイッチ(config-template)# **switchport mode access**	トランキングなし、タグなしの単一VLANイーサネット インターフェイスとして、インターフェイスを設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。アクセス ポートは、デフォルトで、VLAN 1 のトラフィックを送受信します。
ステップ 4	**switchport voice vlan***vlan_id* 例： スイッチ(config-template)# **switchport voice vlan 20**	すべての音声トラフィックを指定された VLAN 経由で転送するように指定します。1 ～ 4094 の値を指定できます。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報，（776 ページ）
ローカル ポリシーの設定に関する制限，（775 ページ）
ローカル ポリシーの監視，（784 ページ）
例：ローカル ポリシーの設定，（785 ページ）

パラメータ マップの作成（CLI）

クラス マップよりパラメータ マップを使用することをお勧めします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map typesubscriberattribute-to-service***parameter-map-name* 例： スイッチ(config)# **parameter-map type subscriber attribute-to-service Aironet-Policy-para**	パラメータ マップのタイプと名前を指定します。
ステップ 3	*map-index***map {device-type|mac-address|oui|user-role|username} {eq|not-eq|regex***filter-name*} 例： スイッチ(config-parameter-map-filter)# **10 map device-type eq "WindowsXP-Workstation"**	パラメータ マップ属性フィルタ基準を指定します。
ステップ 4	**interface-template***interface-template-name* 例： スイッチ(config-parameter-map-filter-submode)# **interface-template cisco-phone-template** スイッチ(config-parameter-map-filter-submode)#	サービス テンプレート コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報，（776 ページ）
ローカル ポリシーの設定に関する制限，（775 ページ）
ローカル ポリシーの監視，（784 ページ）
例：ローカル ポリシーの設定，（785 ページ）

クラス マップの作成（CLI）

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map typecontrol subscriber***class-map-name*{**match-all**|**match-any**|**match-first**} 例： スイッチ(config)# **class-map type control subscriber CLASS_AC_1 match-all**	クラス マップのタイプと名前を指定します。
ステップ 3	**match**{**device-type**|**mac-address**|**oui**|**username**|**userrole**}*filter-type-name* 例： スイッチ(config-class-map)# **match device-type Cisco-IP-Phone-7961**	クラス マップ属性フィルタ基準を指定します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報，（776 ページ）
ローカル ポリシーの設定に関する制限，（775 ページ）
ローカル ポリシーの監視，（784 ページ）
例：ローカル ポリシーの設定，（785 ページ）

ポリシー マップの作成（CLI）

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map typecontrolsubscriber***policy-map-name* 例： スイッチ(config)# **policy-map type control subscriber Aironet-Policy**	ポリシー マップ タイプを指定します。
ステップ 3	**eventidentity-update{match-all|match-first}** 例： スイッチ(config-policy-map)# **event identity-update match-all**	ポリシーマップに対する一致基準を指定します。
ステップ 4	*class_number***class** {*class_map_name*|**always** }{**do-all**| **do-until-failure**| **do-until-success**} 例： スイッチ(config-class-control-policymap)# **1 class local_policy1_class do-until-success**	ローカル プロファイリング ポリシー クラスマップ番号を設定し、処理の実行方法を指定します。クラスマップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。

	コマンドまたはアクション	目的
		• **always**：照合を行わずに実行しますが、成功を返します。 • **do-all**：すべての処理を実行します。 • **do-until-failure**：照合が失敗するまですべての処理を実行します。これはデフォルト値です。 • **do-until-success**：照合が成功するまですべての処理を実行します。
ステップ 5	*action-index* **mapattribute-to-servicetable** *parameter-map-name* 例： スイッチ(config-policy-map)# **10 map attribute-to-service table Aironet-Policy-para**	使用するパラメータ マップ テーブルを指定します。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報，（776 ページ）
ローカル ポリシーの設定に関する制限，（775 ページ）
ローカル ポリシーの監視，（784 ページ）
例：ローカル ポリシーの設定，（785 ページ）

WLAN 上のデバイスのローカル ポリシーの適用（CLI）

はじめる前に

パラメータ マップのサービス ポリシーにデバイス タイプ ベースのルールが含まれる場合、デバイス分類子がイネーブルになっていることを確認します。

（注） **device classification** コマンドを使用して、show コマンドの出力で正しく表示されるようにデバイスを分類する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan***wlan-name* 例： スイッチ(config)# **wlan wlan1**	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**service-policy type controlsubscriber***policymapname* 例： スイッチ(config-wlan)# **service-policy type control subscriber Aironet-Policy**	WLAN にローカル ポリシーを適用します。
ステップ 4	**profiling local http**（任意） 例： スイッチ(config-wlan)# **profiling local http**	HTTP プロトコルに基づいて、デバイスのプロファイリングのみをイネーブルにします（任意）。
ステップ 5	**profiling radius http**（任意） 例： スイッチ(config-wlan)# **profiling radius http**	ISE でデバイスのプロファイリングをイネーブルにします（任意）。
ステップ 6	**no shutdown** 例： スイッチ(config-wlan)# **no shutdown**	WLAN をシャットダウンしないように指定します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報，（776 ページ）
ローカル ポリシーの設定に関する制限，（775 ページ）
ローカル ポリシーの監視，（784 ページ）
例：ローカル ポリシーの設定，（785 ページ）

ローカル ポリシーの監視

次のコマンドを使用して、スイッチ上で設定されたローカル ポリシーを監視できます。

表 *51*：ローカル ポリシーの監視コマンド

コマンド	目的
show access-session	表示されたクライアントまたは MAC アドレスごとの承認ステータス、メソッド、およびドメインを含むアクセスセッションのサマリーを表示します。
show access-session cache	クライアントの最新の分類を表示します。
show device classifier attached detail	Mac、DHCP、HTTP などのパラメータに基づくクライアントの最新の分類を表示します。
Show access-session mac*mac-address***details**	マップされたポリシー、使用されたサービステンプレート、およびクライアントの属性を表示します。
show access-session mac*mac-address***policy**	マップされたポリシー、使用されたサービステンプレート、およびクライアントの属性を表示します。 また、次の情報を表示する [Resultant Policy] も確認できます。 • セッションにローカルで属性が設定されているときに、セッションに適用された最終属性。 • サーバから適用された属性。

関連トピック

インターフェイス テンプレートの作成（CLI），（778 ページ）
パラメータ マップの作成（CLI），（779 ページ）
クラス マップの作成（CLI），（780 ページ）
ポリシー マップの作成（CLI），（781 ページ）
WLAN 上のデバイスのローカル ポリシーの適用（CLI），（782 ページ）
ローカル ポリシーの設定に関する情報，（776 ページ）

例：ローカル ポリシーの設定

（注） 各コンフィギュレーション コマンド ラインの最後で、CTRL Z を入力して、コマンドを実行し、次の行に移動します。

次の例は、インターフェイス テンプレートの作成方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)#template cisco-phone-template
スイッチ(config-template)#switchport mode access
スイッチ(config-template)#switchport voice vlan 20
スイッチ(config-template)# end
```

次の例は、パラメータ マップの作成方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)#parameter-map type subscriber attribute-to-service param-wired
スイッチ(config-parameter-map-filter)#10 map device-type regex Cisco-IP-Phone
スイッチ(config-parameter-map-filter-submode)#10 interface-template cisco-phone-template
スイッチ(config-parameter-map)# end
```

次の例は、ポリシー マップの作成方法を示しています。

```
スイッチ(config)# policy-map type control subscriber apple-tsim
スイッチ(config-policy-map)# event identity-update match-all
スイッチ(config-policy-map)# 1 class always do-until-failure
スイッチ(config-policy-map)# 1 map attribute-to-service table apple-tsim-param
スイッチ(config-policy-map)# end
```

次の例は、WLAN 上のデバイスにポリシーを適用する方法を示しています。

```
スイッチ(config)# wlan wlan1
スイッチ(config-wlan)# client vlan VLAN0054
スイッチ(config-wlan)# profiling local http
スイッチ(config-wlan)# service-policy type control subscriber apple-tsim
スイッチ(config-wlan)# no shutdown
スイッチ# end
```

関連トピック

インターフェイス テンプレートの作成（CLI），（778 ページ）
パラメータ マップの作成（CLI），（779 ページ）
クラス マップの作成（CLI），（780 ページ）
ポリシー マップの作成（CLI），（781 ページ）
WLAN 上のデバイスのローカル ポリシーの適用（CLI），（782 ページ）
ローカル ポリシーの設定に関する情報，（776 ページ）

ローカル ポリシーの設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

ローカル ポリシーの設定の実行に関する機能履歴

リリース	機能情報
Cisco IOS XE 3E	この機能が導入されました。

第 47 章

SPAN および RSPAN の設定

- 機能情報の確認，789 ページ
- SPAN および RSPAN の前提条件，790 ページ
- SPAN および RSPAN の制約事項，790 ページ
- SPAN および RSPAN について，792 ページ
- SPAN および RSPAN の設定方法，806 ページ
- SPAN および RSPAN 動作のモニタリング，833 ページ
- SPAN および RSPAN の設定例，833 ページ
- その他の参考資料，836 ページ
- SPAN および RSPAN の機能の履歴と情報，837 ページ

機能情報の確認

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

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

SPAN および RSPAN の前提条件

SPAN

- SPAN トラフィックを特定の VLAN に制限するには、**filter vlan** キーワードを使用します。トランク ポートをモニタしている場合、このキーワードで指定された VLAN 上のトラフィックのみがモニタされます。デフォルトでは、トランク ポート上のすべての VLAN がモニタされます。

RSPAN

- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。

SPAN および RSPAN の制約事項

SPAN

SPAN の制約事項は次のとおりです。

- 各 スイッチ で 66 のセッションを設定できます。最大 8 の送信元セッションを設定できます。残りのセッションは、RSPAN 宛先セッションとして設定できます。送信元セッションは、ローカル SPAN セッションまたは RSPAN 送信元セッションのどちらかになります。
- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックをモニタできます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- スイッチ ポートを SPAN 宛先ポートとして設定すると、通常のスイッチ ポートではなくなります。SPAN 宛先ポートを通過するのは、監視対象トラフィックのみになります。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、**no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなし、ISL、または IEEE 802.1Q）を伝送します。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。

- ディセーブルのポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN がイネーブルになってからです。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。

SPAN セッションのトラフィック モニタリングには次の制約事項があります。

- ポートまたはVLANを送信元にできますが、同じセッション内に送信元ポートと送信元VLANを混在させることはできません。
- Wireshark は、出力スパンがアクティブな場合は出力パケットをキャプチャしません。
- 同じスイッチまたはスイッチ スタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。スイッチまたはスイッチ スタックは合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つのスイッチ スタックあたりに設定できる宛先ポートは最大で 64 個です。
- SPAN セッションがスイッチの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN がイネーブルの場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- スイッチは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じスイッチまたはスイッチ スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

RSPAN

RSPAN の制約事項は次のとおりです。

- RSPAN は、BPDU パケット モニタリングまたは他のレイヤ 2 スイッチ プロトコルをサポートしません。

- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのスイッチで VLAN RSPAN 機能がサポートされていることを確認してください。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。ただし、スイッチはスパンされたトラフィックをモニタしないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパニングがサポートされません。
- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがプルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラッディングが防止されます。
- RSPAN を使用するには、スイッチが LAN Base イメージを実行している必要があります。

SPAN および RSPAN について

SPAN および RSPAN

ポートまたは VLAN を通過するネットワーク トラフィックを解析するには、SPAN または RSPAN を使用して、そのスイッチ上、またはネットワーク アナライザやその他のモニタ デバイス、あるいはセキュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。SPAN は送信元ポートまたは VLAN 上のネットワーク トラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に出入りするトラフィックだけです。送信元 VLAN にルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックはモニタできません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは、モニタできます。

ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先ポートを使用できます。たとえば、Cisco 侵入検知システム（IDS）センサー装置を宛先ポートに接続した場合、IDS デバイスは TCP リセット パケットを送信して、疑わしい攻撃者の TCP セッションを停止させることができます。

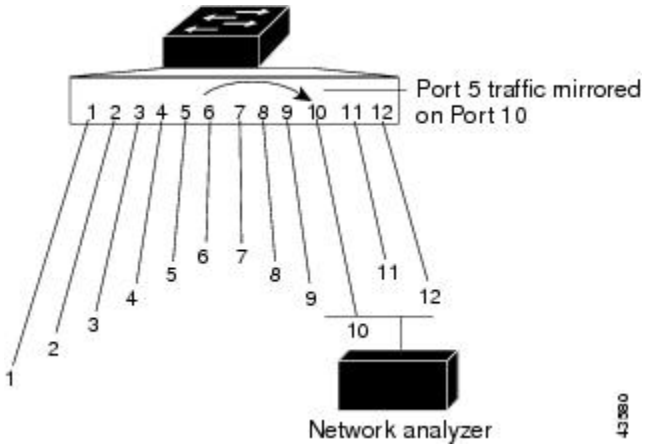
ローカル SPAN

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じスイッチまたはスイッチ スタック内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィッ

ク、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。

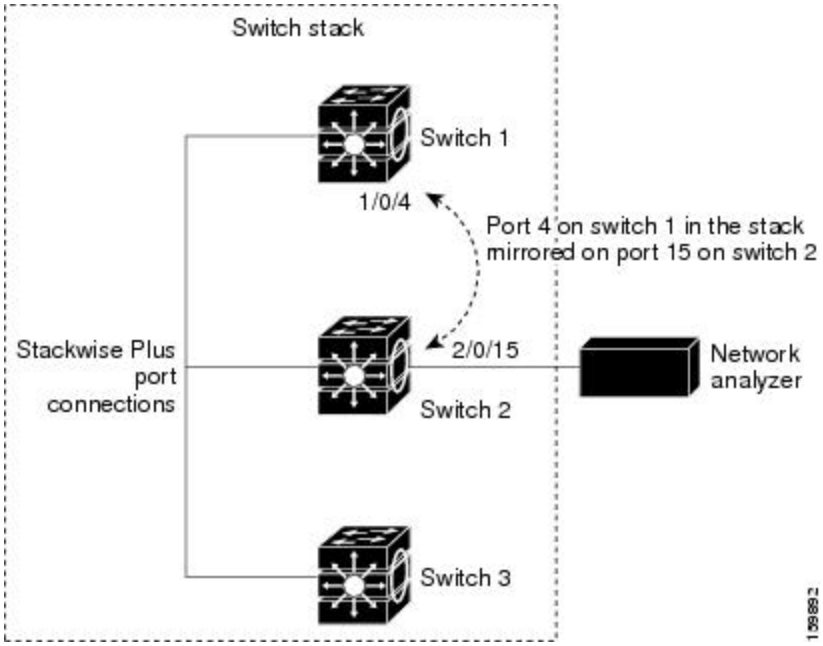
ポート 5（送信元ポート）上のすべてのトラフィックがポート 10（宛先ポート）にミラーリングされます。ポート 10 のネットワーク アナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 からのすべてのネットワーク トラフィックを受信します。

図 *49*：単一デバイスでのローカル *SPAN* の設定例



これは、スイッチ スタック内のローカル SPAN の例です。送信元ポートと宛先ポートは異なるスタック メンバにあります。

図 *50*：デバイス スタックでのローカル *SPAN* の設定例



関連トピック

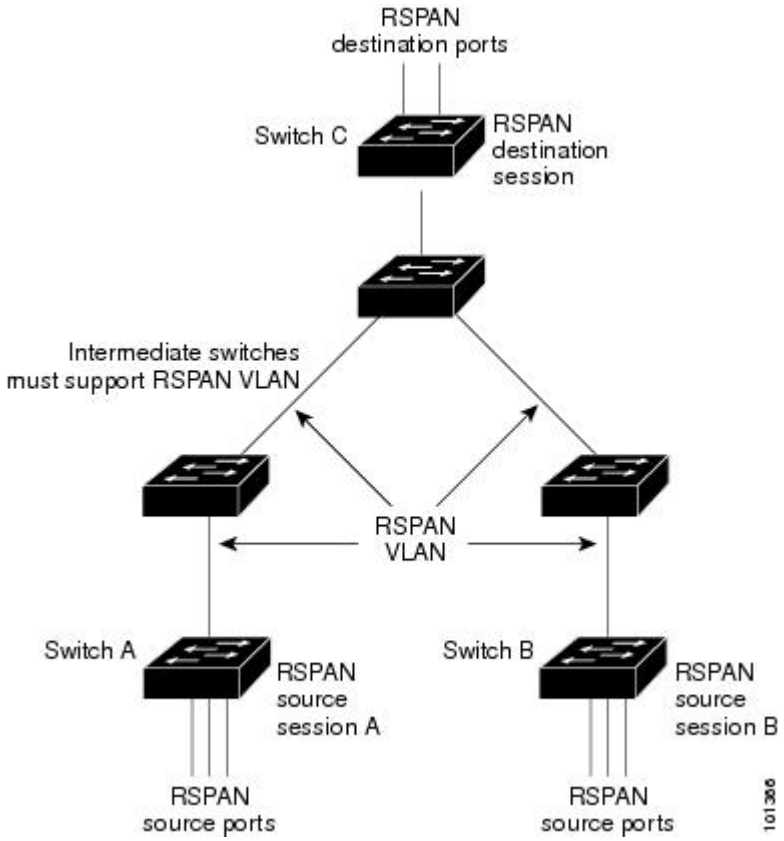
ローカル SPAN セッションの作成, （806 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定, （809 ページ）
例：ローカル SPAN の設定, （833 ページ）

リモート SPAN

RSPANは、異なるスイッチ（または異なるスイッチスタック）上の送信元ポート、送信元VLAN、および宛先ポートをサポートしているので、ネットワーク上で複数のスイッチをリモート モニタリングできます。

下の図にスイッチAとスイッチBの送信元ポートを示します。各RSPANセッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチの RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介して、RSPAN VLAN をモニタする宛先セッションに転送されます。各 RSPAN 送信元スイッチには、ポートまたは VLAN のいずれかが RSPAN 送信元として必要です。図中のスイッチ C のように、宛先は常に物理ポートになります。

図 *51*：*RSPAN* の設定例



関連トピック

RSPAN 送信元セッションの作成, （816 ページ）
RSPAN 宛先セッションの作成, （821 ページ）
RSPAN 宛先セッションの作成および着信トラフィックの設定, （823 ページ）
例：RSPAN VLAN の作成, （835 ページ）

SPAN と RSPAN の概念および用語

- SPAN セッション
- モニタ対象トラフィック
- 送信元ポート
- 送信元 VLAN
- VLAN フィルタリング
- 宛先ポート
- RSPAN VLAN

SPAN セッション

SPANセッション（ローカルまたはリモート）を使用すると、1つまたは複数のポート上、あるいは 1 つまたは複数の VLAN 上でトラフィックをモニタし、そのモニタしたトラフィックを 1 つまたは複数の宛先ポートに送信できます。

ローカルSPANセッションは、宛先ポートと送信元ポートまたは送信元VLAN（すべて単一のネットワーク デバイス上にある）を結び付けたものです。ローカル SPAN には、個別の送信元および宛先のセッションはありません。ローカル SPAN セッションはユーザが指定した入力および出力のパケット セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は少なくとも 1 つの RSPAN 送信元セッション、1 つの RSPAN VLAN、および少なくとも 1 つの RSPAN 宛先セッションで構成されています。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN に関連付けます。宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームが転送される点を除き、ローカル SPAN セッションに非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再設定され、通常のトランク ポートを介して宛先スイッチに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットを取得し、VLAN のタギングを除去し、宛先ポートに送ります。セッションは、（レイヤ 2 制御パケットを除く）すべての RSPAN VLAN パケットのコピーを分析のためにユーザに提供します。

複数のソースおよび宛先ポートを持つ単一 RSPAN セッションを同じセッションに使用できますが、ソースが同じリモート VLAN であるソース セッションの複数使用は許可されていません。

SPAN セッションでのトラフィックのモニタには、次のような制約があります。

- ポートまたはVLANを送信元にできますが、同じセッション内に送信元ポートと送信元VLANを混在させることはできません。
- 同じスイッチまたはスイッチ スタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。スイッチまたはスイッチ スタックは合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つのスイッチ スタックあたりに設定できる宛先ポートは最大で 64 個です。
- SPAN セッションがスイッチの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN がイネーブルの場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。したがって、多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたはVLANをイネーブルにしない限り、SPAN セッションはアクティブになりません。
- スイッチは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じスイッチまたはスイッチ スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

関連トピック

ローカル SPAN セッションの作成, （806 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定, （809 ページ）
例：ローカル SPAN の設定, （833 ページ）

モニタ対象トラフィック

SPAN セッションは、次のトラフィック タイプを監視できます。

- 受信（Rx）SPAN：受信（または入力）SPAN は、スイッチが変更または処理を行う前に、送信元インターフェイスまたはVLANが受信したすべてのパケットをできるだけ多くモニタ

リングします。送信元が受信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。

Diffserv コード ポイント（DSCP）の変更など、ルーティングや Quality of Service（QoS）が原因で変更されたパケットは、変更される前にコピーされます。

受信処理中にパケットをドロップする可能性のある機能は、入力 SPAN には影響を与えません。宛先ポートは、実際の着信パケットがドロップされた場合でも、パケットのコピーを受信します。パケットをドロップする可能性のある機能は、標準および拡張 IP 入力アクセス コントロール リスト（ACL）、入力 QoS ポリシング、VLAN ACL、および出力 QoS ポリシングです。

- 送信（Tx）SPAN：送信（または出力）SPANは、スイッチによる変更または処理がすべて実行されたあとに、送信元インターフェイスから送信されたすべてのパケットをできる限り多くモニタリングします。送信元が送信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。コピーはパケットの変更後に用意されます。

  ルーティングが原因で変更されたパケット（存続可能時間（TTL）、MACアドレス、QoS値の変更など）は、宛先ポートで（変更されて）コピーされます。

  送信処理中にパケットをドロップする可能性のある機能は、SPAN 用の複製コピーにも影響します。これらの機能には、標準および拡張IP出力ACL、出力QoSポリシングがあります。

- 両方：SPAN セッションで、受信パケットと送信パケットの両方について、ポートまたは VLAN をモニタすることもできます。これはデフォルトです。

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。ただし、宛先ポートを設定するときに encapsulation replicate キーワードを入力すると、次の変更が発生します。

- 送信元ポートと同じカプセル化設定（タグなし、または IEEE 802.1Q）を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコル パケットを含むすべてのタイプのパケットがモニタされます。

したがって、カプセル化レプリケーションがイネーブルにされたローカルSPANセッションでは、タグなし、および IEEE 802.1Q タグ付きパケットが宛先ポートに混在することがあります。

スイッチの輻輳により、入力送信元ポート、出力送信元ポート、またはSPAN宛先ポートでパケットがドロップされることがあります。一般に、これらの特性は互いに無関係です。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因でモニタされないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- スイッチの輻輳が原因でドロップされた出力パケットは、出力 SPAN からもドロップされます。

SPANの設定によっては、同一送信元のパケットのコピーが複数、SPAN宛先ポートに送信されます。たとえば、ポート A での RX モニタ用とポート B での TX モニタ用に双方向（RX と TX）SPAN セッションが設定されているとします。パケットがポート A からスイッチに入ってポート B にスイッチされると、着信パケットも発信パケットも宛先ポートに送信されます。このため、両方のパケットは同じものになります。レイヤ 3 書き換えが行われた場合には、パケット変更のため異なるパケットになります。

送信元ポート

送信元ポート（別名モニタ側ポート）は、ネットワーク トラフィック分析のために監視するスイッチド ポートまたはルーテッド ポートです。1 つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向でモニタできます。スイッチは、任意の数の送信元ポート（スイッチで利用可能なポートの最大数まで）と任意の数の送信元 VLAN（サポートされている VLAN の最大数まで）をサポートしています。ただし、スイッチが送信元ポートまたは VLAN でサポートするセッション数には上限（ローカルまたは RSPAN）があります。単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- 複数の SPAN セッションでモニタできます。
- モニタする方向（入力、出力、または両方）を指定して、各送信元ポートを設定できます。
- すべてのポート タイプ（EtherChannel、ギガビット イーサネットなど）が可能です。
- EtherChannel 送信元の場合は、EtherChannel 全体で、または物理ポートがポート チャネルに含まれている場合は物理ポート上で個別に、トラフィックをモニタできます。
- アクセス ポート、トランク ポート、ルーテッド ポート、または音声 VLAN ポートに指定できます。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニタすることが可能です。

送信元 *VLAN*

VLAN ベースの SPAN（VSPAN）では、1 つまたは複数の VLAN のネットワーク トラフィックをモニタできます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスが VLAN ID となり、トラフィックはその VLAN のすべてのポートでモニタされます。

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブ ポートは送信元ポートとして含まれ、単一方向または双方向でモニタできます。
- 指定されたポートでは、モニタ対象のVLAN上のトラフィックのみが宛先ポートに送信されます。
- 宛先ポートが送信元VLANに所属する場合は、送信元リストから除外され、モニタされません。

- ポートが送信元VLANに追加または削除されると、これらのポートで受信された送信元VLANのトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニタできるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブなすべての VLAN がモニタされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニタ対象を特定の VLAN に制限できます。

- VLAN フィルタリングが適用されるのは、トランク ポートまたは音声 VLAN ポートのみです。
- VLANフィルタリングはポートベースセッションにのみ適用され、VLAN送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセス ポートではリスト内の該当 VLAN のみがモニタされます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートおよび VLAN からのトラフィックのコピーを受信し、SPANパケットをユーザ（通常はネットワーク アナライザ）に送信する宛先ポート（別名モニタ側ポート）が必要です。

宛先ポートの特性は、次のとおりです。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチまたはスイッチ スタックに存在している必要があります。RSPAN セッションの場合は、RSPAN 宛先セッションを含むスイッチ上にあります。RSPAN送信元セッションのみを実行するスイッチまたはスイッチ スタックには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先設定を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。

（注） SPAN の宛先ポートに QoS が設定されている場合、QoS はただちに有効になります。

- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。削除されたポートがルーテッドポートであった場合、このポートはルーテッド ポートでなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにすることはできません。
- 送信元ポートにすることはできません。
- EtherChannel グループにできます（**オン** モードのみ）。
- VLAN にすることはできません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。ポートは SPAN セッションに必要なトラフィック以外は送信しません。宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- スイッチまたはスイッチ スタックの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化で次のように動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、各パケットに元のカプセル化が使用されます（タグなし、ISL、または IEEE 802.1Q）。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、**encapsulation replicate** がイネーブルになっているローカル SPAN セッションの出力に、タグなし、ISL、または IEEE 802.1Q タグ付きパケットが混在することがあります。
- RSPAN の場合は、元の VLAN ID は RSPAN VLAN ID で上書きされるため失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

RSPAN VLAN は、RSPAN の送信元セッションと宛先セッション間で SPAN トラフィックを伝送します。RSPAN VLAN には、次の特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上のみです。

- RSPAN VLAN は、**remote-span** VLAN コンフィギュレーション モード コマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN を、プライベート VLAN のプライマリまたはセカンダリ VLAN にはできません。

VLAN トランキング プロトコル（VTP）に対して可視である VLAN 1 ～ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。拡張 VLAN 範囲（1006 ～ 4094）内の RSPAN VLAN ID を割り当てる場合は、すべての中間スイッチを手動で設定する必要があります。

通常は、ネットワークに複数の RSPAN VLAN を配置し、それぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションで、パケットを RSPAN セッションに送信できます。また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN をモニタしたり、ユーザにトラフィックを送信したりできます。セッションは RSPAN VLAN ID によって区別されます。

関連トピック

RSPAN 送信元セッションの作成, （816 ページ）
RSPAN 宛先セッションの作成, （821 ページ）
RSPAN 宛先セッションの作成および着信トラフィックの設定, （823 ページ）
例：RSPAN VLAN の作成, （835 ページ）

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッド トラフィックを監視しません。VSPAN が監視するのはスイッチに出入りするトラフィックに限られ、VLAN 間でルーティングされるトラフィックは監視しません。たとえば、VLAN が受信モニタされ、スイッチが別の VLAN から監視対象 VLAN にトラフィックをルーティングする場合、そのトラフィックは監視されず、SPAN 宛先ポートで受信されません。
- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。
- CDP：SPAN セッションがアクティブな間、SPAN 宛先ポートは CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。
- VTP：VTP を使用すると、スイッチ間で RSPAN VLAN のプルーニングが可能です。
- VLAN およびトランキング：送信元ポート、または宛先ポートの VLAN メンバーシップまたはトランクの設定値を、いつでも変更できます。ただし、宛先ポートの VLAN メンバーシッ

プまたはトランクの設定値に対する変更が有効になるのは、SPAN 宛先設定を削除してからです。送信元ポートのVLANメンバーシップまたはトランクの設定値に対する変更は、ただちに有効になり、対応する SPAN セッションが変更に応じて自動的に調整されます。

- EtherChannel：EtherChannelグループを送信元ポートとして設定することはできますが、SPAN 宛先ポートとして設定することはできません。グループが SPAN 送信元として設定されている場合、グループ全体がモニタされます。

  モニタ対象の EtherChannel グループに物理ポートを追加すると、SPAN 送信元ポート リストに新しいポートが追加されます。モニタ対象の EtherChannel グループからポートを削除すると、送信元ポート リストからそのポートが自動的に削除されます。

  EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータはモニタされます。ただし、EtherChannel グループに含まれる物理ポートを SPAN 宛先として設定した場合、その物理ポートはグループから削除されます。SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。EtherChannel グループから削除されたポートは、グループ メンバのままですが、inactive または suspended ステートになります。

  EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが送信元の場合、ポートはEtherChannel グループおよびモニタ対象ポート リストから削除されます。

- マルチキャスト トラフィックをモニタできます。出力ポートおよび入力ポートのモニタでは、未編集のパケットが 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト パケットの送信回数は反映されません。

- プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。

- セキュア ポートを SPAN 宛先ポートにすることはできません。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。

- IEEE 802.1x ポートは SPAN 送信元ポートにできます。SPAN 宛先ポート上で IEEE 802.1x をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブルに設定されます。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。

SPAN と RSPAN とデバイス スタック

スイッチのスタックは 1 つの論理スイッチを表すため、ローカル SPAN の送信元ポートおよび宛先ポートは、スタック内の異なるスイッチである場合があります。したがって、スタック内でのスイッチの追加または削除は、RSPANの送信元セッションまたは宛先セッションだけではなく、

ローカル SPAN セッションにも影響を及ぼします。スイッチがスタックから削除されると、アクティブ セッションが非アクティブになります。また、スイッチがスタックに追加されると、非アクティブ セッションがアクティブになります。

フローベースの SPAN

送信元ポートで監視されるトラフィックにアクセス コントロール リスト（ACL）を適用するフローベース SPAN（FSPAN）またはフローベース RSPAN（FRSPAN）を使用して、SPAN または RSPAN で監視するネットワーク トラフィックのタイプを制御できます。FSPAN ACL は、IPv4、IPv6、および監視される非 IP トラフィックをフィルタリングするように設定できます。

インターフェイスを通して ACL を SPAN セッションに適用します。ACL は SPAN セッション内のすべてのインターフェイスで監視されるすべてのトラフィックに適用されます。この ACL によって許可されるパケットは、SPAN 宛先ポートにコピーされます。ほかのパケットは SPAN 宛先ポートにコピーされません。

元のトラフィックは継続して転送され、接続している任意のポート、VLAN、およびルータ ACL が適用されます。FSPAN ACL は転送の決定に影響を与えることはありません。同様に、ポート、VLAN、およびルータ ACL は、トラフィックのモニタリングに影響を与えません。セキュリティ入力 ACL がパケットを拒否したために転送されない場合でも、FSPAN ACL が許可すると、パケットは SPAN 宛先ポートにコピーされます。しかし、セキュリティ出力 ACL がパケットを拒否したために転送されない場合、パケットは SPAN 宛先ポートにコピーされません。ただし、セキュリティ出力 ACL がパケットの送信を許可した場合だけ、パケットは、FSPAN ACL が許可した場合 SPAN 宛先ポートにコピーされます。これは RSPAN セッションについてもあてはまります。

SPAN セッションには、次の 3 つのタイプの FSPAN ACL を接続できます。

- IPv4 FSPAN ACL：IPv4 パケットだけをフィルタリングします。
- IPv6 FSPAN ACL：IPv6 パケットだけをフィルタリングします。
- MAC FSPAN ACL：IP パケットだけをフィルタリングします。

スタックに設定された VLAN ベースの FSPAN セッションが 1 つまたは複数のスイッチ上のハードウェア メモリに収まらない場合、セッションはこれらのスイッチ上でアンロードされたものとして処理され、スイッチでの FSPAN ACL およびソーシングのためのトラフィックは、SPAN 宛先ポートにコピーされません。FSPAN ACL は継続して正しく適用され、トラフィックは FSPAN ACL がハードウェア メモリに収まるスイッチの SPAN 宛先ポートにコピーされます。

空の FSPAN ACL が接続されると、一部のハードウェア機能により、その ACL の SPAN 宛先ポートにすべてのトラフィックがコピーされます。十分なハードウェア リソースが使用できない場合、空の FSPAN ACL もアンロードされる可能性があります。

IPv4 および MAC FSPAN ACL は、すべてのフィーチャ セットでサポートされています。IPv6 FSPAN ACL は、拡張 IP Services フィーチャ セットでだけサポートされています。

関連トピック

FSPAN セッションの設定, （826 ページ）
FRSPAN セッションの設定, （829 ページ）

SPAN および RSPAN のデフォルト設定

表 *52*：*SPAN* および *RSPAN* のデフォルト設定

機能	デフォルト設定
SPAN のステート（SPAN および RSPAN）	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィックの両方（**both**）
カプセル化タイプ（宛先ポート）	ネイティブ形式（タグなしパケット）
入力転送（宛先ポート）	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。
RSPAN VLAN	未設定

設定時の注意事項

SPAN 設定時の注意事項

- SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの **no** 形式では、**encapsulation** オプションは無視されます。
- トランク ポート上のすべての VLAN をモニタするには、**no monitor session** *session_number* **filter** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

ローカル SPAN セッションの作成，（806 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定，（809 ページ）
例：ローカル SPAN の設定，（833 ページ）

RSPAN 設定時の注意事項

- すべての SPAN 設定時の注意事項が RSPAN に適用されます。

- RSPAN VLAN には特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定のパケットを選択的にフィルタリングまたはモニタできます。RSPAN 送信元スイッチ内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数のスイッチに分散させることができます。
- RSPAN VLAN 上のアクセス ポート（音声 VLAN ポートを含む）は、非アクティブ ステートになります。
- 次の条件を満たす限り、任意の VLAN を RSPAN VLAN として設定できます。
  - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
  - 参加しているすべてのスイッチで RSPAN がサポートされている。

関連トピック

RSPAN 送信元セッションの作成, （816 ページ）
RSPAN 宛先セッションの作成, （821 ページ）
RSPAN 宛先セッションの作成および着信トラフィックの設定, （823 ページ）
例：RSPAN VLAN の作成, （835 ページ）

FSPAN および FRSPAN 設定時の注意事項

- 少なくとも 1 つの FSPAN ACL が接続されている場合、FSPAN はイネーブルになります。
- SPAN セッションに空ではない FSPAN ACL を少なくとも 1 つ接続し、ほかの 1 つまたは複数の FSPAN ACL を接続しなかった場合（たとえば、空ではない IPv4 ACL を接続し、IPv6 と MAC ACL を接続しなかった場合）、FSPAN は、接続されていない ACL によってフィルタリングされたと思われるトラフィックをブロックします。したがって、このトラフィックは監視されません。

関連トピック

FSPAN セッションの設定, （826 ページ）
FRSPAN セッションの設定, （829 ページ）

SPAN および RSPAN の設定方法

ローカル SPAN セッションの作成

SPANセッションを作成し、送信元（モニタ対象）ポートまたはVLAN、および宛先（モニタ側）ポートを指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***source** {**interface***interface-id* |**vlan** *vlan-id*} [**,** | **-**] [**both** |**rx** | **tx**]
5. **monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**encapsulation replicate**]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number*	**all**	**local**	**remote**} 例： スイッチ(config)# **no monitor session all**	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモートSPANセッションを削除します。

	コマンドまたはアクション	目的
ステップ 4	**monitor session***session_number***source** {**interface***interface-id* |**vlan** *vlan-id*} **[,** | **-] [both** |**rx** | **tx]** 例： スイッチ(config)# **monitor session 1 source interface gigabitethernet1/0/1**	SPANセッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（**port-channel***port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタリングする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （任意）**[,**|**-]** は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**both** | **rx** | **tx**：モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 ◦ **both**：受信トラフィックと送信トラフィックの両方をモニタします。 ◦ **rx**：受信トラフィックをモニタします。 ◦ **tx**：送信トラフィックをモニタします。 （注） **monitor session***session_number***source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。

	コマンドまたはアクション	目的
ステップ 5	**monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**encapsulation replicate**]} 例： `スイッチ(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate`	SPANセッションおよび宛先ポート（モニタ側ポート）を指定します。 （注） ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）**[,|-]** は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 （注） **monitor session***session_number***destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 6	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

ローカル SPAN, （792 ページ）
SPAN セッション, （795 ページ）
SPAN 設定時の注意事項, （804 ページ）

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成し、さらに送信元ポートまたは VLAN および宛先ポートを指定した後、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置等）用に着信トラフィックをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***source** {**interface***interface-id* |**vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**encapsulation replicate**][**ingress** {**dot1q vlan***vlan-id* |**untagged vlan***vlan-id*|**vlan***vlan-id*}]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： スイッチ(config)# **no monitor session all**	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number***source** {**interface***interface-id* |**vlan** *vlan-id*} **[,** | **-]** [**both** | **rx** | **tx**] 例： スイッチ(config)# **monitor session 2 source gigabitethernet1/0/1 rx**	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。
ステップ 5	**monitor session***session_number***destination** {**interface***interface-id***[,** | **-]** [**encapsulation replicate][ingress** {**dot1q vlan***vlan-id* |**untagged vlan***vlan-id*|**vlan***vlan-id*}]} 例： スイッチ(config)# **monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6**	SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 •（任意）**[,**|**-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマまたはハイフンの前後にスペースを 1 つずつ入力します。 •（任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 • **ingress** は、宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。 ◦ **dot1q vlan***vlan-id*：デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカ

	コマンドまたはアクション	目的
		プセル化された着信パケットを受信します。 ◦ **untagged vlan***vlan-id* または **vlan***vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受信します。
ステップ 6	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

ローカル SPAN, （792 ページ）
SPAN セッション, （795 ページ）
SPAN 設定時の注意事項, （804 ページ）
例：ローカル SPAN の設定, （833 ページ）

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number* **source interface***interface-id*
5. **monitor session***session_number***filter vlan***vlan-id*[**,** | **-**]
6. **monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**encapsulation replicate**]}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： スイッチ(config)# **no monitor session all**	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべてのSPANセッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモートSPANセッションを削除します。
ステップ 4	**monitor session***session_number* **source interface***interface-id* 例： スイッチ(config)# **monitor session 2 source interface gigabitethernet1/0/2 rx**	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。指定したインターフェイス

	コマンドまたはアクション	目的
		は、あらかじめトランク ポートとして設定しておく必要があります。
ステップ 5	**monitor session***session_number***filter vlan***vlan-id*[**,**	**-**] 例： スイッチ(config)# **monitor session 2 filter vlan 1 - 5 , 9**	SPAN 送信元トラフィックを特定の VLAN に制限します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* に指定できる範囲は 1 ～ 4094 です。 • （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 6	**monitor session***session_number***destination**{**interface***interface-id*[**,**	**-**] [**encapsulation replicate**]} 例： スイッチ(config)# **monitor session 2 destination interface gigabitethernet1/0/1**	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）[**,**	**-**] は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

RSPAN VLAN としての VLAN の設定

新しい VLAN を作成し、RSPAN セッション用の RSPAN VLAN になるように設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vlan***vlan-id*
4. **remote-span**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan***vlan-id* 例： スイッチ(config)# **vlan 100**	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークンリングおよびFDDI VLAN 専用）にすることはできません。
ステップ 4	**remote-span** 例： スイッチ(config-vlan)# **remote-span**	VLAN を RSPAN VLAN として設定します。
ステップ 5	**end** 例： スイッチ(config-vlan)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

RSPAN に参加するすべてのスイッチに RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲（1005 未満）であり、VTP がネットワーク内でイネーブルである場合は、1 つのスイッチに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のスイッチ

に伝播するように設定できます。拡張範囲VLAN（1005を超えるID）の場合、送信元と宛先の両方のスイッチ、および中間スイッチにRSPAN VLANを設定する必要があります。

VTPプルーニングを使用して、RSPANトラフィックが効率的に流れるようにするか、またはRSPANトラフィックの伝送が不要なすべてのトランクから、RSPAN VLANを手動で削除します。

VLANからリモートSPAN特性を削除して、標準VLANに戻すように変換するには、**no remote-span** VLANコンフィギュレーション コマンドを使用します。

SPANセッションから送信元ポートまたはVLANを削除するには、**no monitor session***session_number***source**{**interface***interface-id* |**vlan** *vlan-id*} グローバル コンフィギュレーション コマンドを使用します。セッションからRSPAN VLANを削除するには、**no monitor session***session_number***destination remote vlan***vlan-id* コマンドを使用します。

RSPAN送信元セッションの作成

RSPAN送信元セッションを作成および開始し、モニタ対象の送信元および宛先RSPAN VLANを指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***source** {**interface***interface-id*| **vlan***vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session***session_number***destinationremote vlan***vlan-id*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： スイッチ(config)# **no monitor session 1**	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number***source** {**interface***interface-id*| **vlan***vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： スイッチ(config)# **monitor session 1 source interface gigabitethernet1/0/1 tx**	RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。 ◦ *interface-id* には、モニタリングする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 48 です。 ◦ *vlan-id* には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。 • （任意）**[,|-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**both** | **rx** | **tx**：モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 ◦ **both**：受信トラフィックと送信トラフィックの両方をモニタします。 ◦ **rx**：受信トラフィックをモニタします。 ◦ **tx**：送信トラフィックをモニタします。

	コマンドまたはアクション	目的
ステップ 5	**monitor session***session_number***destination remote vlan***vlan-id* 例： スイッチ(config)# **monitor session 1 destination remote vlan 100**	RSPAN セッション、宛先 RSPAN VLAN、および宛先ポート グループを指定します。 • *session_number* には、ステップ 4 で指定した番号を入力します。 • *vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

リモート SPAN, （794 ページ）
RSPAN VLAN, （800 ページ）
RSPAN 設定時の注意事項, （804 ページ）

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するように RSPAN 送信元セッションを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number* **source interface***interface-id*
5. **monitor session***session_number***filter vlan***vlan-id*[**,** | **-**]
6. **monitor session***session_number***destinationremote vlan***vlan-id*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： スイッチ(config)# **no monitor session 2**	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number* **source interface***interface-id* 例： スイッチ(config)# **monitor session 2**	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。

	コマンドまたはアクション	目的
	source interface gigabitethernet1/0/2 rx	
ステップ 5	**monitor session***session_number***filter vlan***vlan-id*[**,**	**-**] 例： スイッチ(config)# **monitor session 2 filter vlan 1 - 5 , 9**	SPAN 送信元トラフィックを特定の VLAN に制限します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* に指定できる範囲は 1 ～ 4094 です。 •（任意）**,**	**-**：カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 6	**monitor session***session_number***destination remote vlan***vlan-id* 例： スイッチ(config)# **monitor session 2 destination remote vlan 902**	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは、別のスイッチまたはスイッチ スタック（送信元セッションが設定されていないスイッチまたはスイッチ スタック）に設定します。

このスイッチ上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vlan***vlan-id*
4. **remote-span**
5. **exit**
6. **no monitor session** {*session_number* | **all** | **local** | **remote**}
7. **monitor session***session_number***sourceremote vlan***vlan-id*
8. **monitor session***session_number***destination interface***interface-id*
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan***vlan-id* 例： スイッチ(config)# **vlan 901**	送信元スイッチで作成された RSPAN VLAN の VLAN ID を指定し、VLAN コンフィギュレーション モードを開始します。 両方のスイッチが VTP に参加し、RSPAN VLAN ID が 2 ～ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 3 ～ 5 は不要です。

	コマンドまたはアクション	目的
ステップ 4	**remote-span** 例： スイッチ(config-vlan)# **remote-span**	VLAN を RSPAN VLAN として識別します。
ステップ 5	**exit** 例： スイッチ(config-vlan)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： スイッチ(config)# **no monitor session 1**	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 7	**monitor session***session_number***source remote vlan***vlan-id* 例： スイッチ(config)# **monitor session 1 source remote vlan 901**	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 8	**monitor session***session_number***destination interface***interface-id* 例： スイッチ(config)# **monitor session 1 destination interface gigabitethernet2/0/1**	RSPAN セッションと宛先インターフェイスを指定します。 • *session_number* には、ステップ 7 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 • *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 • **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

リモート SPAN, （794 ページ）
RSPAN VLAN, （800 ページ）
RSPAN 設定時の注意事項, （804 ページ）

RSPAN 宛先セッションの作成および着信トラフィックの設定

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定し、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置等）用に着信トラフィックをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***sourceremote vlan***vlan-id*
5. **monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**ingress**{**dot1q vlan***vlan-id* | **untaggedvlan***vlan-id*|**vlan***vlan-id*}]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： スイッチ(config)# **no monitor session 2**	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカルセッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number***sourceremote vlan***vlan-id* 例： スイッチ(config)# **monitor session 2 source remote vlan 901**	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 5	**monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**ingress**{**dot1q vlan***vlan-id* | **untaggedvlan***vlan-id*|**vlan***vlan-id*}]} 例： スイッチ(config)# **monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6**	SPAN セッション、宛先ポート、パケット カプセル化、および着信 VLAN とカプセル化を指定します。 • *session_number* には、ステップ 5 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 • *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。

	コマンドまたはアクション	目的
		• **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。 • （任意）[,|-] は、一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress** を追加のキーワードと一緒に入力します。 ◦ **dot1q vlan***vlan-id*：デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを転送します。 ◦ **untagged vlan***vlan-id* または **vlan***vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを転送します。
ステップ 6	**end** **例**： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** **例**： `スイッチ# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** **例**： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

リモート SPAN, （794 ページ）
RSPAN VLAN, （800 ページ）
RSPAN 設定時の注意事項, （804 ページ）
例：RSPAN VLAN の作成, （835 ページ）

FSPAN セッションの設定

SPAN セッションを作成し、送信元（監視対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定し、セッションに FSPAN を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***source** {**interface***interface-id*| **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** |**tx**]
5. **monitor session***session_number***destination**{**interface***interface-id* [**,** | **-**] [**encapsulation replicate**]}
6. **monitor session***session_number***filter**{**ip** | **ipv6**| **mac**} **access-group**{*access-list-number* | *name*}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： スイッチ(config)# **no monitor session 2**	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカルセッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number***source** {**interface***interface-id*| **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** |**tx**] 例： スイッチ(config)# **monitor session 2 source interface gigabitethernet1/0/1**	SPANセッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタリングする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （任意）[**,** | **-**]：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意） [**both** | **rx** | **tx**]：モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPANは送信トラフィックと受信トラフィックの両方をモニタします。 ◦ **both**：送信トラフィックと受信トラフィックの両方をモニタします。これはデフォルトです。 ◦ **rx**：受信トラフィックをモニタします。

	コマンドまたはアクション	目的
		◦ **tx**：送信トラフィックをモニタします。 （注） **monitor session***session_number***source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。
ステップ 5	**monitor session***session_number***destination**{**interface***interface-id* [**,** | **-**] [**encapsulation replicate**]} 例： `スイッチ(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate`	SPANセッションおよび宛先ポート（モニタ側ポート）を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • **destination** には、次のパラメータを指定します。 ◦ *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 ◦（任意）**[,** | **-]** は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 ◦（任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 （注） ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 **monitor session***session_number***destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 6	**monitor session***session_number***filter**{**ip** | **ipv6**| **mac**} **access-group**{*access-list-number* | *name*} 例： `スイッチ(config)# monitor session 2 filter ipv6 access-group 4`	SPANセッション、フィルタリングするパケットのタイプ、および FSPAN セッションで使用する ACL を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *access-list-number* には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。

	コマンドまたはアクション	目的
		• *name* には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

フローベースの SPAN, （803 ページ）
FSPAN および FRSPAN 設定時の注意事項, （805 ページ）

FRSPAN セッションの設定

RSPAN 送信元セッションを開始し、監視対象の送信元および宛先 RSPAN VLAN を指定し、セッションに FRSPAN を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***source** {**interface***interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session***session_number***destinationremote vlan***vlan-id*
6. **vlan***vlan-id*
7. **remote-span**
8. **exit**
9. **monitor session***session_number***filter**{**ip** | **ipv6**| **mac**} **access-group**{*access-list-number* | *name*}
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number*	**all**	**local**	**remote**} 例： スイッチ(config)# **no monitor session 2**	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number***source** {**interface***interface-id*	**vlan** *vlan-id*} [**,**	**-**] [**both**	**rx**	**tx**]	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。

	コマンドまたはアクション	目的
	例： スイッチ(config)# **monitor session 2 source interface gigabitethernet1/0/1**	• *interface-id* には、モニタリングする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタリングする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたはVLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （任意）[,|-]：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意） [**both**	**rx**	**tx**]：モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。 • **both**：送信トラフィックと受信トラフィックの両方をモニタします。これはデフォルトです。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。 （注） **monitor session***session_number***source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。
ステップ 5	**monitor session***session_number***destinationremote vlan***vlan-id* 例： スイッチ(config)# **monitor session 2 destination remote vlan 5**	RSPAN セッションと宛先 RSPAN VLAN を指定します。 • *session_number* には、ステップ 4 で指定した番号を入力します。 • *vlan-id* には、モニタリングする宛先 RSPAN VLAN を指定します。

	コマンドまたはアクション	目的
ステップ 6	**vlan***vlan-id* 例： スイッチ(config)# **vlan 10**	VLAN コンフィギュレーション モードを開始します。*vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 7	**remote-span** 例： スイッチ(config-vlan)# **remote-span**	ステップ 5 で指定した VLAN が RSPAN VLAN の一部であることを指定します。
ステップ 8	**exit** 例： スイッチ(config-vlan)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**monitor session***session_number***filter** {**ip** | **ipv6**| **mac**} **access-group** {*access-list-number* | *name*} 例： スイッチ(config)# **monitor session 2 filter ip access-group 7**	RSPANセッション、フィルタリングするパケットのタイプ、および FRSPAN セッションで使用する ACL を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *access-list-number* には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • *name*には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 10	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 11	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

フローベースの SPAN, （803 ページ）
FSPAN および FRSPAN 設定時の注意事項, （805 ページ）

SPAN および RSPAN 動作のモニタリング

次の表で、SPAN および RSPAN 動作の設定と結果を表示して動作を監視するために使用するコマンドについて説明します。

表 *53* : *SPAN* および *RSPAN* 動作のモニタリング

コマンド	目的
show monitor	現在の SPAN、RSPAN、FSPAN、または FRSPAN 設定を表示します。

SPAN および RSPAN の設定例

例：ローカル SPAN の設定

次に、SPAN セッション 1 を設定し、宛先ポートへ向けた送信元ポートのトラフィックをモニタする例を示します。最初に、セッション 1 の既存の SPAN 設定を削除し、カプセル化方式を維持しながら、双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 にミラーリングします。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# no monitor session 1
スイッチ(config)# monitor session 1 source interface gigabitethernet1/0/1
スイッチ(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
スイッチ(config)# end
```

次に、SPAN セッション 1 の SPAN 送信元としてのポート 1 を削除する例を示します。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# no monitor session 1 source interface gigabitethernet1/0/1
スイッチ(config)# end
```

次に、双方向モニタが設定されていたポート 1 で、受信トラフィックのモニタをディセーブルにする例を示します。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx
```

ポート 1 で受信するトラフィックのモニタはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ～ 3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィックを宛先ポート GigabitEthernet 2 に送信する例を示します。さらに、この設定は VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするよう変更されます。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# no monitor session 2
スイッチ(config)# monitor session 2 source vlan 1 - 3 rx
スイッチ(config)# monitor session 2 destination interface gigabitethernet1/0/2
スイッチ(config)# monitor session 2 source vlan 10
スイッチ(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、送信元ポート GigabitEthernet 1 上で受信されるトラフィックをモニタするように SPAN セッション 2 を設定し、送信元ポートと同じ出力カプセル化方式を使用してそれを宛先ポート GigabitEthernet 2 に送信し、VLAN 6 をデフォルトの入力 VLAN として IEEE 802.1Q カプセル化を使用する入力転送をイネーブルにする例を示します。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# no monitor session 2
スイッチ(config)# monitor session 2 source gigabitethernet1/0/1 rx
スイッチ(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 replicate ingress dot1q vlan 6
スイッチ(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、トランク ポート GigabitEthernet 2 で受信されたトラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先ポート GigabitEthernet 1 に送信する例を示します。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# no monitor session 2
スイッチ(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
スイッチ(config)# monitor session 2 filter vlan 1 - 5 , 9
スイッチ(config)# monitor session 2 destination interface gigabitethernet1/0/1
スイッチ(config)# end
```

関連トピック

ローカル SPAN セッションの作成および着信トラフィックの設定, （809 ページ）
ローカル SPAN, （792 ページ）
SPAN セッション, （795 ページ）
SPAN 設定時の注意事項, （804 ページ）

例：RSPAN VLAN の作成

この例は、RSPAN VLAN 901 の作成方法を示しています。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# vlan 901
スイッチ(config-vlan)# remote span
スイッチ(config-vlan)# end
```

次に、セッション 1 に対応する既存の RSPAN 設定を削除し、複数の送信元インターフェイスをモニタするように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# no monitor session 1
スイッチ(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
スイッチ(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
スイッチ(config)# monitor session 1 source interface port-channel 2
スイッチ(config)# monitor session 1 destination remote vlan 901
スイッチ(config)# end
```

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# no monitor session 2
スイッチ(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
スイッチ(config)# monitor session 2 filter vlan 1 - 5 , 9
スイッチ(config)# monitor session 2 destination remote vlan 902
スイッチ(config)# end
```

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# monitor session 1 source remote vlan 901
スイッチ(config)# monitor session 1 destination interface gigabitethernet2/0/1
スイッチ(config)# end
```

次に、RSPAN セッション 2 で送信元リモート VLAN として VLAN 901 を設定し、送信元ポート GigabitEthernet 2 を宛先インターフェイスとして設定し、VLAN 6 をデフォルトの受信 VLAN として着信トラフィックの転送をイネーブルにする例を示します。

```
スイッチ> enable
スイッチ# configure terminal
スイッチ(config)# monitor session 2 source remote vlan 901
スイッチ(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6

スイッチ(config)# end
```

関連トピック

RSPAN 宛先セッションの作成および着信トラフィックの設定, （823 ページ）
リモート SPAN, （794 ページ）
RSPAN VLAN, （800 ページ）
RSPAN 設定時の注意事項, （804 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
system コマンド	*Network Management Command Reference, Cisco IOS XE Release 3E*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	-

MIB

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

シスコのテクニカル サポート

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

SPAN および RSPAN の機能の履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	スイッチ ポート アナライザ（SPAN）：スニファやアナライザまたは RMON プローブを使用してポートまたは VLAN のスイッチのトラフィックを監視できます。 この機能が導入されました。

リリース	変更内容
Cisco IOS XE 3.3SE	フローベースのスイッチ ポート アナライザ（SPAN）：指定されたフィルタを使用してエンド ホスト間の必要なデータのみをキャプチャする手段を提供します。フィルタは、IPv4、IPv6 または IPv4 と IPv6、あるいは指定された送信元と宛先アドレス間の IP トラフィック（MAC）以外を制限するアクセス リストの観点から定義されます。 この機能が導入されました。
Cisco IOS XE 3.3SE	EtherChannel での SPAN 宛先ポートのサポート：EtherChannel で SPAN 宛先ポートを設定できるようにします。 この機能が導入されました。
Cisco IOS XE 3.3SE	スイッチ ポート アナライザ（SPAN）- 分散型出力 SPAN：ラインカードにすでに分散された入力 SPAN とともにラインカードに出力 SPAN 機能を分散させます。出力 SPAN 機能をラインカードに分散させることで、システムのパフォーマンスが向上します。 この機能が導入されました。

第 48 章

パケット キャプチャの設定

- 機能情報の確認，839 ページ
- パケット キャプチャの前提条件，839 ページ
- パケット キャプチャの制約事項，840 ページ
- パケット キャプチャの概要，843 ページ
- パケット キャプチャの設定，857 ページ
- パケット キャプチャのモニタリング，878 ページ
- その他の参考資料，895 ページ

機能情報の確認

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

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

パケット キャプチャの前提条件

パケット キャプチャの前提条件

- パケット キャプチャは Catalyst 3850 および Catalyst 3650 でサポートされています。

- Wireshark は、IP Base イメージおよび IP Services イメージを実行するスイッチのみでサポートされています。
- 組み込みパケット キャプチャは、LAN Base イメージを実行しているスイッチのみでサポートされています。

組み込みパケット キャプチャ（EPC）のソフトウェア サブシステムは、その動作で CPU とメモリ リソースを消費します。さまざまなタイプの操作を行うために十分なシステム リソースを準備する必要があります。システム リソースを使用するためのガイドラインを以下の表に示します。

表 *54*：*EPC* サブシステムのシステム要件

システム リソース	要件
ハードウェア	CPU利用率の要件は、プラットフォームによって異なります。
メモリ	パケット バッファは DRAM に保存されます。パケット バッファのサイズは、ユーザが指定します。
ディスクスペース	パケットは外部のデバイスにエクスポートできます。フラッシュ ディスクでの中間保管は必要ありません。

パケット キャプチャの制約事項

パケット キャプチャの制約事項

- Cisco IOS Release XE 3.3.0(SE) 以降では、Wireshark のグローバル キャプチャはサポートされません。
- Cisco IOS リリース 16.1 から、表示フィルタが Wireshark でサポートされています。
- Wireshark を設定するための CLI では、機能を EXEC モードからのみ実行する必要があります。通常は設定サブモードで発生するアクション（キャプチャ ポイントの定義など）は、代わりに EXEC モードから処理されます。すべての主要コマンドは NVGEN の対象ではなく、NSF と SSO のシナリオではスタンバイ スーパーバイザに同期されません。
- インターフェイスの出力方向にキャプチャされたパケットは、スイッチ rewrite（TTL、VLAN タグ、CoS、チェックサム、MAC アドレス、DSCP、precedent、UP などを含む）によって加えられる変更を反映しない場合があります。
- 入力および出力の両方のパケットの書き換え情報はキャプチャされません。
- ファイル サイズによる循環ファイル保存の制限はサポートされません。
- ファイル制限は、IP Base、および IP Services のフラッシュ ファイルのサイズに制限されています。

- Control and Provisioning of Wireless Access Points（CAPWAP）などのプロトコルのデコードは、IP Base と IP Services でサポートされています。
- IP Base および IP Services では、ファイル モードにおいて、パケットはエクスポートされずにファイルに書き込まれます。
- 組み込みパケット キャプチャ（EPC）は、入力のマルチキャスト パケットのみをキャプチャし、出力の複製パケットはキャプチャしません。

ワイヤレス パケット キャプチャ

- ワイヤレス キャプチャの唯一の形式は CAPWAP トンネル キャプチャです。
- CAPWAP トンネルをキャプチャする場合、同じキャプチャ ポイントで他のインターフェイス タイプを接続ポイントとして使用することはできません。
- 複数の CAPWAP トンネルのキャプチャがサポートされています。
- コア フィルタは適用されず、CAPWAP トンネルをキャプチャする場合は省略する必要があります。
- CAPWAP データ トンネルをキャプチャするために、各 CAPWAP トンネルは物理的ポートにマッピングされ、トラフィックをフィルタするための適切な ACL が適用されます。
- CAPWAP 非データ トンネルをキャプチャするため、スイッチはすべてのポート上のトラフィックをキャプチャし、トラフィックをフィルタするための適切な ACL を適用するように設定されます。

設定の制限

- Cisco IOS リリース 16.1 以降では、最大 8 つのキャプチャ ポイントを定義できる一方で、一度に 1 つのみをアクティブ化することができます。1 つ開始するには 1 つ停止する必要があります。
- VRF、管理ポート、プライベート VLAN はいずれも接続ポイントとして使用することはできません。
- Wireshark クラス マップでは、ACL は各タイプ（IPv4、IPv6、MAC）で 1 つのみ許可されます。クラス マップでは、IPv4 に 1 つ、IPv6 に 1 つ、MAC に 1 つの最大 3 つの ACL が可能です。
- Wireshark は宛先 SPAN ポートでパケットをキャプチャできません。
- Wireshark は、キャプチャ ポイントにアタッチされる接続ポイント（インターフェイス）のいずれかが動作を停止するとキャプチャを停止します。たとえば、接続ポイントに関連付けられているデバイスがスイッチから切断された場合です。キャプチャを再開するには、手動で再起動する必要があります。
- CPU 注入されたパケットは、コントロールプレーン パケットと見なされます。したがって、これらのタイプのパケットはインターフェイスの出力キャプチャではキャプチャされません。

- MAC ACL は、ARP などの非 IP パケットだけに使用されます。レイヤ 3 ポートまたは SVI ではサポートされません。
- MAC フィルタは、MAC アドレスに一致しても IP パケットをキャプチャしません。これは、すべてのインターフェイス（L2 スイッチ ポート、L3 ルーテッド ポート）に適用されます。
- MAC フィルタは、L3 インターフェイスと L2 パケット（ARP）をキャプチャすることはできません。
- IPv6 ベースの ACL は VACL ではサポートされません。
- レイヤ 2 EtherChannels はサポートされません。
- Cisco IOS リリース 16.1 以降では、レイヤ 3 PortChannel サポートが使用できます。
- キャプチャがすでにアクティブである、または開始されている場合、キャプチャ ポイント パラメータを変更することはできません。
- ACL ロギングおよび Wireshark には互換性がありません。Wireshark はアクティブになると優先されます。任意のポートにロギング中の ACL にキャプチャされているものも含めたすべてのトラフィックが Wireshark にリダイレクトされます。Wireshark を開始する前に、ACL ロギングを非アクティブにすることをお勧めします。これを実行しないと、Wireshark のトラフィックは ACL ロギング トラフィックに汚染されます。
- Wireshark は floodblock によってドロップされるパケットをキャプチャしません。
- 同じポートの PACL および RACL の両方をキャプチャすると、1 つのコピーだけが CPU に送信されます。DTLS 暗号化 CAPWAP インターフェイスをキャプチャすると、暗号化されたものと復号化されたものの 2 つのコピーが Wireshark に送信されます。DTLS 暗号化 CAPWAP トラフィックを運ぶレイヤ 2 インターフェイスをキャプチャすると同じ動作が発生します。コア フィルタは外部 CAPWAP ヘッダーに基づいています。
- Cisco IOS リリース 16.1 以降：
  - L3 ポート チャネルのサポートが追加されます。
  - 表示形式がマイナーチェンジされました。
  - cap ファイルのパケット数を表示する機能
  - キャプチャされたバッファをクリアすると、その内容とともにバッファも削除されます。パケット キャプチャがアクティブなときに実行することはできません。
  - 追加の警告メッセージが、コントロール プレーンのキャプチャで表示されます。
  - バッファ モードでは、パケットの表示は停止後のみに許可されます。
  - IP Base および IP Services にて停止のときに表示されるパケットの統計情報。
  - pcap ファイルでキャプチャされたパケット数を問い合わせる機能。
  - 表示が cap ファイルからの場合、packet-number を使用して指定されたパケットの詳細を表示できます。
  - 表示フィルタは、ファイル モードで使用可能です。

- パケット キャプチャの統計情報（受信またはドロップされたパケットおよびバイト）は、キャプチャ中またはキャプチャ停止後のいずれかに表示できます。
- システムは、Wireshark でサポートされるように、pcap/cap ファイルの内容に関する統計情報について問い合わせることができます。
- パケット キャプチャ セッションは、バッファのサイズに関係なく常にストリーミング モードです。ロックステップ モードは使用できません。
- アクティブなキャプチャ ポイントのバッファのクリアは、内容をクリアするだけのため、LAN Base でのみサポートされています。他のすべてのライセンスでは、バッファ自体が削除されるため、キャプチャがアクティブなときに実行することはできません。

警告 コントロール プレーン パケットは、レート制限とパフォーマンスへの影響はありません。コントロール プレーン パケットのキャプチャを制限するフィルタを使用してください。

- ユーザがスイッチ ポートからルーテッド ポート（L2>L3）へ、またはその逆へインターフェイスを変更した場合、インターフェイスが再び起動したときに、そのキャプチャ ポイントを削除し、新しいファイルを作成する必要があります。キャプチャ ポイントの停止/開始が機能しません。
- ユーザがアクティブなキャプチャ セッションで使用されたファイルを削除した場合、そのキャプチャ セッションは新しいファイルを作成できないため、キャプチャされたすべてのパケットが失われます。ユーザは、キャプチャ ポイントを再起動する必要があります。

パケット キャプチャの概要

パケット キャプチャ ツールの概要

パケット キャプチャ機能は、オンボードのパケット キャプチャ ファシリティです。ネットワーク管理者がデバイスを出入りするかデバイスを通るパケットをキャプチャすることで、パケットをローカルで分析したり、Wireshark や Embedded Packet Capture（EPC）のようなツールを使用するオフライン分析に向けてパケットを保存してエクスポートしたりできるようにするものです。この機能は、デバイスがネットワークの管理と操作にアクティブに参加できるようにすることによって、ネットワーク操作を簡略化します。この機能は、パケットの形式に関する情報を収集することによって、トラブルシューティングを容易にします。また、アプリケーションの分析とセキュリティも容易にします。

Embedded Packet Capture は LAN Base でサポートされています。Wireshark を使用する Embedded Packet Capture は、IP Base および IP Services でサポートされています。

Wireshark について

Wireshark の概要

Wireshark は、複数のプロトコルをサポートし、テキストベース ユーザ インターフェイスで情報を提供する、以前は Ethereal と呼ばれていたパケット アナライザ プログラムです。

トラフィックをキャプチャおよび分析する機能により、ネットワーク アクティビティにデータを提供します。Cisco IOS Release XE 3.3.0(SE) 以前のリリースでは、このニーズに対応したのは SPAN およびデバッグ プラットフォーム パケットの 2 つの機能だけでした。これらにはいずれも制限があります。SPAN は、パケットのキャプチャにおいては理想的ですが、指定したローカルまたはリモートの宛先にパケットを転送することによりこれを実現しているだけで、ローカル表示や分析をサポートしていません。

そのため、ハードウェアおよびソフトウェア送信トラフィックの両方に適用可能で、可能なら既知のインターフェイスを使用した高度なパケット キャプチャ、表示、および分析サポートを提供する、トラフィック キャプチャおよび分析機構のニーズが存在します。

Wireshark は、.pcap と呼ばれる既知の形式を使用してファイルへパケットをダンプし、個々のインターフェイスに対して適用されイネーブルになります。EXEC モードでインターフェイスを指定し、フィルタおよび他のパラメータも指定します。Wireshark アプリケーションは、**start** コマンドを入力した場合にだけ適用され、Wireshark が自動または手動でキャプチャを停止した場合にだけ削除されます。

（注） スイッチにインストールされている Wireshark の現在のバージョンは 1.10.8 です。

キャプチャ ポイント

キャプチャ ポイントとは、Wireshark 機能の一元的なポリシー定義です。キャプチャ ポイントは、どのパケットをキャプチャするか、どこからキャプチャするか、キャプチャ パケットに何を実行するか、およびいつ停止するかなど、Wireshark の特定のインスタンスに関連付けられたすべての特徴を説明します。キャプチャ ポイントは作成後に変更される場合があり、**start** コマンドを使用して明示的にアクティブ化しない限り、アクティブになりません。このプロセスは、キャプチャ ポイントのアクティブ化またはキャプチャ ポイントの開始といいます。キャプチャ ポイントは名前で識別され、手動または自動で非アクティブ化または停止する場合もあります。

複数のキャプチャ ポイントを定義してできますが、一度にアクティブにできるのは 1 つだけです。1 つ開始するには 1 つ停止する必要があります。

スタック構成のシステムの場合、キャプチャ ポイントはアクティブなメンバーによりアクティブ化されます。スイッチオーバーが発生すると、アクティブなすべてのパケット キャプチャ セッションが終了し、再起動する必要があります。

関連トピック

キャプチャ ポイントの定義, （857 ページ）

キャプチャ ポイント パラメータの追加または変更，（862 ページ）
キャプチャ ポイント パラメータの削除，（865 ページ）
キャプチャ ポイントの削除，（867 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（868 ページ）
キャプチャ ポイント バッファのクリア，（872 ページ）
例：単純なキャプチャおよび表示，（881 ページ）
例：単純なキャプチャおよび保存，（883 ページ）
例：バッファのキャプチャの使用，（885 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存，（891 ページ）

接続ポイント

接続ポイントは、キャプチャポイントに関連付けられた論理パケットのプロセスパスのポイントです。接続ポイントはキャプチャ ポイントの属性です。接続ポイントに影響するパケットはキャプチャ ポイント フィルタに対してテストされます。一致するパケットはキャプチャ ポイントの関連する Wireshark インスタンスにコピーされ、送信されます。特定のキャプチャ ポイントを複数の接続ポイントに関連付けることができます。異なるタイプ接続ポイントの混合に制限はありません。一部の制限は、異なるタイプの添付ポイントを指定すると適用されます。接続ポイントは、常に双方向であるレイヤ 2 VLAN の接続ポイントを除き、方向性あり（入力/出力/両方）です。

スタック型システムの場合では、すべてのスタック メンバの接続ポイントに有効です。EPC は定義されたすべての接続ポイントからパケットをキャプチャします。ただし、これらのパケットはアクティブ メンバーでのみに処理されます。

関連トピック

キャプチャ ポイントの定義，（857 ページ）
キャプチャ ポイント パラメータの追加または変更，（862 ページ）
キャプチャ ポイント パラメータの削除，（865 ページ）
キャプチャ ポイントの削除，（867 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（868 ページ）
キャプチャ ポイント バッファのクリア，（872 ページ）
例：単純なキャプチャおよび表示，（881 ページ）
例：単純なキャプチャおよび保存，（883 ページ）
例：バッファのキャプチャの使用，（885 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存，（891 ページ）

Filters

フィルタは、Wiresharkにコピーされ、渡されるキャプチャ ポイントの接続ポイントを通過するトラフィックのサブセットを識別し制限するキャプチャ ポイントの属性です。Wiresharkで表示されるためには、パケットは接続ポイントと、キャプチャ ポイントに関連付けられたすべてのフィルタも通過する必要があります。

キャプチャ ポイントには以下のタイプのフィルタがあります。

- コア システム フィルタ：コア システム フィルタはハードウェアによって適用され、一致基準はハードウェアによって制限されます。このフィルタは、ハードウェア転送トラフィックが Wireshark の目的でソフトウェアにコピーするかどうかを決定します。
- 表示フィルタ：表示フィルタは、Wiresharkによって適用されます。表示フィルタに失敗したパケットは表示されません。

コア システム フィルタ

クラス マップまたはACLを使用して、またはCLIを使用して明示的にコア システム フィルタの一致基準を指定できます。

（注） CAPWAP を接続ポイントとして指定すると、コア システム フィルタは使用されません。

一部のインストール済み環境では、承認プロセスが長い場合さらに遅延を引き起こす可能性があるスイッチの設定を変更する権限を取得する必要があります。これにより、ネットワーク管理者の機能がトラフィックの監視および分析に制限される場合があります。この状況に対処するため、Wireshark は、EXEC モード CLI から、コア システム フィルタ一致基準の明示的な仕様をサポートします。この対処方法の欠点は、指定できる一致基準が、クラス マップがサポートする対象の限定的なサブセットである（MAC、IP 送信元アドレスおよび宛先アドレス、イーサネット タイプ、IP プロトコル、および TCP/UDP の発信元および宛先ポートなど）ことです。

コンフィギュレーションモードを使用する場合はACLを定義するか、クラスマップでそこへキャプチャ ポイントを参照させることができます。明示的かつ ACL ベースの一致基準がクラス マップとポリシー マップの作成に内部的に使用されます。

注：ACL およびクラス マップの設定はシステムの一部であり、Wireshark 機能の側面ではありません。

表示フィルタ

表示フィルタを使用すると、.pcapファイルからデコードして表示するときに表示するパケットの集合をさらに絞り込むように Wireshark に指示できます。

関連トピック

その他の参考資料

Actions

Wireshark はライブ トラフィックまたは前の既存 .pcap ファイルで呼び出すことができます。ライブ トラフィックに対して起動されたとき、その表示フィルタを通過するパケットに対して次の 4 種類の処理を実行できます。

- デコード、分析、保存のためにメモリ内バッファへキャプチャ
- .pcap ファイルへ保存
- デコードおよび表示
- 保存および表示

.pcap ファイルのみに対して起動された場合は、デコードと表示の処理だけが適用できます。

キャプチャ パケットのメモリ内のバッファへのストレージ

パケットは、メモリ内のキャプチャ バッファに格納して、後でデコード、分析、または .pcap ファイルへ保存できます。

キャプチャ バッファは線形モードまたは循環モードを選択できます。線形モードでは、バッファが上限に達すると、新しいパケットが廃棄されます。循環モードでは、バッファが上限に達すると、新しいパケットを格納するために最も古いパケットが廃棄されます。必要に応じてバッファをクリアすることもできますが、このモードは、ネットワーク トラフィックのデバッグに主に使用されます。ただし、これを削除せずに、バッファの内容をクリアだけすることはできません。これを有効にするためには、現行のキャプチャを停止し、キャプチャをもう一度再起動します。

（注） パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。

.pcap ファイルにキャプチャされたパケットのストレージ

（注） WireSharkがスタック内のスイッチで使用される場合は、パケット キャプチャをアクティブ スイッチに接続されたフラッシュまたは USB フラッシュ デバイスにのみ保存できます。

たとえば、flash1 がアクティブなスイッチに接続されており、flash2 がセカンダリ スイッチに接続されている場合、flash1 にのみパケット キャプチャを保存できます。

アクティブ スイッチに接続されたフラッシュまたはUSB フラッシュ デバイス以外のデバイスにパケット キャプチャを保存しようとすると、エラーが発生する場合があります。

Wireshark は .pcap ファイルにキャプチャされたパケットを保存できます。キャプチャ ファイルは次のストレージ デバイスに配置可能です。

- スイッチオンボード フラッシュ ストレージ（flash:）

- USB ドライブ(usbflash0:)

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

Wireshark のキャプチャ ポイントを設定する場合は、ファイル名を関連付けることができます。キャプチャ ポイントをアクティブにすると、Wireshark は指定された名前でファイルを作成し、パケットを書き込みます。キャプチャ ポイントの作成時にファイルがすでに存在する場合、Wireshark はファイルを上書きできるかどうかについて問い合わせます。キャプチャポイントの有効化時にファイルがすでに存在する場合、Wireshark は既存のファイルを上書きします。特定のファイル名には 1 つのキャプチャ ポイントのみ関連付けることができます。

Wireshark が書き込んでいるファイル システムが一杯になると、Wireshark はファイルの一部のデータで失敗します。そのため、キャプチャ セッションを開始する前に、ファイル システムに十分な領域があることを確認する必要があります。Cisco IOS Release IOS XE 3.3.0(SE) では、ファイル システムの完全なステータスは一部のストレージ デバイスに対しては検出されません。

パケット全体ではなくセグメントのみを保持して、必要な記憶域を減らすことができます。通常、最初の 64 または 128 バイトを超える詳細は不要です。デフォルトの動作は、パケット全体の保存です。

ファイルシステムを処理し、ファイルシステムへの書き込みを行う際、パケットのドロップの発生を避けるため、Wireshark ではオプションでメモリ バッファを使用してパケットの到着時に一時的に保持できます。メモリ バッファのサイズは、キャプチャ ポイントが .pcap ファイルに関連付けられる際に指定できます。

パケットのデコードおよび表示

Wireshark はコンソールにパケットをデコードして表示できます。この機能は、ライブ トラフィックに適用されるキャプチャ ポイントと前の既存 .pcap ファイルに適用されるキャプチャ ポイントで使用可能です。

（注） パケットをデコードして表示すると、CPU への負荷が高くなる場合があります。

Wireshark は、幅広い種類のパケット形式に対してパケット詳細をデコードおよび表示できます。詳細は、**monitor capture name start** コマンドを以下のキーワード オプション付きですることにより表示されます。これにより、表示およびデコード モードが開始します。

- brief：パケットごとに 1 行表示します（デフォルト）。
- detailed：プロトコルがサポートされているすべてのパケットのすべてのフィールドをデコードして表示します。詳細モードでは、他の 2 種類のモードよりも多くの CPU が必要です。
- (hexadecimal) dump：パケット データの 16 進ダンプおよび各パケットの印刷可能文字としてパケットごとに 1 行表示します。

capture コマンドをデコードおよび表示オプション付きで入力すると、Wireshark 出力が Cisco IOS に返され、変更なしでコンソールに表示されます。

ライブ トラフィックの表示

Wireshark はコア システムからパケットのコピーを受信します。Wireshark は、表示フィルタを適用して、不要なパケットを破棄し、残りのパケットをデコードおよび表示します。

.pcap ファイルの表示

Wireshark は、以前に保存された .pcap ファイルからのパケットをデコードして表示し、選択的にパケットを表示するように表示フィルタに指示できます。

パケットのストレージおよび表示

機能的には、このモードは以前の 2 種類のモードの組み合わせです。Wireshark は指定された .pcap ファイルにパケットを保存し、これらをコンソールにデコードおよび表示します。ここではコア フィルタ フィルタだけが該当します。

Wireshark キャプチャ ポイントのアクティブ化および非アクティブ化

Wireshark のキャプチャ ポイントが、接続ポイント、フィルタ、アクション、およびその他のオプションで定義された場合、Wireshark をアクティブにする必要があります。キャプチャ ポイントがアクティブになるまで、実際にパケットをキャプチャしません。

キャプチャ ポイントがアクティブになる前に、一部の機能性チェックが実行されます。キャプチャ ポイントは、コア システム フィルタと接続ポイントのどちらも定義されていない場合はアクティブにできません。これらの要件を満たしていないキャプチャ ポイントをアクティブ化しようとすると、エラーが生成されます。*

（注） *ワイヤレス キャプチャを CAPWAP トンネリング インターフェイスで実行する場合、コア システムのフィルタは必要なく、使用することができません。

表示フィルタを、必要に応じて指定します。

Wireshark のキャプチャ ポイントはアクティブになると、複数の方法で非アクティブにできます。.pcap ファイルにパケットを格納するだけのキャプチャ ポイントは手動で停止することも、また時間制限またはパケット制限付きで設定することもでき、その後でキャプチャ ポイントは自動的に停止します。

Wireshark のキャプチャ ポイントがアクティブになると、固定レート ポリサーがハードウェアに自動的に適用され、CPU が Wireshark によって指示されたパケットでフラッディングしないようになります。レート ポリサーの短所は、リソースが使用可能な場合でも、確立されたレートを超えて連続するパケットをキャプチャできないことです。

パケット キャプチャ設定レートは、1 秒あたり 1000 パケット（pps）です。1000 pps の制限は、すべての接続ポイントの合計に適用されます。たとえば、3 つの接続ポイントにキャプチャ セッションがあれば、3 つの接続ポイントすべてのレートの合計が 1000 pps にポリシングされます。

（注） ポリサーは、コントロール プレーン パケット キャプチャではサポートされていません。コントロール プレーン キャプチャ ポイントを有効化するときは、CPU があふれないよう慎重に行う必要があります。

Wireshark 機能

ここでは、Wireshark 機能が スイッチ 環境でどのように動作するかについて説明します。

- ポート セキュリティおよび Wireshark が入力キャプチャに適用された場合でも、ポート セキュリティによってドロップされたパケットは Wireshark でキャプチャされます。ポート セキュリティが入力キャプチャに適用され、Wireshark が出力キャプチャに適用された場合、ポート セキュリティによってドロップされたパケットは Wireshark ではキャプチャされません。
- ダイナミック ARP インスペクション（DAI）によってドロップされたパケットは Wireshark ではキャプチャされません。
- STP ブロック ステートのポートが接続ポイントとして使用され、コア フィルタが一致する場合、Wireshark は、パケットがスイッチにドロップされる場合でもポートに入ってくるパケットをキャプチャします。
- 分類ベースのセキュリティ機能：入力分類ベースのセキュリティ機能によってドロップされたパケット（ACL および IPSG など）は同じ層の接続ポイントに接続する Wireshark キャプチャ ポイントでは検出されません。一方、出力分類ベースのセキュリティ機能によってドロップされたパケットは、同じ層の接続ポイントに接続されている Wireshark のキャプチャ ポイントでキャッチされます。論理モデルは、Wireshark の接続ポイントが、入力側のセキュリティ機能のルックアップ後、および出力側のセキュリティ機能のルックアップ前に発生することです。

  入力では、パケットはレイヤ 2 ポート、VLAN、およびレイヤ 3 ポート/SVI を介して送信されます。出力では、パケットはレイヤ 3 ポート/SVI、VLAN、およびレイヤ 2 ポートを介して送信されます。接続ポイントがパケットがドロップされるポイントの前にある場合、Wireshark はパケットをキャプチャします。これ以外の場合は、Wireshark はパケットをキャプチャしません。たとえば、入力方向のレイヤ 2 接続ポイントに接続される Wireshark のキャプチャ ポリシーはレイヤ 3 分類ベースのセキュリティ機能によってドロップされたパケットをキャプチャします。対照的に、出力方向のレイヤ 3 接続ポイントに接続する Wireshark のキャプチャ ポリシーは、レイヤ 2 分類ベースのセキュリティ機能によりドロップされたパケットをキャプチャします。
- ルーテッド ポートおよびスイッチ仮想インターフェイス（SVIs）：SVI の出力から送信されるパケットは CPU で生成されるため、Wireshark は SVI の出力をキャプチャできません。これらのパケットをキャプチャするには、コントロールプレーンを接続ポイントとして含めます。

- VLAN：Cisco IOS リリース 16.1 以降、VLAN が Wireshark の接続ポイントとして使用されている場合、パケット キャプチャは、入力方向と出力方向の両方の L2 と L3 でサポートされます。
- リダイレクション機能：入力方向では、レイヤ 3（PBR および WCCP など）でリダイレクトされる機能トラフィックは、レイヤ 3 の Wireshark の接続ポイントよりも論理的に後です。Wireshark は、後で別のレイヤ 3 インターフェイスにリダイレクトされる可能性がある場合でも、これらのパケットをキャプチャします。対照的に、レイヤ 3 によってリダイレクトされる出力機能（出力 WCCP など）は論理的にレイヤ 3 接続ポイントの前にあり、Wireshark ではキャプチャされません。
- SPAN：Wireshark は、SPAN 宛先として設定されたインターフェイスでパケットをキャプチャできません。
- SPAN：Wireshark は、入力方向の SPAN 送信元として設定されたインターフェイスでパケットをキャプチャできます。出力方向でも使用できる可能性があります。
- ACL が適用されていない場合、最大 1000 の VLAN からパケットを一度にキャプチャできます。ACL が適用されている場合、Wireshark の使用できるハードウェア領域はより少なくなります。結果として、パケット キャプチャに一度に使用できる VLAN の最大数は低くなります。1000 以上の VLAN トンネルを一度に使用したり、ACL を多数使用すると予測されない結果が生じる可能性があります。たとえば、モビリティがダウンする可能性があります。

（注） 過剰な CPU 使用につながり、予測されないハードウェア動作の原因となる可能性があるため、過剰な数の接続ポイントを一度にキャプチャしないことを強くお勧めします。

Wireshark でのワイヤレス パケット キャプチャ

- ワイヤレス トラフィックは CAPWAP パケット内にカプセル化されます。ただし、CAPWAP トンネル内の特定のワイヤレス クライアントのトラフィックだけの検出は、CAPWAP トンネルを接続ポイントとして使用する場合はサポートされません。特定のワイヤレス クライアントのトラフィックだけをキャプチャするには、クライアント VLAN を接続ポイントとして使用し、それに応じてコア フィルタを設定します。
- 内部ワイヤレス トラフィックのデコードは制限付きでサポートされます。暗号化された CAPWAP トンネル内の内部ワイヤレス パケットのデコードはサポートされません。
- 同じキャプチャ ポイント上で他のインターフェイス タイプを CAPWAP トンネリング インターフェイスと併用することはできません。CAPWAP トンネリング インターフェイスおよびレベル 2 ポートは、同じキャプチャ ポイントの接続ポイントにはできません。
- CAPWAP トンネルを介して Wireshark にパケットをキャプチャする場合、コア フィルタの指定はできません。ただし、Wireshark 表示フィルタを使用して、特定のワイヤレス クライアントに対してワイヤレス クライアントをフィルタすることができます。
- ACL が適用されていない場合、最大 135 の CAPWAP トンネルからパケットを一度にキャプチャできます。ACL が適用されている場合、Wireshark の使用できるハードウェア メモリ領

域はより少なくなります。結果として、パケット キャプチャに一度に使用できる CAPWAP トンネルの最大数は低くなります。一度に 135 以上の CAPWAP トンネル、または多くの ACL を使用すると予測できない結果が生じる場合があります。たとえば、モビリティがダウンする可能性があります。

（注） 過剰な CPU 使用につながり、予測されないハードウェア動作の原因となる可能性があるため、過剰な数の接続ポイントを一度にキャプチャしないことを強くお勧めします。

Wireshark のガイドライン

- Wireshark でのパケット キャプチャ中に、ハードウェア転送が同時に発生します。
- Wireshark のキャプチャ プロセスを開始する前に、CPU 使用率が妥当であり、十分なメモリ（少なくとも 200 MB）が使用可能であることを確認します。
- ストレージ ファイルにパケットを保存する予定の場合、Wireshark キャプチャ プロセスを開始する前に十分なスペースが利用可能であることを確認してください。
- Wireshark のキャプチャ中の CPU 使用率は、設定された基準に一致するパケットの数と、一致したパケット用のアクション（ストア、デコードして表示、あるいはこの両方）によって異なります。
- 高 CPU 使用率および他の不要な条件を避けるため、可能な限りキャプチャを最小限に抑えてください（パケット、期間による制限）。
- パケット転送はハードウェアで通常実行されるため、パケットは、ソフトウェア処理のために CPU にコピーされません。Wireshark のパケット キャプチャの場合、パケットは CPU にコピーされ、配信されて、これが CPU 使用率の増加につながります。

  CPU 使用率を高くしないようにするには、次の手順を実行します。

  - 関連ポートだけに接続します。
  - 一致条件を表すにはクラス マップを使用し、二次的にアクセス リストを使用してください。いずれも実行可能でない場合は、明示的な、インライン フィルタを使用します。
  - フィルタ規則に正しく準拠させます。緩和されたのではなく制限的な ACL で、トラフィック タイプを（IPv4 のみなどに）制限して、不要なトラフィックを引き出します。

- パケット キャプチャを短い期間または小さなパケット番号に常に制限します。capture コマンドのパラメータにより、次を指定することができます。

  - キャプチャ期間
  - キャプチャされたパケットの数
  - ファイル サイズ
  - パケットのセグメント サイズ

- コア フィルタと一致するトラフィックが非常に少ないことが判明している場合は、制限なしでキャプチャ セッションを実行します。
- 次の場合に高い CPU（またはメモリ）使用率になる可能性があります。
  - キャプチャセッションをイネーブルにし長期間不在のままにして、予期しないトラフィックのバーストが起きた場合。
  - リング ファイルまたはキャプチャ バッファを使用してキャプチャ セッションを起動して、長期間不在のままにするとし、パフォーマンスまたはシステムヘルスの問題が引き起こされます。
- キャプチャ セッション中に、スイッチ のパフォーマンスやヘルスに影響する可能性のある Wireshark による高い CPU 使用率およびメモリ消費がないか監視します。こうした状況が発生した場合、Wireshark セッションをすぐに停止します。
- 大きなファイルの .pcap ファイルからのパケットをデコードして表示することは避けてください。代わりに、PC に .pcap ファイルを転送し PC 上で Wireshark を実行します。
- Wireshark インスタンスは最大 8 個まで定義できます。 .pcap ファイルまたはキャプチャ バッファからパケットをデコードして表示するアクティブな **show** コマンドは、1 個のインスタンスとしてカウントされます。ただし、アクティブにできるインスタンスは 1 つだけです。
- 実行中のキャプチャに関連付けられた ACL が変更された場合は常に、ACL 変更を有効にするにはキャプチャを再起動する必要があります。キャプチャを再起動しないと、変更前の元の ACL が継続して使用されます。
- パケット損失を防ぐには、次の点を考慮します。
  - ライブ パケットをキャプチャしている間は、CPU に負荷のかかる操作であるデコードと表示ではなく（特に detailed モードの場合）、保存のみを使用します（display オプションを指定しない場合）。
  - パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。
  - デフォルト バッファ サイズを使用し、パケットが失われている場合、バッファ サイズを増加してパケットの喪失を防ぐことができます。
  - フラッシュ ディスクへの書き込みは、CPUに負荷のかかる操作であるため、キャプチャレートが不十分な場合、バッファ キャプチャの使用をお勧めします。
  - Wireshark キャプチャ セッションは 1000 pps のレートで常にストリーミング モードで動作します。
- ストリーミング キャプチャ モードのレートは 1000 pps です。
- コンソール ウィンドウのライブ パケットをデコードして表示する場合は、Wireshark セッションが短いキャプチャ期間によって抑制されていることを確認します。

警告 期間制限がより長いまたはキャプチャ期間がない（**term len 0** コマンドを使用して auto-more サポートのない端末を使用した）Wireshark セッションでは、コンソールまたは端末が使用できなくなる場合があります。

- 高 CPU 使用率につながるライブ トラフィックのキャプチャに Wireshark を使用している場合、QoS ポリシーを一時的に適用して、キャプチャ プロセスが終了するまで実際のトラフィックを制限することを考慮してください。
- すべての Wireshark 関連のコマンドは EXEC モードで、コンフィギュレーション コマンドは、Wireshark にありません。

  Wireshark CLI でアクセス リストまたはクラス マップを使用する必要がある場合は、コンフィギュレーション コマンドでアクセス リストおよびクラス マップを定義する必要があります。
- 特定の順序はキャプチャ ポイントを定義する場合には適用されません。CLI で許可されている任意の順序でキャプチャ ポイント パラメータを定義できます。Wireshark CLI では、単一行のパラメータ数に制限はありません。これはキャプチャ ポイントを定義するために必要なコマンドの数を制限します。
- 接続ポイントを除くすべてのパラメータは、単一の値を取ります。通常、コマンドを再入力することにより、値を新しいものに置き換えることができます。ユーザの確認後にシステムが新しい値を受け入れ、古い値を上書きします。コマンドの **no** 形式は、新しい値の入力には必要はありませんが、パラメータの削除には必要です。
- Wireshark では 1 つ以上の接続ポイントを指定することができます。複数の接続ポイントを追加するには、新しい接続ポイントでコマンドを再入力します。接続ポイントを削除するには、コマンドの **no** 使用します。接続ポイントとしてインターフェイス範囲を指定できます。たとえば、**monitor capture mycap interface GigabitEthernet1/0/1 in** を入力します。ここではインターフェイス GigabitEthernet1/0/1 が接続ポイントです。

  またインターフェイス GigabitEthernet1/0/2 にも接続する必要がある場合、次のように、別の行で指定します。

  monitor capture mycap interface GigabitEthernet1/0/2 in
- キャプチャがアクティブなときは、キャプチャに対する変更を行うことはできません。
- 実行する処理は、いずれのパラメータが必須であるかを決定します。Wireshark CLI では、**start** コマンドを入力する前に任意のパラメータを指定または変更することができます。**Start** コマンドを入力すると、すべての必須パラメータが入力されたと判断した後にのみ Wireshark が開始します。
- キャプチャ ポイントの作成時にファイルがすでに存在する場合、クエリを発行し、ファイルの上書きについて確認します。キャプチャ ポイントのアクティブ化実行中にファイルがすでに存在する場合、Wireshark は既存のファイルを上書きします。
- コア フィルタは明示的なフィルタ、アクセス リスト、またはクラス マップにできます。これらのタイプの新しいフィルタを指定すると、既存のものを置き換えます。

（注） コア フィルタは、CAPWAP トンネル インターフェイスをキャプチャ ポイントの接続ポイントとして使用している場合を除き、必須です。

- 明示的な **stop** コマンドを使用するか、automore モードに **q** を入力して、Wireshark のセッションを終了します。セッションは、期間やパケット キャプチャの制限などの停止の条件が満たされたときに、自動的に終了します。
- ドロップされたパケットはキャプチャの最後に表示されません。ただし、ドロップされたサイズ超過のパケット数のみが表示されます。

デフォルトの Wireshark の設定

次の表は、デフォルトの Wireshark の設定を示しています。

機能	デフォルト設定
持続時間	制限なし
パケット	制限なし
パケット長	制限なし（フル パケット）
ファイル サイズ	制限なし
リング ファイル ストレージ	なし
バッファのストレージ モード	線形

Embedded Packet Capture について

Embedded Packet Capture の概要

Embedded Packet Capture（EPC）は、パケットのトレースとトラブルシューティングに役立つ組み込みシステム管理機能を提供します。この機能を使用すると、ネットワーク管理者は、シスコ デバイスを出入りするか通過するデータ パケットをキャプチャできます。ネットワーク管理者は、キャプチャ バッファ サイズとタイプ（循環またはリニア）およびキャプチャする各パケットの最大バイト数を定義する場合があります。パケット キャプチャ レートは、詳細な管理制御を使用してスロットリングできます。たとえば、アクセス コントロール リストを使用してキャプチャ対象パケットをフィルタリングするオプションや、最大パケット キャプチャ レートまたはサンプリング間隔の指定などの詳細な定義を行うオプションが利用できます。

組み込みパケット キャプチャの利点

- デバイスでIPv4およびIPv6パケットをキャプチャでき、MACフィルタを使用したり、MACアドレスをマッチさせたりして、非IPパケットもキャプチャ可能。
- パケット キャプチャ ポイントをイネーブルにする拡張可能なインフラストラクチャキャプチャ ポイントは、パケットがキャプチャされ、バッファと関連付けられるトラフィック トランジット ポイントです。
- 外部ツールを使用した分析に適したパケット キャプチャ ファイル（PCAP）形式でパケットキャプチャをエクスポートする機能。
- さまざまな詳細レベルでキャプチャされたデータ パケットをデコードする方法。

パケット データ キャプチャ

パケットデータキャプチャは、バッファに格納されるデータパケットのキャプチャです。パケット データ キャプチャは、一意の名前とパラメータを入力することによって定義します。

こうしたキャプチャでは、次のアクションを実行できます。

- インターフェイスでのキャプチャのアクティブ化。
- キャプチャ ポイントへのアクセス コントロール リスト（ACL）やクラス マップの適用。

（注） Network Based Application Recognition（NBAR）とMACスタイルのクラス マップは、サポートされていません。

- キャプチャの破棄。
- サイズやタイプなどのバッファ ストレージ パラメータの指定。サイズの範囲は1 ～ 100 MBです。デフォルトのバッファは線形です。もう1つのバッファ オプションは循環です。
- プロトコル、IPアドレス、ポート アドレスに関する情報を含む一致基準の指定。

関連トピック

パケット データ キャプチャの管理, （874 ページ）

例：パケット データ キャプチャの管理, （893 ページ）

キャプチャされたデータのモニタリングとメンテナンス, （876 ページ）

例：キャプチャされたデータのモニタリングおよびメンテナンス, （893 ページ）

パケット キャプチャの設定

Wireshark の設定方法

Wireshark を設定するには、次の基本的な手順を実行します。

1 キャプチャ ポイントを定義します。

2 （任意）キャプチャ ポイントのパラメータを追加または変更します。

3 キャプチャ ポイントをアクティブ化または非アクティブ化します。

4 キャプチャ ポイントを今後使用しない場合は削除します。

関連トピック

キャプチャ ポイントの定義，（857 ページ）
キャプチャ ポイント パラメータの追加または変更，（862 ページ）
キャプチャ ポイント パラメータの削除，（865 ページ）
キャプチャ ポイントの削除，（867 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（868 ページ）
キャプチャ ポイント バッファのクリア，（872 ページ）
例：単純なキャプチャおよび表示，（881 ページ）
例：単純なキャプチャおよび保存，（883 ページ）
例：バッファのキャプチャの使用，（885 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存，（891 ページ）

キャプチャ ポイントの定義

この手順の例では、非常にシンプルなキャプチャ ポイントを定義します。必要に応じて、**monitor capture** コマンドの 1 つのインスタンスを使用してキャプチャ ポイントとそのすべてのパラメータを定義できます。

（注） 接続ポイント、キャプチャの方向、およびコア フィルタが機能するキャプチャ ポイントを持つよう定義する必要があります。

コア フィルタを定義する必要がないのは、CAPWAP トンネリング インターフェイスを使用してワイヤレス キャプチャ ポイントを定義する場合です。この場合、コア フィルタは定義しません。これは使用できません。

キャプチャ ポイントを定義するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show capwap summary**
3. **monitor capture** {*capture-name*} {**interface** *interface-type interface-id* | **control-plane**} {**in** | **out** | **both**}
4. **monitor capture** {*capture-name*}[**match** {**any** | **ipv4 any any** | **ipv6**} **any any**}]
5. **show monitor capture** {*capture-name*}[**parameter**]
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**show capwap summary** 例： スイッチ# **show capwap summary**	ワイヤレス キャプチャの接続ポイントとして使用できるCAPWAP トンネルを表示します。 （注） このコマンドは、ワイヤレス キャプチャを実行するためにCAPWAP トンネルを接続ポイントとして使用している場合にのみ使用します。例の項のCAPWAP の例を参照してください。
ステップ 3	**monitor capture** {*capture-name*} {**interface** *interface-type interface-id*	**control-plane**} {**in**	**out**	**both**} 例： スイッチ# **monitor capture mycap interface GigabitEthernet1/0/1 in**	キャプチャ ポイントを定義し、キャプチャ ポイントが関連付けられている接続ポイントを指定し、キャプチャの方向を指定します。 キーワードの意味は次のとおりです。 • *capture-name*：定義するキャプチャ ポイントの名前を指定します（例では mycap が使用されています）。キャプチャ名の長さは 8 文字以下にしてください。英数字、アンダースコア（_）のみが許可されます • （任意）**interface***interface-type**interface-id*：キャプチャ ポイントが関連付けられる接続ポイントを指定します（例では GigabitEthernet1/0/1 が使用されています）。 （注） オプションで、このコマンド インスタンス 1 つでこのキャプチャ ポイントの複数の接続ポイントおよびパラメータすべてを定義できます。これらのパラメータについては、キャプチャ ポイント パラメータの変更に関する手順で説明されています。範囲のサポートは、接続ポイントを追加および削除するためにも使用できます。

	コマンドまたはアクション	目的
		interface-type には次のいずれかを使用します。 ◦ **GigabitEthernet**：接続ポイントを GigabitEthernet として指定します。 ◦ **vlan**：接続ポイントを VLAN として指定します。 （注） このインターフェイスを接続ポイントとして使用する場合は、入力キャプチャのみが可能です。 ◦ **capwap**：接続ポイントを CAPWAP トンネルとして指定します。 （注） このインターフェイスを接続ポイントとして使用すると、コア フィルタは使用できません。 • （任意）**control-plane**：接続ポイントとしてコントロール プレーンを指定します。 • **in**	**out**	**both**：キャプチャの方向を指定します。
ステップ 4	**monitor capture** {*capture-name*}[**match** {**any**	**ipv4 any any**	**ipv6**} **any any**}] 例： スイッチ# **monitor capture mycap interface GigabitEthernet1/0/1 in match any**	コア システムのフィルタを定義します。 （注） コア フィルタが使用できなくなるため、CAPWAP のトンネリング インターフェイスを接続ポイントとして使用する場合はこの手順を実行しないでください。 キーワードの意味は次のとおりです。 • *capture-name*：定義するキャプチャ ポイントの名前を指定します（例では mycap が使用されています）。 • **match**：フィルタを指定します。定義されている最初のフィルタはコア フィルタです。 （注） キャプチャ ポイントは、コア システム フィルタと接続ポイントのどちらも定義されていない場合はアクティブにできません。これらの要件を満たしていないキャプチャ ポイントをアクティブ化しようとすると、エラーが生成されます。 • **ipv4**：IP バージョン 4 のフィルタを指定します。 • **ipv6**：IP バージョン 6 のフィルタを指定します。

	コマンドまたはアクション	目的
ステップ 5	**show monitor capture** {*capture-name*}[**parameter**] 例： スイッチ# **show monitor capture mycap parameter** monitor capture mycap interface GigabitEthernet1/0/1 in monitor capture mycap match any	ステップ 2 で定義したキャプチャ ポイント パラメータを表示し、キャプチャ ポイントを定義したことを確認します。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

CAPWAP 接続ポイントでキャプチャ ポイントを定義するには次を実行します。

```
スイッチ# show capwap summary

CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 1
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0


Name   APName                           Type PhyPortIf Mode      McastIf
------ -------------------------------- ---- --------- --------- -------
Ca0    AP442b.03a9.6715                 data Gi3/0/6   unicast   -


Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU   Xact
------ --------------- ------- --------------- ------- ------ ----- ----
Ca0    10.10.14.32     5247    10.10.14.2      38514   No     1449  0

スイッチ# monitor capture mycap interface capwap 0 both
スイッチ# monitor capture mycap file location flash:mycap.pcap
スイッチ# monitor capture mycap file buffer-size 1
スイッチ# monitor capture mycap start

*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on

スイッチ# show monitor capture mycap parameter
   monitor capture mycap interface capwap  0 in
   monitor capture mycap interface capwap  0 out
   monitor capture mycap file location flash:mycap.pcap buffer-size 1
スイッチ#
```

```
スイッチ# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
スイッチ#
スイッチ# show monitor capture file flash:mycap.pcap
 1   0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 2   0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 3   2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 4   2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 5   3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 6   4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 7   4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 8   5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 9   5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
10   6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
11   8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
12   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
13   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
14   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
15   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
16   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
17   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
18   9.236987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
19  10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
20  10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
21  12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
22  12.239993   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
23  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
24  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
25  12.250994   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
26  12.256990   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
27  12.262987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
28  12.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
29  12.802012   10.10.14.3 -> 10.10.14.255 NBNS Name query NB WPAD.<00>
30  13.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
```

次の作業

さらなる接続ポイントを追加して、キャプチャ ポイントのパラメータを変更し、アクティブ化できます。または、キャプチャ ポイントをそのまま使用したい場合はすぐにアクティブ化することもできます。

（注） このトピックで説明されているメソッドを使用してキャプチャ ポイントのパラメータを変更することはできません。

ユーザが誤ったキャプチャ名、または無効/存在しない接続ポイントを入力すると、スイッチは、「Capture Name should be less than or equal to 8 characters.Only alphanumeric characters and underscore (_) is permitted」および「% Invalid input detected at '^' marker」のようなエラーを表示します。

関連トピック

Wireshark の設定方法, （857 ページ）
キャプチャ ポイント, （844 ページ）
接続ポイント, （845 ページ）
例：単純なキャプチャおよび表示, （881 ページ）
例：単純なキャプチャおよび保存, （883 ページ）
例：バッファのキャプチャの使用, （885 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存, （891 ページ）

キャプチャ ポイント パラメータの追加または変更

パラメータの値を指定する手順は、順番にリストされますが、任意の順序で実行できます。1行、2 行、または複数行で指定できます。複数指定が可能な接続ポイントを除き、同じオプションを再定義することで、任意の値をより最近の値に置き換えることができます。すでに指定された特定のパラメータが変更されている場合は、インタラクティブに確認する必要があります。

キャプチャ ポイントのパラメータを変更するには、次の手順を実行します。

はじめる前に

以下の手順を実行する前にキャプチャ ポイントを定義する必要があります。

手順の概要

1. **enable**
2. **monitor capture** {*capture-name*} **match** {**any** | **mac** *mac-match-string* | **ipv4** {**any** | **host** | **protocol**} {**any** | **host**} | **ipv6** {**any** | **host** | **protocol**} {**any** | **host**}}
3. **monitor capture** {*capture-name*} **limit** {[**duration** *seconds*][**packet-length** *size*][**packets** *num*]}
4. **monitor capture** {*capture-name*} **file** {**location** *filename*}
5. **monitor capture** {*capture-name*} **file** {**buffer-size** *size*}
6. **show monitor capture** {*capture-name*}[**parameter**]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture** {*capture-name*} **match** {**any**	**mac** *mac-match-string*	**ipv4** {**any**	**host**	**protocol**} {**any**	**host**}	**ipv6** {**any**	**host**	**protocol**} {**any**	**host**}} 例： スイッチ# **monitor capture mycap match ipv4 any any**	明示的に、またはACLを介して、またはクラス マップを介して定義されたコア システム フィルタ（**ipv4 any any**）を定義します。 （注） CAPWAPトンネリング インターフェイスを使用してワイヤレス キャプチャを定義している場合、このコマンドには効果がないので使用しないでください。
ステップ 3	**monitor capture** {*capture-name*} **limit** {[**duration** *seconds*][**packet-length** *size*][**packets** *num*]} 例： スイッチ# **monitor capture mycap limit duration 60 packet-len 400**	秒単位のセッション制限（60）、キャプチャされたパケット、またはWiresharkによって保持されるパケット セグメント長（400）を指定します。
ステップ 4	**monitor capture** {*capture-name*} **file** {**location** *filename*} 例： スイッチ# **monitor capture mycap file location flash:mycap.pcap**	キャプチャ ポイントがパケットを表示するだけでなくキャプチャできるようにする場合は、ファイルのアソシエーションを指定します。 （注） すでにファイルが存在する場合、それが上書きが可能かどうかを確認する必要があります。 （注） ファイル オプションは、LAN Baseライセンスには存在しません。

	コマンドまたはアクション	目的
ステップ 5	**monitor capture** {*capture-name*} **file** {**buffer-size** *size*} 例： スイッチ# **monitor capture mycap file buffer-size 100**	トラフィック バーストの処理に Wireshark で使用されるメモリ バッファのサイズを指定します。
ステップ 6	**show monitor capture** {*capture-name*}[**parameter**] 例： スイッチ# **show monitor capture mycap parameter** monitor capture mycap interface GigabitEthernet1/0/1 in monitor capture mycap match ipv4 any any monitor capture mycap limit duration 60 packet-len 400 monitor capture point mycap file location bootdisk:mycap.pcap monitor capture mycap file buffer-size 100	以前に定義したキャプチャ ポイント パラメータを表示します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

例

パラメータの変更

キャプチャ ファイルの関連付けまたは関連付け解除

```
スイッチ# monitor capture point mycap file location flash:mycap.pcap
スイッチ# no monitor capture mycap file
```

パケット バーストの処理にメモリ バッファ サイズを指定する

```
スイッチ# monitor capture mycap buffer size 100
```

IPv4 と IPv6 の両方に一致するように、明示的なコア システム フィルタを定義する

```
スイッチ# monitor capture mycap match any
```

次の作業

キャプチャ ポイントに必要なパラメータがすべて含まれている場合はアクティブ化します。

関連トピック

Wireshark の設定方法, （857 ページ）

キャプチャ ポイント, （844 ページ）

接続ポイント，（845 ページ）
例：単純なキャプチャおよび表示，（881 ページ）
例：単純なキャプチャおよび保存，（883 ページ）
例：バッファのキャプチャの使用，（885 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存，（891 ページ）

キャプチャ ポイント パラメータの削除

順番に表示されていますが、パラメータを削除する手順は任意の順序で実行できます。1 行、2 行、または複数行で削除できます。複数が可能な接続ポイントを除いて、任意のパラメータを削除できます。

キャプチャ ポイントのパラメータを削除するには、次の手順を実行します。

はじめる前に

キャプチャ ポイント パラメータは、以下の手順を使用して削除する前に定義する必要があります。

手順の概要

1. **enable**
2. **no monitor capture** {*capture-name*} **match**
3. **no monitor capture** {*capture-name*} **limit** [**duration**][**packet-length**][**packets**]
4. **no monitor capture** {*capture-name*} **file** [**location**] [**buffer-size**]
5. **show monitor capture** {*capture-name*}[**parameter**]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**no monitor capture** {*capture-name*} **match** 例： `スイッチ# no monitor capture mycap match`	キャプチャ ポイント（mycap）で定義されているすべてのフィルタを削除します。

	コマンドまたはアクション	目的
ステップ 3	**no monitor capture** {*capture-name*} **limit** [**duration**][**packet-length**][**packets**] 例： スイッチ# **no monitor capture mycap limit duration packet-len** スイッチ# **no monitor capture mycap limit**	Wireshark によって保持されるセッション タイム制限およびパケット セグメント長を削除します。その他の指定された制限はそのままになります。 Wireshark のすべての制限をクリアします。
ステップ 4	**no monitor capture** {*capture-name*} **file** [**location**] [**buffer-size**] 例： スイッチ# **no monitor capture mycap file** スイッチ# **no monitor capture mycap file location**	ファイルの関連付けを削除します。キャプチャ ポイントはパケットをキャプチャしなくなります。表示だけが実行されます。 ファイル位置の関連付けを削除します。ファイル位置はキャプチャ ポイントとは関連付けられなくなります。ただし、他の定義されたファイル関連付けはこのアクションによっては影響を受けません。
ステップ 5	**show monitor capture** {*capture-name*}[**parameter**] 例： スイッチ# **show monitor capture mycap parameter** monitor capture mycap interface GigabitEthernet1/0/1 in	パラメータの削除操作後にまだ定義されているキャプチャ ポイントパラメータを表示します。このコマンドは、キャプチャ ポイントと関連付けられるパラメータを確認するために手順の任意の地点で実行できます。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

次の作業

キャプチャ ポイントに必要なパラメータがすべて含まれている場合はアクティブ化します。

（注） キャプチャ ポイントがアクティブなときにパラメータが削除されると、スイッチは「キャプチャがアクティブです（Capture is active）」というエラーを表示します。

関連トピック

Wireshark の設定方法，（857 ページ）
キャプチャ ポイント，（844 ページ）
接続ポイント，（845 ページ）

例：単純なキャプチャおよび表示，（881 ページ）
例：単純なキャプチャおよび保存，（883 ページ）
例：バッファのキャプチャの使用，（885 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存，（891 ページ）

キャプチャ ポイントの削除

キャプチャ ポイントを削除するには、次の手順を実行します。

はじめる前に

キャプチャ ポイントは、以下の手順を使用して削除する前に定義する必要があります。削除する前に、キャプチャ ポイントを停止する必要があります。

手順の概要

1. **enable**
2. **no monitor capture** {*capture-name*}
3. **show monitor capture** {*capture-name*}[**parameter**]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**no monitor capture** {*capture-name*} 例： スイッチ# **no monitor capture mycap**	指定されたキャプチャ ポイント（mycap）を削除します。
ステップ 3	**show monitor capture** {*capture-name*}[**parameter**] 例： スイッチ# **show monitor capture mycap parameter** Capture mycap does not exist	指定されたキャプチャ ポイントは削除されたため存在しないことを示すメッセージを表示します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

削除したものと同じ名前の新規キャプチャ ポイントを定義できます。これらの手順は通常、キャプチャ ポイントの定義をやり直したい場合に実行します。

関連トピック

Wireshark の設定方法，（857 ページ）
キャプチャ ポイント，（844 ページ）
接続ポイント，（845 ページ）
例：単純なキャプチャおよび表示，（881 ページ）
例：単純なキャプチャおよび保存，（883 ページ）
例：バッファのキャプチャの使用，（885 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存，（891 ページ）

キャプチャ ポイントをアクティブまたは非アクティブにする

キャプチャ ポイントをアクティブまたは非アクティブにするには、次の手順を実行します。

はじめる前に

接続ポイントおよびコア システム フィルタが定義され、関連付けられたファイル名がすでに存在する場合でも、キャプチャ ポイントはアクティブ化することができます。このようなケースでは、既存のファイルは上書きされます。

関連するファイル名のないキャプチャ ポイントは、表示するためだけにアクティブにできます。ファイル名が指定されていないと、パケットはバッファに保管されます。ライブ表示（キャプチャ時の表示）は、ファイルおよびバッファ モードの両方で使用できます。

表示フィルタを指定しない場合、パケットはライブ表示されず、コア システム フィルタによってキャプチャされたすべてのパケットが表示されます。デフォルトの表示モードは brief です。

（注） CAPWAP のトンネリング インターフェイスを接続ポイントとして使用すると、コア フィルタは使用されないため、この場合は定義する必要はありません。

手順の概要

1. **enable**
2. **monitor capture** {*capture-name*} **start**[**display** [**display-filter** *filter-string*]][**brief** | **detailed** | **dump**]
3. **monitor capture** {*capture-name*} **stop**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture** {*capture-name*} **start**[**display** [**display-filter** *filter-string*]][**brief**	**detailed**	**dump**] 例： スイッチ# **monitor capture mycap start display display-filter "stp"**	キャプチャ ポイントをアクティブ化し、「stp」を含むパケットだけが表示されるように表示をフィルタします。
ステップ 3	**monitor capture** {*capture-name*} **stop** 例： スイッチ# **monitor capture name stop**	キャプチャ ポイントを非アクティブにします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

キャプチャ ポイントをアクティブおよび非アクティブにする際に、いくつかのエラーが発生する可能性があります。次に、発生する可能性のあるエラーのいくつかの例を示します。

アクティブ化する際に接続ポイントが不明

```
Switch#monitor capture mycap match any
Switch#monitor capture mycap start
No Target is attached to capture failed to disable provision featurefailed to remove
policyfailed to disable provision featurefailed to remove policyfailed to disable provision
 featurefailed to remove policy
Capture statistics collected at software (Buffer):
 Capture duration - 0 seconds
 Packets received - 0
 Packets dropped - 0
 Packets oversized - 0

Unable to activate Capture.
Switch# unable to get action unable to get action unable to get action
Switch#monitor capture mycap interface g1/0/1 both
Switch#monitor capture mycap start
Switch#
*Nov 5 12:33:43.906: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

アクティブ化する際にフィルタが不明

```
Switch#monitor capture mycap int g1/0/1 both
Switch#monitor capture mycap start
Filter not attached to capture
Capture statistics collected at software (Buffer):
 Capture duration - 0 seconds
 Packets received - 0
 Packets dropped - 0
 Packets oversized - 0

Unable to activate Capture.
Switch#monitor capture mycap match any
```

```
Switch#monitor capture mycap start
Switch#
*Nov 5 12:35:37.200: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

キャプチャポイントがすでにアクティブ化されているのに、別のキャプチャポイントをアクティブ化しようとする

```
Switch#monitor capture mycap start
PD start invoked while previous run is active Failed to start capture : Wireshark operation
 failure
Unable to activate Capture.
Switch#show monitor capture

Status Information for Capture test
 Target Type:
 Interface: GigabitEthernet1/0/13, Direction: both
 Interface: GigabitEthernet1/0/14, Direction: both
 Status : Active
 Filter Details:
 Capture all packets
 Buffer Details:
 Buffer Type: LINEAR (default)
 Buffer Size (in MB): 10
 File Details:
 Associated file name: flash:cchh.pcap
 Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Maximum number of packets to capture per second: 1000
 Packet sampling rate: 0 (no sampling)

Status Information for Capture mycap
 Target Type:
 Interface: GigabitEthernet1/0/1, Direction: both
 Status : Inactive
 Filter Details:
 Capture all packets
 Buffer Details:
 Buffer Type: LINEAR (default)
 Buffer Size (in MB): 10
 File Details:
 File not associated
 Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Maximum number of packets to capture per second: 1000
 Packet sampling rate: 0 (no sampling)
Switch#monitor capture test stop
Capture statistics collected at software (Buffer & Wireshark):
 Capture duration - 157 seconds
 Packets received - 0
 Packets dropped - 0
 Packets oversized - 0

Switch#
*Nov 5 13:18:17.406: %BUFCAP-6-DISABLE: Capture Point test disabled.
Switch#monitor capture mycap start
Switch#
*Nov 5 13:18:22.664: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
Switch#
```

関連トピック

Wireshark の設定方法, （857 ページ）

キャプチャ ポイント, （844 ページ）

接続ポイント, （845 ページ）

例：単純なキャプチャおよび表示, （881 ページ）
例：単純なキャプチャおよび保存, （883 ページ）
例：バッファのキャプチャの使用, （885 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存, （891 ページ）

キャプチャ ポイント バッファのクリア

次の手順に従ってバッファ コンテンツをクリアするか、外部ファイルにストレージとして保存します。

（注） パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。アクティブなキャプチャ ポイントのバッファをクリアしないでください。

（注） アクティブなキャプチャ ポイントのバッファのクリアは、内容をクリアするだけのため、LAN Base でのみサポートされています。他のすべてのライセンスでは、バッファ自体が削除されるため、キャプチャがアクティブなときに実行することはできません。

手順の概要

1. **enable**
2. **monitor capture** {*capture-name*} [**clear** | **export** *filename*]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**monitor capture** {*capture-name*} [**clear** | **export** *filename*] 例： スイッチ# **monitor capture mycap clear**	clear：完全にバッファを削除します。 （注） clear コマンドを実行すると、 • LAN Base では、このコマンドはバッファを削除せずにバッファの内容をクリアします。 • 他のすべてのライセンスでは、このコマンドはバッファ自体を削除します。 export：バッファでキャプチャされたパケットを保存し、バッファを削除します。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

例：キャプチャ ポイント バッファの処理

キャプチャのファイルへのエクスポート

```
スイッチ# monitor capture mycap export flash:mycap.pcap
Storage configured as File for this capture
```

キャプチャ ポイント バッファのクリア

```
スイッチ# monitor capture mycap clear
 Capture configured with file options
```

次の作業

（注） LAN Base 以外のライセンスでキャプチャ ポイントのバッファをクリアしようとすると、スイッチは「*Failed to clear capture buffer : Capture Buffer BUSY*」エラーを表示します。

関連トピック

Wireshark の設定方法, （857 ページ）
キャプチャ ポイント, （844 ページ）
接続ポイント, （845 ページ）
例：単純なキャプチャおよび表示, （881 ページ）
例：単純なキャプチャおよび保存, （883 ページ）
例：バッファのキャプチャの使用, （885 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存, （891 ページ）

Embedded Packet Capture の実装方法

パケット データ キャプチャの管理

（注） アクティブなキャプチャ ポイントのエクスポートは、LAN Base ライセンスのみでサポートされています。他のすべてのライセンスでは、まずキャプチャを停止してからエクスポートをする必要があります。

バッファ モードでパケット データ キャプチャを管理するには、次の手順を実行します。

手順の概要

1. **enable**
2. **monitor capture***capture-name***access-list***access-list-name*
3. **monitor capture***capture-name***limit duration***seconds*
4. **monitor capture***capture-name***interface***interface-name***both**
5. **monitor capture***capture-name***buffer circular size***bytes*
6. **monitor capture***capture-name***start**
7. **monitor capture***capture-name***stop**
8. **monitor capture***capture-name***export***file-location/file-name*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture***capture-name***access-list***access-list--name* 例： スイッチ# **monitor capture mycap access-list v4acl**	アクセス リストをパケット キャプチャのコア フィルタとして指定し、モニタ キャプチャを設定します。
ステップ 3	**monitor capture***capture-name***limit duration***seconds* 例： スイッチ# **monitor capture mycap limit duration 1000**	モニタ キャプチャの制限を設定します。
ステップ 4	**monitor capture***capture-name***interface***interface--name***both** 例： スイッチ# **monitor capture mycap interface GigabitEthernet 0/0/1 both**	接続ポイントおよびパケット フロー方向を指定して、モニタ キャプチャを設定します。
ステップ 5	**monitor capture***capture-name***buffer circular size***bytes* 例： スイッチ# **monitor capture mycap buffer circular size 10**	パケットデータをキャプチャするようにバッファを設定します。
ステップ 6	**monitor capture***capture-name***start** 例： スイッチ# **monitor capture mycap start**	トラフィック トレース ポイントでパケット データのバッファへのキャプチャを開始します。
ステップ 7	**monitor capture***capture-name***stop** 例： スイッチ# **monitor capture mycap stop**	トラフィック トレース ポイントでパケット データのキャプチャを停止します。

	コマンドまたはアクション	目的
ステップ 8	**monitor capture***capture-name***export***file-location/file--name* 例： `スイッチ# monitor capture mycap export tftp://10.1.88.9/mycap.pcap`	分析のためにキャプチャされたデータをエクスポートします。
ステップ 9	**end** 例： `スイッチ# end`	特権 EXEC モードに戻ります。

次の作業

（注） LAN Base 以外のライセンスでアクティブなキャプチャ ポイントをエクスポートしようとすると、スイッチは、「Failed to Export : Capture Buffer BUSY」というエラーを表示します。

関連トピック

パケット データ キャプチャ，（856 ページ）

例：パケット データ キャプチャの管理，（893 ページ）

キャプチャされたデータのモニタリングとメンテナンス

キャプチャされたパケット データのモニタリングとメンテナンスを行うには、次の作業を実行します。キャプチャ バッファの詳細とキャプチャ ポイントの詳細を表示します。

手順の概要

1. **enable**
2. **show monitor capture***capture-buffer-name***buffer dump**
3. **show monitor capture***capture-buffer-name***parameter**
4. **debug epc capture-point**
5. **debug epc provision**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**show monitor capture***capture-buffer-name***buffer dump** 例： スイッチ# **show monitor capture mycap buffer dump**	（任意）キャプチャ パケットの 16 進数ダンプおよびそのメタデータを表示します。
ステップ 3	**show monitor capture***capture-buffer--name***parameter** 例： スイッチ# **show monitor capture mycap parameter**	（任意）キャプチャを指定するために使用されたコマンドのリストを表示します。
ステップ 4	**debug epc capture-point** 例： スイッチ# **debug epc capture-point**	（任意）パケット キャプチャ ポイントのデバッグをイネーブルにします。
ステップ 5	**debug epc provision** 例： スイッチ# **debug epc provision**	（任意）パケット キャプチャ プロビジョニングのデバッグをイネーブルにします。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

パケット データ キャプチャ，（856 ページ）
例：キャプチャされたデータのモニタリングおよびメンテナンス，（893 ページ）

パケット キャプチャのモニタリング

Wireshark の設定例

例：.pcap ファイルからの概要出力の表示

次のように入力して、.pcap ファイルからの出力を表示できます。

```
スイッチ# show monitor capture file flash:mycap.pcap brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=0/0, ttl=254
  2 0.000051000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=0/0, ttl=255 (request in 1)
  3 0.000908000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=1/256, ttl=254
  4 0.001782000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=1/256, ttl=255 (request in 3)
  5 0.002961000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=2/512, ttl=254
  6 0.003676000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=2/512, ttl=255 (request in 5)
  7 0.004835000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=3/768, ttl=254
  8 0.005579000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=3/768, ttl=255 (request in 7)
  9 0.006850000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=4/1024, ttl=254
 10 0.007586000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=4/1024, ttl=255 (request in 9)
 11 0.008768000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=5/1280, ttl=254
 12 0.009497000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=5/1280, ttl=255 (request in 11)
 13 0.010695000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=6/1536, ttl=254
 14 0.011427000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=6/1536, ttl=255 (request in 13)
 15 0.012728000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=7/1792, ttl=254
 16 0.013458000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=7/1792, ttl=255 (request in 15)
 17 0.014652000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=8/2048, ttl=254
 18 0.015394000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=8/2048, ttl=255 (request in 17)
 19 0.016682000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=9/2304, ttl=254
 20 0.017439000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=9/2304, ttl=255 (request in 19)
 21 0.018655000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=10/2560, ttl=254
 22 0.019385000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=10/2560, ttl=255 (request in 21)
 23 0.020575000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=11/2816, ttl=254
 --More‹
```

例：.pcap ファイルからの詳細出力の表示

次のように入力して、.pcap ファイルの出力詳細を表示できます。

```
スイッチ# show monitor capture file flash:mycap.pcap detailed
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  6, 2015 11:44:48.322497000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1446810288.322497000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 114 bytes (912 bits)
    Capture Length: 114 bytes (912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:icmp:data]
Ethernet II, Src: Cisco_f3:63:46 (00:e1:6d:f3:63:46), Dst: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)

    Destination: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        Address: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        Address: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not
ECN-Capable Transport))
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport)
(0x00)
    Total Length: 100
    Identification: 0x04ba (1210)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
    Header checksum: 0x8fc8 [validation disabled]
        [Good: False]
        [Bad: False]
    Source: 10.10.10.2 (10.10.10.2)
    Destination: 10.10.10.1 (10.10.10.1)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe4db [correct]
    Identifier (BE): 46 (0x002e)
    Identifier (LE): 11776 (0x2e00)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    Data (72 bytes)

0000  00 00 00 00 09 c9 8f 77 ab cd ab cd ab cd ab cd   .......w........
0010  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0020  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0030  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0040  ab cd ab cd ab cd ab cd                           ........
        Data: 0000000009c98f77abcdabcdabcdabcdabcdabcdabcdabcd...
```

```
        [Length: 72]

Frame 2: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
    Interface id: 0
```

例：.pcap ファイルからパケット ダンプ出力の表示

次のように入力して、パケット ダンプの出力を表示できます。

```
スイッチ# show monitor capture file flash:mycap.pcap dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0000  00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00   ..m1....m.cF..E.
0010  00 64 04 ba 00 00 fe 01 8f c8 0a 0a 0a 02 0a 0a   .d..............
0020  0a 01 08 00 e4 db 00 2e 00 00 00 00 00 00 09 c9   ................
0030  8f 77 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   .w..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd                                            ..

0000  00 e1 6d 31 f1 80 00 e1 6d 31 f1 80 08 00 45 00   ..m1....m1....E.
0010  00 64 04 ba 00 00 ff 01 8e c8 0a 0a 0a 01 0a 0a   .d..............
0020  0a 02 00 00 ec db 00 2e 00 00 00 00 00 00 09 c9   ................
0030  8f 77 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   .w..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd                                            ..

0000  00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00   ..m1....m.cF..E.
0010  00 64 04 bb 00 00 fe 01 8f c7 0a 0a 0a 02 0a 0a   .d..............
0020  0a 01 08 00 e4 d7 00 2e 00 01 00 00 00 00 09 c9   ................
0030  8f 7a ab cd ab cd ab cd ab cd ab cd ab cd ab cd   .z..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
```

例：表示フィルタを使用した .pcap ファイルからのパケットの表示

次のように入力して、出力された .pcap ファイルのパケットを表示できます。

```
スイッチ# show monitor capture file flash:mycap.pcap display-filter "ip.src == 10.10.10.2"
brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=0/0, ttl=254
  3 0.000908000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=1/256, ttl=254
  5 0.002961000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=2/512, ttl=254
  7 0.004835000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=3/768, ttl=254
  9 0.006850000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=4/1024, ttl=254
 11 0.008768000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=5/1280, ttl=254
 13 0.010695000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=6/1536, ttl=254
 15 0.012728000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=7/1792, ttl=254
 17 0.014652000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=8/2048, ttl=254
 19 0.016682000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=9/2304, ttl=254
 21 0.018655000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
```

```
seq=10/2560, ttl=254
 23 0.020575000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=11/2816, ttl=254
```

例: .pcap ファイルにキャプチャされたパケットの数を表示

入力して .pcap ファイルにキャプチャされたパケットの数を表示するには、入力:

```
スイッチ# show monitor capture file flash:mycap.pcap packet-count
File name:           /flash/mycap.pcap
Number of packets:   50
```

例：.pcap ファイルから単一パケット ダンプの表示

次のように入力して、.pcap ファイルから単一のパケット ダンプを表示できます。

```
スイッチ#  show monitor capture file flash:mycap.pcap packet-number 10 dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0000  00 e1 6d 31 f1 80 00 e1 6d 31 f1 80 08 00 45 00   ..m1....m1....E.
0010  00 64 04 be 00 00 ff 01 8e c4 0a 0a 0a 01 0a 0a   .d..............
0020  0a 02 00 00 ec ce 00 2e 00 04 00 00 00 00 09 c9   ................
0030  8f 80 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd
```

例: .pcap ファイルにキャプチャされたパケットの統計情報を表示

.pcap ファイルにキャプチャされたパケットの統計情報を表示するには、入力:

```
スイッチ# show monitor capture file flash:mycap.pcap statistics "h225,counter"
================== H225 Message and Reason Counter ==================
RAS-Messages:
Call Signalling:
=====================================================================
```

例：単純なキャプチャおよび表示

次の例は、レイヤ 3 インターフェイス ギガビット イーサネット 1/0/1 でトラフィックをモニタする方法を示しています。

ステップ 1：次のように入力して関連トラフィックで一致するキャプチャ ポイントを定義します。

```
スイッチ# monitor capture mycap interface GigabitEthernet1/0/3 in
スイッチ# monitor capture mycap match ipv4 any any
スイッチ# monitor capture mycap limit duration 60 packets 50
スイッチ# monitor capture mycap buffer size 100
```

CPU使用率の上昇を避けるため、制限として最も低いパケット数および時間が設定されています。

ステップ 2：次のように入力してキャプチャ ポイントが正確に定義されていることを確認します。

```
スイッチ# show monitor capture mycap parameter
      monitor capture mycap interface GigabitEthernet1/0/3 in
   monitor capture mycap match ipv4  any any
   monitor capture mycap buffer size 100
   monitor capture mycap limit packets 50 duration 60
```

```
スイッチ# show monitor capture mycap
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 100
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 50
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：キャプチャ プロセスを開始し、結果を表示します。

```
スイッチ# monitor capture mycap start display
 Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1   0.000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030, seq=0/0,
 ttl=254
  2   0.003682   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=1/256, ttl=254
  3   0.006586   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=2/512, ttl=254
  4   0.008941   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=3/768, ttl=254
  5   0.011138   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=4/1024, ttl=254
  6   0.014099   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=5/1280, ttl=254
  7   0.016868   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=6/1536, ttl=254
  8   0.019210   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=7/1792, ttl=254
  9   0.024785   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=8/2048, ttl=254
 --More--
```

ステップ 4：次のように入力してキャプチャ ポイントを削除します。

```
スイッチ# no monitor capture mycap
```

（注） 制限が設定してあり、その制限に達するとキャプチャは自動的に停止するため、この特定のケースでは、**stop** コマンドは必要ありません。

pcap の統計情報に使用する構文の詳細については、「その他の参考資料」セクションを参照してください。

関連トピック

キャプチャ ポイントの定義, （857 ページ）

キャプチャ ポイント パラメータの追加または変更, （862 ページ）

キャプチャ ポイント パラメータの削除，（865 ページ）
キャプチャ ポイントの削除，（867 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（868 ページ）
キャプチャ ポイント バッファのクリア，（872 ページ）
Wireshark の設定方法，（857 ページ）
キャプチャ ポイント，（844 ページ）
接続ポイント，（845 ページ）

例：単純なキャプチャおよび保存

次の例は、フィルタにパケットをキャプチャする方法を示しています。

ステップ 1：次のように入力して、関連トラフィックで一致するキャプチャ ポイントを定義し、それをファイルに関連付けます。

```
スイッチ# monitor capture mycap interface GigabitEthernet1/0/3 in
スイッチ# monitor capture mycap match ipv4 any any
スイッチ# monitor capture mycap limit duration 60 packets 50
スイッチ# monitor capture mycap file location flash:mycap.pcap
```

ステップ 2：次のように入力してキャプチャ ポイントが正確に定義されていることを確認します。

```
スイッチ# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/3 in
   monitor capture mycap match ipv4  any any
   monitor capture mycap file location flash:mycap.pcap
   monitor capture mycap limit packets 50 duration 60

スイッチ# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
  Limit Details:
   Number of Packets to capture: 50
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：次のように入力してパケットを開始します。

```
スイッチ# monitor capture mycap start
```

ステップ 4: 次のように入力して実行中のエクステンドキャプチャ統計情報を表示します。

```
スイッチ#  show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 15 seconds
        Packets received - 40
        Packets dropped - 0
```

```
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 40
        Bytes received - 7280
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
        Bytes sent ¬ 4560
```

ステップ 5：十分な時間の経過後に、次のように入力してキャプチャを停止します。

```
スイッチ# monitor capture mycap stop
Capture statistics collected at software (Buffer & Wireshark):
        Capture duration - 20 seconds
        Packets received - 50
        Packets dropped - 0
        Packets oversized - 0
```

（注） あるいは、時間の経過またはパケット カウントが一致した後に、キャプチャ操作を自動的に停止させることもできます。

mycap.pcap ファイルには、キャプチャしたパケットが含まれます。

ステップ 6: 次のように入力して停止後のエクステンドキャプチャの統計情報を表示します。

```
スイッチ#  show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 20 seconds
        Packets received - 50
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 50
        Bytes received - 8190
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
        Bytes sent ¬ 5130
```

ステップ 7：次のように入力してパケットを表示します。

```
スイッチ# show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=0/0, ttl=254
  2 0.002555000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=1/256, ttl=254
  3 0.006199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=2/512, ttl=254
  4 0.009199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=3/768, ttl=254
  5 0.011647000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=4/1024, ttl=254
  6 0.014168000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=5/1280, ttl=254
  7 0.016737000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=6/1536, ttl=254
  8 0.019403000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=7/1792, ttl=254
  9 0.022151000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=8/2048, ttl=254
 10 0.024722000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=9/2304, ttl=254
```

```
 11 0.026890000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=10/2560, ttl=254
 12 0.028862000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=11/2816, ttl=254
 --More--
```

pcap の統計情報に使用されるシンタックスの詳細については、「そのほかの参考資料」セクションを参照してください。

ステップ 8：次のように入力して、キャプチャ ポイントを削除します。

```
スイッチ# no monitor capture mycap
```

関連トピック

- キャプチャ ポイントの定義，（857 ページ）
- キャプチャ ポイント パラメータの追加または変更，（862 ページ）
- キャプチャ ポイント パラメータの削除，（865 ページ）
- キャプチャ ポイントの削除，（867 ページ）
- キャプチャ ポイントをアクティブまたは非アクティブにする，（868 ページ）
- キャプチャ ポイント バッファのクリア，（872 ページ）
- Wireshark の設定方法，（857 ページ）
- キャプチャ ポイント，（844 ページ）
- 接続ポイント，（845 ページ）

例：バッファのキャプチャの使用

次に、バッファのキャプチャを使用する例を示します。

ステップ 1：次のように入力してバッファ キャプチャ オプションでキャプチャ セッションを起動します。

```
スイッチ# monitor capture mycap interface GigabitEthernet1/0/3 in
スイッチ# monitor capture mycap match ipv4 any any
スイッチ# monitor capture mycap buffer circular size 1
スイッチ# monitor capture mycap start
```

ステップ 2：次のように入力してキャプチャがアクティブであるかどうかを決定します。

```
スイッチ# show monitor capture mycap
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Active
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
  File Details:
   File not associated
  Limit Details:
```

```
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：次のように入力してランタイム時に拡張キャプチャの統計情報を表示します。

```
スイッチ# show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 88 seconds
        Packets received - 1000
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 1000
        Bytes received - 182000
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
        Bytes sent - 114000
```

ステップ 4：次のように入力してキャプチャを停止します。

```
スイッチ# monitor capture mycap stop
Capture statistics collected at software (Buffer):
        Capture duration - 2185 seconds
        Packets received - 51500
        Packets dropped - 0
        Packets oversized - 0
```

ステップ 5：次のように入力して停止後の拡張キャプチャの統計情報を表示します。

```
スイッチ# show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 156 seconds
        Packets received - 2000
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 2000
        Bytes received - 364000
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
        Bytes sent - 228000
```

ステップ 6：次のように入力してキャプチャがアクティブであるかどうかを決定します。

```
スイッチ# show monitor capture mycap
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
```

```
   Packet sampling rate: 0 (no sampling)
```

ステップ 7：次のように入力してバッファのパケットを表示します。

```
スイッチ# show monitor capture mycap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1   0.000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40057/31132, ttl=254
  2   0.000030   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40058/31388, ttl=254
  3   0.000052   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40059/31644, ttl=254
  4   0.000073   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40060/31900, ttl=254
  5   0.000094   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40061/32156, ttl=254
  6   0.000115   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40062/32412, ttl=254
  7   0.000137   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40063/32668, ttl=254
  8   0.000158   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40064/32924, ttl=254
  9   0.000179   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40065/33180, ttl=254
 10   0.000200   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40066/33436, ttl=254
 11   0.000221   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40067/33692, ttl=254
 12   0.000243   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40068/33948, ttl=254
 --More--
```

パケットがバッファに入ったことに注意してください。

ステップ 8：他の表示モードでパケットを表示します。

```
スイッチ# show monitor capture mycap buffer detailed
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  6, 2015 18:10:06.297972000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1446833406.297972000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 114 bytes (912 bits)
    Capture Length: 114 bytes (912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:icmp:data]
Ethernet II, Src: Cisco_f3:63:46 (00:e1:6d:f3:63:46), Dst: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)

    Destination: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        Address: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        Address: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not
ECN-Capable Transport))
```

```
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport)
(0x00)
    Total Length: 100
    Identification: 0xabdd (43997)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
    Header checksum: 0xe8a4 [validation disabled]
        [Good: False]
        [Bad: False]
    Source: 10.10.10.2 (10.10.10.2)
    Destination: 10.10.10.1 (10.10.10.1)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xa620 [correct]
    Identifier (BE): 56 (0x0038)
    Identifier (LE): 14336 (0x3800)
    Sequence number (BE): 40057 (0x9c79)
    Sequence number (LE): 31132 (0x799c)
    Data (72 bytes)

0000  00 00 00 00 0b 15 30 63 ab cd ab cd ab cd ab cd   ......0c........
0010  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0020  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0030  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0040  ab cd ab cd ab cd ab cd                           ........
       Data: 000000000b153063abcdabcdabcdabcdabcdabcdabcdabcd...
       [Length: 72]

Frame 2: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0


スイッチ# show monitor capture mycap buffer dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0000  00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00   ..m1....m.cF..E.
0010  00 64 ab dd 00 00 fe 01 e8 a4 0a 0a 0a 02 0a 0a   .d..............
0020  0a 01 08 00 a6 20 00 38 9c 79 00 00 00 00 0b 15   ..... .8.y......
0030  30 63 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   0c..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd                                            ..

0000  00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00   ..m1....m.cF..E.
0010  00 64 ab de 00 00 fe 01 e8 a3 0a 0a 0a 02 0a 0a   .d..............
0020  0a 01 08 00 a6 1d 00 38 9c 7a 00 00 00 00 0b 15   .......8.z......
0030  30 65 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   0e..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd
```

ステップ 9：次のように入力してバッファをクリアします。

```
スイッチ# monitor capture mycap clear
```

（注） 注：バッファをクリアすると、その内容とともにバッファが削除されます。

（注） バッファの内容を表示する必要がある場合は、show コマンドの後に clear コマンドを実行します。

ステップ 10：トラフィックを再開し、10 秒待ってから次のように入力してバッファ コンテンツを表示します。

（注） キャプチャがアクティブなときに、バッファから show の実行をすることはできません。バッファから show を実行する前に、キャプチャを停止する必要があります。しかし、ファイルおよびバッファ モードの両方においてキャプチャがアクティブなときに pcap ファイルで show の実行ができます。ファイル モードでは、キャプチャがアクティブなときに、現在のキャプチャ セッションの pcap ファイルでパケットを表示することもできます。

```
スイッチ# monitor capture mycap start
Switch#  show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Active
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
```

ステップ 11：次のように入力して、パケット キャプチャを停止し、バッファの内容を表示します。

```
スイッチ# monitor capture mycap stop
Capture statistics collected at software (Buffer):
 Capture duration - 111 seconds
 Packets received - 5000
 Packets dropped - 0
 Packets oversized - 0
```

ステップ 12：次のように入力してキャプチャがアクティブであるかどうかを決定します。

```
スイッチ# show monitor capture mycap
Status Information for Capture mycap
 Target Type:
  Interface: GigabitEthernet1/0/3, Direction: in
 Status : Inactive
Filter Details:
 IPv4
  Source IP: any
  Destination IP: any
 Protocol: any
```

```
Buffer Details:
 Buffer Type: CIRCULAR
 Buffer Size (in MB): 1
File Details:
 File not associated
Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Maximum number of packets to capture per second: 1000
 Packet sampling rate: 0 (no sampling)
```

ステップ 13：次のように入力してバッファのパケットを表示します。

```
スイッチ# show monitor capture mycap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=0/0, ttl=254
  2 0.000030000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=1/256, ttl=254
  3 0.000051000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=2/512, ttl=254
  4 0.000072000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=3/768, ttl=254
  5 0.000093000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=4/1024, ttl=254
  6 0.000114000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=5/1280, ttl=254
  7 0.000136000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=6/1536, ttl=254
  8 0.000157000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=7/1792, ttl=254
  9 0.000178000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=8/2048, ttl=254
 10 0.000199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=9/2304, ttl=254
 11 0.000220000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=10/2560, ttl=254
 12 0.000241000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=11/2816, ttl=254
 --More‹
```

ステップ 14：次のように入力して、内部 flash: storage デバイス内の mycap1.pcap ファイルにバッファ コンテンツを保存します。

```
スイッチ# monitor capture mycap export flash:mycap.pcap
Exported Successfully
```

（注） 現在のエクスポート実装では、コマンドを実行すると、エクスポートは「開始」されますが、ユーザにプロンプトを返す場合には完了しません。そこで、ファイルでパケットの表示を実行する前に、Wireshark からコンソールにメッセージが表示されるのを待機する必要があります。

ステップ 15：次のように入力してファイルからキャプチャ パケットを表示します。

```
スイッチ#  show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=0/0, ttl=254
  2 0.000030000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=1/256, ttl=254
  3 0.000051000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=2/512, ttl=254
  4 0.000072000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
```

```
seq=3/768, ttl=254
   5 0.000093000    10.10.10.2 -> 10.10.10.1    ICMP 114 Echo (ping) request  id=0x0039,
seq=4/1024, ttl=254
   6 0.000114000    10.10.10.2 -> 10.10.10.1    ICMP 114 Echo (ping) request  id=0x0039,
seq=5/1280, ttl=254
   7 0.000136000    10.10.10.2 -> 10.10.10.1    ICMP 114 Echo (ping) request  id=0x0039,
seq=6/1536, ttl=254
   8 0.000157000    10.10.10.2 -> 10.10.10.1    ICMP 114 Echo (ping) request  id=0x0039,
seq=7/1792, ttl=254
   9 0.000178000    10.10.10.2 -> 10.10.10.1    ICMP 114 Echo (ping) request  id=0x0039,
seq=8/2048, ttl=254
  10 0.000199000    10.10.10.2 -> 10.10.10.1    ICMP 114 Echo (ping) request  id=0x0039,
seq=9/2304, ttl=254
  11 0.000220000    10.10.10.2 -> 10.10.10.1    ICMP 114 Echo (ping) request  id=0x0039,
seq=10/2560, ttl=254
  12 0.000241000    10.10.10.2 -> 10.10.10.1    ICMP 114 Echo (ping) request  id=0x0039,
seq=11/2816, ttl=254
 --More--
```

ステップ 16：次のように入力して、キャプチャ ポイントを削除します。

```
スイッチ# no monitor capture mycap
```

関連トピック

- キャプチャ ポイントの定義，（857 ページ）
- キャプチャ ポイント パラメータの追加または変更，（862 ページ）
- キャプチャ ポイント パラメータの削除，（865 ページ）
- キャプチャ ポイントの削除，（867 ページ）
- キャプチャ ポイントをアクティブまたは非アクティブにする，（868 ページ）
- キャプチャ ポイント バッファのクリア，（872 ページ）
- Wireshark の設定方法，（857 ページ）
- キャプチャ ポイント，（844 ページ）
- 接続ポイント，（845 ページ）

例：出方向のパケットの簡単なキャプチャおよび保存

次の例は、フィルタにパケットをキャプチャする方法を示しています。

ステップ 1：次のように入力して、関連トラフィックで一致するキャプチャ ポイントを定義し、それをファイルに関連付けます。

```
スイッチ# monitor capture mycap interface Gigabit 1/0/1 out match ipv4 any any
スイッチ# monitor capture mycap limit duration 60 packets 100
スイッチ# monitor capture mycap file location flash:mycap.pcap buffer-size 90
```

ステップ 2：次のように入力してキャプチャ ポイントが正確に定義されていることを確認します。

```
スイッチ# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 out
   monitor capture mycap match ipv4  any any
   monitor capture mycap file location flash:mycap.pcap buffer-size 90
   monitor capture mycap limit packets 100 duration 60

スイッチ# show monitor capture mycap
```

```
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/1, Direction: out
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 90
  Limit Details:
   Number of Packets to capture: 100
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：次のように入力してパケットを開始します。

```
スイッチ# monitor capture mycap start
A file by the same capture file name already exists, overwrite?[confirm]
Turning on lock-step mode

スイッチ#
*Oct 14 09:35:32.661: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

（注） 時間の経過またはパケット カウントが一致した後に、キャプチャ操作を自動的に停止させてください。出力に次のメッセージが表示された場合は、キャプチャ処理が停止していることを意味します。

```
*Oct 14 09:36:34.632: %BUFCAP-6-DISABLE_ASYNC: Capture Point mycap disabled. Rea
son : Wireshark Session Ended
```

mycap.pcap ファイルには、キャプチャしたパケットが含まれます。

ステップ 4：次のように入力してパケットを表示します。

```
スイッチ# show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  0.000000    10.1.1.30 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000    10.1.1.31 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000    10.1.1.32 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000    10.1.1.33 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000    10.1.1.34 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000    10.1.1.35 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000    10.1.1.36 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000    10.1.1.37 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.38 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.39 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 5：次のように入力してキャプチャ ポイントを削除します。

```
スイッチ# no monitor capture mycap
```

関連トピック

キャプチャ ポイントの定義，（857 ページ）

キャプチャ ポイント パラメータの追加または変更，（862 ページ）

キャプチャ ポイント パラメータの削除，（865 ページ）

キャプチャ ポイントの削除，（867 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（868 ページ）
キャプチャ ポイント バッファのクリア，（872 ページ）
Wireshark の設定方法，（857 ページ）
キャプチャ ポイント，（844 ページ）
接続ポイント，（845 ページ）

組み込みパケット キャプチャの設定例

例：パケット データ キャプチャの管理

次の例では、パケット データ キャプチャを管理する方法を示します。

```
スイッチ> enable
スイッチ# monitor capture mycap start
スイッチ# monitor capture mycap access-list v4acl
スイッチ# monitor capture mycap limit duration 1000
スイッチ# monitor capture mycap interface GigabitEthernet 0/0/1 both
スイッチ# monitor capture mycap buffer circular size 10
スイッチ# monitor capture mycap start
スイッチ# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
スイッチ# monitor capture mycap stop
スイッチ# end
```

関連トピック

パケット データ キャプチャの管理，（874 ページ）
パケット データ キャプチャ，（856 ページ）

例：キャプチャされたデータのモニタリングおよびメンテナンス

次の例は、ASCII 形式でパケットをダンプする方法を示しています。

```
スイッチ# show monitor capture mycap buffer dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0
0000: 01005E00 00020000 0C07AC1D 080045C0 ..^...........E.
0010: 00300000 00000111 CFDC091D 0002E000 .0..............
0020: 000207C1 07C1001C 802A0000 10030AFA .........*......
0030: 1D006369 73636F00 0000091D 0001 ..example.......
1
0000: 01005E00 0002001B 2BF69280 080046C0 ..^.....+.....F.
0010: 00200000 00000102 44170000 0000E000 . ......D.......
0020: 00019404 00001700 E8FF0000 0000 ..............
2
0000: 01005E00 0002001B 2BF68680 080045C0 ..^.....+.....E.
0010: 00300000 00000111 CFDB091D 0003E000 .0..............
0020: 000207C1 07C1001C 88B50000 08030A6E ...............n
0030: 1D006369 73636F00 0000091D 0001 ..example.......
3
0000: 01005E00 000A001C 0F2EDC00 080045C0 ..^...........E.
0010: 003C0000 00000258 CE7F091D 0004E000 .<.....X........
0020: 000A0205 F3000000 00000000 00000000 ................
```

```
0030: 00000000 00D10001 000C0100 01000000 ................
0040: 000F0004 00080501 0300
```

次の例は、mycap という名前のキャプチャの設定に使用するコマンドのリストを表示する方法を示しています。

```
スイッチ# show monitor capture mycap parameter
monitor capture mycap interface GigabitEthernet 1/0/1 both
monitor capture mycap match any
monitor capture mycap buffer size 10
monitor capture mycap limit pps 1000
```

次の例は、キャプチャ ポイントをデバッグする方法を示しています。

```
スイッチ# debug epc capture-point
EPC capture point operations debugging is on

スイッチ# monitor capture mycap start
*Jun 4 14:17:15.463: EPC CP: Starting the capture cap1
*Jun 4 14:17:15.463: EPC CP: (brief=3, detailed=4, dump=5) = 0
*Jun 4 14:17:15.463: EPC CP: final check before activation
*Jun 4 14:17:15.463: EPC CP: setting up c3pl infra
*Jun 4 14:17:15.463: EPC CP: Setup c3pl acl-class-policy
*Jun 4 14:17:15.463: EPC CP: Creating a class
*Jun 4 14:17:15.464: EPC CP: Creating a class : Successful
*Jun 4 14:17:15.464: EPC CP: class-map Created
*Jun 4 14:17:15.464: EPC CP: creating policy-name epc_policy_cap1
*Jun 4 14:17:15.464: EPC CP: Creating Policy epc_policy_cap1 of type 49 and client type 21
*Jun 4 14:17:15.464: EPC CP: Storing a Policy
*Jun 4 14:17:15.464: EPC CP: calling ppm_store_policy with epc_policy
*Jun 4 14:17:15.464: EPC CP: Creating Policy : Successful
*Jun 4 14:17:15.464: EPC CP: policy-map created
*Jun 4 14:17:15.464: EPC CP: creating filter for ANY
*Jun 4 14:17:15.464: EPC CP: Adding acl to class : Successful
*Jun 4 14:17:15.464: EPC CP: Setup c3pl class to policy
*Jun 4 14:17:15.464: EPC CP: Attaching Class to Policy
*Jun 4 14:17:15.464: EPC CP: Attaching epc_class_cap1 to epc_policy_cap1
*Jun 4 14:17:15.464: EPC CP: Attaching Class to Policy : Successful
*Jun 4 14:17:15.464: EPC CP: setting up c3pl qos
*Jun 4 14:17:15.464: EPC CP: DBG> Set packet rate limit to 1000
*Jun 4 14:17:15.464: EPC CP: creating action for policy_map epc_policy_cap1 class_map
epc_class_cap1
*Jun 4 14:17:15.464: EPC CP: DBG> Set packet rate limit to 1000
*Jun 4 14:17:15.464: EPC CP: Activating Interface GigabitEthernet1/0/1 direction both
*Jun 4 14:17:15.464: EPC CP: Id attached 0
*Jun 4 14:17:15.464: EPC CP: inserting into active lists
*Jun 4 14:17:15.464: EPC CP: Id attached 0
*Jun 4 14:17:15.465: EPC CP: inserting into active lists
*Jun 4 14:17:15.465: EPC CP: Activating Vlan
*Jun 4 14:17:15.465: EPC CP: Deleting all temp interfaces
*Jun 4 14:17:15.465: %BUFCAP-6-ENABLE: Capture Point cap1 enabled.
*Jun 4 14:17:15.465: EPC CP: Active Capture 1

スイッチ# monitor capture mycap1 stop
*Jun 4 14:17:31.963: EPC CP: Stopping the capture cap1
*Jun 4 14:17:31.963: EPC CP: Warning: unable to unbind capture cap1
*Jun 4 14:17:31.963: EPC CP: Deactivating policy-map
*Jun 4 14:17:31.963: EPC CP: Policy epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Deactivating policy-map Successful
*Jun 4 14:17:31.964: EPC CP: removing povision feature
*Jun 4 14:17:31.964: EPC CP: Found action for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:17:31.964: EPC CP: cleanning up c3pl infra
*Jun 4 14:17:31.964: EPC CP: Removing Class epc_class_cap1 from Policy
*Jun 4 14:17:31.964: EPC CP: Removing Class from epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Successfully removed
*Jun 4 14:17:31.964: EPC CP: Removing acl mac from class
*Jun 4 14:17:31.964: EPC CP: Removing acl from class : Successful
*Jun 4 14:17:31.964: EPC CP: Removing all policies
*Jun 4 14:17:31.964: EPC CP: Removing Policy epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Removing Policy : Successful
*Jun 4 14:17:31.964: EPC CP: Removing class epc_class_cap1
*Jun 4 14:17:31.965: EPC CP: Removing class : Successful
```

```
*Jun 4 14:17:31.965: %BUFCAP-6-DISABLE: Capture Point cap1 disabled.
*Jun 4 14:17:31.965: EPC CP: Active Capture 0
```

次の例は、組み込みパケット キャプチャ（EPC）のプロビジョニングをデバッグする方法を示しています。

```
スイッチ# debug epc provision
EPC provisionioning debugging is on

スイッチ# monitor capture mycap start
*Jun 4 14:17:54.991: EPC PROV: No action found for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:17:54.991: EPC PROV:
*Jun 4 14:17:54.991: Attempting to install service policy epc_policy_cap1
*Jun 4 14:17:54.992: EPC PROV: Attached service policy to epc idb subblock
*Jun 4 14:17:54.992: EPC PROV: Successful. Create feature object
*Jun 4 14:17:54.992: EPC PROV:
*Jun 4 14:17:54.992: Attempting to install service policy epc_policy_cap1
*Jun 4 14:17:54.992: EPC PROV: Successful. Create feature object
*Jun 4 14:17:54.992: %BUFCAP-6-ENABLE: Capture Point cap1 enabled.

スイッチ# monitor capture mycap stop
*Jun 4 14:18:02.503: EPC PROV: Successful. Remove feature object
*Jun 4 14:18:02.504: EPC PROV: Successful. Remove feature object
*Jun 4 14:18:02.504: EPC PROV: Destroyed epc idb subblock
*Jun 4 14:18:02.504: EPC PROV: Found action for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:18:02.504: EPC PROV: Deleting EPC action
*Jun 4 14:18:02.504: EPC PROV: Successful. CLASS_REMOVE, policy-map epc_policy_cap1, class
 epc_class_cap1
*Jun 4 14:18:02.504: %BUFCAP-6-DISABLE: Capture Point cap1 disabled.
```

関連トピック

キャプチャされたデータのモニタリングとメンテナンス，（876 ページ）

パケット データ キャプチャ，（856 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
表示フィルタ	表示フィルタの構文については、以下を参照して下さい。 フィルタ リファレンスの表示
pcap ファイル統計情報	pcap ファイル統計情報の表示に使用する構文については、以下で「-z」オプションの詳細を参照してください。 『Tshark Command Reference』

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	-

MIB

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

シスコのテクニカル サポート

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

第 IX 部

QoS

- QoS の設定，899 ページ

第 49 章

QoS の設定

- 機能情報の確認，899 ページ
- QoS の前提条件，900 ページ
- QoS コンポーネント，900 ページ
- QoS の用語，901 ページ
- QoS の概要，901 ページ
- QoS ポリシーのガイドライン，942 ページ
- 有線ターゲットの QoS に関する制約事項，942 ページ
- ワイヤレス ターゲットの QoS に関する制約事項，945 ページ
- QoS の設定方法，949 ページ
- QoS のモニタリング，1004 ページ
- QoS の設定例，1008 ページ
- 次の作業，1025 ページ
- QoS に関する追加情報，1025 ページ
- QoS の機能履歴と情報，1026 ページ

機能情報の確認

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

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

QoS の前提条件

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 標準 QoS の概念。
- ワイヤレスの概念とネットワーク トポロジ。
- 従来の Cisco IOS QoS。
- モジュラ QoS CLI（MQC）
- QoS 実装について。
- 使用するアプリケーションのタイプおよびネットワークのトラフィック パターン
- トラフィックの特性およびネットワークのニーズ。たとえば、ネットワークのトラフィックがバーストであるかどうか。音声およびビデオ ストリーム用の帯域幅確保の必要性
- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

関連トピック

有線ターゲットの QoS に関する制約事項, （942 ページ）
ワイヤレス ターゲットの QoS に関する制約事項, （945 ページ）

QoS コンポーネント

QoS は、次の主要コンポーネントで構成されています。

- 分類：分類は、ACL、DiffServ コードポイント（DSCP）、サービス クラス（CoS）、およびその他の要因に基づいて、トラフィックの 1 つのタイプを区別するプロセスです。
- マーキングと変換：マーキングは、特定の情報をネットワークのダウンストリームデバイスに伝送するか、スイッチ内の 1 つのインターフェイスから別のインターフェイスに情報を伝送するためにトラフィック上で使用されます。トラフィックをマークすると、そのトラフィックの QoS 動作が適用されます。これは、**set** コマンドを直接使用するか、テーブル マップ経由で入力値を受け取って出力の値に直接変換することで実行します。
- シェーピングとポリシング：シェーピングはダウンストリームデバイスで輻輳が発生しないようにトラフィック レートを調整しながら、トラフィックの最大レートを強制するプロセスのことです。最も一般的な形式のシェーピングは、物理または論理インターフェイスから送信されるトラフィックを制限するために使用されます。ポリシングは、トラフィック クラス

に最大レートを強制するために使用されます。レートを超過した場合は、イベント発生直後に特定のアクションが実行されます。

- キューイング：キューイングは、トラフィックの輻輳を防止するために使用されます。トラフィックは、帯域割り当てに基づいて処理およびスケジューリングするために、特定のキューに送信されます。次に、トラフィックはポートを介してスケジュールまたは送信されます。
- 帯域幅：帯域幅の割り当てにより、QoS ポリシーが適用されるトラフィックで使用可能な容量が決まります。
- 信頼：信頼により、トラフィックがスイッチを通過できるようになります。明示なポリシー設定がない場合、エンド ポイントから、またはエンド ポイントへの DSCP 値、precedence 値、または CoS 値は保持されます。

QoS の用語

この QoS コンフィギュレーション ガイドでは、次の用語が同じ意味で使用されます。

- アップストリーム（スイッチに対する方向）は、入力と同じ意味です。
- ダウンストリーム（スイッチに対する方向）は、出力と同じ意味です。

（注） アップストリームは、ワイヤレスから有線への方向を指します。ダウンストリームは、有線からワイヤレスへの方向を指します。ワイヤレスからワイヤレスへの方向を指す用語はありません。

QoS の概要

QoS の概要

Quality of Service（QoS）を設定することで、他のトラフィック タイプの代わりに特定のトラフィック タイプを優先的に処理できます。QoS を設定しなかった場合、スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。スイッチは、信頼性、遅延限界、またはスループットが保証されていないパケットを送信します。

次に、QoS が提供する具体的な機能を示します。

- 低遅延
- 帯域幅保証
- バッファリング能力とドロップ分野
- トラフィック ポリシング
- フレームまたはパケット ヘッダーの属性変更のイネーブル化

- 関連サービス

関連トピック

有線ターゲットの QoS に関する制約事項, （942 ページ）
ワイヤレス ターゲットの QoS に関する制約事項, （945 ページ）

モジュラ QoS コマンドライン インターフェイス

スイッチでは、QoS 機能はモジュラ QoS コマンドライン インターフェイス（MQC）を使用してイネーブルにできます。MQC はコマンドライン インターフェイス（CLI）構造を採用しています。これを使用すると、トラフィック ポリシーを作成し、作成したポリシーをインターフェイスにアタッチできます。1 つのトラフィック ポリシーには、1 つのトラフィック クラスと 1 つ以上の QoS 機能が含まれます。トラフィック クラスがトラフィックを分類するために使用されるのに対して、トラフィック ポリシーの QoS 機能は分類されたトラフィックの処理方法を決定します。MQC の主な目的の 1 つは、プラットフォームに依存しないインターフェイスを提供することにより、シスコ プラットフォーム全体の QoS を設定することです。

ワイヤレス QoS の概要

ワイヤレス QoS は次のワイヤレス ターゲットで設定できます。

- アクセス ポイントを関連付けることができるすべての物理ポートを含むワイヤレス ポート。
- 無線
- SSID（無線単位、AP 単位、SSID 単位で適用可能）
- クライアント

IOS XE Release 3E 以降、入力 SSID のマーキングおよびポリシング アクションとクライアントのポリシーは、アクセス ポイントで適用されます。スイッチで設定する SSID とクライアント入力ポリシーは、アクセスポイントに移動されます。アクセスポイントは各パケットのポリシングおよびマーキング アクションを実行します。ただし、スイッチは QoS ポリシーを選択します。出力 SSID とクライアント ポリシーのマーキングおよびポリシングは、スイッチで適用されます。

次の表に、ワイヤレス ターゲットでポリシーがどのようにサポートされるかを示します。

表 *55*：ワイヤレス ターゲットのポリシーのサポート

ワイヤレス ターゲット	サポートされるワイヤレス ターゲットのポリシー	出力方向をサポートするポリシー	入力方向をサポートするポリシー
ワイヤレス ポート	はい	はい：ユーザ設定可能	いいえ
無線	はい	はい：ただし、ユーザ設定不可	いいえ

ワイヤレスターゲット	サポートされるワイヤレスターゲットのポリシー	出力方向をサポートするポリシー	入力方向をサポートするポリシー
SSID	はい	はい：ユーザ設定可能	はい：ユーザ設定可能
クライアント	はい	はい：ユーザ設定可能	はい：ユーザ設定可能

（注） ユーザが設定可能なその他のポリシーには、複数宛先のポリサーおよびVLANが含まれます。

ワイヤレス QoS は次の機能をサポートします。

- 出力方向のキューイング。
- ワイヤレス トラフィックのポリシング
- ワイヤレス トラフィックのマーキング。
- 出力方向のワイヤレス トラフィックのシェーピング。
- 出力方向の Approximate Fair Drop（AFD）。
- QoS のモビリティ サポート。
- Cisco Unified Wireless Controller で使用可能な貴金属の QoS ポリシーとの互換性。
- CLI/Traffic クラス（TCLAS）および CLI/スヌーピングの組み合わせ。
- AVC QoS クライアント ポリシーの設定によるアプリケーション制御（データ トラフィックのドロップやマーキングが可能）。
- 入力ポリシーのドロップ処理。
- クライアントの QoS 統計情報および入力方向の SSID ターゲット。
- ローカル プロファイリング ポリシーの QoS 属性。
- 階層型ポリシー

ワイヤレス用の QoS および IPv6

スイッチは IPv4 および IPv6 トラフィックの QoS をサポートし、クライアント ポリシーに IPv4 および IPv6 のフィルタを設定できます。

有線およびワイヤレス アクセスでサポートされる機能

次の表で、有線およびワイヤレス アクセスでサポートされる機能について説明します。

表 *56*：有線およびワイヤレス アクセスでサポートされる *QoS* 機能

機能	有線	ワイヤレス
ターゲット	• ギガビットイーサネット • 10 ギガビット イーサネット • VLAN	• ワイヤレス ポート（CAPWAP トンネル） • SSID • クライアント • 無線 • CAPWAP マルチキャスト トンネル
設定手順	**service-policy** コマンドを使用してインストールされる QoS ポリシー。	• アクセスポイントがスイッチに接続すると、スイッチはポートにポリシーをインストールします。ポートポリシーには、port_child_policy という子ポリシーがあります。 • ポリシーは、無線のレートに設定されたシェーパーを持つ無線にインストールされます。デフォルトの無線ポリシー（変更不可）が無線に付加されます。 • WMM クライアントがアソシエートし、アドミッション コントロールが無線でイネーブルにされた場合、デフォルトのクライアントポリシーが有効になります。 • ユーザは port_child_policy を変更して、さらにクラスを追加できます。 • ユーザは SSID レベルでユーザ定義のポリシーを付加できます。 • ユーザはクライアント レベルでユーザ定義のポリシーを付加できます。
ポート レベルで許可されたキューの数	ポートでは最大 8 つのキューがサポートされます。	サポートされているキューは 4 つだけです。

機能	有線	ワイヤレス
分類メカニズム	• DSCP • IP precedence • CoS • QoS-group • 次を含む ACL のメンバーシップ： ◦ IPv4 ACL ◦ IPv6 ACL ◦ MAC ACL	• ポート レベル ◦ 入力：ワイヤレス ポートの入力で QoS ポリシーがサポートされていません。 ◦ 出力：DSCP ベースの分類だけです。 • SSID レベル ◦ 入力： DSCP、UP ◦ 出力：DSCP、CoS、QoS グループ • クライアント レベル ◦ 入力：ACL、DSCP、 Up ◦ 出力：ACL、DSCP、COS

関連トピック

ポート ポリシーの形式, （907 ページ）

ワイヤレス ターゲットでサポートされる QoS 機能

次の表に、ワイヤレス ターゲットで使用可能なさまざまな機能について説明します。

表 *57*：ワイヤレス ターゲットで使用可能な *QoS* 機能

ターゲット	機能	トラフィック	ポリシーが適用される方向	注
ポート	• ポート シェーパー • プライオリティ キューイング • マルチキャストのポリシング	非リアルタイム（NRT）、リアルタイム（RT）	出力	
無線	• シェーピング	非リアルタイム	出力	無線ポリシーはユーザ設定可能ではありません。

ターゲット	機能	トラフィック	ポリシーが適用される方向	注
SSID	• ポリシング • テーブル マップ	非リアルタイム、リアルタイム	入力および出力	
	シェーピング		出力	
	BRR		出力	
	セット アクション • テーブル マップ • Dscp 設定 • Cos 設定		入力	SSID の入力ポリシーのクラス デフォルト クラスおよびユーザ定義クラスの両方でセットを使用できます。 SSID ポリシーのクラスデフォルトクラスのみでテーブルマップを定義できます。
	セット アクション • テーブル マップ • Dscp 設定 • wlan user-priority 設定		出力	
	ドロップ		入力	
クライアント	ポリシング	非リアルタイム、リアルタイム	入力および出力	クライアントポリシーでは、次のフィルタがサポートされます。 • ACL • DSCP • Cos（出力の場合のみ） • WLAN UP • protocol
	ドロップ		入力	
	セット アクション • Dscp 設定 • Cos 設定		入力	
	セット アクション • Dscp 設定 • wlan user-priority 設定		出力	

関連トピック

ポート ポリシー, （907 ページ）
ポート ポリシーの形式, （907 ページ）

無線ポリシー，（909 ページ）
WLAN での SSID またはクライアント ポリシーの適用（CLI），（966 ページ）
SSID ポリシー，（910 ページ）
クライアント ポリシーの設定（CLI）
クライアント ポリシー，（910 ページ）

ポート ポリシー

スイッチはポートベースのポリシーをサポートしています。ポートポリシーには、ポートシェーパーと子ポリシー（port_child_policy）が含まれます。

（注） ポートの子ポリシーは、スイッチの有線ポートには適用されず、ワイヤレス ポートにだけ適用されます。ワイヤレス ポートは、AP が join するポートとして定義されます。デフォルト ポートの子ポリシーは、起動時にスイッチのワイヤレス ポートに適用されます。ポートのシェーパー レートは 1G に制限されています

ポート シェーパーは、デバイスと AP との間に適用可能なトラフィック ポリシーを指定します。これは、アクセス ポイントでサポートされる無線レートの合計です。

子ポリシーは、ポート子ポリシーで定義されたパケットとキューとの間のマッピングを指定します。子ポリシーは、音声、ビデオ、class-default、および non-client-nrt クラスを含めるように設定できます。この音声とビデオは、DSCP 値（外部 CAPWAP ヘッダーの DSCP 値）に基づいています。class-default の定義は、音声およびビデオ DSCP 以外の値としてシステムに認識されます。

DSCP 値は、パケットがポートに到達するときに割り当てられます。パケットがポートに到着する前に、SSID ポリシーがパケットに適用されます。ポートの子ポリシーには、特定のポート トラフィックでのマルチキャストの割合が含まれます。デフォルトでは、ポートの子ポリシーは使用できるレートの最大 10 % を割り当てます。

関連トピック

ワイヤレス ターゲットの QoS に関する制約事項，（945 ページ）
ワイヤレス ターゲットでサポートされる QoS 機能，（905 ページ）
例：音声、ビデオ、およびマルチキャスト トラフィックで分類されたワイヤレス QoS ポリシー，（1013 ページ）

ポート ポリシーの形式

ここでは、スイッチのポートポリシーの動作について説明します。スイッチポートでは、有線またはワイヤレスの物理ポートは区別されません。ポリシーは、スイッチに関連付けられたデバイスの種類に応じて適用されます。たとえば、アクセスポイントがスイッチポートに接続されている場合、スイッチはアクセスポイントをワイヤレスデバイスとして検出し、親子ポリシー形式のデフォルトの階層型ポリシーを適用します。このポリシーは、階層型ポリシーです。親ポリシーは変更できませんが、子ポリシー（port-child ポリシー）は、QoS 設定に合わせて変更できます。スイッチは、デフォルトのクラス マップとポリシー マップで事前に設定されます。

デフォルトのクラス マップ：

```
Class Map match-any non-client-nrt-class
   Match non-client-nrt
```

上記のポート ポリシーは、すべてのネットワーク トラフィックを Q3 キューに向けて処理します。クラス マップは、**show class-map** コマンドを実行して表示します。

デフォルトのポリシー マップ：

```
Policy Map port_child_policy
    Class non-client-nrt-class
      bandwidth remaining ratio 10
```

（注） リストされているクラス マップとポリシー マップはシステム定義のポリシーであり、変更できません。

次に、ワイヤレス デバイスが関連付けられているポートで使用可能なシステム定義のポリシー マップを示します。親ポリシーと子ポリシー サービス（**port_child_policy**）で構成される形式です。ネットワークのニーズに応じてポリシーをカスタマイズするには、ポートの子ポリシーを設定する必要があります。

```
Policy-map policy_map_name
    Class class-default
         Shape average average_rate
         Service-policy port_child_policy
```

（注） 親ポリシーは自動生成され、変更できません。ネットワークの QoS 要件に合わせて *port_child_policy* ポリシーを設定する必要があります。

ネットワーク トラフィックのタイプによっては、ポートの子ポリシーを設定できます。たとえば、一般的なワイヤレス ネットワーク構成において、音声およびビデオ トラフィックに特定のプライオリティを割り当てることができます。次に例を示します。

```
Policy-map port_child_policy
     Class  voice-policy-name (match dscp ef)
          Priority level 1
          Police (multicast-policer-name-voice) Multicast Policer
    Class video-policy-name (match dscp af41)
         Priority level 2
         Police (multicast-policer-name-video) Multicast Policer
Class non-client-nrt-class traffic(match non-client-nrt)
        Bandwidth remaining ratio (brr-value-nrt-q2)
    Class class-default  (NRT Data)
        Bandwidth remaining ratio (brr-value-q3)
```

上記のポートの子ポリシー：

- *voice-policy-name*：音声パケット トラフィック用のルールを指定するクラス名を参照します。ここで DSCP 値は、値 46（キーワード **ef** で表される）にマッピングされます。音声トラフィックにはプライオリティ 1 が割り当てられます。
- *video-policy-name*：ビデオ パケット トラフィック用のルールを指定するクラス名を参照します。DSCP 値は、値 34（キーワード **af41** で表される）にマッピングされます。

- *multicast-policer-name-voice*：マルチキャスト音声トラフィックを設定する必要がある場合、音声クラス マップのポリシングを設定できます。
- *multicast-policer-name-video*：マルチキャスト ビデオ トラフィックを設定する必要がある場合、ビデオ クラス マップのポリシングを設定できます。

上記の設定例では、すべての音声およびビデオ トラフィックはQ0およびQ1キューにそれぞれ送信されます。これらのキューは完全プライオリティを維持します。Q0 および Q1 のパケットはこの順序で処理されます。帯域幅余剰比率 *brr-value-nrt-q2* および *brr-value-q3* はそれぞれ、クラス マップ、*class-default* および *non-client-nrt* で指定された Q2 と Q3 に送信されます。Q2 および Q3 のパケット処理は重み付けラウンドロビンアプローチに基づいています。たとえば*brr-value-nrtq2* の値が 90 で *brr-value-nrtq3* が 10 である場合、キュー 2 とキュー 3 のパケットは 9:1 の比率で処理されます。

関連トピック

ワイヤレス ターゲットの QoS に関する制約事項, （945 ページ）

ワイヤレス ターゲットでサポートされる QoS 機能, （905 ページ）

例：音声、ビデオ、およびマルチキャスト トラフィックで分類されたワイヤレス QoS ポリシー, （1013 ページ）

有線およびワイヤレス アクセスでサポートされる機能, （903 ページ）

ポリシー マップ, （920 ページ）

無線ポリシー

無線ポリシーはシステム定義であり、ユーザは設定できません。無線ワイヤレス ターゲットは、出力方向にだけ適用されます。

無線ポリシーは無線単位、アクセス ポイント単位で適用されます。無線のレート制限は、AP 無線レートの実際の制限です。この値は、アクセス ポイントでサポートされている無線の合計と同じです。

次の無線がサポートされます。

- 802.11 a/n
- 802.11 b/n
- 802.11 ac

関連トピック

ワイヤレス ターゲットの QoS に関する制約事項, （945 ページ）

ワイヤレス ターゲットでサポートされる QoS 機能, （905 ページ）

SSID ポリシー

入力および出力方向で SSID BSSID（基本サービス セット ID）の QoS ポリシーを作成できます。デフォルトでは、SSIDポリシーはありません。ワイヤレストラフィックが信頼できないため、すべてのトラフィックはベスト エフォートとして送信されます。SSID の名前に基づいて SSID ポリシーを設定できます。ポリシーは、BSSID 単位で適用できます。

SSID で作成できるポリシーのタイプには、テーブルマップ（table-map）、シェープ レート、RT1（Real Time 1）および RT2（Real Time 2）ポリサーを使用したマーキングが含まれます。トラフィックが入力の場合、通常は、SSID でマーキングおよびポリシング ポリシーを設定します。トラフィックがダウンストリームの場合は、マーキングおよびキューイングを設定できます。

ポートと SSID で設定されているポリシー間では、1 対 1 のマッピングが必要です。たとえば、ポートでクラス音声とクラス ビデオを設定すると、SSID に同様のポリシーを設定できます。

SSID のプライオリティは、帯域幅余剰比率を設定して指定できます。SSID ポリシーのキューイングは、ダウンストリーム方向で適用されます。

関連トピック

WLAN での SSID またはクライアント ポリシーの適用（CLI）, （966 ページ）

ワイヤレス ターゲットでサポートされる QoS 機能, （905 ページ）

例：SSID ポリシー

例：ダウンストリーム SSID ポリシーの設定, （1013 ページ）

クライアント ポリシー

クライアント ポリシーは、入力方向と出力方向に適用できます。スイッチのワイヤレス制御モジュールは、WMM クライアントでアドミッション制御がイネーブルの場合に、デフォルト クライアントポリシーを適用します。アドミッション制御がディセーブルの場合、デフォルトクライアントポリシーはありません。クライアントではポリシング ポリシーおよびマーキング ポリシーを設定できます。

（注） クライアント ポリシーには、IPv4 フィルタと IPv6 フィルタの両方を設定できます。

クライアント ポリシーは次のように設定できます。

- AAA の使用
- Cisco IOS MQC CLI の使用
  - **service policy client** コマンドは WLAN 設定で使用できます。
- デフォルト設定の使用
- ローカル ポリシーの使用（ネイティブ プロファイリング）

show wireless client mac address*mac_address***service-policy** コマンドを使用して、クライアント ポリシーのソース（ローカルプロファイリング ポリシー、AAA、CLI など）を表示します。クライアント ポリシーの優先順位は、AAA > ローカル ポリシー > WLAN サービス クライアント ポリシー CLI > デフォルト設定です。

（注） ユニファイド ワイヤレス コントローラ手順を設定し、MQC QoS コマンドを使用して AAA を設定した場合は、MQC QoS コマンドによって設定されたポリシーが優先されます。

（注） WLAN にクライアント ポリシーを適用する場合は、クライアント ポリシーを変更する前に WLAN をディセーブルにします。SSID ポリシーは、WLAN がイネーブルでも変更できます。

デフォルトのクライアント ポリシーは、アドミッション制御（ACM）対応の Wi-Fi マルチメディア（WMM）クライアント上でのみイネーブルにされます。

ポリシーの連結

すべてのパケットに最大 2 つのポリシーを適用できます。最初にクライアント ターゲット、次に SSID ターゲットです。クライアントのポリシング アクションは、クライアント ポリシーで指定されたマーキング アクションの前にパケットに適用されます。クライアントのポリシングおよびマーキング アクションがパケットに適用されると、SSID ポリシー アクションが更新されたパケットに適用されます。カスタム ポリシーが指定されていない場合は、システムの信頼設定がパケットに適用されます。出力の信頼は DSCP に基づいており、入力の信頼は WLAN ユーザ プライオリティに基づいています。

関連トピック

クライアント ポリシーの設定（CLI）
ワイヤレス ターゲットでサポートされる QoS 機能, （905 ページ）
例：クライアント ポリシー, （1015 ページ）

階層型 QoS

スイッチは階層型 QoS（HQoS）をサポートします。HQoS を使用すると、次の作業を実行できます。

- 階層型分類：トラフィック分類は、他のクラスに基づいています。
- 階層型ポリシング：階層型ポリシーの複数のレベルでポリシングを設定するプロセス。
- 階層型シェーピング：シェーピングは、階層の複数のレベルで設定できます。

（注） 階層型シェーピングは、ポート シェーパーでのみサポートされます。ポート シェーパーでは、親に対してクラス デフォルトの設定だけが可能で、クラス デフォルトのアクションはシェーピングだけです。

関連トピック

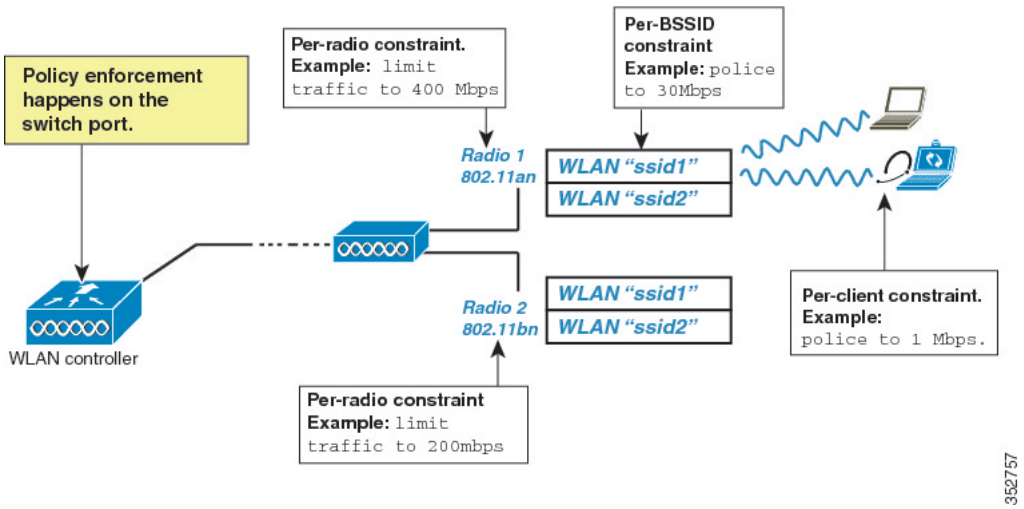
例：階層型分類，（1010 ページ）

例：階層型ポリシーの設定，（1010 ページ）

階層型ワイヤレス QoS

スイッチは、ワイヤレス ターゲットの階層型 QoS をサポートしています。階層型 QoS ポリシーは、ポート、無線、SSID、およびクライアントに適用されます。デバイスに設定された QoS ポリシー（マーキング、シェーピング、ポリシングを含む）は、複数のターゲットに適用できます。ネットワークに非リアルタイム トラフィックが含まれている場合、非リアルタイム トラフィックは Approximate Fair Drop に従います。階層は、デバイスに送信されるパケット上のさまざまな QoS ポリシーの適用プロセスに関係します。親と子ポリシーの両方に対してポリシングを設定できます。

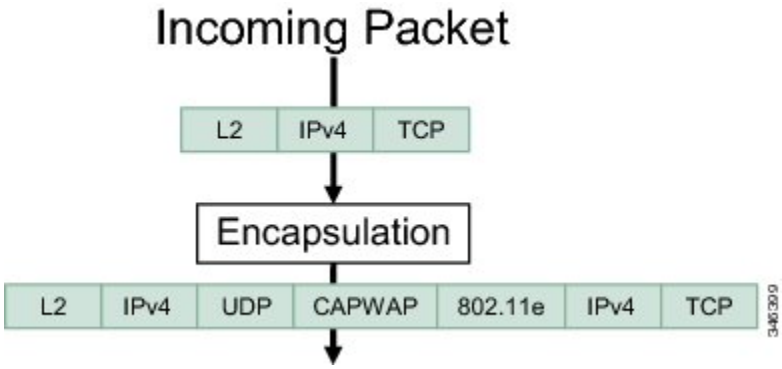
（注） 階層型クライアントおよび SSID ポリシーでは、親または子ポリシーのいずれかに対してのみポリシングを設定できます。



ワイヤレス パケット形式

この図は、階層型ワイヤレス QoS で使用されるワイヤレス パケット フローおよびカプセル化を示します。着信パケットは、スイッチに入ります。スイッチはこの着信パケットをカプセル化し、802.11e および CAPWAP ヘッダーを追加します。

図 *52*：最初のパスでの出力方向のワイヤレス パケット パス



階層型 *AFD*

Approximate Fair Dropping（AFD）は、Cisco IOS の QoS インフラストラクチャが提供する機能です。ワイヤレス ターゲットの場合、AFD は SSID（シェーピングによる）とクライアント（ポリシングによる）で設定できます。AFD のシェーピング レートはダウンストリーム方向のみに適用されます。ユニキャストのリアルタイム トラフィックは AFD ドロップの対象ではありません。

QoS の実装

ネットワークは通常、ベストエフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、正しいタイミングで配信される可能性も同じです。輻輳が発生すると、すべてのトラフィックが等しくドロップされます。

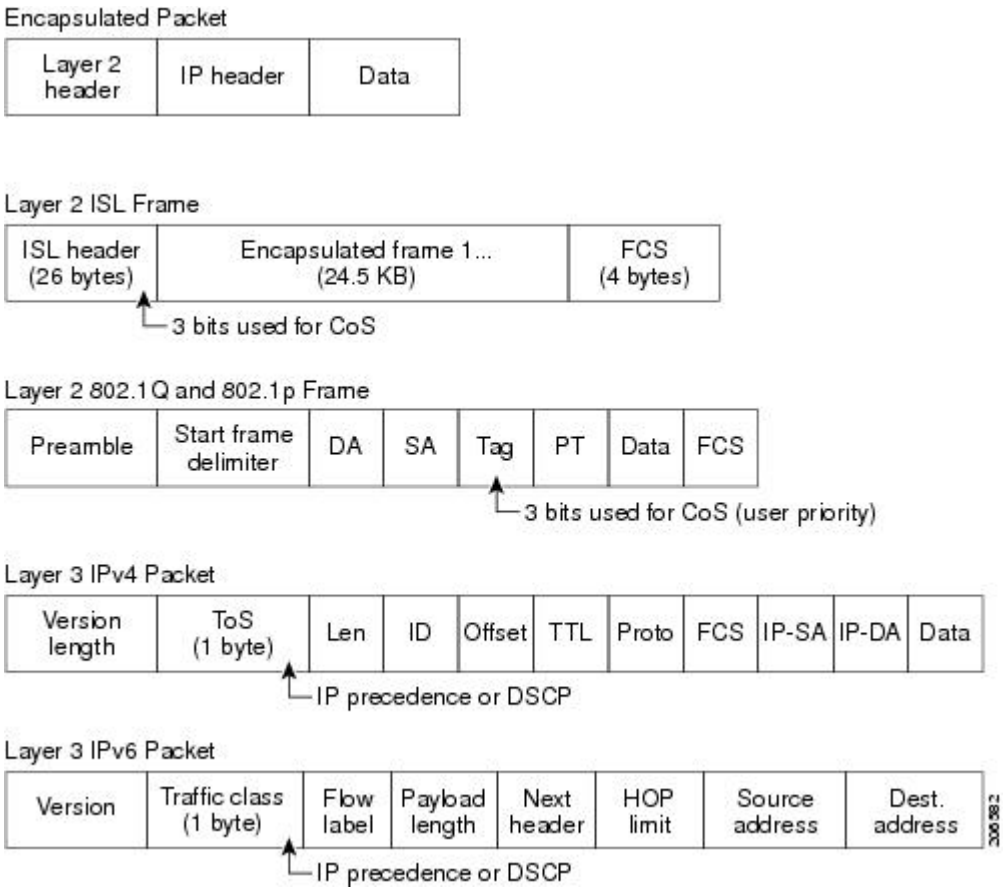
QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、相対的な重要性に応じてそのトラフィックに優先度を指定し、輻輳管理および輻輳回避技術を使用して、優先処理を実行できます。ネットワークに QoS を実装すると、ネットワーク パフォーマンスがさらに予測しやすくなり、帯域幅をより効率的に利用できるようになります。

QoS は、インターネット技術特別調査委員会（IETF）の規格である Differentiated Services（Diff-Serv）アーキテクチャに基づいて実装されます。このアーキテクチャでは、ネットワークに入るときに各パケットを分類することが規定されています。

この分類は IP パケット ヘッダーに格納され、推奨されない IP タイプ オブ サービス（ToS）フィールドの 6 ビットを使用して、分類（クラス）情報として伝達されます。分類情報をレイヤ 2 フレームでも伝達できます。

次の図にレイヤ 2 フレームまたはレイヤ 3 パケットの特殊ビットを示します。

図 *53*：フレームおよびパケットにおける *QoS* 分類レイヤ



関連トピック

有線ターゲットの QoS に関する制約事項, （942 ページ）

ワイヤレス ターゲットの QoS に関する制約事項, （945 ページ）

レイヤ 2 フレームのプライオリティ ビット

レイヤ 2 の ISL（スイッチ間リンク）フレーム ヘッダーには、下位 3 ビットで IEEE 802.1p サービス クラス（CoS）値を伝達する 1 バイトのユーザ フィールドがあります。レイヤ 2 ISL トランクとして設定されたポートでは、すべてのトラフィックが ISL フレームに収められます。

レイヤ 2 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット（ユーザ プライオリティ ビット）で CoS 値が伝達されます。レイヤ 2 802.1Q トランクとして設定されたポートでは、ネイティブ Virtual LAN（VLAN）のトラフィックを除くすべてのトラフィックが 802.1Q フレームに収められます。

他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。

レイヤ 2 CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

レイヤ 3 パケットのプライオリティ ビット

レイヤ 3 IP パケットは、IP precedence 値または Diffserv コード ポイント（DSCP）値のいずれかを伝送できます。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値も使用できます。

IP precedence 値の範囲は 0 ～ 7 です。DSCP 値の範囲は 0 ～ 63 です。

分類を使用したエンドツーエンドの QoS ソリューション

インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンド ホストが割り当てるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳細な検証は、コア スイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィック クラスに割り当てるリソースの量を制限できます。Diff-Serv アーキテクチャでトラフィックを処理するときの、各デバイスの動作をホップ単位動作といいます。パス上のすべてのデバイスに一貫性のあるホップ単位動作をさせることによって、エンドツーエンドの QoS ソリューションを構築できます。

ネットワーク上で QoS を実装する作業は、インターネットワーキング デバイスが提供する QoS 機能、ネットワークのトラフィック タイプおよびパターン、さらには着信および発信トラフィックに求める制御のきめ細かさによって、簡単にも複雑にもなります。

パケット分類

パケット分類は、特定の基準に基づいて定義したポリシーの複数のクラスの 1 つに属するものとしてパケットを識別するプロセスです。モジュラ QoS CLI（MQC）は、ポリシークラス ベースの言語です。ポリシー クラスの言語は、次の定義に使用されています。

- 1 つまたは複数の一致基準があるクラス マップ テンプレート
- 1 つまたは複数のクラスがポリシー マップに関連付けられているポリシーマップ テンプレート

ポリシーマップ テンプレートは、スイッチの 1 つまたは複数のインターフェイスに関連付けられます。

パケット分類は、ポリシー マップで定義されたクラスの 1 つに属するものとしてパケットを識別するプロセスです。分類プロセスは、処理されるパケットがクラス内の特定のフィルタに一致した場合に終了します。これは、最初の一致による終了と呼ばれます。つまり、ポリシー マップ内のクラスの順序に関係なく、パケットがポリシー内の複数のクラスに一致する場合、最初のクラスの一致後に分類プロセスが終了します。

パケットがポリシーのクラスと一致しない場合は、ポリシーのデフォルト クラスに分類されます。すべてのポリシーマップには、システム定義のクラスのデフォルトクラスがあり、どのユーザ定義クラスにも一致しないパケットに一致します。

パケット分類は次のタイプに分類できます。

- パケットと合わせて伝搬される情報に基づく分類
- スイッチ固有の情報に基づく分類
- 階層型分類

パケットと合わせて伝搬される情報に基づく分類

パケットの一部としてエンドツーエンドまたはホップ間で伝搬される情報に基づく分類には、一般的に次のものがあります。

- レイヤ 3 またはレイヤ 4 ヘッダーに基づく分類
- レイヤ 2 情報に基づく分類

レイヤ 3 またはレイヤ 4 ヘッダーに基づく分類

これは最も一般的な導入シナリオです。レイヤ3およびレイヤ4ヘッダーの多くのフィールドは、パケット分類に使用できます。

最もきめ細かいレベルでは、この分類方法はフロー全体を照合するために使用できます。この導入タイプで、アクセス コントロール リスト（ACL）を使用できます。ACL は、フローのさまざまなサブセット（送信元IPアドレスのみ、宛先IPアドレスのみ、または両方の組み合わせなど）に基づく照合に使用することもできます。

分類は、IP ヘッダーの precedence 値または DSCP 値に基づいて実行することもできます。IP precedence フィールドは、特定のパケットを処理する必要がある相対プライオリティを示すために使用されます。これは、IP ヘッダー内のタイプ オブ サービス（ToS）バイトの 3 ビットで構成されます。

次の表に、さまざまな IP precedence ビット値と名前を示します。

（注） IP precedence はワイヤレス QoS ではサポートされません。

表 *58*：*IP precedence* 値と名前

IP precedence 値	IP precedence ビット	IP precedence の名前
0	000	ルーチン
1	001	プライオリティ
2	010	即時
3	011	Flash
4	100	フラッシュ オーバーライド
5	101	Critical
6	110	インターネットワーク制御

IP precedence 値	IP precedence ビット	IP precedence の名前
7	111	ネットワーク制御

（注） ネットワークのルーティング制御トラフィックすべては、IP precedence 値 6 をデフォルトで使用します。また、IP precedence 値 7 は、ネットワーク制御トラフィック用に予約されています。したがって、IP precedence 値 6 および 7 はユーザ トラフィック用に推奨されません。

DSCP フィールドは、IP ヘッダーの 6 ビットで構成され、インターネット技術特別調査委員会（IETF）の DiffServ ワーキング グループにより標準化されています。DSCP ビットが含まれた元の ToS バイトは、DSCP バイトの名前を変更しました。DSCP フィールドは、IP precedence と同様に IP ヘッダーの一部です。DSCP フィールドは、IP precedence フィールドのスーパー セットです。したがって、DSCP フィールドは、IP precedence に関連して説明した内容と同様の方法で使用され、設定されます。

（注） DSCP フィールド定義は IP precedence 値と下位互換性があります。

レイヤ 2 ヘッダーに基づく分類

レイヤ 2 ヘッダー情報に基づく分類は、さまざまな方法で実行できます。最も一般的な方法は次のとおりです。

- MAC アドレスベースの分類（アクセス グループの場合のみ）：分類は送信元 MAC アドレス（入力方向のポリシー用）および宛先 MAC アドレス（出力方向のポリシー用）に基づいています。
- サービス クラス：分類は、IEEE 802.1p 標準に基づくレイヤ 2 ヘッダーの 3 ビットに基づいて行われます。これは通常、IP ヘッダーの ToS バイトにマッピングします。
- VLAN ID：分類は、パケットの VLAN ID に基づいて行われます。

（注） レイヤ2ヘッダー内のこれらフィールドの一部は、ポリシーを使用して設定することもできます。

デバイス固有の情報に基づく分類（*QoS* グループ）

スイッチは分類がパケット ヘッダーまたはペイロードの情報に基づいていない場合に使用できる分類メカニズムを提供します。

複数の入力インターフェイスから出力インターフェイスの特定のクラスに送信されるトラフィックを集約する必要が生じる場合があります。たとえば、複数のカスタマーエッジルータが、異なるインターフェイスの同じアクセス スイッチに接続される可能性があります。サービスプロバイダーは、特定のレートでコアに送信されるすべての集約音声トラフィックをポリシングする場合

があります。ただし、異なるカスタマーからの音声トラフィックには、異なる ToS 設定がなされている可能性があります。QoS グループベースの分類は、次のシナリオで役立つ機能です。

入力インターフェイスで設定されたポリシーは、QoS グループを特定の値に設定します。この値は出力インターフェイスでイネーブルになっているポリシーのパケットの分類に使用できます。

QoS グループは、スイッチ内部のパケット データ構造内のフィールドです。QoS グループは、スイッチの内部ラベルであり、パケット ヘッダーの一部ではないことに注意してください。

階層型分類

スイッチでは、他のクラスに基づく分類を実行できます。通常このアクションは、1 つのクラスマップに複数クラスの分類メカニズム（フィルタ）を組み合わせる場合に必要になります。

QoS 有線モデル

QoS を実装するには、スイッチで次のタスクを実行する必要があります。

- トラフィック分類：パケットまたはフローを相互に区別します。
- トラフィック マーキングおよびポリシング：パケットがスイッチを移動するときに、特定の QoS を示すラベルを割り当て、パケットが設定されたリソース使用率制限に準拠するようにします。
- キューイングおよびスケジューリング：リソース競合があるすべての状況で、異なる処理を行います。
- シェーピング：スイッチから送信されるトラフィックが、特定のトラフィック プロファイルに適合するようにします。

入力ポートのアクティビティ

次のアクティビティはスイッチの入力ポートで発生します。

- 分類：パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。たとえば、スイッチは、ある種類のトラフィックを別の種類のトラフィックと区別するためにパケット内の CoS または DSCP を QoS ラベルにマッピングします。生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを識別します。
- ポリシング：ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィック フローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。
- マーキング：マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットの QoS ラベルをマークダウンするか、またはパケットをドロップするか）を決定します。

（注） ワイヤレス入力ポートでのポリシー適用は、スイッチではサポートされていません。

出力ポートのアクティビティ

次のアクティビティは、スイッチの出力ポートで発生します。

- ポリシング：ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィック フローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。
- マーキング：マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットのQoS ラベルをマークダウンするか、またはパケットをドロップするか）を決定します。
- キューイング：キューイングでは、使用する出力キューを選択する前に、QoSパケット ラベルおよび対応する DSCP 値または CoS 値を評価します。複数の入力ポートが 1 つの出力ポートに同時にデータを送信すると輻輳が発生することがあるため、重み付けテール ドロップ（WTD）によってトラフィック クラスを区別し、QoS ラベルに基づいてパケットに別々のしきい値を適用します。しきい値を超過している場合、パケットはドロップされます。

分類

分類とは、パケットのフィールドを検証して、トラフィックの種類を区別するプロセスです。分類は、スイッチで QoS がイネーブルの場合のみイネーブルになります。デフォルトでは、QoS はスイッチでイネーブルにされています。

分類中に、スイッチは検索処理を実行し、パケットに QoS ラベルを割り当てます。QoS ラベルは、パケットに対して実行するすべての QoS アクション、およびパケットの送信元キューを識別します。

アクセス コントロール リスト

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用すると、同じ特性を備えたパケット グループ（クラス）を定義できます。また IPv6 ACL に基づいて IP トラフィックを分類することもできます。

QoS のコンテキストでは、アクセス コントロール エントリ（ACE）の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なります。

- 許可アクションとの一致が検出されると（最初の一致の原則）、指定のQoS 関連アクションが実行されます。
- 拒否アクションと一致した場合は、処理中の ACL がスキップされ、次の ACL が処理されます。
- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットではQoS 処理は実行されず、スイッチによってベストエフォート型サービスが実行されます。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの一致が見つかると、それ以降の検索処理は中止され、QoS 処理が開始されます。

（注） アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

ACL でトラフィック クラスを定義した後で、そのトラフィック クラスにポリシーを結合できます。ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。ポリシーには、特定の集約としてクラスを分類する（DSCP を割り当てるなど）コマンドまたはクラスのレート制限を実施するコマンドを含めることができます。このポリシーを特定のポートに結合すると、そのポートでポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類する場合は、**access-list** グローバル コンフィギュレーション コマンドを使用します。レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

クラス マップ

クラスマップは、特定のトラフィック フロー（またはクラス）に名前を付けて、他のすべてのトラフィックと区別するためのメカニズムです。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。この条件には、ACL で定義されたアクセス グループとの照合、または DSCP 値や IP precedence 値の特定のリストとの照合を含めることができます。複数のトラフィック タイプを分類する場合は、別のクラスマップを作成し、異なる名前を使用できます。パケットをクラスマップ条件と照合した後で、ポリシーマップを使用してさらに分類します。

クラス マップを作成するには、**class-map** グローバル コンフィギュレーション コマンドまたは **class** ポリシー マップ コンフィギュレーション コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用する必要があります。**class-map** コマンドを入力すると、スイッチによってクラス マップ コンフィギュレーション モードが開始されます。このモードで、**match** クラスマップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

class class-default ポリシー マップ コンフィギュレーション コマンドを使用して、デフォルト クラスを作成できます。デフォルト クラスはシステム定義であり、設定することはできません。分類されていないトラフィック（トラフィック クラスで指定された一致基準を満たさないトラフィック）は、デフォルト トラフィックとして処理されます。

関連トピック

トラフィック クラスの作成（CLI），（949 ページ）

例：アクセス コントロール リストによる分類，（1008 ページ）

ポリシー マップ

ポリシーマップでは、作用対象のトラフィック クラスを指定します。アクションには次が含まれます。

- トラフィック クラスに特定の DSCP 値または IP precedence 値を設定する
- トラフィック クラスに CoS 値を設定する
- QoS グループを設定する
- トラフィック クラスのワイヤレス LAN（WLAN）値を設定する
- トラフィックがアウト オブ プロファイルになった場合の、トラフィックの帯域幅制限やアクションを指定する

ポリシー マップを効率的に機能させるには、ポートにポリシー マップを結合する必要があります。

ポリシー マップを作成して名前を付けるには、**policy-map** グローバル コンフィギュレーション コマンドを使用します。このコマンドを入力すると、スイッチによってポリシーマップ コンフィギュレーション モードが開始されます。このモードでは、**class**、または **set** ポリシー マップ コンフィギュレーション コマンドおよびポリシー マップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行するアクションを指定します。

ポリシーマップは、ポリシーマップ クラス コンフィギュレーション コマンド **police** と **bandwidth** を使用して設定することもできます。これらのコマンドは、ポリサー、トラフィックの帯域幅制限、および制限を超過した場合のアクションを定義します。加えて、ポリシーマップは、、**priority** ポリシーマップ クラス コンフィギュレーション コマンド（クラスの優先順位をスケジューリングする）、またはキューイング ポリシーマップ クラス コンフィギュレーションコマンド（**queue-buffers** および **queue-limit**）を使用すると、より詳細に設定できます。

ポリシー マップを有効化するには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用してポートに接続します。

関連トピック

トラフィック ポリシーの作成（CLI），（952 ページ）

ポート ポリシーの形式，（907 ページ）

物理ポートのポリシー マップ

実行対象となるトラフィック クラスを指定する非階層型ポリシーマップを、物理ポート上に設定できます。アクションには、トラフィック クラスでの特定の DSCP または IP precedence 値の設定、一致する各トラフィック クラス（ポリサー）に対するトラフィックの帯域幅限度の指定、トラフィックがアウト オブ プロファイル（マーキング）の場合の処理などが含まれます。

ポリシー マップには、次の特性もあります。

- 1 つのポリシー マップに、それぞれ異なる一致条件とポリサーを指定した複数のクラス ステートメントを指定できます。
- ポリシー マップには、事前に定義されたデフォルトのトラフィック クラスを含めることができます。デフォルトのトラフィック クラスはマップの末尾に明示的に配置されます。

  class class-default ポリシーマップ コンフィギュレーション コマンドを使用してデフォルトのトラフィック クラスを設定すると、未分類トラフィック（トラフィック クラスで指定され

た一致基準に一致しないトラフィック）はデフォルトのトラフィック クラス（**class-default**）として処理されます。

- 1 つのポートから受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。

関連トピック

トラフィック ポリシーのインターフェイスへの付加（CLI），（964 ページ）

VLAN のポリシー マップ

スイッチは、VLAN の QoS 機能をサポートします。これにより、ユーザは、着信フレームの VLAN 情報を使用して VLAN レベルで QoS 処理（分類と QoS アクション）を実行できます。VLAN ベースの QoS では、サービス ポリシーが SVI インターフェイスに適用されます。VLAN ポリシー マップに属するすべての物理インターフェイスは、ポートベースのポリシー マップの代わりに VLAN ベースのポリシー マップが表示されるようにプログラムする必要があります。

ポリシー マップは VLAN SVI に適用されますが、ポリシング（レート制限）アクションはポート単位でしか実行できません。複数の物理ポートからのトラフィックの合計が認識されるようにポリサーを設定できません。各ポートは、そのポートに着信するトラフィックを制御する別のポリサーを必要とします。

関連トピック

ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング（CLI），（972 ページ）

例：ポリサーの VLAN 設定，（1021 ページ）

ワイヤレス *QoS* マルチキャスト

ポート レベルでマルチキャストのポリシング レートを設定できます。

関連トピック

例：音声、ビデオ、およびマルチキャスト トラフィックで分類されたワイヤレス QoS ポリシー，（1013 ページ）

ポリシング

パケットが分類され、DSCP ベース、CoS ベース、または QoS グループのラベルが割り当てられると、ポリシングおよびマーキング プロセスを開始できます。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。制限を超えるパケットは、「アウトオブプロファイル」または「不適合」になります。各ポリサーはパケットごとに、パケットが適合か不適合かを判別し、パケットに対するアクションを指定します。これらのアクションはマーカーによって実行されます。パケットを変更しないで通過させるアクション、パケットをドロップするアクション、またはパケットに割り当てられた DSCP または CoS 値を変更（マークダウン）してパケットの通過を許可するアクションなどがあります。

パケットの混乱を避けるため、通常、適合トラフィックも不適合トラフィックも同じキューを通過します。

（注） すべてのトラフィックは、ブリッジングされるかルーティングされるかに関係なく、ポリサーの影響を受けます（ポリサーが設定されている場合）。その結果、ブリッジングされたパケットは、ポリシングまたはマーキングが行われたときにドロップされたり、DSCP または CoS フィールドが変更されたりすることがあります。

物理ポートでのみポリシングを設定できます。

ポリシー マップおよびポリシング アクションを設定したら、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、入力ポートまたは SVI にポリシーを付加します。

関連トピック

ポリシングの設定（CLI），（989 ページ）

例：ポリシング アクションの設定，（1020 ページ）

トークンバケット アルゴリズム

ポリシングはトークンバケット アルゴリズムを使用します。各フレームがスイッチに着信すると、バケットにトークンが追加されます。バケットにはホールがあり、平均トラフィック レートとして指定されたレート（ビット/秒）で送信されます。バケットにトークンが追加されるたびに、スイッチはバケット内に十分なスペースがあるかを確認します。十分なスペースがなければ、パケットは不適合とマーキングされ、指定されたポリサー アクション（ドロップまたはマークダウン）が実行されます。

バケットが満たされる速度は、バケット深度（burst-byte）、トークンが削除されるレート（rate-bps）、および平均レートを上回るバースト期間によって決まります。バケットのサイズによってバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バースト期間が短い場合、バケットはオーバーフローせず、トラフィック フローに何のアクションも実行されません。ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシング アクションが実行されます。

バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの burst-byte オプションを使用します。トークンがバケットから削除される速度（平均速度）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの rate オプションを使用します。

関連トピック

ポリシングの設定（CLI），（989 ページ）

例：ポリシングの単位，（1021 ページ）

マーキング

マーキングは、特定の情報をネットワークのダウンストリーム デバイスに伝送するか、スイッチ内の 1 つのインターフェイスから別のインターフェイスに情報を伝送するために使用します。

マーキングは、パケット ヘッダーの特定のフィールド/ビットを設定するか、スイッチ内部のパケット構造内の特定のフィールドを設定するために使用できます。さらに、マーキング機能はフィールド間のマッピングの定義に使用できます。QoS では次のマーキング方法を使用できます。

- パケット ヘッダー
- デバイス（スイッチ）固有の情報
- テーブル マップ

パケット ヘッダーのマーキング

パケット ヘッダー フィールドのマーキングは 2 種類の一般的なカテゴリに分類できます。

- IPv4/v6 ヘッダー ビット マーキング
- レイヤ 2 ヘッダー ビット マーキング

IP レベルのマーキング機能は、precedence を設定したり、IP ヘッダー内の DSCP を特定の値に設定したりして、ダウンストリーム デバイス（スイッチまたはルータ）で特定のホップごとの動作を実行するために使用されます。また、異なる入力インターフェイスからのトラフィックを、出力インターフェイス内の単一のクラスに集約するためにも使用できます。この機能は現在、IPv4 および IPv6 ヘッダーでサポートされています。

レイヤ 2 ヘッダーのマーキングは、通常、ダウンストリーム デバイス（スイッチまたはルータ）のドロップ動作に影響を与えるために使用されます。これは、レイヤ 2 ヘッダーの一致と並行して動作します。ポリシー マップを使用して設定されるレイヤ 2 ヘッダーのビットはサービス クラスです。

スイッチ固有の情報のマーキング

この形式のマーキングには、パケットヘッダーの一部ではないパケットデータ構造内のフィールドのマーキングが含まれます。これにより、後でデータ パスでマーキングを使用できるようになります。これはスイッチ間で伝搬されません。QoS グループのマーキングはこのカテゴリに分類されます。この形式のマーキングは、入力インターフェイスで有効になっているポリシーだけでサポートされます。対応する照合機能を同じスイッチの出力インターフェイスでイネーブルにし、適切な QoS アクションを適用することができます。

テーブル マップのマーキング

テーブルマップマーキングは変換表を使用したフィールド間のマッピングおよび変換を可能にします。この変換表はテーブル マップと呼ばれます。

インターフェイスに接続されているテーブル マップに応じて、パケット内の CoS、DSCP、および UP 値（ワイヤレス パケットに固有の UP）が書き換えられます。スイッチにより、入力のテーブル マップ ポリシーと出力のテーブル マップ ポリシーを設定できます。

（注） スイッチのスタックは、合計 14 のテーブル マップをサポートします。各方向の有線ポート単位で 1 つのテーブル マップだけがサポートされます。

たとえば、テーブル マップは、レイヤ 2 CoS 設定をレイヤ 3 の precedence 値にマッピングするのに使用できます。この機能により、マッピングを実行する方法を示す 1 つのテーブルに複数の **set** コマンドを組み合わせて使用することができます。このテーブルは複数のポリシーで参照するか、または同じポリシー内で複数回参照することができます。

次の表に、現在サポートされているマッピング形式を示します。

表 *59*：*To-From* 関係を確立するために使用されるパケット マーキング タイプ

パケット マーキング タイプ「To」	パケット マーキング タイプ「From」
Precedence	CoS
Precedence	QoS グループ
DSCP	CoS
DSCP	QoS グループ
CoS	Precedence
CoS	DSCP
QoS グループ	Precedence
QoS グループ	DSCP

テーブル マップ ベースのポリシーでは、次の機能がサポートされています。

- 変換：1 つの DSCP 値セットから別の DSCP 値セットにマッピングするテーブル マップを利用できます。また、このテーブル マップは出力ポートに付加できます。
- 書き換え：入力パケットは設定されたテーブル マップに基づいて書き換えられます。
- マッピング：テーブル マップ ベースのポリシーは、set ポリシーの代わりに使用できます。

テーブル マップ マーキングには、次の手順が必要です。

1. テーブル マップの定義：**table-map** グローバル コンフィギュレーション コマンドを使用して値をマッピングします。テーブルが使用されるクラスまたはポリシーは認識されません。テーブル マップのデフォルトのコマンドは、「from」フィールドで一致がない場合に値が「to」フィールドにコピーされることを示すために使用されます。
2. ポリシー マップの定義：テーブル マップを使用するポリシー マップを定義します。

3 ポリシーをインターフェイスに関連付けます。

（注） 入力ポートのテーブル マップ ポリシーによって、そのポートの信頼設定が qos-marking の「from」タイプに変更されます。

関連トピック

テーブル マップの設定（CLI），（975 ページ）

例：テーブル マップのマーキング設定，（1023 ページ）

トラフィックの調整

ネットワークでQoSをサポートするには、サービスプロバイダーネットワークに入るトラフィックをネットワーク境界ルータでポリシングし、トラフィック レートがサービス範囲内に収まるようにする必要があります。ネットワーク コアのプロビジョニングで処理できるように設定されているトラフィックよりも多くのトラフィックがネットワーク境界のいくつかのルータから送信開始されると、トラフィック負荷の増加によってネットワーク輻輳が発生します。ネットワークのパフォーマンスが低下すると、すべてのネットワーク トラフィックでQoSを提供することが困難になります。

トラフィック ポリシング機能（ポリシング機能を使用）およびシェーピング機能（トラフィック シェーピング機能を使用）はトラフィック レートを管理しますが、トークンが不足した場合のトラフィックの処理方法が異なります。トークンの概念は、トークン バケット方式、トラフィック測定機能に基づいています。

（注） ネットワーク トラフィックでQoSテストを実行すると、シェーパー データとポリシング データで異なる結果が生じることがあります。シェーピングからのネットワーク トラフィック データの方が、より正確な結果が得られます。

この表は、ポリシングとシェーピングの機能を比較します。

表 *60*：ポリシングとシェーピングの機能の比較

ポリシング機能	シェーピング機能
適合するトラフィックをライン レートで送信し、バーストを許可します。	トラフィックが固定レートでスムーズに送信されます。
トークンが不足すると、アクションがただちに実行されます。	トークンが不足すると、パケットをバッファし、後でトークンが使用可能になった時点で送信します。シェーピングを使用するクラスにはキューが関連付けられており、このキューを使用してパケットがバッファされます。

ポリシング機能	シェーピング機能
ポリシングは、ビット/秒、パケット/秒、およびセル/秒など複数の単位で設定できます。	シェーピングの設定単位はビット/秒だけです。
ポリシングには、イベントに複数の可能なアクションが関連付けられています。このようなアクションの例としては、イベント、マーキング、ドロッピングなどがあります。	シェーピングはプロファイルを満たさないパケットをマークできません。
入出力両方のトラフィックで機能します。	出力トラフィックに対してのみ実装されます。
ウィンドウサイズを小さくしたためにパケットドロップが発生すると、伝送制御プロトコル（TCP）は、回線速度でラインを検出しますが、設定されたレートに適合します。	TCP は低速回線があることを検出し、再送信タイマーを適切に調整できます。これにより、再送信の範囲が狭くなり、TCP に負担をかけません。

ポリシング

QoS ポリシング機能は、トラフィック クラスに最大レートを強制するために使用されます。QoS ポリシング機能は、プライオリティ機能と合わせて、プライオリティ トラフィックを制限するためにも使用できます。レートを超過した場合は、イベント発生直後に特定のアクションが実行されます。レート（認定情報レート [CIR] および最大情報レート [PIR]）とバースト パラメータ（適合バースト サイズ [B_c] および拡張バースト サイズ [B_e]）は、すべてバイト/秒で設定されます。

QoS では次のポリシング形式またはポリサーがサポートされます。

- シングルレート 2 カラー ポリシング
- デュアルレート 3 カラー ポリシング

（注） シングルレート 3 カラー ポリシングはサポートされません。

シングルレート *2* カラー ポリシング

シングルレート 2 カラー ポリサーは、CIR と B_c だけを設定するモードです。

B_c は任意のパラメータであり、これが指定されていない場合、デフォルトで計算されます。このモードでは、着信パケットに十分なトークンがある場合、パケットは適合すると見なされます。パケットの到着時に、十分なトークンがB_cの範囲内で使用できない場合、パケットは設定レートを超えたと見なされます。

（注） トークン バケット アルゴリズムの詳細については、 トークンバケット アルゴリズム, （923 ページ） を参照してください。

関連トピック

ポリシングの設定（CLI）, （989 ページ）

例：シングルレート 2 カラー ポリシング設定, （1022 ページ）

デュアルレート *3* カラー ポリシング

デュアル レート ポリサーでのスイッチは、カラー ブラインド モードのみをサポートします。このモードでは、認定情報レート（CIR）および最大情報レート（PIR）を設定します。名前からわかるように、この場合、最大レート用に 1 つ、認定レート用に 1 つの、合わせて 2 つのトークン バケットがあります。

（注） トークン バケット アルゴリズムの詳細については、 トークンバケット アルゴリズム, （923 ページ） を参照してください。

カラー ブラインド モードでは、最大レートのバケットの着信パケットが最初にチェックされます。十分な数のトークンがない場合、パケットはレートに違反していると見なされます。十分な数のトークンがある場合、次に適合レートのバケットのトークンをチェックして、十分な数のトークンがあるかどうかを判別します。最大レートのバケットにあるトークンは、パケットのサイズによって減少します。十分な数のトークンがない場合、パケットが設定されているレートを超過していると見なされます。十分な数のトークンがある場合、パケットは適合すると見なされ、両方のバケットのトークンは、パケットのサイズによって減少します。

トークン補充レートは着信パケットによって異なります。あるパケットが時間 T1 に着信し、次のパケットが時間 T2 に着信したとします。T1 と T2 間の時間間隔は、トークン バケットに追加される必要があるトークンの数を決定します。これは次のように計算されます。

パケットの時間間隔（T2-T1）* CIR）/8 バイト

関連トピック

ポリシングの設定（CLI）, （989 ページ）

例：デュアルレート 3 カラー ポリシング設定, （1023 ページ）

シェーピング

シェーピングは、ダウンストリーム スイッチおよびルータで輻輳が発生しないようにトラフィック レートを調整しながら、トラフィックの最大レートを強制するプロセスのことです。最も一般的な形式のシェーピングは、物理または論理インターフェイスから送信されるトラフィックを制限するために使用されます。

シェーピングにはバッファが関連付けられており、十分なトークンがないパケットがすぐにドロップされずにバッファされます。シェーピングされるトラフィックのサブセットで使用可能なバッ

ファ数は制限され、さまざまな要因に基づいて計算されます。使用可能なバッファの数は、特定の QoS コマンドを使用して調整できます。パケットはドロップされずに、バッファが使用可能になった時点でバッファされます。

クラスベース トラフィック シェーピング

スイッチは、クラスベースのトラフィック シェーピングを使用します。このシェーピング機能は、インターフェイスに関連付けられたポリシーのクラスでイネーブルになります。シェーピングが設定されたクラスには、トークンがないパケットを保持する複数のバッファが割り当てられます。バッファされたパケットはFIFOを使用してクラスから送信されます。最も一般的な形式の使用では、クラスベースのシェーピングを使用して、全体として物理インターフェイスまたは論理インターフェイスの最大レートを強制します。クラスでは次のシェーピング形式がサポートされます。

- 平均レート シェーピング
- 階層型シェーピング

シェーピングは、トークン バケットを使用して実行されます。CIR、B_c、B_e の値は、パケットが送信されるレートと、トークンが補充されるレートを決定します。

（注） トークン バケット アルゴリズムの詳細については、トークンバケット アルゴリズム，（923 ページ）を参照してください。

平均レート シェーピング

平均レート シェーピングを設定するには、**shape average** ポリシーマップ クラス コマンドを使用します。

このコマンドは、特定のクラスの最大帯域幅を設定します。キューの帯域幅は、ポートでさらに使用できる帯域幅があってもこの値に制限されます。スイッチでは、割合またはターゲット ビット レート値でシェーピング平均を設定できます。

関連トピック

シェーピングの設定（CLI），（1001 ページ）

例：平均レート シェーピングの設定，（1018 ページ）

階層型シェーピング

シェーピングは、階層内の複数のレベルで設定することもできます。これは、シェーピングを設定した親ポリシーを作成して、追加のシェーピングを設定した子ポリシーを親ポリシーに付加することで実現できます。

次の 2 つの階層型シェーピングがサポートされています。

- ポート シェーパー
- ユーザ設定のシェーピング

ポートシェーパーでは、クラスデフォルトが使用され、親で実行できるアクションはシェーピングだけです。キューアクションはポートシェーパーがある子で実行されます。ユーザ設定のシェーピングを使用すると、子のキューイング アクションを設定することはできません。

関連トピック

シェーピングの設定（CLI），（1001 ページ）

キューイングおよびスケジューリング

スイッチは、トラフィックの輻輳を防止するためにキューイングおよびスケジューリングを使用します。スイッチは、次のキューイングおよびスケジューリング機能をサポートします。

- 帯域幅
- 重み付けテール ドロップ
- プライオリティ キュー
- キュー バッファ

帯域幅

スイッチは次の帯域幅設定をサポートしています。

- 帯域幅の割合
- 帯域幅余剰比率

関連トピック

帯域幅の設定（CLI），（987 ページ）

帯域幅の割合

特定のクラスに最小帯域幅を割り当てるには、**bandwidth percent** ポリシーマップ クラス コマンドを使用します。合計が 100 % を超えることはできず、合計が 100 % 未満である場合は、残りの帯域幅がすべての帯域幅キューで均等に分割されます。

（注） キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。

ポリシー マップで帯域幅タイプを混在させることはできません。たとえば、1 つのポリシー マップで帯域幅の割合と kbps の両方を使用して、帯域幅を設定することはできません。

帯域幅余剰比率

指定されたキューでの未使用帯域幅の共有率を作成するには、**bandwidth remaining ratio** ポリシーマップ クラス コマンドを使用します。未使用帯域幅は、これら指定されたキューにより、設定で

指定されている比率で使用されます。このコマンドは、**priority** コマンドがポリシー内の特定のキューでも使用される場合に使用します。

比率を割り当てる場合には、これらの比率に従って、キューに特定の重みが割り当てられます。

比率は 0 ～ 100 の範囲で指定できます。たとえば、1 つのクラスの帯域幅余剰比率を 2 に設定し、別のクラスで帯域幅余剰比率 4 のキューを設定できます。帯域幅余剰比率 4 は、帯域幅余剰比率 2 の 2 倍の回数スケジュールされます。

ポリシーの全帯域幅の比率の割り当ては 100 を超えることができます。たとえば、1 つのキューの帯域幅余剰比率を 50 に設定し、別のキューに帯域幅余剰比率 100 を設定できます。

重み付けテール ドロップ

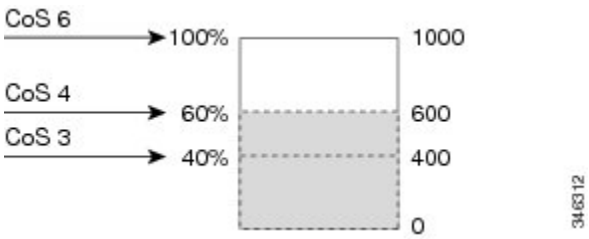
スイッチの出力キューは、重み付けテール ドロップ（WTD）と呼ばれるテール ドロップ輻輳回避メカニズムの拡張バージョンを使用します。WTD はキュー長を管理したり、トラフィック分類ごとにドロップ優先順位を設定したりするために実装されています。

フレームが特定のキューにキューイングされると、WTD はフレームに割り当てられた QoS ラベルを使用して、それぞれ異なるしきい値を適用します。この QoS ラベルのしきい値を超えると（宛先キューの空きスペースがフレーム サイズより小さくなると）、スイッチがフレームをドロップします。

各キューには 3 種類の設定可能なしきい値があります。QoS ラベルは、3 つのしきい値のうちのどれがフレームの影響を受けるかを決定します。

次の図は、サイズが 1000 フレームであるキューでの WTD の動作の例を示しています。ドロップ割合は次のように設定されています。40%（400 フレーム）、60%（600 フレーム）、および 100%（1000 フレーム）です。これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレームをキューイングできるという意味です。

図 *54*：*WTD* およびキューの動作



例では、CoS 値 6 は他の CoS 値よりも重要度が高く、100 %のドロップしきい値（キューフル ステート）に割り当てられます。CoS 値 4 は 60 % しきい値に、CoS 値 3 は 40 % しきい値に割り当てられます。これらのしきい値の割り当てはすべて、**queue-limit cos** コマンドを使用します。

600 のフレームが格納されているキューに、新しいフレームが着信したとします。これは CoS 値 4 を使用し、60 % のしきい値が適用されます。このフレームがキューに追加されると、しきい値を超過するため、スイッチがフレームをドロップします。

関連トピック

キュー制限の設定（CLI），（998 ページ）

例：キュー制限の設定，（1019 ページ）

重み付けテール ドロップのデフォルト値

次に、重み付けテール ドロップ（WTD）のデフォルト値と、WTD しきい値を設定するためのルールを示します。

- WTD に対して 2 つ以下のキュー制限割合を設定する場合、WTD のデフォルト値はこれらのしきい値に割り当てられます。

  次に、WTD しきい値のデフォルト値を示します。

  表 *61*：*WTD* しきい値のデフォルト値

しきい値	デフォルト値の割合
0	80
1	90
2	400

- 異なる 3 つの WTD しきい値が設定されている場合、キューは設定どおりにプログラムされます。
- 2 つの WTD しきい値が設定されている場合、最大値の割合は 400 です。
- 1 つの WTD しきい値が x として設定されている場合、最大値の割合は 400 です。
  - x の値が 90 未満の場合、threshold1 = 90 および threshold 0= x です。
  - x の値が 90 の場合、threshold1 = 90、threshold 0 = 80 です。
  - x の値が 90 より大きい場合、threshold1 = x、threshold 0 = 80 です。

プライオリティ キュー

各ポートは 8 つの出力キューをサポートし、そのうち 2 つにプライオリティを設定できます。

2 つのクラスのプライオリティを設定するには、**priority level** ポリシー クラスマップ コマンドを使用します。1 つのクラスにプライオリティ キュー レベル 1 を設定し、別のクラスにプライオリティ キュー レベル 2 を設定する必要があります。これら 2 つのキューのパケットは、他のキューと比較して、低遅延になります。

（注） プライオリティは 1 つのレベルのみ設定できます。
1 つのポリシーマップで使用できる完全プライオリティまたはレベル付きプライオリティは 1 つだけです。kbps または割合のない同じプライオリティ レベルが設定された複数のプライオリティは、ポリシングですべてが設定された場合にのみ使用できます。

関連トピック

プライオリティの設定（CLI），（992 ページ）

キュー バッファ

スイッチの各 1 ギガビット ポートには、ワイヤレス ポート用の 168 バッファと有線ポート用の 300 バッファが割り当てられます。各 10 ギガビット ポートには、1800 バッファが割り当てられます。ブート時に有線ポートでイネーブルになっているポリシー マップがない場合、デフォルトで作成される 2 つのキューがあります。有線ポートには、MQC ベースのポリシーを使用して最大 8 つのキューを設定できます。次の表に、どのパケットがどのキューに入っているかを示します。

表 *62*：*DSCP*、*Precedence*、*CoS*：キューのしきい値のマッピング テーブル

DSCP、Precedence、CoS	キュー	しきい値
制御パケット	0	2
他のパケット	1	2

（注） バッファのアベイラビリティを保証し、ドロップしきい値を設定し、キューの最大メモリ割り当てを設定できます。キュー バッファを設定するには、**queue-buffers** ポリシーマップ クラス コマンドを使用します。最大しきい値を設定するには、**queue-limit** ポリシーマップ クラス コマンドを使用します。

バッファ割り当ては2種類あります。キューに明示的に予約される厳格なバッファと、特定のポートで未使用時に他のポートで利用可能な柔軟なバッファです。

ワイヤレス ポートのデフォルトでは、キュー 0 には、厳格なバッファとしてインターフェイスで利用可能なバッファの 40% が割り当てられます。つまり、1 ギガビット ポートにおいては、キュー 0 に対して 67 バッファが割り当てられます。このキューの柔軟な最大値は 1 ギガビット ポートに 268（67 * 400/100 で計算）と設定されます。ここで、400 はキューに設定されたデフォルトの最大しきい値です。

有線ポートのデフォルトでは、キュー 0 には、厳格なバッファとしてインターフェイスで利用可能なバッファの 40 % が割り当てられます。つまり、1 ギガビット ポートにおいては、キュー 0 に対して 120 バッファが割り当てられ、10 ギガビット ポートにおいては、720 バッファが割り当てられます。このキューの柔軟な最大値は 1 ギガビット ポートで 480（120 * 400/100 で計算）と設

定され、10 ギガビット ポートで 2880 と設定されます。ここで、400 はキューに設定された最大しきい値です。

キュー 1 に割り当てられた厳格なバッファはありません。デフォルトの柔軟なバッファ制限は 400（最大しきい値）に設定されます。しきい値によって、共通プールから借用できる柔軟なバッファの最大数が決まります。

キュー バッファの割り当て

キューに対するバッファ割り当ては、**queue-buffers ratio** ポリシーマップ クラス コンフィギュレーション コマンドを使用して調整できます。

関連トピック

キュー バッファの設定（CLI）, （995 ページ）

例：キュー バッファの設定, （1020 ページ）

ダイナミックなしきい値および拡張

従来、予約バッファは各キューに静的に割り当てられていました。キューがアクティブかどうかにかかわらず、バッファはキューに保持されます。さらに、キューの数が増えるに従って、各キューに割り当てられた予約バッファの部分が徐々に短くなることがあります。最終的に、すべてのキューのジャンボ フレームをサポートするのに十分な予約バッファがなくなる可能性があります。

スイッチは、バッファ リソースを公平かつ効率的に割り当てる機能として、ダイナミックなしきい値および拡張（DTS）をサポートしています。輻輳が発生すると、この DTS 機能はグローバル/ポート リソースの占有に基づいて、着信データにバッファを柔軟に割り当てます。概念上、DTS は、リソースを他のキューが使用できるように、キュー バッファの割り当てを徐々に縮小します。逆も同様です。この柔軟な方法によって、バッファをより効率的かつ公平に利用できるようになります。

前の項で説明したように、キューには厳格な制限と柔軟な制限の 2 つの制限が設定されています。

厳格な制限は DTS の一部ではありません。これらのバッファはそのキューにだけ使用できます。厳格な制限の合計は、グローバルに設定された厳格な最大制限未満である必要があります。出力キューイング用に設定されたグローバルな厳格な制限は、現在 5705 に設定されています。MQC ポリシーが設定されていないデフォルトのシナリオでは、24 の 1 ギガビット ポートが 24 * 67 = 1608 を使用し、4 つの 10 ギガビット ポートが 4 * 720 = 2880 を使用し、合計 4488 のバッファを使用して、設定に基づいてより厳格なバッファを割り当てることができます。

柔軟なバッファ制限は DTS プロセスに参加します。さらに、柔軟なバッファ割り当ての一部は、グローバルな柔軟な制限の割り当てを超えることができます。出力キューイング用のグローバルな柔軟な制限は、現在 7607 に設定されています。厳格な制限と柔軟な制限の合計は 13312 になり、3.4 MB に変換されます。柔軟なバッファ割り当ての合計がグローバルな制限を超える場合があるため、システムの負荷が軽ければ、特定のキューで多数のバッファを使用できるようになります。DTS プロセスはシステムの負荷が増大するにしたがって、キュー単位の割り当てを動的に調整します。

ワイヤレスでのキューイング

ワイヤレスコンポーネントでのキューイングはポートポリシーに基づいて実行され、ダウンストリーム方向にだけ適用されます。ワイヤレス モジュールは次の 4 種類のキューをサポートします。

- 音声：これは完全プライオリティ キューです。Q0 に代表されるこのキューは、制御トラフィックとマルチキャストまたはユニキャスト音声トラフィックを処理します。すべての制御トラフィック（CAPWAP パケットなど）は、音声キューを介して処理されます。QoS モジュールは、制御パケットおよび音声パケットを処理して、制御パケットが他の非制御パケットよりもプライオリティが高くなるように、音声キュー内の別のしきい値を使用します。
- ビデオ：これは完全プライオリティ キューです。Q1 に代表されるこのキューは、マルチキャストまたはユニキャスト ビデオ トラフィックを処理します。
- データ NRT：Q2 に代表されるこのキューは、すべての非リアルタイム ユニキャスト トラフィックを処理します。
- マルチキャスト NRT：Q3 に代表されるこのキューは、マルチキャスト NRT トラフィックを処理します。Q0、Q1、または Q2 のトラフィックに一致しないトラフィックは、Q3 を通じて処理されます。

（注） デフォルトでは、キュー Q0 および Q1 はイネーブルになっていません。

（注） キュー Q2 および Q3 のトラフィックには、重み付けラウンド ロビン ポリシーが適用されます。

アップストリーム方向では、キューは 1 つだけ使用できます。ポートおよび無線ポリシーは、ダウンストリーム方向にだけ適用できます。

（注） 有線ポートでは 8 つのキューがサポートされます。

信頼動作

有線およびワイヤレス ポートの信頼動作

スイッチ（IP 電話、ラップトップ、カメラ、テレプレゼンス ユニットといったデバイスなどのエンドポイント）に接続された有線またはワイヤレス ポートでは、それらのエンドポイントからの DSCP 値、precedence 値、または CoS 値がスイッチによって信頼されるので、明示的なポリシー設定がない場合でも保持されます。

この信頼動作は、アップストリーム QoS とダウンストリーム QoS の両方に適用できます。

パケットはデフォルトの初期設定ごとに適切なキューに入れられます。デフォルトでは、スイッチでの優先キューイングは実行されません。これは、ユニキャストおよびマルチキャスト パケットに当てはまります。

次の表に、着信パケット タイプが発信パケット タイプと異なる場合の信頼動作およびキューイング動作を示します。ポートのデフォルトの信頼モードが DSCP ベースであることに注意してください。信頼モードは、着信パケットが純粋なレイヤ2パケットの場合、CoSに「フォールバック」します。また、信頼設定を DSCP から CoS に変更できます。この設定変更は、「set cos cos table default default-cos」アクションのクラス デフォルトがある MQC ポリシーによって実現されます。ここで、default-cos は作成されるテーブル マップ名です（デフォルト コピーだけを実行）。

表 *63*：信頼およびキューイング動作

着信パケット	発信パケット	信頼動作	キューイング動作
レイヤ 3	レイヤ 3	DSCP/Precedence の保持	DSCP に基づく
レイヤ 2	レイヤ 2	N/A	CoS に基づく
タグ付き	タグ付き	DSCP および CoS の保持	DSCP に基づく（信頼 DSCP が優先）
レイヤ 3	タグ付き	DSCP の保持、すなわち CoS が 0 に設定される	DSCP に基づく

Cisco IOS XE 3.2 リリースは、有線およびワイヤレス ポートに対して信頼できるさまざまなデフォルト設定をサポートしました。有線ポートの信頼できるデフォルト設定に関して、このソフトウェア リリースでの変更はありません。ワイヤレス ポートの場合、デフォルトのシステム動作は非信頼でした。つまり、スイッチの起動時に、ワイヤレス ポートのマーキングすべてがデフォルトでゼロに設定され、トラフィックはプライオリティ処理されませんでした。既存の有線スイッチとの互換性のために、すべてのトラフィックはデフォルトでベスト エフォートのキューへ送信されていました。アクセス ポイントは、プライオリティ キューイングをデフォルトで実行していました。ダウンストリーム方向では、アクセス ポイントは、キューイング用に音声、ビデオ、ベスト エフォート、およびバックグラウンドのキューを保持していました。アクセスは 11e タグ情報に基づいてキューイング戦略を選択していました。デフォルトでは、アクセス ポイントはすべてのワイヤレス パケットをベスト エフォートとして処理していました。

ワイヤレス ポートの場合、デフォルトの信頼動作は **qos wireless default untrust** コマンドを使用して変更できました。

（注） Cisco IOS XE 3.2 SE リリースからそれ以降のリリースにアップグレードしても、ワイヤレス トラフィックのデフォルトの動作は非信頼のままです。この状況でワイヤレス トラフィックの信頼動作を有効化するには、**no qos wireless-default untrust** コマンドを使用します。ただし、スイッチで Cisco IOS XE 3.3 SE 以降のリリースをインストールすると、ワイヤレス トラフィックのデフォルトの QoS 動作は信頼になります。Cisco IOS XE 3.3 SE リリース以降の新規インストール（アップグレードは不可）では、ワイヤレス トラフィックの出力および入力方向の両方でパケット マーキングが保持されます。

関連トピック

ワイヤレス トラフィックの信頼動作の設定（CLI），（978 ページ）

例：CoS マーキングを保持するテーブル マップの設定，（1024 ページ）

Cisco IP Phone の信頼境界機能のポート セキュリティ

一般的なネットワークでは、スイッチ ポートに Cisco IP Phone を接続し、電話の背後からデータ パケットを生成するデバイスをカスケードします。Cisco IP Phone では、音声パケット CoS レベルをハイ プライオリティ（CoS=5）にマーキングし、データ パケットをロープライオリティ（CoS=0）にマーキングすることで、共有データ リンクを通して音声品質を保証しています。電話からスイッチに送信されたトラフィックは通常 802.1Q ヘッダーを使用するタグでマーキングされています。ヘッダーには VLAN 情報およびパケットのプライオリティになる CoS の 3 ビット フィールドが含まれています。

ほとんどの Cisco IP Phone 設定では、電話からスイッチに送信されるトラフィックは、音声トラフィックがネットワーク内の他のタイプのトラフィックに対して適切にプライオリティ付けがされていることを保証するように信頼されています。 **trust device** インターフェイス コンフィギュレーション コマンドを使用して、電話が接続されているスイッチ ポートを設定し、ポートで受信されたトラフィックを信頼するようにします。

（注） **trust device** *device_type* インターフェイス コンフィギュレーション コマンドは、スイッチのスタンドアロン コマンドとしてではなく、自動 QoS 設定でのみサポートされます。**trust device** *device_type* インターフェイス コンフィギュレーション コマンドを自動 QoS 設定で使用するときに、接続されているピア デバイスが対応デバイス（信頼ポリシーに一致するデバイスとして定義されているデバイス）ではない場合、CoS 値と DSCP 値の両方が「0」に設定され、いずれの入力ポリシーも有効になりません。

信頼設定により、ユーザが電話をバイパスして PC を直接スイッチに接続する場合に、ハイプライオリティ キューの誤使用を避けるのにも信頼境界機能を使用できます。信頼境界機能を使用しないと、（信頼済みの CoS 設定により）PC が生成した CoS ラベルがスイッチで信頼されてしまいます。それに対して、信頼境界機能は CDP を使用してスイッチ ポートにある Cisco IP Phone（Cisco IP Phone 7910、7935、7940、7960 など）の存在を検出します。電話が検出されない場合、信頼境界機能がハイプライオリティ キューの誤使用を避けるためにスイッチ ポートの信頼設定を

ディセーブルにします。信頼境界機能は、PC および Cisco IP Phone がスイッチに接続されているハブに接続されている場合は機能しないことに注意してください。

関連トピック

デバイス タイプの信頼動作の設定

ワイヤレス QoS モビリティ

ワイヤレス QoS モビリティによって、ネットワーク内のどの場所でも同じサービスが提供されるように QoS ポリシーを設定することができます。ワイヤレス クライアントは 1 つの場所から別の場所にローミングできるため、ワイヤレス クライアントは異なるスイッチに関連付けられた異なるアクセス ポイントにクライアントを関連付けることができます。ワイヤレス クライアントのローミングは、次の 2 つのタイプに分類できます。

- スイッチ内ローミング
- スイッチ間ローミング

（注） クライアントのポリシーは、モビリティ グループ内のすべてのスイッチで使用できる必要があります。クライアントに一貫した操作ができるように、同じ SSID およびポート ポリシーをモビリティ グループのすべてのスイッチに適用する必要があります。

スイッチ間ローミング

クライアントが 1 つの場所から別の場所にローミングすると、同じスイッチ（固定スイッチ）または他のスイッチ（外部スイッチ）に関連付けられたアクセス ポイントに関連付けることができます。スイッチ間ローミングは、クライアントのローミング前に同じデバイスに関連付けられていなかったアクセス ポイントに、クライアントが関連付けられるシナリオを示しています。ホスト デバイスは、クライアントが最初に固定されていたデバイスの外部になります。

スイッチ間ローミングの場合、クライアントの QoS ポリシーは、常に外部コントローラで実行されます。クライアントが固定スイッチから外部スイッチにローミングされると、QoS ポリシーは固定スイッチでアンインストールされ、外部スイッチにインストールされます。モビリティのハンドオフ メッセージでは、固定デバイスが 外部スイッチにポリシーの名前を渡します。外部スイッチには、QoS ポリシーが正しく適用できるように同じ名前のポリシーが必要です。

スイッチ間ローミングの場合、QoS ポリシーはすべて、固定デバイスから外部デバイスに移動します。固定デバイスから外部デバイスへの QoS ポリシーの移行中は、外部デバイスのトラフィックがデフォルトで提供されます。これは、クライアントのターゲットの新しいポリシー インストールに似ています。

（注） 外部デバイスがユーザ定義の物理ポート ポリシーを使用して設定されていない場合、デフォルト ポート ポリシーはRT1 キューを通過する制御トラフィックを除き、NRT キューを介してルーティングされるすべてのトラフィックに適用されます。ネットワーク管理者は、固定および未知のデバイスで同じ物理ポートのポリシーを対称的に設定する必要があります。

スイッチ間ローミングでは、クライアントが外部のスイッチに関連付けられている一定の期間だけ、クライアントおよびSSIDポリシー統計情報が収集されます。ローミング全体（固定スイッチおよび外部スイッチ）の累積統計情報は収集されません。

スイッチ内ローミング

スイッチ内ローミングでは、クライアントのローミング前に同じスイッチに関連付けられていたアクセス ポイントに、クライアントが関連付けられます。ただしこのデバイスとの関連付けは、別のアクセス ポイントを通じて行われます。

（注） スイッチ内ローミングの場合、QoS ポリシーはそのまま残ります。

ワイヤレス QoS の貴金属ポリシー

ワイヤレス QoS はユニファイド ワイヤレス コントローラ プラットフォームによって提供される貴金属ポリシーと下位互換性があります。貴金属ポリシーは、コントローラで使用可能なシステム定義のポリシーです。

次のポリシーを使用できます。

- プラチナ：VoIP クライアントに使用されます。
- ゴールド：ビデオ クライアントに使用されます。
- シルバー：ベスト エフォートであると考えられるトラフィックに使用されます。
- ブロンズ：NRT トラフィックに使用されます。

これらのポリシー（別名プロファイル）は、トラフィックに基づいて WLAN に適用できます。Cisco IOS MQC 設定を使用した設定を推奨します。ポリシーは、必要な貴金属ポリシーに基づくシステムで利用可能です。SSIDの入力および出力ポリシーに対してのみ貴金属ポリシーを設定できます。

適用されたポリシーに基づいて、パケット内の 802.1p、802.11e（WMM）、および DSCP フィールドが影響を受けます。これらの値は事前設定されており、スイッチの起動時にインストールされます。

（注） Cisco Unified Wireless Controller に適用できる貴金属ポリシーと異なり、属性 rt-average-rate、nrt-average-rate、および最大レートは、このスイッチ プラットフォームに設定された貴金属ポリシーには適用できません。

関連トピック

貴金属ポリシーの設定（CLI），（1002 ページ）

標準 QoS のデフォルト設定

デフォルトの有線 QoS 設定

スイッチの各有線インターフェイスでは、デフォルトで 2 つのキューが設定されます。すべての制御トラフィックはキュー 0 を通過し、処理されます。その他すべてのトラフィックはキュー 1 を通過し、処理されます。

DSCP マップ

デフォルトの CoS/DSCP マップ

CoS/DSCP マップを使用して、着信パケットの CoS 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングします。次の表に、デフォルトの CoS/DSCP マップを示します。これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 *64*：デフォルトの *CoS/DSCP* マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

デフォルトの IP Precedence/DSCP マップ

着信パケットの IP precedence 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングするには、IP precedence/DSCP マップを使用します。次の表は、デフォルトの IP Precedence/DSCP マップを示しています。これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 *65*：デフォルトの *IP Precedence/DSCP* マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

デフォルトの DSCP/CoS マップ

4 つの出力キューのうち 1 つを選択するために使用される CoS 値を生成するには、DSCP/CoS マップを使用します。次の表に、デフォルトの DSCP/CoS マップを示します。これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 *66*：デフォルトの *DSCP/CoS* マップ

DSCP 値	CoS 値
0 ～ 7	0
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6

DSCP 値	CoS 値
56 ～ 63	7

デフォルトのワイヤレス QoS 設定

スイッチ ポートでは、有線またはワイヤレスの物理ポートは区別されません。ポリシーは、スイッチに関連付けられたデバイスの種類に応じて適用されます。たとえば、アクセス ポイントがスイッチ ポートに接続されている場合、スイッチはアクセス ポイントをワイヤレス デバイスとして検出し、親子ポリシー形式のデフォルトの階層型ポリシーを適用します。このポリシーは、階層型ポリシーです。親ポリシーは変更できませんが、子ポリシー（port-child ポリシー）は、QoS 設定に合わせて変更できます。スイッチは、デフォルトのクラスマップとポリシーマップで事前に設定されます。

QoS ポリシーのガイドライン

不正な形式の QoS ポリシーによりクライアントが除外されるのを防ぐには、次のガイドラインに従います。

- 新しい QoS ポリシーをスイッチに追加する場合、同じ名前の QoS ポリシーは、同じローミングまたはモビリティ ドメイン内の他のスイッチに追加する必要があります。
- スイッチに新しいリリースのソフトウェアイメージがロードされると、新しいポリシー形式がサポートされます。以前のリリースから新しいリリースにソフトウェアイメージをアップグレードした場合は、設定を別々に保存する必要があります。以前のリリースのイメージがロードされると、一部の QoS ポリシーがサポートされていないと表示される場合があり、それらの QoS ポリシーをサポートされるポリシー形式に復元する必要があります。

有線ターゲットの QoS に関する制約事項

ターゲットとは、ポリシーが適用されるエンティティです。有線またはワイヤレス ターゲットにポリシーを適用できます。有線ターゲットには、ポートまたは VLAN を指定できます。ワイヤレス ターゲットには、ポート、無線、SSID、またはクライアントを設定できます。ユーザは、ポート、SSID、およびクライアント ポリシーだけを設定できます。ユーザは、無線ポリシングを設定できません。ポート、無線、SSID、クライアントの QoS ポリシーはダウンストリーム方向に適用されます。アップストリーム方向では、SSID およびクライアント ターゲットだけがサポートされます。ダウンストリームは、トラフィックがスイッチからワイヤレス クライアントに流れていることを示します。アップストリームは、トラフィックがワイヤレス クライアントからスイッチに流れていることを示します。

次に、QoS 機能を有線ターゲットのスイッチに適用する場合の制限事項を示します。

- 有線ターゲットのスイッチ ポートでは、最大 8 つのキューイング クラスがサポートされます。

- 有線ターゲットの有線ポートでは、ポリシーごとに最大63のポリサーがサポートされます。
- QoS 階層でサポートされるのは最大 2 レベルです。
- 階層型ポリシーでは、子ポリシーの親およびキュー機能のポリシーにポートシェーパーがある場合を除き、親子間のオーバーラップは許可されていません。
- QoS ポリシーは、EtherChannel インターフェイスに付加できません。
- 親と子の両方のポリシングは、QoS 階層ではサポートされていません。
- 親と子の両方のマーキングは、QoS 階層ではサポートされていません。
- 同じポリシーでのキュー制限とキュー バッファの混在はサポートされません。

（注） キュー制限の割合は、**queue-buffer** コマンドがこの機能を処理するため、スイッチではサポートされていません。キュー制限は、DSCPおよびCoS拡張でのみサポートされます。

- すべての有線キューイングベースポリシーの分類シーケンスはすべての有線アップストリームポート（10ギガビットイーサネット）で同じであり、すべてのダウンストリーム有線ポート（1 ギガビット イーサネット）で同じです。
- 空のクラスはサポートされません。
- 空のアクションによるクラス マップはサポートされません。
- 有線ターゲットの有線ポートでは、ポリシーごとに最大 256 のクラスがサポートされます。
- ポリシー マップ内のポリサーのアクションには、次の制限事項があります。
  - 適合アクションは送信する必要があります。
  - マークダウン タイプの超過/違反アクションは、cos2cos、prec2prec、dscp2dscp だけです。
  - マークダウン タイプはポリシー内で同じである必要があります。
- 分類カウンタには、次の制限事項があります。
  - 分類カウンタは、バイトの代わりにパケットをカウントします。
  - マーキングまたはポリシングによるQoS設定だけが、分類カウンタをトリガーします。
  - 分類カウンタはポート ベースではありません。これは、分類カウンタが、異なるインターフェイスに接続し、同じポリシーの同じクラスに属するすべてのパケットを集約することを意味します。
  - ポリシー内にポリシングまたはマーキング アクションがある限り、クラス デフォルトは分類カウンタを保持します。
  - クラスに複数の match ステートメントがある場合、分類カウンタは match ステートメントの 1 つにだけトラフィック カウンタを表示します。

- テーブル マップには次の制限事項があります。
  - マークダウンを超過するポリシングのテーブルマップとマークダウンに違反するポリシングのテーブルマップがサポートされるのは、方向およびターゲットごとに1つのみです。
  - テーブル マップは class-default で設定する必要があります。テーブル マップはユーザ定義クラスに対してサポートされません。
- 階層型ポリシーは次の機能で必要になります。
  - ポート シェーパー
  - 集約ポリシング機能
  - PV ポリシー
  - 親シェーピングおよび子マーキング/ポリシング
- 有線ターゲットを含むポートでは、次の階層型ポリシーだけがサポートされています。
  - ワイヤレス クライアントの場合を除き、同じポリシー内でのポリシングの連結はサポートされていません。
  - 同じポリシー内で階層型キューはサポートされていません（ポートシェーパーは例外）。
  - 親クラスでは、すべてのフィルタが同じタイプでなければなりません。子フィルタ タイプは次の例外を除き、親フィルタのタイプと一致している必要があります。
    - IP に一致するように親クラスが設定されている場合、ACL に一致するように子クラスを設定できます。
    - CoS に一致するように親クラスが設定されている場合、ACL に一致するように子クラスを設定できます。
- **trust device** *device_type* インターフェイス コンフィギュレーション コマンドは、スイッチのスタンドアロン コマンドとしてではなく、自動 QoS 設定でのみサポートされます。**trust device** *device_type* インターフェイス コンフィギュレーション コマンドを自動 QoS 設定で使用するときに、接続されているピア デバイスが対応デバイス（信頼ポリシーに一致するデバイスとして定義されているデバイス）ではない場合、CoS 値と DSCP 値の両方が「0」に設定され、いずれの入力ポリシーも有効になりません。

次に、VLAN の QoS 機能を有線ターゲットに適用する場合の制限事項を示します。

- フラットつまり非階層型ポリシーでは、マーキングまたはテーブルマップのみサポートされます。

次に、EtherChannel とチャネル メンバー インターフェイスで QoS 機能を適用するための制限事項と考慮事項を示します。

- QoS は、EtherChannel インターフェイスではサポートされません。

- QoS は、入力および出力方向の EtherChannel メンバー インターフェイスでサポートされます。すべての EtherChannel メンバーが同じ QoS ポリシーを適用する必要があります。QoS ポリシーが同じでない場合、異なるリンクの個々のポリシーは独立して機能します。
- チャネル メンバーへサービス ポリシーを付加すると、EtherChannel 内のすべてのポートに同じポリシーが接続されていることを確認するようユーザに知らせる、次の警告メッセージが表示されます。「Warning: add service policy will cause inconsistency with port xxx in ether channel xxx.」
- 自動 QoS は EtherChannel メンバーではサポートされません。

（注） EtherChannel へサービス ポリシーを付加すると、次のメッセージがコンソールに表示されます。「Warning: add service policy will cause inconsistency with port xxx in ether channel xxx.」この警告メッセージは予期されるメッセージです。この警告メッセージは、同じ EtherChannel 内の他のポートに同じポリシーを付加するように促すものです。同じメッセージがブートアップ中にも表示されます。このメッセージは、EtherChannel メンバー ポート間に不一致があることを意味するものではありません。

関連トピック

ワイヤレス ターゲットの QoS に関する制約事項, （945 ページ）
QoS の前提条件, （900 ページ）
QoS の概要, （901 ページ）
QoS の実装, （913 ページ）

ワイヤレス ターゲットの QoS に関する制約事項

一般的な制約事項

ターゲットとは、ポリシーが適用されるエンティティです。有線またはワイヤレス ターゲットにポリシーを適用できます。有線ターゲットには、ポートまたは VLAN を指定できます。ワイヤレス ターゲットには、ポート、無線、SSID、またはクライアントを設定できます。ユーザは、ポート、SSID、およびクライアント ポリシーだけを設定できます。ユーザは、無線ポリシングを設定できません。ポート、無線、SSID、クライアントの QoS ポリシーはダウンストリーム方向に適用されます。アップストリーム方向では、SSID およびクライアント ターゲットだけがサポートされます。ダウンストリームは、トラフィックがスイッチからワイヤレス クライアントに流れていることを示します。アップストリームは、トラフィックがワイヤレス クライアントからスイッチに流れていることを示します。

- ポート、SSID、および（AAA および Cisco IOS コマンドライン インターフェイスを使用する）クライアント ポリシーのみがユーザ設定可能です。無線ポリシーはワイヤレス制御モジュールで設定されるため、ユーザ設定できません。
- ポートおよび無線ポリシーは、出力方向にのみ適用できます。

- SSID およびクライアント ターゲットには、マーキングおよびポリシング ポリシーのみを設定できます。
- 方向単位ターゲットあたり 1 つのポリシーがサポートされています。
- 出力 class-default SSID ポリシーの場合、平均シェーピング レートを設定した後にキューバッファの割合を 0 に設定する必要があります。
- ポリシー マップのクラス マップには、さまざまなタイプのフィルタを指定できます。ただし、出力方向のマップでサポートされるマーキング アクション（table map、set dscp、または set cos）は 1 つのみです。
- 階層的なクライアントと SSID の入力ポリシーの場合は、親と子ポリシーの両方ともマーキングを設定できません。親ポリシーまたは子ポリシーのいずれかでマーキングを設定できます。
- 同じクラスでの複数の set アクションの設定はできません。
- SSID およびクライアントの入力ポリシーの場合、set アクションは DSCP 値と CoS 値に対してのみサポートされています。
- WLAN グループや QoS ポリシーは削除できません。

ポートのワイヤレス QoS の制約事項

ワイヤレス ポート ターゲットに QoS 機能を適用する場合には、次の制約事項があります。

- すべてのワイヤレス ポートには、1 つのクラス デフォルトとその下に 1 つのアクション シェーピングを持つ同様の親ポリシーが設定されています。シェーピング レートは 802.11a/b/g/ac バンドに依存します。
- `port_chlid_policy` を変更することにより、子ポリシーで最大 4 個のクラスを作成できます。
- ポート レベルの `port_child_policy` に 4 つのクラスがある場合、1 つは non-client-nrt クラス、もう 1 つは class-default である必要があります。
- 2 つのクラスに同じプライオリティ レベルを設定することはできません。プライオリティ レベル 1（音声トラフィックと制御トラフィック用）および 2（ビデオ用）のみがサポートされます。
- マルチキャスト NRT クラス（non-client-nrt クラス）と `class-default` では、プライオリティはサポートされません。
- 4 つのクラスが設定されている場合、いずれか 2 つがプライオリティ クラスでなければなりません。3 つのクラスのみが設定されている場合、少なくとも 1 つがプライオリティ クラスでなければなりません。3 つのクラスが設定されていて、non-client-nrt クラスがない場合、両方のプライオリティ レベルが必要です。
- 一致する DSCP のみサポートされます。
- ワイヤレス制御モジュールによって適用されるポート ポリシーは、CLI を使用して削除することはできません。

- 同じクラスのプライオリティ レートとポリシング CIR（MQC を使用）はサポートされていません。
- キュー制限（重み付けテール ドロップを設定するために使用）はサポートされていません。

SSID に対するワイヤレス QoS の制約事項

次に、SSID で QoS 機能を適用するときの制約事項を示します。

- 入力ポリシーでは 1 つのテーブル マップがサポートされます。
- テーブル マップは、親 class-default でのみサポートされます。最大 2 つのテーブル マップが出力方向でサポートされ、QoS グループが関係する場合、3 つのテーブル マップを設定できます。

（注） テーブル マップは、クライアント ターゲットではサポートされません。

- ワイヤレス ポートのデフォルト ポリシーにキューが 2 つ（マルチキャスト NRT 用に 1 つ、class-default 用に 1 つ）しかない場合、SSID レベルのポリシーは出力方向の音声およびビデオ クラスを設定できません。
- プライオリティのないポリシングは出力方向でサポートされません。
- SSID レベルのプライオリティ設定は、RT1 および RT2 ポリサー（ポリサー用 AFD）を設定する目的でのみ使用されます。プライオリティの設定にシェーピング レートは含まれません。そのため、プライオリティはポリシングのない SSID ポリシーに対して制限されます。
- **set** が class-default で有効にされていない場合、音声やビデオの SSID 分類は、ポート レベルで音声またはビデオ クラスの分類の一部である必要があります。
- DSCP2DSCP および COS2COS テーブルでのマッピングは、ポート レベル ポリシーの音声およびビデオ クラスの分類機能に基づいている必要があります。
- 子ポリシーの class-default ではアクションは許可されません。
- SSID の入力ポリシーでは、UP および DSCP フィルタ（一致基準）のみがサポートされます。ACL およびプロトコルの一致基準はサポートされません。
- 入力方向のフラット ポリシー（非階層型）では、ポリシー設定はセット（テーブル マップ）、ポリシング、またはその両方である必要があります。

クライアントのワイヤレス QoS の制約事項

次は、クライアント ターゲットでの QoS ポリシーの適用に関する制約事項です。

- デフォルトのクライアント ポリシーは、ACM イネーブルの WMM クライアント上でのみイネーブルにされます。
- キューイングはサポートされていません。

- イネーブル状態の WLAN では、クライアント ポリシーの付加、削除また変更はサポートされません。ポリシーを適用、削除、または変更するには、WLAN をシャットダウンする必要があります。
- テーブル マップ設定は、ターゲット クライアントでサポートされていません。
- class-default で一緒に設定されたポリシングとセットは、出力方向でブロックされます。

```
policy-map foo
class class-default
police X
set dscp Y
```

- 親ポリシーが他のユーザ定義クラス マップを含む場合、子ポリシーは class-default でサポートされません。
- フラットな出力クライアント ポリシーでは、class-default 内のポリシングおよび他のクラス内のマーキング アクションはサポートされません。
- クライアント ポリシーでは、セット マーキング アクションのみがサポートされます。
- クライアント入力ポリシーでは、ACL、Up、DSCP、およびプロトコル フィルタ（一致基準）のみがサポートされます。
- クライアントポリシーのポリシーマップ クラスのフィルタすべてに、同じ属性が必要です。IPv4 または IPv6 アドレスなどのプロトコル固有の属性で一致するフィルタは、異なる属性セットと見なされます。
- ACL で一致するフィルタでは、アクセス リストのすべての ACE（アクセス コントロール エントリ）に同じ種類と同じ数の属性が必要です。
- クライアント出力ポリシーでは、マーキング属性で一致するフィルタにおいて、policy-map 内のすべてのフィルタが同じマーキング属性で一致する必要があります。たとえば、フィルタが DSCP で一致する場合、ポリシー内のすべてのフィルタが DSCP で一致する必要があります。
- ポート範囲で一致する ACL とサブネットは、入力方向でのみサポートされます。

関連トピック

ポート ポリシー, （907 ページ）
ポート ポリシーの形式, （907 ページ）
無線ポリシー, （909 ページ）
有線ターゲットの QoS に関する制約事項, （942 ページ）
QoS の前提条件, （900 ページ）
QoS の概要, （901 ページ）
QoS の実装, （913 ページ）

QoS の設定方法

クラス、ポリシー、およびテーブル マップの設定

トラフィック クラスの作成（CLI）

一致基準が含まれるトラフィック クラスを作成するには、**class-map** コマンドを使用してトラフィック クラス名を指定し、必要に応じて、**match** コマンドをクラスマップ コンフィギュレーション モードで使用します。

はじめる前に

この設定作業で指定するすべての match コマンドの使用は任意ですが、1 つのクラスに少なくとも 1 つの一致基準を設定する必要があります。

手順の概要

1. **configureterminal**
2. **class-map**{*class-map name* |**match-any**}
3. **matchaccess-group** {*index number*|*name*}
4. **matchclass-map** *class-map name*
5. **matchcos** *cos value*
6. **matchdscp** *dscp value*
7. **matchip**{**dscp***dscp value*| **precedence***precedence value*}
8. **matchnon-client-nrt**
9. **matchqos-group** *qos group value*
10. **matchvlan** *vlan value*
11. **matchwlanuser-priority***wlan value*
12. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**class-map**{*class-map name* |**match-any**} 例： スイッチ(config)# **class-map test_1000** スイッチ(config-cmap)#	クラスマップ コンフィギュレーション モードを開始します。 • 名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。 • **match-any** を指定すると、トラフィック クラスで受信したトラフィックがトラフィック クラスの一部と分類されるには、一致基準の 1 つを満たす必要があります。これはデフォルトです。
ステップ 3	**matchaccess-group** {*index number*|*name*} 例： スイッチ(config-cmap)# **match access-group 100** スイッチ(config-cmap)#	このコマンドでは次のパラメータを使用できます。 • access-group • class-map • cos • dscp • ip • non-client-nrt • precedence • qos-group • vlan • wlan user priority （任意）この例では、アクセス グループ ID を入力します。 • アクセス リスト インデックス（1 ～ 2799 の値） • 名前付きアクセス リスト
ステップ 4	**matchclass-map** *class-map name* 例： スイッチ(config-cmap)# **match class-map test_2000** スイッチ(config-cmap)#	（任意）別のクラス マップ名に一致します。

	コマンドまたはアクション	目的
ステップ 5	**matchcos** *cos value* 例： スイッチ(config-cmap)# **match cos 2 3 4 5** スイッチ(config-cmap)#	（任意）IEEE 802.1Q または ISL サービス クラス（ユーザ）プライオリティ値に一致します。 • 最大 4 つの CoS 値（0 ～ 7）をスペースで区切って入力します。
ステップ 6	**matchdscp** *dscp value* 例： スイッチ(config-cmap)# **match dscp af11 af12** スイッチ(config-cmap)#	（任意）IPv4 および IPv6 パケットの DSCP 値に一致します。
ステップ 7	**matchip** {**dscp***dscp value*| **precedence***precedence value*} 例： スイッチ(config-cmap)# **match ip dscp af11 af12** スイッチ(config-cmap)#	（任意）次を含む IP 値に一致します。 • **dscp**：IP DSCP（DiffServ コードポイント）に一致します。 • **precedence**：IP precedence（0 ～ 7）に一致します。
ステップ 8	**matchnon-client-nrt** 例： スイッチ(config-cmap)# **match non-client-nrt** スイッチ(config-cmap)#	（任意）非クライアントの NRT（非リアルタイム）に一致します。 （注） この一致は、ワイヤレス ポートのポリシーにのみ適用できます。これは、すべての複数の宛先および AP（非クライアント）宛のトラフィックを伝送します。
ステップ 9	**matchqos-group** *qos group value* 例： スイッチ(config-cmap)# **match qos-group 10** スイッチ(config-cmap)#	（任意）QoS グループ値（0 ～ 31）に一致します。
ステップ 10	**matchvlan** *vlan value* 例： スイッチ(config-cmap)# **match vlan 210** スイッチ(config-cmap)#	（任意）VLAN ID（1 ～ 4095）に一致します。

	コマンドまたはアクション	目的
ステップ 11	**matchwlanuser-priority***wlan value* 例： スイッチ(config-cmap)# **match wlan user priority 7** スイッチ(config-cmap)#	（任意）802.11eに固有の値に一致します。ユーザ プライオリティ 802.11e ユーザ プライオリティ（0 ～ 7）を入力します。
ステップ 12	**end** 例： スイッチ(config-cmap)# **end**	設定の変更内容を保存します。

次の作業

ポリシー マップを設定します。

関連トピック

クラス マップ，（920 ページ）

例：アクセス コントロール リストによる分類，（1008 ページ）

トラフィック ポリシーの作成（CLI）

トラフィック ポリシーを作成するには、**policy-map** グローバル コンフィギュレーション コマンドを使用して、トラフィック ポリシーの名前を指定します。

トラフィック クラスは、**class** コマンドを使用したときにサービス ポリシーと関連付けられます。**class** コマンドは、ポリシー マップ コンフィギュレーション モードを開始した後に実行する必要があります。**class** コマンドを入力すると、スイッチが自動的にポリシー マップ クラス コンフィギュレーション モードを開始します。ここでトラフィック ポリシーの QoS ポリシーを定義します。

次のポリシー マップ クラスのアクションがサポートされます。

- admit：コール アドミッション制御（CAC）の要求を許可します。
- bandwidth：帯域幅設定オプション。
- exit：QoS クラス アクション コンフィギュレーション モードを終了します。
- no：コマンドのデフォルト値を無効にするか、設定します。
- police：ポリシング機能の設定オプション。
- priority：このクラスの完全スケジューリング プライオリティの設定オプション。

- queue-buffers：キューのバッファ設定オプション。
- queue-limit：重み付けテール ドロップ（WTD）設定オプションのキューの最大しきい値。
- service-policy：QoS サービス ポリシーを設定します。
- set：次のオプションを使用して QoS 値を設定します。
  - CoS 値
  - DSCP 値
  - precedence 値
  - QoS グループ値
  - WLAN 値
- shape：トラフィック シェーピング設定オプション。

はじめる前に

最初にクラス マップを作成する必要があります。

手順の概要

1. **configureterminal**
2. **policy-map***policy-map name*
3. **class**{*class-name*|**class-default**}
4. **admit**
5. **bandwidth**{**kb/s***kb/s value*|**percent***percentage* | **remaining**{*percent* | *ratio*}}
6. **exit**
7. **no**
8. **police** {*target_bit_rate*| **cir**| **rate**}
9. **priority**{*kb/s* | **level** *level value* | **percent***percentage value*}
10. **queue-buffersratio** *ratio limit*
11. **queue-limit**{*packets* | **cos**| **dscp** | **percent**}
12. **service-policy***policy-map name*
13. **set** {**cos** |**dscp**|**ip**| **precedence**|**qos-group** |**wlan**}
14. **shape average**{*target _bit_rate*| **percent**}
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map***policy-map name* 例： スイッチ(config)# **policy-map test_2000** スイッチ(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class**{*class-name*|**class-default**} 例： スイッチ(config-pmap)# **class test_1000** スイッチ(config-pmap-c)#	ポリシーを作成または変更するクラスの名前を指定します。 未分類のパケットのシステムデフォルト クラスも作成できます。
ステップ 4	**admit** 例： スイッチ(config-pmap-c)# **admit cac wmm-tspec** スイッチ(config-pmap-c)#	（任意）コール アドミッション制御（CAC）の要求を許可します。このコマンドおよび使用の詳細な例については、コール アドミッション制御の設定（CLI），（979 ページ）を参照してください。 （注）　このコマンドは、ワイヤレス QoS の CAC だけを設定します。
ステップ 5	**bandwidth**{**kb/s***kb/s value*|**percent***percentage* | **remaining**{*percent* | *ratio*}} 例： スイッチ(config-pmap-c)# **bandwidth 50** スイッチ(config-pmap-c)#	（任意）次のいずれかを使用して帯域幅を設定します。 • **kb/s**：kpbs に 20000 ～ 10000000 の値を入力します。 • **percent**：このポリシー マップに使用される総帯域幅の割合を入力します。 • **remaining**：残りの帯域幅の割合を入力します。 このコマンドおよび使用の詳細な例については、帯域幅の設定（CLI），（987 ページ）を参照してください。
ステップ 6	**exit** 例： スイッチ(config-pmap-c)# **exit**	（任意）QoS クラス アクション コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
	スイッチ(config-pmap-c)#	
ステップ 7	**no** 例： スイッチ(config-pmap-c)# **no** スイッチ(config-pmap-c)#	（任意）コマンドを無効にします。
ステップ 8	**police** {*target_bit_rate*| **cir**| **rate**} 例： スイッチ(config-pmap-c)# **police 100000** スイッチ(config-pmap-c)#	（任意）ポリサーを設定します。 • *target_bit_rate*：ビット レート/秒を入力します。8000 ～ 10000000000 の値を入力します。 • **cir**：認定情報レート。 • **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングルレベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。 このコマンドおよび使用の詳細な例については、ポリシングの設定（CLI），（989 ページ）を参照してください。
ステップ 9	**priority**{*kb/s* | **level** *level value* | **percent***percentage value*} 例： スイッチ(config-pmap-c)# **priority percent 50** スイッチ(config-pmap-c)#	（任意）このクラスに完全スケジューリング プライオリティを設定します。コマンド オプションは次のとおりです。 • *kb/s*：kbps に 1 ～ 2000000 の値を入力します。 • **level**：マルチレベル プライオリティ キューを確立します。値を入力します（1 または 2）。 • **percent**：このプライオリティの全帯域幅の割合を入力します。 このコマンドおよび使用の詳細な例については、プライオリティの設定（CLI），（992 ページ）を参照してください。
ステップ 10	**queue-buffersratio** *ratio limit* 例： スイッチ(config-pmap-c)# **queue-buffers ratio 10** スイッチ(config-pmap-c)#	（任意）クラスのキューバッファを設定します。キューバッファの割合制限（0 ～ 100）を入力します。 このコマンドおよび使用の詳細な例については、キューバッファの設定（CLI），（995 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 11	**queue-limit**{*packets* | **cos**| **dscp** | **percent**} 例： スイッチ(config-pmap-c)# **queue-limit cos 7 percent 50** スイッチ(config-pmap-c)#	（任意）テール ドロップに対してキューの最大しきい値を指定します。 • *packets*：デフォルトのパケット数。1 ～ 2000000 の間の値を入力します。 • **cos**：各 CoS 値のパラメータを入力します。 • **dscp**：各 DSCP 値のパラメータを入力します。 • **percent**：しきい値の割合を入力します。 このコマンドおよび使用の詳細な例については、キュー制限の設定（CLI），（998 ページ）を参照してください。
ステップ 12	**service-policy***policy-map name* 例： スイッチ(config-pmap-c)# **service-policy test_2000** スイッチ(config-pmap-c)#	（任意）QoS サービス ポリシーを設定します。
ステップ 13	**set** {**cos** |**dscp**|**ip**| **precedence**|**qos-group** |**wlan**} 例： スイッチ(config-pmap-c)# **set cos 7** スイッチ(config-pmap-c)#	（任意）QoS 値を設定します。使用可能な QoS 設定値は次のとおりです。 • **cos**：IEEE 802.1Q/ISL サービス クラスまたはユーザ プライオリティを設定します。 • **dscp**：IP（v4）および IPv6 パケットの DSCP を設定します。 • **ip**：IP 固有の値を設定します。 • **precedence**：IP（v4）および IPv6 パケットの precedence を設定します。 • **qos-group**：QoS グループを設定します。 • **wlan**：WLAN ユーザ プライオリティを設定します。
ステップ 14	**shape average**{*target _bit_rate*| **percent**} 例： スイッチ(config-pmap-c) #**shape average percent 50** スイッチ(config-pmap-c) #	（任意）トラフィック シェーピングを設定します。コマンド パラメータは次のとおりです。 • *target_bit_rate*：ターゲット ビット レート。 • **percent**：認定情報レートのインターフェイス帯域幅の割合。 このコマンドおよび使用の詳細な例については、シェーピングの設定（CLI），（1001 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 15	**end** 例： スイッチ(config-pmap-c) #**end** スイッチ(config-pmap-c) #	設定の変更内容を保存します。

次の作業

インターフェイスを設定します。

関連トピック

ポリシー マップ，（920 ページ）

クライアント ポリシーの設定

次のいずれかの方法を使用して、クライアント ポリシーを設定できます。

方式	トピック/詳細
デフォルト クライアント ポリシー	アドミッション制御（ACM）が WMM クライアントに対してイネーブルの場合、スイッチのワイヤレス制御モジュールは、デフォルト クライアント ポリシーを適用します。ACM がディセーブルの場合、デフォルト クライアント ポリシーはありません。 デフォルト ポリシーは次のとおりです。 • 入力：cldeffromWMM • 出力：cldeftoWMM **show ap dot11 {5ghz | 24ghz}** コマンドを使用して、ACM がイネーブルにされているかどうかの確認が出来ます。ACM をイネーブルにするには、**ap dot11 {5ghz | 24ghz} cac voice acm** コマンドを使用します。
GUI を使用して WLAN にクライアント ポリシーを適用します。	クライアント ポリシーの設定（GUI）
CLI を使用して WLAN にクライアント ポリシーを適用します。	WLAN での SSID またはクライアント ポリシーの適用（CLI），（966 ページ）

方式	トピック/詳細
CLI によるローカルプロファイリングポリシーを使用して Qos 属性ポリシーを適用します。	WLAN 上のデバイスのローカル ポリシーの適用（CLI），（782 ページ）
GUI によるローカルプロファイリングポリシーを使用して Qos 属性ポリシーを適用します。	• [Configuration] > [Security] > [Local Policies] の順に選択して、ローカル プロファイリング ポリシーを作成します。 • [Configuration] > [Wireless] > [WLAN] > [Policy Mapping] の順に選択して、ローカルプロファイリング ポリシーを WLAN に適用します。 詳細については、次のサイトを参照してください。 WLAN へのローカル ポリシーの適用（GUI），（2133 ページ）
AAA サーバ（ACS/ISE）によりポリシー マップを適用します	『*Cisco Identity Services Engine User Guide*』 『*Cisco Secure Access Control System User Guide*』

クラスベースのパケット マーキングの設定（CLI）

この手順は、次のクラスベースパケット マーキング機能をスイッチで設定する方法を示します。

- CoS 値
- DSCP の値
- IP 値
- precedence 値
- QoS グループ値
- WLAN 値

はじめる前に

この手順を開始する前にクラス マップとポリシー マップを作成する必要があります。

手順の概要

1. **configureterminal**
2. **policy-map***policy name*
3. **class***class name*
4. **set cos** {*cos value* | **cos table***table-map name* | **dscp table** *table-map name* | **precedence table***table-map name* | **qos-group table***table-map name* | **wlan user-priority table***table-map name*}
5. **set dscp** {*dscp value* | **default** | **dscp table** *table-map name* | **ef** | **precedence table***table-map name* | **qos-group table***table-map name* | **wlan user-priority table***table-map name*}
6. **set ip** {**dscp** | **precedence**}
7. **set precedence** {*precedence value* | **cos table***table-map name* | **dscp table** *table-map name* | **precedence table***table-map name* | **qos-group table***table-map name*}
8. **set qos-group** {*qos-group value* | **dscp table** *table-map name* | **precedence table***table-map name*}
9. **set wlan user-priority** {*wlan user-priority value* | **cos table***table-map name* | **dscp table** *table-map name* | **qos-group table***table-map name* | **wlan table***table-map name*}
10. **end**
11. **show policy-map**

手順の詳細

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

ステップ 2	**policy-map***policy name*
	
	例：
	
	`スイッチ(config)# policy-map policy1`
	`スイッチ(config-pmap)#`
		ポリシー マップ コンフィギュレーション モードを開始します。
		
		1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

ステップ 3	**class***class name*
	
	例：
	
	`スイッチ(config-pmap)# class class1`
	`スイッチ(config-pmap-c)#`
		ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。
		
		ポリシー クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。
		
		• **admit**：コール アドミッション制御（CAC）の要求を許可します。
		• **bandwidth**：帯域幅設定オプション。
		• **exit**：QoS クラス アクション コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
		• **no**：コマンドのデフォルト値を無効にするか、設定します。 • **police**：ポリシング機能の設定オプション。 • **priority**：このクラスの完全スケジューリング プライオリティの設定オプション。 • **queue-buffers**：キューのバッファ設定オプション。 • **queue-limit**：重み付けテール ドロップ（WTD）設定オプションのキューの最大しきい値。 • **service-policy**：QoS サービス ポリシーを設定します。 • **set**：次のオプションを使用して QoS 値を設定します。 ◦ CoS 値 ◦ DSCP 値 ◦ precedence 値 ◦ QoS グループ値 ◦ WLAN 値 • **shape**：トラフィック シェーピング設定オプション。 （注） この手順では、**set** コマンド オプションを使用して、使用可能な設定について説明します。その他のコマンド オプション（**admit**、**bandwidth** など）についてはこのマニュアルの他の項で説明します。このタスクでは、使用可能なすべての **set** コマンドが表示されますが、クラス単位でサポートされるのは1つの **set** コマンドだけです。

ステップ 4	**set cos** {*cos value* | **cos table***table-map name* | **dscp table** *table-map name* | **precedence table***table-map name* | **qos-group table***table-map name* | **wlan user-priority table***table-map name*}
	
	例：
	
	`スイッチ(config-pmap)# set cos 5`
	
	`スイッチ(config-pmap)#`
		（任意）発信パケットの固有の IEEE 802.1Q レイヤ 2 CoS 値を設定します。値は 0 ～ 7 です。
		set cos コマンドを使用して次の値を設定することもできます。
		• **cos table**：CoS 値をテーブル マップに基づいて設定します。
		• **dscp table**：コード ポイント値をテーブル マップに基づいて設定します。
		• **precedence table**：コード ポイント値をテーブル マップに基づいて設定します。
		• **qos-group table**：テーブル マップに基づいて QoS グループから CoS 値を設定します。

	コマンドまたはアクション	目的
		• **wlan user-priority table**：テーブル マップに基づいて WLAN ユーザ プライオリティから CoS 値を設定します。
ステップ 5	**set dscp** {*dscp value* | **default** | **dscp table** *table-map name* | **ef** | **precedence table***table-map name* | **qos-group table***table-map name* | **wlan user-priority table***table-map name*} 例： スイッチ(config-pmap)# **set dscp af11** スイッチ(config-pmap)#	（任意）DSCP 値を設定します。 特定の DSCP 値の設定に加えて、**set dscp** コマンドを使用して次を設定できます。 • **default**：パケットをデフォルト DSCP 値（000000）と一致させます。 • **dscp table**：テーブルマップに基づいて DSCP からパケットの DSCP 値を設定します。 • **ef**：パケットを EF DSCP 値（101110）と一致させます。 • **precedence table**：テーブル マップに基づいて優先順位からパケットの DSCP 値を設定します。 • **qos-group table**：テーブル マップに基づいて QoS グループからパケットの DSCP 値を設定します。 • **wlan user-priority table**：パケットの DSCP 値を、テーブル マップに基づいた WLAN ユーザ プライオリティに基づいて設定します。
ステップ 6	**set ip** {**dscp** | **precedence**} 例： スイッチ(config-pmap)# **set ip dscp c3** スイッチ(config-pmap)#	（任意）IP 固有の値を設定します。これらの値は、IP DSCP 値または IP precedence 値です。 **set ip dscp** コマンドを使用して、次の値を設定することができます。 • *dscp value*：特定の DSCP の値を設定します。 • **default**：パケットをデフォルト DSCP 値（000000）と一致させます。 • **dscp table**：テーブルマップに基づいて DSCP からパケットの DSCP 値を設定します。 • **ef**：パケットを EF DSCP 値（101110）と一致させます。 • **precedence table**：テーブル マップに基づいて優先順位からパケットの DSCP 値を設定します。 • **qos-group table**：テーブル マップに基づいて QoS グループからパケットの DSCP 値を設定します。 • **wlan user-priority table**：パケットの DSCP 値を、テーブル マップに基づいた WLAN ユーザ プライオリティに基づいて設定します。

	コマンドまたはアクション	目的
		set ip precedence コマンドを使用して、次の値を設定することができます。 • *precedence value*：precedence 値を設定します（0 ～ 7）。 • **cos table**：テーブル マップに基づいてレイヤ 2 CoS からパケットの precedence 値を設定します。 • **dscp table**：テーブル マップに基づいて DSCP 値からパケットの precedence 値を設定します。 • **precedence table**：テーブルマップに基づいて優先順位から precedence 値を設定します。 • **qos-group table**：テーブル マップに基づいて QoS グループから precedence 値を設定します。

ステップ 7	**set precedence** {*precedence value* | **cos table***table-map name* | **dscp table** *table-map name* | **precedence table***table-map name* | **qos-group table***table-map name*}
	
	例：
	
	`スイッチ(config-pmap)# set precedence 5`
	`スイッチ(config-pmap)#`
		（任意）IPv4 と IPv6 パケットの precedence 値を設定します。
		set precedence コマンドを使用して、次の値を設定することができます。
		• *precedence value*：precedence 値を設定します（0 ～ 7）。
		• **cos table**：レイヤ 2 CoS からのパケットの precedence 値をテーブル マップに基づいて設定します。
		• **dscp table**：テーブル マップに基づいて DSCP 値からパケットの precedence 値を設定します。
		• **precedence table**：テーブルマップに基づいて優先順位から precedence 値を設定します。
		• **qos-group table**：テーブル マップに基づいて QoS グループから precedence 値を設定します。

ステップ 8	**set qos-group** {*qos-group value* | **dscp table** *table-map name* | **precedence table***table-map name*}
	
	例：
	
	`スイッチ(config-pmap)# set qos-group 10`
	`スイッチ(config-pmap)#`
		（任意）QoS グループ値を設定します。このコマンドを使用して次の値を設定できます。
		• *qos-group value*：1 から 31 までの数。
		• **dscp table**：テーブル マップに基づいて DSCP からコード ポイント値を設定します。
		• **precedence table**：テーブル マップに基づいて優先順位からコード ポイント値を設定します。

ステップ 9	**set wlan user-priority** {*wlan user-priority value* | **cos table***table-map name* | **dscp table** *table-map name* | **qos-group**	（任意）WLANユーザプライオリティ値を設定します。このコマンドを使用して次の値を設定できます。 • *wlan user-priority value*：0 ～ 7 の範囲の値。

	コマンドまたはアクション	目的
	table*table-map name* | **wlan table***table-map name*} 例： スイッチ(config-pmap)# **set wlan user-priority 1** スイッチ(config-pmap)#	• **cos table**：テーブル マップに基づいて Cos から WLAN ユーザ プライオリティ値を設定します。 • **dscp table**：テーブル マップに基づいて DSCP から WLAN ユーザ プライオリティ値を設定します。 • **qos-group table**：テーブル マップに基づいて QoS グループから WLAN ユーザ プライオリティ値を設定します。 • **wlan table**：テーブル マップに基づいて WLAN ユーザ プライオリティから WLAN ユーザ プライオリティ値を設定します。
ステップ 10	**end** 例： スイッチ(config-pmap)# **end** スイッチ#	設定変更を保存します。
ステップ 11	**show policy-map** 例： スイッチ# **show policy-map**	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次の作業

service-policy コマンドを使用して、インターフェイスにトラフィック ポリシーを付加します。

音声およびビデオに対するクラス マップの設定（CLI）

音声およびビデオ トラフィックに対するクラス マップを設定するには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **class-map** *class-map-name*
3. **match dscp** *dscp-value-for-voice*
4. **end**
5. **configure terminal**
6. **class-map***class-map-name*
7. **match dscp** *dscp-value-for-video*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** *class-map-name* 例： スイッチ(config)# **class-map voice**	クラス マップを作成します。
ステップ 3	**match dscp** *dscp-value-for-voice* 例： スイッチ(config-cmap)# **match dscp 46**	IPv4 および IPv6 パケットの DSCP 値を照合します。この値を 46 に設定します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 6	**class-map***class-map-name* 例： スイッチ(config)# **class-map video**	クラス マップを設定します。
ステップ 7	**match dscp** *dscp-value-for-video* 例： スイッチ(config-cmap)# **match dscp 34**	IPv4 および IPv6 パケットの DSCP 値を照合します。この値を 34 に設定します。
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

トラフィック ポリシーのインターフェイスへの付加（CLI）

トラフィック クラスとトラフィック ポリシーの作成後、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、トラフィック ポリシーをインターフェイスに付加し、ポリ

シーを適用する方向を指定します（インターフェイスに着信するパケットまたはインターフェイスから送信されるパケット）。

はじめる前に

インターフェイスにトラフィック ポリシーを付加する前に、トラフィック クラスとトラフィック ポリシーを作成する必要があります。

手順の概要

1. **configureterminal**
2. **interface***type*
3. **service-policy**{**input***policy-map* | **output***policy-map* }
4. **end**
5. **show policy map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***type* 例： スイッチ(config)# **interface GigabitEthernet1/0/1** スイッチ(config-if)#	インターフェイス コンフィギュレーション モードを開始し、インターフェイスを設定します。 インターフェイス コンフィギュレーションのコマンド パラメータは次のとおりです。 • **Auto Template**：自動テンプレート インターフェイス • **Capwap**：Capwap トンネル インターフェイス • **GigabitEthernet**：Gigabit Ethernet IEEE 802 • **GroupVI**：グループ仮想インターフェイス • **Internal Interface**：内部インターフェイス • **Loopback**：ループバック インターフェイス • **Null**：ヌル インターフェイス • **Port-channel**：インターフェイスのイーサネット チャネル • **TenGigabitEthernet**：10 ギガビット イーサネット • **Tunnel**：トンネル インターフェイス • **Vlan**：Catalyst VLAN

	コマンドまたはアクション	目的
		• **Range**：インターフェイス範囲
ステップ 3	**service-policy** {**input***policy-map* | **output***policy-map* } 例： スイッチ(config-if)# **service-policy output policy_map_01** スイッチ(config-if)#	ポリシーマップを入力または出力インターフェイスに適用します。このポリシーマップは、そのインターフェイスのサービスポリシーとして使用されます。 この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。
ステップ 4	**end** 例： スイッチ(config-if)# **end** スイッチ#	設定変更を保存します。
ステップ 5	**show policy map** 例： スイッチ# **show policy map**	（任意）指定されたインターフェイスのポリシーの統計情報を表示します。

次の作業

他のトラフィック ポリシーをインターフェイスに付加し、ポリシーを適用する方向を指定します。

関連トピック

物理ポートのポリシー マップ, （921 ページ）

WLAN での SSID またはクライアント ポリシーの適用（CLI）

はじめる前に

SSID に適用する前にサービス ポリシー マップを設定する必要がありますSSID。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **service-policy** [**input** | **output**] *policy-name*
4. **service-policy client** [**input** | **output**] *policy-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `スイッチ# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**service-policy** [**input** | **output**] *policy-name* 例： `スイッチ(config-wlan)# service-policy input policy-map-ssid`	ポリシーを適用します。次のオプションを使用できます。 • **Input**：ポリシーマップを WLAN 入力トラフィックに割り当てます。 • **output**：ポリシーマップを WLAN 出力トラフィックに割り当てます。
ステップ 4	**service-policy client** [**input** | **output**] *policy-name* 例： `スイッチ(config-wlan)# service-policy client input policy-map-client`	ポリシーを適用します。次のオプションを使用できます。 • **input**：クライアント ポリシーを WLAN の入力方向に割り当てます。 • **output**：クライアント ポリシーを WLAN の出力方向に割り当てます。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

SSID ポリシー, （910 ページ）

ワイヤレス ターゲットでサポートされる QoS 機能, （905 ページ）
例：SSID ポリシー
例：ダウンストリーム SSID ポリシーの設定, （1013 ページ）

ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング（CLI）

実行対象となるトラフィック クラスを指定する非階層型ポリシーマップを、物理ポート上に設定できます。サポートされるアクションは再マーキングとポリシングです。

はじめる前に

この手順を開始する前に、ネットワーク トラフィックの分類、ポリシング、およびマーキングについて、あらかじめポリシー マップによって決定しておく必要があります。

手順の概要

1. **configureterminal**
2. **class-map**{*class-map name* |**match-any**}
3. **match access-group** { *access list index* | *access list name* }
4. **policy-map***policy-map-name*
5. **class** {*class-map-name* | **class-default**}
6. **set** {**cos** |**dscp**|**ip**| **precedence**|**qos-group** |**wlan user-priority**}
7. **police** {*target_bit_rate*| **cir**| **rate**}
8. **exit**
9. **exit**
10. **interface***interface-id*
11. **service-policy input***policy-map-name*
12. **end**
13. **show policy-map** [*policy-map-name* [**class***class-map-name*]]
14. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map**{*class-map name* |**match-any**}	クラス マップ コンフィギュレーション モードを開始します。 • 名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。

	コマンドまたはアクション	目的
	例： スイッチ(config)# **class-map ipclass1** スイッチ(config-cmap)# **exit** スイッチ(config)#	• **match-any** を指定すると、トラフィック クラスで受信したトラフィックの場合、一致基準の 1 つに必ず一致し、そのトラフィック クラスの一部と分類されます。これはデフォルトです。
ステップ 3	**match access-group** { *access list index* | *access list name* } 例： スイッチ(config-cmap)# **match access-group 1000** スイッチ(config-cmap)# **exit** スイッチ(config)#	分類基準をクラス マップに一致するように指定します。次の基準について照合できます。 • **access-group**：アクセス グループに一致します。 • **class-map**：別のクラス マップに一致します。 • **cos**：CoS 値に一致します。 • **dscp**：DSCP 値に一致します。 • **ip**：特定の IP 値に一致します。 • **non-client-nrt**：非クライアント NRT に一致します。 • **precedence**：IPv4 および IPv6 パケットの precedence 値に一致します。 • **qos-group**：QoS グループに一致します。 • **vlan**：VLAN に一致します。 • **wlan**：ワイヤレス LAN に一致します。
ステップ 4	**policy-map***policy-map-name* 例： スイッチ(config)# **policy-map flowit** スイッチ(config-pmap)#	ポリシーマップ名を入力することによってポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。
ステップ 5	**class** {*class-map-name* | **class-default**} 例： スイッチ(config-pmap)# **class ipclass1** スイッチ(config-pmap-c)#	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップ クラス マップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **class-default** トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシーマッ

	コマンドまたはアクション	目的
		プの最後に配置されます。暗黙の **match any** が **class-default** クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは **class-default** と一致します。

ステップ 6	**set** {**cos** |**dscp**|**ip**| **precedence**|**qos-group** |**wlan user-priority**}
	
	例：
	
	`スイッチ(config-pmap-c)# set dscp 45`
	`スイッチ(config-pmap-c)#`
		（任意）QoS 値を設定します。使用可能な QoS 設定値は次のとおりです。
		• **cos**：IEEE 802.1Q/ISL サービス クラスまたはユーザ プライオリティを設定します。
		• **dscp**：IP（v4）および IPv6 パケットの DSCP を設定します。
		• **ip**：IP 固有の値を設定します。
		• **precedence**：IP（v4）および IPv6 パケットの precedence を設定します。
		• **qos-group**：QoS グループを設定します。
		• **wlan user-priority**：WLAN ユーザ プライオリティを設定します。
		
		この例では、**set dscp** コマンドが、パケットでの新しい DSCP 値を設定して IP トラフィックを分類します。

ステップ 7	**police** {*target_bit_rate*| **cir**| **rate**}
	
	例：
	
	`スイッチ(config-pmap-c)# police 100000 conform-action transmit exceed-action drop`
	`スイッチ(config-pmap-c)#`
		（任意）ポリサーを設定します。
		• *target_bit_rate*：ビット レート/秒を指定し、8000 ～ 10000000000 の値を入力します。
		• **cir**：認定情報レート。
		• **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングルレベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。
		
		この例では、**police** コマンドが 100000 セットのターゲット ビット レートを超えるトラフィックがドロップされるクラスにポリサーを追加します。

ステップ 8	**exit** 例： `スイッチ(config-pmap-c)# exit`	ポリシー マップ コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： スイッチ(config-pmap)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 2/0/1**	ポリシーマップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 11	**service-policy input***policy-map-name* 例： スイッチ(config-if)# **service-policy input flowit**	ポリシーマップ名を指定し、入力ポートに適用します。サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 12	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 13	**show policy-map** [*policy-map-name* [**class***class-map-name*]] 例： スイッチ# **show policy-map**	（任意）入力を確認します。
ステップ 14	**copy running-config startup-config** 例： スイッチ# **copy-running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

必要に応じて QoS 設定は、ポリシー マップを使用して、SVI のトラフィックの分類、ポリシング、およびマーキングを設定します。

ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング（CLI）

はじめる前に

この手順を開始する前に、ポリシーマップを使用して、ネットワーク トラフィックの分類、ポリシング、およびマーキングについて決定しておく必要があります。

手順の概要

1. **configureterminal**
2. **class-map**{*class-map name* |**match-any**}
3. **match vlan***vlan number*
4. **policy-map***policy-map-name*
5. **description***description*
6. **class** {*class-map-name* | **class-default**}
7. **set** {**cos** |**dscp**|**ip**| **precedence**|**qos-group** |**wlan user-priority**}
8. **police** {*target_bit_rate*| **cir**| **rate**}
9. **exit**
10. **exit**
11. **interface***interface-id*
12. **service-policy input***policy-map-name*
13. **end**
14. **show policy-map** [*policy-map-name* [**class***class-map-name*]]
15. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map**{*class-map name* |**match-any**} 例： スイッチ(config)# **class-map class_vlan100**	クラス マップ コンフィギュレーション モードを開始します。 • 名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。 • **match-any** を指定すると、トラフィック クラスで受信したトラフィックの場合、一致基準の 1 つに必ず一致し、そのトラフィック クラスの一部と分類されます。これはデフォルトです。

	コマンドまたはアクション	目的
ステップ 3	**match vlan***vlan number* 例： スイッチ(config-cmap)# **match vlan 100** スイッチ(config-cmap)# **exit** スイッチ(config)#	VLAN をクラス マップに一致するように指定します。
ステップ 4	**policy-map***policy-map-name* 例： スイッチ(config)# **policy-map policy_vlan100** スイッチ(config-pmap)#	ポリシーマップ名を入力することによってポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。
ステップ 5	**description***description* 例： スイッチ(config-pmap)# **description vlan 100**	（任意）ポリシー マップの説明を入力します。
ステップ 6	**class** {*class-map-name* | **class-default**} 例： スイッチ(config-pmap)# **class class_vlan100** スイッチ(config-pmap-c)#	トラフィック分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップ クラス マップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **class-default** トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシーマップの最後に配置されます。暗黙の **match any** が **class-default** クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは **class-default** と一致します。
ステップ 7	**set** {**cos** |**dscp**|**ip**| **precedence**|**qos-group** |**wlan user-priority**} 例： スイッチ(config-pmap-c)# **set dscp af23** スイッチ(config-pmap-c)#	（任意）QoS 値を設定します。使用可能な QoS 設定値は次のとおりです。 • **cos**：IEEE 802.1Q/ISL サービス クラスまたはユーザ プライオリティを設定します。 • **dscp**：IP（v4）および IPv6 パケットの DSCP を設定します。 • **ip**：IP 固有の値を設定します。

	コマンドまたはアクション	目的
		• **precedence**：IP（v4）および IPv6 パケットの precedence を設定します。 • **qos-group**：QoS グループを設定します。 • **wlan user-priority**：WLAN ユーザ プライオリティを設定します。 この例では、**set dscp** コマンドが AF23（010010）の DSCP 値にパケットを照合することによって、IP トラフィックを分類します。

ステップ 8	**police** {*target_bit_rate*| **cir**| **rate**}
	
	例：
	
	`スイッチ(config-pmap-c)# police 200000 conform-action transmit exceed-action drop`
	`スイッチ(config-pmap-c)#`
		（任意）ポリサーを設定します。
		• *target_bit_rate*：ビット レート/秒を指定します。8000 ～ 10000000000 の範囲で値を入力します。
		• **cir**：認定情報レート。
		• **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングルレベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。
		
		この例では、**police** コマンドが 200000 セットのターゲット ビット レートを超えるトラフィックがドロップされるクラスにポリサーを追加します。

ステップ 9	**exit** 例： `スイッチ(config-pmap-c)# exit`	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 10	**exit** 例： `スイッチ(config-pmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet 1/0/3`	ポリシーマップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。

	コマンドまたはアクション	目的
ステップ 12	**service-policy input***policy-map-name* 例： スイッチ(config-if)# **service-policy input policy_vlan100**	ポリシーマップ名を指定し、入力ポートに適用します。サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 13	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 14	**show policy-map** [*policy-map-name* [**class***class-map-name*]] 例： スイッチ# **show policy-map**	（任意）入力を確認します。
ステップ 15	**copy running-config startup-config** 例： スイッチ# **copy-running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN のポリシー マップ，（922 ページ）
例：ポリサーの VLAN 設定，（1021 ページ）

テーブル マップの設定（CLI）

テーブル マップはマーキングの形式であり、テーブルを使用してフィールド間のマッピングと変換を可能にすることもできます。たとえば、テーブル マップはレイヤ 2 の CoS 設定をレイヤ 3 の precedence 値にマッピングして変換するために使用できます。

（注） テーブル マップは、複数のポリシーで、または同じポリシー内で複数回参照できます。

手順の概要

1. **configureterminal**
2. **table-map***name* {**default** {*default value* | **copy** | **ignore**} | **exit** | **map** {**from***from value***to***to value* } | **no**}
3. **mapfrom***value***to***value*
4. **exit**
5. **exit**
6. **show table-map**
7. **configureterminal**
8. **policy-map**
9. **class class-default**
10. **set cos dscp table***table map name*
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**table-map***name* {**default** {*default value*	**copy**	**ignore**}	**exit**	**map** {**from***from value***to***to value* }	**no**} 例： スイッチ(config)# **table-map table01** スイッチ(config-tablemap)#	テーブルマップを作成し、テーブルマップ コンフィギュレーション モードを開始します。テーブル マップ コンフィギュレーション モードでは、次のタスクを実行できます。 • **default**：テーブルマップのデフォルト値を設定するか、テーブルマップ内にない値についてのデフォルトの動作（コピーまたは無視）を設定します。 • **exit**：テーブルマップ コンフィギュレーション モードを終了します。 • **map**：テーブル マップで *from* 値を *to* 値にマッピングします。 • **no**：コマンドのデフォルト値を無効にするか、設定します。
ステップ 3	**mapfrom***value***to***value* 例： スイッチ(config-tablemap)# **map from 0 to**	この手順では、DSCP 値が 0 のパケットを CoS 値 2 に、DSCP 値が 1 のパケットを CoS 値 4 に、DSCP 値が 24 のパケットを CoS 値 3 に、DSCP 値が 40 のパケットを CoS

	コマンドまたはアクション	目的
	2 スイッチ(config-tablemap)# **map from 1 to 4** スイッチ(config-tablemap)# **map from 24 to 3** スイッチ(config-tablemap)# **map from 40 to 6** スイッチ(config-tablemap)# **default 0** スイッチ(config-tablemap)#	値 6 に、およびそれ以外のすべてのパケットを CoS 値 0 にマークします。 （注） この例の CoS 値から DSCP 値へのマッピングは、後で説明するように、**set** ポリシー マップ クラス コンフィギュレーション コマンドを使用して設定します。
ステップ 4	**exit** 例： スイッチ(config-tablemap)# **exit** スイッチ(config)#	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**exit** 例： スイッチ(config) **exit** スイッチ#	特権 EXEC モードに戻ります。
ステップ 6	**show table-map** 例： スイッチ# **show table-map** Table Map table01 from 0 to 2 from 1 to 4 from 24 to 3 from 40 to 6 default 0	テーブル マップ設定を表示します。
ステップ 7	**configureterminal** 例： スイッチ# **configure terminal** スイッチ(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 8	**policy-map** 例： スイッチ(config)# **policy-map table-policy** スイッチ(config-pmap)#	テーブル マップのポリシー マップを設定します。

	コマンドまたはアクション	目的
ステップ 9	**class class-default** 例： スイッチ(config-pmap)# **class class-default** スイッチ(config-pmap-c)#	クラスをシステム デフォルトに一致させます。
ステップ 10	**set cos dscp table***table map name* 例： スイッチ(config-pmap-c)# **set cos dscp table table01** スイッチ(config-pmap-c)#	このポリシーが入力ポートに適用された場合、そのポートでは trust dscp がイネーブルになり、テーブル マップに応じてマーキングが行われます。
ステップ 11	**end** 例： スイッチ(config-pmap-c)# **end** スイッチ#	特権 EXEC モードに戻ります。

次の作業

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

関連トピック

テーブル マップのマーキング，（924 ページ）

例：テーブル マップのマーキング設定，（1023 ページ）

信頼の設定

ワイヤレス トラフィックの信頼動作の設定（CLI）

Cisco IOS XE 3.2 リリースは、有線およびワイヤレス ポートに対して信頼できるさまざまなデフォルト設定をサポートしました。有線ポートの信頼できるデフォルト設定に関して、このソフトウェア リリースでの変更はありません。ワイヤレス ポートの場合、デフォルトのシステム動作は非信頼でした。つまり、スイッチの起動時に、ワイヤレス ポートのマーキングすべてがデフォルトでゼロに設定され、トラフィックはプライオリティ処理されませんでした。既存の有線スイッチとの互換性のために、すべてのトラフィックはデフォルトでベスト エフォートのキューへ送信され

ていました。アクセスポイントは、プライオリティキューイングをデフォルトで実行していました。ダウンストリーム方向では、アクセス ポイントは、キューイング用に音声、ビデオ、ベストエフォート、およびバックグラウンドのキューを保持していました。アクセスは 11e タグ情報に基づいてキューイング戦略を選択していました。デフォルトでは、アクセス ポイントはすべてのワイヤレス パケットをベスト エフォートとして処理していました。

手順の概要

1. **configure terminal**
2. **qos wireless-default-untrust**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**qos wireless-default-untrust** 例： `スイッチ (config)# qos wireless-default-untrust`	スイッチの動作を設定して、ワイヤレス トラフィックを非信頼にします。ワイヤレス トラフィックをデフォルトで信頼するようにスイッチを設定するには、このコマンドの **no** 形式を使用します。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

有線およびワイヤレス ポートの信頼動作, （935 ページ）

QoS の特性と機能の設定

コール アドミッション制御の設定（CLI）

このタスクでは、スイッチでコール アドミッション制御（CAC）用にクラスベースの無条件パケット マーキング機能を設定する方法を説明します。

手順の概要

1. **configureterminal**
2. **class-map***class name*
3. **matchdscp** *dscp value*
4. **exit**
5. **class-map***class name*
6. **matchdscp** *dscp value*
7. **exit**
8. **table-map***name*
9. **default copy**
10. **exit**
11. **table-map***name*
12. **default copy**
13. **exit**
14. **policy-map***policy name*
15. **class***class-map-name*
16. **prioritylevel***level_value*
17. **police** [*target_bit_rate*| **cir**| **rate**]
18. **admit cac wmm-tspec**
19. **rate***value*
20. **wlan-up***value*
21. **exit**
22. **exit**
23. **class***class name*
24. **prioritylevel***level_value*
25. **police** [*target_bit_rate*| **cir**| **rate**]
26. **admit cac wmm-tspec**
27. **rate***value*
28. **wlan-up***value*
29. **exit**
30. **exit**
31. **policy-map***policy name*
32. **class***class-map-name*
33. **set dscp dscp table***table_map_name*
34. **set wlan user-priority dscp table***table_map_name*
35. **shapeaverage** {*target bit rate*| **percent***percentage*}
36. **queue-buffers** {**ratio***ratio value*}
37. **service-policy***policy_map_name*
38. **end**
39. **show policy-map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map***class name* 例： スイッチ(config)# **class-map voice** スイッチ(config-cmap)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • *word*：クラス マップ名。 • **class-default**：未分類のパケットを照合するシステム デフォルト クラス。
ステップ 3	**matchdscp** *dscp value* 例： スイッチ(config-cmap)# **match dscp 46**	（任意）IPv4およびIPv6パケットのDSCP値に一致します。
ステップ 4	**exit** 例： スイッチ(config-cmap)# **exit** スイッチ(config)#	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**class-map***class name* 例： スイッチ(config)# **class-map video** スイッチ(config-cmap)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • *word*：クラス マップ名。 • **class-default**：未分類のパケットを照合するシステム デフォルト クラス。
ステップ 6	**matchdscp** *dscp value* 例： スイッチ(config-cmap)# **match dscp**	（任意）IPv4およびIPv6パケットのDSCP値に一致します。

	コマンドまたはアクション	目的
	34	
ステップ 7	**exit** 例： スイッチ(config-cmap)# **exit** スイッチ(config)#	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**table-map***name* 例： スイッチ(config)# **table-map dscp2dscp** スイッチ(config-tablemap)#	テーブルマップを作成し、テーブルマップ コンフィギュレーション モードを開始します。
ステップ 9	**default copy** 例： スイッチ(config-tablemap)# **default copy**	コピーするテーブルマップで検出されない値のデフォルト動作を設定します。 （注） これがデフォルトのオプションです。DSCP から DSCP へ値をマッピングすることもできます。
ステップ 10	**exit** 例： スイッチ(config-tablemap)# **exit** スイッチ(config)#	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**table-map***name* 例： スイッチ(config)# **table-map dscp2up** スイッチ(config-tablemap)#	新しいテーブル マップを作成し、テーブル マップ コンフィギュレーション モードを開始します。
ステップ 12	**default copy** 例： スイッチ(config-tablemap)# **default copy**	コピーするテーブルマップで検出されない値のデフォルト動作を設定します。 （注） これがデフォルトのオプションです。DSCP から UP へ値をマッピングすることもできます。

	コマンドまたはアクション	目的
ステップ 13	**exit** 例： スイッチ(config-tablemap)# **exit** スイッチ(config)#	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**policy-map***policy name* 例： スイッチ(config)# **policy-map ssid_child_cac** スイッチ(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 15	**class***class-map-name* 例： スイッチ(config-pmap)# **class voice**	インターフェイス レベルのトラフィック分類を定義し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 16	**prioritylevel***level_value* 例： スイッチ(config-pmap-c)# **priority level 1**	**priority** コマンドは、クラスに完全スケジューリング プライオリティを割り当てます。 （注） プライオリティ レベル 1 はプライオリティ レベル 2 より重要です。プライオリティ レベル 1 は、QoS に最初に処理される帯域幅を予約するため、遅延は非常に低くなります。プライオリティ レベル 1 と 2 はどちらも帯域幅を予約します。
ステップ 17	**police** [*target_bit_rate*| **cir**| **rate**] 例： スイッチ(config-pmap-c)# **police cir 10m**	（任意）ポリサーを設定します。 • *target_bit_rate*：ビット レート/秒を指定します。8000 ～ 10000000000 の範囲で値を入力します。 • **cir**：認定情報レート。 • **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングルレベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。
ステップ 18	**admit cac wmm-tspec** 例： スイッチ(config-pmap-c)# **admit cac wmm-tspec** スイッチ(config-pmap-cac-wmm)#	ポリシー マップに対するコール アドミッション制御を設定します。 （注） このコマンドは、ワイヤレス QoS の CAC だけを設定します。

	コマンドまたはアクション	目的
ステップ 19	**rate***value* 例： スイッチ(config-pmap-admit-cac-wmm)# **rate 5000**	ターゲット ビット レート（kbps）を設定します。8 ～ 10000000 の範囲の数を入力してください。
ステップ 20	**wlan-up***value* 例： スイッチ(config-pmap-admit-cac-wmm)# **wlan-up 6 7**	WLAN UP 値を設定します。0 ～ 7 の範囲の数を入力してください。
ステップ 21	**exit** 例： スイッチ(config-pmap-admit-cac-wmm)# **exit** スイッチ(config-pmap-c)#	ポリシー マップ クラス コンフィギュレーション モードに戻ります。
ステップ 22	**exit** 例： スイッチ(config-pmap-c)# **exit** スイッチ(config-pmap)#	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 23	**class***class name* 例： スイッチ(config-pmap)# **class video** スイッチ(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • *word*：クラス マップ名。 • **class-default**：未分類のパケットを照合するシステム デフォルト クラス。
ステップ 24	**prioritylevel***level_value* 例： スイッチ(config-pmap-c)# **priority level 2**	**priority** コマンドは、クラスに完全スケジューリング プライオリティを割り当てます。 （注） プライオリティ レベル 1 はプライオリティ レベル 2 より重要です。プライオリティ レベル 1 は、QoS に最初に処理される帯域幅を予約するため、遅延は非常に低くなります。プライオリティ レベル 1 と 2 はどちらも帯域幅を予約します。

	コマンドまたはアクション	目的
ステップ 25	**police** [*target_bit_rate*| **cir**| **rate**] 例： スイッチ(config-pmap-c)# **police cir 20m**	（任意）ポリサーを設定します。 • *target_bit_rate*：ビット レート/秒を指定します。8000 ～ 10000000000 の範囲で値を入力します。 • **cir**：認定情報レート。 • **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングルレベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。
ステップ 26	**admit cac wmm-tspec** 例： スイッチ(config-pmap-c)# **admit cac wmm-tspec** スイッチ(config-pmap-admit-cac-wmm)#	ポリシー マップに対するコール アドミッション制御を設定します。 （注） このコマンドは、ワイヤレス QoS の CAC だけを設定します。
ステップ 27	**rate***value* 例： スイッチ(config-pmap-admit-cac-wmm)# **rate 5000**	ターゲット ビット レート（kbps）を設定します。8 ～ 10000000 の範囲の数を入力してください。
ステップ 28	**wlan-up***value* 例： スイッチ(config-pmap-admit-cac-wmm)# **wlan-up 4 5**	WLAN UP 値を設定します。0 ～ 7 の範囲の数を入力してください。
ステップ 29	**exit** 例： スイッチ(config-pmap-cac-wmm)# **exit** スイッチ(config-pmap)#	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 30	**exit** 例： スイッチ(config-pmap)# **exit** スイッチ(config)#	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 31	**policy-map***policy name* 例： スイッチ(config)# **policy-map ssid_cac** スイッチ(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 32	**class***class-map-name* 例： スイッチ(config-pmap)# **class default**	インターフェイス レベルのトラフィック分類を定義し、ポリシーマップ コンフィギュレーション モードを開始します。 この例では、クラス マップはデフォルトに設定されます。
ステップ 33	**set dscp dscp table***table_map_name* 例： スイッチ(config-pmap-c)# **set dscp dscp table dscp2dscp**	（任意）QoS 値を設定します。この例では、**set dscp dscp table** コマンドはテーブル マップを作成し、値を設定します。
ステップ 34	**set wlan user-priority dscp table***table_map_name* 例： スイッチ(config-pmap-c)# **set wlan user-priority dscp table dscp2up**	（任意）QoS 値を設定します。この例では、**set wlan user-priority dscp table** コマンドは WLAN ユーザ プライオリティを設定します。
ステップ 35	**shapeaverage** {*target bit rate*| **percent***percentage*} 例： スイッチ(config-pmap-c)# **shape average 100000000**	平均シェーピング レートを設定します。平均シェーピング レートを、ターゲット ビット レート（bps）または認定情報レート（CIR）のインターフェイス帯域幅の割合で設定できます。
ステップ 36	**queue-buffers** {**ratio***ratio value*} 例： スイッチ(config-pmap-c)# **queue-buffers ratio 0**	キューの相対的なバッファ サイズを設定します。 （注） ポリシーに設定されているすべてのバッファの合計が 100 % 以下である必要があります。未割り当てバッファは、残りのキューに均等に分散されます。

	コマンドまたはアクション	目的
ステップ 37	**service-policy***policy_map_name* 例： スイッチ(config-pmap-c)# **service-policy ssid_child_cac**	サービス ポリシーのポリシー マップを指定します。
ステップ 38	**end** 例： スイッチ(config-pmap)# **end** スイッチ#	設定変更を保存します。
ステップ 39	**show policy-map** 例： スイッチ# **show policy-map**	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次の作業

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

CAC の詳細については、『*System Management Configuration Guide, Cisco IOS XE Release 3SE*（*Catalyst 3650 Switches*）』を参照してください。

帯域幅の設定（CLI）

この手順は、スイッチで帯域幅を設定する方法を示します。

はじめる前に

この手順を開始する前に、帯域幅のクラス マップを作成する必要があります。

手順の概要

1. **configureterminal**
2. **policy-map***policy name*
3. **class***class name*
4. **bandwidth** {*Kb/s* | **percent***percentage* | **remaining** { **ratio***ratio*}}
5. **end**
6. **show policy-map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map***policy name* 例： スイッチ(config)# **policy-map policy_bandwidth01** スイッチ(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class***class name* 例： スイッチ(config-pmap)# **class class_bandwidth01** スイッチ(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • *word*：クラス マップ名。 • **class-default**：未分類のパケットを照合するシステム デフォルト クラス。
ステップ 4	**bandwidth** {*Kb/s*	**percent***percentage*	**remaining** { **ratio***ratio*}} 例： スイッチ(config-pmap-c)# **bandwidth 200000** スイッチ(config-pmap-c)#	ポリシーマップの帯域幅を設定します。パラメータは次のとおりです。 • *Kb/s*：特定の値を kbps で設定します（20000 ～ 10000000）。 • **percent-**：割合に基づいて、特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。100 % 未満の場合、帯域幅の残りは、すべての帯域幅キュー上に均等に分割されます。

	コマンドまたはアクション	目的
		• **remaining**：特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。このコマンドは、ポリシー内の特定のキューに対して **priority** コマンドが使用されている場合に使用します。各キューには、割合ではなく比率を割り当てることもできます。キューにはそれらの比率に従って、特定の重みが割り当てられます。比率は 0 ～ 100 の範囲で指定できます。この場合のポリシーの全帯域幅での比率の割り当ては、100 を超えることができます。 （注） ポリシー マップで帯域幅タイプを混在させることはできません。たとえば、1 つのポリシー マップで帯域幅の割合と kbps の両方を使用して、帯域幅を設定することはできません。

ステップ 5	**end**
	
	例：
	
	`スイッチ(config-pmap-c)# end`
	`スイッチ#`
		設定変更を保存します。

ステップ 6	**show policy-map** 例： `スイッチ# show policy-map`	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次の作業

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用して、インターフェイスにトラフィック ポリシーを付加します。

関連トピック

帯域幅，（930 ページ）

ポリシングの設定（CLI）

この手順は、スイッチでポリシングを設定する方法を説明しています。

はじめる前に

この手順を開始する前に、ポリシングのクラス マップを作成する必要があります。

手順の概要

1. **configureterminal**
2. **policy-map***policy name*
3. **class***class name*
4. **police** {*target_bit_rate* [*burst bytes* | **bc** | **conform-action** | **pir**] | **cir** {*target_bit_rate* | **percent***percentage*} | **rate** {*target_bit_rate* | **percent***percentage*} **conform-actiontransmitexceed-action** {**drop** [**violate action**] | **set-cos-transmit** | **set-dscp-transmit** | **set-prec-transmit** | **transmit** [**violate action**] }}
5. **end**
6. **show policy-map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map***policy name* 例： スイッチ(config)# **policy-map policy_police01** スイッチ(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class***class name* 例： スイッチ(config-pmap)# **class class_police01** スイッチ(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • *word*：クラス マップ名。 • **class-default**：未分類のパケットを照合するシステム デフォルト クラス。
ステップ 4	**police** {*target_bit_rate* [*burst bytes*	**bc**	**conform-action**	**pir**]	**cir** {*target_bit_rate*	**percent***percentage*}	**rate** {*target_bit_rate*	**percent***percentage*} **conform-actiontransmitexceed-action** {**drop** [**violate action**]	**set-cos-transmit**	**set-dscp-transmit**	**set-prec-transmit**	**transmit** [**violate action**] }}	次の **police** サブコマンド オプションを使用できます。 • *target_bit_rate*：ビット/秒（8000 ～ 10000000000）。 ◦ *burst bytes*：1000 ～ 512000000 の値を入力します。 ◦ **bc**：適合バースト。 ◦ **conform-action**：レートが適合バーストより小さくなる場合に実行されるアクション。

	コマンドまたはアクション	目的
	例： スイッチ(config-pmap-c)# **police 8000 conform-action transmit exceed-action drop** スイッチ(config-pmap-c)#	◦ **pir**：最大情報レート。 • **cir**：認定情報レート。 ◦ *target_bit_rate*：ターゲット ビット レート（8000 ～ 10000000000）。 ◦ **percent**：CIR のインターフェイス帯域幅の割合。 • **rate**：ポリシング レート、階層型ポリシーの PCR、またはシングルレベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。 ◦ *target_bit_rate*：ターゲット ビット レート（8000 ～ 10000000000）。 ◦ **percent**：レートのインターフェイス帯域幅の割合。 次の **police conform-action transmit exceed-action** サブコマンド オプションを使用できます。 • **drop**：パケットをドロップします。 • **set-cos-transmit**：CoS 値を設定して送信します。 • **set-dscp-transmit**：DSCP 値を設定して送信します。 • **set-prec-transmit**：パケットの precedence を書き換えて送信します。 • **transmit**：パケットを送信します。 （注） ポリサー ベースのマークダウン アクションは、テーブル マップを使用する場合のみサポートされます。スイッチ内の各マーキング フィールドでは、1つのマークダウン テーブル マップだけが許可されます。
ステップ 5	**end** 例： スイッチ(config-pmap-c)# **end** スイッチ#	設定変更を保存します。

	コマンドまたはアクション	目的
ステップ 6	**show policy-map** 例： スイッチ# **show policy-map**	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。 （注） **show policy-map** コマンドの出力では、適合バイトおよび超過バイトのカウンタを表示しません。

次の作業

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

関連トピック

シングルレート 2 カラー ポリシング，（927 ページ）

例：シングルレート 2 カラー ポリシング設定，（1022 ページ）

デュアルレート 3 カラー ポリシング，（928 ページ）

例：デュアルレート 3 カラー ポリシング設定，（1023 ページ）

ポリシング，（922 ページ）

例：ポリシング アクションの設定，（1020 ページ）

トークンバケット アルゴリズム，（923 ページ）

例：ポリシングの単位，（1021 ページ）

プライオリティの設定（CLI）

この手順は、スイッチでプライオリティを設定する方法を示します。

スイッチでは、指定されたキューにプライオリティを与えることができます。使用可能な 2 つのプライオリティ レベルがあります（1 および 2）。

（注） 音声とビデオに対応するキューには、プライオリティ レベル 1 を割り当てます。

はじめる前に

この手順を開始する前に、プライオリティのクラス マップを作成する必要があります。

手順の概要

1. **configureterminal**
2. **policy-map***policy name*
3. **class***class name*
4. **priority** [*Kb/s* [*burst_in_bytes*] | **level***level_value* [*Kb/s* [*burst_in_bytes*] | **percent***percentage* [*burst_in_bytes*]] | **percent***percentage* [*burst_in_bytes*]]
5. **end**
6. **show policy-map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map***policy name* 例： スイッチ(config)# **policy-map policy_priority01** スイッチ(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class***class name* 例： スイッチ(config-pmap)# **class class_priority01** スイッチ(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • *word*：クラス マップ名。 • **class-default**：未分類のパケットを照合するシステム デフォルト クラス。
ステップ 4	**priority** [*Kb/s* [*burst_in_bytes*]	**level***level_value* [*Kb/s* [*burst_in_bytes*]	**percent***percentage* [*burst_in_bytes*]]	**percent***percentage* [*burst_in_bytes*]] 例： スイッチ(config-pmap-c)# **priority level 1** スイッチ(config-pmap-c)#	（任意）**priority** コマンドは、クラスに完全スケジューリング プライオリティを割り当てます。 コマンド オプションは次のとおりです。 • *Kb/s*：kbps を指定します（1 ～ 2000000）。 ◦ *burst_in_bytes*：バイトでバーストを指定します（32 ～ 2000000）。

	コマンドまたはアクション	目的
		• **level***level_value*：マルチレベル（1 ～ 2）のプライオリティ キューを指定します。 ◦ *Kb/s*：kbps を指定します（1 ～ 2000000）。 ◦ *burst_in_bytes*：バイトでバーストを指定します（32 ～ 2000000）。 ◦ **percent**：総帯域幅の割合。 ◦ *burst_in_bytes*：バイトでバーストを指定します（32 ～ 2000000）。 • **percent**：総帯域幅の割合。 ◦ *burst_in_bytes*：バイトでバーストを指定します（32 ～ 2000000）。 （注） プライオリティ レベル 1 はプライオリティ レベル 2 より重要です。プライオリティ レベル 1 は、 QoS に最初に処理される帯域幅を予約するため、遅延は非常に低くなります。プライオリティ レベル 1 と 2 はどちらも帯域幅を予約します。

ステップ 5	**end**
	例：
	`スイッチ(config-pmap-c)# end`
	`スイッチ#`
		設定変更を保存します。

ステップ 6	**show policy-map** 例： `スイッチ# show policy-map`	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次の作業

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

関連トピック

プライオリティ キュー, （932 ページ）

キューとシェーピングの設定

出力キューの特性の設定

ネットワークおよびQoS ソリューションの複雑さによっては、この項の手順をすべて実行する必要があります。次の特性を決定する必要があります。

- DSCP、CoS、またはQoS グループ値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューに適用されるドロップ割合のしきい値と、トラフィック タイプで必要な予約メモリと最大メモリ
- キューに割り当てる固定バッファ スペース
- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術（シェーピング、共有、または両方）

（注） 出力キューはスイッチでのみ設定できます。

キュー バッファの設定（CLI）

スイッチ を使用すると、キューにバッファを割り当てることができます。バッファが割り当てられていない場合は、すべてのキューに対して均等に分割されます。queue-buffer ratio を使用して、特定の比率で分割できます。デフォルトでDTS（Dynamic Threshold and Scaling）はすべてのキューでアクティブになるため、これらはソフト バッファになります。

（注） queue-buffer ratio は有線ポートと無線ポートの両方でサポートされますが、queue-buffer ratio は queue-limit とともに設定することはできません。

はじめる前に

この手順の前提条件を次に示します。

- この手順を開始する前に、キュー バッファのクラス マップを作成する必要があります。
- キュー バッファを設定する前に、ポリシー マップの帯域幅、シェーピング、またはプライオリティを設定する必要があります。

手順の概要

1. **configureterminal**
2. **policy-map***policy name*
3. **class***class name*
4. **bandwidth** {*Kb/s* | **percent***percentage* | **remaining** {**ratio***ratio value* }}
5. **queue-buffers** {**ratio***ratio value*}
6. **end**
7. **show policy-map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map***policy name* 例： スイッチ(config)# **policy-map policy_queuebuffer01** スイッチ(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class***class name* 例： スイッチ(config-pmap)# **class class_queuebuffer01** スイッチ(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • *word*：クラス マップ名。 • **class-default**：未分類のパケットを照合するシステム デフォルト クラス。
ステップ 4	**bandwidth** {*Kb/s*	**percent***percentage*	**remaining** {**ratio***ratio value* }} 例： スイッチ(config-pmap-c)# **bandwidth percent 80** スイッチ(config-pmap-c)#	ポリシー マップの帯域幅を設定します。コマンド パラメータは次のとおりです。 • *Kb/s*：特定の値を設定するには、このコマンドを使用します。指定できる範囲は 20000 ～ 10000000 です。 • **percent**：割合を使用して特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合

	コマンドまたはアクション	目的
		計が 100 % を超えることはできません。100 % 未満の場合、帯域幅の残りは、すべての帯域幅キュー上に均等に分割されます。 • **remaining**：特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。このコマンドは、ポリシー内の特定のキューに対して **priority** コマンドが使用されている場合に使用します。各キューには、割合ではなく比率を割り当てることもできます。キューにはそれらの比率に従って、特定の重みが割り当てられます。比率は 0 ～ 100 の範囲で指定できます。この場合のポリシーの全帯域幅での比率の割り当ては、100 を超えることができます。 （注） ポリシー マップで帯域幅タイプを混在させることはできません。
ステップ 5	**queue-buffers** {**ratio***ratio value*} 例： スイッチ(config-pmap-c)# **queue-buffers ratio 10** スイッチ(config-pmap-c)#	キューの相対的なバッファ サイズを設定します。 （注） ポリシーに設定されているすべてのバッファの合計が 100 % 以下である必要があります。未割り当てバッファは、残りのキューに均等に分散されます。
ステップ 6	**end** 例： スイッチ(config-pmap-c)# **end** スイッチ#	設定変更を保存します。
ステップ 7	**show policy-map** 例： スイッチ# **show policy-map**	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次の作業

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

関連トピック

キュー バッファの割り当て, （934 ページ）

例：キュー バッファの設定, （1020 ページ）

キュー制限の設定（CLI）

重み付けテール ドロップ（WTD）を設定するためにキュー制限を使用します。WTD を使用すると、キューごとに複数のしきい値を設定できます。各サービス クラスが異なるしきい値でドロップされて QoS 差別化が実現されます。スイッチによって、3 つの明示的にプログラム可能なしきい値クラスとして各キューに 0、1、2 を指定できます。したがって、キューごとに各パケットのキューイング/ドロップの決定は、フレーム ヘッダーの DSCP、CoS、または QoS グループ フィールドに指定されたパケットのしきい値クラスの割り当てによって決定されます。

WTD では柔軟な制限が使用されるため、最大 400 %（共通プールで予約されるバッファの最大 4 倍）のキュー制限を設定できます。この柔軟な制限は、他の機能に影響することなく、共通プールのオーバーランを防止します。

（注） キュー制限は、有線ポートのスイッチの出力キューでのみ設定できます。

はじめる前に

この手順の前提条件を次に示します。

- この手順を開始する前に、キュー制限を使用するクラスマップを作成する必要があります。
- キュー制限を設定する前に、ポリシー マップの帯域幅、シェーピング、またはプライオリティを設定する必要があります。

手順の概要

1. **configureterminal**
2. **policy-map***policy name*
3. **class***class name*
4. **bandwidth** {*Kb/s* | **percent***percentage* | **remaining** {**ratio***ratio value* }}
5. **queue-limit** {*packets***packets** | **cos** {*cos value* { *maximum threshold value* | **percent***percentage* } | **values** {*cos value*| **percent***percentage* } } | **dscp** {*dscp value* {*maximum threshold value* | **percent***percentage*} | *match packet* {*maximum threshold value* | **percent***percentage*} | **default** {*maximum threshold value* | **percent***percentage*} | **ef** {*maximum threshold value* | **percent***percentage*} | **dscp values***dscp value*} | **percent***percentage* }}
6. **end**
7. **show policy-map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map***policy name* 例： スイッチ(config)# **policy-map policy_queuelimit01** スイッチ(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class***class name* 例： スイッチ(config-pmap)# **class class_queuelimit01** スイッチ(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • *word*：クラス マップ名。 • **class-default**：未分類のパケットを照合するシステム デフォルト クラス。
ステップ 4	**bandwidth** {*Kb/s* | **percent***percentage* | **remaining** {**ratio***ratio value* }} 例： スイッチ(config-pmap-c)# **bandwidth 500000** スイッチ(config-pmap-c)#	ポリシー マップの帯域幅を設定します。パラメータは次のとおりです。 • *Kb/s*：特定の値を設定するには、このコマンドを使用します。指定できる範囲は 20000 ～ 10000000 です。 • **percent**：特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。100 % 未満の場合、帯域幅の残りは、すべての帯域幅キュー上に均等に分割されます。 • **remaining**：特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。このコマンドは、ポリシー内の特定のキューに対して **priority** コマンドが使用されている場合に使用します。各キューには、割合ではなく比率を割り当てることもできます。キューにはそれらの比率に従って、特定の重みが割り当てられます。比率は 0 ～ 100 の範囲

	コマンドまたはアクション	目的
		で指定できます。この場合のポリシーの全帯域幅での比率の割り当ては、100 を超えることができます。 （注） ポリシーマップで帯域幅タイプを混在させることはできません。

ステップ 5	**queue-limit** {*packets***packets** | **cos** {*cos value* { *maximum threshold value* | **percent***percentage* } | **values** {*cos value*| **percent***percentage* } } | **dscp** {*dscp value* {*maximum threshold value* | **percent***percentage*} | *match packet* {*maximum threshold value* | **percent***percentage*} | **default** {*maximum threshold value* | **percent***percentage*} | **ef** {*maximum threshold value* | **percent***percentage*} | **dscp values***dscp value*} | **percent***percentage* }}
	
	例：
	
	`スイッチ(config-pmap-c)# queue-limit dscp 3 percent 20`
	`スイッチ(config-pmap-c)# queue-limit dscp 4 percent 30`
	`スイッチ(config-pmap-c)# queue-limit dscp 5 percent 40`
		キュー制限のしきい値の割合を設定します。
		
		すべてのキューで、3 つのしきい値（0、1、2）があり、それぞれのしきい値についてデフォルト値があります。デフォルトまたはその他のキュー制限しきい値設定を変更するには、このコマンドを使用します。たとえば、DSCP 3、4、および 5 のパケットが設定した特定のキューに送信される場合、このコマンドは、この 3 つの DSCP 値のしきい値パーセンテージを設定できます。キュー制限しきい値に関する詳細については、重み付けテール ドロップ, （931 ページ）を参照してください。
		
		（注） スイッチは絶対キュー制限の割合をサポートしません。スイッチは、dscp または cos キュー制限の割合だけをサポートします。

ステップ 6	**end**
	
	例：
	
	`スイッチ(config-pmap-c)# end`
	`スイッチ#`
		設定変更を保存します。

ステップ 7	**show policy-map** 例： `スイッチ# show policy-map`	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次の作業

ネットワークの QoS 用の追加ポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用して、トラフィック ポリシーまたはポリシーをインターフェイスに付加します。

関連トピック

重み付けテール ドロップ, （931 ページ）
例：キュー制限の設定, （1019 ページ）

シェーピングの設定（CLI）

特定のクラスのシェーピング（最大帯域幅）を設定するには、**shape** コマンドを使用します。ポートに残っている追加帯域幅があっても、キューの帯域幅はこの値に制限されます。シェーピングは平均の割合で、または bps のシェーピングの平均値で設定できます。

はじめる前に

この手順を開始する前に、シェーピングのクラス マップを作成する必要があります。

手順の概要

1. **configureterminal**
2. **policy-map***policy name*
3. **class***class name*
4. **shapeaverage** {*target bit rate*| **percent***percentage*}
5. **end**
6. **show policy-map**

手順の詳細

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

ステップ 2	**policy-map***policy name*
	
	例：
	
	`スイッチ(config)# policy-map policy_shaping01`
	`スイッチ(config-pmap)#`
		ポリシーマップ コンフィギュレーション モードを開始します。
		1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。

ステップ 3	**class***class name* 例： `スイッチ(config-pmap)# class class_shaping01`	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • *word*：クラス マップ名。

	コマンドまたはアクション	目的
	スイッチ(config-pmap-c)#	• **class-default**：未分類のパケットを照合するシステムデフォルト クラス。
ステップ 4	**shapeaverage** {*target bit rate*| **percent***percentage*} 例： スイッチ(config-pmap-c)# **shape average percent 50** スイッチ(config-pmap-c)#	平均シェーピング レートを設定します。平均シェーピング レートを、ターゲット ビット レート（bps）または認定情報レート（CIR）のインターフェイス帯域幅の割合で設定できます。 （注） 出力 class-default SSID ポリシーの場合、平均シェーピング レートを設定した後にキュー バッファの割合を 0 に設定する必要があります。
ステップ 5	**end** 例： スイッチ(config-pmap-c)# **end** スイッチ#	設定変更を保存します。
ステップ 6	**show policy-map** 例： スイッチ# **show policy-map**	（任意）すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次の作業

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーをインターフェイスに付加します。

関連トピック

平均レート シェーピング，（929 ページ）
例：平均レート シェーピングの設定，（1018 ページ）
階層型シェーピング，（929 ページ）

貴金属ポリシーの設定（CLI）

WLAN 単位で貴金属 QoS ポリシーを設定できます。

手順の概要

1. **configure terminal**
2. **wlan** *wlan-name*
3. **service-policy** {**input** | **output**} *policy-name*
4. **end**
5. **show wlan** {*wlan-id*|*wlan-name*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コマンド モードを開始します。
ステップ 2	**wlan** *wlan-name* 例： スイッチ**wlan test4**	WLAN コンフィギュレーション サブモードを開始します。
ステップ 3	**service-policy** {**input** | **output**} *policy-name* 例： スイッチ(config-wlan)# **service-policy output platinum** 例： スイッチ(config-wlan)# **service-policy input platinum-up**	QoS ポリシーで WLAN を設定します。貴金属ポリシーで WLAN を設定するには、キーワード **platinum**、**gold**、**silver**、または **bronze** のいずれか 1 つを入力する必要があります。この例に示されるように、**platinum-up** キーワードでアップストリーム ポリシーが指定されます。 （注） アップストリーム ポリシーは、ダウンストリーム ポリシーと異なります。アップストリーム ポリシーには -up サフィックスがあります。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**show wlan** {*wlan-id*|*wlan-name*} 例： スイッチ# **show wlan name qos-wlan**	WLAN の設定済みの QoS ポリシーを検証します。 スイッチ# **show wlan name qos-wlan** . . . . QoS Service Policy - Input Policy Name : platinum-up Policy State : Validated QoS Service Policy - Output Policy Name : platinum Policy State : Validated . . .

	コマンドまたはアクション	目的
		. . .

関連トピック

ワイヤレス QoS の貴金属ポリシー，（939 ページ）

QoS のモニタリング

スイッチでの QoS のモニタリングには、次のコマンドを使用できます。

表 *67*：*QoS* のモニタリング

コマンド	説明
show class-map [*class_map_name*]	設定されているすべてのクラスマップのリストを表示します。
show class-map type control subscriber {**all** | *name* } **show class-map type control subscriber detail**	制御クラスマップと統計情報を表示します。 • all：すべてのクラスマップに関する情報を表示します。 • name：設定済みのクラスマップを表示します。
show policy-map[*policy_map_name*]	設定されているすべてのポリシーマップのリストを表示します。コマンドパラメータは次のとおりです。 • **policy map name** • **interface** • **session**

コマンド	説明
show policy-map interface { **Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Lspvif** | | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output** | **wireless** }	

コマンド	説明
	スイッチで設定されているすべてのポリシーのランタイムと統計情報を表示します。コマンドパラメータは次のとおりです。 • **Auto-template**：Auto-Template インターフェイス • **Capwap**：Capwap トンネルインターフェイス • **GigabitEthernet**：ギガビット イーサネット IEEE.802.3z • **GroupVI**：グループ仮想インターフェイス • **InternalInterface**：内部インターフェイス • **Loopback**：ループバックインターフェイス • **Lspvif**：LSP 仮想インターフェイス • **Null**：ヌルインターフェイス • **port-channel**：インターフェイスのイーサネットチャネル • **TenGigabitEthernet**：10 ギガビット イーサネット • **Tunnel**：トンネルインターフェイス • **Vlan**：Catalyst VLAN • **brief**：ポリシーマップの簡単な説明 • **class**：各クラスの統計情報 • **input**：入力ポリシー • **output**：出力ポリシー

コマンド	説明
	• **Wireless**：ワイヤレス
show policy-map interface wireless ap [*access point*]	スイッチのすべてのワイヤレス AP のランタイムと統計情報を表示します。
show policy-map interface wireless ssid [*ssid*]	スイッチのすべての SSID ターゲットのランタイムと統計情報を表示します。
show policy-map interface wireless client mac [*mac_address*]	スイッチのすべてのクライアントターゲットのランタイムと統計情報を表示します。
show policy-map session [**input** | **output** | **uid***UUID*]	セッションの QoS ポリシーを表示します。コマンドパラメータは次のとおりです。 • **input**：入力ポリシー • **output**：出力ポリシー • **uid**：SSS 固有の ID に基づくポリシー
show policy-map type control subscriber { **all** | **name** }	タイプ QoS ポリシーマップを表示します。
show table-map	すべてのテーブルマップと設定を表示します。
show platform qos wireless {**afd** { **client** | **ssid** } | **stats** { **bssid***bssid-value* | **client***name* | **ssid** {*ssid-value* | **all**} **client all**}}	ワイヤレスのターゲットが表示されます。次のコマンドパラメータがサポートされています。 • afd：AFD 情報 • stats：統計情報
showpolicy-mapinterfacewirelessssidname*ssid-name*[**radio type** {**24ghz** | **5ghz**} **ap name***ap-name* | **ap name***ap-name*]	アクセス ポイントの SSID ポリシー設定を表示します。
show wireless client mac-address*mac_address***service-policy** {**input** | **output**}	クライアント ポリシーの詳細を表示します。

コマンド	説明
show wlan qos service-policies	すべての WLAN に設定された SSID ポリシーを表示します。
show ap name*ap_name***service-policy**	AP 上に設定されているポリシーをすべて表示します。

QoS の設定例

例：アクセス コントロール リストによる分類

この例は、アクセス コントロール リスト（ACL）を使用して QoS のパケットを分類する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# access-list 101 permit ip host 12.4.1.1 host 15.2.1.1
スイッチ(config)# class-map acl-101
スイッチ(config-cmap)# description match on access-list 101
スイッチ(config-cmap)# match access-group 101
スイッチ(config-cmap)#
```

ACL を使用してクラスマップを作成した後で、クラスのポリシーマップを作成し、ポリシーマップを QoS のインターフェイスに適用します。

関連トピック

トラフィック クラスの作成（CLI），（949 ページ）
クラス マップ，（920 ページ）

例：サービス クラス レイヤ 2 の分類

この例は、サービス クラス レイヤ 2 の分類を使用して QoS に対してパケットを分類する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# class-map cos
スイッチ(config-cmap)# match cos ?
  <0-7>  Enter up to 4 class-of-service values separated by white-spaces
スイッチ(config-cmap)# match cos 3 4 5
スイッチ(config-cmap)#
```

CoS レイヤ 2 の分類を使用してクラス マップを作成したら、そのクラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：サービス クラス DSCP の分類

この例は、サービス クラス DSCP の分類を使用して、QoS に対してパケットを分類する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# class-map dscp
スイッチ(config-cmap)# match dscp af21 af22 af23
スイッチ(config-cmap)#
```

DSCP 分類を使用してクラス マップを作成したら、クラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：VLAN ID レイヤ 2 の分類

この例は、VLAN ID レイヤ 2 の分類を使用して QoS に分類する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# class-map vlan-120
スイッチ(config-cmap)# match vlan ?
  <1-4095>  VLAN id
スイッチ(config-cmap)# match vlan 120
スイッチ(config-cmap)#
```

VLAN レイヤ 2 の分類を使用してクラス マップを作成したら、クラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：DSCP 値または precedence 値による分類

この例は、DSCP 値または precedence 値を使用してパケットを分類する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# class-map prec2
スイッチ(config-cmap)# description matching precedence 2 packets
スイッチ(config-cmap)# match ip precedence 2
スイッチ(config-cmap)# exit
スイッチ(config)# class-map ef
スイッチ(config-cmap)# description EF traffic
スイッチ(config-cmap)# match ip dscp ef
スイッチ(config-cmap)#
```

DSCP 値または precedence 値を使用してクラス マップを作成したら、クラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：階層型分類

次の例は、child という名前の別のクラスに一致する parent という名前のクラスが作成される、階層型分類を示しています。child という名前のクラスは、2 に設定された IP precedence に基づいて照合されます。

```
スイッチ# configure terminal
スイッチ(config)# class-map child
スイッチ(config-cmap)# match ip precedence 2
スイッチ(config-cmap)# exit
スイッチ(config)# class-map parent
スイッチ(config-cmap)# match class child
スイッチ(config-cmap)#
```

親クラスマップを作成したら、クラスのポリシーマップを作成し、QoS のインターフェイスにポリシー マップを適用します。

関連トピック

階層型 QoS, （911 ページ）

例：階層型ポリシーの設定

次の例は、階層型ポリシーを使用した設定を示しています。

```
スイッチ# configure terminal
スイッチ(config)# class-map c1
スイッチ(config-cmap)# match dscp 30
スイッチ(config-cmap)# exit

スイッチ(config)# class-map c2
スイッチ(config-cmap)# match precedence 4
スイッチ(config-cmap)# exit

スイッチ(config)# class-map c3
スイッチ(config-cmap)# exit

スイッチ(config)# policy-map child
スイッチ(config-pmap)# class c1
スイッチ(config-pmap-c)# priority level 1
スイッチ(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
スイッチ(config-pmap-c-police)# exit
スイッチ(config-pmap-c)# exit

スイッチ(config-pmap)# class c2
スイッチ(config-pmap-c)# bandwidth 20000
スイッチ(config-pmap-c)# exit
スイッチ(config-pmap)# class class-default
スイッチ(config-pmap-c)# bandwidth 20000
スイッチ(config-pmap-c)# exit
スイッチ(config-pmap)# exit

スイッチ(config)# policy-map parent
スイッチ(config-pmap)# class class-default
スイッチ(config-pmap-c)# shape average 1000000
```

```
スイッチ(config-pmap-c)# service-policy child
スイッチ(config-pmap-c)# end
```

次の例は、テーブル マップを使用した階層型ポリシーを示しています。

```
スイッチ(config)# table-map dscp2dscp
 スイッチ(config-tablemap)# default copy
スイッチ(config)# table-map dscp2up
スイッチ(config-tablemap)# map from 46 to 6
スイッチ(config-tablemap)# map from 34 to 5
スイッチ(config-tablemap)# default copy
スイッチ(config)# policy-map ssid_child_policy
スイッチ(config-pmap)# class voice
スイッチ(config-pmap-c)# priority level 1
スイッチ(config-pmap-c)# police 15000000
スイッチ(config-pmap)# class video
スイッチ(config-pmap-c)# priority level 2
スイッチ(config-pmap-c)# police 10000000
スイッチ(config)# policy-map ssid_policy
スイッチ(config-pmap)# class class-default
スイッチ(config-pmap-c)# shape average 30000000
スイッチ(config-pmap-c)# queue-buffer ratio 0
スイッチ(config-pmap-c)# set dscp dscp table dscp2dscp
スイッチ(config-pmap-c)# service-policy ssid_child_policy
```

関連トピック

階層型 QoS, （911 ページ）

例：音声およびビデオの分類

この例は、スイッチ固有の情報を使用して、音声とビデオのパケット ストリームを分類する方法を示しています。

この例では、音声とビデオがエンドポイント A からスイッチの GigabitEthernet1/0/1 に送信され、それぞれ precedence 値 5 と 6 を持ちます。また、音声とビデオは、エンドポイント B からスイッチの GigabitEthernet1/0/2 にそれぞれ DSCP 値 EF と AF11 で送信されます。

両方のインターフェイスからのすべてのパケットがアップリンク インターフェイスに送信されます。その場合、音声は 100 Mbps にポリシングし、ビデオは 150 Mbps にポリシングする必要があります。

上記の要件ごとに分類するために、GigabitEthernet1/0/1 で送信される音声パケットに一致するクラスが作成されます。これには、precedence 5 に一致する voice-interface-1 という名前が付けらます。同様に、GigabitEthernet1/0/2 の音声パケットに一致する、voice-interface-2 という名前の音声用の別のクラスが作成されます。これらのクラスは、GigabitEthernet1/0/1 に接続される input-interface-1 と、GigabitEthernet1/0/2 に接続される input-interface-2 という 2 つの別個のポリシーに関連付けられます。このクラスのアクションは、qos-group に 10 とマーキングすることです。出力インターフェイスで QoS-group 10 のパケットを照合するために、QoS-group 10 で一致する voice という名前のクラスが作成されます。これは、output-interface という名前の別のポリシーに関連付けられ、アップリンク インターフェイスに関連付けられます。ビデオも同じ方法で処理されますが、QoS-group 20 で一致します。

次の例は、上記のスイッチ固有の情報を使用して分類する方法を示しています。

```
スイッチ(config)#
スイッチ(config)# class-map voice-interface-1
スイッチ(config-cmap)# match ip precedence 5
スイッチ(config-cmap)# exit

スイッチ(config)# class-map video-interface-1
スイッチ(config-cmap)# match ip precedence 6
スイッチ(config-cmap)# exit

スイッチ(config)# class-map voice-interface-2
スイッチ(config-cmap)# match ip dscp ef
スイッチ(config-cmap)# exit

スイッチ(config)# class-map video-interface-2
スイッチ(config-cmap)# match ip dscp af11
スイッチ(config-cmap)# exit

スイッチ(config)# policy-map input-interface-1
スイッチ(config-pmap)# class voice-interface-1
スイッチ(config-pmap-c)# set qos-group 10
スイッチ(config-pmap-c)# exit

スイッチ(config-pmap)# class video-interface-1
スイッチ(config-pmap-c)# set qos-group 20

スイッチ(config-pmap-c)# policy-map input-interface-2
スイッチ(config-pmap)# class voice-interface-2
スイッチ(config-pmap-c)# set qos-group 10
スイッチ(config-pmap-c)# class video-interface-2
スイッチ(config-pmap-c)# set qos-group 20
スイッチ(config-pmap-c)# exit
スイッチ(config-pmap)# exit

スイッチ(config)# class-map voice
スイッチ(config-cmap)# match qos-group 10
スイッチ(config-cmap)# exit

スイッチ(config)# class-map video
スイッチ(config-cmap)# match qos-group 20

スイッチ(config)# policy-map output-interface
スイッチ(config-pmap)# class voice
スイッチ(config-pmap-c)# police 256000 conform-action transmit exceed-action drop
スイッチ(config-pmap-c-police)# exit
スイッチ(config-pmap-c)# exit

スイッチ(config-pmap)# class video
スイッチ(config-pmap-c)# police 1024000 conform-action transmit exceed-action drop
スイッチ(config-pmap-c-police)# exit
スイッチ(config-pmap-c)# exit
```

例：音声、ビデオ、およびマルチキャスト トラフィックで分類されたワイヤレス QoS ポリシー

次の例では、音声とビデオのトラフィックの Quality of Service を管理するポートの子ポリシーを作成するテンプレートを示します。

```
Policy-map port_child_policy
    Class voice (match dscp ef)
            Priority level 1
            Police  Multicast Policer
    Class video (match dscp af41)
            Priority level 2
            Police  Multicast Policer
    Class mcast-data  (match non-client-nrt)
            Bandwidth remaining ratio <>
    Class class-default  (NRT Data)
            Bandwidth remaining ratio <>
```

（注） 上記の例のマルチキャスト ポリサーはキーワードではありません。これは設定されたポリシング ポリシーを示しています。

名前の音声とビデオを使用する 2 つのクラス マップは、46 および 34 の DSCP の割り当てで設定されます。音声トラフィックにはプライオリティ 1 が割り当てられ、ビデオ トラフィックにはプライオリティ レベル 2 が割り当てられ、Q0 および Q1 を使用して処理されます。ネットワークがマルチキャスト音声およびビデオ トラフィックを受信すると、マルチキャストのポリサーを設定できます。非クライアント NRT データおよび NRT データは Q2 および Q3 キューで処理されます。

関連トピック

ポート ポリシー, （907 ページ）

ポート ポリシーの形式, （907 ページ）

ワイヤレス QoS マルチキャスト, （922 ページ）

例：ダウンストリーム SSID ポリシーの設定

ダウンストリーム BSSID ポリシーを設定するには、最初にプライオリティ レベルのキューイングでポートの子ポリシーを設定する必要があります。

ポリシーのタイプ。	例

ユーザ定義のポートの子ポリシー	`policy-map port_child_policy`
	`  class voice`
	`  priority level 1 20000`
	
	`  class video`
	`  priority level 2 10000`
	
	`  class non-client-nrt-class`
	`  bandwidth remaining ratio 10`
	
	`  class class-default`
	`  bandwidth remaining ratio 15`

出力 BSSID ポリシー	`policy-map bssid-policer`
	`  queue-buffer ratio 0`
	`  class class-default`
	`  shape average 30000000`
	`set dscp dscp table dscp2dscp`
	`set wlan user-priority dscp table dscp2up`
	`service-policy ssid_child_qos`

SSID の子 QoS ポリシー	`Policy Map ssid-child_qos`
	`  Class voice`
	`  priority level 1`
	`  police cir 5m`
	`  admit cac wmm-tspec`
	`  UP 6,7  / tells WCM allow 'voice'`
	`TSPEC\SIP snoop for this ssid`
	`  rate 4000 / must be police rate`
	`value is in kbps)`
	`  Class video`
	`  priority level 2`
	`  police cir 60000`

関連トピック

WLAN での SSID またはクライアント ポリシーの適用（CLI），（966 ページ）

SSID ポリシー，（910 ページ）

例：入力 SSID ポリシー

次に、入力 SSID の階層型ポリシーの例を示します。

入力 SSID ポリシーの種類	例

入力 SSID の階層型ポリシー	`policy-map ssid-child-policy`
	`class voice  //match dscp 46`
	`police 3m`
	`class video //match dscp 34`
	`police 4m`
	`policy-map ssid-in-policy`
	`class class-default`
	`set dscp wlan user-priority table up2dscp`
	`service-policy ssid-child-policy`

	`policy-map ssid_in_policy`
	`class dscp-40`
	`set cos 1`
	`police 10m`
	`class up-1`
	`set dscp 34`
	`police 12m`
	`class dscp-10`
	`set dscp 20`
	`police 15m`
	`class class-default`
	`set dscp wlan user-priority table up2dscp`
	
	`police 50m`

例：クライアント ポリシー

クライアントポリシーの種類	例/詳細

デフォルトの出力クライアント ポリシー	すべての着信トラフィックのユーザプライオリティは 0 です。
	（注） デフォルトのクライアントポリシーは、ACMイネーブルの WMM クライアント上でのみイネーブルにされます。
	show ap dot11 5ghz network コマンドを使用して、ACM がイネーブルにされているかどうかの確認が出来ます。ACM をイネーブルにするには、**ap dot11 5ghz cac voice acm** コマンドを使用します。
	`Policy-map client-def-down`
	`  class class-default`
	`  set wlan user-priority 0`

デフォルトの入力クライアント ポリシー	ワイヤレス ネットワークから有線ネットワークに送信されるトラフィックは、DSCP 値が 0 に設定されます。
	（注） デフォルトのクライアントポリシーは、ACMイネーブルの WMM クライアント上でのみイネーブルにされます。
	`Policy-map client-def-up`
	`  class class-default`
	`  set dscp 0`

クライアントポリシーの種類	例/詳細
設定されたQoSレベル属性を使用してクライアントがAAAのプロファイルに認証する際に、自動的に生成され、WMMクライアントに適用されるクライアントポリシー。	Policy Map platinum-WMM Class voice-plat set wlan user-priority 6 Class video-plat set wlan user-priority 4 Class class-default set wlan user-priority 0 Policy Map gold-WMM Class voice-gold set wlan user-priority 4 Class video-gold set wlan user-priority 4 Class class-default set wlan user-priority 0
非WMMクライアントの貴金属ポリシー	Policy Map platinum set wlan user-priority 6
トラフィックがクラスvoice1と一致し、ユーザプライオリティが事前定義の値に設定された出力クライアントポリシー。	クラスはDSCPまたはACLを割り当てるように設定できます。 Policy Map client1-down Class voice1 //match dscp, cos set wlan user-priority <> Class voice2 //match acl set wlan user-priority <> Class voice3 set wlan user-priority <> Class class-default set wlan user-priority 0

クライアントポリシーの種類	例/詳細
AAA および TCLAS に基づくクライアント ポリシー	Policy Map client2-down[AAA+ TCLAS pol example] Class voice\\match dscp police <> set <> Class class-default set <> Class voice1|| voice2 [match acls] police <> class voice1 set <> class voice2 set <>
出力方向のトラフィック用の音声とビデオのクライアント ポリシー	Policy Map client3-down class voice \\match dscp, cos police X class video police Y class class-default police Z
ポリシングを使用する入力方向のトラフィック用の音声とビデオのクライアントポリシー	Policy Map client1-up class voice \\match dscp, up, cos police X class video police Y class class-default police Z
DSCP に基づく音声とビデオのクライアントポリシー	Policy Map client2-up class voice \\match dscp, up, cos set dscp <> class video set dscp <> class class-default set dscp <>
マーキングおよびポリシングを使用したクライアント入力ポリシー	policy-map client_in_policy class dscp-48 //match dscp 48 set cos 3 police 2m class up-4 //match wlan user-priority 4 set dscp 10 police 3m class acl //match acl set cos 2 police 5m class class-default set dscp 20 police 15m
階層型クライアント入力ポリシー	

クライアントポリシーの種類	例/詳細
	policy-map client-child-policy class voice //match dscp 46 set dscp 40 police 5m class video //match dscp 34 set dscp 30 police 7m policy-map client-in-policy class class-default police 15m service-policy client-child-policy

関連トピック

クライアント ポリシーの設定（CLI）
クライアント ポリシー, （910 ページ）

例：平均レート シェーピングの設定

次の例は、平均レート シェーピングを設定する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# class-map prec1
スイッチ(config-cmap)# description matching precedence 1 packets
スイッチ(config-cmap)# match ip precedence 1
スイッチ(config-cmap)# end

スイッチ# configure terminal
スイッチ(config)# class-map prec2
スイッチ(config-cmap)# description matching precedence 2 packets
スイッチ(config-cmap)# match ip precedence 2
スイッチ(config-cmap)# exit

スイッチ(config)# policy-map shaper
スイッチ(config-pmap)# class prec1
スイッチ(config-pmap-c)# shape average 512000
スイッチ(config-pmap-c)# exit

スイッチ(config-pmap)# policy-map shaper
スイッチ(config-pmap)# class prec2
スイッチ(config-pmap-c)# shape average 512000
スイッチ(config-pmap-c)# exit

スイッチ(config-pmap)# class class-default
スイッチ(config-pmap-c)# shape average 1024000
```

クラスマップ、ポリシーマップ、シェーピング平均を設定したら、QoS のインターフェイスにポリシー マップを適用します。

関連トピック

シェーピングの設定（CLI），（1001 ページ）
平均レート シェーピング，（929 ページ）

例：キュー制限の設定

次の例は、DSCP 値および割合に基づいて、キュー制限ポリシーを設定する方法を示しています。

```
スイッチ# configure terminal
スイッチ#(config)# policy-map port-queue
スイッチ#(config-pmap)# class dscp-1-2-3
スイッチ#(config-pmap-c)# bandwidth percent 20
スイッチ#(config-pmap-c)# queue-limit dscp 1 percent 80
スイッチ#(config-pmap-c)# queue-limit dscp 2 percent 90
スイッチ#(config-pmap-c)# queue-limit dscp 3 percent 100
スイッチ#(config-pmap-c)# exit

スイッチ#(config-pmap)# class dscp-4-5-6
スイッチ#(config-pmap-c)# bandwidth percent 20
スイッチ#(config-pmap-c)# queue-limit dscp 4 percent 20
スイッチ#(config-pmap-c)# queue-limit dscp 5 percent 30
スイッチ#(config-pmap-c)# queue-limit dscp 6 percent 20
スイッチ#(config-pmap-c)# exit

スイッチ#(config-pmap)# class dscp-7-8-9
スイッチ#(config-pmap-c)# bandwidth percent 20
スイッチ#(config-pmap-c)# queue-limit dscp 7 percent 20
スイッチ#(config-pmap-c)# queue-limit dscp 8 percent 30
スイッチ#(config-pmap-c)# queue-limit dscp 9 percent 20
スイッチ#(config-pmap-c)# exit

スイッチ#(config-pmap)# class dscp-10-11-12
スイッチ#(config-pmap-c)# bandwidth percent 20
スイッチ#(config-pmap-c)# queue-limit dscp 10 percent 20
スイッチ#(config-pmap-c)# queue-limit dscp 11 percent 30
スイッチ#(config-pmap-c)# queue-limit dscp 12 percent 20
スイッチ#(config-pmap-c)# exit

スイッチ#(config-pmap)# class dscp-13-14-15
スイッチ#(config-pmap-c)# bandwidth percent 10
スイッチ#(config-pmap-c)# queue-limit dscp 13 percent 20
スイッチ#(config-pmap-c)# queue-limit dscp 14 percent 30
スイッチ#(config-pmap-c)# queue-limit dscp 15 percent 20
スイッチ#(config-pmap-c)# end
スイッチ#
```

上記のポリシー マップのキュー制限の設定が終了すると、QoS のインターフェイスにポリシー マップを適用することができます。

関連トピック

キュー制限の設定（CLI），（998 ページ）
重み付けテール ドロップ，（931 ページ）

例：キュー バッファの設定

次の例は、キュー バッファ ポリシーを設定して QoS のインターフェイスに適用する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# policy-map policy1001
スイッチ(config-pmap)# class class1001
スイッチ(config-pmap-c)# bandwidth remaining ratio 10
スイッチ(config-pmap-c)# queue-buffer ratio ?
  <0-100>  Queue-buffers ratio limit
スイッチ(config-pmap-c)# queue-buffer ratio 20
スイッチ(config-pmap-c)# end

スイッチ# configure terminal
スイッチ(config)# interface gigabitEthernet2/0/3
スイッチ(config-if)# service-policy output policy1001
スイッチ(config-if)# end
```

関連トピック

キュー バッファの設定（CLI），（995 ページ）

キュー バッファの割り当て，（934 ページ）

例：ポリシング アクションの設定

次の例は、ポリサーに関連付けることができるさまざまなポリシング アクションを示しています。これらのアクションは、パケット設定の適合、超過、または違反によって実現されます。トラフィック プロファイルを超過または違反したパケットをドロップ、マーク付け、または送信することができます。

たとえば、1 つの一般的な導入シナリオでは、エンタープライズ顧客ポリシー トラフィックがネットワークからサービス プロバイダーに送信され、DSCP 値が異なる、適合、超過、および違反パケットをマーキングします。サービス プロバイダーは、輻輳があると DSCP 値の超過および違反としてマーキングされたパケットをドロップすることができますが、使用可能な帯域幅がある場合は送信することも可能です。

（注） Layer 2 フィールドには CoS フィールドが含まれるようにマーキングでき、Layer 3 フィールドには precedence および DSCP フィールドが含まれるようにマーキングできます。

1 つの便利な機能として、複数のアクションとイベントを関連付ける機能があります。たとえば、すべての適合パケットについて、precedence ビットと CoS を設定できます。アクションを設定するサブモードは、ポリシング機能によって配信できます。

これは、ポリシング アクションの設定例を示しています。

```
スイッチ# configure terminal
```

```
スイッチ(config)# policy-map police
スイッチ(config-pmap)# class class-default
スイッチ(config-pmap-c)# police cir 1000000 pir 2000000
スイッチ(config-pmap-c-police)# conform-action transmit
スイッチ(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table
exceed-markdown-table
スイッチ(config-pmap-c-police)# violate-action set-dscp-transmit dscp table
violate-markdown-table
スイッチ(config-pmap-c-police)# end
```

この例では、exceed-markdown-table と violate-mark-down-table がテーブル マップです。

（注） ポリサー ベースのマークダウン アクションは、テーブル マップを使用する場合のみサポートされます。スイッチの各マーキング フィールドで許可されているマークダウン テーブル マップは 1 つだけです。

関連トピック

ポリシングの設定（CLI），（989 ページ）

ポリシング，（922 ページ）

例：ポリサーの VLAN 設定

次の例では、VLAN のポリサー設定を表示します。この設定の最後に、QoS のインターフェイスに VLAN ポリシー マップを適用します。

```
スイッチ# configure terminal
スイッチ(config)# class-map vlan100
スイッチ(config-cmap)# match vlan 100
スイッチ(config-cmap)# exit
スイッチ(config)# policy-map vlan100
スイッチ(config-pmap)# policy-map class vlan100
スイッチ(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
スイッチ(config-pmap-c-police)# end
スイッチ# configure terminal
スイッチ(config)# interface gigabitEthernet1/0/5
スイッチ(config-if)#  service-policy input vlan100
```

関連トピック

ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング（CLI），（972 ページ）

VLAN のポリシー マップ，（922 ページ）

例：ポリシングの単位

次の例は、QoS でサポートされるポリシングのさまざまな単位を示しています。ポリシングの単位はトークン バケットが動作する基盤です。

次の単位のポリシングがサポートされています。

- CIR および PIR はビット/秒で指定します。バースト パラメータはバイト単位で指定します。これはデフォルトのモードであり、単位が指定されていない場合に使用される単位です。CIR および PIR は、パーセントでも設定できます。その場合バースト パラメータをミリ秒単位で設定する必要があります。
- CIR および PIR はパケット/秒で指定します。この場合、バースト パラメータもパケットで設定されます。

次の例は、ビット/秒のポリサー設定を示しています。

```
スイッチ(config)# policy-map bps-policer
スイッチ(config-pmap)# class class-default
スイッチ(config-pmap-c) # police rate 256000 bps burst 1000 bytes
conform-action transmit exceed-action drop
```

次の例は、パケット/秒のポリサー設定を示しています。この設定では、測定単位がパケットであるデュアル レートの 3 カラー ポリサーが設定されます。バーストおよびピーク バーストはすべてパケットに指定されます。

```
スイッチ(config)# policy-map pps-policer
スイッチ(config-pmap)# class class-default
スイッチ(config-pmap-c)# police rate 5000 pps burst 100 packets
peak-rate 10000 pps peak-burst 200 packets conform-action transmit
exceed-action drop violate-action drop
```

関連トピック

ポリシングの設定（CLI），（989 ページ）
トークンバケット アルゴリズム，（923 ページ）

例：シングルレート 2 カラー ポリシング設定

次の例は、シングルレート 2 カラー ポリサーを設定する方法を示しています。

```
スイッチ(config)# class-map match-any prec1
スイッチ(config-cmap)# match ip precedence 1
スイッチ(config-cmap)# exit
スイッチ(config)# policy-map policer
スイッチ(config-pmap)# class prec1
スイッチ(config-pmap-c)# police cir 256000 conform-action transmit exceed-action drop
スイッチ(config-pmap-c-police)# exit
スイッチ(config-pmap-c)#
```

関連トピック

ポリシングの設定（CLI），（989 ページ）
シングルレート 2 カラー ポリシング，（927 ページ）

例：デュアルレート 3 カラー ポリシング設定

次の例は、デュアルレート 3 カラー ポリサーを設定する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# policy-Map dual-rate-3color-policer
スイッチ(config-pmap)# class class-default
スイッチ(config-pmap-c)# police cir 64000 bc 2000 pir 128000 be 2000
スイッチ(config-pmap-c-police)# conform-action transmit
スイッチ(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table
exceed-markdown-table
スイッチ(config-pmap-c-police)# violate-action set-dscp-transmit dscp table
violate-markdown-table
スイッチ(config-pmap-c-police)# exit
スイッチ(config-pmap-c)#
```

この例では、exceed-markdown-table と violate-mark-down-table がテーブル マップです。

（注） ポリサー ベースのマークダウン アクションは、テーブル マップを使用する場合のみサポートされます。スイッチの各マーキング フィールドで許可されているマークダウン テーブル マップは 1 つだけです。

関連トピック

ポリシングの設定（CLI），（989 ページ）

デュアルレート 3 カラー ポリシング，（928 ページ）

例：テーブル マップのマーキング設定

次のステップと例は、QoS 設定でテーブル マップ マーキングを使用する方法を示しています。

1 テーブル マップを定義します。

table-map コマンドを使用してテーブル マップを定義し、値のマッピングを示します。このテーブルでは、テーブルが使用されるポリシーまたはクラスを認識しません。テーブルマップのデフォルトのコマンドは、一致する「from」フィールドがない場合に、「to」フィールドにコピーされる値を示します。この例では、table-map1 というテーブルマップが作成されます。定義されたマッピングでは、値 0 が 1 に、2 が 3 に変換され、デフォルト値は 4 に設定されます。

```
スイッチ(config)# table-map table-map1
スイッチ(config-tablemap)# map from 0 to 1
スイッチ(config-tablemap)# map from 2 to 3
スイッチ(config-tablemap)# default 4
スイッチ(config-tablemap)# exit
```

2 テーブル マップが使用されるポリシー マップを定義します。

この例では、着信 CoS が table-map1 テーブルで指定されたマッピングに基づいて、DSCP にマッピングされます。この例では、着信パケットの DSCP が 0 である場合、パケット内の CoS は 1 に設定されます。テーブルマップ名が指定されていない場合、このコマンドではデフォルトの動作が実行され、値が「from」フィールド（この場合は DSCP）から「to」フィールド（この場合は CoS）にコピーされます。ただし、CoS が 3 ビット フィールドであっても DSCP は 6 ビット フィールドです。これは、DSCP 内の最初の 3 ビットに CoS がコピーされることを意味します。

```
スイッチ(config)# policy map policy1
スイッチ(config-pmap)# class class-default
スイッチ(config-pmap-c)# set cos dscp table table-map1
スイッチ(config-pmap-c)# exit
```

3 ポリシーをインターフェイスに関連付けます。

```
スイッチ(config)# interface GigabitEthernet1/0/1
スイッチ(config-if)# service-policy output policy1
スイッチ(config-if)# exit
```

関連トピック

テーブル マップの設定（CLI），（975 ページ）

テーブル マップのマーキング，（924 ページ）

例：CoS マーキングを保持するテーブル マップの設定

次の例は、テーブル マップを使用して、QoS 設定のインターフェイスで CoS マーキングを保持する方法を示しています。

（例で設定されている）cos-trust-policy ポリシーは入力方向でイネーブルになり、インターフェイスに着信する CoS マーキングが保持されます。ポリシーがイネーブルになっていない場合は、デフォルトで DSCP だけが信頼されます。純粋なレイヤ 2 パケットがインターフェイスに着信すると、CoS の入力ポートに一致するポリシーがない場合は、CoS 値が 0 に書き換えられます。

```
スイッチ# configure terminal
スイッチ(config)# table-map cos2cos
スイッチ(config-tablemap)# default copy
スイッチ(config-tablemap)# exit


スイッチ(config)# policy map cos-trust-policy
スイッチ(config-pmap)# class class-default
スイッチ(config-pmap-c)# set cos cos table cos2cos
スイッチ(config-pmap-c)# exit

スイッチ(config)# interface GigabitEthernet1/0/2
スイッチ(config-if)# service-policy input cos-trust-policy
スイッチ(config-if)# exit
```

関連トピック

有線およびワイヤレス ポートの信頼動作, （935 ページ）

次の作業

QoS 設定でこれらの自動機能を使用できるかどうかについては、自動 QoS のマニュアルを参照してください。

QoS に関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*IP Multicast Routing Command Reference (Catalyst 3650 Switches)* *Cisco IOS Quality of Service Solutions Command Reference*
コール アドミッション制御（CAC）	*System Management Configuration Guide (Catalyst 3650 Switches)* *System Management Command Reference (Catalyst 3650 Switches)*
マルチキャスト シェーピングおよびポリシング レート	*IP Multicast Routing Configuration Guide (Catalyst 3650 Switches)*
アプリケーションの可視性およびコントロール	*System Management Configuration Guide (Catalyst 3650 Switches)* *System Management Command Reference (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
—	

MIB

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

シスコのテクニカル サポート

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

QoS の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

リリース	変更内容
Cisco IOS XE 3.6E	アップストリーム SSID のマーキングおよびポリシングアクションとクライアントのポリシーは、アクセス ポイントで適用されます。
Cisco IOS XE 3.6E	ワイヤレス ターゲット用に **show policy-map** コマンドで使用可能な新しい分類カウンタ。

第 X 部

無線リソース管理

- 無線リソース管理の設定，1031 ページ
- 設定の最適化されたローミング，1071 ページ
- 設定の Rx SOP，1075 ページ

第 50 章

無線リソース管理の設定

- 機能情報の確認，1031 ページ
- 無線リソース管理の設定の前提条件，1031 ページ
- 無線リソース管理の制約事項，1032 ページ
- 無線リソース管理について，1032 ページ
- RRM の設定方法，1041 ページ
- RRM パラメータと RF グループ ステータスの監視，1065 ページ
- 例：RF グループの設定，1067 ページ
- ED-RRM に関する情報，1068 ページ
- 無線リソース管理に関するその他の参考ドキュメント，1069 ページ
- 無線リソース管理の設定を行うための機能履歴と情報，1070 ページ

機能情報の確認

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

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

無線リソース管理の設定の前提条件

無線リソース管理を設定するには、スイッチをモビリティ アンカーではなくモビリティ コントローラとして設定する必要があります。また、ホーム AP で動的なチャネル割り当て機能のサポートが必要な場合があります。

RRM を機能させるには、モビリティ コントローラとモビリティ エージェントを含む新しいモビリティ アーキテクチャをスイッチまたはコントローラで設定する必要があります。

（注） モビリティ コントローラとモビリティ エージェントの設定については、『Mobility Configuration Guide』を参照してください。

無線リソース管理の制約事項

AP の最大数をすでに保持している RF グループに AP が join しようとすると、デバイスはアプリケーションを拒否し、エラーをスローします。

Apの通信時間公平性モードを有効にするには、ポリシー識別モードを無効にしてから再度適用する必要があります。これは、すべての AP に対し通信時間の公平性の設定を変更します。また ap 名前 <ap-name> dot11 24ghz 通信時間公平性モード識別ポリシーコマンド使用で、個々の AP の通信時間の公平性のモードを変更できます。

無線リソース管理について

無線リソース管理（RRM）ソフトウェアはスイッチに組み込まれており、ワイヤレス ネットワークのリアルタイムでの RF 管理を常時提供する組み込みの RF エンジニアとして機能します。RRM を使用すると、スイッチは次の情報について、アソシエートされている Lightweight アクセス ポイントを継続的に監視できます。

- トラフィックの負荷：トラフィックの送受信に使用される帯域幅の合計量。これにより、無線 LAN 管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越して計画を立てることができます。
- 干渉：他の 802.11 発信元から送られてくるトラフィック量。
- ノイズ：現在割り当てられているチャネルに干渉している 802.11 以外のトラフィック量。
- カバレッジ：接続されているすべてのクライアントの受信信号強度インジケータ（RSSI）と信号対雑音比（SNR）。
- その他：近くにあるアクセス ポイントの数。

RRM は次の機能を実行します。

- 無線リソースの監視
- 送信電力の制御
- チャネルの動的割り当て
- カバレッジ ホールの検出と修正
- RF グループ化

（注） RRM のグループ化は、AP が DCA チャネルのリストにないスタティック チャネルで動作するため、実行されません。NDP は、DCA チャネルでのみ送信され、無線が非 DCA チャネルで動作する場合、NDA はオンチャネルで受信しません。

無線リソースの監視

RRM は、ネットワークに追加された新しいスイッチや Lightweight アクセス ポイントを自動的に検出して設定します。その後、アソシエートされている近くの Lightweight アクセス ポイントを自動的に調整して、カバレッジとキャパシティを最適化します。

Lightweight アクセス ポイントでは、使用国で有効なすべての チャネルをスキャンできます。また、他の地域で使用可能なチャネルも同様です。ローカルモードのアクセスポイントは、これらのチャネルのノイズと干渉を監視するために、最大で 60 ミリ秒の間「オフチャネル」になります。不正アクセスポイント、不正クライアント、アドホック クライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。

（注） 音声トラフィックやその他の重要なトラフィックがある場合（過去100ミリ秒内）、アクセスポイントはオフチャネル測定を延期できます。また、WLAN スキャンの延期プライオリティ設定に基づいて、延期されます。

各アクセス ポイントがオフチャネルになるのはすべての時間のわずか 0.2% です。この動作はすべてのアクセスポイントに分散されるので、隣接するアクセスポイントが同時にスキャンを実行して、無線 LAN のパフォーマンスに悪影響を及ぼすことはありません。

RRM では、モビリティ コントローラ（MC）およびモビリティ エージェント（MA）を含む RF グループ化の新しいモビリティ アーキテクチャがサポートされます。

- モビリティ コントローラ（MC）：Cisco WLC 5700 シリーズ コントローラ、Cisco Catalyst 3850 スイッチ、Cisco Unified Wireless Network ソリューションのコントローラは MC として機能できます。MC には、その中で内部的に実行されている MC 機能および MA 機能があります。
- モビリティ エージェント（MA）：モビリティ エージェントは、モバイル クライアント用のクライアント モビリティ ステート マシンを維持するコンポーネントです。

RF グループについて

RF グループは、無線単位でネットワークの計算を実行するために、グローバルに最適化された方法で RRM の実行を調整する Cisco WLC の論理的な集合です。802.11 ネットワーク タイプごとに RF グループが存在します。単一の RF グループに Cisco WLC をクラスタリングすることによって、RRM アルゴリズムは単一の Cisco WLC の機能を拡張できます。

RF グループは、次のパラメータに基づいて作成されます。

- ユーザ設定の RF ネットワーク名。
- 無線レベルで実行されるネイバー探索。
- MC に設定されている国のリスト。

MC 間で実行する RF グループ化。

Lightweight アクセス ポイントは、定期的にネイバー メッセージを無線で送信します。同じ RF グループ名を使用しているアクセス ポイントは、相互に送信されたメッセージを検証します。

検証されたネイバー メッセージを、異なるコントローラ上のアクセス ポイントが -80 dBm 以上の信号強度で受信すると、Cisco WLC によって自動モードの RF 領域が動的に形成されます。静的モードで、リーダーは手動で選択され、メンバが RF グループに追加されます。RF グループ モードに関する詳細については、「RF グループ リーダー」の項を参照してください。

（注） RF グループとモビリティ グループは、どちらも Cisco WLC のクラスタを定義するという点では同じですが、用途に関しては異なります。RF グループはスケーラブルでシステム全体にわたる動的な RF 管理を実現するのに対して、モビリティ グループはスケーラブルでシステム全体にわたるモビリティと Cisco WLC の冗長性を実現します。

RF グループ リーダー

7.0.116.0 のリリースから、RF グループ リーダーを次の 2 つの方法で設定することができます。

- 自動モード：このモードでは、RF グループのメンバによって、グループの「マスター」電力およびチャネル スキームを管理する RF グループ リーダーが選ばれます。RF グループ アルゴリズムは、RF グループ リーダーを動的に選択し、RF グループ リーダーが常に存在していることを確認します。グループ リーダーの割り当ては変更されることがあります（たとえば、現在の RF グループ リーダーが動作しなくなった場合、または RF グループ メンバが大幅に変更された場合）。
- 静的モード：このモードでは、ユーザは RF グループ リーダーとして Cisco WLC を手動で選択します。このモードでは、リーダーおよびメンバは手動で設定され、固定されます。メンバが RF グループに join できない場合は、理由が表示されます。リーダーは、メンバが前の試行で join しなかった場合、1 分ごとにメンバとの接続を確立しようとします。

RF グループ リーダーは、システムによって収集されたリアルタイムの無線データを分析して、パワーおよびチャネルの割り当てを算出し、RF グループの各 Cisco WLC に送信します。RRM アルゴリズムによって、システム全体の安定性が保証され、チャネルおよびパワー スキームの変更を適切なローカル RF 領域に制限します。

6.0 より前の Cisco WLC ソフトウェア リリースでは、動的チャネル割り当て（DCA）の検索アルゴリズムによって、RF グループの Cisco WLC にアソシエートされた無線について適切なチャネル計画を判別しますが、現在の計画よりも大幅に優れていない限り、新しいチャネル計画は適用されません。両方の計画で最も不適切な無線のチャネル メトリックにより、適用する計画が決定

されます。新しいチャネル計画を適用するための唯一の基準として最もパフォーマンスの低い無線を使用すると、ピンニングまたはカスケードの問題が発生する可能性があります。

ピンニングは、アルゴリズムによって RF グループの一部の無線に適したチャネル計画が検出されても、ネットワーク内の最も条件の悪い無線には適したチャネル オプションがないため、チャネル計画の変更は実施されないことを指します。RF グループ内の最も条件の悪い無線によって、グループ内の他の無線がより適切なチャネル計画を探すことができなくなる場合があります。ネットワークの規模が大きければ大きいほど、よりピンニングになりやすいです。

1 つの無線のチャネルが変更された場合に、RF 領域の残りの無線を最適化するため、連続してチャネル変更が行われると、カスケードが発生します。このような無線を最適化すると、ネイバーおよびネイバーのチャネル計画が次善のものになり、チャネル最適化が起動されます。この影響は、すべてのアクセス ポイント無線が同じ RF グループに属している場合、複数のフロアまたは複数の建物に広がることがあります。この変更は、大きなクライアントの混乱を引き起こし、ネットワークを不安定にします。

ピンニングとカスケードの主な原因は、新しいチャネル計画を検索する方法と、起こる可能性のあるチャネル計画の変更が単一の無線の RF 状態によって制御されていることです。Cisco WLC ソフトウェア リリース 6.0 の DCA アルゴリズムは、ピンニングとカスケードを回避するよう再設計されました。次の変更が実装されました。

- 複数のローカル検索：DCA 検索アルゴリズムでは、単一の無線による単一のグローバル検索ではなく、同じ DCA の処理内で異なる無線によって開始される複数のローカル検索が実行されます。この変更によって、ピンニングとカスケードの両方に対応できるだけでなく、安定性を損なうことなく、DCA に必要な柔軟性と適合性が維持されます。
- 複数のチャネル計画変更イニシエータ（CPCI）：以前は、最も条件の悪い単一の無線が、チャネル計画変更の唯一のイニシエータでした。しかし、RF グループ内の各無線が評価されて、イニシエータ候補として優先順位付けされるようになりました。生成されたリストはインテリジェントにランダム化されるので、最終的にすべての無線が評価され、ピンニングが発生する可能性はなくなります。
- チャネル計画変更の適用制限（ローカリゼーション）：各 CPCI 無線の場合、DCA アルゴリズムは適切なチャネル計画を求めてローカル検索を実行しますが、実際には CPCI 無線自身および 1 ホップ近隣のアクセス ポイントのみが現在の送信チャネルを変更できます。アクセス ポイントによるチャネル計画変更のトリガーの影響は、そのアクセス ポイントの 2 RF ホップ内だけで認識され、実際のチャネル計画変更は 1 ホップ RF 領域内に制限されます。この制限はすべての CPCI 無線にわたって適用されるため、カスケードが発生する可能性はありません。
- 非 RSSI ベースの累積コスト メトリック：累積コスト メトリックによって、全範囲、領域、またはネットワークが指定のチャネル計画でどの程度のパフォーマンスを示すのかを測定します。チャネル計画の品質全体を把握する目的で、その領域内にあるすべてのアクセス ポイントに関する個々のコスト メトリックが考慮されます。これらのメトリックを使用することで、すべてのチャネル計画変更に単一の各無線の品質の向上または低下が含まれるようになります。その目的は、単一の無線の品質は向上するが、他の複数の無線のパフォーマンスが大幅に低下するような、チャネル計画変更を避けることです。

RRM アルゴリズムは、指定された更新間隔（デフォルトでは 600 秒）で実行されます。更新間隔の合間に、RF グループ リーダーは各 RF グループ メンバにキープアライブ メッセージを送信し、リアルタイムの RF データを収集します。

（注） 複数の監視間隔を使用することもできます。詳細については、「RRM の設定」の項を参照してください。

RF Group Name

Cisco WLC には RF グループ名が設定されます。この RF グループ名は、その Cisco WLC に join しているすべてのアクセス ポイントに送信され、アクセス ポイントでは、この名前がハッシュ MIC をネイバー メッセージで生成するための共有秘密として使用されます。RF グループを作成するには、グループに含めるすべての Cisco WLC に同じ RF グループ名を設定します。

Cisco WLC に join しているアクセス ポイントが別の Cisco WLC 上のアクセス ポイントから RF 伝送を受け取る可能性がある場合は、それらの Cisco WLC に同じ RF グループ名を設定する必要があります。アクセス ポイント間の RF 伝送を受信する可能性がある場合、802.11 干渉およびコンテンションをできるだけ回避するには、システム全体にわたる RRM が推奨されます。

モビリティ コントローラ

MC には、グループ リーダーまたはグループ メンバを指定できます。RF グループ化と他の MC とのグループ選出に基づいて、MC の 1 つは RF グループ リーダーとして動作することができます。RF リーダーを選出する優先順位は、コントローラまたはスイッチがサポートできる AP の最大数に基づきます。優先順位が最も高いのは 1 で、最も低いのは 5 です。

1. WiSM 2 コントローラ
2. Cisco WLC 5700 シリーズ コントローラ
3. WiSM 1 コントローラ
4. Catalyst 3850 シリーズ スイッチ
5. Catalyst 3650 シリーズ スイッチ

MC の 1 つが RRM グループ リーダーになる場合、残りの MC は RRM グループ メンバになります。RRM グループ メンバは、グループ リーダーに RF 情報を送信します。グループ リーダーはネットワークのチャネルおよび送信電力の計画を決定し、RF グループ メンバへ情報を戻します。MC は、MA に属する無線の電力計画を MA へ配信します。これらのチャネルおよび電力の計画は、最終的に個々の無線にまで配信されます。

（注） MC 内には MA の機能があります。

Mobility Agent

MA は、MC と通信します。MA と通信している場合は、MC にはスイッチ/コントローラの MAC または IP アドレスが含まれます。

MA は、MC によってポーリングされると、次の情報を提供します。

- 干渉またはノイズのデータ
- ネイバー データ
- 無線機能（サポートされているチャネル、電力レベル）
- 無線設定（電源、チャネル、チャネル幅）
- レーダー データ

MCは、スイッチ/コントローラ（MA）と次の情報を交換します。メッセージには次の内容が含まれます。

- 個々の無線の設定（チャネル、電源、チャネル幅）
- 個々の無線の現在の設定と RF 測定のポーリング要求
- グループ リーダーの更新

一方、MA は次のメッセージを MC に伝達します。

- 無線からの RF 測定（ロード、ノイズ、ネイバー情報など）
- 個々の無線の RF 機能と設定

MCから指示された場合、MAは無線のチャンネル、電源、チャネル幅を設定します。DFS、カバレッジ ホールの検出/緩和、静的なチャネル/電源の設定は、MA によって実行されます。

RF グループ内の不正アクセス ポイント検出について

Cisco WLC の RF グループを作成したら、不正アクセス ポイントを検出するように、Cisco WLC に接続されたアクセスポイントを設定する必要があります。アクセスポイントによって、近隣のアクセス ポイントのメッセージ内のビーコン/プローブ応答フレームが選択され、RF グループの認証情報要素（IE）と一致するものが含まれているかどうかが確認されます。選択が正常に終了すると、フレームは認証されます。正常に終了しなかった場合は、認証されているアクセス ポイントによって、近隣のアクセス ポイントが不正アクセス ポイントとして報告され、その BSSID が不正テーブルに記録されます。さらに、このテーブルは Cisco WLC に送信されます。

送信電力の制御

スイッチは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。

送信電力制御（TPC）アルゴリズムによって、RF環境での変化に応じて、アクセスポイントの電力が増減します。多くの場合、TPCは干渉を低減させるため、アクセスポイントの電力を下げようとします。しかし、アクセスポイントで障害が発生したり、アクセスポイントが無効になったりして、RFカバレッジに急激な変化があると、TPCは周囲のアクセスポイントで電力を上げることもあります。この機能は、主にクライアントと関係があるカバレッジホールの検出とは異なります。TPCはアクセスポイント間におけるチャネルの干渉を最小限に抑えながら、必要なカバレッジレベルを達成するため、十分なRF電力を提供します。

最小/最大送信電力の設定による TPC アルゴリズムの無効化

TPCアルゴリズムは、数多くのさまざまなRF環境でRF電力を分散させます。ただし、自動パワー制御では、アーキテクチャの制約事項またはサイトの制約事項のため、適切なRF設計を実装できなかった一部のケースは解消できない可能性があります。たとえば、すべてのアクセスポイントを互いに近づけて中央の廊下に設置する必要があるが、建物の端までカバレッジが必要とされる場合などです。

このようなケースでは、最大および最小の送信電力制限を設定し、TPCの推奨を無効化することができます。最大および最小のTPC電力設定は、RFネットワークのRFプロファイルを通じてすべてのアクセスポイントに適用されます。

[Maximum Power Level Assignment] および [Minimum Power Level Assignment] を設定するには、[Tx Power Control] ページのテキストボックスにRRMが使用する最大および最小の送信電力を入力します。これらのパラメータの範囲は-10～30 dBmです。最小値を最大値よりも大きくしたり、最大値を最小値よりも小さくしたりすることはできません。

最大送信電力を設定すると、RRMでは、スイッチに接続されているすべてのアクセスポイントはこの送信電力レベルを上回ることはできません（電力がRRM TPCまたはカバレッジホールの検出のどちらで設定されるかは関係ありません）。たとえば、最大送信電力を11 dBmに設定すると、アクセスポイントを手動で設定しない限りは、11 dBmを上回って伝送を行うアクセスポイントはありません。

チャネルの動的割り当て

同じチャネル上の2つの隣接するアクセスポイントによって、信号のコンテンションや信号の衝突が発生することがあります。衝突の場合、アクセスポイントではデータが受信されません。この動作は問題になることがあります。たとえば、誰かがカフェで電子メールを読むことで、近隣の会社のアクセスポイントのパフォーマンスに影響が及ぶような場合です。これらがまったく別のネットワークであっても、チャネル1を使用してカフェにトラフィックが送信されることによって、同じチャネルを使用している会社の通信が妨害される可能性があります。スイッチはアクセスポイントチャネル割り当てを動的に割り当てて、衝突を回避し、キャパシティとパフォーマンスを改善することができます。チャネルは「再利用」され、希少なRFリソースが浪費されるのを防ぐことができます。つまり、チャネル1はカフェから離れた別のアクセスポイントに割り当てられます。これは、チャネル1をまったく使用しない場合に比べてより効率的です。

スイッチの動的チャネル割り当て（DCA）機能は、アクセスポイント間における隣接するチャネルの干渉を最小限に抑える上でも役立ちます。たとえば、チャネル1とチャネル2など、802.11b/g

帯域でオーバーラップする 2 つのチャネルは、同時に 11/54 Mbps を使用できません。スイッチは、チャネルを効果的に再割り当てすることによって、隣接するチャネルを分離します。

（注） 重複しないチャネル（1、6、11、など）だけの使用を推奨します。

スイッチは、さまざまなリアルタイムの RF 特性を検証して、次のようにチャネルの割り当てを効率的に処理します。

- アクセス ポイントの受信エネルギー：各アクセス ポイントとその近隣のアクセス ポイント間で測定された受信信号強度。チャネルを最適化して、ネットワーク キャパシティを最大にします。
- ノイズ：ノイズによって、クライアントおよびアクセスポイントの信号の品質が制限されます。ノイズが増加すると、有効なセル サイズが小さくなり、ユーザ エクスペリエンスが低下します。スイッチでは、ノイズ源を避けるようにチャネルを最適化することで、システム キャパシティを維持しながらカバレッジを最適化できます。過剰なノイズのためにチャネルが使用できない場合は、そのチャネルを回避できます。
- 802.11 干渉：干渉とは、不正アクセス ポイントや近隣の無線ネットワークなど、無線 LAN に含まれない 802.11 トラフィックのことです。Lightweight アクセス ポイントは、常にすべてのチャネルをスキャンして干渉の原因を調べます。802.11 干渉の量が定義済みの設定可能なしきい値（デフォルトは 10 %）を超えると、アクセス ポイントからスイッチにアラートが送信されます。その場合、スイッチでは、RRM アルゴリズムを使用してチャネルの割り当てを動的に調整することで、干渉がある状況でシステムパフォーマンスを向上させることができます。このような調整によって、隣接する Lightweight アクセス ポイントが同じチャネルに割り当てられることがありますが、この設定は、干渉している外部アクセスポイントが原因で使用できないチャネルにアクセスポイントを割り当てたままにしておくよりも効果的です。

  また、他のワイヤレス ネットワークがある場合、スイッチは、他のネットワークを補足するようにチャネルの使用を変更します。たとえば、チャネル 6 に 1 つのネットワークがある場合、隣接する無線 LAN はチャネル 1 または 11 に割り当てられます。この調整によって、周波数の共有が制限され、ネットワークのキャパシティが増加します。チャネルにキャパシティがほとんど残っていない場合、スイッチはそのチャネルを回避できます。すべての非オーバーラップ チャネルが使用される非常に高密度の展開では、スイッチでも最適な処理が行われますが、期待値を設定する際に RF 密度を考慮する必要があります。
- 負荷および利用率：利用率の監視が有効な場合、（たとえば、ロビーとエンジニアリング エリアを比較して）一部のアクセスポイントが他のアクセスポイントよりも多量のトラフィックを伝送するように展開されていることを、キャパシティの計算で考慮できます。これにより、スイッチは、最も低いパフォーマンスが報告されているアクセスポイントを改善するようにチャネルを割り当てることができます。チャネル構造を変更する際には、負荷を考慮して、現在ワイヤレス LAN に存在するクライアントへの影響を最小限に抑えるようにします。このメトリックによって、すべてのアクセスポイントの送信パケットおよび受信パケットの数が追跡されて、アクセスポイントのビジー状態が測定されます。新しいクライアントは過負荷のアクセス ポイントを回避し、別のアクセス ポイントにアソシエートします。このパラメータはデフォルトではディセーブルになっています。

スイッチは、この RF 特性情報を RRM アルゴリズムとともに使用して、システム全体にわたる判断を行います。相反する要求の解決にあたっては、軟判定メトリックを使用して、ネットワーク干渉を最小限に抑えるための最善の方法が選択されます。最終的には、3 次元空間における最適なチャネル設定が実現します。この場合、上下のフロアにあるアクセス ポイントが全体的な無線 LAN 設定において主要な役割を果たします。

（注） 2.4GHz 帯域の 40 MHz チャネル、または 80 MHz チャネルを使用する無線は、DCA ではサポートされていません。

RRM スタートアップ モードは、次のような状況で起動されます

- シングルスイッチ環境では、RRM スタートアップ モードは、スイッチがアップグレードされてリブートしてから起動されます。
- マルチスイッチ環境では、RRM スタートアップ モードは、RF グループ リーダーが選定されてから起動されます。

CLI から RRM スタートアップ モードを開始できます。

RRM スタートアップ モードは、100 分間（10 分間隔で 10 回繰り返し）実行されます。RRM スタートアップ モードの持続時間は、DCA 間隔、感度、およびネットワーク サイズとは関係ありません。スタートアップ モードには、定常ステート チャネル計画に収束するために 10 回の高感度な（チャネルを容易に環境に対して敏感に変更する）DCA 実行が含まれます。スタートアップ モードが終了した後、DCA は指定した間隔と感度で実行を継続します。

（注） DCA アルゴリズムの間隔が 1 時間に設定されても、DCA アルゴリズムは常にデフォルトの 10 分間隔で実行されます。チャネルの割り当ては、最初の 10 サイクルでは 10 分間隔ごとに実行され、チャネルは DCA アルゴリズムによって 10 分ごとに変更されます。その後は、設定された時間間隔に戻ります。これは DCA 間隔とアンカー時間の両方に共通です。定常状態に従うためです。

（注） DCA/TPC が RF グループ メンバでオフになり、RF グループ リーダーが自動に設定されると、メンバのチャネル/送信電力は RF グループ リーダーで実行されるアルゴリズムによって変更されます。

カバレッジ ホールの検出と修正

RRM カバレッジ ホール検出アルゴリズムは、堅牢な無線パフォーマンスに必要なレベルに達しない無線 LAN の無線カバレッジの領域を検出することができます。この機能によって、Lightweight アクセス ポイントを追加（または再配置）する必要があるというアラートが生成されます。

RRM 設定で指定されたレベルを下回るしきい値レベル（RSSI、失敗したクライアントの数、失敗したパケットの割合、および失敗したパケットの数）で Lightweight アクセス ポイント上のクライ

アントが検出されると、アクセスポイントからスイッチに「カバレッジホール」アラートが送信されます。このアラートは、ローミング先の有効なアクセス ポイントがないまま、クライアントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。スイッチでは、修正可能なカバレッジ ホールと不可能なカバレッジ ホールが識別されます。修正可能なカバレッジ ホールの場合、スイッチでは、その特定のアクセス ポイントの送信電力レベルを上げることによってカバレッジ ホールが解消されます。送信電力を増加させることが不可能なクライアントや、電力レベルが静的に設定されているクライアントによって生じたカバレッジ ホールがスイッチによって解消されることはありません。ダウンストリームの送信電力を増加させても、ネットワーク内の干渉を増加させる可能性があるからです。

RRM の設定方法

高度な RRM CCX パラメータの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm ccx location-measurement** *interval*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm ccx location-measurement** *interval* 例： スイッチ(config)# **ap dot11 24ghz rrm ccx location-measurement 15**	802.11 CXX クライアントのロケーション測定の間隔を設定します。範囲は 10 ～ 32400 秒です。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ネイバー探索タイプの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm ndp-type** {**protected | transparent**}
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm ndp-type** {**protected | transparent**} 例： スイッチ(config)#**ap dot11 24ghz rrm ndp-type protected** スイッチ(config)#**ap dot11 24ghz rrm ndp-type transparent**	ネイバー探索タイプを設定します。デフォルトでは、モードは「transparent」に設定されます。 • [protected]：セキュアな通信にネイバー探索タイプを「protected」に設定します。 パケットが暗号化されます。 • [transparent]：ネイバー探索タイプを「transparent」に設定します。 パケットはそのまま送信されます。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RRM プロファイルしきい値、監視チャネル、および監視間隔の設定（GUI）

ステップ 1 [Configuration] > [Wireless] > [802.11a/n/ac] > [RRM] > [General] または [Configuration] > [Wireless] > [802.11b/g/n] > [RRM] > [General] を選択して、RRM の [General] ページを開きます。

ステップ 2 次のように、アラームに使用されるプロファイルしきい値を設定します。

（注） プロファイルしきい値は、RRM アルゴリズムの機能には関係ありません。これらのしきい値パラメータに設定された各 AP の値を超えると、スイッチは、Cisco Prime Infrastructure または他のトラップ レシーバに SNMP トラップ（またはアラート）を送信します。

a) [Interference] テキスト ボックスに、1 つのアクセス ポイントにおける干渉（ワイヤレス ネットワーク外の発信元からの 802.11 トラフィック）の割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 10% です。

b) [Clients] テキスト ボックスに、1 つのアクセス ポイントにおけるクライアントの数を入力します。有効な範囲は 1 ～ 75 で、デフォルト値は 12 です。

c) [Noise] テキスト ボックスに、1 つのアクセス ポイントにおけるノイズ（802.11 以外のトラフィック）のレベルを入力します。有効な値の範囲は –127 ～ 0 dBm で、デフォルト値は –70 dBm です。

d) [Utilization] テキスト ボックスに、1 つのアクセス ポイントで使用されている RF 帯域幅の割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 80% です。

e) [Throughput] テキスト ボックスに、1 つのアクセス ポイントで使用されるスループット レベルを入力します。有効な範囲は 1000 ～ 10000000 で、デフォルト値は 1000000 です。

ステップ 3 [Channel List] ドロップダウン リストから次のオプションのいずれかを選択して、アクセス ポイントで RRM によるスキャンに使用されるチャネルのセットを指定します。

- [All Channels]：選択した無線でサポートされているすべてのチャネルで、RRM によるチャネル スキャンが実行されます。使用国で有効でないチャネルも対象となります。
- [Country Channels]：使用国内の D チャネルのみで、RRM によるチャネル スキャンが実行されます。これはデフォルト値です。
- [DCA Channels]：DCA アルゴリズムによって使用されるチャネル セットのみで、RRM によるチャネル スキャンが実行されます。デフォルトでは、使用国で有効な、オーバーラップしないすべてのチャネルが対象となります。ただし、必要に応じて、DCA で使用するチャネル セットを指定できます。これを行うには、「チャネルの動的割り当て」の手順に従ってください。

ステップ 4 次のように、監視間隔を設定します。

1. [Channel Scan Interval] テキスト ボックスに、無線帯域内の各チャネルでスキャンを実行する時間間隔の合計（秒）を入力します。スキャンプロセス全体の所要時間はチャネル、無線ごとに 50 ミリ秒であり、ここで設定された間隔で実行されます。各チャネルをリッスンするための所要時間は、50 ミリ秒のスキャン時間（設定不可）とスキャン対象チャネル数によって決まります。たとえば、米国の場合、すべての 11 802.11b/g チャネルは、デフォルトの 180 秒の間隔で 50 ミリ秒間スキャンされます。したがって、各スキャン チャネルで 16 秒ごとに 50 ミリ秒がリッスンに費やされます（180/11＝約 16 秒）。Channel Scan Interval パラメータで、スキャンを実行する間隔を指定します。有効な範囲は 60 ～ 3600 秒で、 802.11a/n/ac および 802.11b/g/n 無線のデフォルト値は 180 秒です。
2. [Neighbor Packet Frequency] テキスト ボックスに、ネイバー パケット（メッセージ）が送信される間隔を秒単位で入力します。ネイバー パケットによって最終的にネイバー リストが構築されます。有効な範囲は 60 ～ 3,600 秒です。デフォルト値は 60 秒です。

   （注） アクセス ポイント無線が 60 分以内に既存のネイバーからネイバー パケットを受信しない場合、Cisco WLC によってネイバー リストからそのネイバーが削除されます。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

（注） Cisco WLC の RRM パラメータをすべて工場出荷時のデフォルト値に戻す場合は、[Set to Factory Default] をクリックします。

RF グループの設定

この項では、GUI または CLI によって RF グループを設定する方法について説明します。

（注） 通常、RF グループ名は展開時にスタートアップ ウィザードを使用して設定されます。ただし、必要に応じて変更できます。

（注） 複数の国番号機能を使用している場合、同じ RF グループに join する予定のすべての Cisco WLC は、同じ国を同じ順序で設定する必要があります。

（注） Cisco Prime インフラストラクチャを使用して RF グループを設定することもできます。

（注） Auto モードでは、RF グループ リーダーは RF グループの安定化のためグループ化サイクルの最初の 3 つの実行において TP および DCA をスキップします。

RF グループ モードの設定（GUI）

ステップ 1 [Configuration] > [Wireless] > [802.11a/n/ac] > [RRM] > [RF Grouping] または [Configuration] > [Wireless] > [802.11b/g/n] > [RRM] > [RF Grouping] を選択して、[RF Grouping] ページを開きます。

ステップ 2 [Group Mode] ドロップダウン リストで、この Cisco WLC に設定するモードを選択します。
次のモードで RF グループ化を設定できます。

- [auto]：RF グループ選択を自動更新モードに設定します。

  （注） 設定したスタティック リーダーは、モードが [auto] に設定されるまで、他の Cisco RF のメンバになることはできません。

- [leader]：RF グループ選択を静的モードに設定し、この Cisco WLC をグループ リーダーとして設定します。

- [off]：RF グループ選択をオフに設定します。すべての Cisco WLC が自身のアクセス ポイント パラメータを最適化します。

  （注） 優先順位が高い Cisco WLC が使用可能な場合、優先順位がより低い Cisco WLC はグループ リーダーのロールを担うことはできません。ここでの優先順位は、Cisco WLC の処理能力に関連しています。

（注） Cisco WLC が自動 RF グループ化に加わるように設定することをお勧めします。RRM の設定を無効にする際には、自動 RF グループ化への参加を無効にする必要はありません。

ステップ 3 [Apply] をクリックして設定を保存し、[Restart] をクリックして RRM RF グループ化アルゴリズムを再起動します。

ステップ 4 この Cisco WLC に対して、スタティック リーダーとして RF グループ化モードを設定した場合、次のように [Group Members] セクションからグループ メンバを追加することができます。

1. スイッチの [Name] テキスト ボックスに、このグループにメンバとして追加する Cisco WLC を入力します。
2. [IP Address] テキスト ボックスに、Cisco WLC の IP アドレスを入力します。
3. [Add] をクリックして、このグループにメンバを追加します。

（注） メンバがスタティック リーダーに join されない場合は、失敗の理由がカッコ内に表示されます。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

RF グループ選択モードの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm group-mode{auto | leader | off}**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm group-mode{auto | leader | off}** 例： `スイッチ(config)#ap dot11 24ghz rrm group-mode leader`	802.11 帯域の RF グループ選択モードを設定します。 • [auto]：802.11 RF グループ選択を自動更新モードに設定します。 • [leader]：リーダー モードで 802.11 RF グループ選択をリーダー モードに設定します。

	コマンドまたはアクション	目的
		• [off]：802.11 RF グループ選択をディセーブルにします。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RF グループ名の設定（CLI）

手順の概要

1. **configure terminal**
2. **wireless rf-network** *name*
3. **end**
4. **show network profile** *profile_number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless rf-network** *name* 例： スイッチ (config)# **wireless rf-network test1**	RF グループを作成します。グループ名は、最大 19 文字の ASCII 文字列で、大文字と小文字が区別されます。 （注） RF グループに含める各コントローラについて、この手順を繰り返します。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 4	**show network profile** *profile_number*	RF グループを表示します。 （注） 1 ～ 4294967295 のネットワーク プロファイル番号を表示できます。

RF グループ名の設定（GUI）

ステップ 1 [Configuration] > [Controller] > [General] を選択して、[General] ページを開きます。

ステップ 2 [RF Network Name] テキスト ボックスに RF グループの名前を入力します。名前は最大 19 の ASCII 文字を含むことができ、大文字と小文字が区別されます。

ステップ 3 [Apply] をクリックして、変更を確定します。

ステップ 4 [Save Configuration] をクリックして、変更を保存します。

ステップ 5 RF グループに含める各コントローラについて、この手順を繰り返します。

802.11 静的 RF グループのメンバの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr* 例： スイッチ(config)#**ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1**	802.11 静的 RF グループにメンバを設定します。グループ メンバをアクティブにするには、グループ モードをリーダーに設定する必要があります。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

送信電力制御の設定

送信電力制御のしきい値の設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm tpc-threshold** *threshold_value*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm tpc-threshold** *threshold_value* 例： スイッチ(config)#**ap dot11 24ghz rrm tpc-threshold -60**	自動電力割り当てのためにRRMが使用する送信電力制御のしきい値を設定します。範囲は -80 ～ -50 です。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

送信電力レベルの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm txpower**{*trans_power_level* | **auto** | **max** | **min** | **once**}
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm txpower**{*trans_power_level* | **auto** | **max** | **min** | **once**} 例： スイッチ(config)#**ap dot11 24ghz rrm txpower auto**	802.11 の送信電力レベルを設定します。 • [trans_power_level]：送信電力レベルを設定します。 • [auto]：自動 RF をイネーブルにします。 • [max]：最大自動 RF 送信電力を設定します。 • [min]：最小自動 RF 送信電力を設定します。 • [once]：自動 RF を一度だけイネーブルにします。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

送信電力制御の設定（GUI）

ステップ 1 [Configuration] > [Wireless] > [802.11a/n/ac] > [RRM] > [TPC] または [Configuration] > [Wireless] > [802.11b/g/n] > [RRM] > [TPC] を選択して、RRM の [Tx Power Control (TPC)] ページを開きます。

ステップ 2 [Transmit Power Control] を選択します。
[Coverage Optimal Mode (TPCv1)]：強力な信号カバレッジと安定性を提供します。このモードでは、送信電力を低く維持することでキャパシティを増やし、干渉を減らします。

ステップ 3 [Power Level Assignment Method] ドロップダウン リストから次のオプションのいずれかを選択して、Cisco WLC の動的電力割り当てモードを指定します。

- [Automatic]：Cisco WLC よって、join しているすべてのアクセス ポイントの送信電力が定期的に評価され、必要に応じて更新されます。これはデフォルト値です。
- [On Demand]：Cisco WLC によって、join しているすべてのアクセス ポイントの送信電力が定期的に評価されます。ただし、必要に応じて、[On Demand] を選択してから [Apply] をクリックした場合のみ、Cisco WLC は電力を更新します。

（注） [On Demand] を選択してから [Apply] をクリックしても、Cisco WLC は送信電力をすぐに評価したり、更新したりしません。次の間隔（600 秒）まで待機します。この値は設定可能です。

- [Fixed]：Cisco WLC によって、join しているアクセス ポイントの送信電力が評価されたり、必要に応じて更新されたりすることはありません。電力レベルは、ドロップダウン リストから選択した固定値に設定されます。CLI から設定する場合、[Fixed] に対応するオプションは **once** です。

（注） 送信電力 レベルには、mW 単位または dBm 単位の値の代わりに整数値が割り当てられます。この整数は、アクセス ポイントが展開されている規制区域、チャネル、およびアンテナによって異なる電力レベルに対応します。

（注） 最適なパフォーマンスを確保するには、[Automatic] 設定を使用することを、お勧めします。

ステップ 4 [Maximum Power Level Assignment] および [Minimum Power Level Assignment] テキスト ボックスに最大および最小の電力レベル割り当て値を入力します。
[Maximum Power Level Assignment] の範囲は、-10 ～ 30 dBm です。

[Minimum Power Level Assignment] の範囲は、-10 ～ 30 dBm です。

ステップ 5 [Power Threshold] テキスト ボックスに、アクセス ポイントの電力を減らすかどうか判断する際に RRM で使用する切断信号レベルを入力します。このパラメータのデフォルト値は –70 dBm（TPCv1）ですが、アクセス ポイントの伝送パワー レベルが必要以上に高い（または低い）場合は変更できます。
このパラメータの範囲は –80 ～ –50 dBm です。この値を –65 ～ –50 dBm の範囲で増やすと、アクセス ポイントは高い送信電力で動作するようになります。値を減らすと、逆の効果が得られます。

多数のアクセス ポイントを使用しているアプリケーションでは、ワイヤレス クライアントが認識する BSSID（アクセス ポイント）やビーコンの数を少なくするために、しきい値を –80 dBm または –75 dBm に下げるのが有用です。一部のワイヤレス クライアントは多数の BSSID や高速ビーコンを処理できない場合があり、デフォルトのしきい値では、問題のある動作を起こす可能性があります。

このページには、次のような送信電力レベルのパラメータの設定も表示されますが、これらは設定できません。

- [Power Neighbor Count]：送信電力制御アルゴリズムを実行するためにアクセス ポイントに必要なネイバーの最小数です。
- [Power Assignment Leader]：パワー レベルの割り当てを担当する RF グループ リーダーの MAC アドレスです。
- [Last Power Level Assignment]：RRM が現在の送信電力 レベルの割り当てを最後に評価した時間です。

ステップ 6 [Apply] をクリックします。

ステップ 7 [Save Configuration] をクリックします。

802.11 RRM パラメータの設定

高度な 802.11 チャネル割り当てパラメータの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**high** | **low** | **medium**}
3. **ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** {*channel number* | **anchor-time** | **global** {**auto** | **once**} | **interval** | **min-metric** | **sensitivity** {**high** | **low** | **medium**}}
4. **ap dot11 5ghz rrm channel dca chan-width** {**20** | **40** | **80** | **best**}
5. **ap dot11** {**24ghz** | **5ghz**} **rrm channel device**
6. **ap dot11** {**24ghz** | **5ghz**} **rrm channel foreign**
7. **ap dot11** {**24ghz** | **5ghz**} **rrm channel load**
8. **ap dot11** {**24ghz** | **5ghz**} **rrm channel noise**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11** {**24ghz**	**5ghz**} **rrm channel cleanair-event sensitivity** {**high**	**low**	**medium**} 例： スイッチ(config)#**ap dot11 24ghz rrm channel cleanair-event sensitivity high**	CleanAir のイベント駆動 RRM パラメータを設定します。 • [High]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最高に指定します。 • [Low]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最低に指定します。 • [Medium]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を中間に指定します。
ステップ 3	**ap dot11** {**24ghz**	**5ghz**} **rrm channel dca** {*channel number*	**anchor-time**	**global** {**auto**	**once**}	**interval**	**min-metric**	**sensitivity** {**high**	**low**	**medium**}} 例： スイッチ(config)#**ap dot11 24ghz rrm channel dca interval 2**	802.11 帯域の動的チャネル割り当て（DCA）アルゴリズム パラメータを設定します。 • ***<1-14>***：DCA リストに追加するチャネル番号を入力します。 • [anchor-time]：DCA のアンカー時間を設定します。範囲は 0 ～ 23 時間です。

	コマンドまたはアクション	目的
		• [global]：すべての 802.11 Cisco AP の DCA モードを設定します。 ◦ [auto]：自動 RF をイネーブルにします。 ◦ [once]：自動 RF を一度だけイネーブルにします。 • [interval]：DCA のインターバル値を設定します。値は 1、2、3、4、6、8、12、24 時間です。デフォルト値 0 は 10 分を意味します。 • [min-metric]：DCA の最小 RSSI エネルギー メトリックを設定します。範囲は -100 ～ -60 です。 • [sensitivity]：環境の変化に対する DCA 感度レベルを設定します。 ◦ [high]：最高の感度を指定します。 ◦ [low]：最低の感度を指定します。 ◦ [medium]：中間の感度を指定します。
ステップ 4	**ap dot11 5ghz rrm channel dca chan-width** {**20** | **40** | **80** | **best**}	5 GHz 帯域のすべての 802.11 無線に対して DCA チャネル幅を設定します。チャネル幅を 20 MHz、40 MHz、80 MHz、または最良に設定します。20 Mhz がデフォルト値です。
ステップ 5	**ap dot11** {**24ghz** | **5ghz**} **rrm channel device** 例： `スイッチ(config)#ap dot11 24ghz rrm channel device`	802.11 チャネル割り当てで、非 Wi-Fi デバイスの継続的な回避を設定します。
ステップ 6	**ap dot11** {**24ghz** | **5ghz**} **rrm channel foreign** 例： `スイッチ(config)#ap dot11 24ghz rrm channel foreign`	チャネル割り当てで、外部 AP の 802.11 干渉の回避を設定します。
ステップ 7	**ap dot11** {**24ghz** | **5ghz**} **rrm channel load** 例： `スイッチ(config)#ap dot11 24ghz rrm channel load`	チャネル割り当てで、Cisco AP の 802.11 負荷の回避を設定します。

	コマンドまたはアクション	目的
ステップ 8	**ap dot11** {**24ghz** | **5ghz**} **rrm channel noise** 例： スイッチ(config)#**ap dot11 24ghz rrm channel noise**	チャネル割り当てで、802.11 ノイズの回避を設定します。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

動的チャネル割り当ての設定（GUI）

RRM によるスキャンに使用するチャネルの選択時に、Cisco WLC の GUI を使用して動的チャネル割り当て（DCA）アルゴリズムで考慮されるチャネルを指定できます。

（注） この機能は、クライアントが古いデバイスであるため、またはクライアントに特定の制約事項があるために、クライアントで特定のチャネルがサポートされないことがわかっている場合に役立ちます。

ステップ 1 次のように、802.11a/n/ac または 802.11b/g/n ネットワークをディセーブルにします。

a) [Configuration] > [Wireless] > [802.11a/n/ac] > [Network] または [Configuration] > [Wireless] > [802.11b/g/n] > [Network] を選択して、[Global Parameters] ページを開きます。

b) [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオフにします。

c) [Apply] をクリックします。

ステップ 2 [Configuration] > [Wireless] > [802.11a/n/ac] > [RRM] > [DCA] または [Configuration] > [Wireless] > [802.11b/g/n] > [RRM] > [DCA] を選択して、[Dynamic Channel Assignment (DCA)] ページを開きます。

ステップ 3 [Channel Assignment Method] ドロップダウン リストから次のオプションのいずれかを選択して、Cisco WLC の DCA モードを指定します。

- [Automatic]：Cisco WLC によって、join しているすべてのアクセス ポイントのチャネル割り当てが定期的に評価され、必要に応じて更新されます。これはデフォルト値です。
- [Freeze]：必要に応じて、[Freeze] オプションを選択した後、[Apply] をクリックした場合にだけ、join しているすべてのアクセス ポイントのチャネル割り当てが Cisco WLC によって評価および更新されます。

  （注） [Freeze] オプションを選択した後に [Apply] をクリックすると、Cisco WLC はチャネル割り当てをすぐに評価したり、更新したりしません。次の間隔が経過するまで待機します。

- OFF：DCA をオフにして、帯域の最初のチャネルにすべてのアクセス ポイント無線を設定します。このオプションを選択する場合は、すべての無線のチャネルを手動で割り当てる必要があります。

（注） 最適なパフォーマンスを確保するには、[Automatic] 設定を使用することを、お勧めします。Cisco WLC の動的チャネルおよび電力の設定をディセーブルにする手順については、チャネルおよび電力の動的割り当ての無効化（GUI）の項を参照してください。

ステップ 4 [Interval] ドロップダウン リストで、[10 minutes]、[1 hour]、[2 hours]、[3 hours]、[4 hours]、[6 hours]、[8 hours]、[12 hours]、または [24 hours] のいずれかのオプションを選択し、DCA アルゴリズムを実行する間隔を指定します。デフォルト値は 10 分です。

ステップ 5 [AnchorTime] ドロップダウン リストで、DCA アルゴリズムの開始時刻を指定する数値を選択します。オプションは、0 ～ 23 の数値（両端の値を含む）で、午前 12 時～午後 11 時の時刻を表します。

ステップ 6 [DCA Channel Sensitivity] ドロップダウン リストから、次のオプションのいずれかを選択して、チャネルを変更するかどうかを判断する際の、信号、負荷、ノイズ、干渉などの環境の変化に対する DCA アルゴリズムの感度を指定します。

- [Low]：環境の変化に対する DCA アルゴリズムの感度は特に高くありません。
- [Medium]：環境の変化に対する DCA アルゴリズムの感度は中程度です。
- [High]：環境の変化に対する DCA アルゴリズムの感度が高くなります。

デフォルトでは [Medium] です。DCA の感度のしきい値は、次の表で示すように、無線帯域によって異なります。

表 *68*：*DCA* の感度のしきい値

オプション	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
High	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

ステップ 7 このページには、次のような変更できないチャネル パラメータの設定も表示されます。

- [Channel Assignment Leader]：チャネルの割り当てを担当する RF グループ リーダーの MAC アドレスです。

ステップ 8 [DCA Channel List] 領域の [DCA Channels] テキスト ボックスには、現在選択されているチャネルが表示されます。チャネルを選択するには、[Select] カラムでそのチャネルのチェックボックスをオンにします。チャネルの選択を解除するには、チャネルのチェックボックスをオフにします。
範囲は次のとおりです。

- 802.11a：36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、165（国によって異なる）。
- 802.11b/g：1、2、3、4、5、6、7、8、9、10、11、12、13、14（国によって異なる）。

デフォルトの設定は次のとおりです。

- 802.11a：36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161
- 802.11b/g：1、6、11

ステップ 9 [Apply] をクリックします。

ステップ 10 次の手順で、802.11 ネットワークを再度イネーブルにします。

1. [Configuration] > [Wireless] > [802.11a/n/ac] > [Network] または [Configuration] > [Wireless] > [802.11b/g/n] > [Network] を選択して、[Global Parameters] ページを開きます。
2. [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオンにします。
3. [Apply] をクリックします。

ステップ 11 [Save Configuration] をクリックします。

802.11 カバレッジ ホール検出の設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**}
3. **ap dot11 24ghz | 5ghz rrm coverage exception global** *exception level*
4. **ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min exception level*
5. **ap dot11 24ghz | 5ghz rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**}
6. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ap dot11 24ghz | 5ghz rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**} 例： スイッチ**(config)#ap dot11 24ghz rrm coverage data fail-percentage 60**	データ パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンク データ パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100 % の範囲で設定します。 • [packet-count]：アップリンク データ パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。 • [rssi-threshold]：データ パケットの 802.11 最小受信カバレッジ レベルを、–90 ～ 60 dBm の範囲で設定します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm coverage exception global** *exception level* 例： スイッチ**(config)#ap dot11 24ghz rrm coverage exception global 50**	802.11 Cisco AP のカバレッジ例外レベルを、0 ～ 100 % の範囲で設定します。
ステップ 4	**ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min exception level* 例： スイッチ**(config)#ap dot11 24ghz rrm coverage level global 10**	802.11 Cisco AP クライアントの最小例外を、1 ～ 75 の範囲で指定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**} 例： スイッチ**(config)#ap dot11 24ghz rrm coverage voice packet-count 10**	音声パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンク音声パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100 % の範囲で設定します。 • [packet-count]：アップリンク音声パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。 • [rssi-threshold]：音声パケットの 802.11 最小受信カバレッジ レベルを、–90 ～ -60 dBm の範囲で設定します。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

カバレッジ ホールの検出の設定（GUI）

ステップ 1 次の手順で 802.11 ネットワークをディセーブルにします。

a) [Configuration] > [Wireless] > [802.11a/n/ac] または [Configuration] > [Wireless] > [802.11b/g/n] を選択して、802.11a/n/ac（または 802.11b/g/n）の [Global Parameters] ページを開きます。

b) [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオフにします。

c) [Apply] をクリックします。

ステップ 2 [Configuration] > [Wireless] > [802.11a/n/ac] > [RRM] > [Coverage Thresholds] または [Configuration] > [Wireless] > [802.11b/g/n] > [RRM] > [Coverage Thresholds] を選択して、[coverage] ページを開きます。

ステップ 3 カバレッジ ホールの検出を有効にする場合は [Enable Coverage Hole Detection] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。カバレッジ ホールの検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセス ポイントがあるかどうかを、アクセス ポイントから受信したデータに基づいて Cisco WLC が自動的に判断します。デフォルト値はオンです。

ステップ 4 [Data RSSI] テキスト ボックスに、アクセス ポイントで受信されたデータ パケットの最小の受信信号強度インジケータ（RSSI）値を入力します。入力する値は、ネットワーク内のカバレッジ ホール（またはカバレッジが不完全な領域）を特定するのに使用されます。アクセスポイントによって、ここで入力する値より RSSI 値が小さいパケットがデータ キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は –90 ～ –60 dBm で、デフォルト値は –80 dBm です。アクセス ポイントでは、データ RSSI が 5 秒おきに測定され、それらが 90 秒間隔で Cisco WLC にレポートされます。

ステップ 5 [Voice RSSI] テキスト ボックスに、アクセス ポイントで受信された音声パケットの最小の受信信号強度インジケータ（RSSI）値を入力します。入力する値は、ネットワーク内のカバレッジ ホールを特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットが音声キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は –90 ～ –60 dBm で、デフォルト値は –80 dBm です。アクセス ポイントでは、音声 RSSI が 5 秒おきに測定され、それらが 90 秒間隔で Cisco WLC にレポートされます。

ステップ 6 [Min Failed Client Count per AP] テキスト ボックスに、RSSI 値がデータ RSSI または音声 RSSI のしきい値以下である、アクセス ポイント上のクライアントの最小数を入力します。有効な範囲は 1 ～ 75 で、デフォルト値は 3 です。

ステップ 7 [Coverage Exception Level per AP] テキスト ボックスに、信号レベルが低くなっているにもかかわらず別のアクセス ポイントにローミングできない、アクセス ポイント上のクライアントの割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 25% です。

（注） 5 秒間で失敗したパケットの数と割合の両方が、[Failed Packet Count] および [Failed Packet Percentage]（Cisco WLC の CLI を使用して設定可能）に設定された値を超える場合、クライアントは事前アラーム状態と判断されます。Cisco WLC は、この情報を使用して、真のカバレッジ ホールと偽のカバレッジ ホールを区別します。false positive は通常、大部分のクライアントに実装されているローミング ロジックが不適切であることが原因です。180 秒間（90 秒間の 2 倍）で失敗したクライアントの数と割合の両方が、[Min Failed Client Count per AP] および [Coverage Exception Level per AP] テキスト ボックスに入力された値を満たすか超えている場合、カバレッジ ホールが検出されます。Cisco WLC は、カバレッジ ホールが修正可能かどうかが判断し、適切な場合は、その特定のアクセス ポイントの送信電力 レベルを上げることによってカバレッジ ホールを解消します。

ステップ 8 [Apply] をクリックします。

ステップ 9 次の手順で 802.11 ネットワークを再度イネーブルにします。

a) [Configuration] > [Wireless] > [802.11a/n/ac] > [Network] または [Configuration] > [Wireless] > [802.11b/g/n] > [Network] を選択して、802.11a（または 802.11b/g）の [Global Parameters] ページを開きます。

b) [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオンにします。

c) [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

802.11 イベント ロギングの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm logging**{**channel | coverage | foreign | load | noise | performance | txpower**}
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz	5ghz rrm logging**{**channel	coverage	foreign	load	noise	performance	txpower**}	各種パラメータに対するイベント ロギングを設定します。 • [channel]：802.11 チャネル変更ロギング モードを設定します。

	コマンドまたはアクション	目的
	例： スイッチ(config)#**ap dot11 24ghz rrm logging channel** スイッチ(config)#**ap dot11 24ghz rrm logging coverage** スイッチ(config)#**ap dot11 24ghz rrm logging foreign** スイッチ(config)#**ap dot11 24ghz rrm logging load** スイッチ(config)#**ap dot11 24ghz rrm logging noise** スイッチ(config)#**ap dot11 24ghz rrm logging performance** スイッチ(config)#**ap dot11 24ghz rrm logging txpower**	• [coverage]：802.11 のカバレッジ プロファイル ロギング モードを設定します。 • [foreign]：802.11 外部干渉プロファイル ロギング モードを設定します。 • [load]：802.11 負荷プロファイル ロギング モードを設定します。 • [noise]：802.11 ノイズ プロファイル ロギング モードを設定します。 • [performance]：802.11 パフォーマンス プロファイル ロギング モードを設定します。 • [txpower]：802.11 送信電力変更ロギング モードを設定します。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 統計情報の監視の設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**}
3. **ap dot11 24ghz | 5ghz rrm monitor coverage** *interval*
4. **ap dot11 24ghz | 5ghz rrm monitor load** *interval*
5. **ap dot11 24ghz | 5ghz rrm monitor noise** *interval*
6. **ap dot11 24ghz | 5ghz rrm monitor signal** *interval*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**} 例： スイッチ(config)#**ap dot11 24ghz rrm monitor channel-list all**	noise/interference/rogue などのパラメータに 802.11 監視チャネル リストを設定します。 • [all]：すべてのチャネルを監視します。 • [country]：設定された国コードで使用するチャネルを監視します。 • [dca]：動的なチャネル割り当てで使用されるチャネルを監視します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm monitor coverage** *interval* 例： スイッチ(config)#**ap dot11 24ghz rrm monitor coverage 600**	802.11 のカバレッジ測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 4	**ap dot11 24ghz | 5ghz rrm monitor load** *interval* 例： スイッチ(config)#**ap dot11 24ghz rrm monitor load 180**	802.11 負荷測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm monitor noise** *interval* 例： スイッチ(config)#**ap dot11 24ghz rrm monitor noise 360**	802.11 のノイズ測定間隔（チャネル スキャン間隔）を、60 ～ 3600 秒の範囲で設定します。
ステップ 6	**ap dot11 24ghz | 5ghz rrm monitor signal** *interval* 例： スイッチ(config)#**ap dot11 24ghz rrm monitor signal 480**	802.11 の信号測定間隔（ネイバー パケットの頻度）を、60 ～ 3600 秒の範囲で設定します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： スイッチ(config)# **end**	特権EXECモードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 パフォーマンス プロファイルの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value*
3. **ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value*
4. **ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value*
5. **ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value*
6. **ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value* 例： スイッチ(config)#**ap dot11 24ghz rrm profile clients 20**	802.11 Cisco AP クライアント数のしきい値を、1 ～ 75 の範囲で設定します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value* 例： スイッチ(config)#**ap dot11 24ghz rrm profile foreign 50**	802.11 外部干渉のしきい値を、0 ～ 100 % の範囲で設定します。

	コマンドまたはアクション	目的
ステップ 4	**ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value* 例： スイッチ(config)#**ap dot11 24ghz rrm profile noise -65**	802.11 外部ノイズのしきい値を、-127 ～ 0 dBm の範囲で設定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value* 例： スイッチ(config)#**ap dot11 24ghz rrm profile throughput 10000**	802.11 Cisco AP スループットのしきい値を、1000 ～ 10000000 バイト/秒の範囲で設定します。
ステップ 6	**ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value* 例： スイッチ(config)#**ap dot11 24ghz rrm profile utilization 75**	802.11 RF 使用率のしきい値を、0 ～ 100% の範囲で設定します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RF グループ内の不正アクセス ポイント検出の設定

RF グループ内の不正アクセス ポイント検出の設定（CLI）

はじめる前に

RF グループ内の各 Cisco WLC に同じ RF グループ名が設定されていることを確認します。

（注） この名前は、すべてのビーコン フレーム内の認証 IE を検証するために使用されます。Cisco WLC に異なる名前が設定されている場合は、誤ったアラームが生成されます。

手順の概要

1. **ap name** *Cisco_AP* **mode** {**local** | **monitor**}
2. **end**
3. **configure terminal**
4. **wireless wps ap-authentication**
5. **wireless wps ap-authentication threshold** *value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ap name** *Cisco_AP* **mode** {**local** | **monitor**} 例： `スイッチ# ap name ap1 mode local`	ローカル（通常）モードまたはモニタ（リッスン専用）モードの特定アクセス ポイントを設定します。Cisco WLC に接続されたすべてのアクセス ポイントについて、次の手順を実行します。
ステップ 2	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 3	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**wireless wps ap-authentication** 例： `スイッチ (config)# wireless wps ap-authentication`	不正なアクセス ポイントの検出をイネーブルにします。
ステップ 5	**wireless wps ap-authentication threshold** *value* 例： `スイッチ (config)# wireless wps ap-authentication threshold 50`	不正アクセス ポイント アラームが生成されるタイミングを指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。 しきい値の有効範囲は 1 ～ 255 で、デフォルトのしきい値は 1 です。アラームの誤判定を防止するには、しきい値を高い値に設定してください。 （注） RF グループ内のすべての Cisco WLC で、不正アクセス ポイントの検出としきい値をイネーブルにします。 （注） RF グループ内のすべての Cisco WLC で不正アクセス ポイントの検出がイネーブルになっていない場合、この機能がディセーブルになっている Cisco WLC のアクセス ポイントは不正として報告されます。

RF グループ内の不正アクセス ポイント検出の有効化（GUI）

ステップ 1 RF グループ内の各 Cisco WLC に同じ RF グループ名が設定されていることを確認します。
（注） この名前は、すべてのビーコンフレーム内の認証IEを検証するために使用されます。Cisco WLC に異なる名前が設定されている場合は、誤ったアラームが生成されます。

ステップ 2 [Configuration] > [Wireless] > [Access Points] > [All APs] を選択して、[All APs] ページを開きます。

ステップ 3 アクセス ポイントの名前をクリックして、[All APs] > [Edit] ページを開きます。

ステップ 4 [AP Mode] ドロップダウン リストから [local] または [monitor] を選択し、[Apply] をクリックして変更を確定します。

ステップ 5 [Save Configuration] をクリックして、変更を保存します。

ステップ 6 Cisco WLC に接続されているすべてのアクセス ポイントについて、ステップ 2 からステップ 5 を繰り返します。

ステップ 7 [Configuration] > [Security] > [Wireless Protection Policies] > [AP Authentication/MFP] を選択して、[AP Authentication Policy] ページを開きます。
この Cisco WLC が属する RF グループの名前は、ページの上部に表示されます。

ステップ 8 [Protection Type] ドロップダウン リストから [AP Authentication] を選択して、不正アクセス ポイントの検出を有効にします。

ステップ 9 [Alarm Trigger Threshold] 編集ボックスに数値を入力して、不正アクセス ポイントに関するアラームがいつ生成されるようにするかを指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。
（注） しきい値の有効範囲は 1 ～ 255 で、デフォルト値は 1 です。アラームの誤判定を防止するには、しきい値を高い値に設定してください。

ステップ 10 [Apply] をクリックして、変更を確定します。

ステップ 11 [Save Configuration] をクリックして、変更を保存します。

ステップ 12 RF グループ内のすべての Cisco WLC について、この手順を繰り返します。
（注） RF グループ内のすべての Cisco WLC で不正アクセス ポイントの検出が有効になっていない場合、この機能が無効になっている Cisco WLC のアクセス ポイントは不正として報告されます。

RRM パラメータと RF グループ ステータスの監視

RRM パラメータの監視

表 *69*：無線リソース管理を監視するためのコマンド

コマンド	説明
show ap dot11 24ghz ccx	すべての Cisco AP に対して 802.11b CCX 情報を表示します。
show ap dot11 24ghz channel	802.11b チャネル割り当ての設定および統計情報を表示します。
show ap dot11 24ghz coverage	802.11b カバレッジの設定と統計情報を表示します。
show ap dot11 24ghz group	802.11b グループ化の設定と統計情報を表示します。
show ap dot11 24ghz l2roam	802.11b l2roam 情報を表示します。
show ap dot11 24ghz logging	802.11b イベント ロギングの設定と統計情報を表示します。
show ap dot11 24ghz monitor	802.11b モニタリングの設定および統計情報を表示します。
show ap dot11 24ghz profile	すべての Cisco AP の 802.11b プロファイル情報を表示します。
show ap dot11 24ghz receiver	802.11b レシーバの設定と統計情報を表示します。
show ap dot11 24ghz summary	802.11b Cisco AP の設定と統計情報を表示します。
show ap dot11 24ghz txpower	802.11b 送信電力制御の設定と統計情報を表示します。
show ap dot11 5ghz ccx	すべての Cisco AP の 802.11a CCX 情報を表示します。

コマンド	説明
show ap dot11 5ghz channel	802.11a チャネル割り当ての設定および統計情報を表示します。
show ap dot11 5ghz coverage	802.11a カバレッジの設定と統計情報を表示します。
show ap dot11 5ghz group	802.11a グループ化の設定と統計情報を表示します。
show ap dot11 5ghz l2roam	802.11a l2roam 情報を表示します。
show ap dot11 5ghz logging	802.11a イベント ロギングの設定と統計情報を表示します。
show ap dot11 5ghz monitor	802.11a モニタリングの設定および統計情報を表示します。
show ap dot11 5ghz profile	すべての Cisco AP の 802.11a プロファイル情報を表示します。
show ap dot11 5ghz receiver	802.11a レシーバの設定と統計情報を表示します。
show ap dot11 5ghz summary	802.11a Cisco AP の設定と統計情報を表示します。
show ap dot11 5ghz txpower	802.11a 送信電力制御の設定と統計情報を表示します。

RF グループ ステータスの監視（CLI）

ここでは、RF グループ ステータスの新しいコマンドについて説明します。

次のコマンドがスイッチの RF グループ ステータスを監視するために使用できます。

表 *70*：アグレッシブ ロード バランシング コマンドの監視

コマンド	目的
show ap dot11 5ghz group	802.11a RF ネットワークの RF グループ リーダーである Cisco WLC の名前が表示されます。

show ap dot11 24ghz group	802.11b/g RF ネットワークの RF グループ リーダーである Cisco WLC の名前が表示されます。

RF グループ ステータスの監視（GUI）

ステップ 1 [Configuration] > [Wireless] > [802.11a/n] > または [802.11b/g/n] > [RRM] > [RF Grouping] を選択して、[RF Grouping Algorithm] ページを開きます。
このページは RF グループの詳細を示し、設定可能なパラメータ [Group mode]、この Cisco WLC の [Group role]、[Group Update Interval]、およびこの Cisco WLC の [Group Leader] の Cisco WLC 名と IP アドレスを表示します。

（注） RF グループ化モードは、[Group Mode] ドロップダウン リストを使用して設定できます。

ヒント：一度 Cisco WLC がスタティック メンバとして join してから、グループ化モードを変更する場合は、メンバを設定したスタティック リーダーからそのメンバを削除することをお勧めします。メンバの Cisco WLC が複数のスタティック リーダーでメンバになるように設定されていないことも確認してください。これは、1 つまたは複数の RF スタティック リーダーから join 試行が繰り返されるのを回避します。

ステップ 2 （任意）選択しなかったネットワーク タイプ（802.11a/n または 802.11b/g/n）について、この手順を繰り返します。

例：RF グループの設定

次に、RF グループ名を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wireless rf-network test1
スイッチ(config)# ap dot11 24ghz shutdown
スイッチ(config)# end
スイッチ # show network profile 5
```

次に、RF グループ内の不正アクセス ポイントの検出を設定する例を示します。

```
スイッチ# ap name ap1 mode local
スイッチ# end
スイッチ# configure terminal
スイッチ(config)# wireless wps ap-authentication
スイッチ(config)# wireless wps ap-authentication threshold 50
スイッチ(config)# end
```

ED-RRM に関する情報

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

Cisco ワイヤレス LAN コントローラで ED-RRM の設定（CLI）

ステップ 1 次のコマンドを入力して、Cisco CleanAir 対応のアクセス ポイントで非常に高いレベルの干渉が検出された場合に、Event Driven Radio Resource Management（RRM）の実行がトリガーされるよう設定します。
ap dot11 {**24ghz** | **5ghz**} **rrm channelcleanair-event**：802.11 の Cisco Lightweight アクセス ポイントの CleanAir による RRM パラメータを設定します。

ap dot11 {**24ghz** | **5ghz**} **rrm channelcleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}：802.11 の Cisco Lightweight アクセス ポイントの CleanAir による RRM 感度を設定します。デフォルトの選択は、[Medium] です。

ap dot11 {**24ghz** | **5ghz**} **rrm channelcleanair-event rogue-contribution**：不正コントリビューションを有効にします。

ap dot11 {**24ghz** | **5ghz**} **rrm channelcleanair-event rogue-contributionduty-cycle***thresholdvalue*：不正コントリビューションのしきい値を設定します。値の範囲は 1 ～ 99 で、デフォルトの値は 80 です。

ステップ 2 次のコマンドを入力して、変更を保存します。
write memory

ステップ 3 次のコマンドを入力して、802.11a/n/ac または 802.11b/g/n ネットワークに対する CleanAir の設定を確認します。
show ap dot11 {**24ghz** | **5ghz**} **cleanairconfig**

以下に類似した情報が表示されます。

```
AdditionalClean Air Settings:
CleanAir Event-driven RRM State.............. : Enabled
CleanAir Driven RRM Sensitivity.............. : LOW
CleanAir Event-driven RRM Rogue Option....... : Enabled
CleanAir Event-driven RRM Rogue Duty Cycle... : 80
CleanAir Persistent Devices state............ : Disabled
CleanAir Persistent Device Propagation....... : Disabled
```

ED-RRM の設定（GUI）

ステップ 1 [Configure] > [Radio Configurations] > [2.4 GHZ or 5 GHZ] > [RRM] > [DCA] の順に選択して、[ED-RRM] ページを開きます。

（注） ED-RRM をイネーブルにする前に、[Configure] > [Radio Configurations] > [2.4 GHZ or 5 GHZ] > [Network] > [General] ページから [Network Status] を無効にする必要があります。ED-RRM の設定後に、ネットワークを再度有効にします。

ステップ 2 [Event Driven RRM] セクションで、ED-RRM パラメータを表示するには、[EDRRM] チェックボックスをオンにします。

ステップ 3 [Sensitivity Threshold] のドロップダウンから値を選択します。
オプション：[Low]、[Medium]、[High]。デフォルトの選択は、[Medium] です。

ステップ 4 不正なデューティ サイクル パラメータを表示するには、[Rogue Contribution] チェックボックスをオンにします。

ステップ 5 テキストボックスに、[Rogue Duty Cycle] の値を入力します。
値の範囲は 1 ～ 99 で、デフォルトの値は 80 です。

ステップ 6 [Apply] をクリックします。

ステップ 7 [Save Configuration] をクリックします。

無線リソース管理に関するその他の参考ドキュメント

関連資料

関連項目	マニュアル タイトル
RRM コマンドと詳細	*RRM Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

MIB

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

シスコのテクニカル サポート

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

無線リソース管理の設定を行うための機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 51 章

設定の最適化されたローミング

- ローミングの最適化に関する情報，1071 ページ
- ローミングの最適化の制約事項，1072 ページ
- ローミングの最適化の設定（GUI），1072 ページ
- ローミングの最適化の設定（CLI），1073 ページ

ローミングの最適化に関する情報

ローミングの最適化は、遠隔地のアクセス ポイントに長時間アソシエートし続けているクライアントや、接続が不安定な Wi-Fi ネットワークに接続を試みるアウトバウンド クライアントの問題を解決します。この機能は、クライアント データ パケットの RSSI とデータ レートに基づいてクライアントをアソシエート解除します。クライアントは、RSSI アラーム条件が満たされ、現在のデータ レートが最適化ローミング データ レートのしきい値を下回っている場合にアソシエート解除されます。データ レート オプションを無効にして、RSSI のみをクライアントのアソシエート解除に使用するようにできます。

ローミングの最適化は、クライアントの RSSI が低いときにもクライアント アソシエーションを阻止します。この機能は、RSSI しきい値に照らして受信クライアントの RSSI をチェックします。このチェックで、クライアントに有効な接続がない限り、クライアントの Wi-Fi ネットワークへの接続が阻止されます。クライアントはビーコンを受信して Wi-Fi ネットワークに接続できても、信号が弱いために安定した接続をサポートできない場合がよくあります。

ローミングの最適化を使用することによって、無線に対してクライアント カバレッジ レポート間隔を設定することもできます。クライアント カバレッジの統計情報には、データ パケット RSSI、カバレッジ ホールの検出および軽減（CHDM）の事前アラーム障害、再送信要求と現在のデータ レートが含まれます。

最適化されたローミングは次のシナリオで実行されます。

- 予防的にクライアントを切断して長時間接続しているクライアントの問題に対処します。
- データ RSSI パケットをアクティブに監視します。

- RSSI が、設定されたしきい値よりも低いクライアントの関連付けを解除します。

ローミングの最適化の制約事項

- 802.11a/b ネットワークを無効にするまで、ローミングの最適化の間隔を設定できません。

ローミングの最適化の設定（GUI）

ステップ 1 [Wireless] > [Advanced] > [Optimized Roaming] を選択します。[Optimized Roaming] ページが表示されます。

ステップ 2 802.11 帯域のローミングの最適化を有効にするには、[Enable] チェックボックスをオンにします。
802.11 帯域のローミングの最適化を有効にした後で、ローミングの最適化の間隔、およびデータ レートのしきい値を設定できます。

ステップ 3 [Optimized Roaming Interval] テキスト ボックスで、アクセス ポイントがコントローラに対してクライアント カバレッジの統計情報をレポートする間隔を入力します。
クライアント カバレッジの統計情報には、データ パケット RSSI、カバレッジ ホールの検出および軽減（CHDM）の事前アラーム障害、再送信要求と現在のデータ レートが含まれます。範囲は 5 ～ 90 秒です。デフォルト値は 90 秒です。

（注） ローミングの最適化のレポート間隔を設定する前に、802.11a/b ネットワークを無効にする必要があります。レポートの間隔に対して低い値を設定すると、カバレッジ レポートのメッセージでネットワークが過負荷になることがあります。

ステップ 4 [Optimized Roaming Data Rate Threshold] テキスト ボックスに、クライアントのしきい値データ レートの値を入力します。
次のデータ レートが使用可能です。

- 802.11a：6、9、12、18、24、36、48、および 54。
- 802.11b：1、2、5.5、11、6、9、12、18、24、36、48、および 54。

ローミングの最適化は、クライアントのデータ パケットおよびデータ レートの RSSI に基づいてクライアントのアソシエートを解除します。クライアントの現在のデータ レートが、[Optimized Roaming Data Rate Threshold] よりも小さい値の場合は、クライアントはアソシエート解除されます。

次の作業

ローミングの最適化は、アソシエーションのときにクライアント RSSI をチェックします。この RSSI 値は、設定されている CHDM RSSI に対して 6 db ヒステリシスで検証されます。カバレッジ ホールの検出に対して設定された RSSI しきい値を検証するには、[Wireless] > [802.11a/n/ac]（または [802.11b/g/n]）> [RRM] > [Coverage] を選択して、802.11a/ac（または 802.11b/g/n）をオープンし、[RRM] > [Coverage page] を選択します。

ローミングの最適化の設定（CLI）

ステップ 1 次のコマンドを入力して、ローミングの最適化を有効または無効にします。
config advanced{802.11a| 802.11b} optimized-roaming{enable| disable}

デフォルトでは、ローミングの最適化は無効になっています。

ステップ 2 次のコマンドを入力して、802.11a/b ネットワークのクライアント カバレッジのレポート間隔を設定します。
config advanced{802.11a| 802.11b} optimized-roaming interval*seconds*

範囲は 5 ～ 90 秒です。デフォルト値は 90 秒です。

（注） ローミングの最適化のレポート間隔を設定する前に、802.11a/b ネットワークを無効にする必要があります。

ステップ 3 次のコマンドを入力して、802.11a/b ネットワークのしきい値データ レートを設定します。
config advanced{802.11a| 802.11b} optimized-roaming datarate*mbps*

802.11a の場合、設定可能なデータ レートは 6、9、12、18、24、36、48、および 54 です。802.11b の場合、設定可能なデータ レートは、1、2、5.5、11、6、9、12、18、24、36、48、および 54 です。データ レートを無効にするには 0 を設定します。

ステップ 4 このコマンドを入力して、各帯域のローミングの最適化の情報を表示します。
show advanced{802.11a| 802.11b} optimized-roaming

```
(Cisco Controller) > show advanced 802.11a optimized-roaming
OptimizedRoaming
  802.11a OptimizedRoaming Mode.................. Enabled
  802.11a OptimizedRoaming Reporting Interval.... 20 seconds
  802.11a OptimizedRoaming Rate Threshold........ disabled
```

ステップ 5 次のコマンドを入力して、最適なローミング統計に関する情報を表示します。
show advanced{802.11a| 802.11b} optimized-roaming stats

```
(Cisco Controller) > show advanced 802.11a optimized-roaming stats
OptimizedRoaming Stats
  802.11a OptimizedRoaming Disassociations....... 0
  802.11a OptimizedRoaming Rejections............ 0
```

第 52 章

設定の Rx SOP

- Rx-SOP に関する情報，1075 ページ
- Rx SOP の設定（GUI），1075 ページ
- Rx SOP の設定（CLI），1076 ページ

Rx-SOP に関する情報

レシーバのパケット検出開始しきい値（RxSOP）は、アクセスポイントの無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。Wi-Fi レベルが上がると、無線の受信感度が下がり、レシーバのセルサイズが小さくなります。セルサイズの減少は、ネットワークのクライアントの分散に影響します。

RF リンクが脆弱なクライアント、つなぎっぱなしのクライアント、およびアクセス ポイント全体で負荷分散しているクライアントに対処するために Rx SOP が使用されます。Rx SOP は、アクセス ポイントが最も近くにある最も強力なクライアントを最適化する必要のあるスタジアムやホールなどの高密度展開でネットワーク性能を最大限引き出すのに役立ちます。

Rx SOP の設定（GUI）

Rx SOP モードを設定します。

ステップ 1 [Configure] > [Advanced] > [Rx SOP Threshold] を選択します。

ステップ 2 2.しきい値のモード（auto、high、low、medium）を選択します。

a) 5 GHz：[Rx Sop Threshold 802.11a] ドロップダウン メニューを選択します。

b) 2.4 GHz：[Rx Sop Threshold 802.11b] ドロップダウン メニューを選択します。

Rx SOP の設定（CLI）

ステップ 1 次のコマンドを入力して、Rx SOP モードを設定します。
ap dot11 {24ghz | 5ghz} rx-sop threshold {auto | high | low | medium}

ステップ 2 Rx SOP の高密度パラメータを確認します。
show ap dot11 24ghz high-density

```
Controller# show ap dot11 24ghz high-density
Receiver Start-of-Packet threshold: auto
Multicast Data Rate: auto
AP Name : AP5475.d064.0552
Receiver Start-of-Packet threshold: auto
Multicast Data Rate: auto 2:33 PM
```

第 XI 部

Routing

- MSDP の設定，1079 ページ
- IP ユニキャスト ルーティングの設定，1107 ページ

第 53 章

MSDP の設定

- 機能情報の確認，1079 ページ
- MSDP の設定について，1079 ページ
- MSDP の設定方法，1082 ページ
- MSDP のモニタリングおよびメンテナンス，1103 ページ
- MSDP の設定例，1105 ページ

機能情報の確認

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

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

MSDP の設定について

このセクションでは、スイッチに Multicast Source Discovery Protocol（MSDP）を設定する方法について説明します。MSDP によって、複数の Protocol-Independent Multicast Sparse-Mode（PIM-SM）ドメインが接続されます。

このソフトウェア リリースでは、MSDP と連携して動作する Multicast Border Gateway Protocol（MBGP）がサポートされていないため、MSDP は完全にはサポートされていません。ただし、MBGP が動作していない場合、MSDP と連携して動作するデフォルト ピアを作成できます。

（注） この機能を使用するには、アクティブ スイッチ上で IP Services フィーチャー セットが稼働している必要があります。

MSDP の概要

MSDP を使用すると、さまざまなドメイン内のすべてのランデブー ポイント（RP）に、グループのマルチキャスト送信元を通知できます。各 PIM-SM ドメインでは独自の RP が使用され、他のドメインの RP には依存しません。RP は伝送制御プロトコル（TCP）を通じて MSDP を実行し、他のドメイン内のマルチキャスト送信元を検出します。

PIM-SM ドメイン内の RP は、他のドメイン内の MSDP 対応デバイスと MSDP ピアリング関係にあります。ピアリング関係は TCP 接続を通じて発生します。主に、マルチキャスト グループを送信する送信元のリストを交換します。RP 間の TCP 接続は、基本的なルーティング システムによって実現されます。受信側の RP では、送信元リストを使用して送信元のパスが確立されます。

このトポロジの目的は、ドメインから、他のドメイン内のマルチキャスト送信元を検出することです。マルチキャスト送信元がレシーバーのあるドメインを対象としている場合、マルチキャスト データは PIM-SM の通常の送信元ツリー構築メカニズムを通じて配信されます。MSDP は、グループを送信する送信元のアナウンスにも使用されます。これらのアナウンスは、ドメインの RP で発信する必要があります。

MSDP のドメイン間動作は、Border Gateway Protocol（BGP）または MBGP に大きく依存します。ドメイン内の RP（インターネットへのアナウンス対象であるグローバル グループを送信する送信元用の RP）で、MSDP を実行してください。

MSDP の動作

送信元が最初のマルチキャスト パケットを送信すると、送信元に直接接続された先頭ホップ ルータ（指定ルータまたは RP）によって RP に PIM 登録メッセージが送信されます。RP は登録メッセージを使用し、アクティブな送信元を登録したり、ローカル ドメイン内の共有ツリーの下方向にマルチキャスト パケットを転送します。MSDP が設定されている場合は、Source-Active（SA）メッセージも、すべての MSDP ピアに転送します。送信元、送信元からの送信先であるグループ、および RP のアドレスまたは発信元 ID（RP アドレスとして使用されるインターフェイスの IP アドレス）が設定されている場合は、SA メッセージによってこれらが識別されます。

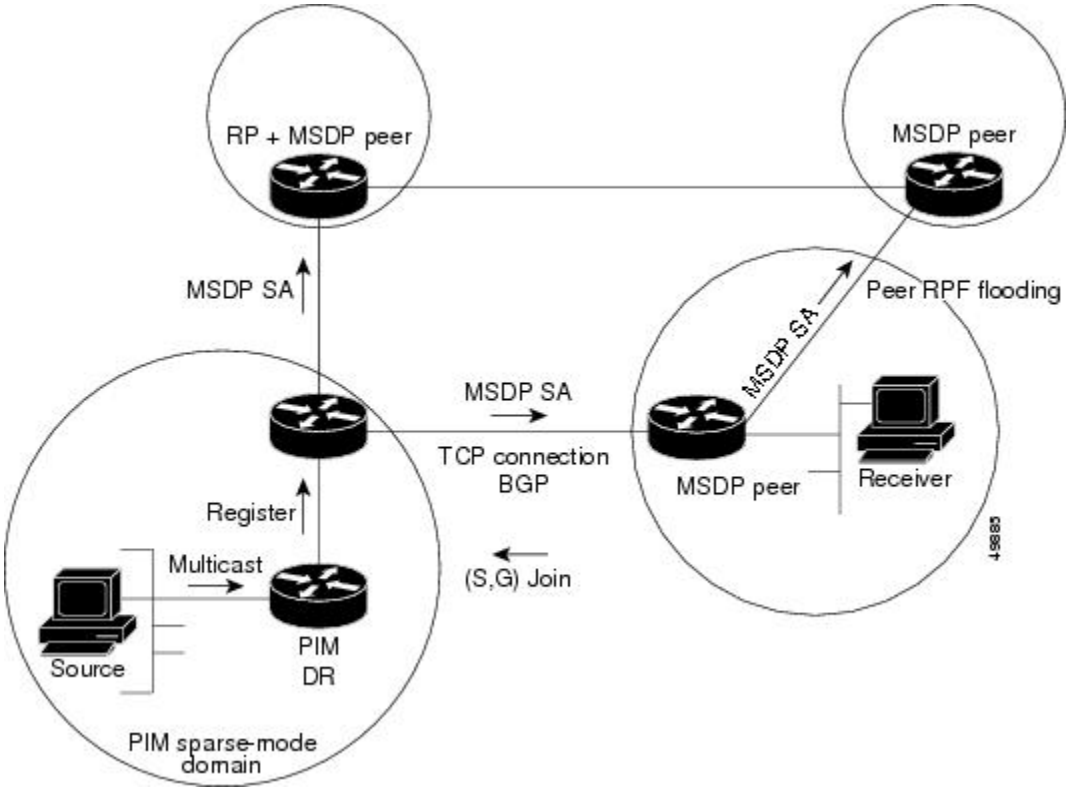
各 MSDP ピアは SA メッセージを発信元の RP から受信して転送し、ピア Reverse-Path Forwarding（RPF）フラッディングを実現します。MSDP デバイスは、BGP または MBGP ルーティング テーブルを調べ、どのピアが SA メッセージの発信元 RP へのネクスト ホップであるかを検出します。このようなピアは *RPF* ピアと呼ばれます。MSDP デバイスでは、RPF ピア以外のすべての MSDP ピアにメッセージが転送されます。BGP および MBGP がサポートされていない場合に MSDP を設定する方法については、デフォルトの MSDP ピアの設定, （1082 ページ）を参照してください。

MSDP ピアは、非 RPF ピアから発信元 RP へ向かう同じ SA メッセージを受信すると、そのメッセージをドロップします。それ以外の場合、すべての MSDP ピアにメッセージが転送されます。

ドメインの RP ピアは MSDP ピアから SA メッセージを受信します。この RP が SA メッセージに記述されているグループへの加入要求を持ち、空でない発信インターフェイス リストに（*,G）エントリが含まれている場合、そのグループはドメインの対象となり、RP から送信元方向に（S,G）Join メッセージが送信されます。（S,G）Join メッセージが送信元の DR に到達してからは、送信元からリモート ドメイン内の RP への送信元ツリーのブランチが構築されています。この結果、マルチキャスト トラフィックを送信元から送信元ツリーを経由して RP へ、そしてリモート ドメイン内の共有ツリーを下ってレシーバへと送信できます。

この図に、2 つの MSDP ピアの間での MSDP の動作を示します。PIM では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP が使用されます。MSDP が設定されている場合は、次のシーケンスが発生します。

図 *55*：*RP* ピア間で動作する *MSDP*



デフォルトでは、スイッチで受信された SA メッセージ内の送信元やグループのペアは、キャッシュに格納されません。また、MSDP SA 情報が転送される場合、この情報はメモリに格納されません。したがって、ローカル RP で SA メッセージが受信された直後にメンバーがグループに加入した場合、そのメンバーは、その次の SA メッセージによって送信元に関する情報が取得されるまで、待機する必要があります。この遅延は加入遅延と呼ばれます。

ローカル RP では、SA 要求を送信し、指定されたグループに対するすべてのアクティブな送信元の要求をすぐに取得できます。デフォルトでは、新しいメンバーがグループに加入してマルチキャスト トラフィックを受信する必要が生じた場合、スイッチは MSDP ピアに SA 要求メッセージを送信しません。新しいメンバーは次の定期的な SA メッセージを受信する必要があります。

グループへの送信元である接続 PIM SM ドメイン内のアクティブなマルチキャスト送信元を、グループの新しいメンバーが学習する必要がある場合は、新しいメンバーがグループに加入したときに、指定された MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定します。

MSDP の利点

MSDP には次の利点があります。

- 共有されたマルチキャスト配信ツリーが分割され、共有ツリーがドメインに対してローカルになるように設定できます。ローカル メンバーはローカル ツリーに加入します。共有ツリーへの Join メッセージはドメインから脱退する必要はありません。
- PIM SM ドメインは独自の RP だけを信頼するため、他のドメインの RP に対する信頼度が低下します。このため、送信元の情報がドメイン外部に漏れないようにでき、セキュリティが高まります。
- レシーバーだけが配置されているドメインは、グループ メンバーシップをグローバルにアドバタイズしなくても、データを受信できます。
- グローバルな送信元マルチキャスト ルーティング テーブル ステートが不要になり、メモリが削減されます。

MSDP の設定方法

MSDP のデフォルト設定

MSDP はイネーブルになっていません。デフォルトの MSDP ピアはありません。

デフォルトの MSDP ピアの設定

はじめる前に

MSDP ピアを設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp default-peer***ip-address* | *name* [**prefix-list***list*] 例： Router(config)# **ip msdp default-peer 10.1.1.1 prefix-list site-a**	すべての MSDP SA メッセージの受信元となるデフォルト ピアを定義します。 • *ip-address* | *name* には、MSDP デフォルト ピアの IP アドレスまたはドメイン ネーム システム（DNS）サーバ名を入力します。 •（任意）**prefix-list***list* を指定する場合は、リスト内のプレフィックス専用のデフォルト ピアとなるピアを指定するリスト名を入力します。プレフィックス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。 **prefix-list** キーワードが指定された **ip msdp default-peer** コマンドを複数入力すると、複数の RP プレフィックスに対してすべてのデフォルト ピアが同時に使用されます。この構文は通常、スタブ サイト クラウドに接続されたサービス プロバイダー クラウドで使用されます。 **prefix-list** キーワードを指定せずに **ip msdp default-peer** コマンドを複数入力すると、単一のアクティブ ピアですべての SA メッセージが受信されます。このピアに障害がある場合は、次の設定済みデフォルト ピアですべての SA メッセージが受信されます。この構文は通常、スタブ サイトで使用されます。
ステップ 4	**ip prefix-list***name* [**description***string*] | **seq***number* {**permit** | **deny**} *networklength* 例： Router(config)# **prefix-list site-a seq 3 permit 12 network length 128**	（任意）ステップ 2 で指定された名前を使用し、プレフィックス リストを作成します。 •（任意）**description***string* には、このプレフィックス リストを説明する 80 文字以下のテキストを入力します。 • **seq***number* には、エントリのシーケンス番号を入力します。指定できる範囲は 1 ～ 4294967294 です。 • **deny** キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。 • **permit** キーワードを指定すると、条件が一致した場合にアクセスが許可されます。 • *network length* には、許可または拒否されているネットワークの番号およびネットワーク マスク長（ビット単位）を指定します。

	コマンドまたはアクション	目的
ステップ 5	**ip msdp description** {*peer-name* | *peer-address*} *text* 例： `Router(config)# ip msdp description peer-name site-b`	（任意）設定内で、または **show** コマンド出力内で簡単に識別できるように、指定されたピアの説明を設定します。 デフォルトでは、MSDP ピアに説明は関連付けられていません。
ステップ 6	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SA ステートのキャッシング

メモリを消費して送信元情報の遅延を短縮する場合は、SA メッセージをキャッシュに格納するようにスイッチを設定できます。送信元とグループのペアのキャッシングをイネーブルにするには、次の手順を実行します。

送信元とグループのペアのキャッシングをイネーブルにするには、次の手順に従います。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp cache-sa-state** [**list***access-list-number*] 例： スイッチ(config)# **ip msdp cache-sa-state 100**	送信元とグループのペアのキャッシングをイネーブルにします（SA ステートを作成します）。アクセス リストを通過したこれらのペアがキャッシュに格納されます。 **list***access-list-number* を指定する場合、範囲は 100 ～ 199 です。 （注） このコマンドの代わりに、**ip msdp sa-reques** グローバル コンフィギュレーション コマンドを使用できます。この代替コマンドを使用すると、グループの新しいメンバがアクティブになった場合に、SA 要求メッセージがスイッチから MSDP ピアに送信されます。
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *protocolsourcesource-wildcarddestination destination-wildcard* 例： スイッチ(config)# **access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255**	IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* の範囲は 100 ～ 199 です。ステップ 2 で作成した番号と同じ値を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

MSDP ピアからの送信元情報の要求

グループへの送信元である接続 PIM SM ドメイン内のアクティブなマルチキャスト送信元を、グループの新しいメンバが学習する必要がある場合は、新しいメンバがグループに加入したときに、指定された MSDP ピアに SA 要求メッセージがスイッチから送信されるようにこのタスクを実行します。ピアは SA キャッシュ内の情報に応答します。ピアにキャッシュが設定されていない場合、このコマンドを実行しても何も起こりません。この機能を設定すると加入遅延は短縮されますが、メモリが消費されます。

新しいメンバがグループに加入し、マルチキャスト トラフィックを受信する必要が生じた場合、MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp sa-request** {*ip-address* | *name*} 例： スイッチ(config)# **ip msdp sa-request 171.69.1.1**	指定された MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定します。 *ip-address* | *name* を指定する場合は、グループの新しいメンバがアクティブになるときにローカル スイッチの SA メッセージの要求元になる MSDP ピアの IP アドレス、または名前を入力します。 SA メッセージを送信する必要がある MSDP ピアごとに、このコマンドを繰り返します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチから発信される送信元情報の制御

スイッチから発信されるマルチキャスト送信元情報を制御できます。

- アドバタイズ対象の送信元（送信元ベース）
- 送信元情報のレシーバー（要求元認識ベース）

詳細については、送信元の再配信，（1088 ページ）およびSA 要求メッセージのフィルタリング，（1090 ページ）を参照してください。

送信元の再配信

SA メッセージは、送信元が登録されている RP で発信されます。デフォルトでは、RP に登録されているすべての送信元がアドバタイズされます。送信元が登録されている場合は、RP に*A* フラグが設定されています。このフラグは、フィルタリングされる場合を除き、送信元が SA に格納されてアドバタイズされることを意味します。

アドバタイズされる登録済みの送信元をさらに制限するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp redistribute** [**list***access-list-name*] [**asn***aspath-access-list-number*] [**route-map***map*] 例： `スイッチ(config)# ip msdp redistribute list 21`	SA メッセージに格納されてアドバタイズされる、マルチキャスト ルーティング テーブル内の（S, G）エントリを設定します。 デフォルトでは、ローカル ドメイン内の送信元だけがアドバタイズされます。 • （任意）**list***access-list-name*：IP 標準または IP 拡張アクセス リストの名前または番号を入力します。標準アクセス リストの範囲は 1 ～ 99、拡張アクセス リストの範囲は 100 ～ 199 です。アクセス リストによって、アドバタイズされるローカルな送信元、および送信されるグループが制御されます。 • （任意）**asn***aspath-access-list-number*：1 ～ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、**ip as-path access-list** コマンドでも設定する必要があります。 • （任意）**route-map***map*：1 ～ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、**ip as-path access-list** コマンドでも設定する必要があります。

	コマンドまたはアクション	目的
		アクセス リストまたは自律システム パス アクセス リストに従って、スイッチが（S, G）ペアをアドバタイズします。

ステップ 4	次のいずれかを使用します。
	• **access-list***access-list-number* {**deny**| **permit**} *source* [*source-wildcard*]
	• **access-list***access-list-number* {**deny**| **permit**} *protocol source source-wildcard destination destination-wildcard*
	例：
	`スイッチ(config)# access list 21 permit 194.1.22.0`
	または
	`スイッチ(config)# access list 21 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1`
		IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。
		または
		IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。
		• *access-list-number*：ステップ 2 で作成した同じ番号を入力します。標準アクセス リストの範囲は 1 ～ 99、拡張アクセス リストの範囲は 100 ～ 199 です。
		• **deny**：条件に合致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。
		• *protocol*：プロトコル名として **ip** を入力します。
		• *source*：パケットの送信元であるネットワークまたはホストの番号を入力します。
		• *source-wildcard*：送信元に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。
		• *destination*：パケットの宛先であるネットワークまたはホストの番号を入力します。
		• *destination-wildcard*：宛先に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。
		アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

ステップ 5	**end** **例**： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** **例**： `スイッチ# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SA 要求メッセージのフィルタリング

デフォルトでは、SA 情報をキャッシングしているスイッチだけが、SA 要求に応答できます。このようなスイッチでは、デフォルトでMSDP ピアからのすべてのSA要求メッセージが採用され、アクティブな送信元の IP アドレスが取得されます。

ただし、MSDP ピアからの SA 要求をすべて無視するように、スイッチを設定できます。標準アクセス リストに記述されたグループのピアからの SA 要求メッセージだけを採用することもできます。アクセス リスト内のグループが指定された場合は、そのグループのピアからのSA要求メッセージが受信されます。他のグループのピアからの他のメッセージは、すべて無視されます。

デフォルト設定に戻すには、**no ip msdp filter-sa-request** {*ip-address*| *name*} グローバル コンフィギュレーション コマンドを使用します。

これらのオプションのいずれかを設定するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **ip msdp filter-sa-request** {*ip-address*| *name*}	指定されたMSDP ピアからのSA要求メッセージをすべてフィルタリングします。 または

	コマンドまたはアクション	目的
	• **ip msdp filter-sa-request** {*ip-address*| *name*} **list***access-list-number* 例： スイッチ(config)# **ip msdp filter sa-request 171.69.2.2**	標準アクセス リストを通過したグループに対して、指定された MSDP ピアからの SA 要求メッセージをフィルタリングします。アクセス リストには、複数のグループ アドレスが記述されています。access-list-number の範囲は 1 ～ 99 です。
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： スイッチ(config)# **access-list 1 permit 192.4.22.0 0.0.0.255**	IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチで転送される送信元情報の制御

デフォルトでは、スイッチで受信されたすべての SA メッセージが、すべての MSDP ピアに転送されます。ただし、フィルタリングするか、または存続可能時間（TTL）値を設定し、発信メッセージがピアに転送されないようにできます。

フィルタの使用法

フィルタを作成すると、次のいずれかの処理を実行できます。

- すべての送信元とグループのペアのフィルタリング
- 特定の送信元とグループのペアだけが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **ip msdp sa-filter out** {*ip-address*| *name*} • **ip msdp sa-filter out** {*ip-address*| *name*} **list***access-list-number*	• 指定された MSDP ピアへの SA メッセージをフィルタリングします。 • 指定したピアに対する IP 拡張アクセス リストを通過した SA メッセージのみを渡します。拡張アクセスリスト番号の範囲は 100 ～ 199 です。 **list** と **route-map** の両方のキーワードを使用すると、すべての条件に一致しなければ、発信 SA メッセージ内のいずれの（S,G）ペアも通過できません。

	コマンドまたはアクション	目的
	• **ip msdp sa-filter out** {*ip-address*| *name*} **route-map***map-tag* 例： スイッチ(config)# **ip msdp sa-filter out switch.cisco.com** または スイッチ(config)# **ip msdp sa-filter out list 100** または スイッチ(config)# **ip msdp sa-filter out switch.cisco.com route-map 22**	• 指定された MSDP ピアへのルート マップ *map-tag* で一致基準を満たす SA メッセージのみを渡します。 すべての一致条件を満たす場合、ルートマップに **permit** が指定されていれば、ルートはフィルタを通過します。**deny** が指定されていれば、ルートはフィルタリングされます。
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *protocolsourcesource-wildcarddestination destination-wildcard* 例： スイッチ(config)# **access list 100 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1**	（任意）IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカードビットをドット付き10進表記で入力します。無視するビット位置には 1 を設定します。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカードビットをドット付き10進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限

TTL 値を使用して、各送信元の最初の SA メッセージにカプセル化されるデータを制御できます。IP ヘッダー TTL 値が *ttl* 引数以上であるマルチキャスト パケットだけが、指定された MSDP ピアに送信されます。たとえば、内部トラフィックの TTL 値を 8 に制限できます。他のグループを外部に送信する場合は、これらのパケットの TTL を 8 より大きく設定して送信する必要があります。

TTL しきい値を確立するには、次の手順に従います。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp ttl-threshold** {*ip-address* | *name*} *ttl* 例： スイッチ(config)# **ip msdp ttl-threshold switch.cisco.com 0**	指定された MSDP ピア宛ての最初の SA メッセージにカプセル化されるマルチキャスト データを制限します。 • *ip-address* | *name* には、TTL の制限が適用される MSDP ピアの IP アドレスまたは名前を入力します。 • *ttl* には、TTL 値を入力します。デフォルトは 0 です。この場合、すべてのマルチキャスト データ パケットは、TTL がなくなるまでピアに転送されます。指定できる範囲は 0 ～ 255 です。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチで受信される送信元情報の制御

デフォルトでは、スイッチは、MSDP の RPF ピアによって送信されたすべての SA メッセージを受信します。ただし、着信 SA メッセージをフィルタリングし、MSDP ピアから受信する送信元情報を制御できます。つまり、特定の着信 SA メッセージを受信しないようにスイッチを設定できます。

次のいずれかの処理を実行できます。

- MSDP ピアからのすべての着信 SA メッセージのフィルタリング
- 特定の送信元とグループのペアが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **ip msdp sa-filter in** {*ip-address*| *name*} • **ip msdp sa-filter in** {*ip-address*| *name*} **list***access-list-number* • **ip msdp sa-filter in** {*ip-address*| *name*} **route-map***map-tag* 例： スイッチ(config)# **ip msdp sa-filter in switch.cisco.com** または スイッチ(config)# **ip msdp sa-filter in list 100**	• 指定された MSDP ピアへの SA メッセージをフィルタリングします。 • IP 拡張アクセス リストを通過する、指定されたピアからの SA メッセージのみを通過させます。拡張アクセス リスト *access-list-number* の範囲は 100 ～ 199 です。 **list** と **route-map** の両方のキーワードを使用すると、すべての条件に一致しなければ、発信SAメッセージ内のいずれの（S,G）ペアも通過できません。 • ルート マップ *map-tag* 内の一致条件を満たす、指定された MSDP ピアからの SA メッセージのみを通過させます。 すべての一致条件を満たす場合、ルート マップに **permit** が指定されていれば、ルートはフィルタを通過します。**deny** が指定されていれば、ルートはフィルタリングされます。

	コマンドまたはアクション	目的
	または スイッチ(config)# **ip msdp sa-filter in switch.cisco.com route-map 22**	
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *protocolsourcesource-wildcarddestination destination-wildcard* 例： スイッチ(config)# **access list 100 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1**	（任意）IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *Access-list-number* には、ステップ 2 で指定した番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

MSDP メッシュ グループの設定

MSDP メッシュ グループは、MSDP によって完全なメッシュ型に相互接続された MSDP スピーカーのグループです。メッシュ グループ内のピアから受信された SA メッセージは、同じメッシュ グループ内の他のピアに転送されません。したがって、SA メッセージのフラッディングが削減され、ピア RPF フラッディングが簡素化されます。ドメイン内に複数の RP がある場合は、**ip msdp mesh-group** グローバル コンフィギュレーション コマンドを使用します。特に、ドメインを越えて SA メッセージを送信する場合に使用します。単一のスイッチに複数のメッシュ グループを（異なる名前で）設定できます。

メッシュ グループを作成するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp mesh-group***name* {*ip-address* | *name*} 例： スイッチ(config)# **ip msdp mesh-group 2 switch.cisco.com**	MSDP メッシュ グループを設定し、そのメッシュ グループに属する MSDP ピアを指定します。 デフォルトでは、MSDP ピアはメッシュ グループに属しません。 • *name* には、メッシュ グループの名前を入力します。

	コマンドまたはアクション	目的
		• *ip-address* | *name* には、メッシュ グループのメンバーになる MSDP ピアの IP アドレスまたは名前を入力します。 グループ内の MSDP ピアごとに、この手順を繰り返します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MSDP ピアのシャットダウン

複数の MSDP コマンドが設定された単一のピアをアクティブにしない場合は、ピアをシャットダウンしてから、あとで起動できます。ピアがシャットダウンすると、TCP 接続が終了し、再起動されません。ピアの設定情報を保持したまま、MSDP セッションをシャットダウンすることもできます。

ピアをシャットダウンするには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp shutdown** {*peer-name* | *peer address*} 例： スイッチ(config)# **ip msdp shutdown switch.cisco.com**	設定情報を保持したまま、指定された MSDP ピアをシャットダウン状態にします。 *peer-name* | *peer address* を指定する場合は、シャットダウンする MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

境界 PIM デンス モード領域の MSDP への包含

デンス モード（DM）領域と PIM スパース モード（SM）領域の境界となるスイッチに MSDP を設定します。デフォルトでは、DM 領域のアクティブな送信元は MSDP に加入しません。

（注） **ip msdp border sa-address** グローバル コンフィギュレーション コマンドの使用は推奨できません。DM ドメイン内の送信元が SM ドメイン内の RP にプロキシ登録されるように SM ドメイン内の境界ルータを設定し、標準 MSDP 手順でこれらの送信元をアドバタイズするように SM ドメインを設定してください。

ip msdp originator-id グローバル コンフィギュレーション コマンドを実行すると、RP アドレスとして使用されるインターフェイスも識別されます。**ip msdp border sa-address** と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスが RP アドレスを指定します。

DM 領域でアクティブな送信元の SA メッセージを MSDP ピアに送信するように境界ルータを設定するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp border sa-address***interface-id* 例： `スイッチ(config)# ip msdp border sa-address 0/1`	DM 領域内のアクティブな送信元に関する SA メッセージを送信するように、DM 領域と SM 領域の境界スイッチを設定します。 *interface-id* には、SA メッセージ内の RP アドレスとして使用される、IP アドレスの配信元となるインターフェイスを指定します。 インターフェイスの IP アドレスは、SA メッセージ内の RP フィールド [Originator-ID] の値として使用されます。
ステップ 4	**ip msdp redistribute** [**list***access-list-name*] [**asn***aspath-access-list-number*] [**route-map***map*] 例： `スイッチ(config)# ip msdp redistribute list 100`	SA メッセージに格納されてアドバタイズされる、マルチキャスト ルーティング テーブル内の（S, G）エントリを設定します。 詳細については、送信元の再配信，（1088 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RP アドレス以外の発信元アドレスの設定

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用する場合は、送信元 ID を変更します。次のいずれかの場合に送信元 ID を変更できます。

- MSDP メッシュ グループ内の複数のスイッチ上で、論理 RP を設定する場合。
- PIM SM ドメインと DM ドメインの境界となるスイッチがある場合。サイトの DM ドメインの境界となるスイッチがあり、SM がその外部で使用されている場合は、DM の送信元を外部に通知する必要があります。このスイッチは RP でないため、SA メッセージで使用される RP アドレスはありません。したがって、このコマンドではインターフェイスのアドレスを指定し、RP アドレスを提供します。

ip msdp bordersa-address と **ip msdp originator-id** グローバル コンフィギュレーション コマンドの両方が設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスが RP アドレスを指定します。

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用できるようにするには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp originator-id***interface-id* 例： スイッチ(config)# **ip msdp originator-id 0/1**	発信元デバイスのインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。 *Interface-id* には、ローカルスイッチのインターフェイスを指定します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MSDP のモニタリングおよびメンテナンス

MSDP SA メッセージ、ピア、状態、ピアのステータスをモニタするコマンドは以下のとおりです。

表 *71*：***MSDP*** のモニタおよびメンテナンスのためのコマンド

コマンド	目的
debug ip msdp [*peer-address* | *name*] [**detail**] [**routes**]	MSDP アクティビティをデバッグします。
debug ip msdp resets	MSDP ピアのリセット原因をデバッグします。
show ip msdp count [*autonomous-system-number*]	SA メッセージに格納され、各自律システムから発信された送信元およびグループの個数を表示します。**ip msdp cache-sa-state** コマンドは、このコマンドによって出力が生成されるように設定する必要があります。
show ip msdp peer [*peer-address* | *name*]	MSDP ピアに関する詳細情報を表示します。
show ip msdp sa-cache [*group-address* | *source-address* | *group-name* | *source-name*] [*autonomous-system-number*]	MSDP ピアから学習した（S,G）ステートを表示します。
show ip msdp summary	MSDP ピア ステータスおよび SA メッセージ数を表示します。

MSDP 接続、統計情報、SA キャッシュ エントリをクリアするコマンドは以下のとおりです。

表 *72*：***MSDP*** 接続、統計情報、または ***SA*** キャッシュ エントリをクリアするためのコマンド

コマンド	目的
clear ip msdp peer*peer-address* | *name*	指定された MSDP ピアへの TCP 接続をクリアし、すべての MSDP メッセージ カウンタをリセットします。
clear ip msdp statistics [*peer-address* | *name*]	セッションをリセットせずに、1 つまたはすべての MSDP ピア統計情報カウンタをクリアします。
clear ip msdp sa-cache [*group-address* | *name*]	すべてのエントリの SA キャッシュ エントリ、特定のグループのすべての送信元、または特定の送信元とグループのペアのすべてのエントリをクリアします。

MSDP の設定例

デフォルト MSDP ピアの設定：例

次に、ルータ A およびルータ C の部分的な設定の例を示します。これらの ISP にはそれぞれに複数のカスタマー（カスタマーと同様）がおり、 デフォルトのピアリング（BGP または MBGP なし）を使用しています。この場合、両方の ISP で類似した設定となります。つまり、両方の ISP では、対応するプレフィックス リストで SA が許可されている場合、デフォルト ピアからの SA だけが受信されます。

ルータ A

```
Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

ルータ C

```
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

SA ステートのキャッシング：例

次に、グループ 224.2.0.0/16 への送信元である 171.69.0.0/16 のすべての送信元のキャッシュ ステートをイネーブルにする例を示します。

```
スイッチ(config)# ip msdp cache-sa-state 100
スイッチ(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

MSDP ピアからの送信元情報の要求：例

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定する例を示します。

```
スイッチ(config)# ip msdp sa-request 171.69.1.1
```

スイッチから発信される送信元情報の制御：例

次に、171.69.2.2 の MSDP ピアからの SA 要求メッセージをフィルタリングするように、スイッチを設定する例を示します。ネットワーク 192.4.22.0 の送信元からの SA 要求メッセージはアクセス リスト 1 に合格して、受信されます。その他のすべてのメッセージは無視されます。

```
スイッチ(config)# ip msdp filter sa-request 171.69.2.2 list 1
スイッチ(config)# access-list 1 permit 192.4.22.0 0.0.0.255
```

スイッチから転送される送信元情報の制御：例

次に、アクセスリスト100を通過する（S,G）ペアだけがSAメッセージに格納され、*switch.cisco.com* という名前のピアに転送されるように設定する例を示します。

```
スイッチ(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
スイッチ(config)# ip msdp sa-filter out switch.cisco.com list 100
スイッチ(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

スイッチで受信される送信元情報の制御：例

次に、*switch.cisco.com* という名前のピアからのすべてのSAメッセージをフィルタリングする例を示します。

```
スイッチ(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
スイッチ(config)# ip msdp sa-filter in switch.cisco.com
```

第 54 章

IP ユニキャスト ルーティングの設定

- 機能情報の確認，1108 ページ
- IP ユニキャスト ルーティングの設定に関する情報，1108 ページ
- IP ルーティングに関する情報，1109 ページ
- IP ルーティングの設定方法，1117 ページ
- IP アドレッシングの設定方法，1118 ページ
- IP アドレスのモニタリングおよびメンテナンス，1139 ページ
- IP ユニキャスト ルーティングの設定方法，1140 ページ
- RIP 情報，1142 ページ
- RIP の設定方法，1143 ページ
- サマリー アドレスおよびスプリット ホライズンの設定例，1151 ページ
- OSPF に関する情報，1152 ページ
- OSPF の設定方法，1156 ページ
- OSPF のモニタリング，1168 ページ
- OSPF の設定例，1169 ページ
- EIGRP に関する情報，1169 ページ
- EIGRP の設定方法，1174 ページ
- EIGRP のモニタリングおよびメンテナンス，1181 ページ
- BGP に関する情報，1182 ページ
- BGP の設定方法，1191 ページ
- BGP のモニタリングおよびメンテナンス，1217 ページ
- BGP の設定例，1218 ページ

- ISO CLNS ルーティングに関する情報，1219 ページ
- ISO CLNS ルーティングの設定方法，1223 ページ
- ISO IGRP と IS-IS のモニタリングおよびメンテナンス，1233 ページ
- ISO CLNS ルーティングの設定例，1235 ページ
- Multi-VRF CE に関する情報，1236 ページ
- Multi-VRF CE の設定方法，1240 ページ
- Multi-VRF CE の設定例，1258 ページ
- ユニキャスト リバース パス転送の設定，1261 ページ
- プロトコル独立機能，1262 ページ
- IP ネットワークのモニタリングおよびメンテナンス，1288 ページ

機能情報の確認

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

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

IP ユニキャスト ルーティングの設定に関する情報

このモジュールでは、スイッチで IP Version 4（IPv4）ユニキャスト ルーティングを設定する方法について説明します。

スイッチ スタックは、ネットワーク内のそれ以外のルータに対して、単一のルータとして動作し、認識されます。スタティック ルーティングなどの基本的なルーティング機能は、で使用できます。拡張ルーティング機能およびその他のルーティング プロトコルを使用するには、スタンドアロン スイッチやアクティブ スイッチで IP サービス フィーチャ セットをイネーブルにする必要があります。

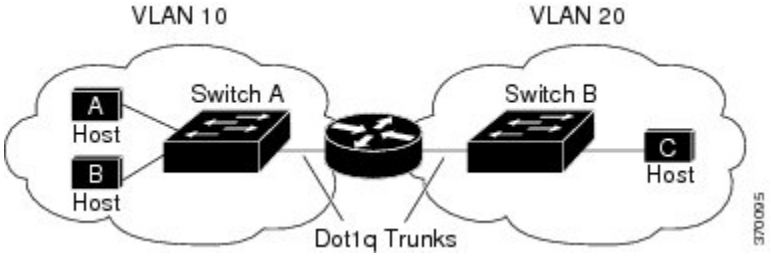
（注） IPv4 トラフィックに加えて、IP バージョン 6（IPv6）ユニキャストルーティングをイネーブルにし、IPv6 トラフィックを転送するようにインターフェイスを設定できます。

IP ルーティングに関する情報

一部のネットワーク環境で、VLAN（仮想 LAN）は各ネットワークまたはサブネットワークに関連付けられています。IP ネットワークで、各サブネットワークは 1 つの VLAN に対応しています。VLAN を設定すると、ブロードキャスト ドメインのサイズを制御し、ローカル トラフィックをローカル内にとどめることができます。ただし、異なる VLAN 内のネットワーク デバイスが相互に通信するには、VLAN 間でトラフィックをルーティング（VLAN 間ルーティング）するレイヤ 3 デバイス（ルータ）が必要です。VLAN 間ルーティングでは、適切な宛先 VLAN にトラフィックをルーティングするため、1 つまたは複数のルータを設定します。

次の図に基本的なルーティング トポロジを示します。スイッチ A は VLAN 10 内、スイッチ B は VLAN 20 内にあります。ルータには各 VLAN のインターフェイスが備わっています。

図 *56*：ルーティング トポロジの例



VLAN 10 内のホスト A が VLAN 10 内のホスト B と通信する場合、ホスト A はホスト B 宛にアドレス指定されたパケットを送信します。スイッチ A はパケットをルータに送信せず、ホスト B に直接転送します。

ホスト A から VLAN 20 内のホスト C にパケットを送信する場合、スイッチ A はパケットをルータに転送し、ルータは VLAN 10 インターフェイスでトラフィックを受信します。ルータはルーティング テーブルを調べて正しい発信インターフェイスを判別し、VLAN 20 インターフェイスを経由してパケットをスイッチ B に送信します。スイッチ B はパケットを受信し、ホスト C に転送します。

ルーティング タイプ

ルータおよびレイヤ 3 スイッチは、次の方法でパケットをルーティングできます。

- デフォルト ルーティング
- 事前にプログラミングされているトラフィックのスタティック ルートの使用
- ルーティング プロトコルによるルートの動的な計算

デフォルト ルーティングとは、宛先がルータにとって不明であるトラフィックをデフォルトの出口または宛先に送信することです。

スタティック ユニキャスト ルーティングの場合、パケットは事前に設定されたポートから単一のパスを通り、ネットワークの内部または外部に転送されます。スタティック ルーティングは安全

で、帯域幅をほとんど使用しません。ただし、リンク障害などのネットワークの変更には自動的に対応しないため、パケットが宛先に到達しないことがあります。ネットワークが拡大するにつれ、スタティック ルーティングの設定は煩雑になります。

LAN ベース フィーチャ セットを実行しているスイッチは、管理インターフェイスで使用するデフォルト ルートに加えて、ユーザが設定した 16 のスタティック ルートをサポートしています。LAN ベース イメージは、SVI でのみスタティック ルーティングをサポートしています。

ルータでは、トラフィックを転送する最適ルートを動的に計算するため、ダイナミック ルーティング プロトコルが使用されます。ダイナミック ルーティング プロトコルには次の 2 つのタイプがあります。

- ディスタンスベクトル プロトコルを使用するルータでは、ネットワーク リソースの距離の値を使用してルーティング テーブルを保持し、これらのテーブルをネイバーに定期的に渡します。ディスタンスベクトル プロトコルは 1 つまたは複数のメトリックを使用し、最適なルートを計算します。これらのプロトコルは、簡単に設定、使用できます。
- リンクステート プロトコルを使用するルータでは、ルータ間のリンクステート アドバタイズメント（LSA）の交換に基づき、ネットワーク トポロジに関する複雑なデータベースを保持します。LSA はネットワークのイベントによって起動され、コンバージェンス時間、またはこれらの変更への対応時間を短縮します。リンクステート プロトコルはトポロジの変更にすばやく対応しますが、ディスタンスベクトル プロトコルよりも多くの帯域幅およびリソースが必要になります。

スイッチでサポートされているディスタンスベクトル プロトコルは、Routing Information Protocol（RIP）および Border Gateway Protocol（BGP）です。RIP は最適パスを決定するために単一の距離メトリック（コスト）を使用し、BGP はパス ベクトル メカニズムを追加します。また、Open Shortest Path First（OSPF）リンクステート プロトコル、および従来の Interior Gateway Routing Protocol（IGRP）にリンクステート ルーティング機能の一部を追加して効率化を図った Enhanced IGRP（EIGRP）もサポートされています。

（注） スイッチまたはスイッチ スタックでサポートされるプロトコルは、アクティブ スイッチ上で稼働しているソフトウェアによって決まります。アクティブ スイッチ上で IP ベース フィーチャ セットが稼働している場合は、デフォルトのルーティング、スタティック ルーティング、および RIP だけがサポートされます。スイッチで LAN ベース フィーチャ セットが稼働している場合、SVI では 16 のスタティック ルートを設定できます。その他のすべてのルーティング プロトコルには、IP サービス フィーチャ セットが必要です。

IP ルーティングおよびスイッチ スタック

スタックのスイッチがルーティング ピアに接続されているかどうかに関係なく、スイッチ スタックはネットワークからは単一のスイッチとして認識されます。

アクティブ スイッチにより、次の機能が実行されます。

- ルーティング プロトコルを初期化し、設定します。

- ルーティング プロトコル メッセージおよびアップデートを他のルータに送信します。
- ピア ルータから受信したルーティング プロトコル メッセージおよびアップデートを処理します。
- distributed Cisco Express Forwarding（dCEF）データベースを生成および維持し、すべてのスタック メンバーに配信します。このデータベースに基づいて、スタック内のすべてのスイッチにルートがプログラミングされます。
- アクティブ スイッチの MAC アドレスはスタック全体のルータ MAC アドレスとして使用され、すべての外部デバイスはこのアドレスを使用して IP パケットをスタックに送信します。
- ソフトウェア転送またはソフトウェア処理を必要とするすべての IP パケットは、アクティブ スイッチの CPU を通ります。

スタック メンバーは、次に示す機能を実行します。

- ルーティング スタンバイ スイッチとして機能します。アクティブ スイッチに障害が発生し、新規アクティブ スイッチとして選択された場合に、処理を引き継ぐことができます。
- ルートをハードウェアにプログラムします。

アクティブ スイッチに障害が発生すると、スタックはアクティブ スイッチがダウンしていることを検出し、スタック メンバの 1 つを新規アクティブ スイッチとして選択します。この期間中に、ハードウェアは一時的な中断を除き、アクティブなプロトコルがない状態でパケットの転送を継続します。

ただし、スイッチ スタックが障害のあとハードウェア ID を維持していても、アクティブ スイッチの再起動前の短い中断の間にルータ ネイバーのルーティング プロトコルがフラップすることがあります。OSPF や EIGRP などのルーティング プロトコルは、ネイバーの移行を認識する必要があります。ルータは、次の 2 つのレベルの Nonstop Forwarding（NSF）を使用して、スイッチオーバーの検出、ネットワーク トラフィックの転送の継続、およびピアデバイスから情報の回復を行います。

- NFS 認識ルータによるネイバー ルータ障害の許容。ネイバー ルータの再起動後、NFS 認識ルータは要求を受けて自身のステート情報とルートの隣接情報を提供します。
- NFS 対応ルータによる NSF のサポート。NSF 対応ルータは、アクティブ スイッチの変更を検出した場合、NFS 認識ネイバーまたは NSF 対応ネイバーからの情報でルーティング情報を再構築します。再起動を待つことはしません。

スイッチ スタックは NSF 対応ルーティングを OSPF および EIGRP に対してサポートします。

新規アクティブ スイッチは、選択されたときに次の機能を実行します。

- ルーティング アップデートの生成、受信、および処理を開始します。
- ルーティング テーブルを構築し、CEF データベースを生成して、スタック メンバーに配信します。

- ルータ MAC アドレスとして自身の MAC アドレスを使用します。新規 MAC アドレスのネットワーク ピアに通知するために、新規ルータ MAC アドレスを使用して余分の ARP 応答を定期的に（5 分間の間、数秒おきに）送信します。

（注） 固定 MAC アドレス機能をスタックに設定していて、アクティブ スイッチに変更があった場合、設定された時間スタック MAC アドレスは変更されません。この期間に前のアクティブ スイッチがメンバ スイッチとしてスタックに再加入する場合、スタック MAC アドレスは前のアクティブ スイッチの MAC アドレスのままになります。

- ARP 要求をプロキシ ARP IP アドレスに送信し、ARP 応答を受信して、各プロキシ ARP エントリの到達可能性を判別しようとします。到達可能なプロキシ ARP IP アドレスごとに、新規ルータ MAC アドレスを使用して gratuitous ARP 応答を生成します。このプロセスは、新規アクティブ スイッチが選択されたあと、5 分間繰り返されます。

（注） アクティブ スイッチが IP サービス フィーチャ セットを実行している場合は、スタックは、Open Shortest Path First（OSPF）、Enhanced IGRP（EIGRP）、およびを含む、サポートされるすべてのプロトコルを実行できます。アクティブ スイッチに障害が発生し、新規に選択されたアクティブ スイッチ上で IP ベースまたは LAN ベース フィーチャ セットが稼働している場合、これらのプロトコルはスタック内で稼働しなくなります。

注意 スイッチ スタックを複数のスタックに分割すると、ネットワークが適切に動作しなくなる場合があります。

スイッチがリロードされると、NSF/SSO 機能である場合でも、そのスイッチのポートがすべてダウンし、ルーティングに関わるインターフェイスにトラフィックの損失が発生します。

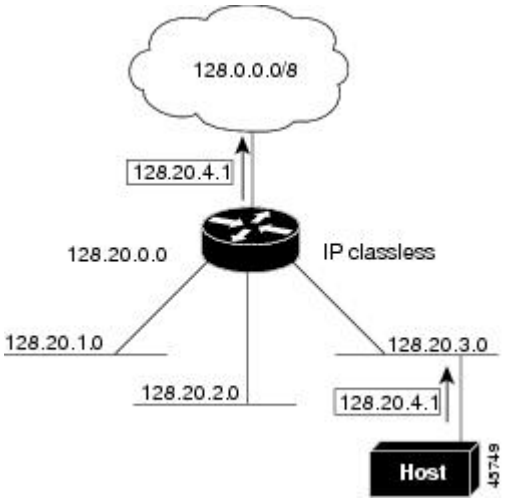
クラスレス ルーティング

ルーティングを行うように設定されたスイッチで、クラスレス ルーティング動作はデフォルトでイネーブルとなっています。クラスレスルーティングがイネーブルの場合、デフォルトルートがないネットワークのサブネット宛てパケットをルータが受信すると、ルータは最適なスーパーネット ルートにパケットを転送します。スーパーネットは、単一の大規模アドレス空間をシミュレートするために使用されるクラスCアドレス空間の連続ブロックで構成されています。スーパーネットは、クラス B アドレス空間の急速な枯渇を回避するために設計されました。

図では、クラスレス ルーティングがイネーブルとなっています。ホストがパケットを 128.20.4.1 に送信すると、ルータはパケットを廃棄せずに、最適なスーパーネット ルートに転送します。ク

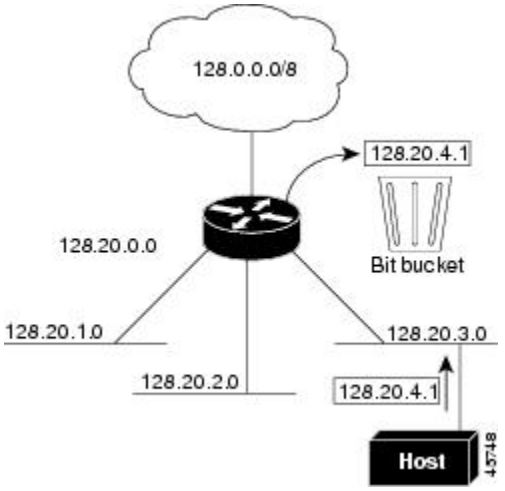
ラスレスルーティングがディセーブルの場合、デフォルトルートがないネットワークのサブネット宛てパケットを受信したルータは、パケットを廃棄します。

図 *57* : *IP* クラスレス ルーティングがイネーブルの場合



図では、ネットワーク 128.20.0.0 のルータはサブネット 128.20.1.0、128.20.2.0、128.20.3.0 に接続されています。ホストがパケットを 128.20.4.1 に送信した場合、ネットワークのデフォルト ルートが存在しないため、ルータはパケットを廃棄します。

図 *58* : *IP* クラスレス ルーティングがディセーブルの場合



スイッチが認識されないサブネット宛てのパケットを最適なスーパーネット ルートに転送しないようにするには、クラスレス ルーティング動作をディセーブルにします。

アドレス解決

インターフェイス固有の IP 処理方法を制御するには、アドレス解決を行います。IP を使用するデバイスには、ローカル セグメントまたは LAN 上のデバイスを一意に定義するローカル アドレス（MAC アドレス）と、デバイスが属するネットワークを特定するネットワーク アドレスがあります。

（注） スイッチスタックでは、スタックの単一のMACアドレスおよびIPアドレスを使用して、ネットワーク通信を行います。

ローカルアドレス（MAC アドレス）は、パケット ヘッダーのデータ リンク層（レイヤ 2）セクションに格納されて、データ リンク（レイヤ 2）デバイスによって読み取られるため、データ リンク アドレスと呼ばれます。ソフトウェアがイーサネット上のデバイスと通信するには、デバイスの MAC アドレスを学習する必要があります。IP アドレスから MAC アドレスを学習するプロセスを、アドレス解決と呼びます。MAC アドレスから IP アドレスを学習するプロセスを、逆アドレス解決と呼びます。

スイッチでは、次の形式のアドレス解決を行うことができます。

- ARP：IP アドレスを MAC アドレスと関連付けるために使用されます。ARP は IP アドレスを入力と解釈し、対応する MAC アドレスを学習します。次に、IP アドレス/MAC アドレス アソシエーションを ARP キャッシュにストアし、すぐに取り出せるようにします。その後、IP データグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化、および ARP 要求や応答については、サブネットワーク アクセス プロトコル（SNAP）で規定されています。
- プロキシ ARP：ルーティング テーブルを持たないホストで、他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにします。スイッチ（ルータ）が送信元と異なるインターフェイス上のホストに宛てた ARP 要求を受信した場合、そのルータに他のインターフェイスを経由してそのホストに至るすべてのルートが格納されていれば、ルータは自身のローカル データ リンク アドレスを示すプロキシ ARP パケットを生成します。ARP 要求を送信したホストはルータにパケットを送信し、ルータはパケットを目的のホストに転送します。

スイッチでは、ARP と同様の機能（ローカル MAC アドレスでなく IP アドレスを要求する点を除く）を持つ Reverse Address Resolution Protocol（RARP）を使用することもできます。RARP を使用するには、ルータ インターフェイスと同じネットワーク セグメント上に RARP サーバを設置する必要があります。サーバを識別するには、**ip rarp-server***address* インターフェイス コンフィギュレーション コマンドを使用します。

RARP の詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』を参照してください。

プロキシ ARP

プロキシ ARP は、他のルートを学習する場合の最も一般的な方法です。プロキシ ARP を使用すると、ルーティング情報を持たないイーサネット ホストと、他のネットワークまたはサブネット上のホストとの通信が可能になります。このホストでは、すべてのホストが同じローカル イーサネット上にあり、ARP を使用して MAC アドレスを学習すると想定されています。スイッチが送信元と異なるネットワーク上にあるホストに宛てた ARP 要求を受信した場合、スイッチはそのホストへの最適なルートがあるかどうかを調べます。最適なルートがある場合、スイッチはスイッチ自身のイーサネット MAC アドレスが格納された ARP 応答パケットを送信します。要求の送信元ホストはパケットをスイッチに送信し、スイッチは目的のホストにパケットを転送します。プロキシ ARP は、すべてのネットワークをローカルな場合と同様に処理し、IP アドレスごとに ARP 処理を実行します。

ICMP Router Discovery Protocol

ルータ ディスカバリを使用すると、スイッチは ICMP Router Discovery Protocol（IRDP）を使用し、他のネットワークへのルートを動的に学習します。ホストは IRDP を使用し、ルータを特定します。クライアントとして動作しているスイッチは、ルータ ディスカバリ パケットを生成します。ホストとして動作しているスイッチは、ルータ ディスカバリ パケットを受信します。スイッチは Routing Information Protocol（RIP）ルーティングのアップデートを受信し、この情報を使用してルータの場所を推測することもできます。実際のところ、ルーティング デバイスによって送信されたルーティング テーブルは、スイッチにストアされません。どのシステムがデータを送信しているのかが記録されるだけです。IRDP を使用する利点は、プライオリティと、パケットが受信されなくなってからデバイスがダウンしていると見なされるまでの期間の両方をルータごとに指定できることです。

検出された各デバイスは、デフォルト ルータの候補となります。現在のデフォルト ルータがダウンしたと宣言された場合、または再送信が多すぎて TCP 接続がタイムアウトになりつつある場合、プライオリティが上位のルータが検出されると、最も高いプライオリティを持つ新しいルータが選択されます。

UDP ブロードキャスト パケットおよびプロトコル

ユーザ データグラム プロトコル（UDP）は IP のホスト間レイヤ プロトコルで、TCP と同様です。UDP はオーバーヘッドが少ない、コネクションレスのセッションを 2 つのエンド システム間に提供しますが、受信されたデータグラムの確認応答は行いません。場合に応じてネットワーク ホストは UDP ブロードキャストを使用し、アドレス、コンフィギュレーション、名前に関する情報を検索します。このようなホストが、サーバを含まないネットワーク セグメント上にある場合、通常 UDP ブロードキャストは転送されません。この状況を改善するには、特定のクラスのブロードキャストをヘルパー アドレスに転送するように、ルータのインターフェイスを設定します。インターフェイスごとに、複数のヘルパー アドレスを使用できます。

UDP 宛先ポートを指定し、転送される UDP サービスを制御できます。複数の UDP プロトコルを指定することもできます。旧式のディスクレス Sun ワークステーションおよびネットワーク セキュリティ プロトコル SDNS で使用される Network Disk（ND）プロトコルも指定できます。

ヘルパー アドレスがインターフェイスに定義されている場合、デフォルトではUDP と ND の両方の転送がイネーブルになっています。『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』の **ip forward-protocol** インターフェイス コンフィギュレーション コマンドの説明には、UDP ポートを指定しない場合にデフォルトで転送されるポートがリストされています。

ブロードキャスト パケットの処理

IP インターフェイス アドレスを設定したあとで、ルーティングをイネーブルにしたり、1 つまたは複数のルーティング プロトコルを設定したり、ネットワーク ブロードキャストへのスイッチの応答方法を設定したりできます。ブロードキャストは、物理ネットワーク上のすべてのホスト宛てのデータ パケットです。スイッチでは、2 種類のブロードキャストがサポートされています。

- ダイレクト ブロードキャスト パケット：特定のネットワークまたは一連のネットワークに送信されます。ダイレクト ブロードキャスト アドレスには、ネットワークまたはサブネット フィールドが含まれます。
- フラッディング ブロードキャスト パケット：すべてのネットワークに送信されます。

（注） **storm-control** インターフェイス コンフィギュレーション コマンドを使用して、トラフィック抑制レベルを設定し、レイヤ 2 インターフェイスでブロードキャスト、ユニキャスト、マルチキャスト トラフィックを制限することもできます。

ルータはローカル ケーブルまでの範囲を制限して、ブロードキャスト ストームを防ぎます。ブリッジ（インテリジェントなブリッジを含む）はレイヤ 2 デバイスであるため、ブロードキャストはすべてのネットワーク セグメントに転送され、ブロードキャスト ストームを伝播します。ブロードキャスト ストーム問題を解決する最善の方法は、ネットワーク上で単一のブロードキャスト アドレス方式を使用することです。最新のIP実装機能ではほとんどの場合、アドレスをブロードキャスト アドレスとして使用するように設定できます。スイッチをはじめ、多数の実装機能では、ブロードキャスト メッセージを転送するためのアドレス方式が複数サポートされています。

IP ブロードキャストのフラッディング

IP ブロードキャストをインターネットワーク全体に、制御可能な方法でフラッディングできるようにするには、ブリッジング STP で作成されたデータベースを使用します。この機能を使用すると、ループを回避することもできます。この機能を使用できるようにするには、フラッディングが行われるインターフェイスごとにブリッジングを設定する必要があります。ブリッジングが設定されていないインターフェイス上でも、ブロードキャストを受信できます。ただし、ブリッジングが設定されていないインターフェイスでは、受信したブロードキャストが転送されません。また、異なるインターフェイスで受信されたブロードキャストを送信する場合、このインターフェイスは使用されません。

IPヘルパーアドレスのメカニズムを使用して単一のネットワークアドレスに転送されるパケットを、フラッディングできます。各ネットワーク セグメントには、パケットのコピーが 1 つだけ送信されます。

フラッディングを行う場合、パケットは次の条件を満たす必要があります（これらの条件は、IP ヘルパー アドレスを使用してパケットを転送するときの条件と同じです）。

- パケットは MAC レベルのブロードキャストでなければなりません。
- パケットは IP レベルのブロードキャストでなければなりません。
- パケットは Trivial File Transfer Protocol（TFTP）、ドメイン ネーム システム（DNS）、Time、NetBIOS、ND、または BOOTP パケット、または **ip forward-protocol udp** グローバル コンフィギュレーション コマンドで指定された UDP でなければなりません。
- パケットの存続可能時間（TTL）値は 2 以上でなければなりません。

フラッディングされた UDP データグラムには、出力インターフェイスで **ip broadcast-address** インターフェイス コンフィギュレーション コマンドによって指定された宛先アドレスが表示されます。宛先アドレスを、任意のアドレスに設定できます。このため、データグラムがネットワーク内に伝播されるにつれ、宛先アドレスが変更されることもあります。送信元アドレスは変更されません。TTL 値が減ります。

フラッディングされたUDPデータグラムがインターフェイスから送信されると（場合によっては宛先アドレスが変更される）、データグラムは通常のIP出力ルーチンに渡されます。このため、出力インターフェイスにアクセス リストがある場合、データグラムはその影響を受けます。

スイッチでは、パケットの大部分がハードウェアで転送され、スイッチのCPUを経由しません。CPU に送信されるパケットの場合は、ターボフラッディングを使用し、スパニングツリーベースの UDP フラッディングを約 4 ～ 5 倍高速化します。この機能は、ARP カプセル化用に設定されたイーサネット インターフェイスでサポートされています。

IP ルーティングの設定方法

スイッチ上で、IP ルーティングはデフォルトでディセーブルとなっているため、ルーティングを行う前に、IP ルーティングをイネーブルにする必要があります。IP ルーティングに関する設定情報については、『*Cisco IOS IP Configuration Guide*』を参照してください。

次の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。

- ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドを使用し、レイヤ 3 ポートとして設定された物理ポートです。
- スイッチ仮想インターフェイス（SVI）：**interface vlan***vlan_id* グローバル コンフィギュレーション コマンドによって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
- レイヤ 3 モードの Etherchannel ポート チャネル：**interface port-channel***port-channel-number* グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャネル グループにバインドして作成されたポートチャネル論理インターフェイスです。詳細に

ついては、『Layer 2 Configuration Guide』の「Configuring Layer 3 EtherChannels」の章を参照してください。

（注） スイッチは、ユニキャスト ルーテッド トラフィックのトンネル インターフェイスをサポートしません。

ルーティングが発生するすべてのレイヤ 3 インターフェイスに、IP アドレスを割り当てる必要があります。

（注） スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。

設定できるルーテッド ポートおよび SVI の個数は 128 に制限されています。推奨個数と実装されている機能の数量を超えると、ハードウェアによって制限されるため、CPU利用率が影響を受けることがあります。

ルーティングを設定するための主な手順は次のとおりです。

- VLAN インターフェイスをサポートするには、スイッチまたはスイッチ スタックで VLAN を作成および設定し、レイヤ 2 インターフェイスに VLAN メンバーシップを割り当てます。詳細については、『VLAN Configuration Guide』の「Configuring VLANs」の章を参照してください。
- レイヤ 3 インターフェイスを設定します。
- スイッチ上で IP ルーティングをイネーブルに設定します。
- レイヤ 3 インターフェイスに IP アドレスを割り当てます。
- 選択したルーティング プロトコルをスイッチ上でイネーブルにします。
- ルーティング プロトコル パラメータを設定します（任意）。

IP アドレッシングの設定方法

IP ルーティングを設定するには、レイヤ 3 ネットワーク インターフェイスに IP アドレスを割り当ててインターフェイスをイネーブルにし、IP を使用するインターフェイスを経由してホストとの通信を許可する必要があります。次の項では、さまざまな IP アドレス指定機能の設定方法について説明します。IP アドレスをインターフェイスに割り当てる手順は必須ですが、その他の手順は任意です。

- アドレス指定のデフォルト設定
- ネットワーク インターフェイスへの IP アドレスの割り当て
- アドレス解決方法の設定

- IP ルーティングがディセーブルの場合のルーティング支援機能
- ブロードキャスト パケットの処理方法の設定
- IP アドレスのモニタリングおよびメンテナンス

IP アドレス指定のデフォルト設定

表 *73*：アドレス指定のデフォルト設定

機能	デフォルト設定
IP アドレス	未定義
ARP	ARP キャッシュに永続的なエントリはありません カプセル化：標準イーサネット形式の ARP 14400 秒（4 時間）
IP ブロードキャスト アドレス	255.255.255.255（すべて 1）
IP クラスレス ルーティング	イネーブル
IP デフォルト ゲートウェイ	ディセーブル
IP ダイレクト ブロードキャスト	ディセーブル（すべての IP ダイレクト ブロードキャストがドロップされます）
IP ドメイン	ドメイン リスト：ドメイン名は未定義 ドメイン検索：イネーブル ドメイン名：イネーブル
IP 転送プロトコル	ヘルパー アドレスが定義されているか、またはユーザ データグラム プロトコル（UDP）フラッディングが設定されている場合、デフォルト ポートでは UDP 転送がイネーブルとなります ローカル ブロードキャスト：ディセーブル スパニングツリー プロトコル（STP）：ディセーブル ターボフラッディング：ディセーブル
IP ヘルパー アドレス	ディセーブル

機能	デフォルト設定
IP ホスト	ディセーブル
ICMP Router Discovery Protocol（IRDP）	ディセーブル イネーブルの場合のデフォルト： • ブロードキャスト IRDP アドバタイズメント • アドバタイズメント間の最大インターバル：600 秒 • アドバタイズ間の最小インターバル：最大インターバルの 0.75 倍 • プリファレンス：0
IP プロキシ ARP	イネーブル
IP ルーティング	ディセーブル
IP サブネットゼロ	ディセーブル

ネットワーク インターフェイスへの IP アドレスの割り当て

IP アドレスは IP パケットの送信先を特定します。一部の IP アドレスは特殊な目的のために予約されていて、ホスト、サブネット、またはネットワーク アドレスには使用できません。RFC 1166 の『Internet Numbers』には IP アドレスに関する公式の説明が記載されています。

インターフェイスには、1 つのプライマリ IP アドレスを設定できます。マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。マスクを使用してネットワークをサブネット化する場合、そのマスクをサブネット マスクと呼びます。割り当てられているネットワーク番号については、インターネット サービス プロバイダーにお問い合わせください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# interface gigabitethernet 1/0/1	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**no switchport** 例： スイッチ(config-if)# no switchport	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 5	**ip address***ip-address subnet-mask* 例： スイッチ(config-if)# ip address 10.1.5.1 255.255.255.0	IP アドレスおよび IP サブネット マスクを設定します。
ステップ 6	**no shutdown** 例： スイッチ(config-if)# no shutdown	物理インターフェイスをイネーブルにします。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip route** 例： スイッチ# show ip route	入力を確認します。
ステップ 9	**show ip interface** [*interface-id*] 例： スイッチ# show ip interface gigabitethernet 1/0/1	入力を確認します。

	コマンドまたはアクション	目的
ステップ 10	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

サブネット ゼロの使用

サブネット アドレスがゼロであるサブネットを作成しないでください。同じアドレスを持つネットワークおよびサブネットがある場合に問題が発生することがあります。たとえば、ネットワーク 131.108.0.0 のサブネットが 255.255.255.0 の場合、サブネット ゼロは 131.108.0.0 と記述され、ネットワーク アドレスと同じとなってしまいます。

すべてが 1 のサブネット（131.108.255.0）は使用可能です。また、IP アドレス用にサブネット スペース全体が必要な場合は、サブネット ゼロの使用をイネーブルにできます（ただし推奨できません）。

デフォルトに戻して、サブネット ゼロの使用をディセーブルにするには、**no ip subnet-zero** グローバル コンフィギュレーション コマンドを使用します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip subnet-zero** 例： `スイッチ(config)# ip subnet-zero`	インターフェイス アドレスおよびルーティングのアップデート時にサブネットゼロの使用をイネーブルにします。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

クラスレス ルーティングのディセーブル化

スイッチが認識されないサブネット宛てのパケットを最適なスーパーネット ルートに転送しないようにするには、クラスレス ルーティング動作をディセーブルにします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ip classless** 例： スイッチ(config)#no ip classless	クラスレスルーティング動作をディセーブルにします。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

アドレス解決方法の設定

アドレス解決を設定するために必要な作業は次のとおりです。

スタティック ARP キャッシュの定義

ARP および他のアドレス解決プロトコルを使用すると、IP アドレスと MAC アドレス間をダイナミックにマッピングできます。ほとんどのホストではダイナミック アドレス解決がサポートされているため、通常の場合、スタティック ARP キャッシュ エントリを指定する必要はありません。スタティック ARP キャッシュ エントリを定義する必要がある場合は、グローバルにそれを定義できます。グローバルに定義すると、IP アドレスを MAC アドレスに変換するためにスイッチが使用するARP キャッシュに永続的なエントリをインストールします。また、指定されたIPアドレス

に属しているかのように、スイッチがARP要求に応答するように指定することもできます。ARPエントリを永続的なエントリにしない場合は、ARPエントリのタイムアウト期間を指定できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ3	**arp***ip-address hardware-address type* 例： スイッチ(config)# ip 10.1.5.1 c2f3.220a.12f4 arpa	ARPキャッシュ内でIPアドレスをMAC（ハードウェア）アドレスに関連付け、次に示すカプセル化タイプのいずれかを指定します。 • **arpa**：ARPカプセル化（イーサネット インターフェイス用） • **snap**：SNAPカプセル化（トークン リングおよびFDDIインターフェイス用） • **sap**：HPのARPタイプ
ステップ4	**arp***ip-address hardware-address type* [**alias**] 例： スイッチ(config)# ip 10.1.5.3 d7f3.220d.12f5 arpa alias	（任意）指定されたIPアドレスがスイッチに属する場合と同じ方法で、スイッチがARP要求に応答するように指定します。
ステップ5	**interface***interface-id* 例： スイッチ(config)# interface gigabitethernet 1/0/1	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ6	**arp***timeout seconds* 例： スイッチ(config-if)# arp 20000	（任意）ARPキャッシュ エントリがキャッシュに保持される期間を設定します。デフォルト値は14400秒（4時間）です。指定できる範囲は0～2147483秒です。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** [*interface-id*] 例： スイッチ# show interfaces gigabitethernet 1/0/1	すべてのインターフェイスまたは特定のインターフェイスで使用される ARP のタイプおよびタイムアウト値を確認します。
ステップ 9	**show arp** 例： スイッチ# show arp	ARP キャッシュの内容を表示します。
ステップ 10	**show ip arp** 例： スイッチ# show ip arp	ARP キャッシュの内容を表示します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ARP のカプセル化の設定

IP インターフェイスでは、イーサネット ARP カプセル化（**arpa** キーワードで表される）がデフォルトでイネーブルに設定されています。ネットワークの必要性に応じて、カプセル化方法を SNAP に変更できます。

カプセル化タイプをディセーブルにするには、**no arp arpa** または **no arp snap** インターフェイス コンフィギュレーション コマンドを使用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet 1/0/2`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**arp** {**arpa** | **snap**} 例： `スイッチ(config-if)# arp arpa`	ARP カプセル化方法を指定します。 • **arpa**：Address Resolution Protocol • **snap**：Subnetwork Address Protocol
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*] 例： `スイッチ# show interfaces`	すべてのインターフェイスまたは指定されたインターフェイスの ARP カプセル化設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

プロキシ ARP のイネーブル化

デフォルトでは、プロキシARPがスイッチで使用されます。ホストが他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにするためです。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet 1/0/2`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip proxy-arp** 例： `スイッチ(config-if)# ip proxy-arp`	インターフェイス上でプロキシ ARP をイネーブルにします。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip interface** [*interface-id*] 例： `スイッチ# show ip interface gigabitethernet 1/0/2`	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `スイッチ# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

IP ルーティングがディセーブルの場合のルーティング支援機能

次のメカニズムを使用することで、スイッチは IP ルーティングがイネーブルでない場合、別のネットワークへのルートを学習できます。

- プロシキ ARP
- デフォルト ゲートウェイ
- ICMP Router Discovery Protocol（IRDP）

プロキシ ARP

プロキシARPは、デフォルトでイネーブルに設定されています。ディセーブル化されたプロキシARPをイネーブルにするには、「プロキシARPのイネーブル化」の項を参照してください。プロキシ ARP は、他のルータでサポートされているかぎり有効です。

デフォルト ゲートウェイ

ルートを特定するもう1つの方法は、デフォルトルータ、つまりデフォルトゲートウェイを定義する方法です。ローカルでないすべてのパケットはこのルータに送信されます。このルータは適切なルーティングを行う、または IP 制御メッセージ プロトコル（ICMP）リダイレクト メッセージを返信するという方法で、ホストが使用するローカル ルータを定義します。スイッチはリダイレクト メッセージをキャッシュに格納し、各パケットをできるだけ効率的に転送します。この方法には、デフォルトルータがダウンした場合、または使用できなくなった場合に、検出が不可能となる制限があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip default-gateway***ip-address* 例： スイッチ(config)# ip default gateway 10.1.5.1	デフォルト ゲートウェイ（ルータ）を設定します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip redirects** 例： スイッチ# show ip redirects	設定を確認するため、デフォルト ゲートウェイ ルータのアドレスを表示します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ICMP Router Discovery Protocol（IRDP）

インターフェイスでIRDPルーティングを行う場合は、インターフェイスでIRDP処理をイネーブルにしてください。IRDP処理をイネーブルにすると、デフォルトのパラメータが適用されます。

これらのパラメータを変更することもできます。**maxadvertinterval** 値を変更すると、**holdtime** 値および**minadvertinterval**値も変更されます。最初に **maxadvertinterval** 値を変更し、次に **holdtime** 値または **minadvertinterval** 値のいずれかを手動で変更することが重要です。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# interface gigabitethernet 1/0/1	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip irdp** 例： スイッチ(config-if)# ip irdp	インターフェイスで IRDP 処理をイネーブルにします。
ステップ 5	**ip irdp multicast** 例： スイッチ(config-if)# ip irdp multicast	（任意）IP ブロードキャストの代わりとして、マルチキャスト アドレス（224.0.0.1）に IRDP アドバタイズを送信します。 （注） このコマンドを使用すると、IRDP パケットをマルチキャストとして送信するサン マイクロシステムズ社の Solaris との互換性を維持できます。実装機能の中には、これらのマルチキャストを受信できないものも多くあります。このコマンドを使用する前に、エンドホストがこの機能に対応していることを確認してください。
ステップ 6	**ip irdp holdtime***seconds* 例： スイッチ(config-if)# ip irdp holdtime 1000	（任意）アドバタイズが有効である IRDP 期間を設定します。デフォルト値は **maxadvertinterval** 値の 3 倍です。**maxadvertinterval** 値よりも大きな値（9000 秒以下）を指定する必要があります。**maxadvertinterval** 値を変更すると、この値も変更されます。

	コマンドまたはアクション	目的
ステップ 7	**ip irdp maxadvertinterval***seconds* 例： スイッチ(config-if)# ip irdp maxadvertinterval 650	（任意）アドバタイズメントの IRDP 最大間隔を設定します。デフォルトは 600 秒です。
ステップ 8	**ip irdp minadvertinterval***seconds* 例： スイッチ(config-if)# ip irdp minadvertinterval 500	（任意）アドバタイズ間の IRDP の最小インターバルを設定します。デフォルト値は **maxadvertinterval** 値の 0.75 倍です。**maxadvertinterval** を変更すると、この値も新しいデフォルト値（**maxadvertinterval** の 0.75 倍）に変更されます。
ステップ 9	**ip irdp preference***number* 例： スイッチ(config-if)# ip irdp preference 2	（任意）デバイスの IRDP プリファレンス レベルを設定します。指定できる範囲は -231 ～ 231 です。デフォルトは 0 です。大きな値を設定すると、ルータのプリファレンス レベルも高くなります。
ステップ 10	**ip irdp address***address* [*number*] 例： スイッチ(config-if)# ip irdp address 10.1.10.10	（任意）プロキシ アドバタイズを行うための IRDP アドレスとプリファレンスを設定します。
ステップ 11	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 12	**show ip irdp** 例： スイッチ# show ip irdp	IRDP 値を表示し、設定を確認します。
ステップ 13	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ブロードキャスト パケットの処理方法の設定

これらの方式をイネーブルにするには、次に示す作業を実行します。

- ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化
- UDP ブロードキャスト パケットおよびプロトコルの転送
- IP ブロードキャスト アドレスの確立
- IP ブロードキャストのフラッディング

ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化

デフォルトでは、IP ダイレクト ブロードキャストがドロップされるため、転送されることはありません。IP ダイレクト ブロードキャストがドロップされると、ルータが DoS 攻撃（サービス拒絶攻撃）にさらされる危険が少なくなります。

ブロードキャストが物理（MAC レイヤ）ブロードキャストになるインターフェイスでは、IP ダイレクト ブロードキャストの転送をイネーブルにできます。**ip forward-protocol** グローバル コンフィギュレーション コマンドを使用し、設定されたプロトコルだけを転送できます。

転送するブロードキャストを制御するアクセス リストを指定できます。アクセス リストを指定すると、アクセス リストで許可されている IP パケットだけが、ダイレクト ブロードキャストから物理ブロードキャストに変換できるようになります。アクセス リストの詳細については、『Security Configuration Guide』の「Information about Network Security with ACLs」の項を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# interface gigabitethernet 1/0/2	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 4	**ip directed-broadcast** [*access-list-number*] 例： `スイッチ(config-if)# ip directed-broadcast 103`	インターフェイス上で、ダイレクトブロードキャストから物理ブロードキャストへの変換をイネーブルにします。転送するブロードキャストを制御するアクセスリストを指定できます。アクセス リストを指定すると、アクセス リストで許可されている IP パケットだけが変換可能になります。
ステップ 5	**exit** 例： `スイッチ(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**} 例： `スイッチ(config)# ip forward-protocol nd`	ブロードキャスト パケットを転送するとき、ルータによって転送されるプロトコルおよびポートを指定します。 • **udp**：UDP データグラムを転送します。 port：（任意）転送される UDP サービスを制御する宛先ポートです。 • **nd**：ND データグラムを転送します。 • **sdns**：SDNS データグラムを転送します。
ステップ 7	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip interface** [*interface-id*] 例： `スイッチ# show ip interface`	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 9	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

UDP ブロードキャスト パケットおよびプロトコルの転送

UDP ブロードキャストの転送を設定するときに UDP ポートを指定しないと、ルータは BOOTP フォワーディング エージェントとして動作するように設定されます。BOOTP パケットはDynamic Host Configuration Protocol（DHCP）情報を伝達します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# interface gigabitethernet 1/0/1	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip helper-address***address* 例： スイッチ(config-if)# ip helper address 10.1.10.1	転送をイネーブルにし、BOOTP などの UDP ブロードキャスト パケットを転送するための宛先アドレスを指定します。
ステップ 5	**exit** 例： スイッチ(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**} 例： スイッチ(config)# ip forward-protocol sdns	ブロードキャスト パケットを転送するときに、ルータによって転送されるプロトコルを指定します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip interface** [*interface-id*] 例： スイッチ# show ip interface gigabitethernet 1/0/1	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 9	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ブロードキャスト アドレスの確立

最も一般的な（デフォルトの）IP ブロードキャスト アドレスは、すべて 1 で構成されているアドレス（255.255.255.255）です。ただし、任意の形式の IP ブロードキャスト アドレスを生成するようにスイッチを設定することもできます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# interface gigabitethernet 1/0/1	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ip broadcast-address***ip-address* 例： スイッチ(config-if)# ip broadcast-address 128.1.255.255	デフォルト値と異なるブロードキャスト アドレス（128.1.255.255 など）を入力します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip interface** [*interface-id*] 例： スイッチ# show ip interface	指定されたインターフェイスまたはすべてのインターフェイスのブロードキャストアドレスを確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ブロードキャストのフラッディング

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip forward-protocol spanning-tree** 例： スイッチ(config)# ip forward-protocol spanning-tree	ブリッジング スパニングツリー データベースを使用し、UDPデータグラムをフラッディングします。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 7	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**ip forward-protocol turbo-flood** 例： `スイッチ(config)# ip forward-protocol turbo-flood`	スパニングツリー データベースを使用し、UDP データグラムのフラッディングを高速化します。
ステップ 9	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP アドレスのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容が無効になっている場合、または無効である可能性がある場合は、**clear** 特権 EXEC コマンドを使用し、すべての内容を削除できます。次の表に、内容をクリアするために使用するコマンドを示します。

表 *74*：キャッシュ、テーブル、データベースをクリアするコマンド

clear arp-cache	IP ARP キャッシュおよび高速スイッチング キャッシュをクリアします。
clear host {*name* | ***}**	ホスト名およびアドレス キャッシュから 1 つまたはすべてのエントリを削除します。
clear ip route {**network** [*mask*] | ***}**	IP ルーティング テーブルから 1 つまたは複数のルートを削除します。

IP ルーティング テーブル、キャッシュ、データベースの内容、ノードへの到達可能性、ネットワーク内のパケットのルーティング パスなど、特定の統計情報を表示できます。次の表に、IP 統計情報を表示するために使用する特権 EXEC コマンドを示します。

表 *75*：キャッシュ、テーブル、データベースを表示するコマンド

show arp	ARP テーブル内のエントリを表示します。
show hosts	デフォルトのドメイン名、検索サービスの方式、サーバ ホスト名、およびキャッシュに格納されているホスト名とアドレスのリストを表示します。
show ip aliases	TCP ポートにマッピングされた IP アドレスを表示します（エイリアス）。
show ip arp	IP ARP キャッシュを表示します。
show ip interface[*interface-id*]	インターフェイスの IP ステータスを表示します。
show ip irdp	IRDP 値を表示します。
show ip masks*address*	ネットワーク アドレスに対して使用されるマスクおよび各マスクを使用するサブネット番号を表示します。
show ip redirects	デフォルト ゲートウェイのアドレスを表示します。
show ip route [*address* [*mask*]] | [*protocol*]	ルーティング テーブルの現在の状態を表示します。
show ip route summary	サマリー形式でルーティング テーブルの現在のステータスを表示します。

IP ユニキャスト ルーティングの設定方法

IP ユニキャスト ルーティングのイネーブル化

デフォルトで、スイッチはレイヤ 2 スイッチング モード、IP ルーティングはディセーブルとなっています。スイッチのレイヤ 3 機能を使用するには、IP ルーティングをイネーブルにする必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip routing** 例： スイッチ(config)# ip routing	IP ルーティングをイネーブルにします。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ルーティングのイネーブル化の例

次に、ルーティング プロトコルとして RIP を使用し、IP ルーティングをイネーブルにする例を示します。

```
スイッチ# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチ(config)# ip routing
スイッチ(config)# router rip
スイッチ(config-router)# network 10.0.0.0
スイッチ(config-router)# end
```

次の作業

ここで、選択したルーティング プロトコルのパラメータを設定できます。具体的な手順は次のとおりです。

- RIP
- OSPF
- EIGRP
- BGP
- ユニキャスト Reverse Path Forwarding
- プロトコル独立機能（任意）

RIP 情報

RIP は、小規模な同種ネットワーク間で使用するために作成された Interior Gateway Protocol（IGP）です。RIP は、ブロードキャスト ユーザ データグラム プロトコル（UDP）データ パケットを使用してルーティング情報を交換するディスタンスベクトルルーティングプロトコルです。このプロトコルは RFC 1058 に文書化されています。RIP の詳細については、『*IP Routing Fundamentals*』（Cisco Press 刊）を参照してください。

（注） RIP は IP Base でサポートされています。

スイッチは RIP を使用し、30 秒ごとにルーティング情報アップデート（アドバタイズメント）を送信します。180 秒以上を経過しても別のルータからアップデートがルータに届かない場合、該当するルータから送られたルートは使用不能としてマークされます。240 秒後もまだ更新がない場合、ルータは更新のないルータのルーティング テーブル エントリをすべて削除します。

RIP では、各ルートの値を評価するためにホップ カウントが使用されます。ホップ カウントは、ルート内で経由されるルータ数です。直接接続されているネットワークのホップ カウントは 0 です。ホップ カウントが 16 のネットワークに到達できません。このように範囲（0 ～ 15）が狭いため、RIP は大規模ネットワークには適していません。

ルータにデフォルトのネットワーク パスが設定されている場合、RIP はルータを疑似ネットワーク 0.0.0.0 にリンクするルートをアドバタイズします。0.0.0.0 ネットワークは存在しません。RIP はデフォルトのルーティング機能を実行するためのネットワークとして、このネットワークを処理します。デフォルト ネットワークが RIP によって学習された場合、またはルータにラスト リゾート ゲートウェイがあり、RIPがデフォルトのメトリックによって設定されている場合、スイッチはデフォルト ネットワークをアドバタイズします。RIP は指定されたネットワーク内のインター

フェイスにアップデートを送信します。インターフェイスのネットワークを指定しなければ、RIP のアップデート中にアドバタイズされません。

サマリー アドレスおよびスプリット ホライズン

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティングループの発生を抑えるために、スプリットホライズンメカニズムが使用されます。スプリットホライズンは、ルートに関する情報の発信元であるインターフェイス上の、ルータによって、その情報がアドバタイズされないようにします。この機能を使用すると、通常の場合は複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。

RIP の設定方法

RIP のデフォルト設定

表 *76*：*RIP* のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル
デフォルト情報送信元	ディセーブル
デフォルト メトリック	自動メトリック変換（組み込み）
IP RIP 認証キーチェーン	認証なし 認証モード：クリア テキスト
IP RIP の起動	ディセーブル
IP スプリット ホライズン	メディアにより異なる
ネイバー	未定義
ネットワーク	指定なし
オフセット リスト	ディセーブル
出力遅延	0 ミリ秒

機能	デフォルト設定
タイマー基準	• 更新：30 秒 • 無効：180 秒 • ホールドダウン：180 秒 • フラッシュ：240 秒
アップデート送信元の検証	イネーブル
バージョン	RIP バージョン 1 およびバージョン 2 パケットを受信し、バージョン 1 パケットを送信します。

基本的な RIP パラメータの設定

RIP を設定するには、ネットワークに対して RIP ルーティングをイネーブルにします。他のパラメータを設定することもできます。スイッチでは、ネットワーク番号を設定するまでRIP コンフィギュレーション コマンドは無視されます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip routing** 例： スイッチ(config)# **ip routing**	IP ルーティングをイネーブルにします。（IP ルーティングがディセーブルになっている場合だけ、必須です）。

	コマンドまたはアクション	目的
ステップ 4	**router rip** 例： スイッチ(config)# **router rip**	RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 5	**network***network number* 例： スイッチ(config)# **network 12**	ネットワークを RIP ルーティング プロセスと関連付けます。複数の **network** コマンドを指定できます。RIP ルーティング アップデートの送受信は、これらのネットワークのインターフェイスを経由する場合だけ可能です。 （注） RIP コマンドを有効にするには、ネットワーク番号を設定する必要があります。
ステップ 6	**neighbor***ip-address* 例： スイッチ(config)# **neighbor 10.2.5.1**	（任意）ルーティング情報を交換する隣接ルータを定義します。このステップを使用すると、RIP（通常はブロードキャスト プロトコル）からのルーティングアップデートが非ブロードキャストネットワークに到達するようになります。
ステップ 7	**offset-list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*] 例： スイッチ(config)# **offset-list 103 in 10**	（任意）オフセット リストをルーティング メトリックに適用し、RIP によって取得したルートへの着信および発信メトリックを増加します。アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。
ステップ 8	**timers basic***update invalid holddown flush* 例： スイッチ(config)# **timers basic 45 360 400 300**	（任意）ルーティングプロトコルタイマーを調整します。すべてのタイマーの有効範囲は 0 ～ 4294967295 秒です。 • *update*：ルーティング アップデートの送信間隔。デフォルトは 30 秒です。 • *invalid*：ルートが無効と宣言されるまでの時間。デフォルト値は 180 秒です。 • *holddown*：ルートがルーティングテーブルから削除されるまでの時間。デフォルト値は 180 秒です。 • *flush*：ルーティングアップデートが延期される時間。デフォルトは 240 秒です。
ステップ 9	**version** {**1** | **2**} 例： スイッチ(config)# **version 2**	（任意）RIP バージョン 1 または RIP バージョン 2 のパケットだけを送受信するようにスイッチを設定します。デフォルトの場合、スイッチではバージョン 1 および 2 を受信しますが、バージョン 1 だけを送信します。 インターフェイス コマンド **ip rip** {**send** | **receive**}

	コマンドまたはアクション	目的
		version 1 | **2** | **1 2**} を使用し、インターフェイスでの送受信に使用するバージョンを制御することもできます。
ステップ 10	**no auto summary** 例： スイッチ(config)# **no auto summary**	（任意）自動要約をディセーブルにします。デフォルトでは、クラスフル ネットワーク境界を通過するときにサブプレフィックスがサマライズされます。サマライズをディセーブルにし（RIP バージョン 2 だけ）、クラスフル ネットワーク境界にサブネットおよびホスト ルーティング情報をアドバタイズします。
ステップ 11	**no validate-update-source** 例： スイッチ(config)# **no validdate-update-source**	（任意）着信 RIP ルーティング アップデートの送信元 IP アドレスの検証をディセーブルにします。デフォルトでは、スイッチが着信 RIP ルーティング アップデートの送信元 IP アドレスを検証します。送信元アドレスが無効な場合は、アップデートが廃棄されます。通常の環境で使用する場合は、この機能をディセーブルにしないでください。ただし、ネットワークに接続されていないルータがあり、そのルータのアップデートを受信する場合は、このコマンドを使用できます。
ステップ 12	**output-delay***delay* 例： スイッチ(config)# **output-delay 8**	（任意）送信する RIP アップデートにパケット間遅延を追加します。デフォルトでは、複数のパケットからなる RIP アップデートのパケットに、パケット間遅延が追加されません。パケットを低速なデバイスに送信する場合は、8 ～ 50 ミリ秒のパケット間遅延を追加できます。
ステップ 13	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 14	**show ip protocols** 例： スイッチ# **show ip protocols**	入力を確認します。
ステップ 15	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RIP 認証の設定

RIP バージョン 1 は認証をサポートしていません。RIP バージョン 2 のパケットを送受信する場合は、インターフェイスで RIP 認証をイネーブルにできます。インターフェイスで使用できる一連のキーは、キーチェーンによって指定されます。キーチェーンが設定されていないと、デフォルトの場合でも認証は実行されません。

RIP 認証がイネーブルであるインターフェイスでは、プレーン テキストと MD5 という 2 つの認証モードがスイッチでサポートされます。デフォルトはプレーン テキストです。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ip rip authentication key-chain***name-of-chain* 例： スイッチ(config-if)# **ip rip authentication key-chain trees**	RIP 認証をイネーブルにします。
ステップ 5	**ip rip authentication mode** {**text** | **md5**} 例： スイッチ(config-if)# **ip rip authentication mode md5**	プレーンテキスト認証（デフォルト）またはMD5ダイジェスト認証を使用するように、インターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

サマリー アドレスおよびスプリット ホライズンの設定

（注） ルートを適切にアドバタイズするため、アプリケーションがスプリット ホライズンをディセーブルにする必要がある場合を除き、通常はこの機能をディセーブルにしないでください。

ダイヤルアップ クライアント用のネットワーク アクセス サーバで、サマライズされたローカル IP アドレス プールをアドバタイズするように、RIP が動作しているインターフェイスを設定する場合は、**ip summary-address rip** インターフェイス コンフィギュレーション コマンドを使用します。

（注） スプリット ホライズンがイネーブルの場合、自動サマリーとインターフェイス IP サマリー アドレスはともにアドバタイズされません。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip address***ip-address subnet-mask* 例： スイッチ(config-if)# **ip address 10.1.1.10 255.255.255.0**	IP アドレスおよび IP サブネットを設定します。
ステップ 5	**ip summary-address rip ip address***ip-network mask* 例： スイッチ(config-if)# **ip summary-address rip ip address 10.1.1.30 255.255.255.0**	サマライズする IP アドレスおよび IP ネットワーク マスクを設定します。
ステップ 6	**no ip split horizon** 例： スイッチ(config-if)# **no ip split horizon**	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show ip interface***interface-id* 例： スイッチ# **show ip interface gigabitethernet 1/0/1**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティングループの発生を抑えるために、スプリットホライズンメカニズムが使用されます。スプリットホライズンは、ルートに関する情報の発信元であるインターフェイス上の、ルータによって、その情報がアドバタイズされないようにします。この機能を使用すると、複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。

（注） ルートを適切にアドバタイズするために、アプリケーションがスプリット ホライズンをディセーブルにする必要がある場合を除き、通常この機能をディセーブルにしないでください。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ip address***ip-address subnet-mask* 例： `スイッチ(config-if)# ip address 10.1.1.10 255.255.255.0`	IP アドレスおよび IP サブネットを設定します。
ステップ 5	**no ip split-horizon** 例： `スイッチ(config-if)# no ip split-horizon`	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 6	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip interface***interface-id* 例： `スイッチ# show ip interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

サマリー アドレスおよびスプリット ホライズンの設定例

次の例では、主要ネットは 10.0.0.0 です。自動サマリー アドレス 10.0.0.0 はサマリー アドレス 10.2.0.0 によって上書きされるため、10.2.0.0 はインターフェイス ギガビット イーサネット ポート 2 からアドバタイズされますが、10.0.0.0 はアドバタイズされません。次の例では、インターフェイスがまだレイヤ 2 モード（デフォルト）の場合、**no switchport** インターフェイス コンフィ

ギュレーション コマンドを入力してから、**ip address** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

（注） スプリット ホライズンがイネーブルである場合、（**ip summary-address rip** ルータ コンフィギュレーション コマンドによって設定される）自動サマリーとインターフェイス サマリー アドレスはともにアドバタイズされません。

```
スイッチ(config)# router rip
スイッチ(config-router)# interface gigabitethernet1/0/2
スイッチ(config-if)# ip address 10.1.5.1 255.255.255.0
スイッチ(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
スイッチ(config-if)# no ip split-horizon
スイッチ(config-if)# exit
スイッチ(config)# router rip
スイッチ(config-router)# network 10.0.0.0
スイッチ(config-router)# neighbor 2.2.2.2 peer-group mygroup
スイッチ(config-router)# end
```

OSPF に関する情報

OSPF は IP ネットワーク専用の IGP で、IP サブネット化、および外部から取得したルーティング情報のタグ付けをサポートしています。OSPF を使用するとパケット認証も可能になり、パケットを送受信するときに IP マルチキャストが使用されます。シスコの実装では、RFC1253 の OSPF 管理情報ベース（MIB）がサポートされています。

（注） OSPF は IP ベースではサポートされません。

シスコの実装は、次の主要機能を含む OSPF バージョン 2 仕様に準拠します。

- スタブ エリアの定義がサポートされています。
- 任意の IP ルーティング プロトコルによって取得されたルートは、別の IP ルーティング プロトコルに再配信されます。つまり、ドメイン内レベルで、OSPF は EIGRP および RIP によって取得したルートを取り込むことができます。OSPF ルートを RIP に伝達することもできます。
- エリア内の隣接ルータ間でのプレーン テキスト認証および MD5 認証がサポートされています。
- 設定可能なルーティング インターフェイス パラメータには、インターフェイス出力コスト、再送信インターバル、インターフェイス送信遅延、ルータ プライオリティ、ルータのデッド インターバルと hello インターバル、認証キーなどがあります。
- 仮想リンクがサポートされています。
- RFC 1587 に基づく Not-So-Stubby-Area（NSSA）がサポートされています。

通常、OSPF を使用するには、多くの内部ルータ、複数のエリアに接続された Area Border Router（ABR; エリア境界ルータ）、および自律システム境界ルータ（ASBR）間で調整する必要があります。最小設定では、すべてのデフォルト パラメータ値、エリアに割り当てられたインターフェイスが使用され、認証は行われません。環境をカスタマイズする場合は、すべてのルータの設定を調整する必要があります。

OSPF NSF

スイッチまたはスイッチ スタックは 2 つのレベルのノンストップ フォワーディング（NSF）をサポートしています。

- OSPF NSF 認識, （1153 ページ）
- OSPF NSF 対応, （1153 ページ）

OSPF NSF 認識

IP サービス フィーチャ セットは、OSPF NSF 認識を IPv4 に対してサポートしています。隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータに障害（クラッシュ）が発生してプライマリ ルート プロセッサ（RP）がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能をディセーブルにできません。

OSPF NSF 対応

IP サービス フィーチャ セットでは、前のリリースでサポートされていた OSPFv2 NSF Cisco フォーマットに加えて、OSPFv2 NSF IETF フォーマットもサポートされます。この機能の詳細については、『*NSF—OSPF (RFC 3623 OSPF Graceful Restart)*』を参照してください。

IP サービス フィーチャ セットは、OSPF NSF 対応ルーティングも IPv4 に対してサポートし、スタック マスター変更後のコンバージェンスの向上と、トラフィック損失の低減を実現します。OSPF NSF 対応スタックでスタック マスターの変更が生じた場合、新しいスタック マスターは自身のリンクステート データベースを OSPF ネイバーと再同期化するために、次の 2 つの処理をする必要があります。

- ネイバー関係をリセットせずにネットワーク上の使用可能な OSPF ネイバーを解放します。
- ネットワークのリンクステート データベースの内容を再取得します。

スタック マスターの変更後、新しいマスターは隣接する NSF 認識デバイスに OSPF NSF 信号を送信します。デバイスはこの信号を、スタックとのネイバー関係をリセットしない指示として認識します。NSF 対応スタック マスターは、ネットワーク上の他のルータから信号を受け取ると、自身のネイバー リストの再構築を開始します。

NSF 対応スタック マスターはネイバー関係を再確立すると、自身のデータベースを NSF 認識ネイバーと再同期化し、OSPF ネイバー間でルーティング情報を交換します。新しいスタック マスターはこのルーティング情報を使用して、新しい情報を基に古いルートの削除、ルーティング情報ベー

ス（RIB）の更新、転送情報ベース（FIB）のアップデートを行います。これで OSPF プロトコルは完全に収束します。

（注） OSPF NSF では、すべてのネイバー ネットワーク デバイスが NSF 認識である必要があります。ネットワーク セグメント上に非 NSF 認識ネイバーが検出された場合、NSF 対応ルータはそのセグメントに対する NSF 機能をディセーブルにします。すべてのデバイスが NSF 認識または NSF 対応デバイスとなっているその他のネットワーク セグメントでは、NSF 対応機能が継続して提供されます。

OSPF NSF ルーティングをイネーブルにするには、**nsf** OSPF ルーティング コンフィギュレーション コマンドを使用します。OSPF NSF ルーティングがイネーブルになっていることを確認するには、**show ip ospf** 特権 EXEC コマンドを使用します。

詳細については、次の URL の『*Cisco Nonstop Forwarding*』を参照してください。 http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-nonstp_fwdg.html

OSPF エリア パラメータ

複数の OSPF エリア パラメータを設定することもできます。設定できるパラメータには、エリア、スタブ エリア、および NSSA への無許可アクセスをパスワードによって阻止する認証用パラメータがあります。スタブ エリアは、外部ルートの情報が送信されないエリアです。が、代わりに、自律システム（AS）外の宛先に対するデフォルトの外部ルートが、ABR によって生成されます。NSSA ではコアからそのエリアへ向かう LSA の一部がフラッディングされませんが、再配信することによって、エリア内の AS 外部ルートをインポートできます。

経路集約は、アドバタイズされたアドレスを、他のエリアでアドバタイズされる単一のサマリー ルートに統合することです。ネットワーク番号が連続する場合は、**area range** ルータ コンフィギュレーション コマンドを使用し、範囲内のすべてのネットワークを対象とするサマリー ルートをアドバタイズするように ABR を設定できます。

その他の OSPF パラメータ

ルータ コンフィギュレーション モードで、その他の OSPF パラメータを設定することもできます。

- ルート集約：他のプロトコルからルートを再配信すると、各ルートは外部 LSA 内で個別にアドバタイズされます。OSPF リンク ステート データベースのサイズを小さくするには、**summary-address** ルータ コンフィギュレーション コマンドを使用し、指定されたネットワーク アドレスおよびマスクに含まれる、再配信されたすべてのルートを単一のルータにアドバタイズします。
- 仮想リンク：OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンが不連続である場合に仮想リンクを確立するには、2 つの ABR を仮想リンクのエンドポイントとして設定します。設定情報には、他の仮想エンドポイント（他の ABR）の ID、および 2 つのルータに共通する非バックボーン リンク（通過エリア）などがあります。仮想リンクをスタブ エリアから設定できません。

- デフォルト ルート：OSPF ルーティング ドメイン内へのルート再配信を設定すると、ルータは自動的に自律システム境界ルータ（ASBR）になります。ASBR を設定し、強制的に OSPF ルーティング ドメインにデフォルト ルートを生成できます。
- すべての OSPF **show** 特権 EXEC コマンドで使用されるドメイン ネーム サーバ（DNS）名を使用すると、ルータ ID やネイバー ID を指定して表示する場合に比べ、ルータを簡単に特定できます。
- デフォルト メトリック：OSPF は、インターフェイスの帯域幅に従ってインターフェイスの OSPF メトリックを計算します。メトリックは、帯域幅で分割された *ref-bw* として計算されます。ここでの *ref* のデフォルト値は 10 で、帯域幅（*bw*）は **bandwidth** インターフェイス コンフィギュレーション コマンドによって指定されます。大きな帯域幅を持つ複数のリンクの場合は、大きな数値を指定し、これらのリンクのコストを区別できます。
- アドミニストレーティブ ディスタンスは、ルーティング情報送信元の信頼性を表す数値です。0 ～ 255 の整数を指定でき、値が大きいほど信頼性は低下します。アドミニストレーティブ ディスタンスが 255 の場合はルーティング情報の送信元をまったく信頼できないため、無視する必要があります。OSPF では、エリア内のルート（エリア内）、別のエリアへのルート（エリア間）、および再配信によって学習した別のルーティング ドメインからのルート（外部）の 3 つの異なるアドミニストレーティブ ディスタンスが使用されます。どのアドミニストレーティブ ディスタンスの値でも変更できます。
- 受動インターフェイス：イーサネット上の 2 つのデバイス間のインターフェイスは 1 つのネットワーク セグメントしか表しません。このため、OSPF が送信側インターフェイスに hello パケットを送信しないようにするには、送信側デバイスを受動インターフェイスに設定する必要があります。両方のデバイスは受信側インターフェイス宛ての hello パケットを使用することで、相互の識別を可能にします。
- ルート計算タイマー：OSPF がトポロジ変更を受信してから SPF 計算を開始するまでの遅延時間、および 2 つの SPF 計算の間のホールド タイムを設定できます。
- ネイバー変更ログ：OSPF ネイバー ステートが変更されたときに Syslog メッセージを送信するようにルータを設定し、ルータの変更を詳細に表示できます。

LSA グループ ペーシング

OSPF LSA グループ ペーシング機能を使用すると、OSPF LSA をグループ化し、リフレッシュ、チェックサム、エージング機能の同期を取って、ルータをより効率的に使用できるようになります。デフォルトでこの機能はイネーブルとなっています。デフォルトのペーシング インターバルは 4 分間です。通常は、このパラメータを変更する必要はありません。最適なグループ ペーシング インターバルは、ルータがリフレッシュ、チェックサム、エージングを行う LSA 数に反比例します。たとえば、データベース内に約 10000 個の LSA が格納されている場合は、ペーシング インターバルを短くすると便利です。小さなデータベース（40 ～ 100 LSA）を使用する場合は、ペーシング インターバルを長くし、10 ～ 20 分に設定してください。

ループバック インターフェイス

OSPF は、インターフェイスに設定されている最大の IP アドレスをルータ ID として使用します。このインターフェイスがダウンした場合、または削除された場合、OSPF プロセスは新しいルータ ID を再計算し、すべてのルーティング情報をそのルータのインターフェイスから再送信します。ループバックインターフェイスがIPアドレスによって設定されている場合、他のインターフェイスにより大きな IP アドレスがある場合でも、OSPF はこの IP アドレスをルータ ID として使用します。ループバック インターフェイスに障害は発生しないため、安定性は増大します。OSPF は他のインターフェイスよりもループバック インターフェイスを自動的に優先し、すべてのループバック インターフェイスの中で最大の IP アドレスを選択します。

OSPF の設定方法

OSPF のデフォルト設定

表 *77*：*OSPF* のデフォルト設定

機能	デフォルト設定
インターフェイス パラメータ	コスト：1. 再送信インターバル：5 秒 送信遅延：1 秒 プライオリティ：1 hello インターバル：10 秒 デッド インターバル：hello インターバルの 4 倍 認証なし パスワードの指定なし MD5 認証はディセーブル
エリア	認証タイプ：0（認証なし） デフォルト コスト：1 範囲：ディセーブル スタブ：スタブ エリアは未定義 NSSA：NSSA エリアは未定義
自動コスト	100 Mb/s
デフォルト情報送信元	ディセーブルイネーブルの場合、デフォルトのメトリック設定は 10 で、外部ルート タイプのデフォルトはタイプ 2 です。

機能	デフォルト設定
デフォルト メトリック	各ルーティング プロトコルに適切な、組み込みの自動メトリック変換
距離 OSPF	dist1（エリア内のすべてのルート）：110。 dist2（エリア間のすべてのルート）：110。 および dist3（他のルーティング ドメインからのルート）：110。
OSPF データベース フィルタ	ディセーブルすべての発信 LSA がインターフェイスにフラッディングされます。
IP OSPF 名検索	ディセーブル
隣接関係変更ログ	イネーブル
ネイバー	指定なし
ネイバーデータベース フィルタ	ディセーブルすべての発信 LSA はネイバーにフラッディングされます。
ネットワーク エリア	ディセーブル
ノンストップ フォワーディング（NSF）認識	イネーブルレイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
NSF 対応	ディセーブル （注） スイッチ スタックは OSPF NSF 対応ルーティングを IPv4 に対してサポートします。
ルータ ID	OSPF ルーティング プロセスは未定義
サマリー アドレス	ディセーブル
タイマー LSA グループのペーシング	240 秒
タイマー Shortest Path First（SPF）	spf 遅延：5 秒; spf ホールドタイム：10 秒

機能	デフォルト設定
仮想リンク	エリア ID またはルータ ID は未定義 hello インターバル：10 秒 再送信インターバル：5 秒 送信遅延：1 秒 デッド インターバル：40 秒 認証キー：キーは未定義 メッセージ ダイジェスト キー（MD5）：キーは未定義

基本的な OSPF パラメータの設定

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、そのルーティング プロセスに関連付けられる IP アドレスの範囲を指定し、その範囲に関連付けられるエリア ID を割り当てます。IP サービス イメージを実行しているスイッチでは、Cisco OSPFv2 NSF フォーマットまたは IETF OSPFv2 NSF フォーマットのいずれかを設定できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** process-id 例： `スイッチ(config)# router ospf 15`	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。プロセス ID はローカルに割り当てられ、内部で使用される識別パラメータで、任意の正の整数を指定できます。各 OSPF ルーティング プロセスには一意の値があります。 （注） OSPF for Routed Access は、OSPFv2 インスタンスと OSPFv3 インスタンスをそれぞれ 1 つずつと、最大 200 のダイナミックに学習されるルートをサポートします。
ステップ 3	**nsf cisco** [**enforce global**] 例： `スイッチ(config)# nsf cisco enforce global`	（任意）OSPF での Cisco NSF 動作をイネーブルにします。**enforce global** キーワードを指定すると、非 NSF 認識のネイバー ネットワーキング デバイスが検出されたときに NSF 再起動がキャンセルされます。 （注） ステップ 3 またはステップ 4 でコマンドを入力し、ステップ 5 に進みます。

	コマンドまたはアクション	目的
ステップ 4	**nsf ietf** [**restart-interval***seconds*] 例： スイッチ(config)# **nsf ietf restart-interval 60**	（任意）OSPF での IETF NSF 動作をイネーブルにします。**restart-interval** キーワードでは、グレースフル リスタート間隔の長さを秒単位で指定します。範囲は 1 ～ 1800 です。デフォルトは 120 です。 （注） ステップ 3 またはステップ 4 でコマンドを入力し、ステップ 5 に進みます。
ステップ 5	**network** address wildcard-mask **area** area-id 例： スイッチ(config)# **network 10.1.1.1 255.240.0.0 area 20**	OSPF が動作するインターフェイス、およびそのインターフェイスのエリア ID を定義します。単一のコマンドにワイルドカード マスクを指定し、特定の OSPF エリアに関連付けるインターフェイスを 1 つまたは複数定義できます。エリア ID には 10 進数または IP アドレスを指定できます。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip protocols** 例： スイッチ# **show ip protocols**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF インターフェイスの設定

ip ospf インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイス固有の OSPF パラメータを変更できます。これらのパラメータを変更する必要はありませんが、一部のインターフェイス パラメータ（hello インターバル、デッド インターバル、認証キーなど）については、接続されたネットワーク内のすべてのルータで統一性を維持する必要があります。これらのパラメータを変更した場合は、ネットワーク内のすべてのルータの値も同様に変更してください。

（注） **ip ospf** インターフェイス コンフィギュレーション コマンドはすべてオプションです。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** interface-id 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip ospf** cost 例： `スイッチ(config-if)# ip ospf 8`	（任意）インターフェイスでパケットを送信するコストを明示的に指定します。
ステップ 4	**ip ospf retransmit-interval** seconds 例： `スイッチ(config-if)# ip ospf transmit-interval 10`	（任意）LSA 送信間隔を秒数で指定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 5 秒です。
ステップ 5	**ip ospf transmit-delay** seconds 例： `スイッチ(config-if)# ip ospf transmit-delay 2`	（任意）リンク ステート アップデート パケットを送信するまでの予測待機時間を秒数で設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 1 秒です。
ステップ 6	**ip ospf priority** number 例： `スイッチ(config-if)# ip ospf priority 5`	（任意）ネットワークに対して、OSPF で指定されたルータを検索するときに役立つプライオリティを設定します。有効な範囲は 0 ～ 255 です。デフォルトは 1 です。
ステップ 7	**ip ospf hello-interval** seconds 例： `スイッチ(config-if)# ip ospf hello-interval 12`	（任意）OSPF インターフェイスで hello パケットの送信間隔を秒数で設定します。ネットワークのすべてのノードで同じ値を指定する必要があります。指定できる範囲は 1 ～ 65535 秒です。デフォルトは 10 秒です。

	コマンドまたはアクション	目的
ステップ 8	**ip ospf dead-interval** seconds 例： `スイッチ(config-if)# ip ospf dead-interval 8`	（任意）最後のデバイスで hello パケットが確認されてから、OSPF ルータがダウンしていることがネイバーによって宣言されるまでの時間を秒数で設定します。ネットワークのすべてのノードで同じ値を指定する必要があります。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は hello インターバルの 4 倍です。
ステップ 9	**ip ospf authentication-key** key 例： `スイッチ(config-if)# ip ospf authentication-key password`	（任意）隣接 OSPF ルータで使用されるパスワードを割り当てます。パスワードには、キーボードから入力した任意の文字列（最大 8 バイト長）を指定できます。同じネットワーク上のすべての隣接ルータには、OSPF 情報を交換するため、同じパスワードを設定する必要があります。
ステップ 10	**ip ospf message digest-key** keyid **md5** key 例： `スイッチ(config-if)# ip ospf message digest-key 16 md5 your1pass`	（任意）MDS 認証をイネーブルにします。 • *keyid*：1 ～ 255 の ID。 • *key*：最大 16 バイトの英数字パスワード
ステップ 11	**ip ospf database-filter all out** 例： `スイッチ(config-if)# ip ospf database-filter all out`	（任意）インターフェイスへの OSPF LSA パケットのフラッディングを阻止します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。
ステップ 12	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show ip ospf interface** [*interface-name*] 例： `スイッチ# show ip ospf interface`	OSPF に関連するインターフェイス情報を表示します。
ステップ 14	**show ip ospf neighbor detail** 例： `スイッチ# show ip ospf neighbor detail`	ネイバースイッチの NSF 認証ステータスを表示します。出力には、次のいずれかが表示されます。 • *Options is 0x52* *LLS Options is 0x1 (LR)* これらの行の両方が表示される場合、ネイバースイッチが NSF 認識です。

	コマンドまたはアクション	目的
		• *Options is 0x42*：ネイバー スイッチが NSF 認識でないことを示します。
ステップ 15	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF エリア パラメータの設定

はじめる前に

（注） OSPF **area** ルータ コンフィギュレーション コマンドはすべて任意です。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** process-id 例： スイッチ(config)# router ospf 109	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**area***area-id***authentication** 例： スイッチ(config-router)# area 1 authentication	（任意）特定のエリアへの無許可アクセスに対して、パスワードベースの保護を可能にします。ID には 10 進数または IP アドレスのいずれかを指定できます。

	コマンドまたはアクション	目的
ステップ 4	**area***area-id***authentication message-digest** 例： `スイッチ(config-router)# area 1 authentication message-digest`	（任意）エリアに関してMD5認証をイネーブルにします。
ステップ 5	**area***area-id***stub** [**no-summary**] 例： `スイッチ(config-router)# area 1 stub`	（任意）エリアをスタブ エリアとして定義します。**no-summary** キーワードを指定すると、ABR はサマリー リンク アドバタイズメントをスタブエリアに送信できなくなります。
ステップ 6	**area***area-id***nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**] 例： `スイッチ(config-router)# area 1 nssa default-information-originate`	（任意）エリアを NSSA として定義します。同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。次のキーワードのいずれかを選択します。 • **no-redistribution**：ルータが NSSA ABR の場合、**redistribute** コマンドを使用して、ルートを NSSA でなく通常のエリアにインポートする場合に選択します。 • **default-information-originate**：タイプ 7 LSA を NSSA にインポートするようにする場合に、ABR で選択します。 • **no-redistribution**：サマリー LSA を NSSA に送信しない場合に選択します。
ステップ 7	**area***area-id***range***address mask* 例： `スイッチ(config-router)# area 1 range 255.240.0.0`	（任意）単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip ospf**[*process-id*] 例： `スイッチ# show ip ospf`	設定を確認するため、一般的な OSPF ルーティング プロセスまたは特定のプロセス ID に関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 10	**show ip ospf** [*process-id* [*area-id*]] **database** 例： スイッチ# show ip osfp database	特定のルータの OSPF データベースに関連する情報のリストを表示します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

その他の OSPF パラメータの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf***process-id* 例： スイッチ(config)# router ospf 10	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**summary-address***address mask* 例： スイッチ(config)# summary-address 10.1.1.1 255.255.255.0	（任意）1 つのサマリールートだけがアドバタイズされるように、再配信されたルートのアドレスおよび IP サブネット マスクを指定します。
ステップ 4	**area***area-id***virtual-link***router-id* [**hello-interval***seconds*] [**retransmit-interval***seconds*] [**trans**] [[**authentication-key***key*] | **message-digest-key***keyid***md5***key*]]	（任意）仮想リンクを確立し、パラメータを設定します。

	コマンドまたはアクション	目的
	例： `スイッチ(config)# area 2 virtual-link 192.168.255.1 hello-interval 5`	
ステップ 5	**default-information originate** [**always**] [**metric***metric-value*] [**metric-type***type-value*] [**route-map***map-name*] 例： `スイッチ(config)# default-information originate metric 100 metric-type 1`	（任意）強制的に OSPF ルーティング ドメインにデフォルト ルートを生成するように ASBR を設定します。パラメータはすべて任意です。
ステップ 6	**ip ospf name-lookup** 例： `スイッチ(config)# ip ospf name-lookup`	（任意）DNS 名検索を設定します。デフォルトではディセーブルになっています。
ステップ 7	**ip auto-cost reference-bandwidth***ref-bw* 例： `スイッチ(config)# ip auto-cost reference-bandwidth 5`	（任意）単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8	**distance ospf** {[**inter-area***dist1*] [**inter-area***dist2*] [**external***dist3*]} 例： `スイッチ(config)# distance ospf inter-area 150`	（任意）OSPF の距離の値を変更します。各タイプのルートのデフォルト距離は 110 です。指定できる範囲は 1 ～ 255 です。
ステップ 9	**passive-interface***type number* 例： `スイッチ(config)# passive-interface gigabitethernet 1/0/6`	（任意）指定されたインターフェイス経由の hello パケットの送信を抑制します。
ステップ 10	**timers throttle spf***spf-delay spf-holdtime spf-wait* 例： `スイッチ(config)# timers throttle spf 200 100 100`	（任意）ルート計算タイマーを設定します。 • *spf-delay*：SPF 計算の変更を受信する間の遅延。指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-holdtime*：最初と 2 番目の SPF 計算の間の遅延。指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-wait*：SPF 計算の最大待機時間（ミリ秒）。指定できる範囲は 1 ～ 600000 ミリ秒です。

	コマンドまたはアクション	目的
ステップ 11	**ospf log-adj-changes** 例： スイッチ(config)# ospf log-adj-changes	（任意）ネイバー ステートが変更されたとき、syslog メッセージを送信します。
ステップ 12	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip ospf** [*process-id* [*area-id*]] **database** 例： スイッチ# show ip ospf database	特定のルータのOSPFデータベースに関連する情報のリストを表示します。
ステップ 14	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

LSA グループ ペーシングの変更

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf***process-id* 例： スイッチ(config)# router ospf 25	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**timers lsa-group-pacing***seconds* 例： スイッチ(config-router)# timers lsa-group-pacing 15	LSA の グループ ペーシングを変更します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ループバック インターフェイスの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface loopback 0** 例： スイッチ(config)# interface loopback 0	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip address** address mask 例： スイッチ(config-if)# ip address 10.1.1.5 255.255.240.0	このインターフェイスに IP アドレスを割り当てます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip interface** 例： スイッチ# show ip interface	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF のモニタリング

IP ルーティング テーブルの内容、キャッシュの内容、およびデータベースの内容など、特定の統計情報を表示できます。

表 *78*：*IP OSPF* 統計情報の表示コマンド

show ip ospf [*process-id*]	OSPF ルーティング プロセスに関する一般情報を表示します。

show ip ospf [*process-id*] **database** [**router**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**router**] [**self-originate**] **show ip ospf** [*process-id*] **database** [**router**] [**adv-router** [*ip-address*]] **show ip ospf** [*process-id*] **database** [**network**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**asbr-summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**external**] [*link-state-id*] **show ip ospf** [*process-id area-id*] **database** [**database-summary**]	OSPF データベースに関連する情報のリストを表示します。
show ip ospf border-routes	内部の OSPF ルーティング ABR および ASBR テーブル エントリを表示します。
show ip ospf interface[*interface-name*]	OSPF に関連するインターフェイス情報を表示します。
show ip ospf neighbor[*interface-name*] [*neighbor-id*] **detail**	OSPF インターフェイス ネイバー情報を表示します。
show ip ospf virtual-links	OSPF に関連する仮想リンク情報を表示します。

OSPF の設定例

例：基本的な OSPF パラメータの設定

次に、OSPF ルーティング プロセスを設定し、プロセス番号 109 を割り当てる例を示します。

```
スイッチ(config)# router ospf 109
スイッチ(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

EIGRP に関する情報

EIGRP は IGRP のシスコ独自の拡張バージョンです。EIGRP は IGRP と同じディスタンス ベクトル アルゴリズムおよび距離情報を使用しますが、EIGRP では収束性および動作効率が大幅に改善されています。

コンバージェンス テクノロジーには、拡散更新アルゴリズム（DUAL）と呼ばれるアルゴリズムが採用されています。DUAL を使用すると、ルート計算の各段階でループが発生しなくなり、ト

ポロジの変更に関連するすべてのデバイスを同時に同期できます。トポロジ変更の影響を受けないルータは、再計算に含まれません。

IP EIGRP を導入すると、ネットワークの幅が広がります。RIP の場合、ネットワークの最大幅は 15 ホップです。EIGRP メトリックは数千ホップをサポートするほど大きいため、ネットワークを拡張するときに問題となるのは、トランスポート レイヤのホップ カウンタだけです。IP パケットが 15 台のルータを経由し、宛先方向のネクスト ホップが EIGRP によって取得されている場合だけ、EIGRP は転送制御フィールドの値を増やします。RIP ルートを宛先へのネクスト ホップとして使用する場合、転送制御フィールドでは、通常どおり値が増加します。

EIGRP の機能

EIGRP には次の機能があります。

- 高速コンバージェンス
- 差分更新：宛先のステートが変更された場合、ルーティング テーブルの内容全体を送信する代わりに差分更新を行い、EIGRP パケットに必要な帯域幅を最小化します。
- 低い CPU 使用率：完全更新パケットを受信ごとに処理する必要がないため、CPU 使用率が低下します。
- プロトコルに依存しないネイバー探索メカニズム：このメカニズムを使用し隣接ルータに関する情報を取得します。
- 可変長サブネット マスク（VLSM）
- 任意のルート集約
- 大規模ネットワークへの対応

EIGRP コンポーネント

EIGRP には次に示す 4 つの基本コンポーネントがあります。

- ネイバー探索および回復：直接接続されたネットワーク上の他のルータに関する情報を動的に取得するために、ルータで使用されるプロセスです。また、ネイバーが到達不能または動作不能になっていることを検出するためにも使用されます。ネイバー探索および回復は、サイズの小さな hello パケットを定期的に送信することにより、わずかなオーバーヘッドで実現されます。hello パケットが受信されているかぎり、Cisco ISO ソフトウェアは、ネイバーが有効に機能していると学習します。このように判別された場合、隣接ルータはルーティング情報を交換できます。
- Reliable Transport Protocol：EIGRP パケットをすべてのネイバーに確実に、順序どおりに配信します。マルチキャスト パケットとユニキャスト パケットが混在した伝送もサポートされます。EIGRP パケットには確実に送信する必要があるものと、そうでないものがあります。効率化のため、信頼性は必要時にのみ提供されます。たとえば、マルチキャスト機能があるマルチアクセス ネットワーク（イーサネットなど）では、すべてのネイバーにそれぞれ hello パケットを確実に送信する必要はありません。そのため、EIGRP は、1 つのマルチキャスト

helloを送信し、パケットに確認応答が必要ないという通知をそのパケットに含めます。他のタイプのパケット（アップデートなど）の場合は、確認応答（ACK パケット）を要求します。信頼性の高い伝送であれば、ペンディング中の未確認応答パケットがある場合、マルチキャストパケットを迅速に送信できます。このため、リンク速度が変化する場合でも、コンバージェンス時間を短く保つことができます。

- DUAL 有限状態マシンには、すべてのルート計算の決定プロセスが組み込まれており、すべてのネイバーによってアドバタイズされたすべてのルートが追跡されます。DUAL は距離情報（メトリックともいう）を使用して、効率的な、ループのないパスを選択し、さらにDUALは適切な後継ルータに基づいて、ルーティングテーブルに挿入するルートを選択します。後継ルータは、宛先への最小コスト パス（ルーティング ループに関連しないことが保証されている）を持つ、パケット転送に使用される隣接ルータです。適切な後継ルータが存在しなくても、宛先にアドバタイズするネイバーが存在する場合は再計算が行われ、この結果、新しい後継ルータが決定されます。ルートの再計算に要する時間によって、コンバージェンス時間が変わります。再計算はプロセッサに負荷がかかるため、必要でない場合は、再計算しないようにしてください。トポロジが変更されると、DUALはフィジブルサクセサの有無を調べます。適切なフィジブルサクセサが存在する場合は、それらを探して使用し、不要な再計算を回避します。
- プロトコル依存モジュールは、ネットワーク層プロトコル固有のタスクを実行します。たとえば、IP EIGRP モジュールは、IP でカプセル化された EIGRP パケットを送受信します。また、EIGRPパケットを解析したり、DUALに受信した新しい情報を通知したりします。EIGRP は DUAL にルーティング決定を行うように要求しますが、結果は IP ルーティング テーブルに格納されます。EIGRP は、他の IP ルーティング プロトコルによって取得したルートの再配信も行います。

（注） EIGRP をイネーブルにするには、スイッチまたはスタック マスター上で IP サービス フィーチャ セットが稼働している必要があります。

EIGRP NSF

スイッチスタックは、次の2つのレベルのEIGRP ノンストップ フォワーディングをサポートします。

- EIGRP NSF 認識
- EIGRP NSF 対応

EIGRP NSF 認識

IP サービス フィーチャ セットは、EIGRP NSF 認識を IPv4 に対してサポートしています。隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグ

レードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能をディセーブルにできません。この機能の詳細については、『*Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*』の「EIGRP Nonstop Forwarding (NSF) Awareness」を参照してください。

EIGRP NSF 対応

IP サービス フィーチャ セットでは、EIGRP Cisco NSF ルーティングがサポートされています。それにより、コンバージェンスの時間が短くなり、スタック マスター変更後のトラフィック損失がなくなります。この NSF 機能の詳細については、『*High Availability Configuration Guide, Cisco IOS XE Release 3S*』の「Configuring Nonstop Forwarding」を参照してください。

IP サービス フィーチャ セットは、EIGRP NSF 対応ルーティングも IPv4 に対してサポートし、スタック マスター変更後のコンバージェンスの向上と、トラフィック損失の低減を実現します。EIGRP NSF 対応のスタック マスターが再起動したとき、または新しいスタック マスターが起動してNSFが再起動したとき、このスイッチにはネイバーが存在せず、トポロジテーブルは空の状態です。スイッチは、スイッチ スタックに対するトラフィックを中断することなく、インターフェイスの起動、ネイバーの再取得、およびトポロジテーブルとルーティングテーブルの再構築を行う必要があります。EIGRPピアルータは新しいスタックマスターから学習したルートを維持し、NSF の再起動処理の間トラフィックの転送を継続します。

ネイバーによる隣接リセットを防ぐために、新しいスタックマスターはEIGRPパケットヘッダーの新しいRestart（RS）ビットを使用して再起動を示します。これを受信したネイバーは、ピア リスト内のスタックと同期を取り、スタックとの隣接関係を維持します。続いてネイバーは、RS ビットがセットされているスタック マスターにトポロジ テーブルを送信して、自身が NSF 認識デバイスであることおよび新しいスタック マスターを補助していることを示します。

スタックのピア ネイバーの少なくとも 1 つが NFS 認識デバイスであれば、スタック マスターはアップデート情報を受信してデータベースを再構築します。各 NSF 認識ネイバーは、最後のアップデートパケットにEnd of Table（EOT）マーカーを付けて送信して、テーブル情報の最後であることを示します。スタック マスターは、EOTマーカーを受信したときにコンバージェンスを認識し、続いてアップデートの送信を始めます。スタック マスターがネイバーからすべてのEOTマーカーを受信した場合、またはNSF コンバージ タイマーが期限切れになった場合、EIGRP は RIB にコンバージェンスを通知し、すべてのNSF認識ピアにトポロジテーブルをフラッディングします。

EIGRP スタブ ルーティング

EIGRP スタブ ルーティング機能は、すべてのフィーチャ セットで使用でき、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を低減させます。

（注） IP Base フィーチャ セットに含まれる EIGRP スタブ ルーティング機能では、ルーティング テーブルからの接続ルートまたはサマリー ルートをネットワーク内のほかのスイッチにアドバタイズすることだけを行います。スイッチはアクセス レイヤで EIGRP スタブ ルーティングを使用することにより、ほかのタイプのルーティング アドバタイズメントの必要性を排除しています。拡張および完全な EIGRP ルーティングでは、スイッチが IP Base 機能セットを実行している必要があります。IP Base フィーチャ セットが稼働するスイッチ上で、Multi-VRF-CE と EIGRP スタブ ルーティングを同時に設定しようとすると、設定は許可されません。IPv6 EIGRP スタブ ルーティングは、IP ベース フィーチャ セットではサポートされません。

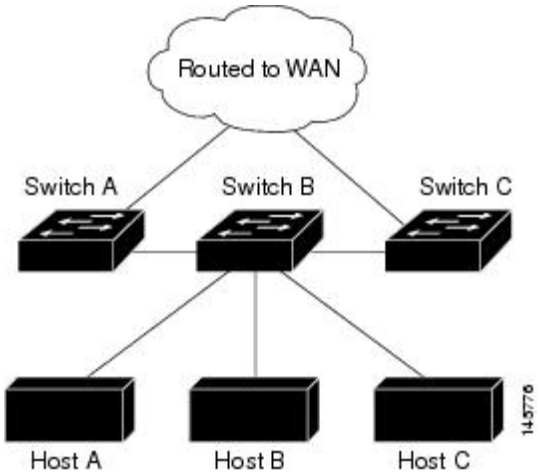
EIGRP スタブ ルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、EIGRP スタブ ルーティングを設定しているスイッチ経由です。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRP スタブ ルーティングを使用しているときは、EIGRP を使用してスイッチだけをスタブとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。指定したルートだけがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブ ルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブ ルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。スタブ ルータは、ディストリビューション ルータを使用して適切なアップデートをすべてのピアに送信します。

次の図では、スイッチ B は EIGRP スタブ ルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配信ルート、およびサマリー ルートをスイッチ A と C にアドバタイズします。スイッチ B はスイッチ A から学習したルートをアドバタイズしません（逆の場合も同様です）。

図 *59* : *EIGRP* スタブ ルータ設定



EIGRP スタブ ルーティングの詳細については、『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols*』の「Configuring EIGRP Stub Routing」の項を参照してください。

EIGRP の設定方法

EIGRP ルーティング プロセスを作成するには、EIGRP をイネーブルにし、ネットワークを関連付ける必要があります。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイス ネットワークを指定しないと、どの EIGRP アップデートでもアドバタイズされません。

（注） ネットワーク上に IGRP 用に設定されているルータがあり、この設定を EIGRP に変更する場合は、IGRP と EIGRP の両方が設定された移行ルータを指定する必要があります。この場合は、この次の項に記載されているステップ 1 ～ 3 を実行し、さらに「スプリット ホライゾンの設定」も参照してください。ルートを自動的に再配信するには、同じ AS 番号を使用する必要があります。

EIGRP のデフォルト設定

表 *79*：*EIGRP* のデフォルト設定

機能	デフォルト設定
自動サマリー	ディセーブル
デフォルト情報	再配信中は外部ルートが許可され、EIGRP プロセス間でデフォルト情報が渡されます。
デフォルト メトリック	デフォルト メトリックなしで再配信できるのは、接続されたルートおよびインターフェイスのスタティック ルートだけです。デフォルト メトリックは次のとおりです。 • 帯域幅：0 以上の kb/s • 遅延（10 マイクロ秒）：0 または 39.1 ナノ秒の倍数である任意の正の数値 • 信頼性：0 ～ 255 の任意の数値（255 の場合は信頼性が 100%） • 負荷：0 ～ 255 の数値で表される有効帯域幅（255 の場合は 100% の負荷） • MTU：バイトで表されたルートの MTU サイズ（0 または任意の正の整数）

機能	デフォルト設定
ディスタンス	内部距離：90 外部距離：170
EIGRP の隣接関係変更ログ	ディセーブル隣接関係の変更はロギングされません。
IP 認証キーチェーン	認証なし
IP 認証モード	認証なし
IP 帯域幅比率	50%
IP hello 間隔	低速非ブロードキャストマルチアクセス（NBMA）ネットワークの場合：60 秒、それ以外のネットワークの場合：5 秒
IP ホールドタイム	低速 NBMA ネットワークの場合：180 秒、それ以外のネットワークの場合：15 秒
IP スプリットホライズン	イネーブル
IP サマリー アドレス	サマリー集約アドレスは未定義
メトリック重み	tos：0、k1 および k3：1、k2、k4、および k5：0
ネットワーク	指定なし
ノンストップ フォワーディング（NSF）認識	IP サービス フィーチャ セットを実行するスイッチ上で IPv4 対してイネーブルになっています。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
NSF 対応	ディセーブル （注） スイッチは EIGRP NSF 対応ルーティングを IPv4 に対してサポートします。
オフセットリスト	ディセーブル
ルータ EIGRP	ディセーブル
メトリック設定	ルート マップにはメトリック設定なし
トラフィック共有	メトリックの比率に応じて配分

機能	デフォルト設定
バリアンス	1（等コスト ロード バランシング）

基本的な EIGRP パラメータの設定

はじめる前に

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** autonomous-system 例： スイッチ(config)# **router eigrp 10**	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。AS 番号によって他のEIGRPルータへのルートを特定し、ルーティング情報をタグ付けします。
ステップ 3	**nsf** 例： スイッチ(config)# **nsf**	（任意）EIGRP NSF をイネーブルにします。スタック マスターおよびそのすべてのピア上でこのコマンドを入力します。
ステップ 4	**network** network-number 例： スイッチ(config)# **network 192.168.0.0**	ネットワークを EIGRP ルーティング プロセスに関連付けます。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。
ステップ 5	**eigrp log-neighbor-changes** 例： スイッチ(config)# **eigrp log-neighbor-changes**	（任意）EIGRP 隣接関係変更のロギングをイネーブルにし、ルーティング システムの安定性をモニタします。
ステップ 6	**metric weights***tos k1 k2 k3 k4 k5* 例： スイッチ(config)# **metric weights 0 2 0 2 0 0**	（任意）EIGRP メトリックを調整します。デフォルト値はほとんどのネットワークで適切に動作するよう入念に設定されていますが、調整することも可能です。 **注意** メトリックを設定する作業は複雑です。熟練したネットワーク設計者の指導がない場合は、行わないでください。

	コマンドまたはアクション	目的
ステップ 7	**offset-list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*] 例： スイッチ(config)# **offset-list 21 out 10**	（任意）オフセットリストをルーティングメトリックに適用し、EIGRP によって取得したルートへの着信および発信メトリックを増加します。アクセスリストまたはインターフェイスを使用し、オフセットリストを制限できます。
ステップ 8	**auto-summary** 例： スイッチ(config)# **auto-summary**	（任意）ネットワークレベルルートへのサブネットルートの自動サマライズをイネーブルにします。
ステップ 9	**ip summary-address eigrp***autonomous-system-number address mask* 例： スイッチ(config)# **ip summary-address eigrp 1 192.168.0.0 255.255.0.0**	（任意）サマリー集約を設定します。
ステップ 10	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 11	**show ip protocols** 例： スイッチ# **show ip protocols**	入力を確認します。 NSF 認識の場合、出力に次のように表示されます。 *** IP Routing is NSF aware *** EIGRP NSF enabled
ステップ 12	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

EIGRP インターフェイスの設定

インターフェイスごとに、他の EIGRP パラメータを任意で設定できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# interface gigabitethernet 1/0/1	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip bandwidth-percent eigrp***percent* 例： スイッチ(config-if)# ip bandwidth-percent eigrp 60	（任意）インターフェイスで EIGRP が使用できる帯域幅の割合を設定します。デフォルト値は 50% です。
ステップ 4	**ip summary-address eigrp***autonomous-system-number address mask* 例： スイッチ(config-if)# ip summary-address eigrp 109 192.161.0.0 255.255.0.0	（任意）指定されたインターフェイスのサマリー集約アドレスを設定します（auto-summary がイネーブルの場合は、通常設定する必要はありません）。
ステップ 5	**ip hello-interval eigrp***autonomous-system-number seconds* 例： スイッチ(config-if)# ip hello-interval eigrp 109 10	（任意）EIGRP ルーティング プロセスの hello タイム インターバルを変更します。指定できる範囲は 1 ～ 65535 秒です。低速 NBMA ネットワークの場合のデフォルト値は 60 秒、その他のすべてのネットワークでは 5 秒です。
ステップ 6	**ip hold-time eigrp***autonomous-system-number seconds* 例： スイッチ(config-if)# ip hold-time eigrp 109 40	（任意）EIGRP ルーティング プロセスのホールド タイム インターバルを変更します。指定できる範囲は 1 ～ 65535 秒です。低速 NBMA ネットワークの場合のデフォルト値は 180 秒、その他のすべてのネットワークでは 15 秒です。 **注意** ホールドタイムを調整する前に、シスコのテクニカルサポートにお問い合わせください。

	コマンドまたはアクション	目的
ステップ 7	**no ip split-horizon eigrp***autonomous-system-number* 例： `スイッチ(config-if)# no ip split-horizon eigrp 109`	（任意）スプリットホライズンをディセーブルにし、ルート情報が情報元インターフェイスからルータによってアドバタイズされるようにします。
ステップ 8	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip eigrp interface** 例： `スイッチ# show ip eigrp interface`	EIGRP がアクティブであるインターフェイス、およびそれらのインターフェイスに関連する EIGRP の情報を表示します。
ステップ 10	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

EIGRP ルート認証の設定

EIGRP ルート認証を行うと、EIGRP ルーティング プロトコルからのルーティング アップデートに関する MD5 認証が可能になり、承認されていない送信元から無許可または問題のあるルーティング メッセージを受け取ることがなくなります。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** interface-id 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip authentication mode eigrp***autonomous-system***md5** 例： `スイッチ(config-if)# ip authentication mode eigrp 104 md5`	IP EIGRP パケットの MD5 認証をイネーブルにします。
ステップ 4	**ip authentication key-chain eigrp** *autonomous-system key-chain* 例： `スイッチ(config-if)# ip authentication key-chain eigrp 105 chain1`	IP EIGRP パケットの認証をイネーブルにします。
ステップ 5	**exit** 例： `スイッチ(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**key chain** *name-of-chain* 例： `スイッチ(config)# key chain chain1`	キーチェーンを識別し、キーチェーン コンフィギュレーション モードを開始します。ステップ 4 で設定した名前を指定します。
ステップ 7	**key***number* 例： `スイッチ(config-keychain)# key 1`	キーチェーン コンフィギュレーション モードで、キー番号を識別します。
ステップ 8	**key-string***text* 例： `スイッチ(config-keychain-key)# key-string key1`	キーチェーン コンフィギュレーション モードで、キーストリングを識別します。
ステップ 9	**accept-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*} 例： `スイッチ(config-keychain-key)#`	（任意）キーを受信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日

	コマンドまたはアクション	目的
	`accept-lifetime 13:30:00 Jan 25 2011 duration 7200`	です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 10	**send-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*} 例： `スイッチ(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600`	（任意）キーを送信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 11	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show key chain** 例： `スイッチ# show key chain`	認証キーの情報を表示します。
ステップ 13	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

EIGRP のモニタリングおよびメンテナンス

ネイバーテーブルからネイバーを削除できます。さらに、各種EIGRPルーティング統計情報を表示することもできます。下の図に、ネイバーを削除し、統計情報を表示する特権 EXEC コマンドを示します。表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

表 *80*：*IP EIGRP* の *clear* および *show* コマンド

clear ip eigrp neighbors [*if-address* | *interface*]	ネイバーテーブルからネイバーを削除します。

show ip eigrp interface [*interface*] [*as number*]	EIGRP に設定されているインターフェイスに関する情報を表示します。
show ip eigrp neighbors [*type-number*]	EIGRP によって検出されたネイバーを表示します。
show ip eigrp topology [*autonomous-system-number*] | [[*ip-address*] *mask*]]	指定されたプロセスの EIGRP トポロジ テーブルを表示します。
show ip eigrp traffic [*autonomous-system-number*]	すべてまたは指定された EIGRP プロセスの送受信パケット数を表示します。

BGP に関する情報

ボーダー ゲートウェイ プロトコル（BGP）は、Exterior Gateway Protocol です。自律システム間で、ループの発生しないルーティング情報交換を保証するドメイン間ルーティング システムを設定するために使用されます。自律システムは、同じ管理下で動作して RIP や OSPF などの Interior Gateway Protocol（IGP）を境界内で実行し、Exterior Gateway Protocol（EGP）を使用して相互接続されるルータで構成されます。BGP バージョン 4 は、インターネット内でドメイン間ルーティングを行うための標準 EGP です。このプロトコルは、RFC 1163、1267、および 1771 で定義されています。BGP の詳細については、『*Internet Routing Architectures*』（Cisco Press 刊）、および『*Cisco IP and IP Routing Configuration Guide*』の「Configuring BGP」を参照してください。

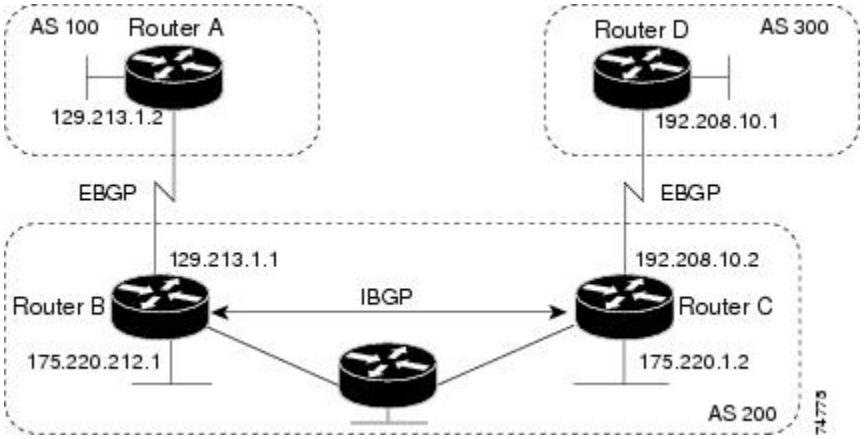
BGP コマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』の「IP Routing Protocols」を参照してください。

BGP ネットワーク トポロジ

同じ自律システム（AS）に属し、BGP アップデートを交換するルータは内部BGP（IBGP）を実行し、異なる自律システムに属し、BGP アップデートを交換するルータは外部 BGP（EBGP）を実行します。大部分のコンフィギュレーション コマンドは、EBGP と IBGP で同じですが、ルーティング アップデートが自律システム間で交換されるか（EBGP）、または AS 内で交換されるか

（IBGP）という点で異なります。下の図に、EBGP と IBGP の両方を実行しているネットワークを示します。

図 *60*：*EBGP*、*IBGP*、および複数の自律システム



外部 AS と情報を交換する前に、BGP は AS 内のルータ間で内部 BGP ピアリングを定義し、IGRP や OSPF など AS 内で稼働する IGP に BGP ルーティング情報を再配信して、AS 内のネットワークに到達することを確認します。

BGP ルーティング プロセスを実行するルータは、通常 BGP スピーカーと呼ばれます。BGP はトランスポート プロトコルとして伝送制御プロトコル（TCP）を使用します（特にポート 179）。ルーティング情報を交換するため相互に TCP 接続された 2 つの BGP スピーカーを、ピアまたはネイバーと呼びます。上の図では、ルータ A と B が BGP ピアで、ルータ B と C、ルータ C と D も同様です。ルーティング情報は、宛先ネットワークへの完全パスを示す一連の AS 番号です。BGP はこの情報を使用し、ループのない自律システム マップを作成します。

このネットワークの特徴は次のとおりです。

- ルータ A および B では EBGP が、ルータ B および C では IBGP が稼働しています。EBGP ピアは直接接続されていますが、IBGP ピアは直接接続されていないことに注意してください。IGP が稼働し、2 つのネイバーが相互に到達するかぎり、IBGP ピアを直接接続する必要はありません。
- AS 内のすべての BGP スピーカーは、相互にピア関係を確立する必要があります。つまり、AS 内の BGP スピーカーは、論理的な完全メッシュ型に接続する必要があります。BGP4 は、論理的な完全メッシュに関する要求を軽減する 2 つの技術（連合およびルート リフレクタ）を提供します。
- AS 200 は AS 100 および AS 300 の中継 AS です。つまり、AS 200 は AS 100 と AS 300 間でパケットを転送するために使用されます。

BGP ピアは完全な BGP ルーティング テーブルを最初に交換し、差分更新だけを送信します。BGP ピアはキープアライブ メッセージ（接続が有効であることを確認）、および通知メッセージ（エラーまたは特殊条件に応答）を交換することもできます。

BGP の場合、各ルートはネットワーク番号、情報が通過した自律システムのリスト（自律システム パス）、および他のパス属性リストで構成されます。BGP システムの主な機能は、AS パスのリストに関する情報など、ネットワークの到達可能性情報を他の BGP システムと交換することです。この情報は、AS が接続されているかどうかを判別したり、ルーティング ループをプルーニングしたり、AS レベル ポリシー判断を行うために使用できます。

Cisco IOS が稼働しているルータまたはスイッチが IBGP ルートを選択または使用するのは、ネクストホップ ルータで使用可能なルートがあり、IGP から同期信号を受信している（IGP 同期がディセーブルの場合は除く）場合です。複数のルートが使用可能な場合、BGP は属性値に基づいてパスを選択します。BGP 属性については、「BGP 判断属性の設定」の項を参照してください。

BGP バージョン 4 ではクラスレス ドメイン間ルーティング（CIDR）がサポートされているため、集約ルートを作成してスーパーネットを構築し、ルーティング テーブルのサイズを削減できます。CIDR は、BGP 内部のネットワーク クラスの概念をエミュレートし、IP プレフィックスのアドバタイズをサポートします。

NSF 認識

BGP NSF 認識は、IP サービス フィーチャ セットで IPv4 に対してサポートされます。BGP ルーティングでこの機能をイネーブルにするには、グレースフル リスタートをイネーブルにする必要があります。隣接ルータが NSF 対応で、この機能がイネーブルである場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能の詳細については、『*Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*』の「BGP Nonstop Forwarding (NSF) Awareness」を参照してください。

BGP ルーティングに関する情報

BGP ルーティングをイネーブルにするには、BGP ルーティング プロセスを確立し、ローカル ネットワークを定義します。BGP はネイバーとの関係を完全に認識する必要があるため、BGP ネイバーも指定する必要があります。

BGP は、内部および外部の 2 種類のネイバーをサポートします。内部ネイバーは同じ AS 内に、外部ネイバーは異なる AS 内にあります。通常の場合、外部ネイバーは相互に隣接し、1 つのサブネットを共有しますが、内部ネイバーは同じ AS 内の任意の場所に存在します。

スイッチではプライベート AS 番号を使用できます。プライベート AS 番号は通常サービス プロバイダーによって割り当てられ、ルートが外部ネイバーにアドバタイズされないシステムに設定されます。プライベート AS 番号の範囲は 64512 ～ 65535 です。AS パスからプライベート AS 番号を削除するように外部ネイバーを設定するには、**neighbor remove-private-as** ルータ コンフィギュレーション コマンドを使用します。この結果、外部ネイバーにアップデートを渡すとき、AS パス内にプライベート AS 番号が含まれている場合は、これらの番号が削除されます。

AS が別の AS からさらに別の AS にトラフィックを渡す場合は、アドバタイズ対象のルートに矛盾が存在しないことが重要です。BGP がルートをアドバタイズしてから、ネットワーク内のすべてのルータが IGP を通してルートを学習した場合、AS は一部のルータがルーティングできなかっ

たトラフィックを受信することがあります。このような事態を避けるため、BGP は IGP が AS に情報を伝播し、BGP が IGP と同期化されるまで、待機する必要があります。同期化は、デフォルトでイネーブルに設定されています。AS が特定の AS から別の AS にトラフィックを渡さない場合、または自律システム内のすべてのルータでBGPが稼働している場合は、同期化をディセーブルにし、IGP内で伝送されるルート数を少なくして、BGPがより短時間で収束するようにします。

ルーティング ポリシーの変更

ピアのルーティング ポリシーには、インバウンドまたはアウトバウンド ルーティング テーブル アップデートに影響する可能性があるすべての設定が含まれます。BGP ネイバーとして定義された2台のルータは、BGP接続を形成し、ルーティング情報を交換します。このあとでBGP フィルタ、重量、距離、バージョン、またはタイマーを変更する場合、または同様の設定変更を行う場合は、BGP セッションをリセットし、設定の変更を有効にする必要があります。

リセットには、ハード リセットとソフト リセットの 2 種類があります。Cisco IOS Release 12.1 以降では、事前に設定を行わなくても、ソフトリセットを使用できます。事前設定なしにソフトリセットを使用するには、両方の BGP ピアでソフト ルート リフレッシュ機能がサポートされていなければなりません。この機能は、ピアによって TCP セッションが確立されたときに送信される OPEN メッセージに格納されてアドバタイズされます。ソフト リセットを使用すると、BGP ルータ間でルート リフレッシュ要求およびルーティング情報を動的に交換したり、それぞれのアウトバウンド ルーティング テーブルをあとで再アドバタイズできます。

- ソフト リセットによってネイバーからインバウンド アップデートが生成された場合、このリセットはダイナミック インバウンド ソフト リセットといいます。
- ソフトリセットによってネイバーに一連のアップデートが送信された場合、このリセットはアウトバウンド ソフト リセットといいます。

ソフト インバウンド リセットが発生すると、新規インバウンド ポリシーが有効になります。ソフトアウトバウンドリセットが発生すると、BGPセッションがリセットされずに、新規ローカルアウトバウンドポリシーが有効になります。アウトバウンドポリシーのリセット中に新しい一連のアップデートが送信されると、新規インバウンド ポリシーも有効になる場合があります。

下の表に、ハード リセットとソフト リセットの利点および欠点を示します。

表 *81*：ハード リセットとソフト リセットの利点および欠点

リセット タイプ	利点	欠点
ハード リセット	メモリ オーバーヘッドが発生しません。	ネイバーから提供されたBGP、IP、およびFIBテーブルのプレフィックスが失われます。推奨しません。
発信ソフト リセット	ルーティングテーブルアップデートが設定、保管されません。	インバウンド ルーティング テーブル アップデートがリセットされません。

リセット タイプ	利点	欠点
ダイナミック インバウンドソフトリセット	BGP セッションおよびキャッシュがクリアされません。 ルーティング テーブル アップデートを保管する必要がなく、メモリ オーバーヘッドが発生しません。	両方の BGP ルータでルート リフレッシュ機能をサポートする必要があります（Cisco IOS Release 12.1 以降）。

BGP 判断属性

BGP スピーカーが複数の自律システムから受信したアップデートが、同じ宛先に対して異なるパスを示している場合、BGP スピーカーはその宛先に到達する最適パスを 1 つ選択する必要があります。選択されたパスはBGPルーティング テーブルに格納され、ネイバーに伝播されます。この判断は、アップデートに格納されている属性値、およびBGPで設定可能な他の要因に基づいて行われます。

BGP ピアはネイバー AS からプレフィックスに対する 2 つの EBGP パスを学習するとき、最適パスを選択してIPルーティング テーブルに挿入します。BGPマルチパス サポートがイネーブルで、同じネイバー自律システムから複数の EBGP パスを学習する場合、単一の最適パスの代わりに、複数のパスがIPルーティング テーブルに格納されます。そのあと、パケット スイッチング中に、複数のパス間でパケット単位または宛先単位のロード バランシングが実行されます。maximum-paths**maximum-paths** ルータ コンフィギュレーション コマンドは、許可されるパス数を制御します。

これらの要因により、BGP が最適パスを選択するために属性を評価する順序が決まります。

1. パスで指定されているネクストホップが到達不能な場合、このアップデートは削除されます。BGP ネクスト ホップ属性（ソフトウェアによって自動判別される）は、宛先に到達するために使用されるネクストホップのIPアドレスです。EBGPの場合、通常このアドレスは**neighbor remote-as router** ルータ コンフィギュレーション コマンドで指定されたネイバーの IP アドレスです。ネクストホップの処理をディセーブルにするには、ルート マップまたは **neighbor next-hop-self** ルータ コンフィギュレーション コマンドを使用します。
2. 最大の重みのパスを推奨します（シスコ独自のパラメータ）。ウェイト属性はルータにローカルであるため、ルーティング アップデートで伝播されません。デフォルトでは、ルータ送信元のパスに関するウェイト属性は 32768 で、それ以外のパスのウェイト属性は 0 です。最大の重みのルートを推奨します。重みを設定するには、アクセス リスト、ルート マップ、または **neighbor weight** ルータ コンフィギュレーション コマンドを使用します。
3. ローカルプリファレンス値が最大のルートを推奨します。ローカルプリファレンスはルーティング アップデートに含まれ、同じ AS 内のルータ間で交換されます。ローカル初期設定属性のデフォルト値は 100 です。ローカルプリファレンスを設定するには、**bgp default local-preference** ルータ コンフィギュレーション コマンドまたはルート マップを使用します。
4. ローカル ルータ上で稼働する BGP から送信されたルートを推奨します。
5. AS パスが最短のルートを推奨します。

6 送信元タイプが最小のルートを推奨します。内部ルートまたはIGPは、EGPによって学習されたルートよりも小さく、EGPで学習されたルートは、未知の送信元のルートまたは別の方法で学習されたルートよりも小さくなります。

7 想定されるすべてのルートについてネイバーASが同じである場合は、MEDメトリック属性が最小のルートを推奨します。MED を設定するには、ルート マップまたは **default-metric** ルータ コンフィギュレーション コマンドを使用します。IBGP ピアに送信されるアップデートには、MED が含まれます。

8 内部（IBGP）パスより、外部（EBGP）パスを推奨します。

9 最も近い IGP ネイバー（最小の IGP メトリック）を通って到達できるルートを推奨します。ルータは、AS 内の最短の内部パス（BGP のネクストホップへの最短パス）を使用し、宛先に到達するためです。

10 次の条件にすべて該当する場合は、このパスのルートを IP ルーティング テーブルに挿入してください。

最適ルートと目的のルートがともに外部ルートである

最適ルートと目的のルートの両方が、同じネイバー自律システムからのルートである

maximum-paths がイネーブルである

11 マルチパスがイネーブルでない場合は、BGP ルータ ID の IP アドレスが最小であるルートを推奨します。通常、ルータ ID はルータ上の最大の IP アドレスまたはループバック（仮想）アドレスですが、実装に依存することがあります。

ルート マップ

BGP内でルートマップを使用すると、ルーティング情報を制御、変更したり、ルーティング ドメイン間でルートを再配信する条件を定義できます。ルートマップの詳細については、「Using Route Maps to Redistribute Routing Information」の項を参照してください。各ルート マップには、ルート マップを識別する名前（マップ タグ）およびオプションのシーケンス番号が付いています。

BGP フィルタリング

BGPアドバタイズメントをフィルタリングするには、**as-path access-list** グローバル コンフィギュレーション コマンドや **neighbor filter-list** ルータ コンフィギュレーション コマンドなどの AS パス フィルタを使用します。**neighbor distribute-list** ルータ コンフィギュレーション コマンドとアクセス リストを併用することもできます。distribute-list フィルタはネットワーク番号に適用されます。**distribute-list** コマンドの詳細については、「ルーティング アップデートのアドバタイズおよび処理の制御」の項を参照してください。

ネイバー単位でルート マップを使用すると、アップデートをフィルタリングしたり、さまざまな属性を変更したりできます。ルートマップは、インバウンドアップデートまたはアウトバウンドアップデートのいずれかに適用できます。ルート マップを渡すルートだけが、アップデート内で送信または許可されます。着信および発信の両方のアップデートで、ASパス、コミュニティ、およびネットワーク番号に基づくマッチングがサポートされています。AS パスのマッチングには

match as-path access-list ルート マップ コマンド、コミュニティに基づくマッチングには **match community-list** ルートマップ コマンド、ネットワークに基づくマッチングには **ip access-list** グローバル コンフィギュレーション コマンドが必要です。

BGP フィルタリングのプレフィックス リスト

neighbor distribute-list ルータ コンフィギュレーション コマンドを含む多数の BGP ルート フィルタリング コマンドでは、アクセス リストの代わりにプレフィックス リストを使用できます。プレフィックス リストを使用すると、大規模リストのロードおよび検索パフォーマンスが改善し、差分更新がサポートされ、コマンドライン インターフェイス（CLI）設定が簡素化され、柔軟性が増すなどの利点が生じます。

プレフィックスリストによるフィルタリングでは、アクセスリストの照合の場合と同様に、プレフィックス リストに記載されたプレフィックスとルートのプレフィックスが照合されます。一致すると、一致したルートが使用されます。プレフィックスが許可されるか、または拒否されるかは、次に示すルールに基づいて決定されます。

- 空のプレフィックス リストはすべてのプレフィックスを許可します。
- 特定のプレフィックスがプレフィックスリストのどのエントリとも一致しなかった場合、実質的に拒否されたものと見なされます。
- 指定されたプレフィックスと一致するエントリがプレフィックスリスト内に複数存在する場合は、シーケンス番号が最小であるプレフィックス リスト エントリが識別されます。

デフォルトでは、シーケンス番号は自動生成され、5 ずつ増分します。シーケンス番号の自動生成をディセーブルにした場合は、エントリごとにシーケンス番号を指定する必要があります。シーケンス番号を指定する場合の増分値に制限はありません。増分値が 1 の場合は、このリストに追加エントリを挿入できません。増分値が大きい場合は、値がなくなることがあります。

BGP コミュニティ フィルタリング

BGP コミュニティ フィルタリングは、COMMUNITIES 属性の値に基づいてルーティング情報の配信を制御する BGP の方法の 1 つです。この属性によって、宛先はコミュニティにグループ化され、コミュニティに基づいてルーティング判断が適用されます。この方法を使用すると、ルーティング情報の配信制御を目的とする BGP スピーカーの設定が簡単になります。

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。各宛先は複数のコミュニティに属します。AS管理者は、宛先が属するコミュニティを定義できます。デフォルトでは、すべての宛先が一般的なインターネット コミュニティに属します。コミュニティは、過渡的でグローバルなオプションの属性である、COMMUNITIES 属性（1 ～ 4294967200 の数値）によって識別されます。事前に定義された既知のコミュニティの一部を、次に示します。

- **internet**：このルートをインターネット コミュニティにアドバタイズします。すべてのルータが所属します。
- **no-export**：EBGP ピアにこのルートをアドバタイズしません。
- **no-advertise**：どのピア（内部または外部）にもこのルートをアドバタイズしません。

- **local-as**：ローカルな AS 外部のピアにこのルートをアドバタイズしません。

コミュニティに基づき、他のネイバーに許可、送信、配信するルーティング情報を制御できます。BGP スピーカーは、ルートを学習、アドバタイズ、または再配信するときに、ルートのコミュニティを設定、追加、または変更します。ルートを集約すると、作成された集約内の COMMUNITIES 属性に、すべての初期ルートの全コミュニティが含まれます。

コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。さらに、アクセスリストの場合と同様、一連のコミュニティ リストを作成することもできます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。

コミュニティに基づいて COMMUNITIES 属性および match 句を設定するには、「ルート マップによるルーティング情報の再配信」に記載されている **match community-list** および **set community** ルート マップ コンフィギュレーション コマンドを参照してください。

BGP ネイバーおよびピア グループ

通常、BGP ネイバーの多くは同じアップデート ポリシー（同じアウトバウンド ルート マップ、配信リスト、フィルタ リスト、アップデート送信元など）を使用して設定されます。アップデートポリシーが同じネイバーをピア グループにまとめると設定が簡単になり、アップデートの効率が高まります。多数のピアを設定した場合は、この方法を推奨します。

BGP ピア グループを設定するには、ピア グループを作成し、そこにオプションを割り当てて、ピア グループ メンバーとしてネイバーを追加します。ピア グループを設定するには、**neighbor** ルータ コンフィギュレーション コマンドを使用します。デフォルトでは、ピア グループ メンバーは remote-as（設定されている場合）、version、update-source、out-route-map、out-filter-list、out-dist-list、minimum-advertisement-interval、next-hop-self など、ピア グループの設定オプションをすべて継承します。すべてのピア グループ メンバーは、ピア グループに対する変更を継承します。また、アウトバウンド アップデートに影響しないオプションを無効にするように、メンバーを設定することもできます。

集約ルート

クラスレス ドメイン間ルーティング（CIDR）を使用すると、集約ルート（またはスーパーネット）を作成して、ルーティング テーブルのサイズを最小化できます。BGP 内に集約ルートを設定するには、集約ルートを BGP に再配信するか、または BGP ルーティング テーブル内に集約エントリを作成します。BGP テーブル内に特定のエントリがさらに 1 つまたは複数存在する場合は、BGP テーブルに集約アドレスが追加されます。

ルーティング ドメイン コンフェデレーション

IBGP メッシュを削減する方法の 1 つは、自律システムを複数のサブ自律システムに分割して、単一の自律システムとして認識される単一の連合にグループ化することです。各自律システムは内部で完全にメッシュ化されていて、同じコンフェデレーション内の他の自律システムとの間には数本の接続があります。異なる自律システム内にあるピアでは EBGP セッションが使用されます

が、ルーティング情報はIBGPピアと同様な方法で交換されます。具体的には、ネクストホップ、MED、およびローカル プリファレンス情報は維持されます。すべての自律システムで単一のIGPを使用できます。

BGP ルート リフレクタ

BGP では、すべての IBGP スピーカーを完全メッシュ構造にする必要があります。外部ネイバーからルートを受信したルータは、そのルートをすべての内部ネイバーにアドバタイズする必要があります。ルーティング情報のループを防ぐには、すべての IBGP スピーカーを接続する必要があります。内部ネイバーは、内部ネイバーから学習されたルートを他の内部ネイバーに送信しません。

ルート リフレクタを使用すると、学習されたルートをネイバーに渡す場合に他の方法が使用されるため、すべての IBGP スピーカーを完全メッシュ構造にする必要はありません。IBGP ピアをルートリフレクタに設定すると、そのIBGPピアはIBGPによって学習されたルートを一連のIBGPネイバーに送信するようになります。ルートリフレクタの内部ピアには、クライアントピアと非クライアント ピア（AS 内の他のすべてのルータ）の 2 つのグループがあります。ルート リフレクタは、これらの 2 つのグループ間でルートを反映させます。ルート リフレクタおよびクライアントピアは、クラスタを形成します。非クライアントピアは相互に完全メッシュ構造にする必要がありますが、クライアント ピアはその必要はありません。クラスタ内のクライアントは、そのクラスタ外の IBGP スピーカーと通信しません。

アドバタイズされたルートを受信したルート リフレクタは、ネイバーに応じて、次のいずれかのアクションを実行します。

- 外部 BGP スピーカーからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズします。
- 非クライアント ピアからのルートをすべてのクライアントにアドバタイズします。
- クライアントからのルートをすべてのクライアントおよび非クライアントピアにアドバタイズします。したがって、クライアントを完全メッシュ構造にする必要はありません。

通常、クライアントのクラスタにはルート リフレクタが 1 つあり、クラスタはルート リフレクタのルータ ID で識別されます。冗長性を高めて、シングル ポイントでの障害を回避するには、クラスタに複数のルート リフレクタを設定する必要があります。このように設定した場合は、ルートリフレクタが同じクラスタ内のルートリフレクタからのアップデートを認識できるように、クラスタ内のすべてのルート リフレクタに同じクラスタ ID（4 バイト）を設定する必要があります。クラスタを処理するすべてのルート リフレクタは完全メッシュ構造にし、一連の同一なクライアント ピアおよび非クライアント ピアを設定する必要があります。

ルート ダンプニング

ルート フラップ ダンプニングは、インターネットワーク内でフラッピング ルートの伝播を最小化するためのBGP機能です。ルートの状態が使用可能、使用不可能、使用可能、使用不可能という具合に、繰り返し変化する場合、ルートはフラッピングと見なされます。ルート ダンプニングがイネーブルの場合は、フラッピングしているルートにペナルティ値が割り当てられます。ルー

トの累積ペナルティが、設定された制限値に到達すると、ルートが稼働している場合であっても、BGP はルートのアドバタイズメントを抑制します。再使用限度は、ペナルティと比較される設定可能な値です。ペナルティが再使用限度より小さくなると、起動中の抑制されたルートのアドバタイズメントが再開されます。

IBGP によって取得されたルートには、ダンプニングが適用されません。このポリシーにより、IBGP ピアのペナルティが AS 外部のルートよりも大きくなることはありません。

BGP の追加情報

BGP 設定の詳しい説明については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Routing Protocols」にある「BGPの設定」を参照してください。特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

BGP の設定方法

BGP のデフォルト設定

下の表に、BGP のデフォルト設定を示します。すべての特性の詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』の特定のコマンドを参照してください。

表 *82* : *BGP* のデフォルト設定

機能	デフォルト設定
集約アドレス	ディセーブル：未定義
AS パス アクセス リスト	未定義
自動サマリー	ディセーブル
最適パス	• ルータはルートを選択する場合に *as-path* を考慮し、外部 BGP ピアからの類似ルートは比較しません。 • ルータ ID の比較：ディセーブル
BGP コミュニティ リスト	• 番号：未定義。コミュニティ番号を示す特定の値を許可すると、許可されていないその他すべてのコミュニティ番号は、暗黙の拒否にデフォルト設定されます。 • フォーマット：シスコデフォルトフォーマット（32 ビット番号）

機能	デフォルト設定
BGP 連合 ID/ピア	• ID：未設定 • ピア：識別なし
BGP 高速外部フォールオーバー	イネーブル
BGP ローカル初期設定	100。指定できる範囲は 0～4294967295 です（大きな値を推奨）。
BGP ネットワーク	指定なし。バックドア ルートのアドバタイズなし
BGP ルート ダンプニング	デフォルトでは、ディセーブルです。イネーブルの場合は、次のようになります。 • 半減期は 15 分 • 再使用は 750（10 秒増分） • 抑制は 2000（10 秒増分） • 最大抑制時間は半減期の 4 倍（60 分）
BGP ルータ ID	ループバック インターフェイスに IP アドレスが設定されている場合は、ループバック インターフェイスの IP アドレス、またはルータの物理インターフェイスに対して設定された最大の IP アドレス
デフォルトの情報送信元（プロトコルまたはネットワーク再配信）	ディセーブル
デフォルト メトリック	自動メトリック変換（組み込み）
ディスタンス	• 外部ルート アドミニストレーティブ ディスタンス：20（有効値は 1 ～ 255） • 内部ルート アドミニストレーティブ ディスタンス：200（有効値は 1 ～ 255） • ローカル ルート アドミニストレーティブ ディスタンス：200（有効値は 1 ～ 255）

機能	デフォルト設定
ディストリビュートリスト	• 入力（アップデート中に受信されたネットワークをフィルタリング）：ディセーブル • 出力（アップデート中のネットワークのアドバタイズを抑制）：ディセーブル
内部ルート再配信	ディセーブル
IP プレフィックス リスト	未定義
Multi Exit Discriminator（MED）	• 常に比較：ディセーブル。異なる自律システム内のネイバーからのパスに対して、MED を比較しません。 • 最適パスの比較：ディセーブル • 最悪パスである MED の除外：ディセーブル • 決定的な MED 比較：ディセーブル

機能	デフォルト設定
ネイバー	• アドバタイズメントインターバル：外部ピアの場合は30秒、内部ピアの場合は 5 秒 • ロギング変更：イネーブル • 条件付きアドバタイズ：ディセーブル • デフォルト送信元：ネイバーに送信されるデフォルト ルートはなし • 説明：なし • ディストリビュート リスト：未定義 • 外部 BGP マルチホップ：直接接続されたネイバーだけを許可 • フィルタ リスト：使用しない • 受信したプレフィックスの最大数：制限なし • ネクストホップ（BGP ネイバーのネクストホップとなるルータ）：ディセーブル • パスワード：ディセーブル • ピア グループ：定義なし、割り当てメンバーなし • プレフィックス リスト：指定なし • リモート AS（ネイバー BGP テーブルへのエントリ追加）：ピア定義なし • プライベート AS 番号の削除：ディセーブル • ルート マップ：ピアへの適用なし • コミュニティ属性送信：ネイバーへの送信なし。 • シャットダウンまたはソフト再設定：ディセーブル • タイマー：60 秒、ホールドタイム：180 秒 • アップデート送信元：最適ローカル アドレス • バージョン：BGP バージョン 4 • 重み：BGP ピアによって学習されたルート：0、ローカル ルータから取得されたルート：32768
NSF[5] 認識	ディセーブル状態の [6]。イネーブル状態の場合、レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。

機能	デフォルト設定
ルート リフレクタ	未設定
同期化（BGP および IGP）	ディセーブル
テーブルマップ アップデート	ディセーブル
タイマー	キープアライブ：60 秒、ホールドタイム：180 秒

5 Nonstop Forwarding

6 NSF 認識は、グレースフル リスタートをイネーブルにすることにより、IP サービス フィーチャ セットを実行するスイッチ上で IPv4 に対してイネーブルにできます

BGP ルーティングのイネーブル化

はじめる前に

（注） BGP をイネーブルにするには、スイッチまたはスタック マスター上で IP サービス フィーチャ セットが稼働している必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： スイッチ(config)# ip routing	IP ルーティングをイネーブルにします。
ステップ 3	**router bgp***autonomous-system* 例： スイッチ(config)# router bgp 45000	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。指定できる AS 番号は 1～65535 です。64512～65535 は、プライベート AS 番号専用です。

	コマンドまたはアクション	目的
ステップ 4	**network***network-number* [**mask***network-mask*] [**route-map***route-map-name*] 例： `スイッチ(config)# network 10.108.0.0`	このASに対してローカルとなるようにネットワークを設定し、BGP テーブルにネットワークを格納します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***number* 例： `スイッチ(config)# neighbor 10.108.1.2 remote-as 65200`	BGP ネイバー テーブルに設定を追加し、IP アドレスによって識別されるネイバーが、指定されたASに属することを示します。 EBGPの場合、通常ネイバーは直接接続されており、IPアドレスは接続のもう一方の端におけるインターフェイスのアドレスです。 IBGPの場合、IPアドレスにはルータ インターフェイス内の任意のアドレスを指定できます。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remove-private-as** 例： `スイッチ(config)# neighbor 172.16.2.33 remove-private-as`	（任意）発信ルーティング アップデート内の AS パスからプライベート AS 番号を削除します。
ステップ 7	同期 例： `スイッチ(config)# synchronization`	（任意）BGP と IGP の同期化をイネーブルにします。
ステップ 8	**auto-summary** 例： `スイッチ(config)# auto-summary`	（任意）自動ネットワーク サマライズをイネーブルにします。IGP から BGP にサブネットが再配信された場合、ネットワーク ルートだけが BGP テーブルに挿入されます。
ステップ 9	**bgp graceful-restart** 例： `スイッチ(config)# bgp graceful-start`	（任意）NSF 認識をスイッチでイネーブルにします。NSF 認識はデフォルトではディセーブルです。
ステップ 10	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**show ip bgp network***network-number* 例： `スイッチ# show ip bgp network 10.108.0.0`	設定を確認します。
ステップ 12	**show ip bgp neighbor** 例： `スイッチ# show ip bgp neighbor`	NSF 認識（グレースフル リスタート）がネイバーでイネーブルにされていることを確認します。 スイッチおよびネイバーで NSF 認識がイネーブルである場合は、次のメッセージが表示されます。 グレースフル リスタート機能*:* アドバタイズおよび受信される スイッチで NSF 認識がイネーブルであり、ネイバーでディセーブルである場合は、次のメッセージが表示されます。 グレースフル リスタート機能*:* アドバタイズされる
ステップ 13	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング ポリシー変更の管理

BGP ピアがルート リフレッシュ機能をサポートするかどうかを学習して、BGP セッションをリセットするには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ip bgp neighbors** 例： `スイッチ# show ip bgp neighbors`	ネイバーがルートリフレッシュ機能をサポートするかどうかを表示します。サポートされている場合は、ルータに関する次のメッセージが表示されます。 *Received route refresh capability from peer*
ステップ 2	**clear ip bgp** {***** | *address* | *peer-group-name*}	指定された接続上でルーティング テーブルをリセットします。 • すべての接続をリセットする場合は、アスタリスク（*）を入力します。

	コマンドまたはアクション	目的
	例： スイッチ# clear ip bgp *	• 特定の接続をリセットする場合は、IPアドレスを入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 3	**clear ip bgp** {* | *address* | *peer-group-name*} **soft out** 例： スイッチ# clear ip bgp * soft out	（任意）指定された接続上でインバウンドルーティングテーブルをリセットするには、アウトバウンドソフトリセットを実行します。このコマンドは、ルートリフレッシュがサポートされている場合に使用してください。 • すべての接続をリセットする場合は、アスタリスク（*）を入力します。 • 特定の接続をリセットする場合は、IPアドレスを入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 4	**show ip bgp** 例： スイッチ# show ip bgp	ルーティング テーブルおよびBGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 5	**show ip bgp neighbors** 例： スイッチ# show ip bgp neighbors	ルーティング テーブルおよびBGP ネイバーに関する情報をチェックし、リセットされたことを確認します。

BGP 判断属性の設定

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**router bgp***autonomous-system* 例： `スイッチ(config)# router bgp 4500`	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp best-path as-path ignore** 例： `スイッチ(config-router)# bgp bestpath as-path ignore`	（任意）ルート選択中に AS パス長を無視するようにルータを設定します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self** 例： `スイッチ(config-router)# neighbor 10.108.1.1 next-hop-self`	（任意）ネクストホップアドレスの代わりに使用される特定の IP アドレスを入力し、ネイバーへの BGP アップデートに関するネクストホップの処理をディセーブルにします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **weight***weight* 例： `スイッチ(config-router)# neighbor 172.16.12.1 weight 50`	（任意）ネイバー接続に重みを割り当てます。指定できる値は 0 ～ 65535 です。最大の重みのルートを推奨します。別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ローカルルータから送信されたルートのデフォルトの重みは 32768 です。
ステップ 6	**default-metric***number* 例： `スイッチ(config-router)# default-metric 300`	（任意）推奨パスを外部ネイバーに設定するように MED メトリックを設定します。MED を持たないすべてのルータも、この値に設定されます。指定できる範囲は 1 ～ 4294967295 です。最小値を推奨します。
ステップ 7	**bgp bestpath med missing-as-worst** 例： `スイッチ(config-router)# bgp bestpath med missing-as-worst`	（任意）MED がない場合は無限の値が指定されていると見なし、MED 値を持たないパスが最も望ましくないパスになるように、スイッチを設定します。
ステップ 8	**bgp always-compare med** 例： `スイッチ(config-router)# bgp always-compare-med`	（任意）異なる AS 内のネイバーからのパスに対して、MED を比較するようにスイッチを設定します。デフォルトでは、MED は同じ AS 内のパス間でだけ比較されます。

	コマンドまたはアクション	目的
ステップ 9	**bgp bestpath med confed** 例： `スイッチ(config-router)# bgp bestpath med confed`	（任意）連合内の異なるサブ AS によってアドバタイズされたパスから特定のパスを選択する場合に、MED を考慮するようにスイッチを設定します。
ステップ 10	**bgp deterministic med** 例： `スイッチ(config-router)# bgp deterministic med`	（任意）同じ AS 内の異なるピアによってアドバタイズされたルートから選択する場合に、MED 変数を考慮するようにスイッチを設定します。
ステップ 11	**bgp default local-preference***value* 例： `スイッチ(config-router)# bgp default local-preference 200`	（任意）デフォルトのローカルプリファレンス値を変更します。指定できる範囲は 0 ～ 4294967295 で、デフォルト値は 100 です。最大のローカル プリファレンス値を推奨します。
ステップ 12	**maximum-paths***number* 例： `スイッチ(config-router)# maximum-paths 8`	（任意）IP ルーティング テーブルに追加するパスの数を設定します。デフォルトでは、最適パスだけがルーティング テーブルに追加されます。指定できる範囲は 1 ～ 16 です。複数の値を指定すると、パス間のロードバランシングが可能になります。スイッチ ソフトウェア では最大 32 の等コスト ルートが許可されていますが、スイッチ ハードウェアはルートあたり 17 パス以上は使用しません。
ステップ 13	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show ip bgp** 例： `スイッチ# show ip bgp`	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 15	**show ip bgp neighbors** 例： `スイッチ# show ip bgp neighbors`	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。

	コマンドまたはアクション	目的
ステップ 16	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルート マップによる BGP フィルタリングの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] 例： スイッチ(config)# route-map set-peer-address permit 10	ルート マップを作成し、ルート マップ コンフィギュレーション モードを開始します。
ステップ 3	**set ip next-hop***ip-address* [*...ip-address*] [**peer-address**] 例： スイッチ(config)# set ip next-hop 10.1.1.3	（任意）ネクストホップ処理をディセーブルにするようにルート マップを設定します。 • インバウンド ルート マップの場合は、一致するルートのネクスト ホップをネイバー ピア アドレスに設定し、サードパーティのネクスト ホップを上書きします。 • BGP ピアのアウトバウンド ルート マップの場合は、ネクスト ホップをローカル ルータのピア アドレスに設定して、ネクストホップ計算をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show route-map** [*map-name*] 例： スイッチ# show route-map	設定を確認するため、設定されたすべてのルートマップ、または指定されたルート マップだけを表示します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ネイバーによる BGP フィルタリングの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： スイッチ(config)# router bgp 109	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** {*ip-address* | *peer-group name*} **distribute-list** {**access-list-number** | *name*} {**in** | **out**} 例： スイッチ(config-router)# neighbor 172.16.4.1 distribute-list 39 in	（任意）アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。

	コマンドまたはアクション	目的
		（注） **neighbor prefix-list** ルータ コンフィギュレーション コマンドを使用して、アップデートをフィルタリングすることもできますが、両方のコマンドを使用して同じ BGP ピアを設定することはできません。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **route-map***map-tag*{**in** | **out**} 例： `スイッチ(config-router)# neighbor 172.16.70.24 route-map internal-map in`	（任意）ルートマップを適用し、着信または発信ルートをフィルタリングします。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors** 例： `スイッチ# show ip bgp neighbors`	設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス リストおよびネイバーによる BGP フィルタリングの設定

BGP 自律システム パスに基づいて着信および発信の両方のアップデートにアクセス リスト フィルタを指定して、フィルタリングすることもできます。各フィルタは、正規表現を使用するアクセス リストです。（正規表現の作成方法については、『*Cisco IOS Dial Technologies Command Reference, Release 12.4*』の付録「Regular Expressions」を参照してください。）この方法を使用するには、自律システムパスのアクセスリストを定義し、特定のネイバーとの間のアップデートに適用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip as-path access-list***access-list-number* {**permit** | **deny**} *as-regular-expressions* 例： スイッチ(config)# ip as-path access-list 1 deny _65535_	BGP-related アクセス リストを定義します。
ステップ 3	**router bgp***autonomous-system* 例： スイッチ(config)# router bgp 110	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **filter-list** {*access-list-number* | *name*} {**in** | **out** | **weight***weight*} 例： スイッチ(config-router)# neighbor 172.16.1.1 filter-list 1 out	アクセス リストに基づいて、BGP フィルタを確立します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors** [**paths***regular-expression*] 例： スイッチ# show ip bgp neighbors	設定を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP フィルタリング用のプレフィックス リストの設定

コンフィギュレーション エントリを削除する場合は、シーケンス番号を指定する必要はありません。**show** コマンドの出力には、シーケンス番号が含まれます。

コマンド内でプレフィックスリストを使用する場合は、あらかじめプレフィックスリストを設定しておく必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip prefix-list***list-name* [**seq***seq-value*] **deny** | **permit***network/len* [**ge***ge-value*] [**le***le-value*] 例： スイッチ(config)# ip prefix-list BLUE permit 172.16.1.0/24	一致条件に合わせてアクセスを拒否（**deny**）または許可（**permit**）するプレフィックスリストを作成します。シーケンス 番号を指定することもできます。少なくとも 1 つの **permit** コマンドまたは **deny** コマンドを入力する必要があります。 • *network/len* は、ネットワーク番号およびネットワーク マスクの長さ（ビット単位）です。 •（任意）**ge** および **le** の値は、照合するプレフィックス長の範囲を指定します。指定された *ge-value* および *le-value* は、次の条件を満たす必要があります。*len* < *ge-value* < *le-value*< 32
ステップ 3	**ip prefix-list***list-name***seq***seq-value***deny** | **permit***network/len* [**ge***ge-value*] [**le***le-value*] 例： スイッチ(config)# ip prefix-list BLUE seq 10 permit 172.24.1.0/24	（任意）プレフィックス リストにエントリを追加し、そのエントリにシーケンス番号を割り当てます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip prefix list** [**detail** | **summary**] *name* [*network/len*] [**seq***seq-num*] [**longer**] [**first-match**]	プレフィックスリストまたはプレフィックスリストエントリに関する情報を表示して、設定を確認します。

	コマンドまたはアクション	目的
	例： スイッチ# show ip prefix list summary test	
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP コミュニティ フィルタリングの設定

デフォルトでは、COMMUNITIES 属性はネイバーに送信されません。COMMUNITIES 属性が特定の IP アドレスのネイバーに送信されるように指定するには、**neighbor send-community** ルータ コンフィギュレーション コマンドを使用します。

手順の概要

1. **configureterminal**
2. **ip community-list***community-list-number* {**permit** | **deny**} *community-number*
3. **router bgp***autonomous-system*
4. **neighbor** {*ip-address* | *peer-group name*} **send-community**
5. **set comm-list***list-num***delete**
6. **exit**
7. **ip bgp-community new-format**
8. **end**
9. **show ip bgp community**
10. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ip community-list***community-list-number* {**permit** | **deny**} *community-number* 例： `スイッチ(config)# ip community-list 1 permit 50000:10`	コミュニティ リストを作成し、番号を割り当てます。 • *community-list-number* は 1 ～ 99 の整数です。この値は、コミュニティの1つ以上の許可または拒否グループを識別します。 • *community-number* は、**set community** ルートマップ コンフィギュレーション コマンドで設定される番号です。
ステップ 3	**router bgp***autonomous-system* 例： `スイッチ(config)# router bgp 108`	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **send-community** 例： `スイッチ(config-router)# neighbor 172.16.70.23 send-community`	この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 5	**set comm-list***list-num***delete** 例： `スイッチ(config-router)# set comm-list 500 delete`	（任意）ルートマップで指定された標準または拡張コミュニティ リストと一致する着信または発信アップデートのコミュニティ属性から、コミュニティを削除します。
ステップ 6	**exit** 例： `スイッチ(config-router)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip bgp-community new-format** 例： `スイッチ(config)# ip bgp-community new format`	（任意）AA:NN の形式で、BGP コミュニティを表示、解析します。 BGP コミュニティは、2 つの部分からなる 2 バイト長形式で表示されます。シスコのデフォルトのコミュニティ形式は、NNAA です。BGP に関する最新の RFC では、コミュニティは AA:NN の形式をとります。最初の部分は AS 番号で、その次の部分は 2 バイトの数値です。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp community** 例： スイッチ# show ip bgp community	設定を確認します。
ステップ 10	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP ネイバーおよびピア グループの設定

各ネイバーに設定オプションを割り当てるには、ネイバーの IP アドレスを使用し、次に示すルータ コンフィギュレーション コマンドのいずれかを指定します。ピア グループにオプションを割り当てるには、ピア グループ名を使用し、いずれかのコマンドを指定します。**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用すると、すべての設定情報を削除せずに、BGP ピアまたはピア グループをディセーブルにできます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor***peer-group-name***peer-group**	BGP ピア グループを作成します。
ステップ 4	**neighbor***ip-address***peer-group***peer-group-name*	BGP ネイバーをピア グループのメンバにします。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***number*	BGP ネイバーを指定します。**remote-as***number* を使用してピア グループが設定されていない場合は、このコマンドを使用し、EBGP ネイバーを含むピア グループを作成します。指定できる範囲は 1 ～ 65535 です。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **description***text*	（任意）ネイバーに説明を関連付けます。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map***map-name*]	（任意）BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **update-source***interface*	（任意）内部 BGP セッションに、TCP 接続に関するすべての操作インターフェイスの使用を許可します。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop**	（任意）ネイバーがセグメントに直接接続されていない場合でも、BGP セッションを使用可能にします。マルチホップ ピア アドレスへの唯一のルートがデフォルト ルート（0.0.0.0）の場合、マルチホップ セッションは確立されません。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **local-as***number*	（任意）ローカル AS として使用する AS 番号を指定します。指定できる範囲は 1 ～ 65535 です。
ステップ 12	**neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval***seconds*	（任意）BGP ルーティング アップデートを送信する最小インターバルを設定します。
ステップ 13	**neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix***maximum* [*threshold*]	（任意）ネイバーから受信できるプレフィックス数を制御します。指定できる範囲は 1 ～ 4294967295 です。*threshold*（任意）は、警告メッセージが生成される基準となる最大値（パーセンテージ）です。デフォルトは 75% です。
ステップ 14	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	（任意）ネイバー宛ての BGP アップデートに関して、ネクストホップでの処理をディセーブルにします。
ステップ 15	neighbor {*ip-address* | *peer-group-name*} password *string*	（任意）TCP 接続での MD5 認証を BGP ピアに設定します。両方の BGP ピアに同じパスワードを設定する必要があります。そうしないと、BGP ピア間に接続が作成されません。

	コマンドまたはアクション	目的
ステップ 16	**neighbor** {*ip-address* | *peer-group-name*} **route-map***map-name* {**in** | **out**}	（任意）着信または発信ルートにルートマップを適用します。
ステップ 17	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 18	**neighbor** {*ip-address* | *peer-group-name*} **timers***keepalive holdtime*	（任意）ネイバーまたはピア グループ用のタイマーを設定します。 • *keepalive* インターバルは、キープアライブ メッセージがピアに送信される間隔です。指定できる範囲は 1 ～ 4294967295 秒です。デフォルト値は 60 秒です。 • *holdtime* は、キープアライブ メッセージを受信しなかった場合、ピアが非アクティブと宣言されるまでのインターバルです。指定できる範囲は 1 ～ 4294967295 秒です。デフォルト値は 180 秒です。
ステップ 19	**neighbor** {*ip-address* | *peer-group-name*} **weight***weight*	（任意）ネイバーからのすべてのルートに関する重みを指定します。
ステップ 20	**neighbor** {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *name*} {**in** | **out**}	（任意）アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。
ステップ 21	**neighbor** {*ip-address* | *peer-group-name*} **filter-list***access-list-number* {**in** | **out** | **weight***weight*}	（任意）BGP フィルタを確立します。
ステップ 22	**neighbor** {*ip-address* | *peer-group-name*} **version***value*	（任意）ネイバーと通信するときに使用する BGP バージョンを指定します。
ステップ 23	**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**	（任意）受信したアップデートのストアを開始するようにソフトウェアを設定します。
ステップ 24	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 25	**show ip bgp neighbors**	設定を確認します。

	コマンドまたはアクション	目的
ステップ 26	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング テーブルでの集約アドレスの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： スイッチ(config)# router bgp 106	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**aggregate-address***address mask* 例： スイッチ(config-router)# aggregate-address 10.0.0.0 255.0.0.0	BGP ルーティング テーブル内に集約エントリを作成します。集約ルートは AS からのルートとしてアドバタイズされます。情報が失われた可能性があることを示すため、アトミック集約属性が設定されます。
ステップ 4	**aggregate-address***address mask***as-set** 例： スイッチ(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set	（任意）AS設定パス情報を生成します。このコマンドは、この前のコマンドと同じルールに従う集約エントリを作成します。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET です。多くのパスを集約するときは、このキーワードを使用しないでください。このルートは絶えず取り消され、アップデートされます。

	コマンドまたはアクション	目的
ステップ 5	**aggregate-address***address-mask***summary-only** 例： スイッチ(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only	（任意）サマリーアドレスだけをアドバタイズします。
ステップ 6	**aggregate-address***address mask***suppress-map***map-name* 例： スイッチ(config-router)# aggregate-address 10.0.0.0 255.0.0.0 suppress-map map1	（任意）選択された、より具体的なルートを抑制します。
ステップ 7	**aggregate-address***address mask***advertise-map***map-name* 例： スイッチ(config-router)# aggregate-address 10.0.0.0 255.0.0.0 advertise-map map2	（任意）ルートマップによって指定された設定に基づいて集約を生成します。
ステップ 8	**aggregate-address***address mask***attribute-map***map-name* 例： スイッチ(config-router)# aggregate-address 10.0.0.0 255.0.0.0 attribute-map map3	（任意）ルートマップで指定された属性を持つ集約を生成します。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 10	**show ip bgp neighbors** [**advertised-routes**] 例： スイッチ# show ip bgp neighbors	設定を確認します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

ルーティング ドメイン連合の設定

自律システムのグループの自律システム番号として機能する連合 ID を指定する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： スイッチ(config)# router bgp 100	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp confederation identifier***autonomous-system* 例： スイッチ(config)# bgp confederation identifier 50007	BGP 連合 ID を設定します。
ステップ 4	**bgp confederation peers***autonomous-system* [*autonomous-system...*] 例： スイッチ(config)# bgp confederation peers 51000 51001 51002	連合に属する AS、および特殊な EBGP ピアとして処理する AS を指定します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbor** 例： スイッチ# show ip bgp neighbor	設定を確認します。
ステップ 7	**show ip bgp network** 例： スイッチ# show ip bgp network	設定を確認します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP ルート リフレクタの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： スイッチ(config)# router bgp 101	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** {*ip-address* | *peer-group-name*} **route-reflector-client** 例： スイッチ(config-router)# neighbor 172.16.70.24 route-reflector-client	ローカル ルータを BGP ルート リフレクタとして、指定されたネイバーをクライアントとして、それぞれ設定します。
ステップ 4	**bgp cluster-id***cluster-id* 例： スイッチ(config-router)# bgp cluster-id 10.0.1.2	（任意）クラスタに複数のルート リフレクタが存在する場合、クラスタ ID を設定します。
ステップ 5	**no bgp client-to-client reflection** 例： スイッチ(config-router)# no bgp client-to-client reflection	（任意）クライアント間のルート反映をディセーブルにします。デフォルトでは、ルート リフレクタ クライアントからのルートは、他のクライアントに反映されます。ただし、クライアントが完全メッシュ構造の場合、ルート リフレクタはルートをクライアントに反映させる必要がありません。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp** 例： スイッチ# show ip bgp	設定を確認します。送信元 ID およびクラスタリスト属性を表示します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルート ダンプニングの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： スイッチ(config)# router bgp 100	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp dampening** 例： スイッチ(config-router)# bgp dampening	BGP ルート ダンプニングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**bgp dampening***half-life reuse suppress max-suppress* [**route-map***map*] 例： `スイッチ(config-router)# bgp dampening 30 1500 10000 120`	（任意）ルート ダンプニング係数のデフォルト値を変更します。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp flap-statistics** [{**regexp***regexp*} | {**filter-list***list*} | {*address mask* [**longer-prefix**]}] 例： `スイッチ# show ip bgp flap-statistics`	（任意）フラッピングしているすべてのパスのフラップを監視します。ルートの抑制が終了し、安定状態になると、統計情報が削除されます。
ステップ 7	**show ip bgp dampened-paths** 例： `スイッチ# show pi bgp dampened-paths`	（任意）抑制されるまでの時間を含めて、ダンプニングされたルートを表示します。
ステップ 8	**clear ip bgp flap-statistics** [{**regexp***regexp*} | {**filter-list***list*} | {*address mask* [**longer-prefix**]} 例： `スイッチ# clear ip bgp flap-statistics`	（任意）BGP フラップ統計情報を消去して、ルートがダンプニングされる可能性を小さくします。
ステップ 9	**clear ip bgp dampening** 例： `スイッチ# clear ip bgp dampening`	（任意）ルート ダンプニング情報を消去して、ルートの抑制を解除します。
ステップ 10	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP のモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。この作業は、特定の構造の内容が無効になる場合、または無効である疑いがある場合に必要となります。

BGPルーティングテーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。さらに、リソースの利用率を取得したり、ネットワーク問題を解決するための情報を使用することもできます。さらに、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のルーティング パスを検出することもできます。

下の図に、BGP を消去および表示するために使用する特権 EXEC コマンドを示します。表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

表 *83*： *IP BGP* の *clear* および *show* コマンド

clear ip bgp*address*	特定の BGP 接続をリセットします。
clear ip bgp *	すべての BGP 接続をリセットします。
clear ip bgp peer-group*tag*	BGP ピア グループのすべてのメンバを削除します。
show ip bgp*prefix*	プレフィックスがアドバタイズされるピア グループ、またはピア グループに含まれないピアを表示します。ネクスト ホップやローカル プレフィックスなどのプレフィックス属性も表示されます。
show ip bgp cidr-only	サブネットおよびスーパーネット ネットワーク マスクを含むすべての BGP ルートを表示します。
show ip bgp community [*community-number*] [**exact**]	指定されたコミュニティに属するルートを表示します。
show ip bgp community-list*community-list-number* [**exact-match**]	コミュニティ リストで許可されたルートを表示します。
show ip bgp filter-list*access-list-number*	指定された AS パス アクセス リストによって照合されたルートを表示します。
show ip bgp inconsistent-as	送信元の AS と矛盾するルートを表示します。
show ip bgp regexp*regular-expression*	コマンドラインに入力された特定の正規表現と一致する AS パスを持つルートを表示します。
show ip bgp	BGP ルーティング テーブルの内容を表示します。

show ip bgp neighbors [*address*]	各ネイバーとの BGP 接続および TCP 接続に関する詳細情報を表示します。
show ip bgp neighbors [*address*] [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths***regular-expression* | **received-routes** | **routes**]	特定の BGP ネイバーから取得されたルートを表示します。
show ip bgp paths	データベース内のすべての BGP パスを表示します。
show ip bgp peer-group [*tag*] [**summary**]	BGP ピア グループに関する情報を表示します。
show ip bgp summary	BGP 接続すべての状況を表示します。

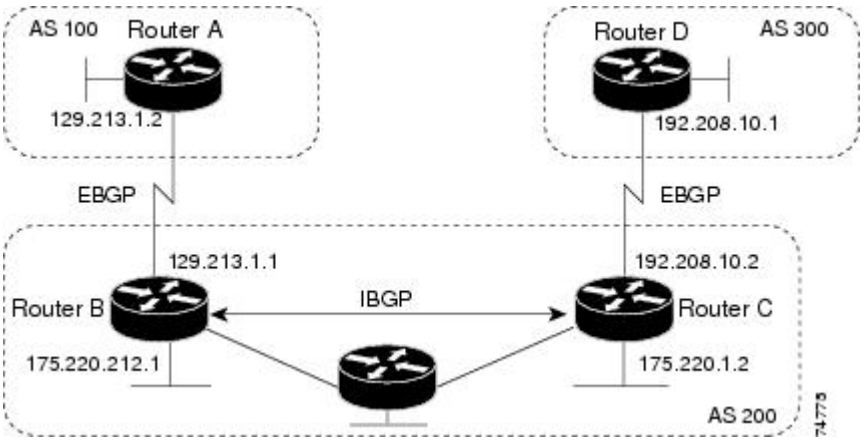
bgp log-neighbor changes コマンドは、デフォルトでイネーブルです。そのため、BGP ネイバーのリセット、起動、またはダウン時に生成されるメッセージをログに記録できます。

BGP の設定例

例：ルータでの BGP の設定

次に、下の図のルータでの BGP の設定例を示します。

図 *61*：*EBGP*、*IBGP*、および複数の自律システム



ルータ A：

```
スイッチ(config)# router bgp 100
スイッチ(config-router)# neighbor 129.213.1.1 remote-as 200
```

ルータ B：

```
スイッチ(config)# router bgp 200
スイッチ(config-router)# neighbor 129.213.1.2 remote-as 100
スイッチ(config-router)# neighbor 175.220.1.2 remote-as 200
```

ルータ C：

```
スイッチ(config)# router bgp 200
スイッチ(config-router)# neighbor 175.220.212.1 remote-as 200
スイッチ(config-router)# neighbor 192.208.10.1 remote-as 300
```

ルータ D：

```
スイッチ(config)# router bgp 300
スイッチ(config-router)# neighbor 192.208.10.2 remote-as 200
```

BGP ピアが稼働していることを確認するには、show ip bgp neighbors 特権 EXEC コマンドを使用します。次に、ルータ A にこのコマンドを実行した場合の出力例を示します。

```
スイッチ# show ip bgp neighbors

BGP neighbor is 129.213.1.1, remote AS 200, external link
 BGP version 4, remote router ID 175.220.212.1
 BGP state = established, table version = 3, up for 0:10:59
 Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
 Minimum time between advertisement runs is 30 seconds
 Received 2828 messages, 0 notifications, 0 in queue
 Sent 2826 messages, 0 notifications, 0 in queue
 Connections established 11; dropped 10
```

state = *established* 以外の情報が出力された場合、ピアは稼働していません。リモート ルータ ID は、ルータ（または最大のループバック インターフェイス）上の最大の IP アドレスです。テーブルが新規情報でアップデートされるたびに、テーブルのバージョン番号は増加します。継続的にテーブル バージョン番号が増加している場合は、ルートがフラッピングし、ルーティング アップデートが絶えず発生しています。

外部プロトコルの場合、**network** ルータ コンフィギュレーション コマンドから IP ネットワークへの参照によって制御されるのは、アドバタイズされるネットワークだけです。これは、**network** コマンドを使用してアップデートの送信先を指定する IGP（EIGRP など）と対照的です。

BGP 設定の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Routing Protocols」を参照してください。特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

ISO CLNS ルーティングに関する情報

コネクションレス型ルーティング

国際標準化機構（ISO）コネクションレス型ネットワーク サービス（CLNS）プロトコルとは、オープン システム インターコネクション（OSI）モデルのネットワーク層の標準の 1 つです。ISO ネットワーク アーキテクチャ内のアドレスは、ネットワーク サービス アクセス ポイント（NSAP）アドレスおよび Network Entity Titles（NETs）と呼ばれます。OSI ネットワークの各ノードには、1 つ以上の NETs が含まれます。さらに、各ノードには、多数の NSAP アドレスが含まれます。

スイッチ上で、**clns routing** グローバル コンフィギュレーション コマンドを使用してコネクションレス型ルーティングをイネーブルにすると、スイッチはルーティング関連の機能を果たさず、転送の決定だけを行います。ダイナミック ルーティングには、ルーティング プロトコルもイネーブルにする必要があります。スイッチは、Intermediate System-to-Intermediate System（IS-IS）ダイナミック ルーティング プロトコルをサポートします。このプロトコルは、ISO CLNS ネットワーク用の OSI ルーティング プロトコルに基づいています。

動的にルーティングを行う場合は、IS-IS を使用します。このルーティング プロトコルは、エリアの概念をサポートします。1 つのエリア内部では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。エリア間では、ルータは適切なエリアに到達する方法を認識しています。IS-IS は、ステーション ルーティング（1 つのエリア内）およびエリア ルーティング（エリア間）という 2 つのレベルのルーティングをサポートします。

ISO IGRP と IS-IS NSAP アドレス方式の主な違いは、エリア アドレスの定義にあります。両方ともレベル 1 ルーティング（1 つのエリア内）にはシステム ID を使用します。ただし、エリア ルーティングに関してアドレスが指定される方法が異なります。ISO IGRP NSAP アドレスには、ドメイン、エリア、およびシステム ID という 3 つの異なるフィールドが含まれます。IS-IS アドレスには、単一の連続的エリア フィールド（ドメイン フィールドおよびエリア フィールドから成る）とシステム ID という 2 つのフィールドが含まれます。

（注） ISO CLNS の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Configuration Guide, Release 12.4*』を参照してください。この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.4*』を参照するか、IOS コマンド リファレンス マスター インデックスを使用するか、オンライン検索を行ってください。

IS-IS ダイナミック ルーティング

IS-IS は、ISO ダイナミック ルーティング プロトコルの 1 つです（ISO 105890 で説明されている）。その他のルーティング プロトコルとは異なり、IS-IS をイネーブルするには、IS-IS ルーティング プロセスを作成し、それをネットワークではなく特定のインターフェイスに割り当てる必要があります。マルチエリア IS-IS コンフィギュレーション構文を使用することで、レイヤ 3 スイッチまたはルータごとに複数の IS-IS ルーティング プロトコルを指定できます。その後、IS-IS ルーティング プロセスのインスタンスごとにパラメータを設定します。

小規模の IS-IS ネットワークは、ネットワーク内にすべてのルータが含まれる単一のエリアとして構築されます。ネットワークの規模が大きくなるに従って、このネットワークは、すべてのエリアに属する、接続されたすべてのレベル 2 ルータのセットから構成されるバックボーン エリア内に再編成され、その後、このネットワークはローカルエリアに接続されます。ローカルエリア内部では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。エリア間では、ルータはバックボーンへの到達方法を認識しており、バックボーン ルータは他のエリアに到達する方法を認識しています。

ルータは、ローカル エリア内でルーティングを実行するために、レベル 1 の隣接関係を確立します（ステーション ルーティング）。ルータは、レベル 1 のエリア間でルーティングを実行するために、レベル 2 の隣接関係を確立します（エリア ルーティング）。

1 つの Cisco ルータは、最大 29 エリアのルーティングに参加でき、バックボーンでレベル 2 ルーティングを実行できます。一般に、ルーティング プロセスごとに 1 つのエリアに対応します。デフォルトでは、ルーティング プロセスの最初のインスタンスが、レベル 1 および レベル 2 両方のルーティングを実行するように設定されます。追加のルーティング インスタンスを設定できます。このインスタンスは、自動的にレベル 1 エリアとして扱われます。IS-IS ルーティング プロセスの各インスタンスごとに個別にパラメータを設定する必要があります。

IS-IS マルチエリア ルーティングでは、シスコの各装置に対して最大 29 個の レベル 1 エリアを定義できますが、レベル 2 ルーティングを実行するプロセスは 1 つだけ設定できます。レベル 2 ルーティングが任意のプロセス上に設定されている場合、追加のプロセスは、すべて自動的にレベル 1 に設定されます。同時に、このプロセスがレベル 1 ルーティングを実行するように設定することもできます。ルータ インスタンスにレベル 2 ルーティングが必要でない場合は、**is-type** グローバル コンフィギュレーション コマンドを使用してレベル 2 の機能を削除します。別のルータ インスタンスをレベル 2 ルータとして設定する場合にも **is-type** コマンドを使用します。

（注） IS-IS の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Routing Protocols」を参照してください。ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS IP Command Reference, Release 12.4*』を参照してください。

NSF 認識

統合型 IS-IS NSF 認識機能は IPv4G でサポートされています。この機能により、NSF を認識する顧客宅内装置（CPE）ルータが、NFS 対応ルータによるパケットのノンストップ転送を実現します。ローカルルータでは、必ずしも NSF を実行している必要はありませんが、このルータが NSF を認識していると、スイッチオーバープロセス時にルーティングデータベースの整合性と精度、および隣接 NSF 対応ルータ上のリンクステート データベースが保持されます。

この機能は、自動的にイネーブルにされ、設定は必要ありません。この機能の詳細については、『*Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

IS-IS グローバル パラメータ

設定可能ないくつかのオプションの IS-IS グローバル パラメータを次に示します。

- ルート マップによって制御されるデフォルト ルートを設定することで、デフォルト ルートを IS-IS ルーティング ドメイン内に強制的に設定できます。ルート マップで設定可能な、その他のフィルタリング オプションも指定できます。
- 内部チェックサム エラーとともに受信された IS-IS LSP を無視したり、破損した LSP を消去するようにルータを設定できます。これにより、LSP の発信側は、LSP を再生成します。
- エリアおよびドメインにパスワードを割り当てられます。

- サマリー アドレスを使用して、ルーティング テーブル内に表示される集約アドレスを作成できます（経路集約）。他のルーティング プロトコルから学習したルートも集約できます。サマリーをアドバタイズするのに使用されるメトリックは、すべての個別ルートにおける最小のメトリックです。
- 過負荷ビットを設定できます。
- LSP リフレッシュ インターバルおよび LSP がリフレッシュなしでルータ データベース内にとどまることができる最大時間を設定できます。
- LSP 生成に対するスロットリング タイマー、最短パス優先計算、および部分ルート計算を設定できます。
- IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、スイッチがログ メッセージを生成するように設定できます。
- ネットワーク内のリンクが、1500 バイト未満の最大伝送単位（MTU）サイズの場合、それでもルーティングが行われるように LSP MTU の値を低くできます。
- パーティション回避ルータ コンフィギュレーション コマンドは、レベル 1-2 境界ルータ、隣接レベル 1 ルータ、およびエンド ホスト間で完全な接続が失われた場合に、エリアがパーティション化されるのを防ぎます。

IS-IS インターフェイス パラメータ

任意で、特定のインターフェイス固有の IS-IS パラメータを、付加されている他のルータとは別に設定できます。ただし、一部の値（乗数およびタイム インターバルなど）をデフォルトから変更する場合、複数のルータおよびインターフェイス上でもこれを変更する必要があります。ほとんどのインターフェイス パラメータは、レベル 1、レベル 2、またはその両方で設定できます。

次に、設定可能なインターフェイス レベル パラメータの一部を示します。

- インターフェイスのデフォルト メトリック：Quality of Service（QoS）ルーティングが実行されない場合に、IS-IS メトリックの値として使用され、割り当てられます。
- hello インターバル（インターフェイスから送信される hello パケットの間隔）またはデフォルトの hello パケット乗数：インターフェイス上で使用されて、IS-IS hello パケットで送信されるホールド タイムを決定します。ホールド タイムは、ネイバーがダウンしていると宣言するまでに、別の hello パケットを待機する時間を決定します。これにより、障害リンクまたはネイバーが検出される速さも決定し、ルートを再計算できるようになります。hello パケットが頻繁に失われ、IS-IS 隣接に無用な障害が発生する場合は、hello 乗数を変更してください。hello 乗数を大きくし、それに対応して hello インターバルを小さくすると、リンク障害を検出するのに必要な時間を増やすことなく、hello プロトコルの信頼性を高めることができます。
- その他のタイム インターバル：
  - Complete Sequence Number PDU（CSNP）インターバルCSNP は、指定ルータにより送信され、データベースの同期を維持します。

- 再送信インターバルこれは、ポイントツーポイント リンクの IS-IS LSP の再送信間隔です。
- IS-IS LSP 再送信スロットル インターバルこれは、IS-IS LSP がポイントツーポイント リンクで再送信される最大レート（パケット間のミリ秒数）です。このインターバルは、同じ LSP が連続する再送信間隔である再送信インターバルとは異なります。

- 指定ルータの選択プライオリティ：マルチアクセス ネットワークで必要な隣接数を削減し、その代わりに、ルーティング プロトコル トラフィックの量およびトポロジ データベースのサイズを削減できます。
- インターフェイス回線タイプ：指定されたインターフェイス上のネイバーに必要な隣接タイプです。
- インターフェイスのパスワード認証

ISO CLNS ルーティングの設定方法

IS-IS のデフォルト設定

表 *84*：*IS-IS* のデフォルト設定

機能	デフォルト設定
リンクステート PDU（LSP）エラーを無視	イネーブル
IS-IS タイプ	従来型の IS-IS：ルータは、レベル 1（ステーション）とレベル 2（エリア） 両方のルータとして機能します。 マルチエリア IS-IS：IS-IS ルーティング プロセスの最初のインスタンスが レベル 1-2 ルータです。残りのインスタンスは、レベル 1 ルータです。
デフォルト情報送信元	ディセーブル
IS-IS 隣接関係のステート変更を記録	ディセーブル
LSP 生成スロットリング タイマー	連続で生成した 2 つの間の最大インターバル：5 秒 初期 LSP 生成遅延：50 ミリ秒 1 番目と 2 番目の LSP 生成間のホールド タイム：5000 ミリ秒

機能	デフォルト設定
LSP 最大ライフ タイム（リフレッシュなし）	LSP パケットが削除されるまで 1200 秒（20 分）
LSP リフレッシュ インターバル	LSP リフレッシュを 900 秒（15 分）ごとに送信
最大 LSP パケット サイズ	1497 バイト
NSF 認識	イネーブルレイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
部分ルート計算（PRC）スロットリング タイマー	最大 PRC 待機インターバル：5 秒 トポロジの変更後の初期 PRC 計算遅延：2000 ミリ秒 1 番目と 2 番目の PRC 計算間のホールド タイム：5000 ミリ秒
パーティション回避	ディセーブル
パスワード	エリアまたはドメインのパスワードが定義されておらず、認証はディセーブルになっています。
過負荷ビットの設定	ディセーブルイネーブルの際に引数が入力されない場合、過負荷ビットがただちに設定され、**no set-overload-bit** コマンドが入力されるまで設定されたままになります。
Shortest Path First（SPF）スロットリング タイマー	連続した SFP 間の最大インターバル：10 秒 トポロジの変更後の初期 SFP 計算：5500 ミリ秒 1 番目と 2 番目の SFP 計算間のホールド タイム：5500 ミリ秒
サマリー アドレス	ディセーブル

IS-IS ルーティングのイネーブル化

IS-IS をイネーブルにするには、各ルーティング プロセスに名前と NET を指定します。その後、インターフェイス上で IS-IS ルーティングをイネーブルにし、ルーティング プロセスの各インスタンスに対してエリアを指定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clns routing** 例： スイッチ(config)# clns routing	スイッチ上で ISO コネクションレス型ルーティングをイネーブルに設定します。
ステップ 3	**router isis** [*area tag*] 例： スイッチ(config)# router isis tag1	指定したルーティング プロセスに対して IS-IS ルーティングをイネーブルにし、IS-IS ルーティング コンフィギュレーション モードを開始します。 （任意）*area tag* 引数を使用して、IS-IS ルータが割り当てられているエリアを特定します。複数の IS-IS エリアを設定する場合は、値を入力する必要があります。 最初に設定された IS-IS インスタンスは、デフォルトでレベル 1-2 です。後のインスタンスは、自動的にレベル 1 になります。**is-type** グローバル コンフィギュレーション コマンドを使用してルーティングのレベルを変更できます。
ステップ 4	**net** network-entity-title 例： スイッチ(config-router)# net 47.0004.004d.0001.0001.0c11.1111.00	ルーティング プロセスに NET を設定します。マルチエリア IS-IS を設定する場合、各ルーティング プロセスに NET を指定します。NET およびアドレスの名前を指定できます。
ステップ 5	**is-type** {**level-1** | **level-1-2** | **level-2-only**} 例： スイッチ(config-router)# is-type level-2-only	（任意）レベル 1（ステーション）ルータ、マルチエリア ルーティング用のレベル 2（エリア）ルータ、または両方（デフォルト）として機能するようにルータを設定します。 • **level-1**：ステーション ルータとしてだけ機能します。 • **level-1-2**：ステーション ルータおよびエリア ルータの両方として機能します。 • **level 2**：エリア ルータだけとして機能します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `スイッチ(config-router)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	IS-IS をルーティングするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがまだレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力し、インターフェイスをレイヤ 3 モードにします。
ステップ 8	**ip router isis** [*area tag*] 例： `スイッチ(config-if)# ip router isis tag1`	インターフェイス上の ISO CLNS に対して IS-IS ルーティング プロセスを設定し、ルーティング プロセスにエリア デジグネータを接続します。
ステップ 9	**clns router isis** [*area tag*] 例： `スイッチ(config-if)# clns router isis tag1`	インターフェイス上で ISO CLNS をイネーブルにします。
ステップ 10	**ip address***ip-address-mask* 例： `スイッチ(config-if)# ip address 10.0.0.5 255.255.255.0`	インターフェイスの IP アドレスを定義します。インターフェイスのいずれかで IS-IS ルーティングが設定されている場合は、IS-IS がイネーブルになっているエリアに含まれるすべてのインターフェイスで IP アドレスが必要です。
ステップ 11	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show isis** [*area tag*] **database detail** 例： `スイッチ# show isis database detail`	入力を確認します。
ステップ 13	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IS-IS グローバル パラメータの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clns routing** 例： スイッチ(config)# clns routing	スイッチ上で ISO コネクションレス型ルーティングをイネーブルに設定します。
ステップ 3	**router isis** 例： スイッチ(config)# router isis	IS-IS ルーティング プロトコルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**default-information originate** [**route-map***map-name*] 例： スイッチ(config-router)# default-information originate route-map map1	（任意）デフォルト ルートを IS-IS ルーティング ドメインに強制的に設定します。**route-map***map-name* を入力すると、ルートマップが条件に一致している場合にルーティング プロセスによってデフォルト ルートが生成されます。
ステップ 5	**ignore-lsp-errors** 例： スイッチ(config-router)# ignore-lsp-errors	（任意）LSP を消去する代わりに、内部チェックサムにエラーがある LSP を無視するようにルータを設定します。このコマンドは、デフォルトでイネーブルになっています（破損した LSP はドロップされます）。破損した LSP を消去するには、**no ignore-lsp-errors** ルータ コンフィギュレーション コマンドを入力します。
ステップ 6	**area-password***password* 例： スイッチ(config-router)# area-password 1password	（任意）レベル 1（ステーション ルータ レベル）LSP に挿入されるエリア認証パスワードを設定します。

	コマンドまたはアクション	目的
ステップ 7	**domain-password***password* 例： スイッチ(config-router)# domain-password 2password	（任意）レベル2（エリア ルータ レベル）LSPに挿入されるルーティング ドメイン認証パスワードを設定します。
ステップ 8	**summary-address***address mask* [**level-1** | **level-1-2** | **level-2**] 例： スイッチ(config-router)# summary-address 10.1.0.0 255.255.0.0 level-2	（任意）所定のレベルのアドレスのサマリーを作成します。
ステップ 9	**set-overload-bit** [**on-startup** {*seconds* | **wait-for-bgp**}] 例： スイッチ(config-router)# set-overload-bit on-startup wait-for-bgp	（任意）ルータに問題がある場合に、他のルータが最短パス優先（SPF）計算でこのルータを無視するように過負荷ビット（hippity ビット）を設定します。 • （任意）**on-startup**：起動時だけ過負荷ビットを設定します。**on-startup** が指定されない場合、過負荷ビットが即座に設定され、**no set-overload-bit** コマンドを入力するまで設定されたままになります。**on-startup** が指定された場合、秒数または **wait-for-bgp** を入力する必要があります。 • *seconds*：**on-startup** キーワードが設定されている場合、システム起動時に過負荷ビットが設定されて、この秒数の間設定されたままになります。指定できる範囲は 5 ～ 86400 秒です。 • **wait-for-bgp**：**on-startup** キーワードが設定されている場合、システム起動時に過負荷ビットが設定されて、BGP が収束するまで設定されたままになります。BGP が収束されたことが IS-IS に通知されない場合、IS-IS は 10 分後に過負荷ビットをオフにします。
ステップ 10	**lsp-refresh-interval***seconds* 例： スイッチ(config-router)# lsp-refresh-interval 1080	（任意）LSP リフレッシュ インターバル（秒）を設定します。範囲は 1 ～ 65535 秒です。デフォルトでは、LSP リフレッシュを 900 秒（15 分）ごとに送信します。
ステップ 11	**max-lsp-lifetime***seconds* 例： スイッチ(config-router)# max-lsp-lifetime 1000	（任意）LSPパケットがリフレッシュされずにルータ データベース内に存続する最大時間を設定します。範囲は 1 ～ 65535 秒です。デフォルト値は 1200 秒（20 分）です。指定されたタイム インターバルのあと、LSP パケットは削除されます。

	コマンドまたはアクション	目的
ステップ 12	**lsp-gen-interval**[**level-1** | **level-2**] *lsp-max-wait*[*lsp-initial-wait lsp-second-wait*] 例： `スイッチ(config-router)# lsp-gen-interval level-2 2 50 100`	（任意）IS-IS 生成スロットリング タイマーを設定します。 • *lsp-max-wait*：2 つの連続する LSP 生成間の最大インターバル（秒）。指定できる範囲は 1 ～ 120 秒です。デフォルト値は 5 秒です。 • *lsp-initial-wait*：最初の LSP 生成遅延（ミリ秒）。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。 • *lsp-second-wait*：最初と 2 番目の LSP 生成間（ミリ秒）のホールド タイム。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
ステップ 13	**spf-interval**[**level-1** | **level-2**] *spf-max-wait*[*spf-initial-wait spf-second-wait*] 例： `スイッチ(config-router)# spf-interval level-2 5 10 20`	（任意）IS-IS SPF スロットリング タイマーを設定します。 • *spf-max-wait*：連続する SFP 間（秒）の最大インターバル。指定できる範囲は 1 ～ 120 で、デフォルトは 10 です。 • *spf-initial-wait*：トポロジ変更後の最初の SFP 計算（ミリ秒）。指定できる値の範囲は 1 ～ 10000 です。デフォルトは 5500 です。 • *spf-second-wait*：最初と 2 番目の SFP 計算間（ミリ秒）のホールド タイム。指定できる値の範囲は 1 ～ 10000 です。デフォルトは 5500 です。
ステップ 14	**prc-interval***prc-max-wait*[*prc-initial-wait prc-second-wait*] 例： `スイッチ(config-router)# prc-interval 5 10 20`	（任意）IS-IS PRC スロットリング タイマーを設定します。 • *prc-max-wait*：2 つの連続する PRC 計算間の最大インターバル（秒）。指定できる範囲は 1 ～ 120 秒です。デフォルト値は 5 秒です。 • *prc-initial-wait*：トポロジ変更後の最初の PRC 計算遅延（ミリ秒）。指定できる範囲は 1 ～ 10,000 ミリ秒です。デフォルト値は 2000 ミリ秒です。 • *prc-second-wait*：最初と 2 番目の PRC 計算間（ミリ秒）のホールド タイム。指定できる範囲は 1 ～ 10,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
ステップ 15	**log-adjacency-changes** [**all**] 例： `スイッチ(config-router)# log-adjacency-changes all`	（任意）IS-IS 隣接ステート変更をログするようルータを設定します。End System-to-Intermediate System PDU およびリンクステートパケット（LSP）など、IS-IS Hello に関連しないイベントにより生成されたすべての変更をログに含めるには、**all** を入力します。

	コマンドまたはアクション	目的
ステップ 16	**lsp-mtu***size* 例： スイッチ(config-router)# lsp mtu 1560	（任意）最大 LSP パケット サイズ（バイト）を指定します。指定できる範囲は 128 ～ 4352 バイトです。デフォルト値は 1497 バイトです。 （注） ネットワーク内の任意のリンクで MTU サイズが縮小された場合、ネットワーク内のすべてのルータで LSP MTU サイズを変更する必要があります。
ステップ 17	**partition avoidance** 例： スイッチ(config-router)# partition avoidance	（任意）境界ルータ、すべての隣接レベル 1 ルータ、およびエンド ホスト間で、フル接続が切断された場合、IS-IS レベル 1-2 境界ルータがレベル 1 エリア プレフィックスをレベル 2 バックボーンにアドバタイズしないようにします。
ステップ 18	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 19	**show clns** 例： スイッチ# show clns	入力を確認します。
ステップ 20	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IS-IS インターフェイス パラメータの設定

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがまだレイヤ3インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力し、インターフェイスをレイヤ 3 モードにします。
ステップ 3	**isis metric***default-metric* [**level-1** | **level-2**] 例： `スイッチ(config-if)# isis metric 15`	（任意）指定したインターフェイスにメトリック（またはコスト）を設定します。範囲は 0 ～ 63 です。デフォルトは 10 です。レベルが入力されない場合は、レベル 1 およびレベル 2 ルータの両方にデフォルト値が適用されます。
ステップ 4	**isis hello-interval** {*seconds* | **minimal**} [**level-1** | **level-2**] 例： `スイッチ(config-if)# isis hello-interval minimal`	（任意）スイッチが hello パケットを送信する間隔を指定します。デフォルトでは、hello インターバル *seconds* の 3 倍の値が、送信される hello パケットの *holdtime* としてアドバタイズされます。hello インターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。 • **minimal**：ホールドタイムが 1 秒になるように、システムが hello 乗数に基づいて hello インターバルを計算するようにします。 • *seconds*：範囲は 1 ～ 65535 秒です。デフォルトは 10 秒です。
ステップ 5	**isis hello-multiplier***multiplier* [**level-1** | **level-2**] 例： `スイッチ(config-if)# isis hello-multiplier 5`	（任意）ルータが隣接装置のダウンを宣言するまでに、ネイバーが損失する IS-IS hello パケット数を指定します。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。hello 乗数を小さくすると、高速コンバージェンスとなりますが、ルーティングが不安定になる場合があります。
ステップ 6	**isis csnp-interval***seconds* [**level-1** | **level-2**] 例： `スイッチ(config-if)# isis csnp-interval 15`	（任意）インターフェイスに IS-IS CSNP を設定します。範囲は 0 ～ 65535 です。デフォルトは 10 秒です。
ステップ 7	**isis retransmit-interval***seconds* 例： `スイッチ(config-if)# isis retransmit-interval 7`	（任意）ポイントツーポイント リンクの IS-IS LSP の再送信間隔（秒）を設定します。指定する値は、ネットワーク上の任意の2つのルータ間の予測ラウンドトリップ遅延よりも大きい整数である必要があります。範囲は 0 ～ 65535 です。デフォルトは 5 秒です。

	コマンドまたはアクション	目的
ステップ 8	**isis retransmit-throttle-interval***milliseconds* 例： `スイッチ(config-if)# isis retransmit-throttle-interval 4000`	（任意）IS-IS LSP 再送信スロットルインターバルを設定します。これは、IS-IS LSP がポイントツーポイント リンク上で再送信される最大レート（パケット間のミリ秒数）です。範囲は 0 ～ 65535 です。デフォルト値は、**isis lsp-interval** コマンドにより決定します。
ステップ 9	**isis priority***value* [**level-1** | **level-2**] 例： `スイッチ(config-if)# isis priority 50`	（任意）指定ルータ選択で使用するプライオリティを設定します。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。
ステップ 10	**isis circuit-type** {**level-1** | **level-1-2** | **level-2-only**} 例： `スイッチ(config-if)# isis circuit-type level-1-2`	（任意）指定されたインターフェイス上のネイバーで必要な隣接タイプを設定します（インターフェイスの回線タイプを指定します）。 • **level-1**：このノードとネイバーの両方に共通のエリア アドレスが少なくとも 1 つある場合、レベル 1 隣接関係が確立されます。 • **level-1-2**：ネイバーもレベル 1 およびレベル 2 の両方として設定されていて、少なくとも 1 つの共通のエリアがある場合、レベル 1 およびレベル 2 隣接関係が確立されます。共通のエリアがない場合は、レベル 2 隣接関係が確立されます。これはデフォルト設定です。これはデフォルトです。 • **level 2**：レベル 2 隣接関係が確立されます。ネイバー ルータがレベル 1 ルータである場合、隣接関係は確立されません。
ステップ 11	**isis password***password* [**level-1** | **level-2**] 例： `スイッチ(config-if)# isis password secret`	（任意）インターフェイスの認証パスワードを設定します。デフォルトでは、認証はディセーブルに設定されています。レベル 1 またはレベル 2 を指定すると、それぞれレベル 1 またはレベル 2 ルーティング用のパスワードだけがイネーブルになります。レベルを指定しない場合、デフォルトはレベル 1 およびレベル 2 です。
ステップ 12	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 13	**show clns interface***interface-id* 例： スイッチ# show clns interface gigabitethernet 1/0/1	入力を確認します。
ステップ 14	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

ISO IGRP と IS-IS のモニタリングおよびメンテナンス

CLNSキャッシュのすべての内容または特定のネイバーまたはルートの情報を削除できます。ルーティング テーブル、キャッシュ、およびデータベースの内容など、特定の CLNS または IS-IS の統計情報を表示できます。また、特定のインターフェイス、フィルタ、またはネイバーに関する情報も表示できます。

次の表に、ISO CLNS および IS-IS ルーティングを消去および表示するために使用する特権 EXEC コマンドを示します。出力フィールドの詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference,* 』を参照するか、Cisco IOS コマンド リファレンス マスター インデックスを使用するか、オンライン検索を行ってください。

表 *85*：*ISO CLNS* と *IS-IS* の *clear* および *show* コマンド

コマンド	目的
clear clns cache	CLNSルーティング キャッシュをクリアおよび再初期化します。
clear clns es-neighbors	隣接データベースから End System（ES）ネイバー情報を削除します。
clear clns is-neighbors	隣接データベースから Intermediate System（IS）ネイバー情報を削除します。

コマンド	目的
clear clns neighbors	隣接データベースから CLNS ネイバー情報を削除します。
clear clns route	動的に派生した CLNS ルーティング情報を削除します。
show clns	CLNS ネットワークに関する情報を表示します。
show clns cache	CLNS ルーティング キャッシュ内のエントリを表示します。
show clns es-neighbors	ES ネイバー エントリ（関連のあるエリアなど）を表示します。
show clns filter-expr	フィルタ式を表示します。
show clns filter-set	フィルタ セットを表示します。
show clns interface [*interface-id*]	各インターフェイスの CLNS 固有の情報または ES-IS 情報を表示します。
show clns neighbor	IS-IS ネイバーに関する情報を表示します。
show clns protocol	このルータの IS-IS または ISO IGRP ルーティング プロセスごとにプロトコル固有の情報を表示します。
show clns route	このルータが CLNS パケットをルーティングする方法を把握している宛先をすべて表示します。
show clns traffic	このルータで確認された CLNS パケットに関する情報を表示します。

コマンド	目的
show ip route isis	ISIS IP ルーティング テーブルの現在のステートを表示します。
show isis database	IS-IS リンクステート データベースを表示します。
show isis routes	IS-IS レベル 1 ルーティング テーブルを表示します。
show isis spf-log	IS-IS の Shortest Path First（SPF）計算の履歴を表示します。
show isis topology	すべてのエリアで接続済みルータのリストを表示します。
show route-map	設定されたすべてのルートマップ、または指定した1つのルート マップだけを表示します。
trace clns*destination*	ネットワークのパケットが指定された宛先までに経由するパスを検出します。
which-route {*nsap-address* | *clns-name*}	指定されたCLNSの宛先が見つかったルーティングテーブルを表示します。

ISO CLNS ルーティングの設定例

例：IS-IS ルーティングの設定

次に、従来型の IS-IS を IP ルーティング プロトコルとして実行するために 3 つのルータを設定する方法を示します。従来型の IS-IS では、すべてのルータはレベル 1 およびレベル 2 のルータとして機能します（デフォルト）。

ルータ A：

```
スイッチ(config)# clns routing
スイッチ(config)# router isis
スイッチ(config-router)# net 49.0001.0000.0000.000a.00
スイッチ(config-router)# exit
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# ip router isis
スイッチ(config-if)# clns router isis
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# ip router isis
スイッチ(config-if)# clns router isis
スイッチ(config-router)# exit
```

ルータ B：

```
スイッチ(config)# clns routing
スイッチ(config)# router isis
スイッチ(config-router)# net 49.0001.0000.0000.000b.00
スイッチ(config-router)# exit
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# ip router isis
スイッチ(config-if)# clns router isis
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# ip router isis
スイッチ(config-if)# clns router isis
スイッチ(config-router)# exit
```

ルータ C：

```
スイッチ(config)# clns routing
スイッチ(config)# router isis
スイッチ(config-router)# net 49.0001.0000.0000.000c.00
スイッチ(config-router)# exit
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# ip router isis
スイッチ(config-if)# clns router isis
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# ip router isis
スイッチ(config-if)# clns router isis
スイッチ(config-router)# exit
```

Multi-VRF CE に関する情報

バーチャル プライベート ネットワーク（VPN）は、ISP バックボーン ネットワーク上でお客様にセキュアな帯域幅共有を提供します。VPNは、共通ルーティングテーブルを共有するサイトの集合です。カスタマー サイトは、1 つまたは複数のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーは、VRF テーブルと呼ばれる VPN ルーティング テーブルと各インターフェイスを関連付けます。

スイッチ上で IP サービスまたは拡張 IP サービス フィーチャ セットが稼働している場合、スイッチはカスタマー エッジ（CE）デバイスの複数の VRF ルーティング/転送（Multi-VRF）インスタンスをサポートします（Multi-VRF CE）。サービス プロバイダーは、Multi-VRF CE により、重複する IP アドレスで複数の VPN をサポートできます。

（注） スイッチでは、VPN のサポートのためにマルチプロトコル ラベル スイッチング（MPLS）が使用されません。

Multi-VRF CE の概要

Multi-VRF CE は、サービス プロバイダーが複数の VPN をサポートし、VPN 間で IP アドレスを重複して使用できるようにする機能です。Multi-VRF CE は入力インターフェイスを使用して、さまざまな VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスと各 VRF を関連付けて仮想パケット転送テーブルを形成します。VRF 内のインターフェイスは、イーサネット ポートのように物理的なもの、または VLAN SVI のように論理的なものにもできますが、複数の VRF に属すことはできません。

（注） Multi-VRF CE インターフェイスは、レイヤ 3 インターフェイスである必要があります。

Multi-VRF CE には、次のデバイスが含まれます。

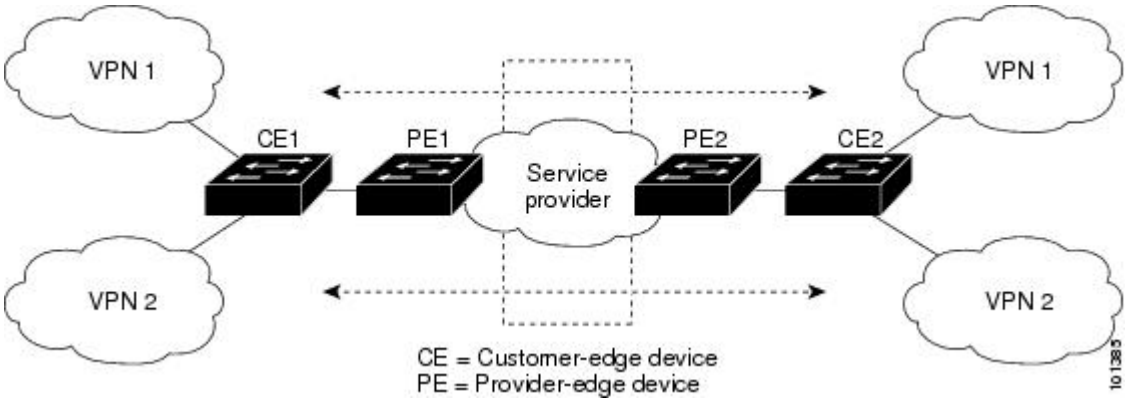
- お客様は、CE デバイスにより、1 つまたは複数のプロバイダー エッジ（PE）ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE デバイスは、サイトのローカル ルートをルータにアドバタイズし、リモート VPN ルートをそこから学習します。スイッチを CE に設定することができます。
- PE ルータは、スタティック ルーティング、または BGP、RIPv2、OSPF、EIGRP などのルーティング プロトコルを使用して、CE デバイスとルーティング情報を交換します。PE は、直接接続している VPN に対する VPN ルートのみを保守する必要があります。そのため、すべてのサービス プロバイダー VPN ルートを PE が保守する必要はありません。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に存在する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。PE ルータは、ローカル VPN ルートを CE から学習したあとで、IBGP を使用して別の PE ルータと VPN ルーティング情報を交換します。
- CE デバイスに接続していないサービス プロバイダー ネットワークのルータは、プロバイダー ルータやコア ルータになります。

Multi-VRF CE では、複数のお客様が 1 つの CE を共有でき、CE と PE の間で 1 つの物理リンクだけが使用されます。共有 CE は、お客様ごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、お客様ごとにパケットをスイッチングまたはルーティングします。Multi-VRF CE は、制限付きの PE 機能を CE デバイスに拡張して、別々の VRF テーブルを維持し、VPN のプライバシーおよびセキュリティをブランチ オフィスに拡張します。

ネットワーク トポロジ

次の図に、スイッチを複数の仮想 CE として使用した構成例を示します。このシナリオは、中小企業など、VPN サービスの帯域幅要件の低いお客様に適しています。この場合、スイッチにはマルチ VRF CE のサポートが必要です。Multi-VRF CE はレイヤ 3 機能なので、VRF のそれぞれのインターフェイスはレイヤ 3 インターフェイスである必要があります。

図 *62*：複数の仮想 *CE* として機能するスイッチ



CE スイッチは、レイヤ 3 インターフェイスを VRF に追加するコマンドを受信すると、Multi-VRF CE 関連のデータ構造で VLAN ID と Policy Label（PL）の間に適切なマッピングを設定し、VLAN ID と PL を VLAN データベースに追加します。

Multi-VRF CE を設定すると、レイヤ 3 フォワーディング テーブルは、次の 2 つのセクションに概念的に分割されます。

- Multi-VRF CE ルーティング セクションには、さまざまな VPN からのルートが含まれます。
- グローバル ルーティング セクションには、インターネットなど、VPN 以外のネットワークへのルートが含まれます。

さまざまな VRF の VLAN ID はさまざまな PL にマッピングされ、処理中に VRF を区別するために使用されます。レイヤ3設定機能では、学習した新しいVPNルートごとに、入力ポートのVLAN ID を使用して PL を取得し、Multi-VRF CE ルーティング セクションに PL および新しいルートを挿入します。ルーテッド ポートからパケットを受信した場合は、ポート内部 VLAN ID 番号が使用されます。SVI からパケットを受信した場合は、VLAN 番号が使用されます。

パケット転送処理

Multi-VRF CE 対応ネットワークのパケット転送処理は次のとおりです。

- スイッチは、VPN からパケットを受信すると、入力 PL 番号に基づいてルーティング テーブルを検索します。ルートが見つかると、スイッチはパケットを PE に転送します。
- 入力 PE は、CE からパケットを受信すると、VRF 検索を実行します。ルートが見つかると、ルータは対応する MPLS ラベルをパケットに追加し、MPLS ネットワークに送信します。

- 出力 PE は、ネットワークからパケットを受信すると、ラベルを除去してそのラベルを使用し、正しい VPN ルーティング テーブルを識別します。次に、通常のルート検索を実行します。ルートが見つかると、パケットを正しい隣接デバイスに転送します。
- CE は、出力 PE からパケットを受信すると、入力 PL を使用して正しい VPN ルーティング テーブルを検索します。ルートが見つかると、パケットを VPN 内で転送します。

ネットワーク コンポーネント

VRF を設定するには、VRF テーブルを作成し、VRF に関連するレイヤ 3 インターフェイスを指定します。次に、VPN、および CE と PE 間でルーティング プロトコルを設定します。プロバイダーのバックボーンで VPN ルーティング情報を配信する場合は、BGP が優先ルーティング プロトコルです。Multi-VRF CE ネットワークには、次の 3 つの主要コンポーネントがあります。

- VPN ルート ターゲット コミュニティ：VPN コミュニティのその他すべてのメンバのリスト。VPN コミュニティ メンバーごとに VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング：VPN コミュニティのすべてのメンバーに VRF 到達可能性情報を伝播します。VPN コミュニティのすべての PE ルータで BGP ピアリングを設定する必要があります。
- VPN 転送：VPN サービス プロバイダー ネットワークを介し、全 VPN コミュニティ メンバー間で、全トラフィックを伝送します。

VRF 認識サービス

IP サービスはグローバル インターフェイスに設定可能で、グローバル ルーティング インスタンスで稼働します。IP サービスは複数のルーティング インスタンス上で稼働するように拡張されます。これが、VRF 認識です。システム内の任意の設定済み VRF であればいずれも、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームに依存しないモジュールに実装されます。VRF とは、Cisco IOS 内の複数のルーティング インスタンスを意味します。各プラットフォームには、サポートする VRF 数に関して独自の制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに ping を実行できます。
- ARP エントリは、個別の VRF で学習されます。ユーザは、特定の VRF の ARP エントリを表示できます。

Multi-VRF CE の設定方法

Multi-VRF CE のデフォルト設定

表 ***86*** : ***VRF*** のデフォルト設定

機能	デフォルト設定
VRF	ディセーブルVRF は定義されていません。
マップ	インポートマップ、エクスポートマップ、ルートマップは定義されていません。
VRF 最大ルート数	ファスト イーサネット スイッチ：8000 ギガビット イーサネット スイッチ：12000
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブルです。

Multi-VRF CE の設定時の注意事項

（注） Multi-VRF CE を使用するには、スイッチで IP サービスまたは拡張 IP サービス フィーチャ セットをイネーブルにする必要があります。

- Multi-VRF CE を含むスイッチは複数のお客様によって共有され、各お客様には独自のルーティング テーブルがあります。
- お客様は別々の VRF テーブルを使用するので、同じ IP アドレスを再利用できます。別々の VPN では IP アドレスの重複が許可されます。
- Multi-VRF CE では、複数のお客様が、PE と CE の間で同じ物理リンクを共有できます。複数の VLAN を持つトランク ポートでは、パケットがお客様間で分離されます。それぞれのお客様には独自の VLAN があります。
- Multi-VRF CE ではサポートされない MPLS-VRF 機能があります。ラベル交換、LDP 隣接関係、ラベル付きパケットはサポートされません。
- PE ルータの場合、Multi-VRF CE の使用と複数の CE の使用に違いはありません。図 41-6 では、複数の仮想レイヤ 3 インターフェイスが Multi-VRF CE デバイスに接続されています。
- スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合わせを使用して、VRF を設定できます。SVI は、アクセス ポートまたはトランク ポートで接続できます。
- お客様は、別のお客様と重複しないかぎり、複数の VLAN を使用できます。お客様の VLAN は、スイッチに保存されている適切なルーティング テーブルの識別に使用される特定のルーティング テーブル ID にマッピングされます。
- スイッチは、1 つのグローバル ネットワークおよび最大 26 の VRF をサポートします。
- CE と PE の間では、ほとんどのルーティング プロトコル（BGP、OSPF、RIP、およびスタティック ルーティング）を使用できます。ただし、次の理由から External BGP（EBGP）を使用することを推奨します。
  - BGP では、複数の CE とのやり取りに複数のアルゴリズムを必要としません。
  - BGP は、さまざまな管理者によって稼働するシステム間でルーティング情報を渡すように設計されています。
  - BGP では、ルートの属性を CE に簡単に渡すことができます。
- Multi-VRF CE は、パケットのスイッチング レートに影響しません。
- VPN マルチキャストはサポートされません。
- プライベート VLAN で VRF をイネーブルにできます（逆も同様です）。
- インターフェイスでポリシーベース ルーティング（PBR）がイネーブルになっている場合は、VRF をイネーブルにできません（逆も同様です）。
- インターフェイスで Web Cache Communication Protocol（WCCP）がイネーブルになっている場合は、VRF をイネーブルにできません（逆も同様です）。

VRF の設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： スイッチ(config)# ip routing	IP ルーティングをイネーブルにします。
ステップ 3	**ip vrf***vrf-name* 例： スイッチ(config)# ip vrf vpn1	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd***route-distinguisher* 例： スイッチ(config-vrf)# rd 100:2	ルート識別子を指定して VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： スイッチ(config-vrf)# route-target both 100:2	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同一にする必要があります。
ステップ 6	**import map***route-map* 例： スイッチ(config-vrf)# import map importmap1	（任意）VRF にルート マップを対応付けます。

	コマンドまたはアクション	目的
ステップ 7	**interface***interface-id* 例： スイッチ(config-vrf)# interface gigabitethernet 1/0/1	VRF に関連付けるレイヤ3インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスにはルーテッドポートまたは SVI を設定できます。
ステップ 8	**ip vrf forwarding***vrf-name* 例： スイッチ(config-if)# ip vrf forwarding vpn1	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 10	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： スイッチ# show ip vrf interfaces vpn1	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VRF 認識サービスの設定

次のサービスは、VRF 認識です。

- ARP
- ping
- 簡易ネットワーク管理プロトコル（SNMP）
- ユニキャスト RPF（uRPF）
- Syslog
- traceroute

- FTP および TFTP

（注） このスイッチでは、ユニキャスト RPF（uRPF）およびネットワーク タイム プロトコル（NTP）に対して VRF 認識のサービスはサポートされません。

ARP 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ip arp vrf***vrf-name* 例： `スイッチ# show ip arp vrf vpn1`	指定された VRF 内の ARP テーブルを表示します。

ping 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ping vrf***vrf-name***ip-host** 例： `スイッチ# ping vrf vpn1 ip-host`	指定された VRF 内の ARP テーブルを表示します。

SNMP 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server trap authentication vrf** 例： スイッチ(config)# snmp-server trap authentication vrf	VRF で、パケットに対して SNMP トラップをイネーブルにします。
ステップ 3	**snmp-server engineID remote***host***vrf***vpn-instance engine-id string* 例： スイッチ(config)# snmp-server engineID remote 172.16.20.3 vrf vpn1 80000009030000B064EFE100	スイッチ上で、リモート SNMP エンジンの名前を設定します。
ステップ 4	**snmp-server host***host***vrf***vpn-instance***traps***community* 例： スイッチ(config)# snmp-server host 172.16.20.3 vrf vpn1 traps comaccess	SNMP トラップ動作の受信側、および SNMP トラップの送信に使用される VRF テーブルを指定します。
ステップ 5	**snmp-server host***host***vrf***vpn-instance***informs***community* 例： スイッチ(config)# snmp-server host 172.16.20.3 vrf vpn1 informs comaccess	SNMP 通知動作の受信先を指定し、SNMP 通知の送信に使用される VRF テーブルを指定します。
ステップ 6	**snmp-server user***user group***remote***host***vrf***vpn-instance security model* 例： スイッチ(config)# snmp-server user abcd remote 172.16.20.3 vrf vpn1 priv v2c 3des secure3des	SNMP アクセス用に、VRF 上にあるリモートホストの SNMP グループにユーザを追加します。
ステップ 7	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

uRPF 用 VRF 認識サービスの設定

uRPF は、VRF に割り当てられたインターフェイス上で設定でき、送信元検索が VRF テーブルで実行されます。

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no switchport** 例： `スイッチ(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	**ip vrf forwarding***vrf-name* 例： `スイッチ(config-if)# ip vrf forwarding vpn2`	インターフェイス上で VRF を設定します。
ステップ 5	**ip address***ip-address* 例： `スイッチ(config-if)# ip address 10.1.5.1`	インターフェイスの IP アドレスを入力します。
ステップ 6	**ip verify unicast reverse-path** 例： `スイッチ(config-if)# ip verify unicast reverse-path`	インターフェイス上で uRPF をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

VRF 認識 RADIUS の設定

VRF 認識 RADIUS を設定するには、まず RADIUS サーバ上で AAA をイネーブルにする必要があります。『Per VRF AAA Feature Guide』で説明されているとおり、スイッチで **ip vrf forwarding** *vrf-name* サーバグループ コンフィギュレーション コマンドと **ip radius source-interface** グローバル コンフィギュレーション コマンドがサポートされます。

syslog 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging on** 例： スイッチ(config)# logging on	ストレージ ルータ イベント メッセージのロギングを、イネーブルまたは一時的にディセーブルにします。
ステップ 3	**logging host***ip-address***vrf***vrf-name* 例： スイッチ(config)# logging host 10.10.1.0 vrf vpn1	ロギング メッセージが送信される Syslog サーバのホスト アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 4	**logging buffered***logging buffered size***debugging** 例： `スイッチ(config)# logging buffered critical 6000 debugging`	メッセージを内部バッファにロギングします。
ステップ 5	**logging trap debugging** 例： `スイッチ(config)# logging trap debugging`	Syslog サーバに送信されるロギング メッセージを制限します。
ステップ 6	**logging facility***facility* 例： `スイッチ(config)# logging facility user`	ロギング ファシリティにシステム ロギング メッセージを送信します。
ステップ 7	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

traceroute 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『Cisco IOS Switching Services Command Reference, Release 12.4』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**traceroute vrf***vrf-name ipaddress* 例： `スイッチ(config)# traceroute vrf vpn2 10.10.1.1`	宛先アドレスを取得する VPN VRF の名前を指定します。

FTP および TFTP 用 VRF 認識サービスの設定

FTP および TFTP を VRF 認識とするには、いくつかの FTP/TFTP CLI を設定する必要があります。たとえば、インターフェイスに付加される VRF テーブルを使用する場合、E1/0 であれば、ip tftp source-interface E1/0 コマンドまたは ip ftp source-interface E1/0 コマンドを設定して、特定のルーティング テーブルを使用するように TFTP または FTP サーバに通知する必要があります。この例では、VRF テーブルが宛先 IP アドレスを検索するのに使用されます。これらの変更には下位互換性があり、既存の動作には影響を及ぼしません。つまり、VRF がそのインターフェイスに設定されていない場合でも、送信元インターフェイス CLI を使用して、特定のインターフェイスにパケットを送信できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip ftp source-interface***interface-type interface-number* 例： スイッチ(config)# ip ftp source-interface gigabitethernet 1/0/2	FTP 接続の発信元 IP アドレスを指定します。
ステップ 3	**end** 例： スイッチ(config)#end	特権 EXEC モードに戻ります。
ステップ 4	**configure terminal** 例： スイッチ# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 5	**ip tftp source-interface***interface-type interface-number* 例： スイッチ(config)# ip tftp source-interface gigabitethernet 1/0/2	TFTP 接続用の送信元 IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**end** 例： スイッチ(config)#end	特権 EXEC モードに戻ります。

マルチキャスト VRF の設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS IP Multicast Command Reference*』を参照してください。

Multi-VRF CE 内でのマルチキャスト設定の詳細については、『*IP Routing: Protocol-Independent Configuration Guide, Cisco IOS Release 15S*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： スイッチ(config)# ip routing	IP ルーティング モードをイネーブルにします
ステップ 3	**ip vrf***vrf-name* 例： スイッチ(config)# ip vrf vpn1	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**rd***route-distinguisher* 例： `スイッチ(config-vrf)# rd 100:2`	ルート識別子を指定して VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `スイッチ(config-vrf)# route-target import 100:2`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同一にする必要があります。
ステップ 6	**import map***route-map* 例： `スイッチ(config-vrf)# import map importmap1`	（任意）VRF にルート マップを対応付けます。
ステップ 7	**ip multicast-routing vrf***vrf-name***distributed** 例： `スイッチ(config-vrf)# ip multicast-routing vrf vpn1 distributed`	（任意）VRF テーブルでグローバル マルチキャスト ルーティングをイネーブルにします。
ステップ 8	**interface***interface-id* 例： `スイッチ(config-vrf)# interface gigabitethernet 1/0/2`	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスはルーテッド ポートまたは SVI に設定できます。
ステップ 9	**ip vrf forwarding***vrf-name* 例： `スイッチ(config-if)# ip vrf forwarding vpn1`	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 10	**ip address***ip-address***mask** 例： `スイッチ(config-if)# ip address 10.1.5.1 255.255.255.0`	レイヤ 3 インターフェイスの IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 11	**ip pim sparse-dense mode** 例： `スイッチ(config-if)# ip pim sparse-dense mode`	VRF に関連付けられているレイヤ 3 インターフェイス上で、PIM をイネーブルにします。
ステップ 12	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： `スイッチ# show ip vrf detail vpn1`	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 14	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされている任意のルーティング プロトコル（RIP、OSPF、EIGRP、BGP）、またはスタティック ルーティングで設定できます。ここで説明する設定はOSPF のものですが、その他のプロトコルでも手順は同じです。

（注） VRF インスタンス内で EIGRP ルーティング プロセスが実行されるように設定するには、**autonomous-system***autonomous-system-number* アドレス ファミリ コンフィギュレーション モード コマンドを入力して、自律システム番号を設定する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf***process-id* **vrf***vrf-name* 例： `スイッチ(config)# router ospf 1 vrf vpn1`	OSPF ルーティングをイネーブルにして VPN 転送テーブルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**log-adjacency-changes** 例： `スイッチ(config-router)# log-adjacency-changes`	（任意）隣接ステートの変更を記録します。これは、デフォルトの状態です。
ステップ 4	**redistribute bgp***autonomous-system-number* **subnets** 例： `スイッチ(config-router)# redistribute bgp 10 subnets`	BGP ネットワークから OSPF ネットワークに情報を再配布するようにスイッチを設定します。
ステップ 5	**network***network-number* **area***area-id* 例： `スイッチ(config-router)# network 1 area 2`	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**end** 例： `スイッチ(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip ospf***process-id* 例： `スイッチ# show ip ospf 1`	OSPF ネットワークの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP PE/CE ルーティング セッションの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system-number* 例： `スイッチ(config)# router bgp 2`	その他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**network***network-number***mask***network-mask* 例： `スイッチ(config-router)# network 5 mask 255.255.255.0`	BGP を使用してアナウンスするネットワークおよびマスクを指定します。
ステップ 4	**redistribute ospf***process-id***match internal** 例： `スイッチ(config-router)# redistribute ospf 1 match internal`	OSPF 内部ルートを再配布するようにスイッチを設定します。
ステップ 5	**network***network-number***area***area-id* 例： `スイッチ(config-router)# network 5 area 2`	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**address-family ipv4 vrf***vrf-name* 例： `スイッチ(config-router)# address-family ipv4 vrf vpn1`	PE/CE ルーティング セッションの BGP パラメータを定義し、VRF アドレス ファミリ モードを開始します。
ステップ 7	**neighbor***address***remote-as***as-number* 例： `スイッチ(config-router)# neighbor 10.1.1.2 remote-as 2`	PE と CE ルータの間の BGP セッションを定義します。

	コマンドまたはアクション	目的
ステップ 8	**neighbor***address***activate** 例： `スイッチ(config-router)# neighbor 10.2.1.1 activate`	IPv4 アドレス ファミリのアドバタイズメントをアクティブ化します。
ステップ 9	**end** 例： `スイッチ(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip bgp** [**ipv4**] [**neighbors**] 例： `スイッチ# show ip bgp ipv4 neighbors`	BGP 設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Multi-VRF CE のモニタリング

表 *87*：***Multi-VRF CE*** 情報を表示するコマンド

show ip protocols vrf *vrf-name*	VRF に対応付けられたルーティング プロトコル情報を表示します。
show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**] [**supernets-only**]	VRF に対応付けられた IP ルーティング テーブル情報を表示します。
show ip vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]	定義された VRF インスタンスに関する情報を表示します。

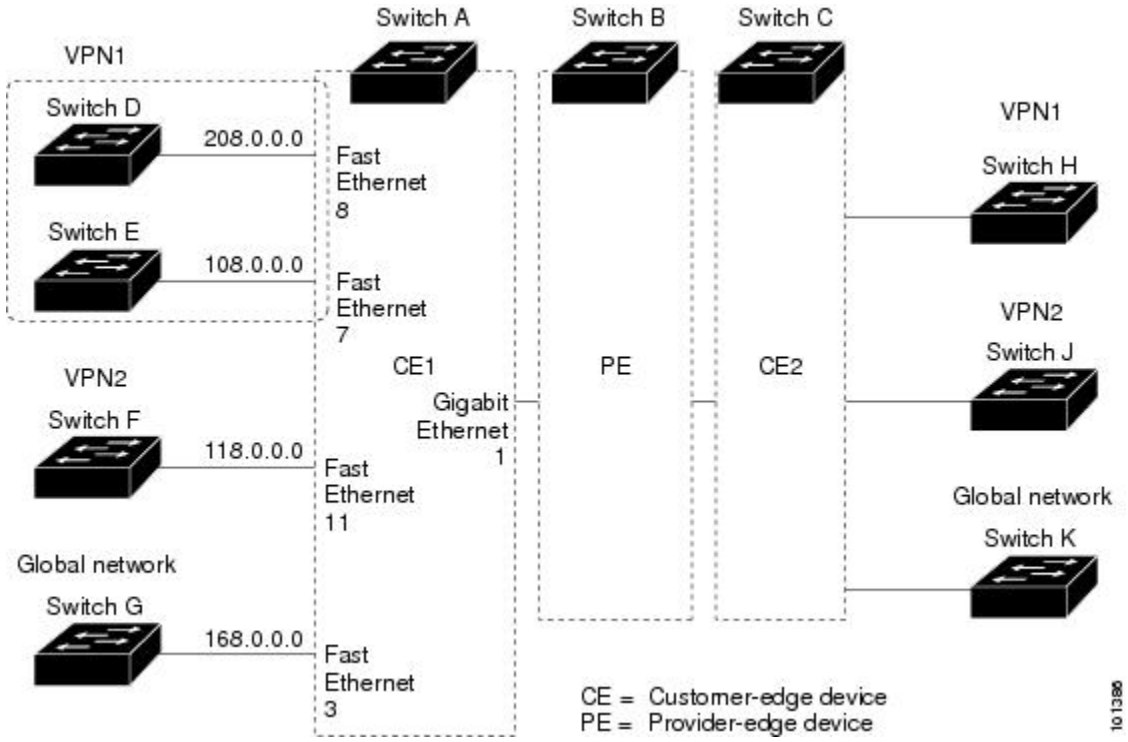
表示される情報の詳細については、『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

Multi-VRF CE の設定例

Multi-VRF CE の設定例

VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。CE/PE 接続には BGP が使用されます。図のあとに続く出力は、スイッチを CE スイッチ A として設定する例、およびカスタマー スイッチ D と F の VRF 設定を示しています。CE スイッチ C とその他のカスタマー スイッチを設定するコマンドは含まれていませんが、内容は同様です。この例には、PE ルータとして動作する Catalyst 6000 スイッチまたは Catalyst 6500 スイッチのスイッチ A へのトラフィックを設定するコマンドも含まれています。

図 *63*：*Multi-VRF CE* の設定例



スイッチ A では、ルーティングをイネーブルにして VRF を設定します。

```
スイッチ# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチ(config)# ip routing
スイッチ(config)# ip vrf v11
スイッチ(config-vrf)# rd 800:1
スイッチ(config-vrf)# route-target export 800:1
スイッチ(config-vrf)# route-target import 800:1
スイッチ(config-vrf)# exit
スイッチ(config)# ip vrf v12
スイッチ(config-vrf)# rd 800:2
```

```
スイッチ(config-vrf)# route-target export 800:2
スイッチ(config-vrf)# route-target import 800:2
スイッチ(config-vrf)# exit
```

スイッチ A のループバックおよび物理インターフェイスを設定します。ギガビット イーサネット ポート 1 は PE へのトランク接続です。ギガビット イーサネット ポート 8 と 11 は VPN に接続されます。

```
スイッチ(config)# interface loopback1
スイッチ(config-if)# ip vrf forwarding v11
スイッチ(config-if)# ip address 8.8.1.8 255.255.255.0
スイッチ(config-if)# exit

スイッチ(config)# interface loopback2
スイッチ(config-if)# ip vrf forwarding v12
スイッチ(config-if)# ip address 8.8.2.8 255.255.255.0
スイッチ(config-if)# exit

スイッチ(config)# interface gigabitethernet1/0/5
スイッチ(config-if)# switchport trunk encapsulation dot1q
スイッチ(config-if)# switchport mode trunk
スイッチ(config-if)# no ip address
スイッチ(config-if)# exit
スイッチ(config)# interface gigabitethernet1/0/8
スイッチ(config-if)# switchport access vlan 208
スイッチ(config-if)# no ip address
スイッチ(config-if)# exit
スイッチ(config)# interface gigabitethernet1/0/11
スイッチ(config-if)# switchport trunk encapsulation dot1q
スイッチ(config-if)# switchport mode trunk
スイッチ(config-if)# no ip address
スイッチ(config-if)# exit
```

スイッチ A で使用する VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。VLAN 118 と 208 は、それぞれスイッチ F とスイッチ D を含む VPN に使用されます。

```
スイッチ(config)# interface vlan10
スイッチ(config-if)# ip vrf forwarding v11
スイッチ(config-if)# ip address 38.0.0.8 255.255.255.0
スイッチ(config-if)# exit
スイッチ(config)# interface vlan20
スイッチ(config-if)# ip vrf forwarding v12
スイッチ(config-if)# ip address 83.0.0.8 255.255.255.0
スイッチ(config-if)# exit
スイッチ(config)# interface vlan118
スイッチ(config-if)# ip vrf forwarding v12
スイッチ(config-if)# ip address 118.0.0.8 255.255.255.0
スイッチ(config-if)# exit
スイッチ(config)# interface vlan208
スイッチ(config-if)# ip vrf forwarding v11
スイッチ(config-if)# ip address 208.0.0.8 255.255.255.0
スイッチ(config-if)# exit
```

VPN1 と VPN2 で OSPF ルーティングを設定します。

```
スイッチ(config)# router ospf 1 vrf vl1
スイッチ(config-router)# redistribute bgp 800 subnets
スイッチ(config-router)# network 208.0.0.0 0.0.0.255 area 0
```

```
スイッチ(config-router)# exit
スイッチ(config)# router ospf 2 vrf vl2
スイッチ(config-router)# redistribute bgp 800 subnets
スイッチ(config-router)# network 118.0.0.0 0.0.0.255 area 0
スイッチ(config-router)# exit
```

CE/PE ルーティングに BGP を設定します。

```
スイッチ(config)# router bgp 800
スイッチ(config-router)# address-family ipv4 vrf vl2
スイッチ(config-router-af)# redistribute ospf 2 match internal
スイッチ(config-router-af)# neighbor 83.0.0.3 remote-as 100
スイッチ(config-router-af)# neighbor 83.0.0.3 activate
スイッチ(config-router-af)# network 8.8.2.0 mask 255.255.255.0
スイッチ(config-router-af)# exit
スイッチ(config-router)# address-family ipv4 vrf vl1
スイッチ(config-router-af)# redistribute ospf 1 match internal
スイッチ(config-router-af)# neighbor 38.0.0.3 remote-as 100
スイッチ(config-router-af)# neighbor 38.0.0.3 activate
スイッチ(config-router-af)# network 8.8.1.0 mask 255.255.255.0
スイッチ(config-router-af)# end
```

スイッチ D は VPN 1 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
スイッチ# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチ(config)# ip routing
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# no switchport
スイッチ(config-if)# ip address 208.0.0.20 255.255.255.0
スイッチ(config-if)# exit

スイッチ(config)# router ospf 101
スイッチ(config-router)# network 208.0.0.0 0.0.0.255 area 0
スイッチ(config-router)# end
```

スイッチ F は VPN 2 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
スイッチ# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチ(config)# ip routing
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# switchport trunk encapsulation dot1q
スイッチ(config-if)# switchport mode trunk
スイッチ(config-if)# no ip address
スイッチ(config-if)# exit

スイッチ(config)# interface vlan118
スイッチ(config-if)# ip address 118.0.0.11 255.255.255.0
スイッチ(config-if)# exit

スイッチ(config)# router ospf 101
スイッチ(config-router)# network 118.0.0.0 0.0.0.255 area 0
スイッチ(config-router)# end
```

このコマンドをスイッチ B（PE ルータ）で使用すると、CE デバイス、スイッチ A に対する接続だけが設定されます。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
```

```
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit
Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/1/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/1/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf vl
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end
```

ユニキャスト リバース パス転送の設定

uRPF 機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造（スプーフィングされた）送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。たとえば、Smurf や Tribal Flood Network（TFN）など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタすることを攻撃者が阻止できるようにします。パブリック アクセスを提供するインターネット サービス プロバイダー（ISP）の場合、uRPF が IP ルーティング テーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、そのような攻撃をそらします。この処理により、ISP のネットワーク、その顧客、および残りのインターネットが保護されます。

（注）
- uRPF は、IP サービス でサポートされます。
- スイッチが複数のスイッチ タイプが混在する混合ハードウェア スタック内にある場合は、uRPF を設定しないでください。たとえば、Catalyst 3750-X、Catalyst 3750-E、Catalyst 3750 スイッチです。

IP uRPF 設定の詳細については、『*Cisco IOS Security Configuration Guide*』の「*Other Security Features*」の章を参照してください。

プロトコル独立機能

この項では、IP ルーティング プロトコルに依存しない機能について説明します。これらの機能は、IP Baseまたは IP Services フィーチャ セットが稼働するスイッチ上で使用できますが、IP Base フィーチャ セット付属のプロトコル関連機能は RIP でだけ使用できます。この章の IP ルーティング プロトコル独立コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』の「IP Routing Protocol-Independent Commands」の章を参照してください。

分散型シスコ エクスプレス フォワーディング

シスコ エクスプレス フォワーディングに関する情報

シスコエクスプレス フォワーディング（CEF）は、ネットワーク パフォーマンスを最適化するために使用されるレイヤ 3 IP スイッチング技術です。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に割り当てることができます。スイッチ スタックでは、ハードウェアによって distributed CEF（dCEF）が使用されます。動的なネットワークでは、ルーティングの変更によって、高速スイッチング キャッシュ エントリが頻繁に無効になります。高速スイッチング キャッシュ エントリが無効になると、トラフィックがルート キャッシュによって高速スイッチングされずに、ルーティング テーブルによってプロセス スイッチングされることがあります。CEF および dCEF は転送情報ベース（FIB）検索テーブルを使用して、宛先ベースの IP パケット スイッチングを実行します。

CEF および dCEF での 2 つの主要なコンポーネントは、分散 FIB と分散隣接テーブルです。

- FIB はルーティング テーブルや情報ベースと同様、IP ルーティング テーブルに転送情報のミラーイメージが保持されます。ネットワーク内でルーティングまたはトポロジが変更されると、IP ルーティング テーブルがアップデートされ、これらの変更が FIB に反映されます。FIB には、IP ルーティング テーブル内の情報に基づいて、ネクストホップのアドレス情報が保持されます。FIB にはルーティング テーブル内の既知のルートがすべて格納されているため、CEF はルート キャッシュをメンテナンスする必要がなく、トラフィックのスイッチングがより効率化され、トラフィック パターンの影響も受けません。

- リンク層上でネットワーク内のノードが 1 ホップで相互に到達可能な場合、これらのノードは隣接関係にあると見なされます。CEF は隣接テーブルを使用し、レイヤ 2 アドレッシング情報を付加します。隣接テーブルには、すべての FIB エントリに対する、レイヤ 2 のネクストホップのアドレスが保持されます。

スイッチまたはスイッチスタックは、ギガビット速度の回線レート IP トラフィックを達成するため特定用途向け集積回路（ASIC）を使用しているので、CEF または dCEF 転送はソフトウェア転送パス（CPU により転送されるトラフィック）にだけ適用されます。

シスコ エクスプレス フォワーディングの設定方法

デフォルトで、CEF または dCEF はグローバルにイネーブルに設定されています。何らかの理由でこれがディセーブルになった場合は、**ip cef** または **ip cef distributed** グローバル コンフィギュレーション コマンドを使用し、再度イネーブルに設定できます。

デフォルト設定では、すべてのレイヤ 3 インターフェイスで CEF または dCEF がイネーブルです。**no ip route-cache cef** インターフェイス コンフィギュレーション コマンドを入力すると、ソフトウェアが転送するトラフィックに対して CEF がディセーブルになります。このコマンドは、ハードウェア転送パスには影響しません。CEF をディセーブルにして **debug ip packet detail** 特権 EXEC コマンドを使用すると、ソフトウェア転送トラフィックをデバッグするのに便利です。ソフトウェア転送パス用のインターフェイスで CEF をイネーブルにするには、**ip route-cache cef** インターフェイス コンフィギュレーション コマンドを使用します。

注意 CLI には、インターフェイス上で CEF をディセーブルにする **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドが表示されますが、デバッグ以外の目的でインターフェイス上で CEF または dCEF をディセーブルにしないようにしてください。

ディセーブルである CEF または dCEF をグローバルにイネーブルにしたり、ソフトウェア転送トラフィックのインターフェイス上でイネーブルにするには、次の手順を実行します。

手順の概要

1. **configureterminal**
2. **ip cef**
3. **ip cef distributed**
4. **interface***interface-id*
5. **ip route-cache cef**
6. **end**
7. **show ip cef**
8. **show cef linecard** [**detail**]
9. **show cef linecard** [*slot-number*] [**detail**]
10. **show cef interface** [*interface-id*]
11. **show adjacency**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip cef** 例： スイッチ(config)# ip cef	非スタッキング スイッチで CEF の動作をイネーブルにします。 ステップ 4 に進みます。
ステップ 3	**ip cef distributed** 例： スイッチ(config)# ip cef distributed	アクティブ スイッチで CEF の動作をイネーブルにします。
ステップ 4	**interface***interface-id* 例： スイッチ(config)# interface gigabitethernet 1/0/1	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 5	**ip route-cache cef** 例： スイッチ(config-if)# ip route-cache cef	ソフトウェア転送トラフィック用のインターフェイスで CEF をイネーブルにします。
ステップ 6	**end** 例： スイッチ(config-if)# end	特権 EXEC モードに戻ります。
ステップ 7	**show ip cef** 例： スイッチ# show ip cef	すべてのインターフェイスの CEF ステータスを表示します。
ステップ 8	**show cef linecard** [**detail**] 例： スイッチ# show cef linecard detail	（任意）非スタッキング スイッチの CEF 関連インターフェイス情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	**show cef linecard** [*slot-number*] [**detail**] 例： `スイッチ# show cef linecard 5 detail`	（任意）スタック内のすべてのスイッチ、または指定されたスイッチに対して、スイッチのCEF関連インターフェイス情報をスタック メンバ別に表示します。 （任意）*slot-number* には、スタック メンバーのスイッチ番号を入力します。
ステップ 10	**show cef interface** [*interface-id*] 例： `スイッチ# show cef interface gigabitethernet 1/0/1`	すべてのインターフェイスまたは指定されたインターフェイスの詳細な CEF 情報を表示します。
ステップ 11	**show adjacency** 例： `スイッチ# show adjacency`	CEF の隣接テーブル情報を表示します。
ステップ 12	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

等コスト ルーティング パスの個数

等コスト ルーティング パスに関する情報

同じネットワークへ向かう同じメトリックのルートが複数ルータに格納されている場合、これらのルートは等価コストを保有していると見なされます。ルーティング テーブルに複数の等コスト ルートが含まれる場合は、これらをパラレル パスと呼ぶこともあります。ネットワークへの等コスト パスがルータに複数格納されている場合、ルータはこれらを同時に使用できます。パラレル パスを使用すると、パスに障害が発生した場合に冗長性を確保できます。また、使用可能なパスにパケットの負荷を分散し、使用可能な帯域幅を有効利用することもできます。等コスト ルートは、スタック内の各スイッチでサポートされます。

等コスト ルートはルータによって自動的に取得、設定されますが、ルーティング テーブルの IP ルーティング プロトコルでサポートされるパラレル パスの最大数は制御可能です。スイッチ ソフトウェア では最大 32 の等コスト ルーティングが許可されていますが、スイッチ ハードウェアはルートあたり 17 パス以上は使用しません。

等コスト ルーティング パスの設定方法

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**bgp** | **rip** | **ospf** | **eigrp**} 例： `スイッチ(config)# router eigrp`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**maximum-paths** *maximum* 例： `スイッチ(config-router)# maximum-paths 2`	プロトコル ルーティング テーブルのパラレル パスの最大数を設定します。指定できる範囲は 1 ～ 16 です。ほとんどの IP ルーティング プロトコルでデフォルトは 4 ですが、BGP の場合だけ 1 です。
ステップ 4	**end** 例： `スイッチ(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols** 例： `スイッチ# show ip protocols`	*Maximum path* フィールドの設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スタティック ユニキャスト ルート

スタティック ユニキャスト ルートに関する情報

スタティック ユニキャスト ルートは、特定のパスを通過して送信元と宛先間でパケットを送受信するユーザ定義のルートです。ルータが特定の宛先へのルートを構築できない場合、スタティッ

ク ルートは重要で、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

ユーザによって削除されるまで、スタティック ルートはスイッチに保持されます。ただし、アドミニストレーティブディスタンスの値を割り当て、スタティック ルートをダイナミック ルーティング情報で上書きできます。各ダイナミック ルーティング プロトコルには、デフォルトのアドミニストレーティブ ディスタンスが設定されています（表 10 を参照）。ダイナミック ルーティング プロトコルの情報でスタティック ルートを上書きする場合は、スタティック ルートのアドミニストレーティブ ディスタンスがダイナミック プロトコルのアドミニストレーティブ ディスタンスよりも大きな値になるように設定します。

表 *88*：ダイナミック ルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルト距離
接続されているインターフェイス	0
スタティック ルート	1
EIGRP サマリー ルート	5
外部 BGP	20
内部 EIGRP	90
IGRP	100
OSPF	110
内部 BGP	200
不明（Unknown）	225

インターフェイスを指し示すスタティック ルートは、RIP、IGRP、およびその他のダイナミック ルーティング プロトコルを通してアドバタイズされます。**redistribute** スタティック ルータ コンフィギュレーション コマンドが、これらのルーティング プロトコルに対して指定されているかどうかは関係ありません。これらのスタティック ルートがアドバタイズされるのは、インターフェイスを指し示すスタティック ルートが接続された結果、静的な性質を失ったとルーティング テーブルで見なされるためです。ただし、network コマンドで定義されたネットワーク以外のインターフェイスに対してスタティック ルートを定義する場合は、ダイナミック ルーティング プロトコルに **redistribute** スタティック コマンドを指定しない限り、ルートはアドバタイズされません。

インターフェイスがダウンすると、ダウンしたインターフェイスを経由するすべてのスタティック ルートが IP ルーティング テーブルから削除されます。転送ルータのアドレスとして指定されたアドレスへ向かう有効なネクスト ホップがスタティック ルート内に見つからない場合は、IP ルーティング テーブルからそのスタティック ルートも削除されます。

スタティック ユニキャスト ルートの設定

スタティックユニキャストルートは、特定のパスを通過して送信元と宛先間でパケットを送受信するユーザ定義のルートです。ルータが特定の宛先へのルートを構築できない場合、スタティック ルートは重要で、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

スタティック ルートを設定するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip routeprefix mask** {*address* | *interface*} [*distance*] 例： スイッチ(config)# ip route prefix mask gigabitethernet 1/0/4	スタティック ルートを確立します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip route** 例： スイッチ# show ip route	設定を確認するため、ルーティングテーブルの現在の状態を表示します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

スタティック ルートを削除するには、**no ip route***prefix mask*{*address*| *interface*} グローバル コンフィギュレーション コマンドを使用します。ユーザによって削除されるまで、スタティック ルートはスイッチに保持されます。

デフォルトのルートおよびネットワーク

デフォルトのルートおよびネットワークに関する情報

ルータは、他のすべてのネットワークへのルートを学習できません。完全なルーティング機能を実現するには、一部のルータをスマート ルータとして使用し、それ以外のルータのデフォルト ルートをスマート ルータ宛てに指定します（スマート ルータにはインターネットワーク全体のルーティング テーブルに関する情報が格納されます）。これらのデフォルト ルートは動的に学習できますが、ルータごとに設定することもできます。ほとんどのダイナミックな内部ルーティング プロトコルには、スマート ルータを使用してデフォルト情報を動的に生成し、他のルータに転送するメカニズムがあります。

指定されたデフォルト ネットワークに直接接続されたインターフェイスがルータに存在する場合は、そのデバイス上で動作するダイナミック ルーティング プロトコルによってデフォルト ルートが生成されます。RIP の場合は、疑似ネットワーク 0.0.0.0 がアドバタイズされます。

ネットワークのデフォルトを生成しているルータには、そのルータ自身のデフォルト ルートも指定する必要があります。ルータが自身のデフォルト ルートを生成する方法の 1 つは、適切なデバイスを経由してネットワーク 0.0.0.0 に至るスタティック ルートを指定することです。

ダイナミック ルーティング プロトコルによってデフォルト情報を送信するときは、特に設定する必要はありません。ルーティング テーブルは定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。IGRP ネットワークでは、システムのデフォルト ネットワークの候補が複数存在する場合もあります。Cisco ルータでは、デフォルト ルートまたは最終ゲートウェイを設定するため、アドミニストレーティブ ディスタンスおよびメトリック情報を使用します。

ダイナミックなデフォルト情報がシステムに送信されない場合は、**ip default-network** グローバル コンフィギュレーション コマンドを使用し、デフォルト ルートの候補を指定します。このネットワークが任意の送信元のルーティング テーブルに格納されている場合は、デフォルト ルートの候補としてフラグ付けされます。ルータにデフォルト ネットワークのインターフェイスが存在しなくても、そこへのパスが格納されている場合、そのネットワークは 1 つの候補と見なされ、最適なデフォルト パスへのゲートウェイが最終ゲートウェイになります。

デフォルトのルートおよびネットワークの設定方法

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip default-network***network number* 例： `スイッチ(config)# ip default-network 1`	デフォルト ネットワークを指定します。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ip route** 例： `スイッチ# show ip route`	最終ゲートウェイで選択されたデフォルト ルートを表示します。
ステップ 5	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング情報を再配信するためのルート マップ

ルート マップの概要

スイッチでは複数のルーティング プロトコルを同時に実行し、ルーティング プロトコル間で情報を再配信できます。ルーティング プロトコル間での情報の再配信は、サポートされているすべての IP ベース ルーティング プロトコルに適用されます。

2 つのドメイン間で拡張パケット フィルタまたはルート マップを定義することにより、ルーティング ドメイン間でルートの再配信を条件付きで制御することもできます。**match** および **set** ルート マップ コンフィギュレーション コマンドは、ルート マップの条件部を定義します。**match** コマンドは、条件が一致する必要があることを指定しています。**set** コマンドは、ルーティング アッ

プデートが match コマンドで定義した条件を満たす場合に行われる処理を指定します。再配信はプロトコルに依存しない機能ですが、**match** および **set** ルート マップ コンフィギュレーション コマンドの一部は特定のプロトコル固有のものです。

route-map コマンドのあとに、**match** コマンドおよび **set** コマンドをそれぞれ 1 つまたは複数指定します。**match** コマンドを指定しない場合は、すべて一致すると見なされます。**set** コマンドを指定しない場合、一致以外の処理はすべて実行されません。このため、少なくとも 1 つの **match** または **set** コマンドを指定する必要があります。

（注） **set** ルート マップ コンフィギュレーション コマンドを使用しないルート マップは、CPU に送信されるので、CPU の使用率が高くなります。

ルートマップ ステートメントは、**permit** または **deny** として識別することもできます。ステートメントが拒否としてマークされている場合、一致基準を満たすパケットは通常の転送チャネルを通じて送り返されます（宛先ベース ルーティング）、ステートメントが許可としてマークされている場合は、一致基準を満たすパケットに set コマンドが適用されます。一致基準を満たさないパケットは、通常のルーティング チャネルを通じて転送されます。

ルート マップの設定方法

次に示すステップ 3 ～ 14 はそれぞれ任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

（注） キーワードは、ルート配信を制御する手順で定義されているものと同じです。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map***map-tag* [**permit** | **deny**] [*sequence number*] 例： `スイッチ(config)# route-map rip-to-ospf permit 4`	再配信を制御するために使用するルートマップを定義し、ルートマップ コンフィギュレーション モードを開始します。 *map-tag*：ルートマップ用のわかりやすい名前を指定します。**redistribute** ルータ コンフィギュレーション コマンドはこの名前を使用して、このルートマップを参照します。複数のルート マップで同じマップ タグ名を共有できます。

	コマンドまたはアクション	目的
		（任意）**permit** が指定され、このルート マップの一致条件が満たされている場合は、set アクションの制御に従ってルートが再配信されます。**deny** が指定されている場合、ルートは再配信されません。 *sequence number*（任意）：同じ名前によってすでに設定されているルート マップのリスト内で、新しいルート マップの位置を指定する番号です。
ステップ 3	**match as-path***path-list-number* 例： `スイッチ(config-route-map)#match as-path 10`	BGP AS パス アクセス リストと照合します。
ステップ 4	**match community-list***community-list-number* [**exact**] 例： `スイッチ(config-route-map)# match community-list 150`	BGP コミュニティ リストのマッチングを行います。
ステップ 5	**match ip address** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*] 例： `スイッチ(config-route-map)# match ip address 5 80`	名前または番号を指定し、標準アクセス リストと照合します。1 ～ 199 の整数を指定できます。
ステップ 6	**match metric** metric-value 例： `スイッチ(config-route-map)# match metric 2000`	指定されたルート メトリックと一致させます。*metric-value* には、0 ～ 4294967295 の値が指定された、EIGRP のメトリックを指定できます。
ステップ 7	**match ip next-hop** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*] 例： `スイッチ(config-route-map)# match ip next-hop 8 45`	指定されたアクセス リスト（番号 1 ～ 199）のいずれかで送信される、ネクストホップのルータ アドレスと一致させます。

	コマンドまたはアクション	目的
ステップ 8	**match tag** *tag value* [*...tag-value*] 例： `スイッチ(config-route-map)# match tag 3500`	1 つまたは複数のルート タグ値からなるリスト内の指定されたタグ値と一致させます。0 ～ 4294967295 の整数を指定できます。
ステップ 9	**match interface***type number* [*...type-number*] 例： `スイッチ(config-route-map)# match interface gigabitethernet 1/0/1`	指定されたインターフェイスの 1 つから、指定されたネクスト ホップへのルートと一致させます。
ステップ 10	**match ip route-source** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*] 例： `スイッチ(config-route-map)# match ip route-source 10 30`	アドバタイズされた指定のアクセス リストによって指定したアドレスに一致します。
ステップ 11	**match route-type** {**local** | **internal** | **external** [**type-1** | **type-2**]} 例： `スイッチ(config-route-map)# match route-type local`	指定された **route-type** と一致させます。 • **local**：ローカルに生成された BGP ルート。 • **internal**：OSPF エリア内およびエリア間ルート、または EIGRP 内部ルート。 • **external**：OSPF 外部ルート（タイプ 1 またはタイプ 2）または EIGRP 外部ルート。
ステップ 12	**set dampening***halflife reuse suppress max-suppress-time* 例： `スイッチ(config-route-map)# set dampening 30 1500 10000 120`	BGP ルート ダンプニング係数を設定します。
ステップ 13	**set local-preference***value* 例： `スイッチ(config-route-map)# set local-preference 100`	ローカル BGP パスに値を割り当てます。

	コマンドまたはアクション	目的
ステップ 14	**set origin** {**igp** | **egp***as* | **incomplete**} 例： `スイッチ(config-route-map)#set origin igp`	BGP 送信元コードを設定します。
ステップ 15	**set as-path** {**tag** | **prepend***as-path-string*} 例： `スイッチ(config-route-map)# set as-path tag`	BGP の自律システム パスを変更します。
ステップ 16	**set level** {**level-1** | **level-2** | **level-1-2** | **stub-area** | **backbone**} 例： `スイッチ(config-route-map)# set level level-1-2`	ルーティング ドメインの指定エリアにアドバタイズされるルートのレベルを設定します。**stub-area** および **backbone** は、OSPF NSSA およびバックボーン エリアです。
ステップ 17	**set metric** *metric value* 例： `スイッチ(config-route-map)# set metric 100`	再配布されるルートを指定するためのメトリック値を設定します（EIGRP のみ）。*metric value* は -294967295 ～ 294967295 の整数です。
ステップ 18	**set metric***bandwidth delay reliability loading mtu* 例： `スイッチ(config-route-map)# set metric 10000 10 255 1 1500`	再配布されるルートを指定するためのメトリック値を設定します（EIGRP のみ）。 • *bandwidth*：0 ～ 4294967295 の範囲のルートのメトリック値または IGRP 帯域幅（キロビット/秒単位）。 • *delay*：0 ～ 4294967295 の範囲のルート遅延（10 マイクロ秒単位）。 • *reliability*：0 ～ 255 の数値で表されるパケット伝送の成功可能性。255 は信頼性が 100% であること、0 は信頼性がないことを意味します。 • *loading*：0 ～ 255 の数値で表されるルートの有効帯域幅（255 は 100% の負荷）。 • *mtu*：ルートの MTU の最小サイズ（バイト単位）。範囲は 0 ～ 4294967295 です。

	コマンドまたはアクション	目的
ステップ 19	**set metric-type** {**type-1** | **type-2**} 例： `スイッチ(config-route-map)# set metric-type type-2`	再配信されるルートに OSPF 外部メトリック タイプを設定します。
ステップ 20	**set metric-type internal** 例： `スイッチ(config-route-map)# set metric-type internal`	ネクスト ホップの IGP メトリックと一致するように、EBGP ネイバーにアドバタイズされるプレフィックスの Multi-Exit 識別子（MED）値を設定します。
ステップ 21	**set weight***number* 例： `スイッチ(config-route-map)# set weight 100`	ルーティング テーブルの BGP 重みを設定します。指定できる値は 1 ～ 65535 です。
ステップ 22	**end** 例： `スイッチ(config-route-map)# end`	特権 EXEC モードに戻ります。
ステップ 23	**show route-map** 例： `スイッチ# show route-map`	設定を確認するため、設定されたすべてのルートマップ、または指定されたルート マップだけを表示します。
ステップ 24	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルート配信の制御方法

次に示すステップ 3 ～ 14 はそれぞれ任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

（注） キーワードは、再配信用にルート マップを設定する手順で定義されているものと同じです。

ルーティングプロトコルのメトリックを、必ずしも別のルーティングプロトコルのメトリックに変換する必要はありません。たとえば、RIPメトリックはホップカウントで、IGRPメトリックは5つの特性の組み合わせです。このような場合は、メトリックを独自に設定し、再配信されたルートに割り当てます。ルーティング情報を制御せずにさまざまなルーティング プロトコル間で交換するとルーティング ループが発生し、ネットワーク動作が著しく低下することがあります。

メトリック変換の代わりに使用されるデフォルトの再配信メトリックが定義されていない場合は、ルーティング プロトコル間で自動的にメトリック変換が発生することがあります。

- RIPはスタティック ルートを自動的に再配信できます。スタティック ルートにはメトリック1（直接接続）が割り当てられます。
- デフォルト モードになっている場合、どのプロトコルも他のルーティング プロトコルを再配信できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ2	**router** {**rip** | **ospf** | **eigrp**} 例： `スイッチ(config)# router eigrp 10`	ルータ コンフィギュレーション モードを開始します。
ステップ3	**redistribute***protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric***metric-value*] [**metric-type***type-value*] [**match internal** | **external***type-value*] [**tag***tag-value*] [**route-map***map-tag*] [**weight***weight*] [**subnets**] 例： `スイッチ(config-router)# redistribute eigrp 1`	ルーティングプロトコル間でルートを再配信します。route-map を指定しないと、すべてのルートが再配信されます。キーワード**route-map**に*map-tag*を指定しないと、ルートは配信されません。
ステップ4	**default-metric***number* 例： `スイッチ(config-router)# default-metric 1024`	現在のルーティング プロトコルが、再配信されたすべてのルートに対して同じメトリック値を使用するように設定します（RIP、OSPF）。

	コマンドまたはアクション	目的
ステップ 5	**default-metric** bandwidth delay reliability loading mtu 例： `スイッチ(config-router)# default-metric 1000 100 250 100 1500`	EIGRP ルーティング プロトコルが、EIGRP 以外で再配信されたすべてのルートに対して同じメトリック値を使用するように設定します。
ステップ 6	**end** 例： `スイッチ(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show route-map** 例： `スイッチ# show route-map`	設定を確認するため、設定されたすべてのルートマップ、または指定されたルート マップだけを表示します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Policy-Based Routing：ポリシーベース ルーティング

ポリシーベース ルーティングの概要

PBR を使用すると、トラフィック フローに定義済みポリシーを設定できます。PBR を使用してルーティングをより細かく制御するには、ルーティング プロトコルから取得したルートの信頼度を小さくします。PBR は、次の基準に基づいて、パスを許可または拒否するルーティング ポリシーを設定したり、実装したりできます。

- 特定のエンド システムの ID
- アプリケーション
- プロトコル

PBR を使用すると、等価アクセスや送信元依存ルーティング、インタラクティブ対バッチ トラフィックに基づくルーティング、専用リンクに基づくルーティングを実現できます。たとえば、在庫記録を本社に送信する場合は高帯域で高コストのリンクを短時間使用し、電子メールなど日常的に使用するアプリケーション データは低帯域で低コストのリンクで送信できます。

PBRがイネーブルの場合は、アクセスコントロールリスト（ACL）を使用してトラフィックを分類し、各トラフィックがそれぞれ異なるパスを経由するようにします。PBR は着信パケットに適用されます。PBR がイネーブルのインターフェイスで受信されたすべてのパケットは、ルートマップを通過します。ルート マップで定義された基準に基づいて、パケットは適切なネクストホップに転送（ルーティング）されます。

- 許可とマークされているルート マップ文は次のように処理されます。
  - match コマンドは長さまたは複数の ACL で照合できます。ルート マップ文には複数の match コマンドを含めることができます。論理関数またはアルゴリズム関数は、許可または拒否の決定がされるまで、すべての match コマンドで実行されます。
    次に例を示します。

    match length A B

    match ip address acl1 acl2

    match ip address acl3

  パケットは、match length A B または acl1 または acl2 または acl3 により許可される場合に許可されます。

  - 決定が許可の場合は、setコマンドで指定されたアクションがパケットで適用されます。
  - 下された決定が拒否の場合は、PBR アクション（set コマンドで指定された）が適用されません。代わりに、処理ロジックが、シーケンス内の次のルートマップ文（シーケンス番号が次に高い文）に移動します。次の文が存在しない場合は、PBR処理が終了し、パケットがデフォルトの IP ルーティング テーブルを使用してルーティングされます。

- PBR では、拒否としてマークされているルートマップ ステートメントはサポートされません。

標準 IP ACL を使用すると、アプリケーション、プロトコル タイプ、またはエンド ステーションに基づいて一致基準を指定するように、送信元アドレスまたは拡張IP ACLの一致基準を指定できます。一致が見つかるまで、ルート マップにこのプロセスが行われます。一致が見つからない場合、通常の宛先ベース ルーティングが行われます。match ステートメント リストの末尾には、暗黙の拒否ステートメントがあります。

match 句が満たされた場合は、set 句を使用して、パス内のネクスト ホップ ルータを識別する IP アドレスを指定できます。

PBR コマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』を参照してください。

PBR の設定方法

- PBR を使用するには、スイッチまたはスタック マスター上で IP Base フィーチャ セットをイネーブルにしておく必要があります。
- マルチキャスト トラフィックには、ポリシーによるルーティングが行われません。PBR が適用されるのはユニキャスト トラフィックだけです。

- ルーテッド ポートまたは SVI 上で、PBR をイネーブルにできます。
- スイッチは一致長に基づき PBR をサポートします。
- レイヤ 3 モードの EtherChannel ポート チャネルにはポリシー ルート マップを適用できますが、EtherChannel のメンバーである物理インターフェイスには適用できません。適用しようとすると、コマンドが拒否されます。ポリシールートマップが適用されている物理インターフェイスは、EtherChannel のメンバーになることができません。
- スイッチまたはスイッチ スタックには最大 128 個の IP ポリシー ルート マップを定義できます。
- スイッチまたはスイッチ スタックには、PBR 用として最大 512 個のアクセス コントロール エントリ（ACE）を定義できます。
- ルート マップに一致基準を設定する場合は、次の注意事項に従ってください。
  - ローカル アドレス宛てのパケットを許可する ACL と照合させないでください。PBR がこれらのパケットを転送するため、ping または Telnet の失敗やルート プロトコルのフラッピングを発生させる可能性があります。
- VRF と PBR は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、VRF をイネーブルにはできません。その反対の場合も同じで、VRF がインターフェイスでイネーブルになっているときは、PBR をイネーブルにできません。
- WCCP と PBR は、スイッチ インターフェイスで相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、WCCP をイネーブルにできません。その反対の場合も同じで、WCCP がインターフェイスでイネーブルになっているときは、PBR をイネーブルにできません。
- PBR で使用されるハードウェア エントリ数は、ルート マップ自体、使用される ACL、ACL およびルート マップ エントリの順序によって異なります。
- TOS、DSCP、および IP Precedence に基づく PBR はサポートされません。
- set interface、set default next-hop、および set default interface はサポートされません。
- Cisco Catalyst リリース 15.2(4) 以前では、**ip next-hop recursive** および **ip next-hop verify availability** 機能は使用できません。next-hop は、直接接続される必要があります。
- set アクションのないポリシーマップはサポートされます。一致パケットは通常どおりにルーティングされます。
- match 句のないポリシーマップはサポートされます。set アクションはすべてのパケットに適用されます。

デフォルトでは、PBR はスイッチ上でディセーブルです。PBR をイネーブルにするには、一致基準および結果アクションを指定するルート マップを作成する必要があります。次に、特定のインターフェイスでそのルートマップ用の PBR をイネーブルにします。指定したインターフェイスに着信したパケットのうち、match 句と一致したものはすべて PBR の対象になります。

スイッチで生成されたパケットまたはローカルパケットは、通常どおりにポリシールーティングされません。スイッチ上でローカル PBR をグローバルにイネーブルにすると、そのスイッチから送信されたすべてのパケットがローカル PBR の影響を受けます。ローカル PBR は、デフォルトでディセーブルに設定されています。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map***map-tag*[**permit**] [*sequence number*] 例： `スイッチ(config)# route-map pbr-map permit`	パケットの出力場所を制御するために使用するルートマップを定義し、ルートマップのコンフィギュレーションモードを開始します。 • *map-tag*：ルート マップ用のわかりやすい名前。**ip policy route-map** インターフェイス コンフィギュレーション コマンドは、この名前を使用して、このルートマップを参照します。同じ map-tag がある複数の route-map 文は、1 つの route-map を定義します。 •（任意）**permit**：**permit** が指定され、このルートマップの一致条件が満たされている場合は、set アクションの制御に従ってルートがポリシー ルーティングされます。 •（任意）*sequence number*：シーケンス番号は、特定のルート マップ内の route-map ステートメントの位置を示します。
ステップ 3	**match ip address** {*access-list-number* | *access-list-name*} [*access-list-number* |*...access-list-name*] 例： `スイッチ(config-route-map)# match ip address 110 140`	1 つ以上の標準または拡張アクセス リストで許可されている送信元および宛先 IP アドレスを照合します。ACL は、複数の送信元および宛先 IP アドレスでも照合できます。 **match** コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。
ステップ 4	**match length min max** 例： `スイッチ(config-route-map)# match length 64 1500`	パケット長と照合します。
ステップ 5	**set ip next-hop***ip-address* [*...ip-address*] 例： `スイッチ(config-route-map)# set ip next-hop 10.1.6.2`	基準と一致するパケットの動作を指定します。パケットのルーティング先となるネクストホップを設定します（ネクストホップは隣接している必要があります）。

	コマンドまたはアクション	目的
ステップ 6	**set ip next-hop verify-availability** [*next-hop-address sequence***track***object*] 例： `スイッチ(config-route-map)# set ip next-hop verify-availability 95.1.1.2.1 track 100`	ルートマップを設定し、トラッキング対象オブジェクトの到達可能性を確認します。 トラック オブジェクトの設定については、「Configuring IP SLAs Object Tracking」 を参照してください。 （注） このコマンドは、IPv6 および VRF ではサポートされません。
ステップ 7	**exit** 例： `スイッチ(config-route-map)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するインタフェースを指定します。
ステップ 9	**ip policy route-map***map-tag* 例： `スイッチ(config-if)# ip policy route-map pbr-map`	レイヤ 3 インターフェイス上で PBR をイネーブルにし、使用するルート マップを識別します。1 つのインターフェイスに設定できるルート マップは、1 つだけです。ただし、異なるシーケンス番号を持つ複数のルートマップエントリを設定できます。これらのエントリは、最初の一致が見つかるまで、シーケンス番号順に評価されます。一致が見つからない場合、パケットは通常どおりにルーティングされます。
ステップ 10	**ip route-cache policy** 例： `スイッチ(config-if)# ip route-cache policy`	（任意）PBR の高速スイッチングをイネーブルにします。PBR の高速スイッチングをイネーブルにするには、PBR をイネーブルにする必要があります。
ステップ 11	**exit** 例： `スイッチ(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**ip local policy route-map***map-tag* 例： `スイッチ(config)# ip local policy route-map local-pbr`	（任意）ローカル PBR をイネーブルにして、スイッチから送信されるパケットに PBR を実行します。ローカル PBR は、スイッチによって生成されるパケットに適用されます。着信パケットには適用されません。
ステップ 13	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 14	**show route-map** [*map-name*] 例： スイッチ# show route-map	（任意）設定を確認するため、設定されたすべてのルートマップ、または指定されたルートマップだけを表示します。
ステップ 15	**show ip policy** 例： スイッチ# show ip policy	（任意）インターフェイスに付加されたポリシールートマップを表示します。
ステップ 16	**show ip local policy** 例： スイッチ# show ip local policy	（任意）ローカルPBRがイネーブルであるかどうか、およびイネーブルである場合は使用されているルートマップを表示します。

ルーティング情報のフィルタリング

ルーティング プロトコル情報をフィルタリングする場合は、以下の作業を実行します。

（注） OSPF プロセス間でルートが再配信される場合、OSPF メトリックは保持されません。

受動インターフェイスの設定

ローカル ネットワーク上の他のルータが動的にルートを取得しないようにするには、**passive-interface** ルータ コンフィギュレーション コマンドを使用し、ルーティング アップデート メッセージがルータ インターフェイスから送信されないようにします。OSPF プロトコルでこのコマンドを使用すると、パッシブに指定したインターフェイス アドレスが OSPF ドメインのスタブ ネットワークとして表示されます。OSPFルーティング情報は、指定されたルータ インターフェイスから送受信されません。

多数のインターフェイスが存在するネットワークで、インターフェイスを手動でパッシブに設定する作業を回避するには、**passive-interface default** ルータ コンフィギュレーション コマンドを使用し、すべてのインターフェイスをデフォルトでパッシブになるように設定します。このあとで、隣接関係が必要なインターフェイスを手動で設定します。

パッシブとしてイネーブルにしたインターフェイスを確認するには、**show ip ospf interface** などのネットワーク モニタリング用特権 EXEC コマンドを使用します。アクティブとしてイネーブルにしたインターフェイスを確認するには、**show ip interface** 特権 EXEC コマンドを使用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**rip** | **ospf** | **eigrp**} 例： `スイッチ(config)# router ospf`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**passive-interface***interface-id* 例： `スイッチ(config-router)# passive-interface gigabitethernet 1/0/1`	指定されたレイヤ 3 インターフェイス経由のルーティング アップデートの送信を抑制します。
ステップ 4	**passive-interface default** 例： `スイッチ(config-router)# passive-interface default`	（任意）すべてのインターフェイスを、デフォルトでパッシブとなるように設定します。
ステップ 5	**no passive-interface***interface type* 例： `スイッチ(config-router)# no passive-interface gigabitethernet1/0/3 gigabitethernet 1/0/5`	（任意）隣接関係を送信する必要があるインターフェイスだけをアクティブにします。
ステップ 6	**network***network-address* 例： `スイッチ(config-router)# network 10.1.1.1`	（任意）ルーティング プロセス用のネットワーク リストを指定します。*network-address* は IP アドレスです。
ステップ 7	**end** 例： `スイッチ(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング アップデートのアドバタイズおよび処理の制御

アクセス コントロール リストと **distribute-list** ルータ コンフィギュレーション コマンドを組み合わせて使用すると、ルーティング アップデート中にルートのアドバタイズを抑制し、他のルータが 1 つまたは複数のルートを取得しないようにできます。この機能を OSPF で使用した場合は外部ルートにだけ適用されるため、インターフェイス名を指定できません。

distribute-list ルータ コンフィギュレーション コマンドを使用し、着信したアップデートのリストのうち特定のルートを処理しないようにすることもできます。（OSPF にこの機能は適用されません）。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**rip** | **eigrp**} 例： `スイッチ(config)# router eigrp 10`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**distribute-list** {*access-list-number* | *access-list-name*} **out** [*interface-name* | *routing process* | *autonomous-system-number*] 例： `スイッチ(config-router)# distribute 120 out gigabitethernet 1/0/7`	アクセスリスト内のアクションに応じて、ルーティングアップデート内のルートのアドバタイズを許可または拒否します。
ステップ 4	**distribute-list** {*access-list-number* | *access-list-name*} **in** [*type-number*] 例： `スイッチ(config-router)# distribute-list 125 in`	アップデートにリストされたルートの処理を抑制します。
ステップ 5	**end** 例： `スイッチ(config-router)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング情報の送信元のフィルタリング

一部のルーティング情報が他の情報よりも正確な場合があるため、フィルタリングを使用して、さまざまな送信元から送られる情報にプライオリティを設定できます。「アドミニストレーティブ ディスタンス」は、ルータやルータのグループなど、ルーティング情報の送信元の信頼性を示す数値です。大規模ネットワークでは、他のルーティング プロトコルよりも信頼できるルーティング プロトコルが存在する場合があります。アドミニストレーティブ ディスタンスの値を指定すると、ルータはルーティング情報の送信元をインテリジェントに区別できるようになります。常にルーティング プロトコルのアドミニストレーティブ ディスタンスが最短（値が最小）であるルートが選択されます。

各ネットワークには独自の要件があるため、アドミニストレーティブ ディスタンスを割り当てる一般的な注意事項はありません。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**rip** | **ospf** | **eigrp**} 例： `スイッチ(config)# router eigrp 10`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**distance***weight*{*ip-address* {*ip-address mask*}} [*ip access list*] 例： `スイッチ(config-router)# distance 50 10.1.5.1`	アドミニストレーティブ ディスタンスを定義します。 *weight*：アドミニストレーティブ ディスタンスは 10 ～ 255 の整数です。単独で使用した場合、*weight* はデフォルトのアドミニストレーティブ ディスタンスを指定します。ルーティング情報の送信元に他の指定がない場合に使用されます。アドミニストレーティブ ディスタンスが 255 のルートはルーティング テーブルに格納されません。

	コマンドまたはアクション	目的
		（任意）*ip access list*：着信ルーティング アップデートに適用される IP 標準または IP 拡張アクセス リストです。
ステップ 4	**end** 例： `スイッチ(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols** 例： `スイッチ# show ip protocols`	指定されたルーティング プロセス用のデフォルトのアドミニストレーティブ ディスタンスを表示します。
ステップ 6	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

認証キーの管理

キー管理を使用すると、ルーティング プロトコルで使用される認証キーを制御できます。一部のプロトコルでは、キー管理を使用できません。認証キーは EIGRP および RIP バージョン 2 で使用できます。

前提条件

認証キーを管理する前に、認証をイネーブルにする必要があります。プロトコルに対して認証をイネーブルにする方法については、該当するプロトコルについての説明を参照してください。認証キーを管理するには、キー チェーンを定義してそのキー チェーンに属するキーを識別し、各キーの有効期間を指定します。各キーには、ローカルにストアされる独自のキー ID（**key** *number* キー チェーン コンフィギュレーション コマンドで指定）があります。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5（MD5）認証キーが一意に識別されます。

認証キーの設定方法

有効期間が指定された複数のキーを設定できます。存在する有効なキーの数にかかわらず、送信される認証パケットは 1 つだけです。最小の番号から順にキー番号が調べられ、最初に見つかった有効なキーが使用されます。キー変更中は、有効期間が重なっても問題ありません。これらの有効期間は、ルータに通知する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**key chain***name-of-chain* 例： `スイッチ(config)# key chain key10`	キー チェーンを識別し、キーチェーン コンフィギュレーション モードを開始します。
ステップ 3	**key***number* 例： `スイッチ(config-keychain)# key 2000`	キー番号を識別します。指定できる範囲は 0 ～ 2147483647 です。
ステップ 4	**key-string***text* 例： `スイッチ(config-keychain)# Room 20, 10th floor`	キー ストリングを確認します。ストリングには 1 ～ 80 文字の大文字および小文字の英数字を指定できますが、最初の文字に数字を指定できません。
ステップ 5	**accept-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*} 例： `スイッチ(config-keychain)# accept-lifetime 12:30:00 Jan 25 1009 infinite`	（任意）キーを受信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 6	**send-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*} 例： `スイッチ(config-keychain)# accept-lifetime 23:30:00 Jan 25 1019 infinite`	（任意）キーを送信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 7	**end** 例： `スイッチ(config-keychain)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show key chain** 例： `スイッチ# show key chain`	認証キーの情報を表示します。
ステップ 9	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ネットワークのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定の統計情報を表示することもできます。

表 *89*：*IP* ルートの削除またはルート ステータスの表示を行うコマンド

clear ip route {*network* [*mask* | ***]}	1 つまたは複数のルートを IP ルーティング テーブルから消去します。
show ip protocols	アクティブなルーティング プロトコル プロセスのパラメータおよびステートを表示します。
show ip route [*address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]]	ルーティング テーブルの現在の状態を表示します。
show ip route summary	サマリー形式でルーティングテーブルの現在のステータスを表示します。
show ip route supernets-only	スーパーネットを表示します。
show ip cache	IP トラフィックのスイッチングに使用されるルーティング テーブルを表示します。
show route-map [*map-name*]	設定されたすべてのルート マップ、または指定した 1 つのルート マップだけを表示します。

第 XII 部

セキュリティ

- 不正アクセスの防止，1291 ページ
- パスワードおよび権限レベルによるスイッチ アクセスの制御，1293 ページ
- TACACS+ の設定，1315 ページ
- RADIUS の設定，1333 ページ
- Kerberos の設定，1387 ページ
- ローカル認証および許可の設定，1395 ページ
- セキュア シェル（SSH）の設定，1401 ページ
- SSH 認証の X.509v3 証明書，1413 ページ
- Secure Socket Layer HTTP の設定，1423 ページ
- IPv4 ACL の設定，1437 ページ
- IPv6 ACL の設定，1497 ページ
- DHCP の設定，1509 ページ
- IP ソース ガードの設定，1537 ページ
- ダイナミック ARP インスペクションの設定，1547 ページ
- IEEE 802.1x ポートベースの認証の設定，1569 ページ
- Web ベース認証の設定，1673 ページ

- ポート単位のトラフィック制御の設定，1705 ページ
- IPv6 ファースト ホップ セキュリティの設定，1751 ページ
- Cisco TrustSec の設定，1801 ページ
- ワイヤレス ゲスト アクセスの設定，1807 ページ
- 不正なデバイスの管理，1835 ページ
- 不正なアクセス ポイントの分類，1847 ページ
- wIPS の設定，1863 ページ
- 侵入検知システムの設定，1875 ページ

第 55 章

不正アクセスの防止

- 機能情報の確認，1291 ページ
- 不正アクセスの防止，1291 ページ

機能情報の確認

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

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

不正アクセスの防止

不正ユーザによる、スイッチの再設定や設定情報の閲覧を防止できます。一般的には、ネットワーク管理者からスイッチへのアクセスを許可する一方、非同期ポートを用いてネットワーク外からダイヤルアップ接続するユーザや、シリアル ポートを通じてネットワーク外から接続するユーザ、またはローカル ネットワーク内の端末またはワークステーションから接続するユーザによるアクセスを制限します。

スイッチへの不正アクセスを防止するには、次のセキュリティ機能を 1 つまたは複数設定します。

- 最低限のセキュリティとして、各スイッチポートでパスワードおよび権限を設定します。このパスワードは、スイッチにローカルに保存されます。ユーザがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。

- 追加のセキュリティ レイヤとして、ユーザ名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。
- ユーザ名とパスワードのペアを使用したいが、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティ サーバ上のデータベースに保存できます。これにより、複数のネットワーキング デバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。
- また、失敗したログイン試行をログに記録するログイン拡張機能もイネーブルにすることもできます。ログイン拡張は、設定した回数のログインが失敗したあとに、それ以降のログイン試行をブロックするために設定することもできます。詳細については、『Cisco IOS Login Enhancements』マニュアルを参照してください。

関連トピック

ユーザ名とパスワードのペアの設定, （1304 ページ）
TACACS+ およびスイッチ アクセス, （1317 ページ）
端末回線に対する Telnet パスワードの設定, （1302 ページ）

第 56 章

パスワードおよび権限レベルによるスイッチ アクセスの制御

- 機能情報の確認，1293 ページ
- パスワードおよび権限によるスイッチ アクセスの制御の制約事項，1293 ページ
- パスワードおよび権限レベルに関する情報，1294 ページ
- パスワードおよび権限レベルでスイッチ アクセスを制御する方法，1297 ページ
- スイッチ アクセスのモニタリング，1311 ページ
- パスワードおよび権限レベルの設定例，1311 ページ
- その他の参考資料，1312 ページ

機能情報の確認

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

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

パスワードおよび権限によるスイッチ アクセスの制御の制約事項

パスワードおよび権限によるスイッチ アクセスの制御の制約事項は、次のとおりです。

- パスワード回復のディセーブル化は、**boot manual** グローバル コンフィギュレーション コマンドを使用して手動でブートするようにスイッチを設定している場合は無効です。このコマンドは、スイッチの電源の再投入後、ブートローダ プロンプト（*switch:*）を表示させます。

関連トピック

パスワード回復のディセーブル化，（1301 ページ）
パスワードの回復，（1295 ページ）

パスワードおよび権限レベルに関する情報

デフォルトのパスワードおよび権限レベル設定

ネットワークで端末のアクセス コントロールを行う簡単な方法は、パスワードを使用して権限レベルを割り当てることです。パスワード保護によって、ネットワークまたはネットワーク デバイスへのアクセスが制限されます。権限レベルによって、ネットワーク デバイスにログイン後、ユーザがどのようなコマンドを使用できるかが定義されます。

次の表に、デフォルトのパスワードおよび権限レベル設定を示します。

表 *90*：デフォルトのパスワードおよび権限レベル設定

機能	デフォルト設定
イネーブル パスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です（特権 EXEC レベル）。パスワードは、コンフィギュレーション ファイル内では暗号化されていない状態です。
イネーブル シークレット パスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です（特権 EXEC レベル）。パスワードは、暗号化されてからコンフィギュレーション ファイルに書き込まれます。
回線パスワード	パスワードは定義されていません。

追加のパスワード セキュリティ

追加のセキュリティ レイヤを、特にネットワークを越えるパスワードやTrivial File Transfer Protocol（TFTP）サーバに保存されているパスワードに対して設定する場合には、**enable password** または **enable secret** グローバル コンフィギュレーション コマンドを使用できます。コマンドの作用はどちらも同じです。このコマンドにより、暗号化されたパスワードを設定できます。特権EXECモード（デフォルト設定）または特定の権限レベルにアクセスするユーザは、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムが使用されるので、**enable secret** コマンドを使用することを推奨します。

enable secret コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

パスワードの暗号化をイネーブルにすると、ユーザ名パスワード、認証キー パスワード、イネーブル コマンド パスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

関連トピック

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護, （1299 ページ）
例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護, （1311 ページ）

パスワードの回復

スイッチに物理的にアクセスできるエンド ユーザは、デフォルトで、スイッチの電源投入時にブート プロセスに割り込み、新しいパスワードを入力することによって、失われたパスワードを回復できます。

パスワード回復ディセーブル化機能では、この機能の一部をディセーブルにすることによりスイッチのパスワードへのアクセスを保護できます。この機能がイネーブルの場合、エンド ユーザは、システムをデフォルト設定に戻すことに同意した場合に限り、ブート プロセスに割り込むことができます。パスワード回復をディセーブルにしても、ブート プロセスに割り込んでパスワードを変更できますが、コンフィギュレーション ファイル（config.text）および VLAN データベース ファイル（vlan.dat）は削除されます。

パスワード回復をディセーブルにする場合は、エンドユーザがブートプロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。VTP（VLAN トランキング プロトコル）トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

パスワードの回復を再びイネーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

パスワード回復のディセーブル化, （1301 ページ）
パスワードおよび権限によるスイッチ アクセスの制御の制約事項, （1293 ページ）

端末回線の Telnet 設定

初めてスイッチに電源を投入すると、自動セットアップ プログラムが起動して IP 情報を割り当て、この後続けて使用できるようにデフォルト設定を作成します。さらに、セットアップ プログラムは、パスワードによるTelnetアクセス用にスイッチを設定することを要求します。セットアップ プログラムの実行中にこのパスワードを設定しなかった場合は、端末回線に対する Telnet パスワードを設定するときに設定できます。

関連トピック

端末回線に対する Telnet パスワードの設定, （1302 ページ）
例：端末回線に対する Telnet パスワードの設定, （1311 ページ）

ユーザ名とパスワードのペア

ユーザ名とパスワードのペアを設定できます。このペアはスイッチ上でローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

関連トピック

ユーザ名とパスワードのペアの設定, （1304 ページ）

権限レベル

Cisco スイッチ（および他のデバイス）では、権限レベルを使用して、スイッチ動作の異なるレベルに対してパスワードセキュリティを提供します。デフォルトでは、Cisco IOS ソフトウェアは、パスワードセキュリティの2つのモード（権限レベル）で動作します。ユーザ EXEC（レベル1）および特権 EXEC（レベル 15）です。各モードに、最大 16 個の階層レベルからなるコマンドを設定できます。複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

回線の権限レベル

ユーザは、回線にログインし、別の権限レベルをイネーブルに設定することにより、**privilege level** ラインコンフィギュレーションコマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっていれば、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

たとえば、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 のセキュリティを割り当て、レベル 2 のパスワードを広範囲のユーザに配布できます。また、**configure** コマンドへのアクセス制限を強化する場合は、レベル 3 のセキュリティを割り当て、そのパスワードを限られたユーザ グループに配布することもできます。

コマンド権限レベル

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。たとえば、**show ip traffic** コマンドをレベル 15 に設定すると、**show** コマンドおよび **show ip** コマンドは、それぞれ別のレベルに設定しない限り、自動的にレベル 15 に設定されます。

関連トピック

コマンドの特権レベルの設定，（1307 ページ）
例：コマンドの権限レベルの設定，（1312 ページ）
回線のデフォルト特権レベルの変更，（1308 ページ）
権限レベルへのログインおよび終了，（1310 ページ）

パスワードおよび権限レベルでスイッチ アクセスを制御する方法

スタティック イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。スタティック イネーブル パスワードを設定または変更するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **enable password***password*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**enable password***password* 例： スイッチ(config)# **enable password secret321**	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 デフォルトでは、パスワードは定義されません。 *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符（?）は、パスワードを作成する場合に、疑問符の前に Ctrl+v を入力すれば使用できます。たとえば、パスワード abc?123 を作成するときは、次のようにします。 **1** **abc** を入力します。 **2** Ctrl+v を入力します。 **3** **?123** を入力します。 システムからイネーブルパスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：スタティック イネーブル パスワードの設定または変更, （1311 ページ）

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

特権 EXEC モード（デフォルト）または指定された特権レベルにアクセスするためにユーザが入力する必要がある暗号化パスワードを確立するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. 次のいずれかを使用します。
   - **enable password**[**level***level*] {*password*| *encryption-type encrypted-password*}
   - **enable secret**[**level***level*] {*password*| *encryption-type encrypted-password*}
4. **service password-encryption**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **enable password**[**level***level*] {*password*| *encryption-type encrypted-password*} • **enable secret**[**level***level*] {*password*| *encryption-type encrypted-password*}	• 特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 • シークレット パスワードを定義します。これは非可逆的な暗号化方式を使用して保存されます。 ◦（任意）*level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です（特権 EXEC モード権限）。

	コマンドまたはアクション	目的
	例： スイッチ(config)# **enable password example102** または スイッチ(config)# **enable secret level 1 password secret123sample**	◦ *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。 ◦（任意）*encryption-type* には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか使用できません。暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、別のスイッチの設定からコピーします。 （注） 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。
ステップ 4	**service password-encryption** 例： スイッチ(config)# **service password-encryption**	（任意）パスワードの定義時または設定の書き込み時に、パスワードを暗号化します。 暗号化を行うと、コンフィギュレーションファイル内でパスワードが読み取り可能な形式になるのを防止できます。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

追加のパスワード セキュリティ，（1294 ページ）

例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護，（1311 ページ）

パスワード回復のディセーブル化

パスワードの回復をディセーブルにしてスイッチのセキュリティを保護するには、次の手順を実行します。

はじめる前に

パスワード回復をディセーブルにする場合は、エンドユーザがブートプロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。VTP（VLAN トランキング プロトコル）トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

手順の概要

1. **enable**
2. **configureterminal**
3. **no service password-recovery**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**no service password-recovery** 例： スイッチ(config)# **no service password-recovery**	パスワード回復をディセーブルにします。 この設定は、フラッシュ メモリの中で、ブートローダおよび Cisco IOS イメージがアクセスできる領域に保存されますが、ファイル システムには含まれません。また、ユーザがアクセスすることはできません。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

パスワードの回復を再びイネーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

パスワードの回復，（1295 ページ）

パスワードおよび権限によるスイッチ アクセスの制御の制約事項，（1293 ページ）

端末回線に対する Telnet パスワードの設定

接続された端末回線に対する Telnet パスワードを設定するには、ユーザ EXEC モードで次の手順を実行します。

はじめる前に

- エミュレーション ソフトウェアを備えた PC またはワークステーションをスイッチ コンソール ポートに接続するか、または PC をイーサネット管理ポートに接続します。

- コンソール ポートのデフォルトのデータ特性は、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなしです。コマンドラインプロンプトが表示されるまで、Return キーを何回か押す必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **line vty 0 15**
4. **password***password*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	（注） パスワードが特権EXECモードへのアクセスに必要な場合は、その入力が求められます。 特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line vty 0 15** 例： スイッチ(config)# **line vty 0 15**	Telnetセッション（回線）の数を設定し、ライン コンフィギュレーション モードを開始します。 コマンド対応スイッチでは、最大 16 のセッションが可能です。0 および 15 を指定すると、使用できる 16 の Telnet セッションすべてを設定することになります。
ステップ 4	**password***password* 例： スイッチ(config-line)# **password abcxyz543**	1 つまたは複数の回線に対応する Telnet パスワードを設定します。 *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config-line)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

パスワードおよび権限レベルに関する情報
不正アクセスの防止，（1291 ページ）
端末回線の Telnet 設定，（1296 ページ）
例：端末回線に対する Telnet パスワードの設定，（1311 ページ）

ユーザ名とパスワードのペアの設定

ユーザ名とパスワードのペアを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **username***name* [**privilege***level*] {**password***encryption-typepassword*}
4. 次のいずれかを使用します。
   - **line console 0**
   - **line vty 0 15**
5. **login local**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**username***name* [**privilege***level*] {**password***encryption-typepassword*} 例： スイッチ(config)# **username adamsample privilege 1 password secret456** スイッチ(config)# **username 111111111111 mac attribute**	各ユーザのユーザ名、権限レベル、パスワードを設定します。 • *name* には、ユーザ ID を 1 ワードで指定するか、または MAC アドレスを指定します。スペースと引用符は使用できません。 • ユーザ名と MAC フィルタの両方に対し、最大 12000 のクライアントを個別に設定できます。 • （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は0～15です。レベル15では特権EXECモードでのアクセスが可能です。レベル1では、ユーザEXECモードでのアクセスとなります。

	コマンドまたはアクション	目的
		• *encryption-type* には、暗号化されていないパスワードが後ろに続く場合は0を入力します。暗号化されたパスワードが後ろに続く場合は 7 を指定します。 • *password* には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。

ステップ 4	次のいずれかを使用します。
	• **line console 0**
	• **line vty 0 15**
	例：
	`スイッチ(config)# line console 0`
	または
	`スイッチ(config)# line vty 15`
		ライン コンフィギュレーション モードを開始し、コンソール ポート（回線 0）または VTY 回線（回線 0 ～ 15）を設定します。

ステップ 5	**login local** 例： `スイッチ(config-line)# login local`	ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 3 で指定されたユーザ名に基づきます。
ステップ 6	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

パスワードおよび権限レベルに関する情報
不正アクセスの防止，（1291 ページ）
ユーザ名とパスワードのペア，（1296 ページ）

コマンドの特権レベルの設定

コマンドの権限レベルを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **privilege***mode***level***levelcommand*
4. **enable password level***levelpassword*
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**privilege***mode***level***levelcommand* 例： `スイッチ(config)# privilege exec level 14 configure`	コマンドの特権レベルを設定します。 • *mode* には、グローバル コンフィギュレーション モードの場合は **configure** を、EXEC モードの場合は **exec** を、インターフェイス コンフィギュレーション モードの場合は **interface** を、ライン コンフィギュレーション モードの場合は **line** をそれぞれ入力します。 • *level* の範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。

	コマンドまたはアクション	目的
		• *command* には、アクセスを制限したいコマンドを指定します。
ステップ 4	**enable password level***levelpassword* 例： スイッチ(config)# **enable password level 14 SecretPswd14**	権限レベルをイネーブルにするためのパスワードを指定します。 • *level* の範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。 • *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

権限レベル，（1296 ページ）
例：コマンドの権限レベルの設定，（1312 ページ）

回線のデフォルト特権レベルの変更

指定した回線のデフォルトの権限レベルを変更するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **line vty***line*
4. **privilege level***level*
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line vty***line* 例： `スイッチ(config)# line vty 10`	アクセスを制限する仮想端末回線を選択します。
ステップ 4	**privilege level***level* 例： `スイッチ(config)# privilege level 15`	回線のデフォルト特権レベルを変更します。 *level* の範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `スイッチ# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

次の作業

ユーザは、回線にログインし、別の権限レベルをイネーブルに設定することにより、**privilege level** ラインコンフィギュレーションコマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっていれば、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

関連トピック

権限レベル，（1296 ページ）

権限レベルへのログインおよび終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、ユーザ EXEC モードで次の手順を実行します。

手順の概要

1. **enable***level*
2. **disable***level*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable***level* 例： `スイッチ> enable 15`	指定された特権レベルにログインします。 この例で、レベル 15 は特権 EXEC モードです。 *level* に指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable***level* 例： `スイッチ# disable 1`	指定した特権レベルを終了します。 この例で、レベル 1 はユーザ EXEC モードです。 *level* に指定できる範囲は 0 ～ 15 です。

関連トピック

権限レベル，（1296 ページ）

スイッチ アクセスのモニタリング

表 *91*：*DHCP* 情報を表示するためのコマンド

show privilege	権限レベルの設定を表示します。

パスワードおよび権限レベルの設定例

例：スタティック イネーブル パスワードの設定または変更

次に、イネーブル パスワードを*l1u2c3k4y5* に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モード アクセス）。

```
スイッチ(config)# enable password l1u2c3k4y5
```

関連トピック

スタティック イネーブル パスワードの設定または変更，（1297 ページ）

例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

次に、権限レベル 2 に対して暗号化パスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

```
スイッチ(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

関連トピック

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護，（1299 ページ）
追加のパスワード セキュリティ，（1294 ページ）

例：端末回線に対する Telnet パスワードの設定

次に、Telnet パスワードを *let45me67in89* に設定する例を示します。

```
スイッチ(config)# line vty 10
スイッチ(config-line)# password let45me67in89
```

関連トピック

端末回線に対する Telnet パスワードの設定，（1302 ページ）
端末回線の Telnet 設定，（1296 ページ）

例：コマンドの権限レベルの設定

configure コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして *SecretPswd14* を定義する例を示します。

```
スイッチ(config)# privilege exec level 14 configure
スイッチ(config)# enable password level 14 SecretPswd14
```

関連トピック

コマンドの特権レベルの設定，（1307 ページ）
権限レベル，（1296 ページ）

その他の参考資料

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

第 57 章

TACACS+ の設定

- 機能情報の確認，1315 ページ
- TACACS+ の前提条件，1315 ページ
- TACACS+ の概要，1317 ページ
- TACACS+ を設定する方法，1322 ページ
- TACACS+ のモニタリング，1331 ページ

機能情報の確認

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

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

TACACS+ の前提条件

TACACS+ によるスイッチ アクセスのセット アップと設定の前提条件は、次のとおりです（示されている順序で実行する必要があります）。

1. スイッチに TACACS+ サーバ アドレスとスイッチを設定します。
2. 認証キーを設定します。
3. TACACS+ サーバでステップ 2 からキーを設定します。
4. 認証、許可、アカウンティング（AAA）をイネーブルにする。

5 ログイン認証方式リストを作成します。

6 端末回線にリストを適用します。

7 認証およびアカウンティング方式のリストを作成します。

TACACS+ によるスイッチ アクセスの制御の前提条件は、次のとおりです。

- スイッチ上で TACACS+ 機能を設定するには、設定済みの TACACS+ サーバにアクセスする必要があります。また、通常 LINUX または Windows ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されている TACACS+ サービスにもアクセスする必要があります。
- スイッチ スタックと TACACS+ サーバとの間に冗長接続を設定することを推奨します。これによって、接続済みのスタック メンバの 1 つがスイッチ スタックから削除された場合でも、TACACS+ サーバにアクセスできます。
- スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼働するシステムが必要です。
- TACACS+ を使用するには、それをイネーブルにする必要があります。
- 許可は、使用するスイッチでイネーブルにする必要があります。
- ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
- この項または他の項で示す AAA コマンドを使用するには、まず **aaa new-model** コマンドを使用して AAA をイネーブルにする必要があります。
- 最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウンティングの方式リストを定義できます。
- 方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。
- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。

関連トピック

TACACS+ の概要, （1317 ページ）
TACACS+ の動作, （1319 ページ）
TACACS+ を設定する方法, （1322 ページ）
方式リスト, （1320 ページ）
TACACS+ ログイン認証の設定, （1324 ページ）

TACACS+ ログイン認証，（1320 ページ）
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定，（1327 ページ）
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可，（1321 ページ）

TACACS+ の概要

TACACS+ およびスイッチ アクセス

ここでは、TACACS+ について説明します。TACACS+ は詳細なアカウンティング情報を提供し、認証と許可のプロセスを柔軟に管理します。TACACS+は、認証、許可、アカウンティング（AAA）機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用する必要があります。

関連トピック

パスワードおよび権限レベルに関する情報
不正アクセスの防止，（1291 ページ）
スイッチのローカル認証および許可の設定，（1395 ページ）
SSH サーバ、統合クライアント、およびサポートされているバージョン，（1403 ページ）

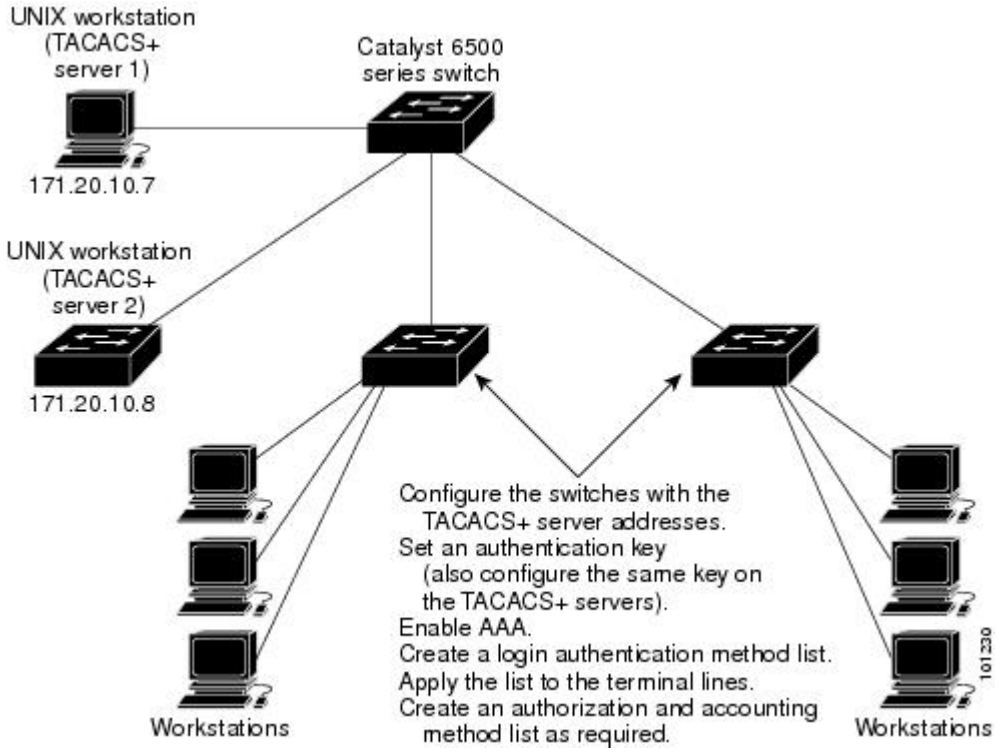
TACACS+ の概要

TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）が各サービス（認証、許可、およびアカウンティング）を別個に提供します。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ の目的は、1 つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他の Cisco ルータやアクセス サーバとともにネットワーク アクセス サーバにできます。

図 *64*：一般的な *TACACS+* ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージ サポートによって認証の完全制御を行います。

  認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードが入力された後、自宅の住所、母親の旧姓、サービス タイプ、社会保険番号などのいくつかの質問をすることによりユーザを試します）。TACACS+ 認証サービスは、ユーザ画面にメッセージを送信することもできます。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。

- 許可：autocommand、アクセス コントロール、セッション期間、プロトコル サポートの設定といった、ユーザセッション時のユーザ機能についてきめ細かく制御します。また、TACACS+ 許可機能によって、ユーザが実行できるコマンドを制限することもできます。

- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供した

りできます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

関連トピック

TACACS+ の前提条件, （1315 ページ）

TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これをユーザに表示します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワード プロンプトを取得します。スイッチによってパスワード プロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

2 スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。

- ACCEPT：ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
- REJECT：ユーザは認証されません。TACACS+ デーモンに応じて、ユーザはアクセスを拒否されるか、ログイン シーケンスを再試行するように求められます。
- ERROR：デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
- CONTINUE：ユーザは、さらに認証情報の入力を求められます。

認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3 TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛ての属性の形式でデータが含まれています。

- Telnet、セキュア シェル（SSH）、rlogin、または特権 EXEC サービス

- 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

関連トピック

TACACS+ の前提条件, （1315 ページ）

方式リスト

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティ プロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

関連トピック

TACACS+ を設定する方法, （1322 ページ）
TACACS+ の前提条件, （1315 ページ）

TACACS+ 設定オプション

認証用に 1 つのサーバを使用することも、また、既存のサーバ ホストをグループ化するために AAA サーバ グループを使用するように設定することもできます。サーバをグループ化して設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバ グループは、グローバル サーバ ホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストが含まれています。

関連トピック

TACACS+ サーバ ホストの指定および認証キーの設定, （1322 ページ）

TACACS+ ログイン認証

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

関連トピック

TACACS+ ログイン認証の設定, （1324 ページ）
TACACS+ の前提条件, （1315 ページ）

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザデータベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

関連トピック

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定, （1327 ページ）
TACACS+ の前提条件, （1315 ページ）

TACACS+ アカウンティング

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

関連トピック

TACACS+ アカウンティングの起動, （1328 ページ）

TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

（注） TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

TACACS+ を設定する方法

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。

関連トピック

方式リスト, （1320 ページ）

TACACS+ の前提条件, （1315 ページ）

TACACS+ サーバ ホストの指定および認証キーの設定

TACACS+ サーバ ホストを特定し、認証キーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **tacacs-server host***hostname*
4. **aaa new-model**
5. **aaa group server tacacs+***group-name*
6. **server***ip-address*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**tacacs-server host***hostname* 例： スイッチ(config)# **tacacs-server host yourserver**	TACACS+ サーバを維持する IP ホストを特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 *hostname* には、ホストの名前または IP アドレスを指定します。
ステップ 4	**aaa new-model** 例： スイッチ(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 5	**aaa group server tacacs+***group-name* 例： スイッチ(config)# **aaa group server tacacs+ your_server_group**	（任意）グループ名で AAA サーバグループを定義します。 このコマンドによって、スイッチはサーバ グループ サブコンフィギュレーション モードになります。
ステップ 6	**server***ip-address* 例： スイッチ(config)# **server 10.1.2.3**	（任意）特定の TACACS+ サーバを定義済みサーバ グループに関連付けます。AAA サーバ グループの TACACS+ サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 3 で定義済みのものでなければなりません。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

TACACS+ 設定オプション，（1320 ページ）

TACACS+ ログイン認証の設定

TACACS+ ログイン認証を設定するには、次の手順を実行します。

はじめる前に

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。

（注） AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ip http authentication コマンドの詳細については、『*Cisco IOS Security Command Reference, Release 12.4*』を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
5. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
6. **login authentication** {**default** | *list-name*}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： スイッチ(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： スイッチ(config)# **aaa authentication login default tacacs+ local**	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • *enable*：イネーブルパスワードを認証に使用します。この認証方式を使用するには、あらかじめ **enable***password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 • *group tacacs+*：TACACS+ 認証を使用します。この認証方式を使用するには、あらかじめ TACACS+ サーバを設定しておく必要があります。詳細については、TACACS+ サーバ ホストの指定および認証キーの設定，（1322 ページ）を参照してください。 • *line*：回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。**password***password* ライン コンフィギュレーション コマンドを使用します。 • *local*：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。

	コマンドまたはアクション	目的
		username*password* グローバル コンフィギュレーション コマンドを使用します。 • *local-case*：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username***name* **password** グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 • *none*：ログインに認証を使用しません。
ステップ 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `スイッチ(config)# line 2 4`	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 6	**login authentication** {**default** | *list-name*} 例： `スイッチ(config-line)# login authentication default`	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 7	**end** 例： `スイッチ(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

TACACS+ ログイン認証, （1320 ページ）
TACACS+ の前提条件, （1315 ページ）

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

aaa authorization グローバル コンフィギュレーション コマンドと **tacacs+** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa authorization network tacacs+**
4. **aaa authorization exec tacacs+**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**aaa authorization network tacacs+** 例： スイッチ(config)# **aaa authorization network tacacs+**	ネットワーク関連のすべてのサービス要求に対してユーザ TACACS+ 認可を行うことを設定します。
ステップ 4	**aaa authorization exec tacacs+** 例： スイッチ(config)# **aaa authorization exec tacacs+**	ユーザの特権 EXEC アクセスに対してユーザ TACACS+ 認可を行うことを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可, （1321 ページ）

TACACS+ の前提条件, （1315 ページ）

TACACS+ アカウンティングの起動

TACACS+ アカウンティングを開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa accounting network start-stop tacacs+**
4. **aaa accounting exec start-stop tacacs+**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting network start-stop tacacs+** 例： スイッチ(config)# **aaa accounting network start-stop tacacs+**	ネットワーク関連のすべてのサービス要求について、TACACS+ アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting exec start-stop tacacs+** 例： スイッチ(config)# **aaa accounting exec start-stop tacacs+**	TACACS+ アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

関連トピック

TACACS+ アカウンティング，（1321 ページ）

AAA サーバが到達不能な場合のルータとのセッションの確立

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

TACACS+ のモニタリング

表 *92* : *TACACS+* 情報を表示するためのコマンド

コマンド	目的
show tacacs	TACACS+ サーバの統計情報を表示します。

第 58 章

RADIUS の設定

- 機能情報の確認，1333 ページ
- RADIUS を設定するための前提条件，1333 ページ
- RADIUS の設定に関する制約事項，1334 ページ
- RADIUS に関する情報，1335 ページ
- RADIUS の設定方法，1365 ページ
- CoA 機能のモニタリング，1384 ページ
- その他の参考資料，1385 ページ

機能情報の確認

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

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

RADIUS を設定するための前提条件

ここでは、RADIUS によるスイッチ アクセスの制御の前提条件を示します。

一般:

- この章のいずれかのコンフィギュレーション コマンドを使用するには、RADIUS および認証、許可、ならびにアカウンティング（AAA）をイネーブルにする必要があります。

- RADIUS は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。
- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。
- 最低限、RADIUS サーバ ソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS 認証の方式リストを定義する必要があります。また、任意で RADIUS 許可およびアカウンティングの方式リストを定義できます。
- スイッチ上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。
- RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアが稼働しているマルチユーザ システムです。詳細については、RADIUS サーバのマニュアルを参照してください。
- Change-of-Authorization（CoA）インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。CoA を使用すると、セッションの識別と接続解除要求を実行できます。アップデートは、指定されたセッションにだけ作用します。
- スイッチ スタックと RADIUS サーバとの間に冗長接続を設定することを推奨します。これによって、接続済みのスタック メンバの 1 つがスイッチ スタックから削除された場合でも、RADIUS サーバにアクセスできます。

RADIUS 操作の場合：

- ユーザは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります（イネーブルに設定されている場合）。

関連トピック

RADIUS およびスイッチ アクセス, （1335 ページ）
RADIUS の動作, （1336 ページ）

RADIUS の設定に関する制約事項

ここでは、RADIUS によるスイッチ アクセスの制御の制約事項について説明します。

一般:

- セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。

RADIUS は次のネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は、AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

関連トピック

RADIUS の概要, （1335 ページ）

RADIUS に関する情報

RADIUS およびスイッチ アクセス

この項では、RADIUS をイネーブルにし、設定する方法について説明します。RADIUS を使用すると、アカウンティングの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます。

関連トピック

RADIUS を設定するための前提条件, （1333 ページ）
スイッチのローカル認証および許可の設定, （1395 ページ）
SSH サーバ、統合クライアント、およびサポートされているバージョン, （1403 ページ）

RADIUS の概要

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。RADIUS クライアントは、サポート対象の Cisco ルータおよびスイッチ上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。

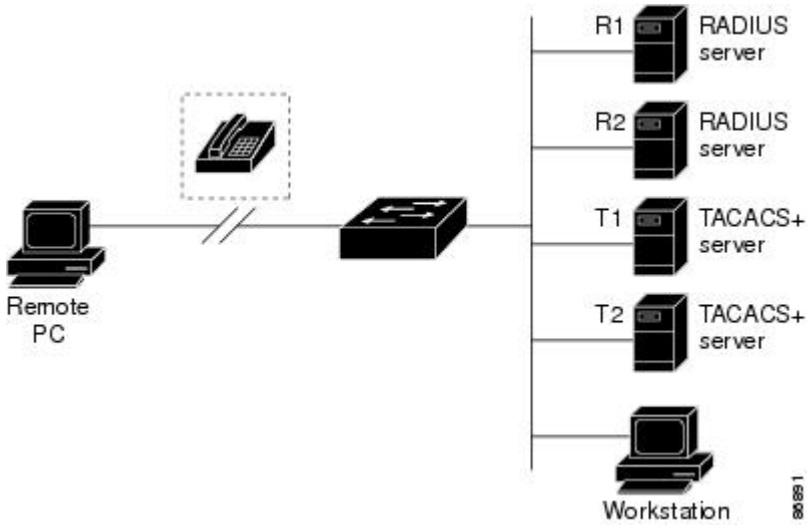
RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カード アクセス コントロール システムを使用するアクセス

環境。あるケースでは、RADIUS は Enigma のセキュリティ カードとともに使用してユーザを確認し、ネットワーク リソースのアクセスを許可します。

- すでに RADIUS を使用中のネットワーク。RADIUS クライアント装備のシスコのスイッチをネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。下の図 2「RADIUS サービスから TACACS+ サービスへの移行」を参照してください。
- ユーザが 1 つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1x などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、第 11 章「IEEE 802.1x ポートベース認証の設定」を参照してください。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

図 *65*：*RADIUS* サービスから *TACACS+* サービスへの移行



関連トピック

RADIUS の設定に関する制約事項, （1334 ページ）

RADIUS の動作

RADIUS サーバによってアクセス コントロールされるスイッチに、ユーザがログインおよび認証を試みると、次のイベントが発生します。

1 ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。

2 ユーザ名および暗号化されたパスワードが、ネットワーク経由でRADIUSサーバに送信されます。

3 ユーザは、RADIUS サーバから次のいずれかの応答を受信します。

- ACCEPT：ユーザが認証されたことを表します。
- REJECT：ユーザの認証が失敗し、ユーザ名およびパスワードの再入力が要求されるか、またはアクセスが拒否されます。
- CHALLENGE：ユーザに追加データを要求します。
- CHALLENGE PASSWORD：ユーザは新しいパスワードを選択するように要求されます。

ACCEPT またはREJECT応答には、特権EXEC またはネットワーク許可に使用する追加データがバンドルされています。ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

関連トピック

RADIUS を設定するための前提条件, （1333 ページ）

RADIUS 許可の変更

RADIUS 許可の変更（CoA）は、認証、認可、およびアカウンティング（AAA）セッションの属性を認証された後に変更するためのメカニズムを提供します。AAA でユーザ、またはユーザ グループのポリシーが変更された場合、管理者は、AAA サーバからCisco Secure Access Control Server（ACS）などの RADIUS CoA パケットを送信し、認証を再初期化して新しいポリシーを適用することができます。このセクションでは、使用可能なプリミティブおよびそれらのCoA での使用方法を含む、RADIUS インターフェイスの概要について説明します。

- Change-of-Authorization 要求
- CoA 要求応答コード
- CoA 要求コマンド
- セッション再認証
- セッション強制終了のスタック構成ガイドライン

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。Catalyst スイッチは、RFC 5176 で規定された（通常はプッシュ モデルで使用される）RADIUS CoA 拡張機能をサポートし、外部のAAA またはポリシーサーバからのセッションを動的に再設定できるようにします。

スイッチは、次のセッション単位の CoA 要求をサポートしています。

- セッション再認証
- セッション終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了

この機能は、Cisco Secure Access Control Server (ACS) 5.1 に統合されています。

Catalyst スイッチでは、RADIUS インターフェイスはデフォルトでイネーブルに設定されています。ただし、次の属性については、一部の基本的な設定が必要になります。

- セキュリティおよびパスワード：このガイドの「スイッチへの不正アクセスの防止」を参照してください。
- アカウンティング：このガイドの「スイッチベース認証の設定」の章の「RADIUSアカウンティングの起動」の項を参照してください。

Cisco IOS ソフトウェアは、RFC 5176 で定義されている RADIUS CoA の拡張をサポートします。この拡張は、一般に、外部 AAA またはポリシー サーバからのセッションのダイナミックな再構成を可能にするプッシュ モデルで使用されます。セッションの特定、セッションの終了、ホストの再認証、ポートのシャットダウン、およびポートバウンスでは、セッションごとのCoA要求がサポートされます。このモデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgement（ACK）[CoA-ACK]
- CoA nonacknowledgement（NAK）[CoA-NAK]

要求は CoA クライアント（通常は AAA またはポリシー サーバ）から開始されて、リスナーとして動作するデバイスに転送されます。

次の表は、Identity-Based Networking Services でサポートされている RADIUS CoA コマンドとベンダー固有属性（VSA）を示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 *93*：*Identity-Based Networking Services* でサポートされている *RADIUS CoA* コマンド

CoA コマンド	**シスコの VSA**
Activate service	Cisco:Avpair="subscriber:command=activate-service" Cisco:Avpair="subscriber:service-name=<*service-name*>" Cisco:Avpair="subscriber:precedence=<*precedence-number*>" Cisco:Avpair="subscriber:activation-mode=replace-all"
Deactivate service	Cisco:Avpair="subscriber:command=deactivate-service" Cisco:Avpair="subscriber:service-name=<*service-name*>"

CoA コマンド	シスコの VSA
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Session query	Cisco:Avpair=“subscriber:command=session-query”
Session reauthenticate	Cisco:Avpair="subscriber:command=reauthenticate" Cisco:Avpair=“subscriber:reauthenticate-type=last” または Cisco:Avpair=“subscriber:reauthenticate-type=rerun”
Session terminate	これは、VSA を必要としない、標準の接続解除要求です。
Session terminate	Cisco:AVpair="interface-template-name=<*interfacetemplate*>"

Change-of-Authorization 要求

Change of Authorization（CoA）要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。このモデルは、1 つの要求（CoA-Request）と 2 つの可能な応答コードで構成されています。

- CoA acknowledgment（ACK）[CoA-ACK]
- CoA non-acknowledgment（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から発信されて、リスナーとして動作するスイッチに送信されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してスイッチでサポートされています。

次の表に、この機能でサポートされている IETF 属性を示します。

表 *94*：サポートされている *IETF* 属性

属性番号	属性名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 *95*：*Error-Cause* の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット（無視）
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求（プロキシ）
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチセッションの選択がサポートされてない

CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。属性フィールドは、シスコのベンダー固有属性（VSA）を送信するために使用します。

関連トピック

CoA 要求コマンド, （1342 ページ）

セッションの識別

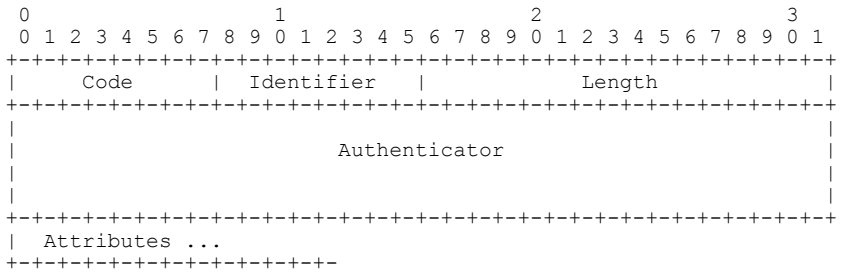
特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id VSA（シスコの VSA）
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）
- 次のいずれかの IPv6 属性。
  - Framed-IPv6-Prefix（IETF 属性 #97）および Framed-Interface-Id（IETF 属性 #96）。ともに RFC 3162 に従った完全な IPv6 アドレスを作成する
  - Framed-IPv6-Address
- プレーン IP アドレス（IETF 属性 #8）

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、スイッチは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

複数のセッション ID 属性がメッセージ含まれる場合は、すべての属性がセッションと一致しなければなりません。そうでない場合は、スイッチが Disconnect - negative acknowledgement（NAK）または CoA -NAK と、「Invalid Attribute Value」エラー コードを返します。

RFC 5176 で定義されている CoA 要求コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。



属性フィールドは、シスコのベンダー固有属性（VSA）を送信するために使用します。

特定の適用ポリシーを対象とする CoA 要求の場合、上記のセッション ID 属性のいずれかがメッセージに含まれていると、デバイスはエラー コードが「Invalid Attribute Value」の CoA-NAK を返します。

関連トピック

CoA 接続解除要求, （1343 ページ）
CoA 要求：ホスト ポートのディセーブル化, （1344 ページ）
CoA 要求：バウンス ポート, （1344 ページ）

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なり、個々の CoA コマンドで検討されます。

CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。CoA が成功したかを確認するには、**show** コマンドを使用します。

CoA 要求コマンド

表 *96*：スイッチでサポートされる *CoA* コマンド

コマンド [7]	シスコの VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	これは、VSA を要求しない、標準の接続解除要求です。
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

[7] すべての CoA コマンドには、スイッチと CoA クライアント間のセッション識別情報が含まれている必要があります。

関連トピック

CoA 要求応答コード, （1340 ページ）

セッション再認証

不明な ID またはポスチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファイル（たとえば、ゲスト VLAN）に関連付けられると、AAA サーバは通常、セッション再認証要求を生成します。再認証要求は、クレデンシャルが不明である場合にホストが適切な認証グループに配置されることを許可します。

セッション認証を開始するために、AAA サーバは *Cisco:Avpair="subscriber:command=reauthenticate"* の形式で Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。

現在のセッション ステートは、メッセージに対するスイッチの応答を決定します。セッションが現在、IEEE 802.1x によって認証されている場合、スイッチは EAPOL（LAN 経由の拡張認証プロトコル）RequestId メッセージをサーバに送信することで応答します。

現在、セッションが MAC 認証バイパス（MAB）で認証されている場合は、スイッチはサーバにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

スイッチがコマンドを受信したときにセッション認証が実行中である場合は、スイッチはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションがまだ認証されてない、あるいはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認証されている場合は、再認証メッセージがアクセス コントロール方式を再開し、最初に試行されるように設定された方式で開始します。セッションの現在の許可は、再認証によって異なる認証結果になるまで維持されます。

スイッチ スタックでのセッションの再認証

スイッチ スタックでセッション再認証メッセージを受信すると、次の動作が発生します。

- 確認応答（ACK）を戻す前に、再認証の必要性がチェックされます。
- 適切なセッションで再認証が開始されます。
- 認証が成功または失敗のいずれかで完了すると、再認証をトリガーする信号がスタック メンバから削除されます。
- 認証の完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、再認証が開始されます。
- ACK の送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再転送コマンドが新しいコマンドとして扱われます。

セッションの終了

セッションを終了させる 3 種類の CoA 要求があります。CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。このコマンドを使用すると、指定されたホストのオーセンティケータ ステートマシンが再初期化されますが、そのホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA の設定で CoA 要求を使用します。このコマンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であり、そのホストに対してネットワーク アクセスをただちにブロックする必要があります。ポートへのネットワーク アクセスを復旧する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

プリンタなどのサプリカントを持たないデバイスが新しい IP アドレスを取得する必要がある場合（たとえば、VLAN 変更後）は、ポート バウンスでホスト ポート上のセッションを終了します（ポートを一時的にディセーブルした後、再びイネーブルにする）。

CoA 接続解除要求

このコマンドは標準の接続解除要求です。セッションが見つからない場合、スイッチは Disconnect-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。セッ

ションがある場合は、スイッチはセッションを終了します。セッションが完全に削除された後、スイッチは接続解除 ACK を返します。

スイッチがクライアントに接続解除 ACK を返す前にスタンバイ スイッチにフェールオーバーする場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。再送信後もセッションが見つからない場合は、Disconnect-ACK と「Session Context Not Found」エラー コード属性が送信されます。

関連トピック

セッションの識別, （1341 ページ）

CoA 要求：ホスト ポートのディセーブル化

RADIUS サーバの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元するには、非 RADIUS メカニズムを使用して再びイネーブルにします。このコマンドは、次の新しいベンダー固有属性（VSA）が含まれている標準 CoA 要求メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチは CoA-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。このセッションがある場合は、スイッチはホスト ポートをディセーブルにし、CoA-ACK メッセージを返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

（注） 再送信コマンドの後に接続解除要求が失敗すると、（接続解除 ACK が送信されてない場合に）チェンジオーバー前にセッションが正常終了し、または元のコマンドが実行されてスタンバイ スイッチがアクティブになるまでの間に発生した他の方法（たとえば、リンク障害）によりセッションが終了することがあります。

関連トピック

セッションの識別, （1341 ページ）

CoA 要求：バウンス ポート

RADIUS サーバの CoA bounce port が RADIUS サーバから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生

する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチは CoA-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。このセッションがある場合は、スイッチはホスト ポートを 10 秒間ディセーブルし、再びイネーブルにし（ポート バウンス）、CoA-ACK を返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

関連トピック

セッションの識別, （1341 ページ）

セッション強制終了のスタック構成ガイドライン

スイッチ スタックでは、CoA 接続解除要求メッセージに必要な特別な処理はありません。

CoA 要求バウンス ポートのスタック構成 ガイドライン

bounce-port コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

スタック マスターで Auth Manager コマンド ハンドラが有効な **bounce-port** コマンドを受信すると、CoA-ACK メッセージを返す前に次の情報が確認されます。

- ポート バウンスの必要性
- ポート ID（ローカル セッション コンテキストで検出された場合）

スイッチで、ポート バウンスが開始されます（ポートが 10 秒間ディセーブルになり、再びイネーブルにされます）。

ポート バウンスが正常に実行された場合、ポート バウンスをトリガーした信号がスタンバイ スタック マスターから削除されます。

ポート バウンスの完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、ポート バウンスが開始されます。

CoA-ACK メッセージの送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再送信コマンドが新しいコマンドとして扱われます。

CoA 要求ディセーブル ポートのスタック構成 ガイドライン

disable-port コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

スタック マスターにある Auth Manager コマンド ハンドラで、有効な **disable-port** コマンドを受信した場合、CoA-ACK メッセージを返す前に次の情報が検証されます。

- ポート ディセーブルの必要性
- ポート ID（ローカル セッション コンテキストで検出された場合）

スイッチで、ポートをディセーブルする操作が試行されます。

ポートをディセーブルする操作が正常に実行された場合、ポートをディセーブルする操作をトリガーした信号がスタンバイ スタック マスターから削除されます。

ポートをディセーブルする操作の完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、ポートがディセーブルにされます。

CoA-ACK メッセージの送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再送信コマンドが新しいコマンドとして扱われます。

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

RADIUS サーバ ホスト

スイッチと RADIUS サーバの通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS ホストとして個々のポートを定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバーバックアップとして動作します。この例では、最初のホストエントリがアカウンティング サービスを提供できなかった場合、スイッチは「%RADIUS-4-RADIUS_DEAD」メッ

セージを表示し、その後、同じデバイス上で 2 番めに設定されたホスト エントリでアカウンティング サービスを試みます（RADIUS ホスト エントリは、設定した順序に従って試行されます）。

RADIUS サーバとスイッチは、共有するシークレット テキスト ストリングを使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバ デーモンが稼働するホストと、そのホストがスイッチと共有するシークレット テキスト（キー）ストリングを指定する必要があります。

タイムアウト、再送信回数、および暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定することもできますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単位での設定を組み合わせることもできます。

関連トピック

RADIUS サーバ ホストの識別, （1365 ページ）
AAA サーバ グループの定義, （1370 ページ）
すべての RADIUS サーバの設定, （1376 ページ）
RADIUS ログイン認証の設定, （1367 ページ）

RADIUS ログイン認証

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外は、デフォルトの方式リストです。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

関連トピック

RADIUS ログイン認証の設定, （1367 ページ）

AAA サーバ グループ

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホストエントリを含めることもできますが、各エントリが一意の ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の異なる UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホストエントリのフェールオーバーバックアップとして動作します。最初のホスト エントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じデバイス上でアカウンティング サービス用に設定されている 2 番めのホスト エントリを試行します。（試行される RADIUS ホストエントリの順番は、設定されている順序に従います）。

関連トピック

AAA サーバ グループの定義, （1370 ページ）

AAA 許可

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可をイネーブルにすると、スイッチは（ローカル ユーザ データベースまたはセキュリティ サーバ上に存在する）ユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

関連トピック

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定, （1372 ページ）

RADIUS アカウンティング

AAA アカウンティング機能は、ユーザが使用したサービスと、消費したネットワーク リソース量を追跡します。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で RADIUS セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。

関連トピック

RADIUS アカウンティングの起動, （1374 ページ）

ベンダー固有の RADIUS 属性

Internet Engineering Task Force（IETF）ドラフト規格に、ベンダー固有の属性（属性 26）を使用して、スイッチと RADIUS サーバ間でベンダー固有の情報を通信するための方式が定められています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には

適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダー タイプ 1（名前は *cisco-avpair*）です。この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

protocol は、特定の認証タイプに使用するシスコのプロトコル属性の値です。 *attribute* および *value* は、シスコの TACACS+ 仕様で定義されている、該当の属性値（AV）ペアです。*sep* は、必須の属性の場合は =、任意指定の属性の場合は * です。TACACS+ 認証で使用できるすべての機能は、RADIUS でも使用できます。

たとえば、次の AV ペアにより、IP 認証中（PPP の IPCP アドレス割り当て中）には、シスコの「multiple named IP address pools」機能がアクティブになります。

```
cisco-avpair= ″ip:addr-pool=first″
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」はオプションになります。AV ペアはオプションにすることが可能である、ということに注意してください。

```
cisco-avpair= ″ip:addr-pool*first″
```

次に、ネットワーク アクセス サーバからユーザがログインしたらすぐに EXEC コマンドが実行されるようにする方法の例を示します。

```
cisco-avpair= ″shell:priv-lvl=15″
```

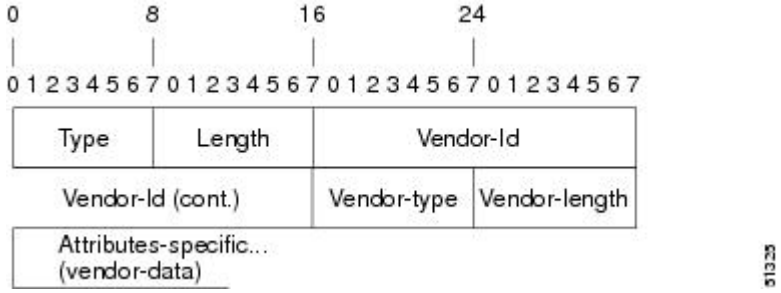
他のベンダーにも、それぞれ独自のベンダー ID、オプション、および関連する VSA があります。ベンダー ID および VSA の詳細については、RFC 2138『Remote Authentication Dial-In User Service（RADIUS）』を参照してください。

属性 26 には、次の 3 つの要素が含まれています。

- タイプ
- 長さ
- ストリング（またはデータ）
  - Vendor-Id
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

次の図は、属性 26 の「背後で」カプセル化される VSA のパケット形式を示します。

図 *66*：属性 *26* の背後でカプセル化される *VSA*



（注） VSA の形式はベンダーが指定します。Attribute-Specific フィールド（Vendor-Data とも呼ばれる）は、ベンダーによるその属性の定義によって異なります。

次の表に、「ベンダー固有 RADIUS IETF 属性テーブル」（次の 2 番目の表）で表示される重要なフィールドを示します。これは、サポート対象のベンダー固有 RADIUS 属性（IETF 属性 26）を表示します。

表 *97*：「ベンダー固有属性テーブル」のフィールドの説明

フィールド	説明
Number	次の表に示されるすべての属性は、IETF 属性 26 の拡張です。
Vendor-Specific Command Codes	特定のベンダーの識別に使用する定義されたコード。コード 9 は Cisco VSA、311 は Microsoft VSA、529 は Ascend VSA を定義します。
Sub-Type Number	属性 ID 番号。この番号は、属性 26 の背後でカプセル化される「2 番めのレイヤ」の ID 番号であること以外、IETF 属性の ID 番号に似ています。
Attribute	属性の ASCII ストリング名。
Description	属性の説明。

表 *98* : ベンダー固有 *RADIUS IETF* 属性

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
MS-CHAP 属性				
26	311	1	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでしか使用されません。この属性は、PPP CHAP ID と同じです（RFC 2548）
26	311	11	MSCHAP-Challenge	ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャレンジが含まれます。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。（RFC 2548）
VPDN 属性				
26	9	1	l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウ サイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。
26	9	1	l2tp-drop-out-of-order	正しくない順序で受信したデータ パケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データ パケット上でシーケンス番号が送信されるわけではありません。

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	l2tp-hello-interval	hello キープアライブ インターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。
26	9	1	l2tp-hidden-avp	イネーブルにすると、L2TP 制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。
26	9	1	l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。
26	9	1	tunnel-tos-reflect	LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロード パケットの IP ヘッダーからトンネル パケットの IP ヘッダーにコピーします。
26	9	1	l2tp-tunnel-authen	この属性を設定すると、L2TP トンネル認証が実行されます。
26	9	1	l2tp-tunnel-password	L2TP トンネル認証および AVP 隠蔽に使用される共有秘密。

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	l2tp-udp-checksum	これは認可属性で、L2TP がデータ パケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」と「no」です。デフォルトは「no」です。
Store and Forward Fax 属性				
26	9	3	Fax-Account-Id-Origin	**mmoipaaareceive-id** コマンドまたは **mmoipaaasend-id** コマンドについて、アカウント ID の発信元がシステム管理者によって定義されたものとして示します。
26	9	4	Fax-Msg-Id=	Store and Forward Fax 機能によって割り当てられた一意のファクス メッセージ識別番号を示します。
26	9	5	Fax-Pages	このファクス セッション中に送信または受信したページ数を示します。このページ数には、カバー ページも含まれます。

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	6	Fax-Coverpage-Flag	カバー ページがこのファクス セッションのオフランプ ゲートウェイで生成されたかどうかを示します。true はカバー ページが生成されたことを示します。false はカバー ページが生成されなかったことを意味します。
26	9	7	Fax-Modem-Time	モデムがファクス データを送信した時間（x）、およびファクス セッションの合計時間（y）を秒単位で示します。これには、fax-mail および PSTN 時間が x/y の形式で含まれます。たとえば、10/15 は送信時間が 10 秒で、合計ファクス セッションが 15 秒であったことを示します。
26	9	8	Fax-Connect-Speed	この fax-mail が最初に送信または受信された時点のモデム速度を示します。有効値は、1200、4800、9600、および 14400 です。
26	9	9	Fax-Recipient-Count	このファクス送信の受信者数を示します。E メール サーバがセッション モードをサポートするまで、この数字は 1 にする必要があります。

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	10	Fax-Process-Abort-Flag	ファクス セッションが中断したこと、または正常に終了したことを示します。true はセッションが中断したことを示します。false はセッションが成功したことを示します。
26	9	11	Fax-Dsn-Address	DSN の送信先のアドレスを示します。
26	9	12	Fax-Dsn-Flag	DSN がイネーブルにされているかどうかを示します。true は DSN がイネーブルにされていることを示します。false は DSN がイネーブルにされていないことを示します。
26	9	13	Fax-Mdn-Address	MDN の送信先のアドレスを示します。
26	9	14	Fax-Mdn-Flag	メッセージ配信通知（MDN）がイネーブルにされているかどうかを示します。true は MDN がイネーブルにされていることを示します。false は MDN がイネーブルにされていないことを示します。
26	9	15	Fax-Auth-Status	このファクス セッションに対する認証が成功したかどうかを示します。このフィールドに対する有効値は、success、failed、bypassed、または unknown です。

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	16	Email-Server-Address	オンランプ fax-mail メッセージを処理する E メール サーバの IP アドレスを示します。
26	9	17	Email-Server-Ack-Flag	オンランプ ゲートウェイが fax-mail メッセージを受け入れる E メール サーバから肯定確認応答を受信したことを示します。
26	9	18	Gateway-Id	ファクス セッションを処理したゲートウェイの名前を示します。名前は、hostname.domain-name という形式で表示されます。
26	9	19	Call-Type	ファクスのアクティビティのタイプを、fax receive または fax send のどちらかで記述します。
26	9	20	Port-Used	この fax-mail の送受信いずれかに使用される Cisco AS5300 のスロット/ポート番号を示します。

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	21	Abort-Cause	ファクス セッションが中断した場合、中断の信号を送信したシステム コンポーネントを示します。中断する可能性のあるシステム コンポーネントには、FAP（Fax Application Process）、TIFF（TIFF リーダーまたは TIFF ライター）、fax-mail クライアント、fax-mail サーバ、ESMTP クライアント、ESMTP サーバなどがあります。
H323 属性				
26	9	23	Remote-Gateway-ID（h323-remote-address）	リモート ゲートウェイの IP アドレスを示します。
26	9	24	Connection-ID（h323-conf-id）	会議 ID を識別します。
26	9	25	Setup-Time（h323-setup-time）	以前、グリニッジ標準時（GMT）およびズール タイムと呼ばれていた協定世界時（UTC）でのこの接続のセットアップ時間を示します。
26	9	26	Call-Origin（h323-call-origin）	ゲートウェイに対するコールの発行元を示します。有効値は、originating および terminating です（回答）。

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	27	Call-Type（h323-call-type）	コールのレグ タイプを示します。有効値は、**telephony** および **VoIP** です。
26	9	28	Connect-Time（h323-connect-time）	このコール レッグの UTC での接続時間を示します。
26	9	29	Disconnect-Time（h323-disconnect-time）	このコール レッグが UTC で接続解除された時間を示します。
26	9	30	Disconnect-Cause（h323-disconnect-cause）	Q.931 仕様によって、接続がオフラインにされた理由を示します。
26	9	31	Voice-Quality（h323-voice-quality）	コールの音声品質に影響する Impairment Factor（ICPIF）を指定します。
26	9	33	Gateway-ID（h323-gw-id）	下位のゲートウェイの名前を示します。
大規模のダイヤルアウト属性				
26	9	1	callback-dialstring	コールバックに使用するダイヤリング文字列を定義します。
26	9	1	data-service	説明はありません。
26	9	1	dial-number	ダイヤルする番号を定義します。
26	9	1	force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	map-class	ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップ クラスで設定される情報の参照を許可します。
26	9	1	send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	send-name	

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
				PPP 名前認証。PAP に適用する場合は、インターフェイス上で **ppppapsent-namepassword** コマンドを設定しないでください。PAP の場合、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAPの場合、「preauth:send-name」は、アウトバウンド認証だけでなく、インバウンド認証にも使用されます。CHAPインバウンドの場合、NAS は発信元のボックスへのチャレンジ パケットに、「preauth:send-name」で定義された名前を使用します。 （注） send-name 属性は時間の経過とともに変わっています。最初は、現在 send-name および remote-name 属性の両方で提供されている機能を実行していました。remote-name 属性が追加され

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
				たため、send-name 属性は現在の動作に制限されています。
26	9	1	send-secret	PPPパスワード認証。ベンダー固有属性（VSA）の場合、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAPアウトバウンドの場合、「preauth:send-name」と「preauth:send-secret」の両方が応答パケットで使用されます。
26	9	1	remote-name	大規模のダイヤルアウトで使用するリモートホストの名前を提供します。ダイヤラは、大規模のダイヤルアウトのリモート名が認証された名前と一致することを確認し、偶発的なユーザ RADIUS 設定ミスから保護します（有効な電話番号にダイヤルしたが誤ったデバイスに接続されるなどのミスです）。
その他の属性				

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	2	Cisco-NAS-Port	NAS-Port アカウンティングに追加的なベンダー固有属性（VSA）を指定します。追加的な NAS-Port 情報を属性値ペア（AVPair）の形式で指定するには、**radius-servervsasend** グローバル コンフィギュレーション コマンドを使用します。 （注） この VSA は、通常アカウンティングで使用されますが認証（Access-Request）パケットで使用される場合もあります。
26	9	1	min-links	MLP に対するリンクの最小数を設定します。
26	9	1	proxyacl#<n>	ダウンロード可能なユーザ プロファイル（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	spi	登録中にホーム エージェントがモバイル ノードの認証で必要とする認証情報を伝送します。この情報は、**ipmobilesecurehost<addr>** コンフィギュレーション コマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーション コマンドはそのまま含まれます。これにはセキュリティ パラメータ インデックス（SPI）、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。

関連トピック

ベンダー固有の RADIUS 属性を使用するスイッチ設定, （1378 ページ）

ベンダー独自仕様の RADIUS サーバ通信

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバ間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS 属性セットを独自に機能拡張しているベンダーもあります。Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

前述したように、RADIUS（ベンダーの独自仕様によるものか、IETF ドラフトに準拠するものかを問わず）を設定するには、RADIUS サーバ デーモンが稼働しているホストと、そのホストがスイッチと共有するシークレット テキスト ストリングを指定する必要があります。RADIUS ホストおよびシークレット テキスト ストリングを指定するには、**radius-server** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定, （1379 ページ）

RADIUS の設定方法

RADIUS サーバ ホストの識別

スイッチと通信するすべての RADIUS サーバに対して、これらの設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** の 3 つの固有のグローバル コンフィギュレーション コマンドを使用します。

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。詳細については、次の関連項目を参照してください。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチのIPアドレス、およびサーバとスイッチの双方で共有するキーストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、次の手順を実行します。

はじめる前に

スイッチ上にグローバルな機能とサーバ単位での機能（タイムアウト、再送信回数、およびキー コマンド）を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、およびキーに関するコマンドは、グローバルに設定したタイムアウト、再送信回数、およびキーに関するコマンドを上書きします。すべての RADIUS サーバに対してこれらの値を設定する方法については、次の関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius server***server name*
4. **address**{**ipv4 | ipv6**}*ip address*{ **auth-port***port number* | **acct-port***port number*}
5. **key***string*
6. **retransmit***value*
7. **timeout***seconds*
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server***server name* 例： スイッチ(config)# **radius server rsim**	
ステップ 4	**address**{**ipv4** | **ipv6**}*ip address*{ **auth-port***port number* | **acct-port***port number*} 例： スイッチ(config-radius-server)# **address ipv4 124.2.2.12 auth-port 1612**	（任意）RADIUS サーバのパラメータを指定します。 **auth-port***port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1645 です。指定できる範囲は 0 ～ 65536 です。 **auth-port***port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1646 です。
ステップ 5	**key***string* 例： スイッチ(config-radius-server)# **key rad123**	（任意）**key***string* には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に **radius server** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。

	コマンドまたはアクション	目的
ステップ 6	**retransmit***value* 例： スイッチ(config-radius-server)# **retransmit 10**	（任意）サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ～ 100 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。
ステップ 7	**timeout***seconds* 例： スイッチ(config-radius-server)# **timeout 60**	（任意）スイッチが、再度要求を送信する前に、RADIUS サーバからの応答を待機する時間間隔を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

RADIUS サーバ ホスト，（1346 ページ）
AAA サーバ グループの定義，（1370 ページ）
すべての RADIUS サーバの設定，（1376 ページ）

RADIUS ログイン認証の設定

RADIUS ログイン認証を設定するには、次の手順を実行します。

はじめる前に

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
5. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
6. **login authentication** {**default** | *list-name*}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： スイッチ(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： スイッチ(config)# **aaa**	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定しま

	コマンドまたはアクション	目的
	authentication login default local	す。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 ◦ *enable*：イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ **enable***password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 ◦ *group radius*：RADIUS 認証を使用します。この認証方式を使用するには、あらかじめ RADIUS サーバを設定しておく必要があります。 ◦ *line*：回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。**password***password* ライン コンフィギュレーション コマンドを使用します。 ◦ *local*：ローカルユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username***name***password** グローバル コンフィギュレーション コマンドを使用します。 ◦ *local-case*：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username***password* グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 ◦ *none*：ログインに認証を使用しません。
ステップ 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： スイッチ(config)# **line 1 4**	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。

	コマンドまたはアクション	目的
ステップ 6	**login authentication** {**default** | *list-name*} 例： `スイッチ(config)# login authentication default`	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 7	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

RADIUS ログイン認証, （1347 ページ）
RADIUS サーバ ホスト, （1346 ページ）

AAA サーバ グループの定義

定義したグループ サーバに特定のサーバを関連付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することも、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを特定することもできます。

AAA サーバ グループを定義するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **radiusserver***name*
4. **address**{**ipv4**| **ipv6**} {*ip-address*| *hostname*} **auth-port***port-number***acct-port***port-number*
5. **end** {{**0**| **7**} *string*}*string*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radiusserver***name* 例： スイッチ(config)# **radius server ISE**	RADIUS サーバの設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。 スイッチは、IPv6 対応の RADIUS をサポートしています。
ステップ 4	**address**{**ipv4**| **ipv6**} {*ip-address*| *hostname*} **auth-port***port-number***acct-port***port-number* 例： スイッチ(config-radius-server)# **address ipv4 10.1.1.1 auth-port 1645 acct-port 1646**	RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。
ステップ 5	**end** {{**0**| **7**} *string*}*string* 例： スイッチ(config-radius-server)# **key**	デバイスと RADIUS サーバとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。

	コマンドまたはアクション	目的
	cisco123	
ステップ 6	**end** 例： スイッチ(config-radius-server)# **end**	RADIUS サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

RADIUS サーバ ホストの識別, （1365 ページ）
RADIUS サーバ ホスト, （1346 ページ）
AAA サーバ グループ, （1347 ページ）

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

ユーザ特権アクセスおよびネットワーク サービスに関する RADIUS 許可を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa authorization network radius**
4. **aaa authorization exec radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization network radius** 例： スイッチ(config)# **aaa authorization network radius**	ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。
ステップ 4	**aaa authorization exec radius** 例： スイッチ(config)# **aaa authorization exec radius**	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ RADIUS 許可をスイッチに設定します。 **exec** キーワードを指定すると、ユーザプロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

aaa authorization グローバル コンフィギュレーション コマンドと **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

関連トピック

AAA 許可，（1348 ページ）

RADIUS アカウンティングの起動

RADIUS アカウンティングを開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa accounting network start-stop radius**
4. **aaa accounting exec start-stop radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting network start-stop radius** 例： スイッチ(config)# **aaa accounting network start-stop radius**	ネットワーク関連のあらゆるサービス要求に関して、RADIUS アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting exec start-stop radius** 例： スイッチ(config)# **aaa accounting exec start-stop radius**	RADIUS アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。このコマンドは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

関連トピック

RADIUS アカウンティング，（1348 ページ）

すべての RADIUS サーバの設定

すべての RADIUS サーバを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **radius-server key***string*
3. **radius-server retransmit***retries*
4. **radius-server timeout***seconds*
5. **radius-server deadtime***minutes*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server key***string* 例： `スイッチ(config)# radius-server key`	スイッチとすべての RADIUS サーバ間で共有されるシークレット テキスト ストリングを指定します。

	コマンドまたはアクション	目的
	your_server_key スイッチ(config)# **key your_server_key**	（注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキストストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 3	**radius-server retransmit***retries* 例： スイッチ(config)# **radius-server retransmit 5**	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ～ 1000 です。
ステップ 4	**radius-server timeout***seconds* 例： スイッチ(config)# **radius-server timeout 3**	スイッチが RADIUS 要求に対する応答を待って、要求を再送信するまでの時間（秒）を指定します。デフォルトは 5 秒です。指定できる範囲は 1 ～ 1000 です。
ステップ 5	**radius-server deadtime***minutes* 例： スイッチ(config)# **radius-server deadtime 0**	RADIUS サーバが認証要求に応答していない場合、このコマンドはそのサーバに対する要求を停止する時刻を指定します。これにより、要求がタイムアウトするまで待たずとも、次に設定されているサーバを試行することができます。デフォルトは 0 です。指定できる範囲は 0 ～ 1440 分です。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

RADIUS サーバ ホストの識別, （1365 ページ）
RADIUS サーバ ホスト, （1346 ページ）

ベンダー固有の RADIUS 属性を使用するスイッチ設定

ベンダー固有仕様の RADIUS 属性を使用するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server vsa send** [**accounting**	**authentication**] 例： `スイッチ(config)# radius-server vsa send accounting`	スイッチが VSA（RADIUS IETF 属性 26 で定義）を認識して使用できるようにします。 • （任意）認識されるベンダー固有属性の集合をアカウンティング属性だけに限定するには、**accounting** キーワードを使用します。

	コマンドまたはアクション	目的
		• （任意）認識されるベンダー固有属性の集合を認証属性だけに限定するには、**authentication** キーワードを使用します。 キーワードを指定せずにこのコマンドを入力すると、アカウンティングおよび認証のベンダー固有属性の両方が使用されます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ベンダー固有の RADIUS 属性, （1348 ページ）

ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定

ベンダー独自仕様の RADIUS サーバ通信を使用するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius server***server name*
4. **address** { **ipv4 | ipv6**}*ip address*
5. **non-standard**
6. **key***string*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server***server name* 例： スイッチ(config)# **radius server rsim**	RADIUS サーバを指定します。
ステップ 4	**address** { **ipv4	ipv6**}*ip address* 例： スイッチ(config-radius-server)# **address ipv4 172.24.25.10**	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 5	**non-standard** 例： スイッチ(config-radius-server)# **non-standard**	RADIUS サーバが RADIUS ベンダー独自の実装を使用していることを示します。

	コマンドまたはアクション	目的
ステップ 6	**key***string* 例： スイッチ(config-radius-server)# **key rad123**	スイッチとベンダー独自仕様の RADIUS サーバとの間で共有されるシークレット テキスト ストリングを指定します。スイッチと RADIUS サーバはこのテキスト ストリングを使用してパスワードを暗号化し、応答を交換します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ベンダー独自仕様の RADIUS サーバ通信, （1364 ページ）

スイッチ上での CoA の設定

CoA をスイッチで設定するには、次の手順を実行します。この手順は必須です。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name*} [**vrf***vrfname*] [**server-key***string*]
6. **server-key** [**0** | **7**] *string*
7. **port***port-number*
8. **auth-type** {**any** | **all** | **session-key**}
9. **ignore session-key**
10. **ignore server-key**
11. **authentication command bounce-port ignore**
12. **authentication command disable-port ignore**
13. **end**
14. **show running-config**
15. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： スイッチ(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa server radius dynamic-author** 例： スイッチ(config)# **aaa server radius**	スイッチを認証、許可、アカウンティング（AAA）サーバに設定し、外部ポリシーサーバとの相互作用を促進します。

	コマンドまたはアクション	目的
	dynamic-author	
ステップ 5	**client** {*ip-address* | *name*} [**vrf***vrfname*] [**server-key***string*]	ダイナミック許可ローカル サーバ コンフィギュレーション モードを開始し、デバイスが CoA を受け取り、要求を取り外す RADIUS クライアントを指定します。
ステップ 6	**server-key** [**0** | **7**] *string* 例： スイッチ(config-sg-radius)# **server-key your_server_key**	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 7	**port***port-number* 例： スイッチ(config-sg-radius)# **port 25**	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。
ステップ 8	**auth-type** {**any** | **all** | **session-key**} 例： スイッチ(config-sg-radius)# **auth-type any**	スイッチが RADIUS クライアントに使用する許可のタイプを指定します。 クライアントは、許可用に設定されたすべての属性と一致していなければなりません。
ステップ 9	**ignore session-key**	（任意）セッション キーを無視するようにスイッチを設定します。 **ignore** コマンドの詳細については、Cisco.com 上の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。
ステップ 10	**ignore server-key** 例： スイッチ(config-sg-radius)# **ignore server-key**	（任意）サーバ キーを無視するようにスイッチを設定します。 **ignore** コマンドの詳細については、Cisco.com 上の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。
ステップ 11	**authentication command bounce-port ignore** 例： スイッチ(config-sg-radius)# **authentication command bounce-port ignore**	（任意）CoA 要求を無視して、セッションをホスティングするポートを一時的にディセーブルにするようにスイッチを設定します。ポートを一時的にディセーブルにする目的は、VLANの変更が発生しても、その変更を検出するサプリカントがエンドポイント上にない場合に、ホストから DHCP 再ネゴシエーションを行わせることです。

	コマンドまたはアクション	目的
ステップ 12	**authentication command disable-port ignore** 例： スイッチ(config-sg-radius)# **authentication command disable-port ignore**	（任意）セッションをホスティングしているポートを管理上のシャットダウン状態にすることを要求する非標準コマンドを無視するようにスイッチを設定します。ポートをシャットダウンすると、セッションが終了します。 ポートを再びイネーブルにするには、標準の CLI または SNMP コマンドを使用します。
ステップ 13	**end** 例： スイッチ(config-sg-radius)# **end**	特権 EXEC モードに戻ります。
ステップ 14	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 15	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

CoA 機能のモニタリング

表 *99*：特権 *EXEC* 表示コマンド

コマンド	目的
show aaa attributes protocol radius	RADIUS コマンドの AAA 属性を表示します。

表 *100*：グローバル トラブルシューティング コマンド

コマンド	目的
debug radius	RADIUS のトラブルシューティングを行うための情報を表示します。

コマンド	目的
debug aaa coa	CoA 処理のトラブルシューティングを行うための情報を表示します。
debug aaa pod	POD パケットのトラブルシューティングを行うための情報を表示します。
debug aaa subsys	POD パケットのトラブルシューティングを行うための情報を表示します。
debug cmdhd [**detail** | **error** | **events**]	コマンドヘッダーのトラブルシューティングを行うための情報を表示します。

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セッションアウェアなネットワーキングに対するアイデンティティ コントロール ポリシーおよびアイデンティティ サービス テンプレートの設定。	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル

MIB

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

シスコのテクニカル サポート

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

第 59 章

Kerberos の設定

- 機能情報の確認，1387 ページ
- Kerberos によるスイッチ アクセスの制御の前提条件，1387 ページ
- Kerberos に関する情報，1388 ページ
- Kerberos を設定する方法，1393 ページ
- Kerberos 設定のモニタリング，1393 ページ
- その他の参考資料，1393 ページ

機能情報の確認

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

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

Kerberos によるスイッチ アクセスの制御の前提条件

Kerberos によるスイッチ アクセスの制御の前提条件は、次のとおりです。

- リモート ユーザがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定し、ユーザとネットワーク サービスの両方に通信を行い、相互に認証させる必要があります。これを実現するには、互いの識別が必要です。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成

した KEYTAB ファイルを追加します。また、KDC データベースにユーザ用のエントリも作成します。

- Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるスイッチを使用できます。

ホストおよびユーザのエントリを追加または作成する場合の注意事項は次のとおりです。

- Kerberos プリンシパル名はすべて小文字でなければなりません。
- Kerberos インスタンス名はすべて小文字でなければなりません。
- Kerberos レルム名はすべて大文字でなければなりません。

Kerberos に関する情報

ここでは、Kerberos の情報を提供します。

Kerberos とスイッチ アクセス

ここでは、Kerberosセキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。

（注） Kerberosの設定例では、信頼できるサードパーティを、Kerberosをサポートし、ネットワーク セキュリティ サーバとして設定され、Kerberosプロトコルを使用してユーザを認証するスイッチとすることができます。

Kerberos の概要

Kerberos はマサチューセッツ工科大学（MIT）が開発した秘密キーによるネットワーク認証プロトコルです。データ暗号規格（DES）という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサードパーティという概念を使ってユーザとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティをキー発行局（KDC）と呼びます。

Kerberos は、ユーザが誰であるか、そのユーザが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC（つまり信頼できる Kerberos サーバ）がユーザにチケットを発行します。これらのチケットには有効期限があり、ユーザ クレデンシャルのキャッシュに保存されます。Kerberosサーバは、ユーザ名やパスワードの代わりにチケットを使ってユーザとネットワーク サービスを認証します。

（注） Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるのであれば、どのスイッチも使用できます。

Kerberos のクレデンシャル発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザを 1 回認証すると、ユーザ クレデンシャルが有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、（UNIX サーバや PC などの）他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh

次の表に、一般的な Kerberos 関連用語とその定義を示します。

表 *101*：*Kerberos* の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
認証	ユーザがネットワークやスイッチにおいてどのような権限を有しており、またどのような動作を実行できるかを、スイッチが識別する手段
クレデンシャル	認証チケット（TSG[8]、サービス クレデンシャルなど）を表す総称。Kerberos クレデンシャルで、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することにした場合、ユーザ名やパスワードを再入力する代わりにこれを使用できます。証明書の有効期限は、8 時間がデフォルトの設定です。

用語	定義
インスタンス	Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、*user@REALM* という形式です（たとえば、smith@EXAMPLE.COM）。Kerberos インスタンスのある Kerberos プリンシパルは、*user/instance@REALM* という形式です（たとえば、smith/admin@EXAMPLE.COM）。Kerberos インスタンスは、認証が成功した場合のユーザの承認レベルを指定するために使用できます。各ネットワーク サービスのサーバは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。 （注） Kerberos プリンシパル名およびインスタンス名はすべて小文字でなければなりません。 （注） Kerberos レルム名はすべて大文字でなければなりません。
KDC[9]	ネットワーク ホストで稼働する Kerberos サーバおよびデータベース プログラムで構成されるキー発行局
Kerberos 対応	Kerberos クレデンシャルのインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク サービスの ID を検証します。 （注） Kerberos レルム名はすべて大文字でなければなりません。
Kerberos サーバ	ネットワーク ホストで稼働しているデーモン。ユーザおよびネットワーク サービスはそれぞれ Kerberos サーバに ID を登録します。ネットワーク サービスは Kerberos サーバにクエリーを送信して、他のネットワーク サービスの認証を得ます。

用語	定義
KEYTAB[10]	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス クレデンシャルを暗号解除して認証します。Kerberos 5 よりも前のバージョンでは、KEYTAB は SRVTAB[11] と呼ばれます。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。 （注） Kerberos プリンシパル名はすべて小文字でなければなりません。
サービス クレデンシャル	ネットワーク サービスのクレデンシャル。KDC からクレデンシャルが発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。ユーザ TGT ともパスワードを共有します。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。SRVTAB は、Kerberos 5 以降のバージョンでは KEYTAB と呼ばれています。
TGT	身分証明書のことで、KDC が認証済みユーザに発行するクレデンシャル。TGT を受け取ったユーザは、KDC が示した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

8 チケット認可チケット
9 キー発行局
10 キー テーブル
11 サーバ テーブル

Kerberos の動作

Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてリモート ユーザを認証できるスイッチを使用できます。Kerberos をカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモート ユーザは、3 つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

リモート ユーザがスイッチを Kerberos サーバとして使用してネットワーク サービスで認証されるには、次の手順を実行する必要があります。

境界スイッチに対する認証の取得

ここでは、リモートユーザが通過しなければならない最初のセキュリティ レイヤについて説明します。ユーザは、まず境界スイッチに対して認証を得なければなりません。リモート ユーザが境界スイッチに対して認証を得る場合、次のプロセスが発生します。

1. ユーザが境界スイッチに対して、Kerberos 未対応の Telnet 接続を開始します。
2. ユーザ名とパスワードの入力を求めるプロンプトをスイッチが表示します。
3. スイッチが、このユーザの TGT を KDC に要求します。
4. KDC がユーザ ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使って TGT の暗号解除を試行します。
   - 暗号解除に成功した場合は、ユーザはスイッチに対して認証を得ます。
   - 暗号解除に成功しない場合は、ユーザ名とパスワードを再入力（Caps Lock または Num Lock のオン/オフに注意）するか、別のユーザ名とパスワードを入力してステップ 2 の手順を繰り返します。

Kerberos 未対応の Telnet セッションを開始し、境界スイッチの認証を得ているリモート ユーザはファイアウォールの内側にいますが、ネットワーク サービスにアクセスするには、KDC から直接認証を得る必要があります。ユーザが KDC から認証を得なければならないのは、KDC が発行する TGT はスイッチに保存されており、ユーザがこのスイッチにログオンしないかぎり、追加の認証に使用できないからです。

KDC からの TGT の取得

ここでは、リモート ユーザが通過しなければならない 2 番めのセキュリティ レイヤについて説明します。ユーザは、ネットワーク サービスにアクセスするために、このレイヤで KDC の認証を得て、KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章にある「Obtaining a TGT from a KDC」を参照してください。

ネットワーク サービスに対する認証の取得

ここでは、リモート ユーザが通過しなければならない 3 番めのセキュリティ レイヤについて説明します。TGT を取得したユーザは、このレイヤで Kerberos レルム内のネットワーク サービスに対して認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章の「Authenticating to Network Services」を参照してください。

Kerberos を設定する方法

Kerberos 認証済みサーバ/クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

Kerberos 設定のモニタリング

Kerberos 設定を表示するには、次のコマンドを使用します。

- **show running-config**
- **showkerberoscreds**：現在のユーザの認定証キャッシュに含まれる認定証を一覧表示します。
- **clearkerberoscreds**：転送済みの認定証を含め、現在のユーザの認定証キャッシュに含まれるすべての認定証を破棄します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セッションアウェアなネットワーキングに対するアイデンティティ コントロール ポリシーおよびアイデンティティ サービス テンプレートの設定。	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
RADIUS、TACACS+、Secure Shell、802.1x およびAAA の設定	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html
Kerberos コマンド	*Cisco IOS Security Command Reference, Release 12.4*
Kerberos 設定の例	*Cisco IOS Security Configuration Guide, Release 12.4.*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

第 60 章

ローカル認証および許可の設定

- 機能情報の確認，1395 ページ
- ローカル認証および許可の設定方法，1395 ページ
- ローカル認証および許可のモニタリング，1398 ページ
- その他の参考資料，1399 ページ

機能情報の確認

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

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

ローカル認証および許可の設定方法

スイッチのローカル認証および許可の設定

ローカル モードで AAA を実装するようにスイッチを設定すると、サーバがなくても動作するように AAA を設定できます。この場合、スイッチは認証および許可の処理を行います。この設定ではアカウンティング機能は使用できません。

（注） AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ローカル モードで AAA を実装するようにスイッチを設定して、サーバがなくても動作するように AAA を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa authentication login default local**
5. **aaa authorization exec local**
6. **aaa authorization network local**
7. **username***name* [**privilege***level*] {**password***encryption-typepassword*}
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**aaa authentication login default local** 例： スイッチ(config)# **aaa authentication login default local**	ローカル ユーザ名データベースを使用するログイン認証を設定します。**default** キーワードにより、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ 5	**aaa authorization exec local** 例： スイッチ(config)# **aaa authorization exec local**	ユーザの AAA 許可を設定し、ローカル データベースを確認して、そのユーザに EXEC シェルの実行を許可します。
ステップ 6	**aaa authorization network local** 例： スイッチ(config)# **aaa authorization network local**	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。
ステップ 7	**username***name* [**privilege***level*] {**password***encryption-typepassword*} 例： スイッチ(config)# **username your_user_name privilege 1 password 7 secret567**	ローカル データベースを入力し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 • *name* には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。 • （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type* には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 • *password* には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

SSH サーバ、統合クライアント、およびサポートされているバージョン，（1403 ページ）
TACACS+ およびスイッチ アクセス，（1317 ページ）
RADIUS およびスイッチ アクセス，（1335 ページ）
SSH を実行するためのスイッチの設定，（1405 ページ）
SSH 設定時の注意事項，（1404 ページ）

ローカル認証および許可のモニタリング

ローカル認証および許可の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

その他の参考資料

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

第 61 章

セキュア シェル（SSH）の設定

- 機能情報の確認，1401 ページ
- セキュア シェルを設定するための前提条件，1401 ページ
- セキュア シェルの設定に関する制約事項，1402 ページ
- SSH に関する情報，1403 ページ
- SSH の設定方法，1405 ページ
- SSH の設定およびステータスのモニタリング，1410 ページ
- その他の参考資料，1410 ページ

機能情報の確認

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

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

セキュア シェルを設定するための前提条件

セキュア シェル（SSH）用にスイッチを設定するための前提条件は、次のとおりです。

- SSH を動作させるには、スイッチに Rivest、Shamir、および Adleman（RSA）の公開キーと秘密キーのペアが必要です。これは SSH が必要なセキュア コピー プロトコル（SCP）も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。
- SCP はセキュリティについて SSH に依存します。
- SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。
- ユーザが SCP を使用するには適切な許可が必要です。
- 適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System（IFS）のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには **copy** コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。
- セキュア シェル（SSH）サーバは、IPsec（データ暗号規格（DES）または 3DES）の暗号化ソフトウェア イメージを必要とします。SSH クライアントは、IPsec（DES または 3DES）の暗号化ソフトウェア イメージが必要です。）
- グローバル コンフィギュレーション モードで **hostname** および **ip domain-name** コマンドを使用して、デバイスのホスト名とホスト ドメインを設定します。

関連トピック

Secure Copy Protocol（SCP），（1405 ページ）

セキュア シェルの設定に関する制約事項

セキュア シェル用にスイッチを設定するための制約事項は、次のとおりです。

- スイッチは、Rivest, Shamir, and Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、データ暗号規格（DES）（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアでのみサポートされます。DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。
- スイッチは、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES）暗号化アルゴリズムをサポートします。ただし、キーを暗号化する対称暗号化 AES はサポートされません。
- このソフトウェア リリースは、IP Security（IPSec）をサポートしていません。
- SCP を使用する場合、**copy** コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

- ログイン バナーはセキュア シェル バージョン 1 ではサポートされません。セキュア シェル バージョン 2 ではサポートされています。
- リバース SSH の代替手段をコンソール アクセス用に設定する場合、-l キーワード、userid :{number} {ip-address} デリミタ、および引数が必須です。

関連トピック

Secure Copy Protocol（SCP），（1405 ページ）

SSH に関する情報

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

SSH およびスイッチ アクセス

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

IPv6 の SSH 機能は IPv4 における機能と同じです。IPv6 の場合、SSH は IPv6 アドレスをサポートし、IPv6 トランスポート上において、リモート IPv6 ノードとのセキュリティ保護および暗号化された接続を有効化します。

SSH サーバ、統合クライアント、およびサポートされているバージョン

セキュア シェル（SSH）統合クライアント機能は、SSH プロトコル上で動作し、デバイスの認証および暗号化を実現するアプリケーションです。SSH クライアントによって、シスコ デバイスは別のシスコデバイスなど SSH サーバを実行するデバイスに対して、セキュアで暗号化された接続を実行できます。この接続は、接続が暗号化される点を除いて Telnet のアウトバウンド接続と同様の機能を提供します。SSH クライアントは、認証および暗号化により、保護されていないネットワーク上でもセキュアな通信ができます。

SSH サーバおよび SSH 統合クライアントは、スイッチ上で実行されるアプリケーションです。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。SSH クライアントは、市販の一般的な SSH サーバと連動します。SSH クライアントは、Data Encryption Standard（DES）、3DES、およびパスワード認証の暗号をサポートします。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは、SSHv1 クライアントをサポートしています。

（注） SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

ユーザ認証は、デバイスに対する Telnet セッションの認証と同様に実行されます。SSH は、次のユーザ認証方式もサポートします。

- TACACS+
- RADIUS
- ローカル認証および許可

関連トピック

スイッチのローカル認証および許可の設定，（1395 ページ）
TACACS+ およびスイッチ アクセス，（1317 ページ）
RADIUS およびスイッチ アクセス，（1335 ページ）

SSH 設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できます（逆の場合も同様です）。
- スタック マスターで SSH サーバが実行されている場合で、スタック マスターに障害が発生した場合、新しいスタック マスターでは、前のスタック マスターによって生成された RSA キー ペアが使用されます。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力した後、CLI エラーメッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。詳細については、次の関連項目を参照してください。
- RSA キーのペアを生成する場合に、メッセージ「No host name specified」が表示されることがあります。このメッセージが表示された場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

関連トピック

SSH を実行するためのスイッチの設定，（1405 ページ）

スイッチのローカル認証および許可の設定, （1395 ページ）

セキュア コピー プロトコルの概要

Secure Copy Protocol（SCP）機能は、スイッチの設定やイメージ ファイルのコピーにセキュアな認証方式を提供します。SCP にはセキュア シェル（SSH）が必要です（Berkeley の r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルです）。

SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

また、SSH には AAA 認証が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。

（注） SCP を使用する場合、copy コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

Secure Copy Protocol（SCP）

Secure Copy Protocol（SCP）機能は、スイッチの設定やスイッチ イメージ ファイルのコピーにセキュアな認証方式を提供します。SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol（RCP）と類似しています。また、SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、スイッチはユーザが正しい権限レベルを保有しているか確認する必要があります。Secure Copy 機能を設定するには、SCP の概念を理解する必要があります。

関連トピック

セキュア シェルを設定するための前提条件, （1401 ページ）

セキュア シェルの設定に関する制約事項, （1402 ページ）

SSH の設定方法

SSH を実行するためのスイッチの設定

SSH を実行するようにスイッチを設定するには、次の手順を実行します。

はじめる前に

ローカルアクセスまたはリモートアクセス用にユーザ認証を設定します。この手順は必須です。詳細については、次の関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **hostname***hostname*
4. **ip domain-name***domain_name*
5. **crypto key generate rsa**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname***hostname* 例： `スイッチ(config)# hostname your_hostname`	スイッチのホスト名および IP ドメイン名を設定します。 （注） この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
ステップ 4	**ip domain-name***domain_name* 例： `スイッチ(config)# ip domain-name your_domain`	スイッチのホスト ドメインを設定します。

	コマンドまたはアクション	目的
ステップ 5	**crypto key generate rsa** 例： スイッチ(config)# **crypto key generate rsa**	スイッチ上でローカルおよびリモート認証用に SSH サーバをイネーブルにし、RSA キー ペアを生成します。スイッチの RSA キー ペアを生成すると、SSH が自動的にイネーブルになります。 最小モジュラス サイズは、1024 ビットにすることを推奨します。 RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。 （注） この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

SSH 設定時の注意事項，（1404 ページ）
スイッチのローカル認証および許可の設定，（1395 ページ）

SSH サーバの設定

SSH サーバを設定するには、次の手順を実行します。

（注） スイッチを SSH サーバとして設定する場合にのみ、この手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sshversion** [**1** | **2**]
4. **ip ssh** {**timeout***seconds* | **authentication-retries***number*}
5. 次のいずれかまたは両方を使用します。
   - **line vty***line_number*[*ending_line_number*]
   - **transport input ssh**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sshversion** [**1**	**2**] 例： `スイッチ(config)# ip ssh version 1`	（任意）SSH バージョン 1 または SSH バージョン 2 を実行するようにスイッチを設定します。 • **1**：SSH バージョン 1 を実行するようにスイッチを設定します。 • **2**：SSH バージョン 2 を実行するようにデバイスを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。たとえば、SSH クライアント

	コマンドまたはアクション	目的
		が SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。
ステップ 4	**ip ssh** {**timeout***seconds* | **authentication-retries***number*} 例： スイッチ(config)# **ip ssh timeout 90 authentication-retries 2**	SSH 制御パラメータを設定します。 • タイムアウト値は秒単位で指定します（デフォルト値は 120 秒）。指定できる範囲は 0 ～ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続が確立されると、スイッチは CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク上の複数の CLI ベース セッション（セッション 0 ～ 4）に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントをサーバへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。
ステップ 5	次のいずれかまたは両方を使用します。 • **line vty***line_number*[*ending_line_number*] • **transport input ssh** 例： スイッチ(config)# **line vty 1 10** または スイッチ(config-line)# **transport input ssh**	（任意）仮想端末回線設定を設定します。 • ラインコンフィギュレーションモードを開始して、仮想端末回線設定を設定します。*line_number* および *ending_line_number* には、回線のペアを指定します。指定できる範囲は 0 ～ 15 です。 • スイッチで非 SSH Telnet 接続を回避するように設定します。これにより、ルータは SSH 接続に限定されます。
ステップ 6	**end** 例： スイッチ(config-line)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSH の設定およびステータスのモニタリング

次の表に、SSH サーバの設定およびステータスを示します。

表 *102*：*SSH* サーバの設定およびステータスを表示するコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セッションアウェアなネットワーキングに対するアイデンティティ コントロール ポリシーおよびアイデンティティ サービス テンプレートの設定。	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html

関連項目	マニュアル タイトル
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル

MIB

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

シスコのテクニカル サポート

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

第 62 章

SSH 認証の X.509v3 証明書

- SSH 認証の X.509v3 証明書, 1413 ページ

SSH 認証の X.509v3 証明書

SSH 認証の X.509v3 証明書 機能はサーバで X.509v3 デジタル証明書を使用し、セキュア シェル（SSH）サーバ側でユーザ認証を使用します。

このモジュールでは、デジタル証明書用のサーバおよびユーザ証明書プロファイルを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

SSH 認証の X.509v3 証明書 の前提条件

- SSH 認証機能の X.509v3 証明書では、**ip ssh server authenticate user** コマンドに代わり **ip ssh server algorithm authentication** コマンドが導入されています。**ip ssh server authenticate user** コマンドを使用すると、次の非推奨メッセージが表示されます。

```
Warning: SSH command accepted but this CLI will be deprecated soon. Please move to new
 CLI “ip ssh server algorithm authentication”. Please configure “default ip ssh server
 authenticate user” to make CLI ineffective.
```

- **default ip ssh server authenticate user** コマンドを使用して、**ip ssh server authenticate user** コマンドが動作しないようにします。こうすると、IOS セキュア シェル（SSH）サーバが **ip ssh server algorithm authentication** コマンドを使用するようになります。

SSH 認証の X.509v3 証明書 の制約事項

- SSH 認証の X.509v3 証明書機能の実装は、IOS セキュア シェル（SSH）サーバ側だけに適用されます。
- IOS SSH サーバでは、x509v3-ssh-rsa アルゴリズム ベースの証明書、および IOS SSH サーバ側でのサーバとユーザの認証のみがサポートされます。

SSH 認証の X.509v3 証明書について

デジタル証明書

認証の有効性は、署名の公開キーと署名者の ID との間の連携強度によって異なります。X.509v3 形式（RFC5280）のデジタル証明書を使用して、ID を管理できるようにします。信頼されたルート認証局とその中間認証局による一連の署名で、特定の署名の公開キーと特定のデジタル ID とがバインドされます。

Public Key Infrastructure（PKI）トラストポイントは、デジタル証明書の管理を支援します。証明書とトラストポイントとが関連付けられることで、証明書を追跡できるようになります。トラストポイントには、認証局（CA）、さまざまな ID パラメータ、デジタル証明書に関する情報が含まれています。さまざまな証明書と関連付けるために、トラストポイントは複数作成できます。

X.509v3 を使用したサーバとユーザの認証

サーバ認証では、IOS セキュア シェル（SSH）サーバは確認のため自身の証明書を SSH クライアントに送信します。このサーバ証明書は、サーバ証明書プロファイル（ssh-server-cert-profile-server コンフィギュレーション モード）で設定されているトラストポイントに関連付けられます。

ユーザ認証では、SSH クライアントは確認のため当該ユーザの証明書を IOS SSH サーバに送信します。SSH サーバは、サーバ証明書プロファイル（ssh-server-cert-profile-user コンフィギュレーション モード）で設定されている Public Key Infrastructure（PKI）トラストポイントを使用して、着信するユーザ証明書を検証します。

デフォルトでは、証明書ベースの認証は IOS SSH サーバ側でサーバおよびユーザに対して有効になります。

SSH 認証の X.509v3 証明書の設定方法

サーバ認証用のデジタル証明書を使用する IOS SSH サーバの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ip ssh server algorithm hostkey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]}
4. **ip ssh server certificate profile**
5. **server**
6. **trustpoint sign***PKI-trustpoint-name*
7. **ocsp-response include**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh server algorithm hostkey** {**x509v3-ssh-rsa** [**ssh-rsa**]	**ssh-rsa** [**x509v3-ssh-rsa**]} 例： `Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa`	ホスト キー アルゴリズムの順序を定義します。設定されたアルゴリズムのみ、Secure Shell（SSH）クライアントとネゴシエートされます。 （注） IOS SSH サーバでは、少なくとも 1 つの設定済みホスト キー アルゴリズムが必要です。 • ssh-rsa：公開キーによる認証 • x509v3-ssh-rsa：証明書ベースの認証
ステップ 4	**ip ssh server certificate profile** 例： `Device(config)# ip ssh server certificate profile`	サーバ証明書プロファイルおよびユーザ認可書プロファイルを設定し、SSH 証明書プロファイルのコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**server** 例： `Device(ssh-server-cert-profile)# server`	サーバ証明書プロファイルを設定して、SSH サーバ証明書プロファイルのサーバコンフィギュレーションモードを開始します。
ステップ 6	**trustpoint sign***PKI-trustpoint-name* 例： `Device(ssh-server-cert-profile-server)# trustpoint sign trust1`	サーバ証明書プロファイルに公開キー インフラストラクチャ（PKI）のトラストポイントをアタッチします。SSH サーバは、サーバ認証用にこの PKI トラストポイントに関連付けられた証明書を使用します。
ステップ 7	**ocsp-response include** 例： `Device(ssh-server-cert-profile-server)# ocsp-response include`	（任意）Online Certificate Status Protocol（OCSP）応答またはサーバ証明書と共に OCSP Stapling を送信します。 （注） デフォルトでは、このコマンドの「no」形式で設定され、OCSP 応答はサーバ証明書と共に送信されません。
ステップ 8	**end** 例： `Device(ssh-server-cert-profile-server)# end`	SSH サーバ証明書プロファイルのサーバコンフィギュレーションモードを終了し、特権 EXEC モードを開始します。

ユーザ認証用のユーザのデジタル証明書を検証する IOS SSH サーバの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ip ssh server algorithm authentication** {**publickey** | **keyboard** | **password**}
4. **ip ssh server algorithm publickey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]}
5. **ip ssh server certificate profile**
6. **user**
7. **trustpoint verify***PKI-trustpoint-name*
8. **ocsp-response required**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh server algorithm authentication** {**publickey** | **keyboard** | **password**} 例： `Device(config)# ip ssh server algorithm authentication publickey`	ユーザ認証アルゴリズムの順序を定義します。設定されたアルゴリズムのみ、Secure Shell（SSH）クライアントとネゴシエートされます。 （注） IOS SSH サーバでは、少なくとも 1 つの設定済みユーザ認証アルゴリズムが必要です。 （注） ユーザ認証に証明書方式を使用するには、**publickey** キーワードを設定する必要があります。 （注） **ip ssh server algorithm authentication** コマンドは、**ip ssh server authenticate user** コマンドを置き換えます。
ステップ 4	**ip ssh server algorithm publickey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]} 例： `Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa`	公開キー アルゴリズムの順序を定義します。設定されたアルゴリズムのみ、ユーザ認証のために SSH クライアントで受け入れられます。 （注） IOS SSH クライアントには、少なくとも 1 つの設定済みの公開キー アルゴリズムが必要です。 • ssh-rsa：公開キーによる認証 • x509v3-ssh-rsa：証明書ベースの認証
ステップ 5	**ip ssh server certificate profile** 例： `Device(config)# ip ssh server certificate profile`	サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイルのコンフィギュレーション モードを開始します。
ステップ 6	**user** 例： `Device(ssh-server-cert-profile)# user`	ユーザ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユーザ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	**trustpoint verify***PKI-trustpoint-name* 例： `Device(ssh-server-cert-profile-user)# trustpoint verify trust2`	受信するユーザ証明書を確認するために使用される公開キーインフラストラクチャ（PKI）のトラストポイントを設定します。 （注） 同じコマンドを複数回実行することで、複数のトラストポイントを設定します。最大 10 のトラストポイントを設定できます。
ステップ 8	**ocsp-response required** 例： `Device(ssh-server-cert-profile-user)# ocsp-response required`	（任意）受信するユーザ証明書と共に Online Certificate Status Protocol（OCSP）の応答の存在は必須です。 （注） デフォルトでは、このコマンドの「no」形式で設定され、ユーザ証明書は OCSP 応答なしで受け入れられます。
ステップ 9	**end** 例： `Device(ssh-server-cert-profile-user)# end`	SSH サーバ証明書プロファイルのユーザ設定モードを終了し、特権 EXEC モードを開始します。

サーバの設定と、デジタル証明書を使用したユーザ認証の確認

手順の概要

1. **enable**
2. **show ip ssh**

手順の詳細

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show ip ssh**
現在設定されている認証方法を表示します。証明書ベースの認証を使用していることを確認するために、x509v3 ssh rsaアルゴリズムがホスト キー アルゴリズムに設定されているようにします。

例：

```
Device# show ip ssh

SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
```

SSH 認証の X.509v3 証明書の設定例

例：サーバ認証用のデジタル証明書を使用する IOS SSH サーバの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# server
Device(ssh-server-cert-profile-server)# trustpoint sign trust1
Device(ssh-server-cert-profile-server)# exit
```

例：ユーザ認証のためのユーザのデジタル証明書を検証する IOS SSH サーバの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm authentication publickey
Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# user
Device(ssh-server-cert-profile-user)# trustpoint verify trust2
Device(ssh-server-cert-profile-user)# end
```

SSH 認証の X.509v3 証明書に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
SSH 認証	『*Secure Shell Configuration Guide*』の「Secure Shell-Configuring User Authentication Methods」の章
公開キー インフラストラクチャ（PKI）のトラストポイント	『*Public Key Infrastructure Configuration Guide*』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章

シスコのテクニカル サポート

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

SSH 認証の X.509v3 証明書 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *103*：*SSH* 認証の *X.509v3* 証明書 の機能情報

機能名	リリース	機能情報
SSH 認証の X.509v3 証明書	Cisco IOS XE リリース 3.14S	SSH 認証の X.509v3 証明書 機能はサーバで X.509v3 デジタル証明書を使用し、セキュア シェル（SSH）サーバ側でユーザ認証を使用します。 次のコマンドが導入または変更されました。 **ip ssh server algorithm hostkey**、**ip ssh server algorithm authentication**、および **ip ssh server certificate profile**

第 63 章

Secure Socket Layer HTTP の設定

- 機能情報の確認，1423 ページ
- Secure Sockets Layer（SSL）HTTP に関する情報，1423 ページ
- セキュア HTTP サーバおよびクライアントの設定方法，1427 ページ
- セキュア HTTP サーバおよびクライアントのステータスのモニタリング，1434 ページ
- その他の参考資料，1434 ページ

機能情報の確認

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

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

Secure Sockets Layer（SSL）HTTP に関する情報

セキュア HTTP サーバおよびクライアントの概要

セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。シスコが実装するセキュア HTTP サーバおよび HTTP クライアントでは、アプリケーション層の暗号化に SSL バージョン 3.0 を使用します。HTTP over SSL は、HTTPS と省略されます（セキュアな接続の場合、URL が http://の代わりに https://で始まります）。

（注） SSL は 1999 年に Transport Layer Security（TLS）に発展しましたが、このような特定のコンテキストでまだ使用されています。

セキュア HTTP サーバ（スイッチ）の主な役割は、指定のポート（デフォルトの HTTPS ポートは 443）で HTTPS 要求を待ち受けて、HTTP 1.1 Web サーバへその要求を渡すことです。HTTP 1.1 サーバはその要求を処理して、セキュア HTTP サーバへ応答（呼び出す）します。セキュア HTTP サーバは HTTP 1.1 サーバの代わりに、元の要求に応えます。

セキュア HTTP クライアント（Web ブラウザ）の主な役割は、Cisco IOS アプリケーション要求に応答して、そのアプリケーションが要求した HTTPS User Agent サービスを実行し、応答を（そのアプリケーションに）返すことです。

CA のトラストポイント

認証局（CA）は、要求を認可して参加するネットワーク デバイスに証明書を発行します。これらのサービスは、参加するデバイスに対する中央集中的なセキュリティ キーおよび証明書の管理を提供します。特定の CA サーバはトラストポイントと呼ばれます。

接続が実行されると、HTTPS サーバは、トラストポイントとなる特定の CA から得た X.509v3 の証明書を発行することで、セキュアな接続をクライアントに提供します。クライアント（通常、Web ブラウザ）は、その証明書の認証に必要な公開キーを保有しています。

セキュア HTTP 接続には、CA のトラストポイントを設定することを強く推奨します。HTTPS サーバを実行しているデバイスに CA のトラストポイントが設定されていないと、サーバは自身を認証して必要な RSA のキーのペアを生成します。自身で認証した（自己署名）証明書は適切なセキュリティではないので、接続するクライアントはその証明書が自己証明書であることを通知し、ユーザに接続の選択（確立または拒否）をさせる必要があります。この選択肢は内部ネットワーク トポロジ（テスト用など）に役立ちます。

CA のトラストポイントを設定していないと、セキュア HTTP 接続を有効にした場合、そのセキュア HTTP サーバ（またはクライアント）に対する一時的または永続的な自己署名証明書が自動的に生成されます。

- スイッチにホスト名とドメイン名が設定されてない場合、生成される自己署名証明書は一時的なものです。スイッチを再起動すると、この一時的な自己署名証明書は失われ、新たに自己署名証明書（一時的に）が割り当てられます。
- スイッチにホスト名とドメイン名が設定されている場合、生成される自己署名証明書は永続的なものです。この証明書は、スイッチを再起動しても、セキュア HTTP サーバを無効にしても有効のままです。そのため、再度セキュア HTTP 接続を有効にしたときに使用できます。

（注） 認証局およびトラストポイントは、個々のデバイスで設定する必要があります。他のデバイスからコピーすると、それらはスイッチ上で無効になります。

自己署名証明書が生成された場合、その情報は **show running-config** 特権 EXEC コマンドで出力できます。自己署名証明書を表示するコマンドの出力（show running-config コマンド）を例として一部示します。

```
スイッチ# show running-config
Building configuration...

<output truncated>

crypto pki trustpoint TP-self-signed-3080755072
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3080755072
 revocation-check none
 rsakeypair TP-self-signed-3080755072
!
!
crypto ca certificate chain TP-self-signed-3080755072
 certificate self-signed 01
  3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109
  02161743 45322D33 3535302D 31332E73 756D6D30 342D3335 3530301E 170D3933
  30333031 30303030 35395A17 0D323030 31303130 30303030 305A3059 312F302D

<output truncated>
```

自己署名証明書は、セキュア HTTP サーバを無効にして、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで削除できます。その後、セキュア HTTP サーバを再度有効にすると、自己署名証明書が新たに生成されます。

（注） *TP self-signed* の後ろに表示されている値は、デバイスのシリアル番号によって異なります。

オプションのコマンド（**ip http secure-client-auth**）を使用すると、HTTPS サーバがクライアントからの X.509v3 証明書を要求します。クライアントの認証は、サーバ自身の認証よりも高いセキュリティを提供します。

認証局の詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Configuring Certification Authority Interoperability」の章を参照してください。

CipherSuite

CipherSuite は暗号化アルゴリズムおよびダイジェスト アルゴリズムを指定して、SSL 接続に使用します。HTTPS サーバに接続すると、クライアントの Web ブラウザは、サポート対象の CipherSuite のリストを提供します。その後クライアントとサーバは、両方でサポートされている暗号化アルゴリズムで最適なものをリストから選択してネゴシエートします。たとえば、Netscape Communicator 4.76 は、米国のセキュリティ（RSA 公開キー暗号 MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC）をサポートしています。

最適な暗号化には、128 ビット暗号化をサポートするクライアント ブラウザ（Microsoft Internet Explorer バージョン 5.5 以降または Netscape Communicator バージョン 4.76 以降など）が必要です。SSL_RSA_WITH_DES_CBC_SHA CipherSuite は、128 ビット暗号化を提供しないため、他の CipherSuite よりもセキュリティが低くなります。

CipherSuite は、よりセキュリティが高く、複雑になればなるほど、わずかですが処理時間が必要になります。次に、スイッチでサポートされる CipherSuite およびルータの処理負荷（速さ）による CipherSuite のランク（速い順）を定義します。

1. SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化に DES-CBC、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換（RSA 公開キー暗号化）
2. SSL_RSA_WITH_NULL_SHA：メッセージの暗号化に NULL、およびメッセージ ダイジェストに SHA を使用したキー交換（SSL 3.0 専用）。
3. SSL_RSA_WITH_NULL_MD5：メッセージの暗号化に NULL、およびメッセージ ダイジェストに MD5 を使用したキー交換（SSL 3.0 専用）。
4. SSL_RSA_WITH_RC4_128_MD5：RC4 128 ビット暗号化、およびメッセージ ダイジェストに MD5 を使用した RSA のキー交換
5. SSL_RSA_WITH_RC4_128_SHA：RC4 128 ビット暗号化、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換
6. SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換（RSA 公開キー暗号化）
7. SSL_RSA_WITH_AES_128_CBC_SHA：AES 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。
8. SSL_RSA_WITH_AES_256_CBC_SHA：AES 256 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。
9. SSL_RSA_WITH_AES_128_CBC_SHA：AES 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。
10. SSL_RSA_WITH_AES_256_CBC_SHA：AES 256 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。

（注） Chrome の最新バージョンは 4 つの元の暗号スイートをサポートしません。そのため、Web GUI とゲスト ポータル両方へのアクセスが拒否されます。

（暗号化およびダイジェスト アルゴリズムをそれぞれ指定して組み合わせた）RSA は、SSL 接続においてキーの生成および認証の両方に使用されます。これは、CA のトラストポイントが設定されているかどうかにかかわりません。

SSL のデフォルト設定

標準の HTTP サーバはイネーブルに設定されています。

SSL はイネーブルに設定されています。

CA のトラストポイントは設定されていません。

自己署名証明書は生成されていません。

SSL の設定時の注意事項

SSL をスイッチ クラスタで使用すると、SSL セッションがクラスタ コマンダで終了します。クラスタ メンバのスイッチは標準の HTTP で動作させる必要があります。

CA のトラストポイントを設定する前に、システム クロックが設定されていることを確認してください。クロックが設定されていないと、不正な日付により証明書が拒否されます。

スイッチ スタック内のスタック マスターで、SSL セッションが強制終了されます。

セキュア HTTP サーバおよびクライアントの設定方法

CA のトラストポイントの設定

セキュア HTTP 接続には、CA のトラストポイントを正式に設定することを推奨します。CA のトラストポイントは、自己署名証明書より高いセキュリティがあります。

CA のトラストポイントを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **hostname***hostname*
3. **ip domain-name***domain-name*
4. **crypto key generate rsa**
5. **crypto ca trustpoint***name*
6. **enrollment url***url*
7. **enrollment http-proxy***host-name port-number*
8. **crlquery***url*
9. **primary** *name*
10. **exit**
11. **crypto ca authentication***name*
12. **crypto ca enroll***name*
13. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**hostname***hostname* 例： スイッチ(config)# **hostname your_hostname**	スイッチのホスト名を指定します（以前ホスト名を設定していない場合のみ必須）。ホスト名はセキュリティ キーと証明書に必要です。
ステップ 3	**ip domain-name***domain-name* 例： スイッチ(config)# **ip domain-name your_domain**	スイッチの IP ドメイン名を指定します（以前 IP ドメイン名を設定していない場合のみ必須）。IP ドメイン名はセキュリティ キーと証明書に必要です。
ステップ 4	**crypto key generate rsa** 例： スイッチ(config)# **crypto key generate rsa**	（任意）RSA キー ペアを生成します。RSA キーのペアは、スイッチの証明書を入手する前に必要です。RSA キーのペアは自動的に生成されます。必要であれば、このコマンドを使用してキーを再生成できます。
ステップ 5	**crypto ca trustpoint***name* 例： スイッチ(config)# **crypto ca trustpoint your_trustpoint**	CA のトラストポイントにローカルの設定名を指定して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 6	**enrollment url***url* 例： スイッチ(ca-trustpoint)# **enrollment url http://your_server:80**	スイッチによる証明書要求の送信先の URL を指定します。
ステップ 7	**enrollment http-proxy***host-name port-number* 例： スイッチ(ca-trustpoint)# **enrollment http-proxy your_host 49**	（任意）HTTP プロキシ サーバを経由して CA から証明書を入手するようにスイッチを設定します。 • *host-name* には、CA を取得するために使用するプロキシ サーバを指定します。 • *port-number* には、CA にアクセスするために使用するポート番号を指定します。
ステップ 8	**crlquery***url* 例： スイッチ(ca-trustpoint)# **crl query ldap://your_host:49**	ピアの証明書が取り消されていないかを確認するために、証明書失効リスト（CRL）を要求するようにスイッチを設定します。

	コマンドまたはアクション	目的
ステップ 9	**primary** *name* 例： スイッチ(ca-trustpoint)# **primary your_trustpoint**	（任意）トラストポイントが CA 要求に対してプライマリ（デフォルト）トラストポイントとして使用されるように指定します。 • *name* には、設定したトラストポイントを指定します。
ステップ 10	**exit** 例： スイッチ(ca-trustpoint)# **exit**	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto ca authentication***name* 例： スイッチ(config)# **crypto ca authentication your_trustpoint**	CA の公開キーを取得して CA を認証します。ステップ 5 で使用した名前と同じものを使用します。
ステップ 12	**crypto ca enroll***name* 例： スイッチ(config)# **crypto ca enroll your_trustpoint**	指定した CA トラストポイントから証明書を取得します。このコマンドは、各 RSA キーのペアに対して 1 つの署名入りの証明書を要求します。
ステップ 13	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

セキュア HTTP サーバの設定

セキュア HTTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

はじめる前に

証明に証明書の認証を使用する場合、前の手順を使用してスイッチの CA トラストポイントを設定してから、HTTP サーバを有効にする必要があります。CA のトラストポイントを設定していない場合、セキュア HTTP サーバを最初に有効にした時点で、自己署名証明書が生成されます。サーバを設定した後、標準およびセキュア HTTP サーバ両方に適用するオプション（パス、適用するアクセス リスト、最大接続数、またはタイムアウト ポリシー）を設定できます。

Web ブラウザを使用してセキュア HTTP 接続を確認するには、https://*URL* を入力します（URL は IPアドレス、またはサーバスイッチのホスト名）。デフォルトポート以外のポートを設定している場合、URL の後ろにポート番号も指定する必要があります。次に例を示します。

```
https://209.165.129:1026
```

または

```
https://host.domain.com:1026
```

手順の概要

1. **show ip http server status**
2. **configure terminal**
3. **ip http secure-server**
4. **ip http secure-port***port-number*
5. **ip http secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}
6. **ip http secure-client-auth**
7. **ip http secure-trustpoint***name*
8. **ip http path***path-name*
9. **ip http access-class***access-list-number*
10. **ip http max-connections***value*
11. **ip http timeout-policyidle***seconds***life***seconds***requests***value*
12. **end**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show ip http server status**
	
	例：
	
	スイッチ# **show ip http server status**
		（任意）HTTP サーバのステータスを表示して、セキュア HTTP サーバの機能がソフトウェアでサポートされているかどうかを判断します。出力で、次のラインのどちらかを確認してください。
		
		`HTTP secure server capability: Present`
		
		または
		
		`HTTP secure server capability: Not present`

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http secure-server** 例： スイッチ(config)# **ip http secure-server**	HTTPS サーバがディセーブルの場合、イネーブルにします。HTTPS サーバは、デフォルトでイネーブルに設定されています。
ステップ 4	**ip http secure-port***port-number* 例： スイッチ(config)# **ip http secure-port 443**	（任意）HTTPS サーバに使用するポート番号を指定します。デフォルトのポート番号は 443 です。443 または 1025 ～ 65535 の範囲で指定できます。
ステップ 5	**ip http secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]} 例： スイッチ(config)# **ip http secure-ciphersuite rc4-128-md5**	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これはデフォルトです。
ステップ 6	**ip http secure-client-auth** 例： スイッチ(config)# **ip http secure-client-auth**	（任意）HTTP サーバを設定して、接続処理の間、認証のために、クライアントからの X.509v3 証明書を要求します。デフォルトでは、クライアントがサーバからの証明書を要求する設定になっていますが、サーバはクライアントを認証しないようになっています。
ステップ 7	**ip http secure-trustpoint***name* 例： スイッチ(config)# **ip http secure-trustpoint your_trustpoint**	X.509v3 セキュリティ証明書の取得およびクライアントの証明書接続の認証に使用する CA のトラストポイントを指定します。 （注） このコマンドの使用は、前の手順に従って CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。
ステップ 8	**ip http path***path-name* 例： スイッチ(config)# **ip http path /your_server:80**	（任意）HTML ファイルのベースとなる HTTP パスを設定します。パスは、ローカル システムにある HTTP サーバ ファイルの場所を指定します（通常、システムのフラッシュ メモリを指定します）。

	コマンドまたはアクション	目的
ステップ 9	**ip http access-class***access-list-number* 例： スイッチ(config)# **ip http access-class 2**	（任意）HTTP サーバへのアクセスの許可に使用するアクセス リストを指定します。
ステップ 10	**ip http max-connections***value* 例： スイッチ(config)# **ip http max-connections 4**	（任意）HTTP サーバへの同時最大接続数を指定します。値は 10 以上にすることを推奨します。これは、UI が想定どおりに機能するために必要な値です。
ステップ 11	**ip http timeout-policyidle***seconds***life***seconds***requests***value* 例： スイッチ(config)# **ip http timeout-policy idle 120 life 240 requests 1**	（任意）指定の状況下における、HTTP サーバへの接続最大時間を指定します。 • **idle**：データの受信がないか、応答データが送信できない場合の最大時間。指定できる範囲は 1 ～ 600 秒です。デフォルト値は 180 秒（3 分）です。 • **life**：接続を確立している最大時間です。指定できる範囲は 1 ～ 86400 秒（24 時間）です。デフォルト値は 180 秒です。 • **requests**：永続的な接続で処理される要求の最大数。最大値は 86400 です。デフォルトは 1 です。
ステップ 12	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

セキュア HTTP クライアントの設定

セキュア HTTP クライアントを設定するには、特権 EXEC モードで次の手順を実行します。

はじめる前に

標準の HTTP クライアントおよびセキュア HTTP クライアントは常にイネーブルです。証明書の認証にはセキュア HTTP クライアントの証明書が必要です。次の手順では、前の手順で CA のトラストポイントをスイッチに設定していることを前提にしています。CA のトラストポイントが設定されておらず、リモートの HTTPS サーバがクライアントの認証を要求した場合、セキュア HTTP クライアントへの接続は失敗します。

手順の概要

1. **configureterminal**
2. **ip http client secure-trustpoint***name*
3. **ip http client secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip http client secure-trustpoint***name* 例： スイッチ(config)# **ip http client secure-trustpoint your_trustpoint**	（任意）リモートの HTTP サーバがクライアント認証を要求した場合に使用する、CA のトラストポイントを指定します。このコマンドの使用は、前の手順を使用して CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。クライアント認証が必要ない場合、またはプライマリのトラストポイントがすでに設定されている場合は、このコマンドは任意です。
ステップ 3	**ip http client secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]} 例： スイッチ(config)# **ip http client secure-ciphersuite rc4-128-md5**	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これはデフォルトです。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

セキュア HTTP サーバおよびクライアントのステータスのモニタリング

SSL セキュア サーバおよびクライアントのステータスをモニタするには、次の表の特権 EXEC コマンドを使用します。

表 *104* : *SSL* セキュア サーバおよびクライアントのステータスを表示するコマンド

コマンド	目的
show ip http client secure status	セキュア HTTP クライアントの設定を表示します。
show ip http server secure status	セキュア HTTP サーバの設定を表示します。
show running-config	セキュア HTTP 接続に対して生成された自己署名証明書を表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セッションアウェアなネットワーキングに対するアイデンティティ コントロール ポリシーおよびアイデンティティ サービス テンプレートの設定。	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル

MIB

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

シスコのテクニカル サポート

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

第 64 章

IPv4 ACL の設定

- 機能情報の確認，1437 ページ
- IPv4 アクセス コントロール リストを設定するための前提条件，1437 ページ
- IPv4 アクセス コントロール リストの設定に関する制約事項，1438 ページ
- ACL によるネットワーク セキュリティに関する情報，1439 ページ
- ACL の設定方法，1454 ページ
- IPv4 ACL のモニタリング，1478 ページ
- ACL の設定例，1479 ページ
- その他の参考資料，1494 ページ

機能情報の確認

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

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

IPv4 アクセス コントロール リストを設定するための前提条件

ここでは、アクセス コントロール リスト（ACL）によるネットワーク セキュリティの設定の前提条件を示します。

- LAN ベース フィーチャ セットが実行しているスイッチでは、VLAN マップはサポートされません。

IPv4 アクセス コントロール リストの設定に関する制約事項

一般的なネットワーク セキュリティ

次は、ACL によるネットワーク セキュリティの設定の制約事項です。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。インターフェイスのパケット フィルタおよびルート フィルタ用の ACL では、名前を使用できます。また、VLAN マップでも名前を指定できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- **appletalk** は、コマンドラインのヘルプ ストリングに表示されますが、**deny** および **permit** MAC アクセス リスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。

IPv4 ACL ネットワーク インターフェイス

次の制限事項が、ネットワーク インターフェイスへの IPv4 ACL に適用されます。

- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2（ポート）ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。
- レイヤ 3 インターフェイスに ACL が適用され、スイッチ上でルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。
- レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。

（注） パケットがレイヤ 3 インターフェイスのアクセス グループによって拒否された場合、デフォルトでは、ルータは ICMP 到達不能メッセージを送信します。アクセスグループによって拒否されたこれらのパケットはハードウェアでドロップされず、スイッチの CPU にブリッジングされて、ICMP 到達不能メッセージを生成します。ポート ACL は ICMP 到達不能メッセージを生成しません。 ICMP 到達不能メッセージは、ルータ ACL で **no ip unreachables** インターフェイス コマンドを使用してディセーブルにできます。

レイヤ 2 インターフェイスの MAC ACL

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に留意してください。

- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

（注） **mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用される場合のみ有効です。このコマンドは、EtherChannel ポート チャネルでは使用できません。

IP アクセス リスト エントリ シーケンス番号

- この機能は、ダイナミック アクセス リスト、再帰アクセス リスト、またはファイアウォール アクセス リストをサポートしていません。

関連トピック

インターフェイスへの IPv4 ACL の適用, （1467 ページ）
IPv4 ACL のインターフェイスに関する注意事項, （1453 ページ）
名前付き MAC 拡張 ACL の作成, （1469 ページ）
レイヤ 2 インターフェイスへの MAC ACL の適用, （1471 ページ）

ACL によるネットワーク セキュリティに関する情報

この章では、アクセス コントロール リスト（ACL）を使用して、スイッチのネットワーク セキュリティを設定する方法について説明します。コマンドや表では、ACL をアクセス リストと呼ぶこともあります。

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACL はルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスまたは VLAN（仮想 LAN）でパケットを許可、または拒否します。ACL は、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。パケットがインターフェイスに着信すると、スイッチはパケット内の

フィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。スイッチは、VLAN 内でブリッジングされるパケットを含めて、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ 3 スイッチにアクセスリストを設定します。ACL を設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラフィックの種類を決定したりできます。たとえば、電子メール トラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。ACL を着信トラフィック、発信トラフィック、またはその両方をブロックするように設定することもできます。

アクセス コントロール エントリ

ACL には、アクセス コントロール エントリ（ACE）の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

ACL でサポートされるタイプ

スイッチは、IP ACL とイーサネット（MAC）ACL をサポートしています。

- IP ACL は、TCP、ユーザ データグラム プロトコル（UDP）、インターネット グループ管理プロトコル（IGMP）、およびインターネット制御メッセージ プロトコル（ICMP）などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

このスイッチは、Quality of Service（QoS）分類 ACL もサポートしています。

サポートされる ACL

スイッチでは、トラフィックをフィルタリングするために、次に示す 3 種類の ACL がサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。レイヤ 2 インターフェイスに適用できるのは IP アクセス リストを 1 つと MAC アドレス リストを 1 つだけです。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御し、レイヤ 3 インターフェイスで特定の方向（着信または発信）に適用されます。

- VLAN ACL または VLAN マップは、すべてのパケット（ブリッジドパケットおよびルーテッド パケット）のアクセスを制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。VLAN マップは、IPv4 のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されています。イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプロトコルがアクセス コントロールされます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケット（ルーテッドパケットまたはブリッジドパケット）が VLAN マップと照合されます。パケットは、スイッチ ポートを介して、または、ルーティングされたパケットの場合、ルーテッド ポートを介して、VLAN に入ることができます。

ACL 優先順位

VLAN マップ、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、フィルタの優先順位（最大から最小）はポート ACL、ルータ ACL、次に VLAN マップです。次の例で、簡単な使用例を説明します。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- スイッチ仮想インターフェイス（SVI）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。
- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

関連トピック

IPv4 アクセス コントロール リストの設定に関する制約事項, （1438 ページ）

ポート ACL

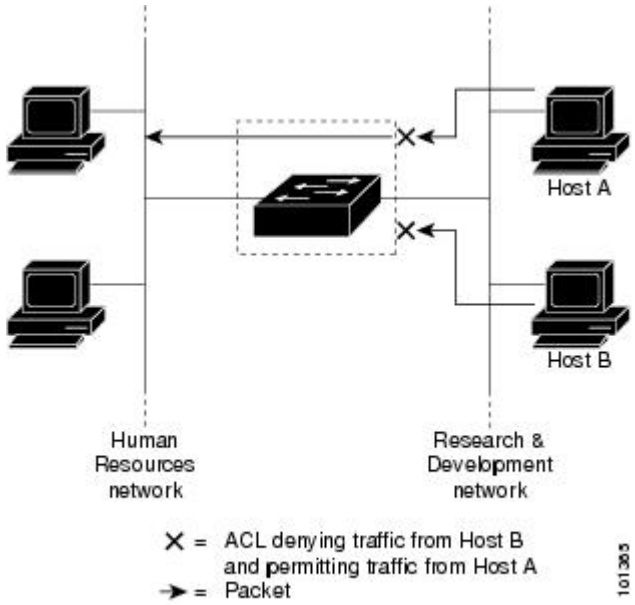
ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL を使用できるのは、物理インターフェイスだけです。EtherChannel インターフェイスでは使用できません。ポート ACL は、アウトバウンドおよびインバウンド方向のインターフェイスに適用できます。次のアクセス リストがサポートされています。

- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイス上の ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。

次に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマン リソース ネットワークにアクセスすることを許可しますが、ホスト B が同一のネットワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2 インターフェイスだけに適用できます。

図 *67* : *ACL* によるネットワーク内のトラフィックの制御



ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。

（注） レイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスであるスイッチ仮想インターフェイス（SVI）、物理層 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

スイッチは、IPv4 トラフィックの次のアクセス リストをサポートしています。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチはインターフェイスに設定されている機能に関連付けられている ACL が照合されます。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。パケットがルーティングされてからネクスト ホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセス コントロールが行えます。

VLAN マップ

VLAN ACL または VLAN マップを使用して、すべてのトラフィックをアクセス コントロールできます。VLAN との間でルーティングされる、またはスイッチまたはスイッチ スタックの VLAN 内でブリッジングされるすべてのパケットに、VLAN マップを適用します。

VLAN マップはセキュリティ パケット フィルタリングに使用してください。VLAN マップで方向（着信または発信）は定義されません。

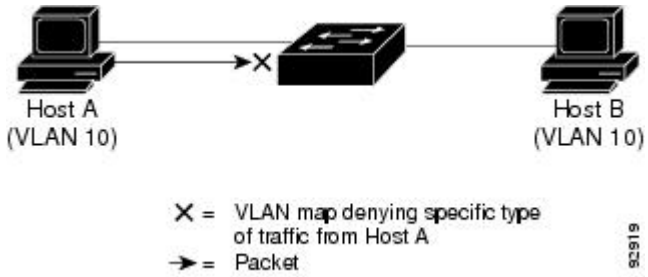
VLAN マップを設定して、IPv4 トラフィックのレイヤ 3 アドレスを照合できます。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます（IP トラフィックは、MAC VACL マップではアクセス制御されません）。VLAN マップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

次に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用できます。

図 *68*：*VLAN* マップによるトラフィックの制御



ACE およびフラグメント化されるトラフィックとフラグメント化されていないトラフィック

IP パケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

アクセス コントロール エントリ（ACE）には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ 4 情報が含まれておらず、ACE が一部のレイヤ 4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報（TCP や UDP などのプロトコル タイプを含む）をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。
- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例

次のコマンドで構成され、フラグメント化された 3 つのパケットに適用されるアクセス リスト 102 を例に取って説明します。

```
スイッチ(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
スイッチ(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
スイッチ(config)# access-list 102 permit tcp any host 10.1.1.2
スイッチ(config)# access-list 102 deny tcp any any
```

（注） 最初の 2 つの ACE には宛先アドレスの後に *eq* キーワードがありますが、これは既知の TCP 宛先ポート番号がそれぞれシンプル メール転送プロトコル（SMTP）および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE（permit）と一致します。残りのフラグメントも最初の ACE と一致します。これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ 3 情報だけをチェックするからです。この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです。
- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて揃っているため、最初のフラグメントが 2 つめの ACE（deny）と一致します。残りのフラグメントは、レイヤ 4 情報が含まれていないため、2 つめの ACE と一致しません。残りのフラグメントは 3 つめの ACE（permit）と一致します。

  最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。
- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE（deny）と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

ACL とスイッチ スタック

スイッチ スタックの ACL サポートは、スタンドアロン スイッチと同じです。ACL の構成情報は、スタック内のすべてのスイッチに送信されます。アクティブ スイッチを含むスタック内のすべてのスイッチでは、情報が処理され、ハードウェアがプログラムされます

アクティブ スイッチおよびACLの機能

アクティブ スイッチにより、次の ACL 機能が実行されます。

- ACL 構成情報が処理され、情報がすべてのスタック メンバに送信されます。
- ACL 情報は、スタックに加入しているすべてのスイッチに配信されます。
- （たとえば、十分なハードウェア リソースがないなど）何らかの理由で、ソフトウェアによってパケットが送信される必要がある場合、ACLをパケットに適用後にのみ、アクティブ スイッチによってパケットが転送されます。
- そのハードウェアは、処理する ACL 情報でプログラムされます。

スタック メンバおよびACLの機能

スタック メンバにより、次の ACL 機能が実行されます。

- スタック メンバでは、アクティブ スイッチから ACL 情報を受信し、ハードウェアがプログラムされます。
- スタンバイ スイッチとして設定されたスタック メンバがアクティブ スイッチが失敗したイベント内のアクティブ スイッチ機能を実行します。

アクティブ スイッチの障害およびACL

アクティブとスタンバイの両方のスイッチに ACL 情報があります。アクティブ スイッチに障害が発生すると、スタンバイが役割を引き継ぎます。新しいアクティブ スイッチにより、すべてのスタック メンバーに ACL 情報が配信されます。

標準IPv4 ACLおよび拡張IPv4 ACL

ここでは、IP ACL について説明します。

ACLは、許可条件と拒否条件の順序付けられた集まりです。スイッチは、アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致する最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、IPv4 について次の ACL（アクセス リスト）をサポートします。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることもできます。

IPv4 ACL スイッチでサポートされていない機能

このスイッチで IP v4ACL を設定する手順は、他の Cisco スイッチやルータで IP v4ACL を設定する手順と同じです。

以下の ACL 関連の機能はサポートされていません。

- 非 IP プロトコル ACL
- IP アカウンティング
- 再帰 ACL およびダイナミック ACL はサポートされていません。

アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。

次の一覧に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト（1 ～ 199 および 1300 ～ 2699）をサポートします。

表 *105*：アクセス リスト番号

アクセス リスト番号	タイプ	サポートあり
1 ～ 99	IP 標準アクセス リスト	Yes
100 ～ 199	IP 拡張アクセス リスト	Yes
200 ～ 299	プロトコル タイプコード アクセス リスト	No
300 ～ 399	DECnet アクセス リスト	No
400 ～ 499	XNS 標準アクセス リスト	No
500 ～ 599	XNS 拡張アクセス リスト	No
600 ～ 699	AppleTalk アクセス リスト	No
700 ～ 799	48 ビット MAC アドレス アクセス リスト	No
800 ～ 899	IPX 標準アクセス リスト	No
900 ～ 999	IPX 拡張アクセス リスト	No
1000 ～ 1099	IPX SAP アクセス リスト	No
1100 ～ 1199	拡張 48 ビット MAC サマリー アドレス アクセス リスト	No

アクセス リスト番号	タイプ	サポートあり
1200 ～ 1299	IPX サマリー アドレス アクセス リスト	No
1300 ～ 1999	IP 標準アクセス リスト（拡張範囲）	Yes
2000 ～ 2699	IP 拡張アクセス リスト（拡張範囲）	Yes

番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

番号付き標準 IPv4 ACL

ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

スイッチは、**host** 一致条件があるエントリと *don't care* マスク 0.0.0.0 を含む一致条件があるエントリがリストの先頭に移動し、0 以外の *don't care* マスクを含むエントリよりも前に位置するように、標準アクセス リストの順序を書き換えます。そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号付き標準 IPv4 ACL を VLAN、端末回線、またはインターフェイスに適用できます。

番号付き拡張 IPv4 ACL

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

このスイッチは、ダイナミックまたはリフレクシブ アクセス リストをサポートしていません。また、タイプ オブ サービス（ToS）の minimize-monetary-cost ビットに基づくフィルタリングもサポートしていません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

拡張 TCP、UDP、ICMP、IGMP、またはその他の IP ACL を定義できます。また、このスイッチはこれらの IP プロトコルをサポートします。

（注） ICMP エコー応答はフィルタリングできません。他の ICMP コードまたはタイプは、すべてフィルタリングできます。

これらの IP プロトコルがサポートされます。

- 認証ヘッダー プロトコル（**ahp**）
- 暗号ペイロード（**esp**）
- Enhanced Interior Gateway Routing Protocol（**eigrp**）
- 総称ルーティング カプセル化（**gre**）
- インターネット制御メッセージ プロトコル（**icmp**）
- インターネット グループ管理プロトコル（**igmp**）
- すべての内部プロトコル（**ip**）
- IP in IP トンネリング（**ipinip**）
- KA9Q NOS 互換 IP over IP トンネリング（**nos**）
- Open Shortest Path First ルーティング（**ospf**）
- ペイロード圧縮プロトコル（**pcp**）
- プロトコル独立型マルチキャスト（**pim**）
- 伝送制御プロトコル（**tcp**）
- ユーザ データグラム プロトコル（**udp**）

名前付き IPv4 ACL

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング（名前）を使用できます。名前付き ACL を使用すると、ルータ上で番号付きアクセス リストの場合より多くの IPv4 アクセス リストを設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付きアクセス リストで使用できるわけではありません。

（注） 標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。標準 IP ACL の名前は 1 ～ 99 で、。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定するときには、次の注意事項に留意してください。

- また、番号付き ACL も使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。

ACL ロギング

標準 IP アクセス リストによって許可または拒否されたパケットに関するログ メッセージが、スイッチのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、syslog メッセージを管理する **logging console** コマンドで管理されます。

（注） ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可（*permit*）または拒否（*deny*）ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

（注） ロギング メッセージが多すぎて処理できない場合、または 1 秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作によって、ロギング パケットが多すぎてルータがクラッシュすることを回避します。そのため、課金ツールや、アクセス リストと一致する数の正確な情報源としてロギング設備をを使用しないでください。

ハードウェアおよびソフトウェアによる IP ACL の処理

ACL 処理はハードウェアで実行されます。ハードウェアで ACL の設定を保存する領域が不足すると、そのインターフェイス上のすべてのパケットがドロップします。

（注） スイッチまたはスタック メンバーのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受けるのは、スイッチに着信した該当 VLAN 内のトラフィックだけです。

show ip access-lists 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。スイッチド パケットおよびルーテッド パケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、 特権 EXEC コマンドを使用します。

VLAN マップの設定時の注意事項

VLAN マップは、VLAN 内でフィルタリングを制御する唯一の方法です。VLAN マップには方向の指定がありません。VLAN マップを使用して、特定の方向のトラフィックをフィルタリングす

るには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。VLAN マップ内に該当パケット タイプ（IP または MAC）に対する match 句がある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットはドロップされます。該当パケット タイプに対する match コマンドがない場合、デフォルトでは、パケットが転送されます。

次は、VLAN マップ設定の注意事項です。

- インターフェイスでトラフィックを拒否するように設定された ACL がなく、VLAN マップが設定されていない場合、すべてのトラフィックが許可されます。
- 各 VLAN マップは一連のエントリで構成されます。VLAN マップのエントリの順序は重要です。スイッチに着信したパケットは、VLAN マップの最初のエントリに対してテストされます。一致した場合は、VLAN マップのその部分に指定されたアクションが実行されます。一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。
- 該当パケット タイプ（IP または MAC）に対する match 句が VLAN マップに 1 つまたは複数ある場合でも、パケットがそれらの match 句に一致しない場合、デフォルトではパケットがドロップされます。該当パケット タイプに対する match 句が VLAN マップ内にない場合、デフォルトではパケットが転送されます。
- VLAN マップのロギングはサポートされていません。
- レイヤ 2 インターフェイスに適用された IP アクセス リストまた MAC アクセス リストがスイッチにあって、ポートが属する VLAN に VLAN マップを適用する場合、ポート ACL が VLAN マップに優先します。
- ハードウェアに VLAN マップの設定を適用できない場合は、その VLAN 内のすべてのパケットがドロップします。

VLAN マップとルータ ACL

ブリッジングされたトラフィックおよびルーティングされたトラフィックの両方に対してアクセス コントロールを行うには、VLAN マップを単独で使用するか、またはルータ ACL と VLAN マップを組み合わせて使用します。入力と出力両方のルーテッド VLAN インターフェイスでルータ ACL を定義したり、ブリッジングされたトラフィックのアクセスをコントロールする VLAN マップを定義したりできます。

パケット フローが ACL 内 VLAN マップの deny ステートメントと一致した場合、ルータ ACL の設定に関係なく、パケット フローは拒否されます。

（注） ルータ ACL を VLAN マップと組み合わせて使用し、ルータ ACL でのロギングを必要とするパケットが VLAN マップで拒否された場合、これらのパケットはロギングされません。

該当パケット タイプ（IP または MAC）に対する match 句が VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトではパケットがドロップされます。VLAN マップ内に match 句がなく、アクションが指定されていない場合、どの VLAN マップ エントリとも一致しないパケットは転送されます。

VLAN マップとルータ ACL の設定時の注意事項

ここに記載された注意事項は、ルータ ACL および VLAN マップを同じ VLAN 上で使用する必要がある設定に適用されます。ルータ ACL および VLAN マップを異なる VLAN に割り当てる設定には、これらの注意事項は適用されません。

ルータ ACL および VLAN マップを同じ VLAN に設定する必要がある場合は、ルータ ACL と VLAN マップの両方の設定に関し、ここで説明する注意事項に従ってください。

- VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつに限り設定できます。
- 可能な限り、すべてのエントリのアクションが同一で、末尾のデフォルトアクションだけが反対のタイプとなるように ACL を記述します。次のいずれかの形式を使用して、ACL を記述します。

  permit... permit... permit... deny ip any any

  または

  deny... deny... deny... permit ip any any

- ACL 内で複数のアクション（許可、拒否）を定義する場合は、それぞれのアクション タイプをまとめて、エントリ数を削減します。
- ACL 内にレイヤ 4 情報を指定しないでください。レイヤ 4 情報を追加すると、統合プロセスが複雑になります。ACL のフィルタリングが、full-flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）でなく、IP アドレス（送信元および宛先）に基づいて行われる場合に、最適な統合結果が得られます。可能な限り、IP アドレスには *don't care* ビットを使用してください。

  IP ACE とレイヤ 4 情報を含む TCP/UDP/ICMP ACE が両方とも ACL 内に存在し、full-flow モードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

ACL の時間範囲

time-range グローバル コンフィギュレーション コマンドを使用することによって、時刻および曜日に基づいて拡張 ACL を選択的に適用できます。まず、時間範囲の名前を定義し、その時間範囲内の時刻および日付または曜日を設定します。次に、ACL を適用してアクセス リストに制限を設定するときに時間範囲を入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間（指定期間内や指定曜日など）を定義できます。**time-range** キーワードおよび引数については、名前付きおよび番号付き拡張 ACL タスクの表を参照してください。

時間範囲を使用するいくつかの利点を次に示します。

- アプリケーションなどのリソース（IP アドレスとマスクのペア、およびポート番号で識別）へのユーザ アクセスをより厳密に許可または拒否できます。

- ログ メッセージを制御できます。ACL エントリを使用して特定の時刻に関してのみトラフィックをロギングできるため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセス リストを使用すると、CPUに負荷が生じます。これは、アクセス リストの新規設定を他の機能や、ハードウェア メモリにロードされた結合済みの設定とマージする必要があるためです。そのため、複数のアクセス リストが短期間に連続して（互いに数分以内に）有効となるような設定とならないように注意する必要があります。

（注） 時間範囲は、スイッチのシステム クロックに基づきます。したがって、信頼できるクロック ソースが必要です。ネットワーク タイム プロトコル（NTP）を使用してスイッチ クロックを同期させることを推奨します。

関連トピック

ACL の時間範囲の設定, （1464 ページ）

IPv4 ACL のインターフェイスに関する注意事項

ip access-group インターフェイス コンフィギュレーション コマンドをレイヤ 3 インターフェイス（SVI、レイヤ 3 EtherChannel、またはルーテッド ポート）に適用するには、そのインターフェイスに IP アドレスが設定されている必要があります。レイヤ 3 アクセス グループは、CPU のレイヤ 3 プロセスによってルーティングまたは受信されるパケットをフィルタリングします。このグループは、VLAN 内でブリッジングされるパケットに影響を与えません。

着信 ACL の場合、パケットの受信後スイッチはパケットを ACL と照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

発信ACLの場合、パケットを受信し制御対象インターフェイスにルーティングしたあと、スイッチはパケットを ACL と照合します。ACL がパケットを許可した場合は、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスのACLまたは発信インターフェイスの ACL のいずれであっても、常に入力インターフェイスから ICMP 到達不能メッセージが送信されます。ICMP 到達不能メッセージは通常、入力インターフェイス 1 つにつき、0.5 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

関連トピック

インターフェイスへの IPv4 ACL の適用, （1467 ページ）
IPv4 アクセス コントロール リストの設定に関する制約事項, （1438 ページ）

ACL の設定方法

IPv4 ACL の設定

このスイッチで IP ACL を使用する手順は次のとおりです。

手順の概要

1. アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。
2. その ACL をインターフェイスまたは端末回線に適用します。標準および拡張 IP ACL を VLAN マップに適用することもできます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。	
ステップ 2	その ACL をインターフェイスまたは端末回線に適用します。標準および拡張 IP ACL を VLAN マップに適用することもできます。	

番号付き標準 ACL の作成

番号付き標準 ACL を作成するには、次の手順に従ってください。

手順の概要

1. **enable**
2. **configureterminal**
3. **access-list***access-list-number* {**deny** | **permit**} *source source-wildcard*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list***access-list-number* {**deny** | **permit**} *source source-wildcard*] 例： スイッチ(config)# **access-list 2 deny your_host**	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。 *access-list-number* には、1 ～ 99 または 1300 ～ 1999 の 10 進数値を指定します。 条件が一致した場合にアクセスを拒否する場合は **deny**、許可する場合は **permit** を指定します。 *source* には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • キーワード **any** は 0.0.0.0 255.255.255.255 という *source* および *source-wildcard* の省略形です。source-wildcard を入力する必要はありません。 • キーワード **host** は送信元および *source* 0.0.0.0 の *source-wildcard* の省略形です。 （任意）*source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 （注） ロギングは、レイヤ 3 インターフェイスに割り当てられた ACL でだけサポートされます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

VLAN マップの設定，（1473 ページ）

番号付き拡張 ACL の作成

番号付き拡張 ACL を作成するには、次の手順に従ってください。

手順の概要

1. **configureterminal**
2. **access-list***access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence***precedence*] [**tos** tos] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*]
3. **access-list***access-list-number* {**deny** | **permit**} **tcp***sourcesource-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**established**] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*] [*flag*]
4. **access-list***access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*]
5. **access-list***access-list-number* {**deny** | **permit**} **icmp***sourcesource-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**time-range***time-range-name*] [**dscp***dscp*]
6. **access-list***access-list-number* {**deny** | **permit**} **igmp***sourcesource-wildcard destination destination-wildcard* [*igmp-type*] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list***access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence***precedence*] [**tos** tos] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*] 例： スイッチ(config)# **access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log**	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 *access-list-number* には、100 ～ 199 または 2000 ～ 2699 の 10 進数を指定します。 条件が一致した場合にパケットを拒否する場合は **deny**、許可する場合は **permit** を指定します。 *protocol* には、IP プロトコルの名前または番号を指定します。**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、または **udp**、あるいは IP プロトコル番号を表す 0 ~ 255 の範囲の整数を使用できます。一致条件としてインターネット プロトコル（ICMP、TCP、UDP など）を指定するには、キーワード **ip** を使用します。 （注） この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加の特定パラメータについては、次のステップを参照してください。 *source* には、パラメータの送信元であるネットワークまたはホストの番号を指定します。 *source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 *destination* には、パラメータの宛先であるネットワークまたはホストの番号を指定します。 *destination-wildcard* は、ワイルドカード ビットを宛先アドレスに適用します。 source、source-wildcard、destination、および destination-wildcard の値は、次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード **any**。 • 単一のホスト 0.0.0.0 を表すキーワード **host**。 その他のキーワードはオプションであり、次の意味を持ちます。 • **precedence**：パケットを 0 ～ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、**routine**（0）、

	コマンドまたはアクション	目的
		priority（1）、**immediate**（2）、**flash**（3）、**flash-override**（4）、**critical**（5）、**internet**（6）、**network**（7）です。 • **fragments**：2 つ目以降のフラグメントをチェックする場合に入力します。 • **tos**：パケットを 0 ～ 15 の番号または名前で指定するサービス タイプ レベルと一致させる場合に入力します。指定できる値は、**normal**（0）、**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）です。 • **log**：エントリと一致するパケットに関するログ通知メッセージを作成し、コンソールに送信します。**log-input** を指定すると、ログ エントリに入力インターフェイスが追加されます。 • **time-range**：時間範囲名を指定します。 • **dscp**：0 ～ 63 の番号で指定された DSCP 値を使用してパケットを照合します。疑問符（?）を使用すると、使用可能な値のリストが表示されます。 （注） **dscp** 値を入力した場合、**tos** または **precedence** は入力できません。**dscp** を入力しない場合は、**tos** と **precedence** 値の両方を入力できます。
ステップ 3	**access-list***access-list-number* {**deny** | **permit**} **tcp***sourcesource-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**established**] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*] [*flag*] 例： `スイッチ(config)# access-list 101 permit tcp any any eq 500`	拡張 TCP アクセス リストおよびアクセス条件を定義します。 次に示す例外を除き、拡張 IPv4 ACL に対して説明するパラメータと同じパラメータを使用します。 （任意）*operator* および *port* を入力すると、送信元ポート（*source source-wildcard* の後に入力した場合）または宛先ポート（*destination destination-wildcard* の後に入力した場合）が比較されます。使用可能な演算子は、**eq**（等しい）、**gt**（より大きい）、**lt**（より小さい）、**neq**（等しくない）、**range**（包含範囲）などです。演算子にはポート番号を指定する必要があります（range の場合は 2 つのポート番号をスペースで区切って指定する必要があります）。 *port* には、10 進数（0 ～ 65535）のポート番号または TCP ポート名を入力します。TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。 他のオプションのキーワードの意味は次のとおりです。 • **established**：確立された接続と照合する場合に入力します。このキーワードは、**ack** または **rst** フラグでの照合と同じ機能を果たします。

	コマンドまたはアクション	目的
		• *flag*：指定された TCP ヘッダー ビットを基準にして照合します。入力できるフラグは、**ack**（確認応答）、**fin**（終了）、**psh**（プッシュ）、**rst**（リセット）、**syn**（同期）、または **urg**（緊急）です。
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*] 例： `スイッチ(config)# access-list 101 permit udp any any eq 100`	（任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。 UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[operator [port]] ポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP では、**flag** および **established** キーワードは無効です。
ステップ 5	**access-list***access-list-number* {**deny** | **permit**} **icmp***sourcesource-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**time-range***time-range-name*] [**dscp***dscp*] 例： `スイッチ(config)# access-list 101 permit icmp any any 200`	拡張 ICMP アクセス リストおよびアクセス条件を定義します。 ICMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-code*：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。
ステップ 6	**access-list***access-list-number* {**deny** | **permit**} **igmp***sourcesource-wildcard destination destination-wildcard* [*igmp-type*] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*] 例： `スイッチ(config)# access-list 101`	（任意）拡張 IGMP アクセス リストおよびアクセス条件を定義します。 IGMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。 *igmp-type*：IGMP メッセージ タイプと照合するには、0 ～ 15 の番号を入力するか、またはメッセージ名である **dvmrp**、**host-query**、**host-report**、**pim**、または **trace** を入力します。

	コマンドまたはアクション	目的
	permit igmp any any 14	
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

VLAN マップの設定, （1473 ページ）

名前付き標準 ACL の作成

名前を使用して標準 ACL を作成するには、次の手順に従ってください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip access-list standard***name*
4. 次のいずれかを使用します。
   - **deny** {*source* [*source-wildcard*] | **host***source* | **any**} [**log**]
   - **permit** {*source* [*source-wildcard*] | **host***source* | **any**} [**log**]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list standard***name* 例： スイッチ(config)# **ip access-list standard 20**	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、1 ～ 99 の番号を使用できます。
ステップ 4	次のいずれかを使用します。 • **deny** {*source* [*source-wildcard*] | **host***source* | **any**} [**log**] • **permit** {*source* [*source-wildcard*] | **host***source* | **any**} [**log**] 例： スイッチ(config-std-nacl)# **deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255** または スイッチ(config-std-nacl)# **permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0**	アクセス リスト コンフィギュレーション モードで、パケットを転送するのかドロップするのかを決定する 1 つ以上の拒否条件または許可条件を 指定します。 • **host***source*：*source* 0.0.0.0.0.0.0.0 の送信元および送信元ワイルドカード。 • **any**：source および source wildcard の値 0.0.0.0 255.255.255.255。
ステップ 5	**end** 例： スイッチ(config-std-nacl)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的

名前付き拡張 ACL の作成

名前を使用して拡張 ACL を作成するには、次の手順に従ってください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip access-list extended***name*
4. {**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host***source* | **any**} {*destination* [*destination-wildcard*] | host *destination* | **any**} [**precedence***precedence*] [**tos***tos*] [**established**] [**log**] [**time-range***time-range-name*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list extended***name* 例： `スイッチ(config)# ip access-list extended 150`	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、100 ～ 199 の番号を使用できます。

	コマンドまたはアクション	目的
ステップ 4	{**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host***source* | **any**} {*destination* [*destination-wildcard*] | host *destination* | **any**} [**precedence***precedence*] [**tos***tos*] [**established**] [**log**] [**time-range***time-range-name*] 例： `スイッチ(config-ext-nacl)# permit 0 any any`	アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。**log** キーワードを使用して、違反を含む、アクセス リスト ロギング メッセージを取得します。 • **host***source*：*source* 0.0.0.0.0.0.0.0 の送信元および送信元ワイルドカード。 • **host***destintation*：*destination* 0.0.0.0 の宛先および宛先ワイルドカード • **any**：source および source wildcard の値または destination および destination wildcard の値である 0.0.0.0 255.255.255.255
ステップ 5	**end** 例： `スイッチ(config-ext-nacl)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、関連付けられた IP ホスト アドレス アクセス リストの指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に選択的に追加できません。ただし、**no permit** および **no deny** アクセス リスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

次の作業

作成した名前付き ACL は、インターフェイスまたは VLAN に適用できます。

ACL の時間範囲の設定

ACL の時間範囲パラメータを設定するには、次の手順に従ってください。

手順の概要

1. **enable**
2. **configureterminal**
3. **time-range***time-range-name*
4. 次のいずれかを使用します。
   - **absolute** [**start***time date*] [**end***time date*]
   - **periodic***day-of-the-week hh:mmto* [*day-of-the-week*] *hh:mm*
   - **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ(config)# enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**time-range***time-range-name* 例： `スイッチ(config)# time-range workhours`	作成する時間範囲には意味のある名前（*workhours* など）を割り当て、時間範囲コンフィギュレーションモードを開始します。名前にスペースや疑問符を含めることはできません。また、文字から始める必要があります。
ステップ 4	次のいずれかを使用します。	適用対象の機能がいつ動作可能になるかを指定します。

	コマンドまたはアクション	目的

	• **absolute** [**start***time date*] [**end***time date*]
	• **periodic***day-of-the-week hh:mmto* [*day-of-the-week*] *hh:mm*
	• **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*
	
	例：
	`スイッチ(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006`
	または
	`スイッチ(config-time-range)# periodic weekdays 8:00 to 12:00`
		• 時間範囲には、**absolute** ステートメントを 1 つだけ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。
		• 複数の **periodic** ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。
		
		設定例を参照してください。

ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

複数の項目をそれぞれ異なる時間に有効にする場合は、上記の手順を繰り返してください。

関連トピック

ACL の時間範囲, （1452 ページ）

端末回線への IPv4 ACL の適用

番号付き ACL を使用して、1 つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

仮想端末回線とACLに指定されたアドレス間の着信接続および発信接続を制限するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **line** [**console** | **vty**] *line-number*
4. **access-class***access-list-number* {**in** | **out**}
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ(config)# enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** [**console**	**vty**] *line-number* 例： `スイッチ(config)# line console 0`	設定する回線を指定し、インライン コンフィギュレーション モードを開始します。 • **console**：コンソール端末回線を指定します。コンソール ポートは DCE です。 • **vty**：リモート コンソール アクセス用の仮想端末を指定します。 *line-number* は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。指定できる範囲は 0 ～ 16です。

	コマンドまたはアクション	目的
ステップ 4	**access-class***access-list-number* {**in** | **out**} 例： スイッチ(config-line)# **access-class 10 in**	（デバイスへの）特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信接続および発信接続を制限します。
ステップ 5	**end** 例： スイッチ(config-line)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスへの IPv4 ACL の適用

ここでは、IPv4 ACL をネットワーク インターフェイスへ適用する方法について説明します。

インターフェイスへのアクセスを制御する管理には、特権EXECモードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **ip access-group** {*access-list-number* | *name*} {**in** | **out**}
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスには、レイヤ 2 インターフェイス（ポート ACL）またはレイヤ 3 インターフェイス（ルータ ACL）を指定できます。
ステップ 3	**ip access-group** {*access-list-number* | *name*} {**in** | **out**} 例： スイッチ(config-if)# **ip access-group 2 in**	指定されたインターフェイスへのアクセスを制御します。 **out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv4 ACL のインターフェイスに関する注意事項, （1453 ページ）

IPv4 アクセス コントロール リストの設定に関する制約事項, （1438 ページ）

名前付き MAC 拡張 ACL の作成

VLAN またはレイヤ 2 インターフェイスで非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。その手順は、他の名前付き拡張 ACL を設定する場合と同様です。

名前付き MAC 拡張 ACL を作成するには、次の手順に従ってください。

手順の概要

1. **enable**
2. **configureterminal**
3. **mac access-list extended***name*
4. {**deny** | **permit**} {**any** | **host***source MAC address* | *source MAC address mask*} {**any** | **host***destination MAC address* | *destination MAC address mask*} [*type mask* | **lsap***lsap mask* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp** | 0-*65535*] [**cos***cos*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mac access-list extended***name* 例： スイッチ(config)# **mac access-list extended mac1**	名前を使用して MAC 拡張アクセス リストを定義します。
ステップ 4	{**deny** | **permit**} {**any** | **host***source MAC address* | *source MAC address mask*} {**any** | **host***destination MAC address* | *destination MAC address mask*} [*type mask* | **lsap***lsap mask*	拡張 MAC アクセス リスト コンフィギュレーション モードでは、すべての（**any**）送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定のホスト（**host**）送信元

	コマンドまたはアクション	目的

	| **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp** | 0-*65535*] [**cos***cos*]
	
	例：
	`スイッチ(config-ext-macl)# deny any any decnet-iv`
	または
	`スイッチ(config-ext-macl)# permit any any`
		MAC アドレス、およびすべての（any）宛先 MAC アドレス、マスク付き宛先MACアドレス、または特定の宛先MACアドレスに、**permit** または **deny** を指定します。
		（任意）次のオプションを入力することもできます。
		• *type mask*：Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号。10 進数、16 進数、または 8 進数で表記できます。一致検査の前に、任意で指定できる *don't care* ビットのマスクが EtherType に適用されます。
		• **lsap***lsap mask*：IEEE 802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。任意で *don't care* ビットのマスクを指定できます。
		• **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**—A non-IP protocol.
		• **cos***cos*：プライオリティを設定する 0 ～ 7 の IEEE 802.1Q CoS 番号。

ステップ 5	**end** 例： `スイッチ(config-ext-macl)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv4 アクセス コントロール リストの設定に関する制約事項, （1438 ページ）
VLAN マップの設定, （1473 ページ）

レイヤ 2 インターフェイスへの MAC ACL の適用

レイヤ2インターフェイスへのアクセスを制御するためにMACアクセス リストを適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **mac access-group** {*name*} {**in** | **out** }
5. **end**
6. **show mac access-group** [**interface***interface-id*]
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。指定するインターフェイスは物理レイヤ 2 インターフェイス（ポート ACL）でなければなりません。

	コマンドまたはアクション	目的
ステップ 4	**mac access-group** {*name*} {**in** | **out** } 例： `スイッチ(config-if)# mac access-group mac1 in`	MAC アクセス リストを使用して、指定されたインターフェイスへのアクセスを制御します。 ポート ACL は発信および着信方向サポートされます。
ステップ 5	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show mac access-group** [**interface***interface-id*] 例： `スイッチ# show mac access-group interface gigabitethernet1/0/2`	そのインターフェイスまたはすべてのレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。
ステップ 7	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチは、パケットを受信すると、着信 ACL とパケットを照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

関連トピック

IPv4 アクセス コントロール リストの設定に関する制約事項, （1438 ページ）

VLAN マップの設定

VLANマップを作成して、1つまたは複数のVLANに適用するには、次のステップを実行します。

はじめる前に

VLAN に適用する標準 IPv4 ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。

手順の概要

1. **vlan access-map** *name* [**number**]
2. **match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*]
3. IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1 つ以上のACL（標準または拡張）とそのパケットを照合するには、次のコマンドのいずれかを入力します。
   - **action** { **forward**}

     ```
     スイッチ(config-access-map)# action forward
     ```

   - **action** { **drop**}

     ```
     スイッチ(config-access-map)# action drop
     ```

4. **vlan filter** *mapname* **vlan-list** *list*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vlan access-map** *name* [**number**] 例： `スイッチ(config)# vlan access-map map_1 20`	VLAN マップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。 同じ名前のVLANマップを作成すると、10ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。 VLAN マップでは、特定の permit または deny キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致するという意味です。ACL 内の deny は、一致しないという意味です。 このコマンドを入力すると、アクセスマップ コンフィギュレーション モードに変わります。

	コマンドまたはアクション	目的
ステップ 2	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*] 例： スイッチ(config-access-map)# **match ip address ip2**	1 つまたは複数の標準または拡張アクセス リストに対してパケットを照合します（IP または MAC アドレスを使用）。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ照合されます。 （注） パケット タイプ（IP または MAC）に対する match 句が VLAN マップに設定されている場合で、そのマップ アクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。match 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。
ステップ 3	IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1 つ以上の ACL（標準または拡張）とそのパケットを照合するには、次のコマンドのいずれかを入力します。 • **action** { **forward**} スイッチ(config-access-map)# **action forward** • **action** { **drop**} スイッチ(config-access-map)# **action drop**	マップ エントリに対するアクションを設定します。
ステップ 4	**vlan filter** *mapname* **vlan-list** *list* 例： スイッチ(config)# **vlan filter map 1 vlan-list 20-22**	VLAN マップを 1 つまたは複数の VLAN に適用します。 list には単一の VLAN ID（22）、連続した範囲（10 ～ 22）、または VLAN ID のストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。

関連トピック

番号付き標準 ACL の作成, （1454 ページ）
番号付き拡張 ACL の作成, （1456 ページ）
名前付き MAC 拡張 ACL の作成, （1469 ページ）
VLAN マップの作成, （1475 ページ）

VLAN への VLAN マップの適用, （1476 ページ）

VLAN マップの作成

各 VLAN マップは順番に並べられた一連のエントリで構成されます。VLAN マップ エントリを作成、追加、または削除するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **vlan access-map** *name* [**number**]
3. **match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*]
4. **action** {**drop** | **forward**}
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan access-map** *name* [**number**] 例： `スイッチ(config)# vlan access-map map_1 20`	VLAN マップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。 同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。 VLAN マップでは、特定の permit または deny キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致するという意味です。ACL 内の deny は、一致しないという意味です。 このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。

	コマンドまたはアクション	目的
ステップ 3	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*] 例： `スイッチ(config-access-map)# match ip address ip2`	1 つまたは複数の標準または拡張アクセス リストに対してパケットを照合します（IP または MAC アドレスを使用）。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ照合されます。
ステップ 4	**action** {**drop** | **forward**} 例： `スイッチ(config-access-map)# action forward`	（任意）マップ エントリに対するアクションを設定します。デフォルトは転送（forward）です。
ステップ 5	**end** 例： `スイッチ(config-access-map)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**show running-config** 例： `スイッチ# show running-config`	アクセス リストの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN マップの設定, （1473 ページ）

VLAN への VLAN マップの適用

1 つの VLAN マップを 1 つまたは複数の VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **vlan filter** *mapname* **vlan-list** *list*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan filter** *mapname* **vlan-list** *list* 例： スイッチ(config)# **vlan filter map 1 vlan-list 20-22**	VLAN マップを 1 つまたは複数の VLAN に適用します。 list には単一の VLAN ID（22）、連続した範囲（10 ～ 22）、または VLAN ID のストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** 例： スイッチ# **show running-config**	アクセス リストの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN マップの設定, （1473 ページ）

IPv4 ACL のモニタリング

スイッチに設定されている ACL、およびインターフェイスと VLAN に適用された ACL を表示して IPv4 ACL をモニタできます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 またはレイヤ 3 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセス グループを表示できます。また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、次の表に記載された特権 EXEC コマンドを使用します。

表 *106*：アクセス リストおよびアクセス グループを表示するコマンド

コマンド	目的
show access-lists [*number* | *name*]	最新の IP および MAC アドレス アクセス リストの全体やその一部、または特定のアクセス リスト（番号付きまたは名前付き）の内容を表示します。
show ip access-lists [*number* | *name*]	最新の IP アクセス リスト全体、または特定の IP アクセス リスト（番号付きまたは名前付き）を表示します。
show ip interface*interface-id*	インターフェイスの詳細設定およびステータスを表示します。IP がイネーブルになっているインターフェイスに、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示されます。
show running-config [**interface***interface-id*]	スイッチまたは指定されたインターフェイスのコンフィギュレーション ファイルの内容（設定されたすべての MAC および IP アクセス リストや、どのアクセス グループがインターフェイスに適用されたかなど）を表示します。
show mac access-group [**interface***interface-id*]	すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リスト を表示します。

ACL の設定例

例：ACL での時間範囲を使用

次の例に、*workhours*（営業時間）の時間範囲および会社の休日（2006 年 1 月 1 日）を設定し、設定を確認する例を示します。

```
スイッチ# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張ACL内に時間範囲名を入力します。次に、拡張アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての TCP トラフィックを許可します。

```
スイッチ(config)# access-list 188 deny tcp any any time-range new_year_day_2006
スイッチ(config)# access-list 188 permit tcp any any time-range workhours
スイッチ(config)# end
スイッチ# show access-lists
Extended IP access list 188
   10 deny tcp any any time-range new_year_day_2006 (inactive)
   20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
スイッチ(config)# ip access-list extended deny_access
スイッチ(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
スイッチ(config-ext-nacl)# exit
スイッチ(config)# ip access-list extended may_access
スイッチ(config-ext-nacl)# permit tcp any any time-range workhours
スイッチ(config-ext-nacl)# end
スイッチ# show ip access-lists
Extended IP access list lpip_default
    10 permit ip any any
Extended IP access list deny_access
    10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
    10 permit tcp any any time-range workhours (inactive)
```

例：ACL へのコメントの挿入

remark キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント（注釈）を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、permit ステートメントまたは deny ステートメントの前後どちらにでも配置できます。コメントがどの permit ステートメントまたは deny ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは

対応する permit または deny ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list** *access-list number* **remark** *remark* グローバル コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
スイッチ(config)# access-list 1 remark Permit only Jones workstation through
スイッチ(config)# access-list 1 permit 171.69.2.88
スイッチ(config)# access-list 1 remark Do not allow Smith through
スイッチ(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリには、**remark** アクセス リスト コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

```
スイッチ(config)# ip access-list extended telnetting
スイッチ(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
スイッチ(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

IPv4 ACL の設定例

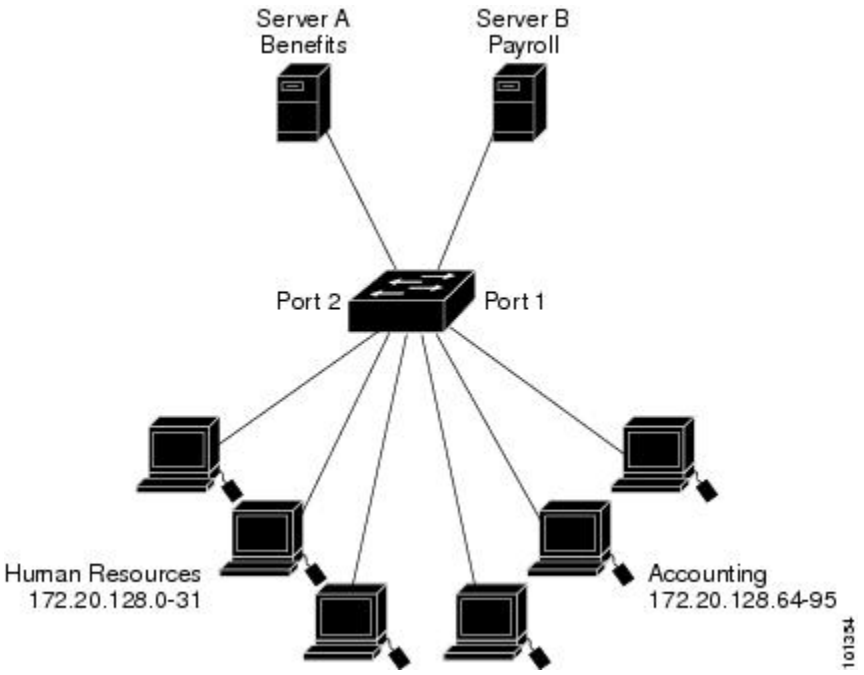
ここでは、IPv4 ACL を設定および適用する例を示します。ACL のコンパイルに関する詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』および『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Adderssing and Services」の章にある「Configuring IP Services」の項を参照してください。

小規模ネットワークが構築されたオフィス用の ACL

次に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッド ポート 2 に接続されたサーバ A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。

サーバ A にはすべてのユーザがアクセスできますが、サーバ B にアクセスできるユーザは制限されています。

図 *69*：ルータ *ACL* によるトラフィックの制御



ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準ACLを作成し、ポート1からサーバに着信するトラフィックをフィルタリングします。
- 拡張ACLを作成し、サーバからポート1に着信するトラフィックをフィルタリングします。

例：小規模ネットワークが構築されたオフィスの ACL

次に、標準ACLを使用してポートからサーバBに着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ～ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッド ポート 1 から送信されるトラフィックに適用されます。

```
スイッチ(config)# access-list 6 permit 172.20.128.64 0.0.0.31
スイッチ(config)# end
スイッチ# how access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# ip access-group 6 out
```

次に、拡張ACLを使用してサーバBからポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバB）から経理部の宛先アドレス172.20.128.64～172.20.128.95に送信されるトラフィックだけを許可する例を示します。この ACL は、ルーテッド ポート 1 に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可し

ます。拡張 ACL を使用する場合は、送信元および宛先情報の前に、プロトコル（IP）を入力する必要があります。

```
スイッチ(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
スイッチ(config)# end
スイッチ# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# ip access-group 106 in
```

例：番号付き ACL

次の例のネットワーク 36.0.0.0 は、2 番めのオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネット マスクは 255.255.0.0 です。ネットワーク アドレス 36.0.0.0 の 3 番めおよび 4 番めのオクテットは、特定のホストを指定します。アクセス リスト 2 を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセス リストの最終行は、ネットワーク 36.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。この ACL は、ポートに着信するパケットに適用されます。

```
スイッチ(config)# access-list 2 permit 36.48.0.3
スイッチ(config)# access-list 2 deny 36.48.0.0 0.0.255.255
スイッチ(config)# access-list 2 permit 36.0.0.0 0.255.255.255
スイッチ(config)# interface gigabitethernet2/0/1
スイッチ(config-if)# ip access-group 2 in
```

例：拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番めの行は、ホスト 128.88.1.2 の SMTP ポートへの着信 TCP 接続を許可します。3 番めの行は、エラーフィードバック用の着信 ICMP メッセージを許可します。

```
スイッチ(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
スイッチ(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
スイッチ(config)# access-list 102 permit icmp any any
スイッチ(config)# interface gigabitethernet2/0/1
スイッチ(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。ただし、IP ホストからは、専用メール ホストのメール（SMTP）ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。発信パケットのポート番号は予約されています。安全なネットワークのシステムでは常にポート 25 でのメール接続が使用されているため、着信サービスと発信サービス

を個別に制御できます。ACL は発信インターフェイスの入力 ACL および着信インターフェイスの出力 ACL として設定される必要があります。

```
スイッチ(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
スイッチ(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# ip access-group 102 in
```

次の例では、ネットワークはアドレスが 128.88.0.0 のクラス B ネットワークで、メール ホストのアドレスは 128.88.1.2 です。**established** キーワードは、確立された接続を表示する TCP 専用のキーワードです。TCP データグラムに ACK または RST ビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。スタック メンバー 1 のギガビット イーサネット インターフェイス 1 は、ルータをインターネットに接続するインターフェイスです。

```
スイッチ(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
スイッチ(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# ip access-group 102 in
```

例：名前付き ACL

名前付き標準 ACL および名前付き拡張 ACL の作成

次に、*Internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。*Internet_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
スイッチ(config)# ip access-list standard Internet_filter
スイッチ(config-ext-nacl)# permit 1.2.3.4
スイッチ(config-ext-nacl)# exit
```

marketing_group ACL は、宛先アドレスとワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ～ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
スイッチ(config)# ip access-list extended marketing_group
スイッチ(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
スイッチ(config-ext-nacl)# deny tcp any any
スイッチ(config-ext-nacl)# permit icmp any any
スイッチ(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
スイッチ(config-ext-nacl)# deny ip any any log
スイッチ(config-ext-nacl)# exit
```

Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
スイッチ(config)# interface gigabitethernet3/0/2
スイッチ(config-if)# no switchport
```

```
スイッチ(config-if)# ip address 2.0.5.1 255.255.255.0
スイッチ(config-if)# ip access-group Internet_filter out
スイッチ(config-if)# ip access-group marketing_group in
```

名前付き ACL からの個別 ACE の削除

次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```
スイッチ(config)# ip access-list extended border-list
スイッチ(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

例：IP ACL に適用される時間範囲

次に、月曜日から金曜日の午前 8 時 ～午後 6 時（18 時）の間、IP の HTTP トラフィックを拒否する例を示します。UDP トラフィックは、土曜日および日曜日の正午～午後 8 時（20 時）の間だけ許可されます。

```
スイッチ(config)# time-range no-http
スイッチ(config)# periodic weekdays 8:00 to 18:00
!
スイッチ(config)# time-range udp-yes
スイッチ(config)# periodic weekend 12:00 to 20:00
!
スイッチ(config)# ip access-list extended strict
スイッチ(config-ext-nacl)# deny tcp any any eq www time-range no-http
スイッチ(config-ext-nacl)# permit udp any any time-range udp-yes
!
スイッチ(config-ext-nacl)# exit
スイッチ(config)# interface gigabitethernet2/0/1
スイッチ(config-if)# ip access-group strict in
```

例：コメント付き IP ACL エントリの設定

次に示す番号付き ACL の例では、Jones が所有するワークステーションにはアクセスを許可し、Smith が所有するワークステーションにはアクセスを許可しません。

```
スイッチ(config)# access-list 1 remark Permit only Jones workstation through
スイッチ(config)# access-list 1 permit 171.69.2.88
スイッチ(config)# access-list 1 remark Do not allow Smith workstation through
スイッチ(config)# access-list 1 deny 171.69.3.13
```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しません。

```
スイッチ(config)# access-list 100 remark Do not allow Winter to browse the web
スイッチ(config)# access-list 100 deny host 171.69.3.85 any eq www
スイッチ(config)# access-list 100 remark Do not allow Smith to browse the web
スイッチ(config)# access-list 100 deny host 171.69.3.13 any eq www
```

次に示す名前付き ACL の例では、Jones のサブネットにアクセスを許可しません。

```
スイッチ(config)# ip access-list standard prevention
スイッチ(config-std-nacl)# remark Do not allow Jones subnet through
スイッチ(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次に示す名前付き ACL の例では、Jones のサブネットに発信 Telnet の使用を許可しません。

```
スイッチ(config)# ip access-list extended telnetting
スイッチ(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
スイッチ(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

例：ACL ロギング

ルータ ACL では、2 種類のロギングがサポートされています。**log** キーワードを指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。**log-input** キーワードを指定すると、ログ エントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセス リスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。**log** キーワードも指定されています。

```
スイッチ(config)# ip access-list standard stan1
スイッチ(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
スイッチ(config-std-nacl)# permit any log
スイッチ(config-std-nacl)# exit
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# ip access-group stan1 in
スイッチ(config-if)# end
スイッチ# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 37 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 37 messages logged
    File logging: disabled
    Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems

<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次に、名前付き拡張アクセス リスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```
スイッチ(config)# ip access-list extended ext1
スイッチ(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
スイッチ(config-ext-nacl)# deny udp any any log
スイッチ(config-std-nacl)# exit
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# ip access-group ext1 in
```

次に、拡張 ACL のログの例を示します。

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
01:26:12:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1 packet
01:31:33:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8 packets
```

IP ACL のすべてのロギング エントリは %SEC-6-IPACCESSLOG で開始します。エントリの形式は、一致した ACL やアクセス エントリの種類に応じて若干異なります。

次に、**log-input** キーワードを指定した場合の出力メッセージの例を示します。

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400)
 ->
10.1.1.61 (0/0), 1 packet
```

log キーワードを指定した場合、同様のパケットに関するログ メッセージには入力インターフェイス情報が含まれません。

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0), 1
 packet
```

ACL および VLAN マップの設定例

例：パケットを拒否する ACL および VLAN マップの作成

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、*ip1* ACL（TCP パケット）に一致するすべてのパケットがドロップされます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する *ip1* ACL を作成します。VLAN マップには IP パケットに対する match 句が存在するため、デフォルトのアクションでは、どの match 句とも一致しない IP パケットがすべてドロップされます。

```
スイッチ(config)# ip access-list extended ip1
スイッチ(config-ext-nacl)# permit tcp any any
スイッチ(config-ext-nacl)# exit
スイッチ(config)# vlan access-map map_1 10
スイッチ(config-access-map)# match ip address ip1
スイッチ(config-access-map)# action drop
```

例：パケットを許可する ACL および VLAN マップの作成

次に、パケットを許可する VLAN マップを作成する例を示します。ACL *ip2* は UDP パケットを許可し、*ip2* ACL と一致するすべてのパケットが転送されます。このマップでは、これ以前のどの ACL とも一致しないすべての IP パケット（TCP でも UDP でもないパケット）がドロップされます。

```
スイッチ(config)# ip access-list extended ip2
スイッチ(config-ext-nacl)# permit udp any any
スイッチ(config-ext-nacl)# exit
```

```
スイッチ(config)# vlan access-map map_1 20
スイッチ(config-access-map)# match ip address ip2
スイッチ(config-access-map)# action forward
```

例：IP パケットのドロップおよび MAC パケットの転送のデフォルト アクション

次の例の VLAN マップでは、デフォルトで IP パケットがドロップされ、MAC パケットが転送されます。標準の ACL 101 および名前付き拡張アクセス リスト **igmp-match** および **tcp-match** をこのマップと組み合わせて使用すると、次のようになります。

- すべての UDP パケットが転送されます。
- すべての IGMP パケットがドロップされます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- すべての非 IP パケットが転送されます。

```
スイッチ(config)# access-list 101 permit udp any any
スイッチ(config)# ip access-list extended igmp-match
スイッチ(config-ext-nacl)# permit igmp any any

スイッチ(config-ext-nacl)# permit tcp any any
スイッチ(config-ext-nacl)# exit
スイッチ(config)# vlan access-map drop-ip-default 10
スイッチ(config-access-map)# match ip address 101
スイッチ(config-access-map)# action forward
スイッチ(config-access-map)# exit
スイッチ(config)# vlan access-map drop-ip-default 20
スイッチ(config-access-map)# match ip address igmp-match
スイッチ(config-access-map)# action drop
スイッチ(config-access-map)# exit
スイッチ(config)# vlan access-map drop-ip-default 30
スイッチ(config-access-map)# match ip address tcp-match
スイッチ(config-access-map)# action forward
```

例：MAC パケットのドロップおよび IP パケットの転送のデフォルト アクション

次の例の VLAN マップでは、デフォルトで MAC パケットがドロップされ、IP パケットが転送されます。MAC 拡張アクセス リスト **good-hosts** および **good-protocols** をこのマップと組み合わせて使用すると、次のようになります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- decnet-iv または vines-ip プロトコルを使用する MAC パケットが転送されます。
- その他のすべての非 IP パケットがドロップされます。
- すべての IP パケットが転送されます。

例：すべてのパケットをドロップするデフォルト アクション

次の例の VLAN マップでは、デフォルトですべてのパケット（IP および非 IP）がドロップされます。例 2 および例 3 のアクセス リスト **tcp-match** および **good-hosts** をこのマップと組み合わせて使用すると、次のようになります。

- すべての TCP パケットが転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- その他のすべての MAC パケットがドロップされます。

```
スイッチ(config)# vlan access-map drop-all-default 10
スイッチ(config-access-map)# match ip address tcp-match
スイッチ(config-access-map)# action forward
スイッチ(config-access-map)# exit
スイッチ(config)# vlan access-map drop-all-default 20
スイッチ(config-access-map)# match mac address good-hosts
スイッチ(config-access-map)# action forward
```

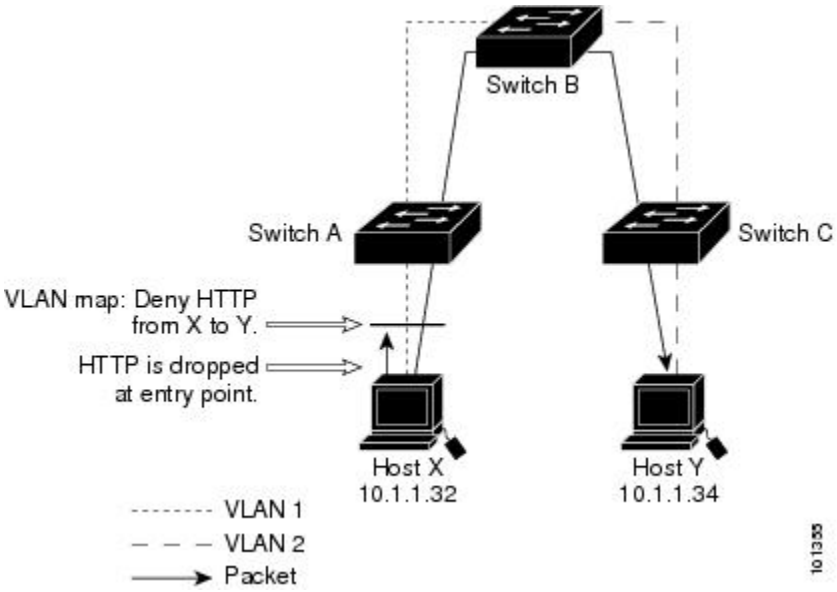
ネットワークでの VLAN マップの使用方法の設定例

例：ワイヤリング クローゼットの設定

ワイヤリング クローゼット構成では、ルーティングがスイッチ上でイネーブルにされていない場合があります。ただし、この設定でも VLAN マップおよび QoS 分類 ACL はサポートされています。ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリング クローゼット スイッチ A およびスイッチ C に接続されていると想定します。ホスト X からホスト Y へのトラフィックは、ルーティングがイネーブルに設定されたレイヤ 3 スイッチであるスイッチ B によって最終的にルー

ティングされます。ホストXからホストYへのトラフィックは、トラフィックのエントリ ポイントであるスイッチ A でアクセス コントロールできます。

図 *70*：ワイヤリング クローゼットの設定



HTTP トラフィックをホスト X からホスト Y へスイッチングしない場合は、ホスト X（IP アドレス 10.1.1.32）からホスト Y（IP アドレス 10.1.1.34）に向かうすべての HTTP トラフィックがスイッチ A でドロップされ、スイッチ B にブリッジングされないように、スイッチ A の VLAN マップを設定できます。

最初に、HTTP ポート上ですべての TCP トラフィックを許可（一致）する IP アクセス リスト *http* を定義します。

```
スイッチ(config)# ip access-list extended http
スイッチ(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
スイッチ(config-ext-nacl)# exit
```

次に、*http* アクセス リストと一致するトラフィックがドロップされ、その他のすべての IP トラフィックが転送されるように、VLAN アクセス マップ *map2* を作成します。

```
スイッチ(config)# vlan access-map map2 10
スイッチ(config-access-map)# match ip address http
スイッチ(config-access-map)# action drop
スイッチ(config-access-map)# exit
スイッチ(config)# ip access-list extended match_all
スイッチ(config-ext-nacl)# permit ip any any
スイッチ(config-ext-nacl)# exit
スイッチ(config)# vlan access-map map2 20
スイッチ(config-access-map)# match ip address match_all
スイッチ(config-access-map)# action forward
```

次に、VLAN アクセス マップ *map2* を VLAN 1 に適用します。

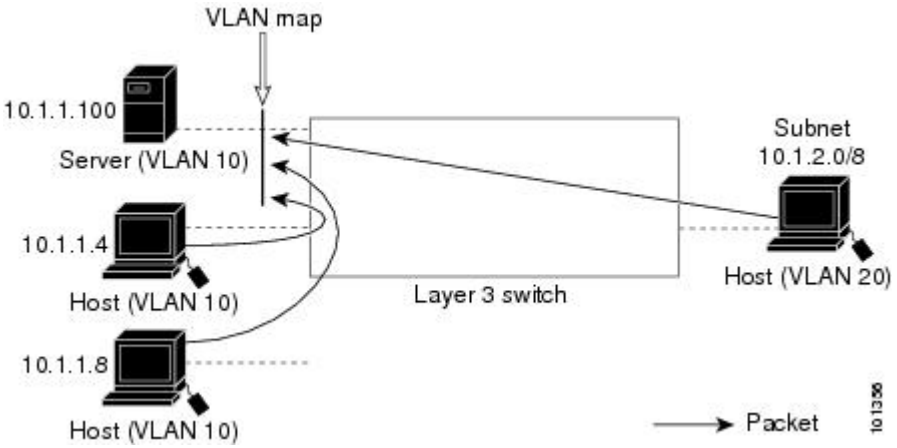
```
スイッチ(config)# vlan filter map2 vlan 1
```

例：別の VLAN にあるサーバへのアクセスの制限

別の VLAN にあるサーバへのアクセスを制限できます。たとえば、VLAN 10 内のサーバ 10.1.1.100 では、次のホストへのアクセスを拒否する必要があります。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスを禁止します。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスを禁止します。

図 *71*：別の *VLAN* 上のサーバへのアクセスの制限



例：別の VLAN にあるサーバへのアクセスの拒否

次に、サブネット 10.1.2.0.8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 のアクセスを拒否し、その他の IP トラフィックを許可する VLAN マップ SERVER1-ACL を作成して、別の VLAN 内のサーバへのアクセスを拒否する例を示します。最後のステップでは、マップ SERVER1 を VLAN 10 に適用します。

正しいパケットと一致する IP ACL を定義します。

```
スイッチ(config)# ip access-list extended SERVER1_ACL
スイッチ(config-ext-nacl))# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
スイッチ(config-ext-nacl))# permit ip host 10.1.1.4 host 10.1.1.100
スイッチ(config-ext-nacl))# permit ip host 10.1.1.8 host 10.1.1.100
スイッチ(config-ext-nacl))# exit
```

SERVER1_ACL と一致する IP パケットをドロップして、この ACL と一致しない IP パケットを転送する ACL を使用して、VLAN マップを定義します。

```
スイッチ(config)# vlan access-map SERVER1_MAP
スイッチ(config-access-map)# match ip address SERVER1_ACL
```

```
スイッチ(config-access-map)# action drop
スイッチ(config)# vlan access-map SERVER1_MAP 20
スイッチ(config-access-map)# action forward
スイッチ(config-access-map)# exit
```

VLAN 10 に VLAN マップを適用します。

```
スイッチ(config)# vlan filter SERVER1_MAP vlan-list 10
```

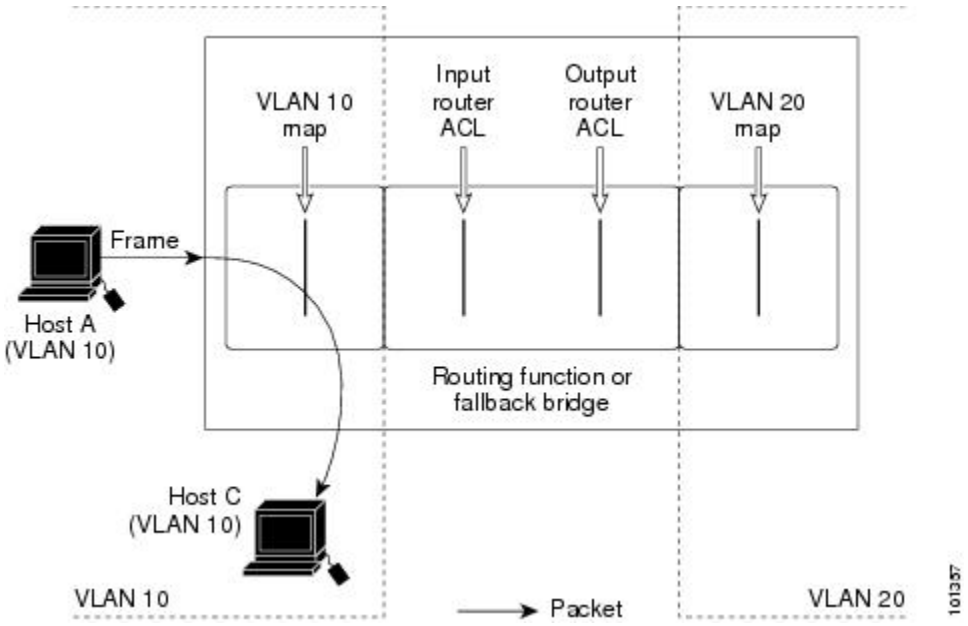
VLAN に適用されるルータ ACL と VLAN マップの設定例

ここでは、ルータ ACL および VLAN マップを VLAN に適用し、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットを処理する例を示します。次の図ではそれぞれの宛先に転送されるパケットを示します。パケットのパスが VLAN マップや ACL を示す線と交差するポイントで、パケットを転送せずにドロップする可能性もあります。

例：ACL およびスイッチド パケット

次の例に、VLAN 内でスイッチングされるパケットに ACL を適用する方法を示します。フォールバック ブリッジングによってルーティングまたは転送されず、VLAN 内でスイッチングされるパケットには、入力 VLAN の VLAN マップだけが適用されます。

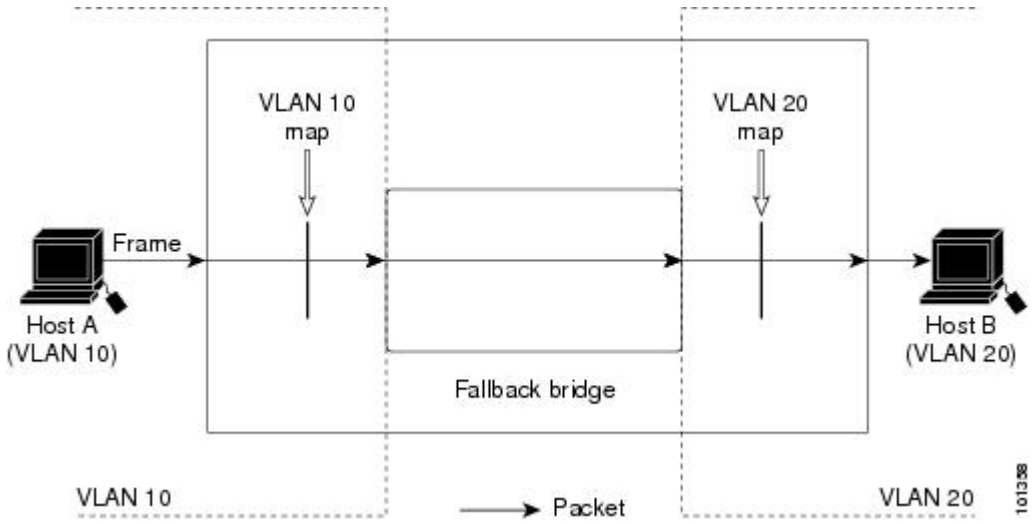
図 *72*：スイッチド パケットへの *ACL* の適用



例：ACL およびブリッジド パケット

次の例に、フォールバック ブリッジド パケットに ACL を適用する方法を示します。ブリッジド パケットの場合は、入力 VLAN にレイヤ 2 ACL だけが適用されます。また、非 IP および非 ARP パケットだけがフォールバック ブリッジド パケットとなります。

図 *73*：ブリッジド パケットへの *ACL* の適用

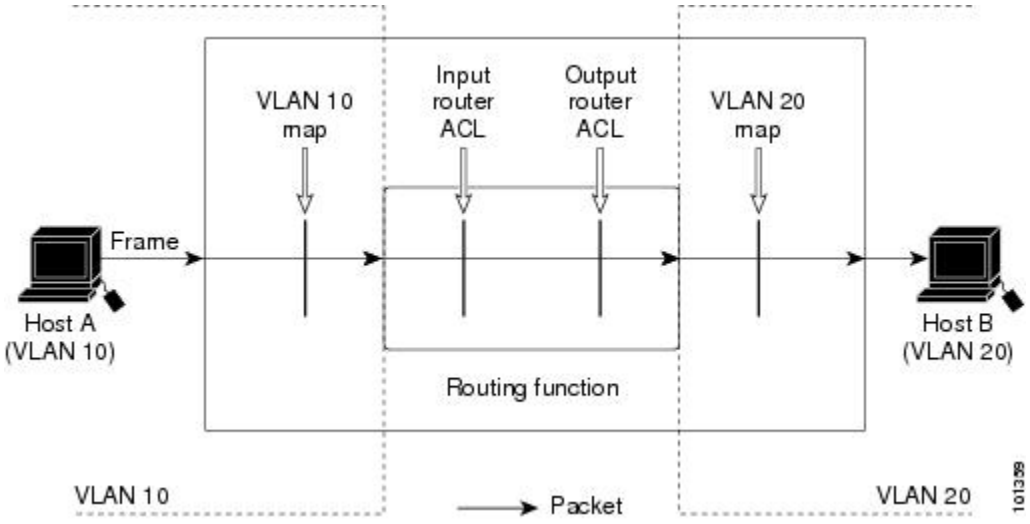


例：ACL およびルーテッド パケット

次の例に、ルーテッド パケットに ACL を適用する方法を示します。ACL は次の順番で適用されます。

1. 入力 VLAN の VLAN マップ
2. 入力ルータ ACL
3. 出力ルータ ACL
4. 出力 VLAN の VLAN マップ

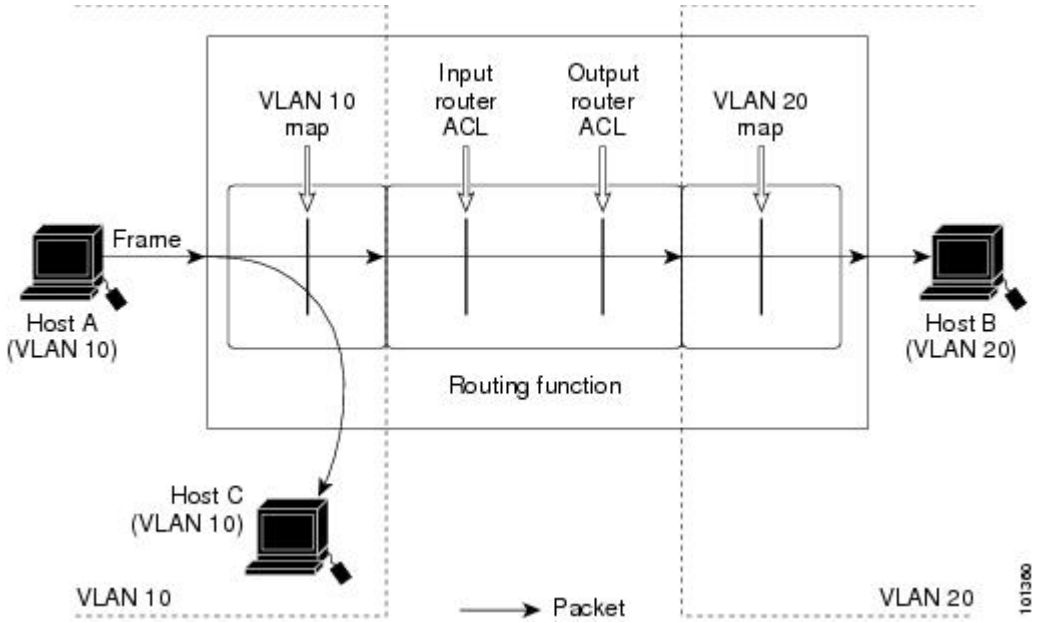
図 *74*：ルーテッド パケットへの *ACL* の適用



例：ACL およびマルチキャスト パケット

次の例に、IP マルチキャスト用に複製されたパケットに ACL を適用する方法を示します。ルーティングされるマルチキャスト パケットには、2 つの異なるフィルタが適用されます。1 つは、宛先が入力 VLAN 内の他のポートである場合に使用され、もう 1 つは、宛先がパケットのルーティング先である別の VLAN 内にある場合に使用されます。パケットは複数の出力 VLAN にルーティングされる場合がありますが、この場合は宛先 VLAN ごとに異なるルータ出力 ACL および VLAN マップが適用されます。最終的に、パケットは一部の出力 VLAN 内で許可され、それ以外の VLAN で拒否されます。パケットのコピーが、許可された宛先に転送されます。ただし、入力 VLAN マップによってパケットがドロップされる場合、パケットのコピーは宛先に送信されません。

図 *75* : マルチキャスト パケットへの *ACL* の適用



その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv4 アクセス コントロール リストのトピック	Securing the Data Plane Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 スイッチ) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secdata-xe-3se-3850-library.html

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

第 65 章

IPv6 ACL の設定

- 機能情報の確認，1497 ページ
- IPv6 ACL の概要，1497 ページ
- IPv6 ACL の制限，1499 ページ
- IPv6 ACL のデフォルト設定，1500 ページ
- IPv6 ACL の設定，1500 ページ
- インターフェイスへの IPv6 ACL の付加，1504 ページ
- IPv6 ACL のモニタリング，1506 ページ
- その他の参考資料，1507 ページ

機能情報の確認

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

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

IPv6 ACL の概要

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。また、スイッチで IP ベースおよび LAN

ベース フィーチャ セットが稼働している場合、入力ルータ ACL を作成し、それを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

スイッチは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンド トラフィックまたはインバウンド トラフィックでサポートされます。IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。
- IPv6 ポート ACL は、インバウンドおよびアウトバウンドのレイヤ 2 インターフェイスでトラフィックでサポートされます。IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。

スイッチは、IPv6 トラフィックの Virtual LAN（VLAN）ACL（VLAN マップ）をサポートしません。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

スイッチ スタックおよび IPv6 ACL

アクティブ スイッチは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバに配信します。

スタンバイ スイッチがアクティブ スイッチを引き継ぐと、ACL 設定がすべてのスタック メンバに配信されます。メンバスイッチは、新しいスアクティブスイッチによって配信された設定を同期し、不要なエントリを消去します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、アクティブ スイッチは変更内容をすべてのスタック メンバーに配信します。

他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージプロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリに空きがない場合、パケットはインターフェイスでドロップされ、アンロードのエラー メッセージが記録されます。

IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは再起 ACL（**reflect** キーワード）をサポートしません。
- このリリースが IPv6 用にサポートしているのは、ポート ACL およびルータ ACL だけです。VLAN ACL（VLAN マップ）はサポートしていません。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- レイヤ 2 EtherChannel に IPv6 ポート ACL を適用できません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうか判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ（ACE）を追加しようとする場合、スイッチは現在インターフェイスに適用されている ACL に ACE が追加されるのを許可しません。

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム（IPv4 では **fragments** キーワード）がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。
- スイッチのハードウェア スペースがなくなった場合、ACL に関連付けられたパケットはインターフェイスでドロップされます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。
- スイッチは、プレフィックス長の最大範囲の IPv6 アドレス一致をサポートしません。

IPv6 ACL のデフォルト設定

デフォルトの IPv6 ACL 設定は次のとおりです。

```
Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します

手順の概要

1. **enable**
2. **configureterminal**
3. [**no**]{**ipv6 access-list***list-name*| **client permit-control-packets**| **log-update threshold**|**role-based***list-name*}
4. [**no**]{**deny** | **permit**} protocol {*source-ipv6-prefix/|prefix-length*|**any threshold**| **host***source-ipv6-address*} [operator [*port-number*]] { *destination-ipv6-prefix/ prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]][**dscp***value*] [**fragments**] [**log**] [**log-input**] [**routing**][**sequence***value*] [**time-range***name*]
5. {**deny** | **permit**} **tcp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [**operator** [**port-number**]] {*destination-ipv6- prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [**ack**] [**dscp***value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {**port** | protocol}] [**psh**] [**range** {**port** | protocol}] [**rst**] [**routing**] [**sequence***value*] [**syn**] [**time-range***name*] [**urg**]
6. {**deny** | **permit**} **udp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [**dscp***value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**][**sequence***value*] [**time-range***name*]]
7. {**deny** | **permit**} **icmp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [*icmp-type* [*icmp-code*] | icmp-message] [**dscp***value*] [**log**] [**log-input**] [**routing**][**sequence***value*] [**time-range***name*]
8. **end**
9. **show ipv6 access-list**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**]{**ipv6 access-list***list-name*| **client permit-control-packets**| **log-update threshold**|**role-based***list-name*} 例： スイッチ(config)# **ipv6 access-list example_acl_list**	IPv6 ACL 名を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	[**no**]{**deny** | **permit**} protocol {*source-ipv6-prefix/|prefix-length*|**any threshold**| **host***source-ipv6-address*} [operator [*port-number*]] { *destination-ipv6-prefix/ prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]][**dscp***value*] [**fragments**] [**log**] [**log-input**] [**routing**][**sequence***value*] [**time-range***name*]	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、**udp**、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • *source-ipv6-prefix/prefix-length* または *destination-ipv6-prefix/ prefix-length* は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 • **host***source-ipv6-address* または *destination-ipv6-address* には、拒否条件または許可条件を設定する送信元または宛先IPv6ホストアドレスを入力します。アドレスはコロン区切りの16ビット値を使用した 16 進形式で指定します。 •（任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、**range**（包含範囲）があります。

	コマンドまたはアクション	目的
		source-ipv6-prefix/prefix-length 引数のあとの operator は、送信元ポートに一致する必要があります。*destination-ipv6-prefix/prefix-length* 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）**port-number** は、0 ～ 65535 の 10 進数または TCP あるいはUDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）**dscp** value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）**fragments** を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • （任意）**log** を指定すると、エントリと一致するパケットに関するログ メッセージがコンソールに送信されます。**log-input** を指定すると、ログ エントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 • （任意）**routing** を入力して、IPv6 パケットのルーティングを指定します。 • （任意）**sequence***value* を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4,294,967,295 です。 • （任意）**time-range** name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 5	{**deny** | **permit**} **tcp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [**operator** [**port-number**]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [**ack**] [**dscp***value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {**port** | protocol}] [**psh**] [**range** {**port** | protocol}] [**rst**] [**routing**] [**sequence***value*] [**syn**] [**time-range***name*] [**urg**]	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は **tcp** を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 • **ack**：確認応答（ACK）ビット セット • **established**：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • **fin**：終了ビットセット。送信元からのデータはそれ以上ありません。

	コマンドまたはアクション	目的
		• **neq** {*port* | protocol}：所定のポート番号上にないパケットだけを照合します。 • **psh**：プッシュ機能ビット セット • **range** {*port* | protocol}：ポート番号の範囲内のパケットだけを照合します。 • **rst**：リセット ビット セット • **syn**：同期ビット セット • **urg**：緊急ポインタ ビット セット
ステップ 6	{**deny** | **permit**} **udp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [**dscp***value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**][**sequence***value*] [**time-range***name*]]	（任意）UDP アクセス リストおよびアクセス条件を定義します。 ユーザ データグラム プロトコルの場合は、**udp** を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [*port*]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。
ステップ 7	{**deny** | **permit**} **icmp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [*icmp-type* [*icmp-code*] | icmp-message] [**dscp***value*] [**log**] [**log-input**] [**routing**][**sequence***value*] [**time-range***name*]	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージプロトコルの場合は、**icmp** を入力します。ICMP パラメータはステップ 1 の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-code*：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、?キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。

	コマンドまたはアクション	目的
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ipv6 access-list**	アクセス リストの設定を確認します。
ステップ 10	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

インターフェイスに IPv6 ACL をアタッチします。

インターフェイスへの IPv6 ACL の付加

レイヤ 3 インターフェイスで発信または着信トラフィックに、あるいはレイヤ 2 インターフェイスで着信トラフィックに ACL を適用できます。レイヤ 3 インターフェイスで着信トラフィックにだけ ACL を適用できます。

インターフェイスへのアクセスを制御するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **no switchport**
5. **ipv6 address***ipv6-address*
6. **ipv6traffic-filter***access-list-name* {**in** | **out**}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id*	アクセス リストを適用するレイヤ2インターフェイス（ポート ACL 用）またはレイヤ3インターフェイス（ルータ ACL 用）を特定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no switchport**	ルータ ACL を適用する場合は、これによってインターフェイスがレイヤ 2 モード（デフォルト）からレイヤ 3 モードに変化します。
ステップ 5	**ipv6 address***ipv6-address*	レイヤ 3 インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。
ステップ 6	**ipv6traffic-filter***access-list-name* {**in** | **out**}	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。 （注）
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

IPv6 ACL のモニタリング

次の表に示された 1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

コマンド	目的
show access-lists	スイッチに設定されたすべてのアクセス リストを表示します。
show ipv6 access-list [*access-list-name*]	設定済みのすべての IPv6 アクセス リストまたは名前で指定されたアクセス リストを表示します。

次に、show access-lists 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Switch # show access-lists
Extended IP access list hello
    10 permit ip any any
IPv6 access list ipv6
    permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet (15 matches) sequence 20
    permit udp any any sequence 30

IPv6 access list outbound
    deny udp any any sequence 10
    deny tcp any any eq telnet sequence 20
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 セキュリティ設定のトピック	『IPv6 Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』 http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/xe-3se/3850/ipv6-xe-3se-3850-library.html
IPv6 コマンド リファレンス	『IPv6 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』 http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-xe-3se-3850-cr-book.html

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

第 66 章

DHCP の設定

- 機能情報の確認，1509 ページ
- DHCP に関する情報，1509 ページ
- DHCP 機能の設定方法，1517 ページ
- DHCP サーバ ポートベースのアドレス割り当ての設定，1529 ページ

機能情報の確認

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

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

DHCP に関する情報

DHCP サーバ

DHCP サーバは、スイッチまたはルータ上の指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、それらのアドレスを管理します。DHCP サーバがそのデータベースから要求された設定パラメータを取得して DHCP クライアントに渡すことができない場合は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに要求を転送します。スイッチは、DHCP サーバとして機能できます。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送するレイヤ 3 デバイスです。リレー エージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは、DHCP メッセージを受け取ると、新しい DHCP メッセージを生成して、出力インターフェイス上で送信します。

DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと DHCP スヌーピング バインディング データベース（DHCP スヌーピング バインディング テーブルとも呼ばれる）の作成および管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。DHCP スヌーピングを使用することにより、エンド ユーザに接続された信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。

（注） DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。

信頼できない DHCP メッセージとは、信頼できないインターフェイス経由で送信されたメッセージのことです。デフォルトでは、スイッチはすべてのインターフェイスを信頼できないものと見なします。そのため、スイッチはいくつかのインターフェイスを信頼して DHCP スヌーピングを使用するように設定する必要があります。サービス プロバイダー環境で DHCP スヌーピングを使用する場合は、カスタマーのスイッチなど、サービスプロバイダーネットワーク内には存在しないデバイスから送信されたメッセージが信頼できないメッセージとなります。不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカル インターフェイスのインターフェイス情報が含まれています。このデータベースには、信頼できるインターフェイスに接続されたホストの情報はありません。

サービスプロバイダーネットワークでは、信頼できるインターフェイスとして設定できるものの例として、同じネットワーク内のデバイスのポートに接続されたインターフェイスがあります。信頼できないインターフェイスには、ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスがあります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。アドレスが一致した場合（デフォルト）、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットをドロップします。

- DHCPOFFER パケット、DHCPACK パケット、DHCPNAK パケット、DHCPLEASEQUERY パケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスが一致しない。
- スイッチが DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バインディング データベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP Option 82 情報を挿入するエッジ スイッチに接続されているスイッチは、Option 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットをドロップします。DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジ スイッチに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジ スイッチによって挿入された Option 82 情報を含むパケットを受け入れます。集約スイッチは、信頼できないスイッチ インターフェイスを介して接続されたホストのバインディングを認識します。集約スイッチで、ダイナミック ARP インスペクションや IP ソース ガードなど、DHCP セキュリティ機能をイネーブルに設定することもできますが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない入力インターフェイスで受信します。集約スイッチ上のエッジ スイッチとの接続ポートは、信頼できるインターフェイスとして設定する必要があります。

通常、ワイヤレス クライアントにパケットをブロードキャストするのは望ましくありません。したがって、DHCP スヌーピングは、宛先ブロードキャスト MAC アドレス（ffff.ffff.ffff）をサーバからワイヤレス クライアントに送信される DHCP パケットのユニキャスト MAC アドレスに置き換えます。ユニキャスト MAC アドレスは DHCP ペイロードの CHADDR フィールドから取得されます。この処理は、DHCP OFFER、DHCP ACK および DHCP NACK メッセージなどのクライアント パケットにサーバ用に適用されます。**ip dhcp snooping wireless bootp-broadcast enable** は、この動作を戻すために使用できます。ワイヤレス BOOTP ブロードキャストがイネーブルの場合、サーバからのブロードキャスト DHCP パケットは、宛先 MAC アドレスを変更せずにワイヤレス クライアントに転送されます。

関連トピック

DHCP スヌーピングおよび Option 82 を設定するための前提条件, （1523 ページ）

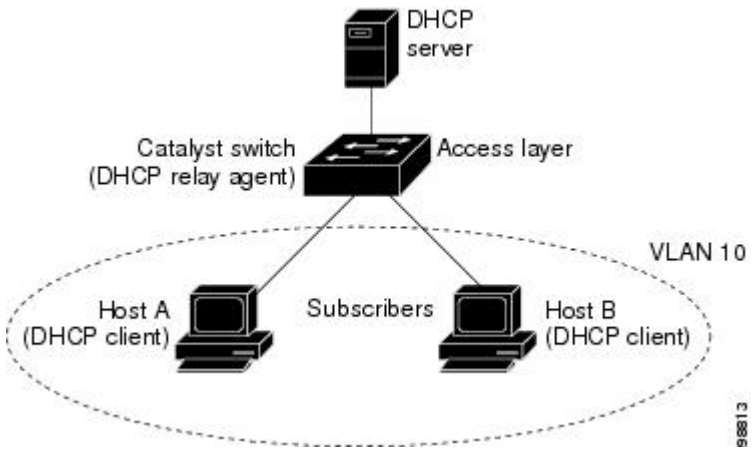
Option 82 データ挿入

住宅地域にあるメトロポリタン イーサネット アクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチ ポートによっても識別されます。サブスクライバ LAN 上の複数のホストをアクセス スイッチの同じポートに接続できます。これらのホストは一意に識別されます。

（注） DHCP Option 82 機能は、DHCP スヌーピングがグローバルにイネーブルであり、Option 82 を使用する加入者装置が割り当てられた VLAN でイネーブルである場合に限りサポートされます。

次の図に、一元的な DHCP サーバがアクセス レイヤのスイッチに接続された加入者に IP アドレスを割り当てるメトロポリタン イーサネット ネットワークを示します。DHCP クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレー エージェント（Catalyst スイッチ）にヘルパー アドレスを設定することにより、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 *76*：メトロポリタン イーサネット ネットワークにおける *DHCP* リレー エージェント



スイッチで DHCP スヌーピング情報 Option 82 をイネーブルにすると、次のイベントがこの順序で発生します。

- ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。デフォルトでは、リモート ID サブオプションがスイッチの MAC アドレスで、回線 ID サブオプションはパケットを受信するポート ID（**vlan-mod-port**）です。リモート ID および回線 ID は設定できます。サブオプションの設定の詳細については、を参照してください。

- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するようなポリシーを実装したりできます。次に DHCP サーバは、DHCP 応答内にオプション 82 フィールドをエコーします。
- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、次のフィールドの値は変化しません（図「サブオプションのパケット形式」を参照）。

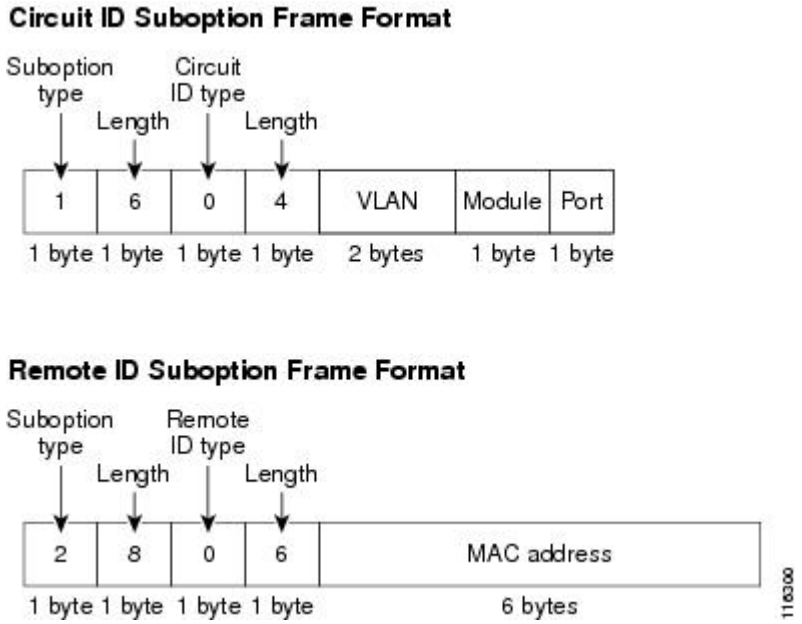
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号が 3 から始まります。たとえば、24 個の 10/100/1000 ポートおよび 4 つの Small Form-Factor Pluggable（SFP）モジュール スロットを搭載するスイッチでは、ポート 3 がギガビット イーサネット 1/0/1 ポート、ポート 4 がギガビット イーサネット 1/0/2 ポートとなり、以降同様に続きます。ポート 27 は SFP モジュール スロットのギガビット イーサネット 1/0/25 となり、以降同様に続きます。

図「サブオプションのパケット形式」に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。回線 ID サブオプションでは、モジュール番号は、スタックにあるスイッチ番号に対応します。スイッチがこれらのパケット形式を使用するのは、DHCP スヌーピングをグローバルにイネーブルにし、

ip dhcp snooping information option グローバル コンフィギュレーション コマンドを入力した場合です。

図 77 : サブオプションのパケット形式



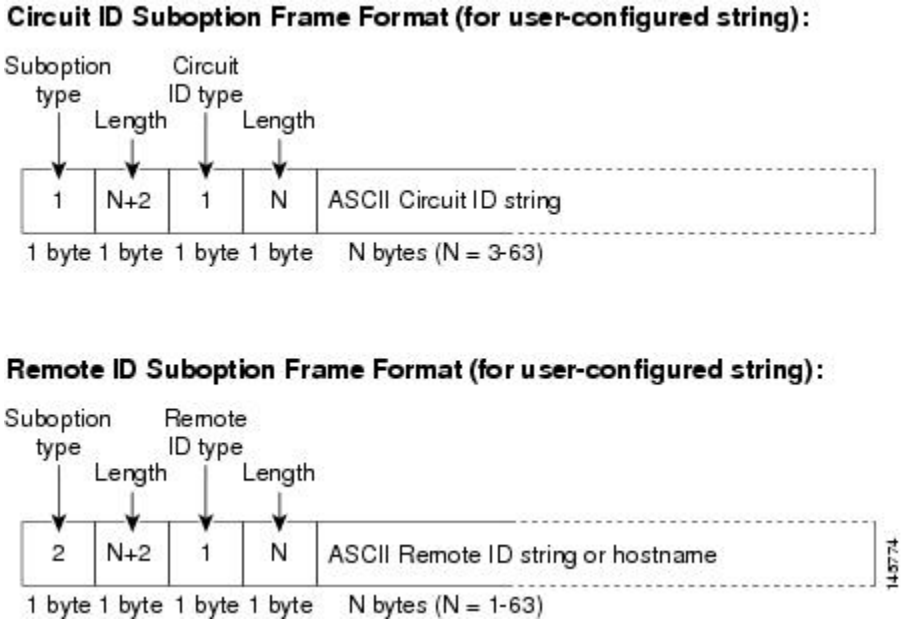
図「ユーザ設定のサブオプションのパケット形式」は、ユーザ設定のリモート ID サブオプション、および回線 ID サブオプションのパケット形式を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力した場合に、これらのパケット形式が使用されます。

パケットでは、リモート ID および回線 ID サブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

- 回線 ID サブオプション フィールド
  - 回線 ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
  - リモート ID タイプが 1 である。

◦設定した文字列の長さに応じて、長さの値が変化する。

図 *78*：ユーザ設定のサブオプションのパケット形式



Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。これには IP アドレス、アドレス バインディング、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てること、または、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てることが可能です。手動および自動アドレス バインディングの詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章を参照してください。

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピング バインディング データベースに保存します。データベースには、64,000 のバインディングを含めることができます。

各データベース エントリ（バインディング）は、IP アドレス、それに関連付けられた MAC アドレス、リース期間（16 進形式）、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。データベース エージェントは、設定された場所のファイルにバインディングを保存します。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、まず 72 バイトのデータがあり、その後に 1 つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP インスペクションまたは IP ソース ガードがイネーブルにされ、DHCP スヌーピング バインディング データベースがダイナミック バインディングされている場合、スイッチは接続を切断されます。このエージェントがディセーブルで、DHCP スヌーピングだけがイネーブルである場合、スイッチの接続は切断されませんが、DHCP スヌーピングは DHCP スプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディング データベースを作成します。スイッチは、データベースに変更が加えられたときにはバインディング ファイルを更新します。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、ただちにデータベース内のエントリを更新します。スイッチはバインディング ファイル内のエントリも更新します。バインディング ファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイルが指定された時間内（書き込み遅延および中断タイムアウトの値によって設定される）に更新されない場合、更新は停止します。

バインディングが含まれるファイルの形式は次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の initial-checksum エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Gi1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 584a38f0
END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを DHCP スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スイッチがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している（スイッチはリース期間の終了時にバインディング エントリを削除しないことがある）。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- インターフェイスがルーテッドインターフェイスまたはDHCP スヌーピングにおける信頼できるインターフェイスである。

DHCP スヌーピングおよびスイッチ スタック

DHCP スヌーピングは、スタック マスターで管理されます。新しいスイッチがスタックに加入すると、スイッチでは、スタック マスターから DHCP スヌーピング設定を受信します。メンバがスタックから除外されると、スイッチに関連付けられているすべての DHCP スヌーピング アドレス バインディングがエージング アウトします。

すべてのスヌーピング統計情報は、スタック マスター上で生成されます。新しいスタック マスターが選出された場合、統計カウンタはリセットされます。

スタックのマージが発生し、スタックマスターではなくなった場合、スタック マスターにあったすべての DHCP スヌーピング バインディングが失われます。スタック パーティションでは、既存のスタック マスターに変更はなく、パーティション化スイッチに属しているバインディングは、エージング アウトします。パーティション化スイッチの新しいマスターでは、新たな着信 DHCP パケットの処理が開始されます。

DHCP 機能の設定方法

DHCP スヌーピングのデフォルト設定

表 *107* : *DHCP* のデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要[12]
DHCP リレー エージェント	イネーブル[13]
DHCP パケット転送アドレス	未設定

機能	デフォルト設定
リレー エージェント情報の確認	イネーブル（無効なメッセージは廃棄）。
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置換。
DHCP スヌーピングをグローバルにイネーブル	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
パケットを信頼できない入力インターフェイスで受け取る DHCP スヌーピング オプション[14]	ディセーブル
DHCP スヌーピング レート制限	未設定
DHCP スヌーピング信頼状態	信頼できない
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピングの MAC アドレス検証	イネーブル
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブル、設定が必要。 （注） スイッチは、DHCP サーバとして設定されているデバイスからだけ、ネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブル、設定が必要。この機能は宛先が設定されている場合に限り有効。

12 スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。
13 スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。
14 この機能は、スイッチがエッジ スイッチによって Option 82 情報が挿入されたパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

- スイッチ ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチ ポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。

- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報を表示したり、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報をクリアしたりできるようになりました。

DHCP サーバの設定

スイッチは、DHCP サーバとして機能できます。

スイッチを DHCP サーバとして設定するときの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の項の「Configuring DHCP」を参照してください。

DHCP サーバとスイッチ スタック

DHCP バインディング データベースは、スタック マスターで管理されます。新しいスタック マスターが割り当てられると、新しいマスターでは、TFTP サーバから保存されているバインディング データベースがダウンロードされます。スタック マスターに障害が発生した場合、未保存のすべてのバインディングが失われます。失われたバインディングに関連付けられていた IP アドレスは、解放されます。自動バックアップは、**ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*] グローバル コンフィギュレーション コマンドを使用して設定する必要があります。

スタックのマージが発生すると、スタック メンバになるスタック マスターでは、すべての DHCP リース バインディングが失われます。スタック パーティションでは、パーティションにある新しいマスターが、既存の DHCP リース バインディングなしで、新しい DHCP サーバとして動作します。

DHCP リレー エージェントの設定

スイッチ上で DHCP リレー エージェントをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **service dhcp**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service dhcp** 例： スイッチ(config)# **service dhcp**	スイッチ上で DHCP サーバおよび DHCP リレー エージェントをイネーブルにします。デフォルトでは、この機能はイネーブルです。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

これらの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の「*Configuring DHCP*」の項を参照してください。

- リレー エージェント情報のチェック（検証）
- リレー エージェント転送ポリシーの設定

パケット転送アドレスの指定

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合、スイッチを **ip helper-address***address* インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的なルールは、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。**ip helper-address** コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、どの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface vlan***vlan-id*
4. **ip address***ip-address subnet-mask*
5. **ip helper-address***address*
6. **end**
7. 次のいずれかを使用します。
   - **interface range***port-range*
   - **interface***interface-id*
8. **switchport mode access**
9. **switchport access vlan***vlan-id*
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface vlan***vlan-id* 例： スイッチ(config)# interface vlan 1	VLAN ID を入力してスイッチ仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address***ip-address subnet-mask* 例： スイッチ(config-if)# ip address 192.108.1.27 255.255.255.0	インターフェイスに IP アドレスおよび IP サブネットを設定します。
ステップ 5	**ip helper-address***address* 例： スイッチ(config-if)# ip helper-address 172.16.1.2	DHCP パケット転送アドレスを指定します。 ヘルパー アドレスは特定の DHCP サーバ アドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 6	**end** 例： スイッチ(config-if)# end	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	次のいずれかを使用します。 • **interface range***port-range* • **interface***interface-id* 例： スイッチ(config)# interface gigabitethernet1/0/2	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス範囲コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**switchport mode access** 例： `スイッチ(config-if)# switchport mode access`	ポートの VLAN メンバーシップ モードを定義します。
ステップ 9	**switchport access vlan***vlan-id* 例： `スイッチ(config-if)# switchport access vlan 1`	ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。
ステップ 10	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP スヌーピングおよび Option 82 を設定するための前提条件

DHCP スヌーピングおよび Option 82 の前提条件は次のとおりです。

- DHCP スヌーピングは、スイッチ上でグローバルにイネーブルにする必要があります。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレーエージェントとして機能するデバイスが設定され、イネーブルになっていることを確認してください。
- スイッチを DHCP 要求に応答するようにする場合は、DHCP サーバとして設定する必要があります。

- スイッチで DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能するデバイスを設定してください。DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。サービスプロバイダーネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。
- DHCP スヌーピングで Cisco IOS DHCP サーバ バインディング データベースを使用するには、Cisco IOS DHCP サーバ バインディング データベースを使用するようにスイッチを設定する必要があります。
- 信頼できない入力でパケットを受け入れる DHCP スヌーピング オプションを使用するには、スイッチがエッジ スイッチから Option 82 情報を含むパケットを受信する集約スイッチである必要があります。
- 次の前提条件が DHCP スヌーピング バインディング データベースの設定に適用されます。
  - DHCP スヌーピング用にスイッチを使用するには、DHCP スヌーピング バインディング データベースで宛先を設定する必要があります。
  - NVRAM とフラッシュ メモリは、いずれも記憶容量が限られているため、バインディング ファイルを TFTP サーバに保存することを推奨します。
  - ネットワーク ベースの URL（TFTP や FTP など）については、スイッチがバインディングをその URL のバインディング ファイルに初めて書き込む前に、設定された URL に空のファイルを作成する必要があります。空のファイルをサーバ上に作成する必要があるかどうかについては、TFTP サーバのマニュアルを参照してください。TFTP サーバによっては、そのように設定できないことがあります。
  - データベースに正しいリース期間が記録されるように、ネットワーク タイム プロトコル（NTP）をイネーブルにし、設定することを推奨します。
  - NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディング ファイルに書き込みます。
- スイッチで DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスを設定してください。DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、デバイスの DHCP オプションを設定するか、または DHCP データベース エージェントをセットアップする必要があります。
- スイッチが DHCP パケットをリレーするようにする場合は、DHCP サーバの IP アドレスは DHCP クライアントのスイッチ仮想インターフェイス（SVI）に設定する必要があります。
- スイッチ ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。

- スイッチ ポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。

関連トピック

DHCP スヌーピング，（1510 ページ）

DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチ上で DHCP スヌーピングをイネーブルにするには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip dhcp snooping**
4. **ip dhcp snooping vlan***vlan-range*
5. **ip dhcp snooping information option**
6. **ip dhcp snooping information option allow-untrusted**
7. **interface***interface-id*
8. **ip dhcp snooping vlan***vlan***information option format-type circuit-id** [**override**] **string***ASCII-string*
9. **ip dhcp snooping trust**
10. **ip dhcp snooping limit rate***rate*
11. **exit**
12. **ip dhcp snooping verify mac-address**
13. **end**
14. **show running-config**
15. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp snooping** 例： スイッチ(config)# **ip dhcp snooping**	DHCP スヌーピングをグローバルにイネーブル化します。
ステップ 4	**ip dhcp snooping vlan***vlan-range* 例： スイッチ(config)# **ip dhcp snooping vlan 10**	VLAN または VLAN 範囲で DHCP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 4094 です。VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。 • VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。
ステップ 5	**ip dhcp snooping information option** 例： スイッチ(config)# **ip dhcp snooping information option**	スイッチが、転送された DHCP 要求メッセージにある DHCP リレー情報（オプション 82 フィールド）を DHCP サーバに挿入したり削除したりできるようにイネーブルにします。これがデフォルト設定です。
ステップ 6	**ip dhcp snooping information option allow-untrusted** 例： スイッチ(config)# **ip dhcp snooping information option allow-untrusted**	（任意）スイッチが、エッジ スイッチに接続された集約スイッチである場合、エッジ スイッチからのオプション 82 情報付き着信 DHCP スヌーピング パケットを受け入れるようにこのコマンドによってスイッチをイネーブルにします。 デフォルト設定では無効になっています。 （注） このコマンドは、信頼できるデバイスに接続された集約スイッチだけで入力してください。
ステップ 7	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**ip dhcp snooping vlan***vlan***information option format-type circuit-id** [**override**] **string***ASCII-string* 例： `スイッチ(config-if)# ip dhcp snooping vlan 1 information option format-type curcuit-id override string ovrride2`	（任意）指定したインターフェイスの回線 ID サブオプションを設定します。 1 ～ 4094 の範囲の VLAN ID を使用して、VLAN およびポート ID を指定します。デフォルトの回線 ID はポート ID で、フォーマットは **vlan-mod-port** です。 回線 ID は 3 ～ 63 の ASCII 文字列（スペースなし）を設定できます。 （任意）**override** キーワードは、加入者情報を定義するための TLV 形式に回線 ID サブオプションを挿入したくない場合に使用します。
ステップ 9	**ip dhcp snooping trust** 例： `スイッチ(config-if)# ip dhcp snooping trust`	（任意）インターフェイスの信頼性を trusted または untrusted に設定します。信頼できないクライアントからのメッセージを受信するようにインターフェイスを設定するには、**no** キーワードを使用します。デフォルト設定は untrusted です。
ステップ 10	**ip dhcp snooping limit rate***rate* 例： `スイッチ(config-if)# ip dhcp snooping limit rate 100`	（任意）インターフェイスが受信できる 1 秒あたりの DHCP パケット数を設定します。指定できる範囲は 1 ～ 2048 です。デフォルトでは、レート制限は設定されません。 （注） 信頼できないインターフェイスのレート制限を 1 秒あたり 100 パケット以下に設定することを推奨します。信頼できるインターフェイスのレート制限を設定する場合、DHCP スヌーピングを使った複数の VLAN に割り当てられたトランク ポートでは、レート制限の値を大きくすることが必要になることがあります。
ステップ 11	**exit** 例： `スイッチ(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**ip dhcp snooping verify mac-address** 例： `スイッチ(config)# ip dhcp snooping verify mac-address`	（任意）信頼できないポートに着信した DHCP パケットの送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認するようにスイッチを設定します。デフォルトでは、送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認します。
ステップ 13	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 14	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 15	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『Cisco IOS IP Configuration Guide, Release 12.4』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

DHCP スヌーピング情報のモニタリング

表 ***108*** : ***DHCP*** 情報を表示するためのコマンド

show ip dhcp snooping	スイッチの DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングだけを表示します。このようなバインディングは、バインディング テーブルとも呼ばれます。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピングの統計情報を要約または詳細形式で表示します。
show ip source binding	動的および静的に設定されたバインディングを表示します。

（注） DHCP スヌーピングがイネーブルでインターフェイスがダウン ステートに変更された場合、静的に設定されたバインディングは削除されません。

DHCP サーバ ポートベースのアドレス割り当ての設定

DHCP サーバ ポートベースのアドレス割り当ての設定の概要

DHCP サーバ ポートベースのアドレス割り当ては、接続されたデバイス クライアントの ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポートで同じ IP アドレスを維持できるようにする機能です。

ネットワークに導入されたイーサネット スイッチは、直接接続されたデバイスに接続を提供します。工場の作業場など、一部の環境では、あるデバイスで不具合が発生した場合は、それと同時に、そのネットワークで代わりのデバイスが動作を開始しなければなりません。現在の DHCP 実装では、この代わりのデバイスに、DHCP が同じ IP アドレスを提供する保証はありません。コントロールやモニタリングなどを行うソフトウェアは、各デバイスに関連付けられた IP アドレスが一定であることを期待しています。デバイスを交換した場合、DHCP クライアントが変更された場合でも、アドレスの割り当ては一定のままでなければなりません。

DHCP サーバ ポートベースのアドレス割り当て機能が設定されている場合、この機能により、ある接続ポートで受信された DHCP メッセージでクライアント ID やクライアント ハードウェア アドレスが変更されたとしても、同じ接続ポートには常に同じ IP アドレスが提供されることが保証されます。DHCP プロトコルは、DHCP パケットのクライアント ID オプションにより、DHCP クライアントを識別します。クライアント ID オプションを含まないクライアントは、クライアント ハードウェア アドレスにより識別されます。この機能を設定すると、インターフェイスのポート名が、クライアント ID またはハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアント ID になります。

すべてのケースで、同じポートにイーサネット ケーブルを接続することにより、接続されたデバイスに、DHCP 経由で同じ IP アドレスが割り当てられます。

DHCP サーバ ポートベースのアドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけです。サードパーティ製のサーバではサポートされていません。

ポートベースのアドレス テーブルのデフォルト設定

デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。

ポートベースのアドレス割り当て設定時の注意事項

- デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。

- DHCP プールから事前に設定された予約への割り当てを制限する（予約されていないアドレスはクライアントに提供されず、その他のクライアントはプールによるサービスを受けない）ために、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力することができます。

DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチ上でDHCPスヌーピングバインディングデータベースエージェントをイネーブルにし、設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip dhcp snooping database** {**flash**[*number*]**:**/*filename* | **ftp:**//*user***:***password***@***host*/*filename* | **http://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** | **rcp:**//*user***@***host*/*filename*}| **tftp:**//*host*/*filename*
4. **ip dhcp snooping database timeout***seconds*
5. **ip dhcp snooping database write-delay***seconds*
6. **end**
7. **ip dhcp snooping binding***mac-address***vlan***vlan-idip-address***interface***interface-id***expiry***seconds*
8. **show ip dhcp snooping database** [**detail**]
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp snooping database** {**flash**[*number*]**:**/*filename*	**ftp:**//*user***:***password***@***host*/*filename*	**http://**[[*username***:***password*]**@**]{*hostname*	*host-ip*}[/*directory*] /*image-name***.tar**	**rcp:**//*user***@***host*/*filename*}| **tftp:**//*host*/*filename*	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイルの URL を指定します。

	コマンドまたはアクション	目的
	例： スイッチ(config)# **ip dhcp snooping database tftp://10.90.90.90/snooping-rp2**	• **flash**[*number*]**:**/*filename* （任意）スタック マスターのスタック メンバ番号を指定するには、*number* パラメータを使用します。*number* の指定できる範囲は 1 ～ 9 です。 • **ftp:**//*user***:***password***@***host*/*filename* • **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** • **rcp:**//*user***@***host*/*filename* • **tftp:**//*host*/*filename*
ステップ 4	**ip dhcp snooping database timeout***seconds* 例： スイッチ(config)# **ip dhcp snooping database timeout 300**	データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間（秒数）を指定します。 デフォルトは 300 秒です。指定できる範囲は 0 ～ 86400 です。無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。
ステップ 5	**ip dhcp snooping database write-delay***seconds* 例： スイッチ(config)# **ip dhcp snooping database write-delay 15**	バインディング データベースが変更されてから転送を開始するまでの遅延時間を指定します。指定できる範囲は 15 ～ 86400 秒です。デフォルトは 300 秒（5 分）です。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**ip dhcp snooping binding***mac-address***vlan***vlan-id ip-address***interface***interface-id***expiry***seconds* 例： スイッチ# **ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000**	（任意）DHCP スヌーピング バインディング データベースにバインディング エントリを追加します。*vlan-id* に指定できる範囲は 1 ～ 4904 です。*seconds* の範囲は 1 ～ 4294967295 です。 このコマンドは、追加するエントリごとに入力します。

	コマンドまたはアクション	目的
		このコマンドは、スイッチをテストまたはデバッグするときに使用します。
ステップ 8	**show ip dhcp snooping database** [**detail**] 例： スイッチ# show ip dhcp snooping database detail	DHCP スヌーピング バインディング データベース エージェントのステータスおよび統計情報を表示します。
ステップ 9	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルにイネーブル化し、インターフェイス上で加入者 ID を自動的に生成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip dhcp use subscriber-id client-id**
4. **ip dhcp subscriber-id interface-name**
5. **interface***interface-id*
6. **ip dhcp server use subscriber-id client-id**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp use subscriber-id client-id** 例： スイッチ(config)# **ip dhcp use subscriber-id client-id**	すべての着信 DHCP メッセージで、加入者 ID がクライアント ID としてグローバルに使用されるように DHCP サーバを設定します。
ステップ 4	**ip dhcp subscriber-id interface-name** 例： スイッチ(config)# **ip dhcp subscriber-id interface-name**	インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。 特定のインターフェイスで設定された加入者 ID は、このコマンドで優先されます。
ステップ 5	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip dhcp server use subscriber-id client-id** 例： スイッチ(config-if)# **ip dhcp server use subscriber-id client-id**	インターフェイス上ですべての着信 DHCP メッセージで、加入者 ID がクライアント ID として使用されるように DHCP サーバを設定します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

スイッチ上でのDHCPポートベースのアドレス割り当てをイネーブルにした後で、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用して、IPアドレスの事前割り当てと、クライアントへの関連付けを行います。

DHCP サーバ ポートベースのアドレス割り当てのモニタリング

表 *109* : *DHCP* ポートベースのアドレス割り当て情報を表示するためのコマンド

コマンド	目的
show interface*interface id*	特定のインターフェイスのステータスおよび設定を表示します。
show ip dhcp pool	DHCP アドレス プールを表示します。
show ip dhcp binding	Cisco IOS DHCP サーバのアドレス バインディングを表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
DHCP 設定情報および手順	『IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3S』 http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/dhcp-xe-3s-book.html

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

第 67 章

IP ソース ガードの設定

IP ソース ガード（IPSG）は、ルーティングされないレイヤ2インターフェイス上の IP トラフィックを制限するセキュリティ機能で、DHCP スヌーピング バインディング データベースと手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングすることで実現されます。

この章は、次の内容で構成されています。

- 機能情報の確認，1537 ページ
- IP ソース ガードの概要，1538 ページ
- IP ソース ガードの設定方法，1540 ページ
- IP ソース ガードのモニタリング，1544 ページ
- その他の参考資料，1545 ページ

機能情報の確認

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

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

IP ソース ガードの概要

IP ソース ガード

ネイバーの IP アドレスを使用する場合に、トラフィック攻撃を防ぐために IP ソース ガードを使用でき、そして信頼できないインターフェイスで DHCP スヌーピングがイネーブルの場合に、IP アドレスを使用しようとすると、IP ソース ガードをイネーブルにできます。

インターフェイス上でIPSGをイネーブルにすると、スイッチは、DHCPスヌーピングにより許可された DHCP パケットを除き、このインターフェイスで受信したすべての IP トラフィックをブロックします。

スイッチは IP アドレスをポートにバインドするためにハードウェアの発信元 IP 検索テーブルを使用します。IP および MAC のフィルタリングでは、送信元 IP 検索および送信元 MAC 検索が組み合わせが使用されます。送信元 IP アドレスを使用する IP トラフィックでは、バインディング テーブルが許可され、他のすべてのトラフィックは拒否されます。

IP ソース バインディング テーブルには、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング（スタティック IP 送信元バインディング）があります。このテーブルのエントリには IP アドレスと、関連 MAC アドレス、および関連 VLAN 番号があります。スイッチは、IP ソース ガードがイネーブルにされている場合だけ、IP ソース バインディング テーブルを使用します。

IPSGは、アクセス ポートおよびトランク ポートを含むレイヤ2ポートだけでサポートされます。送信元 IP アドレスと送信元 IP および MAC アドレス フィルタリングで IPSG を設定できます。

スタティック ホスト用 IP ソース ガード

（注） アップリンク ポート、またはトランク ポートで、スタティック ホスト用 IP ソース ガード（IPSG）を使用しないでください。

スタティック ホスト用 IPSG は、IPSG の機能を DHCP ではない、スタティックな環境に拡張するものです。これまでの IPSG は、DHCP スヌーピングにより作成されたエントリを使用して、スイッチに接続されたホストを検証していました。ホストから受信したトラフィックのうち、有効な DHCP を持たないものはすべてドロップされます。このセキュリティ機能によって、ルーティングされないレイヤ2インターフェイス上のIP トラフィックが制限されます。この機能は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングします。前バージョンの IPSG では、IPSG を動作させるために DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしで IPSG を動作させることができます。スタティック ホスト用 IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブル エントリに依存しています。このスイッチは、指定されたポートで有効なホストのリストを維持するために、ARP リクエスト、またはその他の IP パケットに基づいてスタティック エントリ

を作成します。また、指定されたポートにトラフィックを送信できるホストの数を指定することもできます。これはレイヤ 3 でのポート セキュリティと同じです。

スタティック ホスト用 IPSG はダイナミック ホストもサポートしています。ダイナミック ホストが、IP DHCP スヌーピング テーブルに存在する DHCP が割り当てられた IP アドレスを受信すると、IP デバイス トラッキング テーブルは同じエントリを学習します。スタック化環境では、マスターのフェールオーバーが発生すると、メンバ ポートに接続されたスタティック ホストの IP ソース ガード エントリは、そのまま残ります。**show ip device tracking all** 特権 EXEC コマンドを入力すると、IP デバイス トラッキング テーブルには、これらのエントリが ACTIVE であると表示されます。

（注） 複数のネットワーク インターフェイスを持つ IP ホストの一部は、ネットワーク インターフェイスに無効なパケットを注入することができます。この無効なパケットには、ソース アドレスとして、別のホスト ネットワーク インターフェイスの IP アドレス、または MAC アドレスが含まれます。この無効パケットは、スタティック ホスト用 IPSG がホストに接続され、無効な IP アドレス バインディングまたは MAC アドレス バインディングが学習されて、有効なバインディングが拒否される原因となります。ホストによる無効なパケットの注入を回避する方法については、対応するオペレーティング システムとネットワーク インターフェイスのベンダーにお問い合わせください。

最初、スタティック ホスト用 IPSG は ACL ベースのスヌーピング メカニズムを通じて、動的に IP バインディング、または MAC バインディングを学習します。IP バインディング、または MAC バインディングは、ARP パケット、および IP パケットにより、スタティック ホストから学習されます。これらはデバイス トラッキング データベースに保存されます。指定されたポートで動的に学習、または静的に設定された IP アドレスの数が最大値に達した場合、新しい IP アドレスを持つパケットはすべて、ハードウェアによりドロップされます。何らかの理由で移動された、またはなくなったホストを解決するために、スタティック ホスト用 IPSG は IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングをエージング アウトします。この機能は、DHCP スヌーピングとともに使用できます。複数バインディングは、DHCP ホストとスタティック ホストの両方に接続されたポートに確立されます。たとえば、バインディングは、デバイス トラッキング データベースと DHCP スヌーピング バインディング データベースの両方に保存されます。

IP ソース ガードの設定時の注意事項

- スタティック IP バインディングは、非ルーテッド ポートだけで設定できます。ルーテッド インターフェイスで **ip source binding***mac-address***vlan***vlan-id ip-address***interface***interface-id* グローバル コンフィギュレーション コマンドを入力すると、次のエラー メッセージが表示されます。

```
Static IP source binding can only be configured on switch port.
```

- 送信元 IP フィルタリング機能を持つ IP ソース ガードがインターフェイスでイネーブルにされている場合、このインターフェイスのアクセス VLAN で、DHCP スヌーピングをイネーブルにしておく必要があります。

- 複数の VLAN を持つトランク インターフェイス上で IP ソース ガードをイネーブルにし、これらすべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。

（注） IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切にトラフィックをフィルタリングできない可能性があります。

- この機能は、802.1x ポートベースの認証がイネーブルにされている場合にイネーブルにできます。

IP ソース ガードの設定方法

IP ソース ガードのイネーブル化

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip verify source** [**mac-check**]
5. **exit**
6. **ip source binding***mac-address***vlan***vlan-id ip-address***interface***interface-id*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip verify source** [**mac-check**] 例： スイッチ(config-if)# **ip verify source**	送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 （任意）**mac-check**：送信元 IP アドレスによる IP ソース ガードおよび MAC アドレス フィルタリングをイネーブルにします。
ステップ 5	**exit** 例： スイッチ(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip source binding***mac-address***vlan***vlan-id ip-address***interface***interface-id* 例： スイッチ(config)# **ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1**	スタティック IP ソース バインディングを追加します。 スタティック バインディングごとにこのコマンドを入力します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定

スタティック ホスト用 IPSG を動作させるには、**ip device trackingmaximum***limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルにイネーブルにしていない、または IP device tracking maximum をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip device tracking**
4. **interface***interface-id*
5. **switchport mode access**
6. **switchport access vlan***vlan-id*
7. **ip verify source**[**tracking**] [**mac-check**]
8. **ip device tracking maximum***number*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip device tracking** 例： スイッチ(config)# **ip device tracking**	IP ホスト テーブルをオンにし、IP デバイス トラッキングをグローバルにイネーブルにします。
ステップ 4	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access** 例： スイッチ(config-if)# **switchport mode access**	アクセスとしてポートを設定します。
ステップ 6	**switchport access vlan***vlan-id* 例： スイッチ(config-if)# **switchport access vlan 10**	このポートに VLAN を設定します。
ステップ 7	**ip verify source**[**tracking**] [**mac-check**] 例： スイッチ(config-if)# **ip verify source tracking mac-check**	送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 （任意）**tracking**：スタティック ホスト用 IP ソース ガードをイネーブルにします。 （任意）**mac-check**：MAC アドレス フィルタリングをイネーブルにします。 **ip verify source tracking mac-check** コマンドは、MAC アドレス フィルタリングのあるスタティック ホストに対して IP ソース ガードをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 8	**ip device tracking maximum***number* 例： スイッチ(config-if)# **ip device tracking maximum 8**	そのポートで、IPデバイストラッキングテーブルにより許可されるスタティック IP 数の上限を設定します。指定できる範囲は 1 ～ 10 です。最大値は 10 です。 （注） **ip device trackingmaximum***limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

IP ソース ガードのモニタリング

表 *110*：特権 *EXEC* 表示コマンド

コマンド	目的
show ip verify source [**interface***interface-id*]	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。
show ip device tracking { **all** | **interface***interface-id* | **ip***ip-address* | **mac***imac-address*}	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。

表 *111*：インターフェイス コンフィギュレーション コマンド

コマンド	目的
ip verify source tracking	データ ソースを確認します。

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

その他の参考資料

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

第 68 章

ダイナミック ARP インスペクションの設定

- 機能情報の確認，1547 ページ
- ダイナミック ARP インスペクションの制約事項，1548 ページ
- ダイナミック ARP インスペクションの概要，1549 ページ
- ダイナミック ARP インスペクションのデフォルト設定，1554 ページ
- ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ，1554 ページ
- 非 DHCP 環境での ARP ACL の設定，1555 ページ
- DHCP 環境でのダイナミック ARP インスペクションの設定，1558 ページ
- 着信 ARP パケットのレート制限，1561 ページ
- ダイナミック ARP インスペクション検証チェックの実行，1564 ページ
- DAI のモニタリング，1565 ページ
- DAI の設定の確認，1566 ページ
- その他の参考資料，1567 ページ

機能情報の確認

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

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

ダイナミック ARP インスペクションの制約事項

ここでは、スイッチにダイナミック ARP インスペクションを設定するときの制約事項および注意事項を示します。

- ダイナミック ARP インスペクションは入力セキュリティ機能です。出力チェックはまったく行いません。
- ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションをサポートしていないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されるホストに対しては有効ではありません。中間者攻撃は単一のレイヤ 2 ブロードキャスト ドメインに制限されているため、チェックされないドメインと、ダイナミック ARP インスペクションによりチェックされるドメインは区別します。このアクションは、ダイナミック ARP インスペクションのためにイネーブルにされているドメインでホストの ARP キャッシュを保護します。
- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

  DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可または拒否を行います。
- ダイナミック ARP インスペクションは、アクセス ポート、トランク ポート、および EtherChannel ポートでサポートされます。

  （注） RSPAN VLAN では、ダイナミック ARP インスペクションをイネーブルにしないでください。RSPAN VLAN でダイナミック ARP インスペクションをイネーブルにすると、ダイナミック ARP インスペクション パケットが RSPAN 宛先ポートに届かない可能性があります。
- 物理ポートを EtherChannel ポートチャネルに結合するには、この物理ポートとチャネル ポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポートチャネル内で中断状態のままとなります。ポートチャネルは、チャネルと結合された最初の物理ポートの信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態と一致する必要はありません。

  逆に、ポートチャネルで信頼状態を変更すると、スイッチは、チャネルを構成するすべての物理ポートで新しい信頼状態を設定します。
- レート制限は、スイッチ スタックの各スイッチで別々に算出されます。クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも高い可能性があることを意味します。たとえば、レート制限が 30 pps に設定された EtherChannel で、スイッチ 1 に 1 つのポート、およびスイッチ 2 に 1 つのポートがある場合、EtherChannel が errdisable にならずに、各ポートは 29 pps でパケットを受信できます。

- ポートチャネルの動作レートは、チャネル内のすべての物理ポートによる累積値です。たとえば、ポートチャネルの ARP レート制限を 400 pps に設定すると、このチャネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャネル メンバーからの受信パケット レートの合計となります。EtherChannel ポートのレート制限は、各チャネル ポート メンバーが受信する ARP パケットのレートを確認してから設定してください。

  物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポートチャネルの設定に照合して検査されます。ポートチャネルのレート制限設定は、物理ポートの設定には依存しません。

  EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャネル（すべての物理ポートを含む）は errdisable ステートとなります。

- 着信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートの集約を反映し、複数のダイナミック ARP インスペクションがイネーブルにされた VLAN にわたってパケットを処理するために、トランク ポートのレートをより高く設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用して、レートを無制限に設定することもできます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。

- スイッチで、ダイナミック ARP インスペクションをイネーブルにすると、ARP トラフィックをポリシングするように設定されたポリサーの有効性は失われます。この結果、すべての ARP トラフィックは CPU に送信されます。

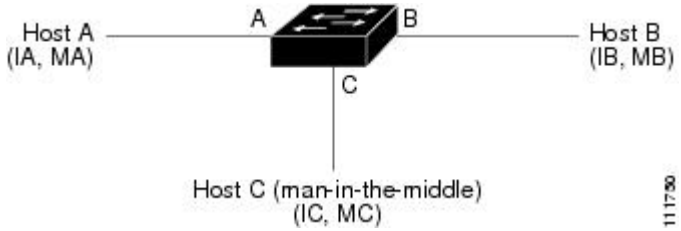
ダイナミック ARP インスペクションの概要

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B はホスト A に情報を送信する必要がありますが、ARP キャッシュにホスト A の MAC アドレスを持っていないとします。ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャスト ドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロードキャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。しかし、ARP は、ARP 要求が受信されなった場合でも、ホストからの余分な応答を許可するため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生することがあります。攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイ

ヤ2ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。図 26-1 に、ARP キャッシュ ポイズニングの例を示します。

図 *79*：*ARP* キャッシュ ポイズニング



ホストA、B、およびCは、インターフェイスA、B、およびC上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。カッコ内に示されているのは、これらのIPアドレス、およびMACアドレスです。たとえば、ホストAが使用するIPアドレスはIA、MACアドレスは MA です。ホスト A が IP レイヤにあるホスト B と通信する必要がある場合、ホスト A はIP アドレス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。スイッチとホスト B は、この ARP 要求を受信すると、IP アドレスが IA で、MAC アドレスが MA のホストに対する ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は、MAC アドレス MA にバインドされています。ホスト B が応答すると、スイッチ、およびホスト A は、IP アドレスが IB で、MAC アドレスが MB のホストに対するバインディングを ARP に読み込みます。

ホスト C は、IP アドレスが IA（または IB）で、MAC アドレスが MC のホストに対するバインディングを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホストA、およびホスト B の ARP キャッシュをポイズニングすることができます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は自身をホスト A からホスト B へのトラフィック ストリームに挿入します。従来の中間者攻撃です。

ダイナミック ARP インスペクションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。この機能により、ネットワークをある種の中間者攻撃から保護することができます。

ダイナミック ARP インスペクションにより、有効な ARP 要求と応答だけが確実にリレーされるようになります。スイッチが実行する機能は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカルARPキャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

ダイナミック ARP インスペクションは、信頼できるデータベースである DHCP スヌーピング バインディング データベースに格納されている有効な IP/MAC アドレス バインディングに基づいて、ARP パケットの正当性を判断します。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピングにより構築されます。信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、このパケットを転送します。信頼できないインターフェイスでは、スイッチはこのパケットが有効である場合だけ、このパケットを転送します。

ip arp inspection vlan *vlan-range* グローバル コンフィギュレーション コマンドを使用して、VLAN ごとにダイナミック ARP インスペクションをイネーブルにすることができます。

非 DHCP 環境では、ダイナミック ARP インスペクションは、静的に設定された IP アドレスを持つホストに対するユーザ設定の ARP アクセス コントロール リスト（ACL）と照らし合わせて、ARP パケットの正当性を確認することができます。ARP ACL を定義するには、**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用します。

パケットの IP アドレスが無効である場合、または ARP パケットの本文にある MAC アドレスが、イーサネット ヘッダーで指定されたアドレスと一致しない場合、ARP パケットをドロップするようにダイナミック ARP インスペクションを設定することができます。このためには、**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} グローバル コンフィギュレーション コマンドを使用します。

インターフェイスの信頼状態とネットワーク セキュリティ

ダイナミック ARP インスペクションは、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイスに到着するパケットは、ダイナミック ARP インスペクションの確認検査をすべてバイパスし、信頼できないインターフェイスに到着するパケットには、ダイナミック ARP インスペクションの検証プロセスを受けます。

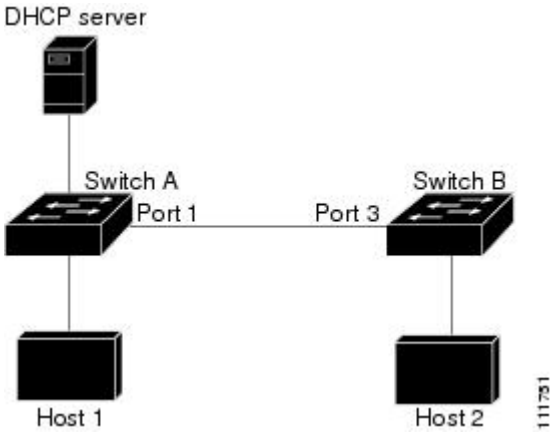
一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチ ポートすべてを信頼できるものに設定します。この構成では、指定されたスイッチからネットワークに入ってくる ARP パケットはすべて、セキュリティ チェックをバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、ip arp inspection trust インターフェイス コンフィギュレーション コマンドを使用します。

注意 信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

次の図では、スイッチ A とスイッチ B の両方が、ホスト 1 とホスト 2 を含む VLAN でダイナミック ARP インスペクションを実行しているとします。ホスト 1 とホスト 2 が、スイッチ A に接続している DHCP サーバから IP アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。したがって、スイッチ A とスイッチ B 間のインターフェイス

が信頼できない場合は、ホスト 1 からの ARP パケットはスイッチ B ではドロップされ、ホスト 1 およびホスト 2 の間の接続は切断されます。

図 *80*：ダイナミック *ARP* インスペクションのためにイネーブルにされた *VLAN* 上の *ARP* パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティ ホールが生じます。スイッチ A でダイナミック ARP インスペクションが実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの間のリンクが信頼できるものとして設定されている場合はホスト 2）。この状況は、スイッチ B がダイナミック ARP インスペクションを実行している場合でも発生します。

ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションを実行しているスイッチに接続された（信頼できないインターフェイス上の）ホストが、そのネットワークにあるその他のホストの ARP キャッシュをポイズニングしていないことを保証します。しかし、ダイナミック ARP インスペクションにより、ネットワークの他の部分にあるホストが、ダイナミック ARP インスペクションを実行しているスイッチに接続されているホストのキャッシュをポイズニングできないようにすることはできません。

VLAN のスイッチの一部がダイナミック ARP インスペクションを実行し、残りのスイッチは実行していない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定します。ただし、非ダイナミック ARP インスペクションスイッチからパケットのバインディングを検証するには、ARP ACL を使用して、ダイナミック ARP インスペクションを実行するスイッチを設定します。このようなバインディングが判断できない場合は、レイヤ 3 で、ダイナミック ARP インスペクション スイッチを実行していないスイッチから、ダイナミック ARP インスペクションを実行しているスイッチを分離します。

（注） DHCP サーバとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。デフォルトでは、信頼できないインターフェイスのレートは 15 パケット/秒（pps）です。信頼できるインターフェイスはレート制限されません。この設定を変更するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。ユーザが介入するまで、ポートはこの状態を維持します。**errdisable recovery** グローバル コンフィギュレーション コマンドを使用すると、errdisable ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。

（注） EtherChannel のレート制限は、スタックにある各スイッチに個別に適用されます。たとえば、EtherChannel で 20 pps の制限が設定されている場合、EtherChannel にあるポートの各スイッチでは、最大 20 pps まで実行できます。スイッチが制限を超過した場合、EtherChannel 全体が errdisable ステートになります。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのは、ACL が **ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用して設定されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

廃棄パケットのロギング

スイッチがパケットをドロップすると、ログ バッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。各ログ エントリには、受信側の VLAN、ポート番号、送信元 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定します。記録されるパケットの種類を指定するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ARP インスペクションのデフォルト設定

機能	デフォルト設定
ダイナミック ARP インスペクション	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
着信 ARP パケットのレート制限	1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチドネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。 信頼できるすべてのインターフェイスでは、レート制限は行われません。 バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。
ログ バッファ	ダイナミック ARP インスペクションがイネーブル化されると、拒否またはドロップされた ARP パケットはすべてが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは 1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのは、ACL が ip arp inspection filter vlan グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

非 DHCP 環境での ARP ACL の設定

この手順は、図 2 に示すスイッチ B がダイナミック ARP インスペクション、または DHCP スヌーピングをサポートしていないときにダイナミック ARP インスペクションを設定する方法を示しています。

スイッチ A のポート 1 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、スイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが作り出されます。これを阻止するには、スイッチ A のポート 1 を信頼できないものとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない（スイッチ A で ACL 設定を適用することは不可能である）場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを使用してパケットをルートする必要があります。

スイッチ A で ARP ACL を設定するには、次の手順を実行します。この手順は、非 DHCP 環境では必須です。

手順の概要

1. **enable**
2. **configureterminal**
3. **arp access-list***acl-name*
4. **permit ip host***sender-ip***mac host***sender-mac*
5. **exit**
6. **ip arp inspection filter***arp-acl-name* **vlan***vlan-range* [**static**]
7. **interface***interface-id*
8. **no ip arp inspection trust**
9. **end**
10. 次の show コマンドを使用します。
    - **show arp access-list**acl-name
    - **show ip arp inspection vlan***vlan-range*
    - **show ip arp inspection interfaces**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**arp access-list***acl-name*	ARP ACL を定義し、ARP アクセス リスト コンフィギュレーション モードを開始します。デフォルトでは、ARPアクセスリストは定義されません。 （注） ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。
ステップ 4	**permit ip host***sender-ip***mac host***sender-mac*	指定されたホスト（ホスト 2）からの ARP パケットを許可します。 • *sender-ip* には、ホスト 2 の IP アドレスを入力します。 • *sender-mac* には、ホスト 2 の MAC アドレスを入力します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip arp inspection filter***arp-acl-name* **vlan***vlan-range* [**static**]	VLAN に ARP ACL を適用します。デフォルトでは、定義済みの ARP ACL は、どのような VLAN にも適用されません。 • *arp-acl-name* には、ステップ 2 で作成した ACL の名前を指定します。 • *vlan-range* では、スイッチとホストが存在する VLAN を指定します。VLAN ID 番号により識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）**static** を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットは廃棄されます。DHCP バインディングは使用されません。 このキーワードを指定しない場合は、ACL内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、

	コマンドまたはアクション	目的
		ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。 IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセス リストで許可された場合だけに許可されます。
ステップ 7	**interface***interface-id*	スイッチ B に接続されたスイッチ A のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**no ip arp inspection trust**	スイッチ B に接続されたスイッチ A のインターフェイスを untrusted として設定します。 デフォルトでは、すべてのインターフェイスは信頼できません。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	次の show コマンドを使用します。 • **show arp access-list**acl-name • **show ip arp inspection vlan***vlan-range* • **show ip arp inspection interfaces**	入力を確認します。
ステップ 11	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	例： スイッチ# **copy running-config startup-config**	

DHCP 環境でのダイナミック ARP インスペクションの設定

はじめる前に

この手順では、2つのスイッチがダイナミック ARPインスペクションをサポートしているときに、この機能を設定する方法を示します。ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B にそれぞれ接続されています。スイッチは両方とも、ホストが配置されている VLAN 1 でダイナミック ARP インスペクションを実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。したがって、スイッチ A はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。

（注） 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

ダイナミック ARPインスペクションを設定するには、次の手順を実行します。この処理は、両方のスイッチで行う必要があります。この手順は必須です。

手順の概要

1. **enable**
2. **show cdp neighbors**
3. **configureterminal**
4. **ip arp inspection vlan***vlan-range*
5. **Interface***interface-id*
6. **ip arp inspection trust**
7. **end**
8. **show ip arp inspection interfaces**
9. **show ip arp inspection vlan***vlan-range*
10. **show ip dhcp snooping binding**
11. **show ip arp inspection statistics vlan***vlan-range*
12. **configureterminal**
13. **configureterminal**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**show cdp neighbors** 例： スイッチ(config-if)#**show cdp neighbors**	スイッチ間の接続を確認します。
ステップ 3	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**ip arp inspection vlan***vlan-range* 例： スイッチ(config)# **ip arp inspection vlan 1**	VLAN 単位で、ダイナミック ARP インスペクションをイネーブルにします。デフォルトでは、すべての VLAN 上でダイナミック ARP インスペクションはディセーブルになっています。vlan-range には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。両方のスイッチに同じ VLAN ID を指定します。

	コマンドまたはアクション	目的
ステップ 5	**Interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	他のスイッチに接続されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip arp inspection trust** 例： スイッチ(config-if)#**ip arp inspection trust**	スイッチ間の接続を trusted に設定します。デフォルトでは、すべてのインターフェイスは信頼できません。 スイッチは、信頼できるインターフェイスにあるもう 1 つのスイッチから受信した ARP パケットは確認しません。この場合、パケットはそのまま転送されます。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。
ステップ 7	**end** 例： スイッチ(config-if)#**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip arp inspection interfaces** 例：	インターフェイスでダイナミック ARP インスペクションの設定を検証します。
ステップ 9	**show ip arp inspection vlan***vlan-range* 例： スイッチ(config-if)#**show ip arp inspection vlan 1**	VLAN でダイナミック ARP インスペクションの設定を検証します。
ステップ 10	**show ip dhcp snooping binding** 例： スイッチ(config-if)#**show ip dhcp snooping binding**	DHCP バインディングを確認します。
ステップ 11	**show ip arp inspection statistics vlan***vlan-range* 例： スイッチ(config-if)#**show ip arp inspection statistics vlan 1**	VLAN でダイナミック ARP インスペクションの統計情報を確認します。

	コマンドまたはアクション	目的
ステップ 12	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

着信 ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。errordisable 回復をイネーブルにして、指定されたタイムアウト時間の後にポートがこのステートから自動的に抜け出すようにするまで、ポートはこのステートのままです。

（注） インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、レート制限をその信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

着信 ARP パケットのレートを制限するには、次の手順を実行します。この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip arp inspection limit {rate pps [burst interval seconds] | none}**
5. **exit**
6. 次のコマンドを使用します。
   - **errdisable detect cause arp-inspection**
   - **errdisable recovery cause arp-inspection**
   - **errdisable recovery interval** *interval*
7. **exit**
8. 次の show コマンドを使用します。
   - **show ip arp inspection interfaces**
   - **show errdisable recovery**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id*	レート制限されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip arp inspection limit {rate pps [burst interval seconds] | none}**	インターフェイス上の着信 ARP 要求および ARP 応答のレートを制限します。デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。バースト インターバルは 1 秒です。

	コマンドまたはアクション	目的
		キーワードの意味は次のとおりです。 • **rate***pps* には、1秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ～ 2048 pps です。 • （任意）**burst interval***seconds* は、レートの高い ARP パケットの有無についてインターフェイスがモニタリングされる間隔（秒）を指定します。指定できる範囲は 1 ～ 15 です。 • **rate none** では、処理できる着信 ARP パケットのレートの上限を設定しません。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	次のコマンドを使用します。 • **errdisable detect cause arp-inspection** • **errdisable recovery cause arp-inspection** • **errdisable recovery interval** *interval*	（任意）ダイナミック ARP インスペクションの errdisable ステートからのエラー回復をイネーブルにし、ダイナミック ARP インスペクションの回復メカニズムで使用する変数を設定します。 デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。 **interval***interval* には、error-disabled ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。
ステップ 7	**exit**	特権 EXEC モードに戻ります。
ステップ 8	次の show コマンドを使用します。 • **show ip arp inspection interfaces** • **show errdisable recovery**	設定を確認します。
ステップ 9	**show running-config** **例：** スイッチ# **show running-config**	入力を確認します。
ステップ 10	**copy running-config startup-config** **例：** スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ダイナミック ARP インスペクション検証チェックの実行

ダイナミック ARP インスペクションは、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。宛先 MAC アドレス、送信側および宛先の IP アドレス、および送信元 MAC アドレスで追加検証を実行するように、スイッチを設定できます。

着信 ARP パケットで特定のチェックを実行するには、次の手順を実行します。この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip arp inspection validate {[src-mac] [dst-mac] [ip]}**
4. **exit**
5. **show ip arp inspection vlan***vlan-range*
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip arp inspection validate {[src-mac] [dst-mac] [ip]}**	着信 ARP パケットで特定の検査を実行します。デフォルトでは、検証は実行されません。 キーワードの意味は次のとおりです。 • **src-mac** では、イーサネット ヘッダーの送信元 MAC アドレスと ARP 本文の送信元 MAC アドレスが比較されます。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。

	コマンドまたはアクション	目的
		• **dst-mac** では、イーサネットヘッダーの宛先MACアドレスとARP本文の宛先 MAC アドレスが比較されます。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なるMACアドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **ip** では、ARP 本文から、無効な IP アドレスや予期しない IP アドレスがないかを確認します。アドレスには0.0.0.0、255.255.255.255、およびすべての IP マルチキャストアドレスが含まれます。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。 少なくとも1つのキーワードを指定する必要があります。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが src および dst mac の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番めのコマンドによって src および dst mac の検証がディセーブルになります。
ステップ 4	**exit**	特権 EXEC モードに戻ります。
ステップ 5	**show ip arp inspection vlan***vlan-range*	設定を確認します。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DAI のモニタリング

DAI をモニタするには、次のコマンドを使用します。

コマンド	説明
clear ip arp inspection statistics	ダイナミック ARP インスペクション統計情報をクリアします。
show ip arp inspection statistics [**vlan** *vlan-range*]	指定の VLAN において、転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。
clear ip arp inspection log	ダイナミック ARP インスペクション ログ バッファをクリアします。
show ip arp inspection log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

show ip arp inspection statistics コマンドでは、スイッチは信頼されたダイナミック ARP インスペクション ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

DAI の設定の確認

DAI の設定を表示して確認するには、次のコマンドを使用します。

コマンド	説明
show arp access-list [*acl-name*]	ARP ACL についての詳細情報を表示します。
show ip arp inspection interfaces [interface-id]	指定されたインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。

コマンド	説明
show ip arp inspection vlan *vlan-range*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。

その他の参考資料

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

第 69 章

IEEE 802.1x ポートベースの認証の設定

この章では、IEEE 802.1x ポート ベース認証を設定する方法について説明します。IEEE 802.1x 認証は、不正なデバイス（クライアント）によるネットワーク アクセスを防止します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチまたはスイッチ スタックを意味します。

- 機能情報の確認，1569 ページ
- 802.1x ポートベース認証について，1569 ページ
- 802.1x ポートベース認証の設定方法，1608 ページ
- 802.1x の統計情報およびステータスのモニタリング，1670 ページ
- その他の参考資料，1671 ページ

機能情報の確認

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

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

802.1x ポートベース認証について

802.1x 規格では、一般の人がアクセス可能なポートから不正なクライアントが LAN に接続しないように規制する（適切に認証されている場合を除く）、クライアント/サーバ型のアクセス コントロールおよび認証プロトコルを定めています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN が提供するサービスを利用できるようにします。

（注） TACACS は、802.1x 認証ではサポートされていません。

802.1x アクセス コントロールでは、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、およびスパニングツリー プロトコル（STP）トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

（注） RADIUS および AAA のデバッグのログを表示するには、**show platform software trace message smd** コマンドを使用します。詳細については、『*Command Reference Guide, Cisco IOS XE Denali 16.1.1*』の「Trace Commands」の項を参照してください。

ポートベース認証プロセス

IEEE 802.1X ポートベース認証を設定するには、認証、認可、およびアカウンティング（AAA）を有効にし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

AAA プロセスは認証から始まります。802.1x ポートベース認証がイネーブルであり、クライアントが 802.1x 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

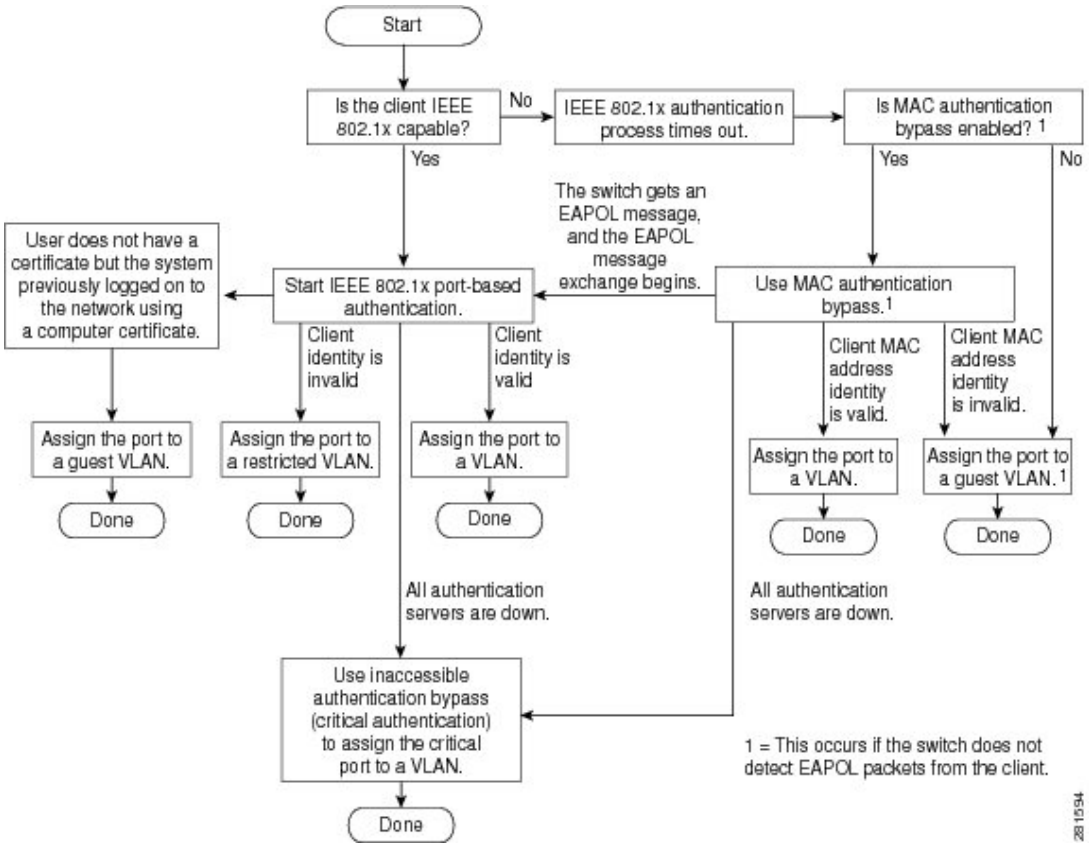
- クライアント ID が有効で 802.1x 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。

（注） アクセスできない認証バイパスは、クリティカル認証、または AAA 失敗ポリシーとも呼ばれます。

ポートでMulti Domain Authentication（MDA）がイネーブルになっている場合、音声許可に該当する例外をいくつか伴ったフローを使用できます。

次の図は認証プロセスを示します。

図 *81*：認証フローチャート



次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

  スイッチ固有の値を使用するか、RADIUS サーバからの値に基づいて再認証タイマーを設定できます。

  RADIUS サーバを使用した 802.1x 認証の後で、スイッチは Session-Timeout RADIUS 属性（Attribute[27]）、および Termination-Action RADIUS 属性（Attribute[29]）に基づいてタイマーを使用します。

  Session-Timeout RADIUS 属性（Attribute[27]）には再認証が行われるまでの時間を指定します。

  Termination-Action RADIUS 属性（Attribute[29]）には、再認証中に行われるアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。アクションに *Initialize*（属性値は *DEFAULT*）を設定した場合、802.1x セッションは終了し、認証中、接続は失わ

れます。アクションに *ReAuthenticate*（属性値は RADIUS-Request）を設定した場合、セッションは再認証による影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface***interface-id* 特権 EXEC コマンドを入力します。

ポートベース認証の開始およびメッセージ交換

802.1x 認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにすると、スイッチは、リンク ステートがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

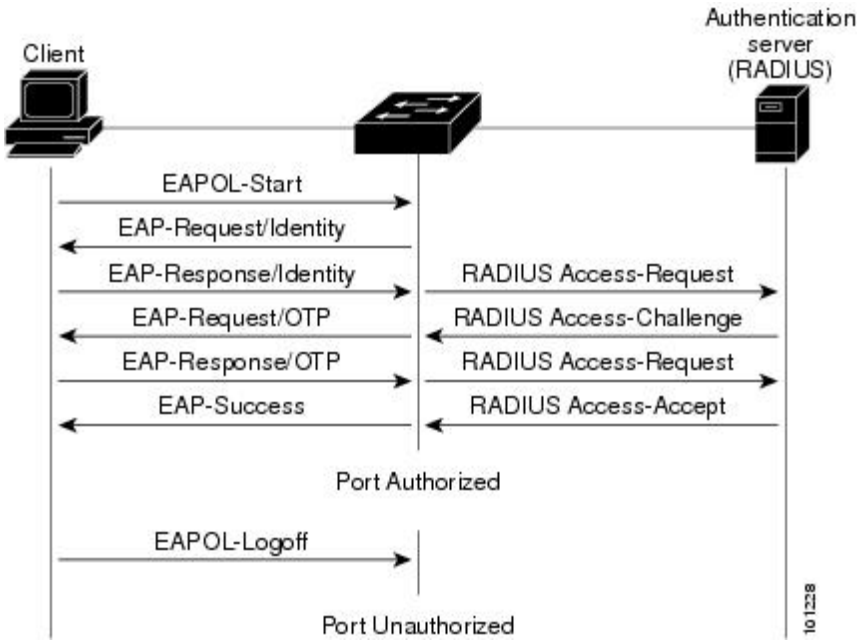
（注） ネットワーク アクセス デバイスで 802.1x 認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。

次の図に、クライアントがRADIUSサーバとの間でOTP（ワンタイム パスワード）認証方式を使用する際に行われるメッセージ交換を示します。

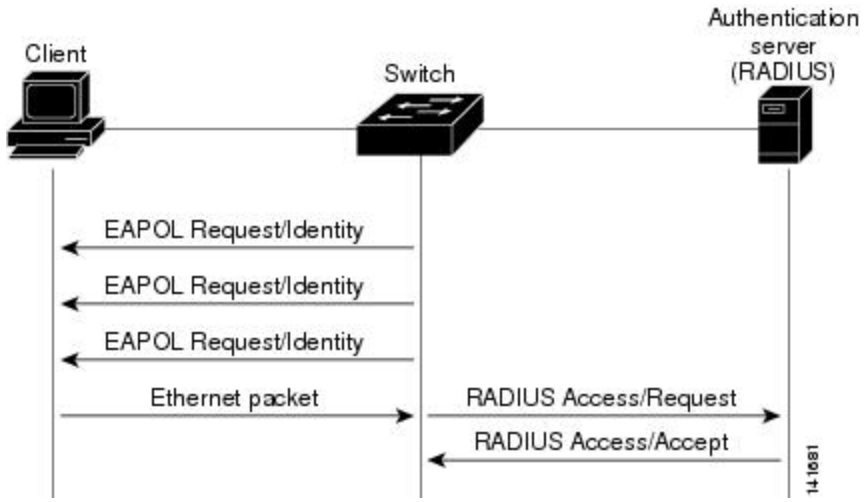
図 *82*：メッセージ交換



EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネット パケットを検出するとそのクライアントを認証できます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS Access/Request フレームにこの情報を保存します。サーバがスイッチに RADIUS Access/Accept フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネット パケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、802.1x 認証を開始します。

次の図に、MAC 認証バイパス中のメッセージ交換を示します。

図 *83* : *MAC* 認証バイパス中のメッセージ交換



ポートベース認証の認証マネージャ

Port-Based 認証方法

表 *112* : *802.1x* 機能

認証方法	モード			
	シングル ホスト	マルチ ホスト	MDA	複数認証
802.1x	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[15] リダイレクト URL	VLAN 割り当て	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL

認証方法	モード			
	シングル ホスト	マルチ ホスト	MDA	複数認証
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL
スタンドアロン Web 認証	プロキシ ACL、Filter-ID 属性、ダウンロード可能 ACL			
NAC レイヤ 2 IP 検証	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL
フォールバック方式としての Web 認証[16]	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL

15 Cisco IOS Release 12.2(50)SE 以降でサポートされています。
16 802.1x 認証をサポートしないクライアント用。

ユーザ単位 ACL および Filter-Id

（注） **any** は、ACL の発信元としてだけ設定できます。

（注） マルチホスト モードで設定された ACL では、ステートメントの発信元部分は *any* でなければなりません。（たとえば、**permit icmp** *any* **host 10.10.1.1**）

定義された ACL の発信元ポートには **any** を指定する必要があります。指定しない場合、ACL は適用できず、認証は失敗します。シングル ホストは唯一例外的に後方互換性をサポートします。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。ホストに適用される ACL ポリシーは、別のホストのトラフィックには影響を与えません。マルチ ホスト ポートで認証されるホストが 1 つだけで、他のホストが認証なしでネットワーク アクセスを取得する場合、発信元アドレスに any を指定することで、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

ポートベース認証マネージャ CLI コマンド

認証マネージャ インターフェイス コンフィギュレーション コマンドは、802.1x、MAC 認証バイパスおよびWeb認証など、すべての認証方法を制御します。認証マネージャ コマンドは、接続ホストに適用される認証方法のプライオリティと順序を決定します。

認証マネージャ コマンドは、ホストモード、違反モードおよび認証タイマーなど、一般的な認証機能を制御します。一般的な認証コマンドには、**authentication host-mode**、**authentication violation** および **authentication timer** インターフェイス コンフィギュレーション コマンドがあります。

802.1x 専用コマンドは、先頭に **dot1x** キーワードが付きます。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにします。ただし、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドは常にグローバルに 802.1x 認証をイネーブルまたはディセーブルにします。

（注） 802.1x 認証がグローバルにディセーブル化されても、Web 認証など他の認証方法はそのポートでイネーブルのままです。

authentication manager コマンドは従来の 802.1x コマンドと同様の機能を提供します。

認証マネージャが生成する冗長なシステム メッセージをフィルタリングすると、通常は、フィルタリングされた内容が認証の成功に結びつきます。802.1x 認証および MAB 認証の冗長なメッセージをフィルタリングすることもできます。認証方式ごとに異なるコマンドが用意されています。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの冗長なメッセージをフィルタリングします。
- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1x 認証の冗長なメッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC 認証バイパス（MAB）の冗長なメッセージをフィルタリングします。

表 *113*：認証マネージャ コマンドおよび以前の *802.1x* コマンド

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
authentication control-direction {**both** | **in**}	**dot1x control-direction** {**both** | **in**}	Wake-on-LAN（WoL）機能を使用して 802.1x 認証をイネーブルにし、ポート制御を単一方向または双方向に設定します。
authentication event	**dot1x auth-fail vlan** **dot1x critical**（インターフェイス コンフィギュレーション） **dot1x guest-vlan6**	ポート上で制限付き VLAN をイネーブルにします。 アクセス不能認証バイパス機能をイネーブルにします。 アクティブ VLAN を 802.1x ゲスト VLAN として指定します。
authentication fallback*fallback-profile*	**dot1x fallback***fallback-profile*	802.1x 認証をサポートしていないクライアント用に、Web 認証をフォールバック方式として使用するようにポートを設定します。
authentication host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]	**dot1x host-mode** {**single-host** | **multi-host** | **multi-domain**}	802.1x 許可ポートで単一のホスト（クライアント）または複数のホストの接続を許可します。
authentication order	**mab**	使用される認証方法の順序を柔軟に定義できるようにします。
authentication periodic	**dot1x reauthentication**	クライアントの定期的再認証をイネーブルにします。
authentication port-control {**auto** | **force-authorized** | **force-un authorized**}	**dot1x port-control** {**auto** | **force-authorized** | **force-unauthorized**}	ポートの許可ステートの手動制御をイネーブルにします。
authentication timer	**dot1x timeout**	802.1x タイマーを設定します。
authentication violation {**protect** | **restrict** | **shutdown**}	**dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続された後に新しいデバイスがそのポートに接続された場合に発生する違反モードを設定します。

許可ステートおよび無許可ステートのポート

802.1x 認証中に、スイッチのポート ステートによって、スイッチはネットワークへのクライアント アクセスを許可します。ポートは最初、無許可ステートです。このステートでは、音声 VLAN（仮想 LAN）ポートとして設定されていないポートは 802.1x 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは許可ステートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN ポートとして設定されている場合、VoIP トラフィックおよび 802.1x プロトコル パケットが許可された後クライアントが正常に認証されます。

（注） CDP バイパスはサポートされていないため、ポートが error-disabled ステートになる場合があります。

802.1x をサポートしていないクライアントが、無許可ステートの 802.1x ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x 対応のクライアントが、802.1x 標準が稼働していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

authentication port-control インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized**：802.1x 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized**：クライアントからの認証の試みをすべて無視し、ポートを無許可ステートのままにします。スイッチはポートを介してクライアントに認証サービスを提供できません。
- **auto**：802.1x 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、スイッチは要求を再送信します。所定の回数だけ試

行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

ポートのリンク ステートがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信した場合に、ポートは無許可ステートに戻ります。

ポートベース認証とスイッチ スタック

スイッチが、スイッチ スタックに追加されるか、スイッチ スタックから削除される場合、RADIUS サーバとスタックとの間の IP 接続が正常な場合、802.1x 認証は影響を受けません。これは、スタック マスターがスイッチ スタックから削除される場合も、適用されます。スタック マスターに障害が発生した場合、スタック メンバは、選択プロセスを使用することによって新しいスタック マスターになり、802.1x 認証プロセスは通常どおり続行されます。

サーバに接続されていたスイッチが削除されたか、そのスイッチに障害が発生したために、RADIUS サーバへの IP 接続が中断された場合、これらのイベントが発生します。

- すでに認証済みで、定期的な再認証がイネーブルではないポートは、認証ステートのままです。RADIUS サーバとの通信は、必要ではありません。
- すでに認証済みで、（**dot1x re-authentication** グローバル コンフィギュレーション コマンドを使用）定期的な再認証がイネーブルにされているポートは、再認証の発生時に、認証プロセスに失敗します。ポートは、再認証プロセス中に、非認証ステートに戻ります。RADIUS サーバとの通信が必要です。

  進行中の認証については、サーバ接続が行われていないため、認証はただちに失敗します。

障害が発生したスイッチが実行状態になり、スイッチ スタックに再加入した場合、ブートアップの時刻と、認証の試行時までに RADIUS サーバへの接続が再確立されたかどうかによって、認証は失敗する場合と、失敗しない場合があります。

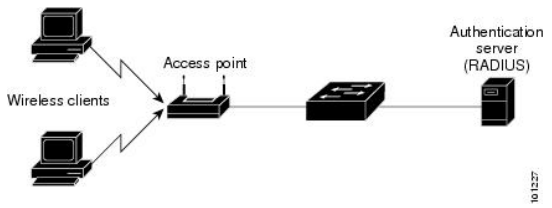
RADIUS サーバへの接続を失うことを避けるには、冗長接続を設定する必要があります。たとえば、スタック マスターへの冗長接続と、スタック メンバへの別の接続を設定できます。スタック マスターに障害が発生した場合でも、スイッチ スタックは、RADIUS サーバに接続されたままです。

802.1X のホスト モード

802.1x ポートは、シングル ホスト モードまたはマルチ ホスト モードで設定できます。シングル ホスト モードでは、802.1x 対応のスイッチ ポートに接続できるのはクライアント 1 つだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチ ホスト モードでは、複数のホストを単一の 802.1x 対応ポートに接続できます。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

図 *84*：マルチ ホスト モードの例



（注） すべてのホスト モードで、ポートベース認証が設定されている場合、ライン プロトコルは許可の前にアップのままです。

スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチ ポートに接続できます。

802.1x 複数認証モード

複数認証（multiauth）モードでは、データ VLAN で複数のクライアントを認証できます。各ホストは個別に認証されます。音声 VLAN が設定されている場合、このモードでは、VLAN で 1 クライアントだけ認証できます（ポートが他の音声クライアントを検出すると、これらはポートから廃棄されますが、違反エラーは発生しません）。

ハブまたはアクセス ポイントが 802.1x 対応ポートに接続されている場合、接続されている各クライアントを認証する必要があります。802.1x 以外のデバイスでは、MAC 認証バイパスまたは Web 認証をホスト単位認証フォールバック メソッドとして使用し、単一のポートで異なる方法で異なるホストを認証できます。

複数認証ポートで認証できるデータ ホストの数には制限はありません。ただし、音声 VLAN が設定されている場合、許可される音声デバイスは 1 台だけです。ホスト制限がないため、定義された違反はトリガーされません。たとえば、別の音声デバイスが検出された場合、これは通知なしで廃棄され、違反はトリガーされません。音声 VLAN の MDA 機能の場合、複数認証モードでは、認証サーバから受け取った VSA に応じて、認証されたデバイスがデータまたは音声のいずれかの VLAN に割り当てられます。

（注） ポートがマルチ認証モードの場合、ゲスト VLAN、および認証失敗 VLAN 機能はアクティブになりません。

次の条件で、RADIUS サーバから提供された VLAN をマルチ認証モードで割り当てることができます。

- ホストがポートで最初に許可されたホストであり、RADIUS サーバが VLAN 情報を提供している。
- 後続のホストが、動作 VLAN に一致する VLAN を使用して許可される。
- ホストは VLAN が割り当てられていないポートで許可され、後続のホストでは VLAN 割り当てが設定されていないか、VLAN 情報が動作 VLAN と一致している。
- ポートで最初に許可されたホストにはグループ VLAN が割り当てられ、後続のホストでは VLAN 割り当てが設定されていないか、グループ VLAN がポート上のグループ VLAN と一致している。後続のホストが、最初のホストと同じ VLAN グループの VLAN を使用する必要がある。VLAN リストが使用されている場合、すべてのホストは VLAN リストで指定された条件に従う。
- マルチ認証ポート上で、1 つの音声 VLAN 割り当てのみがサポートされている。
- VLAN がポート上のホストに割り当てられると、後続のホストは一致する VLAN 情報を持つ必要があり、この情報がなければポートへのアクセスを拒否される。
- ゲスト VLAN または認証失敗 VLAN をマルチ認証モードに設定できない。
- クリティカル認証 VLAN の動作が、マルチ認証モード用に変更されない。ホストが認証を試みたときにサーバに到達できない場合、許可されたすべてのホストは、設定された VLAN で再初期化される。

ユーザごとのマルチ認証 VLAN 割り当て

（注） この機能は、LAN base イメージを実行している Catalyst 2960X スイッチのみでサポートされています。

ユーザごとのマルチ認証 VLAN 割り当て機能を使用すると、単一の設定済みアクセス VLAN を持つポート上のクライアントに割り当てられた VLAN に基づいて複数の運用アクセス VLAN を作成することができます。データ ドメインに関連付けられたすべての VLAN に対するトラフィックが dot1q とタグ付けされていないアクセス ポートとして設定されているポートおよびこれらの VLAN は、ネイティブ VLAN として処理されます。

マルチ認証ポート 1 つあたりのホストの数は 8 ですが、さらに多くのホストが存在する場合があります。

（注） ユーザごとのマルチ認証 VLAN 割り当て機能は、音声ドメインではサポートされません。ポート上の音声ドメインのすべてのクライアントが同じ VLAN を使用する必要があります。

次のシナリオは、ユーザごとのマルチ認証 VLAN 割り当てに関連しています。

シナリオ 1

ハブがアクセスポートに接続されている場合、およびポートがアクセスVLAN（V0）で設定されている場合。

ホスト（H1）は、ハブを介してVLAN（V1）に割り当てられます。ポートの運用VLANはV1に変更されます。この動作は、単一ホスト ポートまたはマルチ ドメイン認証ポートで同様です。

2番目のホスト（H2）が接続され、VLAN（V2）に割り当てられる場合、ポートには2つの運用VLANがあります（V1およびV2）。H1とH2がタグなし入力トラフィックを送信すると、H1トラフィックはVLAN（V1）に、H2トラフィックはVLAN（V2）にマッピングされ、VLAN（V1）およびVLAN（V2）のポートからの出トラフィックはすべてタグなしになります。

両方のホストH1とH2がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN（V1）とVLAN（V2）がポートから削除され、設定されたVLAN（V0）がポートに復元されます。

シナリオ 2

ハブがアクセスポートに接続されている場合、およびポートがアクセスVLAN（V0）で設定されている場合。ホスト（H1）は、ハブを介してVLAN（V1）に割り当てられます。ポートの運用VLANはV1に変更されます。

2番目のホスト（H2）が接続され明示的なVLANポリシーなしで承認されると、H2はポート上で復元される設定済みVLAN（V0）を使用することを予期されます。2つの運用VLAN、VLAN（V0）およびVLAN（V1）からの出トラフィックはすべてタグなしになります。

ホスト（H2）がログアウトするか、またはセッションがなんらかの理由で削除されると、設定されたVLAN（V0）がポートから削除され、VLAN（V1）がそのポートでの唯一の運用VLANになります。

シナリオ 3

ハブがオープンモードでアクセスポートに接続されている場合、およびポートがアクセスVLAN（V0）で設定されている場合。

ホスト（H1）は、ハブを介してVLAN（V1）に割り当てられます。ポートの運用VLANはV1に変更されます。2番目のホスト（H2）が接続され無許可のままだと、オープン モードにより、運用VLAN（V1）に引き続きアクセスできます。

ホストH1がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN（V1）はポートから削除され、ホスト（H2）はVLAN（V0）に割り当てられます。

（注） オープン モードとVLAN割り当ての組み合わせは、ホスト（H2）に悪影響を与えます。そのホストはVLAN（V1）に対応するサブネット内にIPアドレスを含んでいるからです。

ユーザごとのマルチ認証 *VLAN* 割り当ての制限

ユーザごとのマルチ認証VLAN割り当て機能では、複数のVLANからの出トラフィックは、ホストが自分宛てではないトラフィックを受信するポート上ではタグなしになります。これは、ブロードキャストおよびマルチキャスト トラフィックで問題になる可能性があります。

- **IPv4 ARP**：ホストは他のサブネットからのARPパケットを受信します。これは、IPアドレス範囲が重複する異なる仮想ルーティングおよび転送（VRF）テーブルの2個のサブネット

がポート上でアクティブな場合に問題となります。ホストのARPキャッシュが無効なエントリを受け取る可能性があります。

- **IPv6 制御パケット**：IPv6 の導入環境では、ルータ アドバタイズメント（RA）は、その受信を想定されていないホストによって処理されます。ある VLAN からのホストが別の VLAN からの RA を受信すると、ホストはそれ自身に間違った IPv6 アドレスを割り当てます。このようなホストは、ネットワークにアクセスできません。

  回避策は、IPv6 ファースト ホップ セキュリティをイネーブルにして、ブロードキャスト ICMPv6 パケットがユニキャストに変換され、マルチ認証がイネーブルのポートから送信されるようにすることです。パケットはVLANに属するマルチ認証ポートの各クライアント用に複製され、宛先 MAC が個々のクライアントに設定されます。1 つの VLAN を持つポートで、ICMPv6 パケットは正常にブロードキャストされます。

- **IP マルチキャスト**：送信先のマルチキャスト グループへのマルチキャスト トラフィックは、異なるVLAN上のホストがそのマルチキャスト グループに参加している場合それらのVLAN用に複製されます。異なる VLAN の 2 つのホストが（同じマルチ認証ポート上の）マルチキャスト グループに参加している場合、各マルチキャスト パケットのコピー2部がそのポートから送信されます。

MAC 移動

あるスイッチ ポートで MAC アドレスが認証されると、そのアドレスは同じスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じMACアドレスを別の認証マネージャ対応ポートで検出すると、そのアドレスは許可されなくなります。

場合によっては、MACアドレスを同じスイッチ上のポート間で移動する必要があります。たとえば、認証ホストとスイッチ ポート間に別のデバイス（ハブまたは IP Phone など）がある場合、ホストをデバイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC 移動をグローバルにイネーブルにできます。ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再認証されます。MAC 移動はすべてのホスト モードでサポートされます（認証ホストは、ポートでイネーブルにされているホスト モードに関係なく、スイッチの任意のポートに移動できます）。MACアドレスがあるポートから別のポートに移動すると、スイッチは元のポートで認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。MAC移動の機能は、音声およびデータ ホストの両方に適用されます。

（注） オープン認証モードでは、MACアドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

MAC 置換

MAC置換機能は、ホストが、別のホストがすでに認証済みであるポートに接続しようとすると発生する違反に対処するように設定できます。

（注） 違反はマルチ認証モードでは発生しないため、マルチ認証モードのポートにこの機能は適用されません。マルチホスト モードで認証が必要なのは最初のホストだけなので、この機能はこのモードのポートには適用されません。

replace キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、マルチドメイン モードのポートでの認証プロセスは、次のようになります。

- 既存の認証済み MAC アドレスを使用するポートで新しい MAC アドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータ ホストの MAC アドレスを、新しい MAC アドレスで置き換えます。
- 認証マネージャは、新しい MAC アドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MACアドレスはただちにMACアドレス テーブルに追加されます。

802.1x アカウンティング

802.1x 標準では、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1xアカウンティングは、デフォルトでディセーブルです。802.1x アカウンティングをイネーブルにすると、次の処理を 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。
- 再認証が失敗します。

スイッチは 802.1x アカウンティング情報を記録しません。その代わり、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティング メッセージを記録するように設定する必要があります。

802.1x アカウンティング属性値ペア

RADIUS サーバに送信された情報は、属性値（AV）ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます（たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性の情報が必要です）。

AV ペアは、802.1x アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START：新規ユーザ セッションが始まると送信されます。
- INTERIM：既存のセッションが更新されると送信されます。
- STOP：セッションが終了すると送信されます。

（注） RADIUS および AAA のデバッグのログを表示するには、**show platform software trace message smd** コマンドを使用します。詳細については、『*Command Reference Guide, Cisco IOS XE Denali 16.1.1*』のセクション「Tracing Commands」を参照してください。

次の表に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 *114*：アカウンティング *AV* ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	Always	Always	Always
属性 [4]	NAS-IP-Address	Always	Always	Always
属性 [5]	NAS-Port	Always	Always	Always
属性 [8]	Framed-IP-Address	非送信	条件に応じて送信[17]	条件に応じて送信
属性 [30]	Called-Station-ID	Always	Always	Always
属性 [31]	Calling-Station-ID	Always	Always	Always
属性 [40]	Acct-Status-Type	Always	Always	Always
属性 [41]	Acct-Delay-Time	Always	Always	Always
属性 [42]	Acct-Input-Octets	非送信	Always	Always
属性 [43]	Acct-Output-Octets	非送信	Always	Always
属性[47]	Acct-Input-Packets	非送信	Always	Always
属性 [48]	Acct-Output-Packets	非送信	Always	Always
属性 [44]	Acct-Session-ID	Always	Always	Always
属性 [45]	Acct-Authentic	Always	Always	Always

属性番号	AV ペア名	START	INTERIM	STOP
属性 [46]	Acct-Session-Time	非送信	Always	Always
属性 [49]	Acct-Terminate-Cause	非送信	非送信	Always
属性 [61]	NAS-Port-Type	Always	Always	Always

17 有効な静的 IP アドレスが設定されているか、ホストに対する Dynamic Host Control Protocol（DHCP）バインディングが DHCP スヌーピング バインディング テーブルに存在している場合に、Framed-IP-Address の AV ペアが送信されます。

802.1x 準備状態チェック

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。802.1x 機能をサポートしていないデバイスでは、MAC 認証バイパスまたは Web 認証などの代替認証を使用します。

この機能が有用なのは、クライアントのサプリカントで NOTIFY EAP 通知パケットでのクエリーがサポートされている場合だけです。クライアントは、802.1x タイムアウト値内に応答しなければなりません。

関連トピック

802.1x 準備状態チェックの設定, （1613 ページ）

スイッチと RADIUS サーバ間の通信

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

関連トピック

スイッチと RADIUS サーバ間の通信の設定, （1623 ページ）

VLAN 割り当てを使用した 802.1x 認証

スイッチは、VLAN 割り当てを使用した 802.1x 認証をサポートしています。ポートの 802.1x 認証が成功すると、RADIUS サーバは VLAN 割り当てを送信し、スイッチ ポートを設定します。RADIUS サーバ データベースは、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに

接続するクライアントのユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

音声デバイス認証は、Cisco IOS Release 12.2(37)SE のマルチドメイン ホスト モードでサポートされています。Cisco IOS Release 12.2(40)SE 以降、音声デバイスが許可されており、RADIUS サーバが許可された VLAN を返した場合、割り当てられた音声 VLAN 上でパケットを送受信するようにポート上の音声 VLAN が設定されます。音声 VLAN 割り当ては、マルチドメイン認証（MDA）対応のポートでのデータ VLAN 割り当てと同じように機能します。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 802.1x 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1x 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN とは、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべて、この VLAN に所属します。
- 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

  設定エラーには、ルーテッド ポートの VLAN、間違った VLAN ID、存在しないまたは内部（ルーテッド ポート）の VLAN ID、RSPAN VLAN、シャットダウンしている VLAN、あるいは一時停止している VLAN ID の指定などがあります。マルチドメイン ホスト ポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行（またはその逆）のために発生するものもあります。
- 802.1x 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。
- 802.1x ポートでマルチ ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN（RADIUS サーバにより指定）に配置されます。
- ポート セキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
  - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
  - 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を dot1p または untagged に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウン ステートの場合、ポートは設定済みのアクセスVLANに配置されます。

802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセスVLAN設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。

- あるデバイスでVLAN設定を変更したことにより、他のデバイスに設定済または割り当て済みのVLANと一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みのVLANが一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
- 音声デバイスが許可されて、ダウンロードされた音声VLANを使用している場合、音声VLAN設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウン ステートの場合、ポートは設定済みのアクセスVLANに配置されます。

トランク ポート、ダイナミック ポート、またはVLANメンバーシップ ポリシー サーバ（VMPS）によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用してAAA認証をイネーブルにし、RADIUSサーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。（アクセス ポートで 802.1x 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN 名または VLAN ID
  - [83] Tunnel-Preference

  属性 [64] は、値 *VLAN*（タイプ 13）でなければなりません。属性 [65] は、値*802*（タイプ 6）でなければなりません。属性 [81] は、IEEE 802.1x 認証ユーザに割り当てられた *VLAN* 名または *VLAN ID* を指定します。

ユーザ単位 ACL を使用した 802.1x 認証

ユーザ単位アクセス コントロール リスト（ACL）をイネーブルにして、異なるレベルのネットワーク アクセスおよびサービスを 802.1x 認証ユーザに提供できます。RADIUS サーバは、802.1x ポートに接続されるユーザを認証する場合、ユーザ ID に基づいて ACL 属性を受け取り、これらをスイッチに送信します。スイッチは、ユーザ セッションの期間中、その属性を 802.1x ポートに適用します。セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザ単位 ACL 設定が削除されます。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションには保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

ユーザは同一のスイッチ上で、ルータ ACL および入力ポート ACL を使用できます。ただし、ポートの ACL はルータ ACL より優先されます。入力ポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力ルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド パケットは、ルータ ACL によってフィルタリングされます。発信するルーテッド パケットには、ルータ ACL のフィルタが適用されます。コンフィギュレーションの矛盾を回避するには、RADIUS サーバに保存するユーザ プロファイルを慎重に計画しなければなりません。

RADIUS は、ベンダー固有属性などのユーザ単位属性をサポートします。ベンダー固有属性（VSA）は、オクテット ストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では inacl#<*n*> で、出力方向では outacl#<*n*> です。MAC ACL は、入力方向に限りサポートされます。VSA は入力方向に限りサポートされます。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザ単位コンフィギュレーションを定義します。RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。属性には、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す *.in* または *.out* が含まれています。RADIUS サーバが *.in* または *.out* 構文を許可しない場合、アクセス リストはデフォルトで発信 ACL に適用されます。スイッチでの Cisco IOS のアクセス リストに関するサポートが制限されているため、Filter-ID 属性は 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL および IP 拡張 ACL）に対してだけサポートされます。

ユーザ単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズにより制限されます。

ユーザ単位の ACL を設定するには、次の手順に従います。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。

- 802.1x ポートをシングル ホスト モードに設定します。

（注） ユーザ単位 ACL がサポートされるのはシングル ホスト モードだけです。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証

ACL およびリダイレクト URL は、ホストの 802.1x 認証または MAC 認証バイパス中に、RADIUS サーバからスイッチにダウンロードできます。また、Web 認証中に ACL をダウンロードすることもできます。

（注） ダウンロード可能な ACL は *dACL* とも呼ばれます。

複数のホストが認証され、それらのホストがシングル ホスト モード、MDA モード、またはマルチ認証モードである場合、スイッチは ACL の送信元アドレスをホスト IP アドレスに変更します。

ACL およびリダイレクト URL は、802.1x 対応のポートに接続されるすべてのデバイスに適用できます。

ACL が 802.1x 認証中にダウンロードされない場合、スイッチは、ポートのスタティック デフォルト ACL をホストに適用します。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、スイッチは ACL を認証ポリシーの一部として電話にだけ適用します。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、ポート上にスタティック ACL がない場合、ダイナミックな認証デフォルト ACL が作成され、dACL がダウンロードされて適用される前にポリシーが実施されます。

（注） 認証デフォルト ACL は、実行コンフィギュレーションでは表示されません。

認証デフォルト ACL は、ポートで許可ポリシーを持つホストが 1 つ以上検出されると作成されます。認証デフォルト ACL は、最後の認証セッションが終了すると削除されます。認証デフォルト ACL は、**ip access-list extended auth-default-acl** グローバル コンフィギュレーション コマンドを使用して設定できます。

（注） 認証デフォルト ACL は、シングル ホスト モードの Cisco Discovery Protocol（CDP）バイパスをサポートしていません。CDP バイパスをサポートするには、インターフェイス上のスタティック ACL を設定する必要があります。

802.1x および MAB 認証方式では、オープンおよびクローズの 2 つの認証方式がサポートされます。クローズ認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL が作成されます。

- 認証デフォルトACLは、ポリシーが実施されるまでDHCPトラフィックのみを許可します。
- 最初のホスト認証では、許可ポリシーはIPアドレスを挿入せずに適用されます。
- 別のホストが検出されると、最初のホストのポリシーがリフレッシュされ、最初のセッションと後続セッションのポリシーがIPアドレスを挿入して実施されます。

オープン認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL-OPEN が作成され、すべてのトラフィックが許可されます。
- セキュリティ違反を防ぐために、IP アドレスを挿入してポリシーが実施されます。
- Web 認証は、認証デフォルト ACL-OPEN に従います。

許可ポリシーのないホストへのアクセスを制御するために、ディレクティブを設定することができます。サポートされているディレクティブの値は、*open* と *default* です。*open* ディレクティブを設定すると、すべてのトラフィックが許可されます。*default* ディレクティブは、ポートから提供されるアクセスにトラフィックを従わせます。ディレクティブは、AAA サーバ上のユーザ プロファイル、またはスイッチ上のいずれかで設定できます。AAA サーバ上でディレクティブを設定するには、**authz-directive =<open/default>** グローバル コマンドを使用します。スイッチ上でディレクティブを設定するには、**epm access-control open** グローバル コンフィギュレーション コマンドを使用します。

（注） ディレクティブのデフォルト値は *default* です。

設定された ACL なしでポート上の Web 認証にホストがフォールバックする場合は、次のようになります。

- ポートがオープン認証モードの場合、認証デフォルト ACL-OPEN が作成されます。
- ポートがクローズ認証モードの場合、認証デフォルト ACL が作成されます。

フォールバック ACL のアクセス コントロール エントリ（ACE）は、ユーザ単位のエントリに変換されます。設定されたフォールバック プロファイルにフォールバック ACL が含まれていない場合、ホストはポートに関連付けられた認証デフォルト ACL に従います。

（注） Web 認証でカスタム ロゴを使用し、それを外部サーバに格納する場合、認証の前にポートの ACL で外部サーバへのアクセスを許可する必要があります。外部サーバに適切なアクセスを提供するには、スタティック ポート ACL を設定するか、認証デフォルト ACL を変更する必要があります。

Cisco Secure ACS およびリダイレクト URL の属性と値のペア

スイッチはこれらの *cisco-av-pair* VSA を使用します。

- url-redirect は HTTP URL または HTTPS URL です。

- url-redirect-acl はスイッチ ACL 名または番号です。

スイッチは、CiscoSecure-defined-ACL 属性値ペアを使用して、エンド ポイントからの HTTP または HTTPS リクエストを代行受信します。スイッチは、クライアント Web ブラウザを指定されたリダイレクト アドレスに転送します。Cisco Secure ACS 上の url-redirect AV ペアには、Web ブラウザがリダイレクトされる URL が格納されます。url-redirect-acl 属性値ペアには、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号が含まれます。

（注）

- ACL の permit ACE と一致するトラフィックがリダイレクトされます。
- スイッチの URL リダイレクト ACL およびデフォルト ポート ACL を定義します。

リダイレクト URL が認証サーバのクライアントに設定される場合は、接続されるクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア

Cisco Secure ACS で、RADIUS cisco-av-pair ベンダー固有属性（VSA）を使用して、CiscoSecure-Defined-ACL 属性と値（AV）ペアを設定できます。このペアは、#ACL#-IP-name-number 属性を使って、Cisco Secure ACS でダウンロード可能な ACL の名前を指定します。

- *name* は ACL の名前です。
- *number* はバージョン番号（たとえば 3f783768）です。

ダウンロード可能な ACL が認証サーバのクライアントに設定される場合、接続されるクライアント スイッチ ポートのデフォルト ポート ACL も設定する必要があります。

デフォルト ACL がスイッチで設定されている場合、Cisco Secure ACS がホスト アクセス ポリシーをスイッチに送信すると、スイッチは、スイッチ ポートに接続されるホストからのトラフィックにこのポリシーを適用します。ポリシーが適用されない場合、デフォルト ACL が適用されます。Cisco Secure ACS がダウンロード可能な ACL をスイッチに送信する場合、この ACL は、スイッチ ポートに設定されているデフォルト ACL より優先されます。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信し、デフォルト ACL が設定されていない場合、許可失敗が宣言されます。

VLAN ID ベース MAC 認証

ダウンロード可能な VLAN ではなくスタティック VLAN ID に基づいてホストを認証する場合、VLAN ID ベース MAC 認証を使用できます。スタティック VLAN ポリシーがスイッチで設定されている場合、認証用の各ホストの MAC アドレスとともに、VLAN 情報が IAS（Microsoft）RADIUS サーバに送信されます。接続ポートに設定されている VLAN ID は MAC 認証に使用されます。VLAN ID ベース MAC 認証を IAS サーバで使用することで、ネットワークで一定数の VLAN を使用できます。

機能は、STP によってモニタおよび処理される VLAN の数も制限します。ネットワークは固定 VLAN として管理できます。

（注） この機能は Cisco ACS Server ではサポートされていません（ACS サーバは、新しいホストに送信される VLAN-ID を無視して、MAC アドレスに基づいた認証だけを行います）。

ゲスト VLAN を使用した 802.1x 認証

スイッチ上の各 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます（802.1x クライアントのダウンロードなど）。これらのクライアントは 802.1x 認証用にシステムをアップグレードできる場合がありますが、一部のホスト（Windows 98 システムなど）は IEEE 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチは EAPOL パケット履歴を保持します。EAPOL パケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが IEEE 802.1x 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

スイッチが 802.1x 対応の音声デバイスを許可しようとしたが、AAA サーバが使用できない場合、許可は失敗します。ただし、EAPOL パケットの検出は EAPOL 履歴に保存されます。この音声デバイスは、AAA サーバが使用可能になると許可されます。ただし、他のデバイスによるゲスト VLAN へのアクセスは許可されなくなります。この状況を防ぐには、次のいずれかのコマンド シーケンスを使用します。

- **authentication event no-response action authorize vlan***vlan-id* インターフェイス コンフィギュレーション コマンドを入力し、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。

（注） インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1x 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに 802.1x 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲストVLANは、単一のホスト、複数のホスト、複数認証、またはマルチドメインモードにおける 802.1x ポートでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x ゲスト VLANとして設定できます。ゲストVLAN機能は、内部VLAN（ルーテッドポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

スイッチは*MAC*認証バイパス をサポートします。MAC認証バイパスが802.1xポートでイネーブルの場合、スイッチは、IEEE 802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアントMACアドレスに基づいてクライアントを許可できます。スイッチは、802.1x ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。

制限付き VLAN による 802.1x 認証

ゲストVLANにアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチ スタックまたはスイッチの各 IEEE 802.1x ポートに対して制限付き VLAN（認証失敗*VLAN*と呼ばれることもあります）を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1x 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効なクレデンシャルを持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。

（注） 両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチ ポートがスパニングツリーのブロッキング ステートから変わることができなくなります。制限付きVLANの機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。VLAN内のポートは設定された間隔に従って再認証を試みます（デフォルトは60秒）。再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルにすることもできますが、ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しない限り、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。クライアント

の接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の疑似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントによっては（Windows XP が稼働しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、すべてのホスト モードでの 802.1x ポート上、およびレイヤ 2 ポート上でサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

ダイナミック ARP インスペクション、DHCP スヌーピング、IP 送信元ガードなどの他のセキュリティ ポート機能は、制限付き VLAN に対して個別に設定できます。

アクセス不能認証バイパスを使用した 802.1x 認証

スイッチが設定された RADIUS サーバに到達できず、新しいホストを認証できない場合、アクセス不能認証バイパス機能を使用します。この機能は、クリティカル認証または *AAA* 失敗ポリシーとも呼ばれます。これらのホストをクリティカル ポートに接続するようにスイッチを設定できます。

新しいホストがクリティカル ポートに接続しようとすると、そのホストはユーザ指定のアクセス VLAN、クリティカル *VLAN* に移動されます。管理者はこれらのホストに制限付き認証を付与します。

スイッチは、クリティカル ポートに接続されているホストを認証しようとする場合、設定されている RADIUS サーバのステータスをチェックします。利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワーク アクセスを許可して、ポートを認証ステートの特別なケースであるクリティカル認証ステートにします。

複数認証ポートのアクセス不能認証バイパスのサポート

ポートが任意のホスト モードで設定されていて、AAA サーバを使用できない場合、ポートはマルチホスト モードに設定され、クリティカル VLAN に移動されます。マルチ認証（multiauth）ポートで、このアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan** *vlan-id* コマンドを使用します。新しいホストがクリティカル ポートに接続しようとすると、そのポートは再初期化され、接続されているすべてのホストがユーザ指定のアクセス VLAN に移動されます。

このコマンドは、すべてのホスト モードでサポートされます。

アクセス不能認証バイパスの認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカル ポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカル ポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイム アウトとなり、スイッチは次の認証試行の間にクリティカル ポートをクリティカル認証ステートとします。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、クリティカル VLAN から移動するように、クリティカル ポートを設定できます。このように設定した場合、クリティカル認証ステートのすべてのクリティカル ポートは自動的に再認証されます。

アクセス不能認証バイパス機能の相互作用

アクセス不能認証バイパスは、次の機能と相互に作用します。

- ゲスト VLAN：アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 8021.x ポートでイネーブルの場合、この機能は次のように相互に作用します。
  - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカル ポートを RADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- 制限付き VLAN：ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。

- 802.1x アカウンティング：RADIUS サーバが使用できない場合、アカウンティングは影響を受けません。
- プライベート VLAN：プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声VLAN：アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer（RSPAN）：アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

スイッチ スタックで、次の動作が発生します。

- キープアライブ パケットを送信することによって、スタック マスターにより、RADIUS サーバのステータスがチェックされます。RADIUS サーバのステータスが変更されると、スタック マスターからスタック メンバへ、情報が送信されます。クリティカル ポートの再認証時に、スタック メンバにより、RADIUS サーバのステータスがチェックされます。
- 新しいスタック マスターが選択されると、スイッチ スタックと RADIUS サーバとの間のリンクが変更される可能性があり、新しいスタックにより、キープアライブ パケットがただちに送信され、RADIUS サーバのステータスがアップデートされます。サーバのステータスが *dead* から *alive* に変化すると、スイッチはクリティカル認証ステートの状態にあるすべてのスイッチ ポートを再認証します。

メンバがスタックに追加されると、スタック マスターからメンバへサーバ ステータスが送信されます。

（注） スイッチ スタックは、LAN Base イメージを実行している Catalyst 2960-S スイッチだけでサポートされています。

802.1x クリティカル音声 VLAN

ポートに接続されている IP Phone がアクセス コントロール サーバ（ACS）によって認証されるとき、電話機は音声ドメインに参加します。ACS が到達不能である場合、スイッチはデバイスが音声デバイスなのかどうかを判断できません。サーバが使用できない場合、電話機は音声ネットワークにアクセスできないため、動作できません。

データ トラフィックの場合、アクセス不能認証バイパス（クリティカル認証）を設定し、サーバが使用できない場合にトラフィックがネイティブ VLAN を通過できるようにすることができます。RADIUS 認証サーバが使用できず（ダウンしていて）、アクセスできない認証バイパスがイネーブルの場合、スイッチは、クライアントにネットワークのアクセスを許可し、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN でポートをクリティカル認証ステートにします。設定された RADIUS サーバにスイッチが到達できず、新しいホストを認証できない場合、スイッチはこれらのホストをクリティカル ポートに接続します。クリティカル ポートに接続を試行している新

しいホストは、ユーザ指定のアクセス VLAN（クリティカル VLAN）に移動され、制限付き認証を許可されます。

authentication event server dead action authorize voice インターフェイス コンフィギュレーション コマンドを使用して、クリティカル音声 VLAN 機能を設定できます。ACS が応答しない場合、ポートはクリティカル認証モードになります。ホストからのトラフィックが音声 VLAN でタグ付けされると、接続デバイス（電話機）は、ポートに対して設定された音声 VLAN に配置されます。IP Phone は CDP（シスコ デバイス）や LLDP または DHCP を介して音声 VLAN ID を学習します。

switchport voice vlan*vlan-id* インターフェイス コンフィギュレーション コマンドを入力して、ポートの音声 VLAN を設定できます。

この機能は、マルチドメインモードおよびマルチ認証ホストモードでサポートされます。スイッチがシングルホストモードまたはマルチホストモードの場合にコマンドを入力できますが、デバイスがマルチドメインまたはマルチ認証ホスト モードに変わらない限りコマンドは有効になりません。

802.1x ユーザ ディストリビューション

802.1x ユーザ ディストリビューションを設定すると、複数の異なる VLAN で同じグループ名のユーザのロード バランシングを行うことができます。

VLAN は、RADIUS サーバにより提供されるか、VLAN グループ名でスイッチ CLI を介して設定します。

- RADIUS サーバを設定して、ユーザの複数の VLAN 名を送信します。複数の VLAN 名は、ユーザへの応答の一部として送信できます。802.1x ユーザ ディストリビューションは、特定の VLAN のすべてのユーザを追跡し、許可されたユーザをユーザ数が最も少ない VLAN に移動することでロード バランシングを行います。
- RADIUS サーバを設定してユーザの VLAN グループ名を送信します。VLAN グループ名は、ユーザへの応答の一部として送信できます。スイッチ CLI を使用して設定した VLAN グループ名で、選択された VLAN グループ名を検索できます。VLAN グループ名が検出されると、この VLAN グループ名で対応する VLAN を検索して、ユーザ数が最も少ない VLAN が検出されます。ロード バランシングは、対応する許可済みユーザをその VLAN に移動することで行われます。

（注） RADIUS サーバは、VLAN-ID、VLAN 名または VLAN グループを任意に組み合わせて VLAN 情報を送信できます。

802.1x ユーザ ディストリビューションの設定時の注意事項

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされることを確認してください。
- 複数の VLAN を VLAN グループにマッピングできます。

- VLAN を追加または削除することで、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアする場合、VLAN の認証済みポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブ VLAN がグループにマッピングされても VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内で任意の VLAN の認証ステートであるポートまたはユーザはクリアされませんが、VLAN の VLAN グループへのマッピングはクリアされます。

音声 VLAN ポートを使用した IEEE 802.1x 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の 2 つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータ トラフィックを伝送する PVID。PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、IP Phone は IEEE 802.1x 認証とは独立して動作できます。

シングル ホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチ ホスト モードでは、サプリカントが PVID で認証された後、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチ ホスト モードがイネーブルの場合、サプリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで IEEE 802.1x 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

IEEE 802.1x 認証をスイッチ ポート上でイネーブルにすると、音声 VLAN でもあるアクセス ポート VLAN を設定できます。

IP 電話がシングル ホスト モードで 802.1x 対応のスイッチ ポートに接続されている場合、スイッチは認証を行わずに電話ネットワーク アクセスを承認します。ポートで Multidomain Authentication（MDA）を使用して、データ デバイスと IP フォンなどの音声デバイスの両方を認証することを推奨します。

（注） 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

ポート セキュリティを使用した IEEE 802.1x 認証

通常、IEEE 802.1x がイネーブルの場合に、ポート セキュリティをイネーブルにすることは推奨されません。IEEE 802.1x ではポート単位（IP テレフォニーに MDA が設定されている場合は VLAN 単位）で単一の MAC アドレスが適用されるため、ポート セキュリティは冗長であり、場合によっては期待される IEEE 802.1x の動作と干渉することがあります。

WoL 機能を使用した IEEE 802.1x 認証

IEEE 802.1x 認証の Wake-on-LAN（WoL）機能を使用すると、スイッチにマジック パケットと呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが IEEE 802.1x ポートを通じて接続され、ホストの電源がオフになると、IEEE 802.1x ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした IEEE 802.1x 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の IEEE 802.1x ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。

（注） PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

authentication control-direction in インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向に設定すると、そのポートはスパニングツリー フォワーディング ステートに変わります。ポートは、ホストにパケットを送信できますが、受信はできません。

authentication control-direction both インターフェイス コンフィギュレーション コマンドを使用してポートを双方向に設定すると、そのポートのアクセスが双方向で制御されます。ポートは、ホストとの間でパケットを送受信しません。

MAC 認証バイパスを使用した IEEE 802.1x 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレスに基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された IEEE 802.1x ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が IEEE 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。スイッチは、IEEE 802.1x ポート上のクライ

アントを検出した後で、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。このプロセスは、ほとんどのクライアント デバイスで動作します。ただし、代替の MAC アドレス形式を使用しているクライアントでは動作しません。標準の形式とは異なる MAC アドレスを持つクライアントに対して MAB 認証をどのように実行するかや、RADIUS の設定のどこでユーザ名とパスワードが異なることが要求されるかを設定できます。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが 802.1x 対応サプリカントであることを確認し、（MAC 認証バイパス機能ではなく）802.1x 認証を使用してインターフェイスを認証します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、IEEE 802.1x サプリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生するときに、Termination-Action RADIUS 属性値が DEFAULT であるために前のセッションが終了した場合、スイッチはポートに設定されている認証または再認証手法を使用します。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、IEEE 802.1x を使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てられた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS 属性（Attribute[27]）、および Termination-Action RADIUS 属性（Attribute[29]）に基づいて行われるときに、Termination-Action RADIUS 属性（Attribute[29]）のアクションが *Initialize*（属性値は *DEFAULT*）である場合、MAC 認証バイパス セッションは終了し、再認証の間の接続は失われます。MAC 認証バイパス機能が IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。これらの AV ペアの詳細については、RFC 3580『IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- IEEE 802.1x 認証：802.1x 認証がポートでイネーブルの場合にのみ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：IEEE 802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ
- 音声 VLAN
- VLAN メンバーシップ ポリシー サーバ（VMPS）：IEEE 802.1x および VMPS は相互に排他的です。
- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。

- Network Edge Access Topology（NEAT）：MAB と NEAT は相互に排他的です。インターフェイス上で NEAT がイネーブルの場合は、MAB をイネーブルにできません。また、インターフェイス上で MAB がイネーブルの場合は、NEAT をイネーブルにできません。

Cisco IOS Release 12.2(55)SE 以降では、冗長 MAB システム メッセージのフィルタリングをサポートします。

Network Admission Control レイヤ 2 IEEE 802.1x 検証

スイッチは、デバイスのネットワーク アクセスを許可する前にエンドポイント システムやクライアントのウイルス対策の状態またはポスチャを調べる Network Admission Control（NAC）レイヤ 2 IEEE 802.1x 検証をサポートしています。NAC レイヤ 2 IEEE 802.1x 検証を使用すると、以下の作業を実行できます。

- Session-Timeout RADIUS 属性（属性 [27]）と Termination-Action RADIUS 属性（属性 [29]）を認証サーバからダウンロードします。
- Session-Timeout RADIUS 属性（属性 [27]）の値として再認証試行間の秒数を指定し、RADIUS サーバからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS 属性（属性[29]）を使用してクライアントを再認証する際のアクションを設定します。値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- VLAN の番号や名前、または VLAN グループ名のリストを Tunnel Group Private ID（属性 [81]）の値として設定し、VLAN の番号や名前、または VLAN グループ名のプリファレンスを Tunnel Preference（属性 [83]）の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID（属性 [81]）属性がリストから選択されます。
- **show authentication** 特権 EXEC コマンドを使用して、クライアントのポスチャを表示する NAC ポスチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 IEEE 802.1x 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があることを除いて、IEEE 802.1x ポートベース認証と似ています。

柔軟な認証の順序設定

柔軟な認証の順序設定を使用して、ポートが新しいホストを認証するときに使用する方法の順序を設定できます。The IEEE 802.1X の柔軟な認証機能では、以下の 3 つの認証方法をサポートしています。

- dot1X：IEEE 802.1X 認証はレイヤ 2 の認証方式です。
- mab：MAC 認証バイパスはレイヤ 2 の認証方式です。
- webauth：Web 認証はレイヤ 3 の認証方式です。

この機能を使用すると、各ポートでどの認証方式を使用するかを制御できます。また、そのポートの方式についてフェールオーバー順も制御できます。たとえば、MAC認証バイパスおよび802.1xは、プライマリまたはセカンダリ認証方法として使用し、Web認証は、これらの認証のいずれか、または両方が失敗した場合のフォールバック方法として使用できます。

The IEEE 802.1X の柔軟な認証機能では、以下のホスト モードをサポートしています。

- multi-auth：マルチ認証では、音声 VLAN に 1 つの認証、データ VLAN に複数の認証を使用できます。
- multi-domain：マルチドメイン認証では、音声 VLAN に 1 つ、データ VLAN に 1 つ、計 2 つの認証を使用できます。

関連トピック

柔軟な認証順序の設定，（1664 ページ）

Open1x 認証

Open1x認証によって、デバイスが認証される前に、そのデバイスがポートにアクセスできるようになります。オープン認証が設定されている場合、新しいホストはポートに定義されているアクセス コントロール リスト（ACL）に基づいてトラフィックを渡します。ホストが認証されると、RADIUS サーバに設定されているポリシーがそのホストに適用されます。

オープン認証を次の状況で設定できます。

- シングル ホスト モードでのオープン認証：1 人のユーザだけが認証の前後にネットワークにアクセスできます。
- MDA モードでのオープン認証：音声ドメインの 1 人のユーザだけ、およびデータ ドメインの 1 人のユーザだけが許可されます。
- マルチ ホスト モードでのオープン認証：任意のホストがネットワークにアクセスできます。
- 複数認証モードでのオープン認証：MDA の場合と似ていますが、複数のホストを認証できます。

（注） オープン認証が設定されている場合は、他の認証制御よりも優先されます。これは、**authentication open** インターフェイス コンフィギュレーション コマンドを使用した場合、**authentication port-control** インターフェイス コンフィギュレーション コマンドに関係なく、ポートがホストにアクセス権を付与することを意味します。

関連トピック

Open1x の設定，（1666 ページ）

マルチドメイン認証

スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチ ポート上で認証できます。ポートはデータ ドメインと音声ドメインに分割されます。

（注） すべてのホスト モードで、ポートベース認証が設定されている場合、ライン プロトコルは許可の前にアップのままです。

MDA では、デバイス認証の順序が指定されません。ただし、最適な結果を得るには、MDA 対応のポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA のスイッチ ポートを設定する必要があります。
- ホスト モードがマルチドメインに設定されている場合、IP Phone の音声 VLAN を設定する必要があります。
- MDA 対応ポートでの音声 VLAN 割り当ては、Cisco IOS Release 12.2(40)SE 以降でサポートされています。

（注） MDA 対応のスイッチポートで音声デバイスにダイナミック VLAN を割り当てることができますが、スイッチポートに設定されたスタティック音声 VLAN が RADIUS サーバの音声デバイスに割り当てられたダイナミック VLAN と同じである場合、その音声デバイスの認証は失敗します。

- 音声デバイスを認可するには、値を *device-traffic-class=voice* に設定した Cisco 属性値（AV）ペア属性を送信するように AAA サーバを設定する必要があります。この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応のポートのデータ デバイスだけに適用されます。許可に失敗した音声デバイスは、データ デバイスとして扱われます。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、errordisable になります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。他社製 IP Phone または音声デバイスはデータおよび音声 VLAN の両方に許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。音声デバイスが 音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポートセキュリティ MAC アドレス制限にカウントされません。
- データ デバイスにだけ RADIUS サーバからダイナミック VLAN 割り当てを使用できます。

- MDA では、IEEE 802.1x 認証をサポートしていないデバイスへのスイッチ ポートの接続を許可するフォールバック メカニズムとして、MAC 認証バイパスを使用できます。
- データまたは音声デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスがデータ VLAN で検出された場合や、複数の音声デバイスが音声 VLAN で検出された場合、ポートは errdisable になります。
- ポートのホスト モードをシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変更すると、ポートでは許可されたデータ デバイスは許可されたままになります。ただし、ポートの音声 VLAN で許可されている Cisco IP Phone は自動的に削除されるので、そのポートでは再認証を行う必要があります。
- ゲスト VLAN や制限付き VLAN などのアクティブ フォールバック メカニズムは、ポートをシングル モードまたはマルチホスト モードからマルチドメイン モードに変更したあとでも設定されたままになります。
- ポートのホスト モードをマルチドメイン モードからシングル モードまたはマルチホスト モードに変更すると、許可されているすべてのデバイスがポートから削除されます。
- まずデータ ドメインを許可してゲスト VLAN に参加させる場合、IEEE 802.1x 非対応の音声デバイスは、音声 VLAN のパケットをタグ付けして、認証を開始する必要があります。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーを備えた、許可されたデバイスは、ポートの音声 VLAN とデータ VLAN の両方のトラフィックに影響を与えることがあります。このようなデバイスを使用する場合は、ポートでユーザ単位 ACL を適用するデバイスは 1 台だけにしてください。

Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ

Network Edge Access Topology（NEAT）機能は、ワイヤリング クローゼット（会議室など）外の領域まで識別を拡張します。これにより、任意のタイプのデバイスをポートで認証できます。

- 802.1x スイッチ サプリカント：802.1x サプリカント機能を使用することで、別のスイッチのサプリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼット外にあり、トランク ポートを介してアップストリーム スイッチに接続される場合に役に立ちます。802.1x スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチで認証します。サプリカント スイッチが認証に成功すると、ポート モードがアクセスからトランクに変更されます。
- アクセス VLAN は、オーセンティケータ スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

デフォルトでは、BPDU ガードがイネーブルにされたオーセンティケータ スイッチにサプリカントのスイッチを接続する場合、オーセンティケータのポートはサプリカント スイッチが認証する

前にスパニングツリー プロトコル（STP）のブリッジ プロトコル データ ユニット（BPDU）を受信した場合、errdisable 状態になる可能性があります。Cisco IOS Release 15.0(1) SE 以降では、認証中にサプリカントのポートから送信されるトラフィックを制御できます。**dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証が完了する前にオーセンティケータ ポートがシャットダウンすることがないように、認証中に一時的にサプリカントのポートをブロックします。認証に失敗すると、サプリカントのポートが開きます。**no dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証期間中にサプリカント ポートが開きます。これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドによりオーセンティケータのスイッチ ポートでイネーブルになっている場合、サプリカント スイッチで **dot1x supplicant controlled transient** コマンドを使用することを強く推奨します。

（注） **spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用して、グローバルにオーセンティケータ スイッチで BPDU ガードをイネーブルにした場合、**dot1x supplicant controlled transient** コマンドを入力すると、BPDU の違反が避けられなくなります。

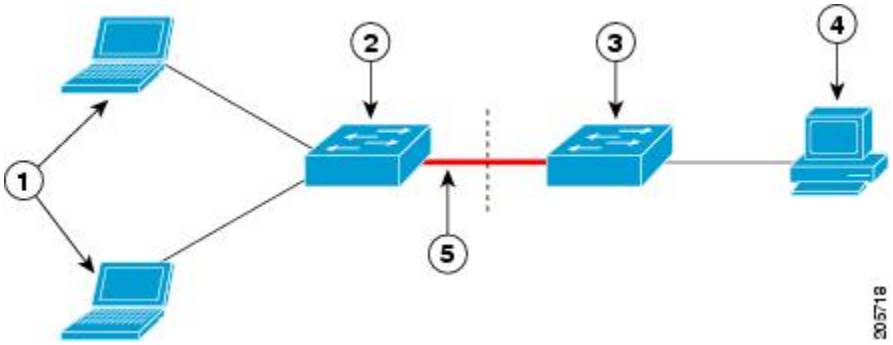
1 つ以上のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで MDA または multiauth モードをイネーブルにできます。マルチホスト モードはオーセンティケータ スイッチ インターフェイスではサポートされていません。

すべてのホスト モードで機能するように **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを Network Edge Access Topology（NEAT）のサプリカント スイッチで使用します。

- ホスト許可：許可済み（サプリカントでスイッチに接続する）ホストからのトラフィックだけがネットワークで許可されます。これらのスイッチは、Client Information Signalling Protocol（CISP）を使用して、サプリカント スイッチに接続する MAC アドレスをオーセンティケータ スイッチに送信します。
- 自動イネーブル化：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的にイネーブル化します。これにより、サプリカント スイッチから着信する複数の VLAN

のユーザ トラフィックが許可されます。ACS で cisco-av-pair を *device-traffic-class=switch* として設定します（この設定は *group* または *user* 設定で行うことができます）。

図 *85*：*CISP* を使用したオーセンティケータまたはサプリカント スイッチ



1	ワークステーション（クライアント）	2	サプリカント スイッチ（ワイヤリング クローゼット外）
3	オーセンティケータ スイッチ	4	Access Control Server（ACS）
5	トランク ポート		

（注） **switchport nonegotiate** コマンドは、NEAT を使用したサプリカントおよびオーセンティケータ スイッチではサポートされません。このコマンドは、トポロジのサプリカント側で設定しないでください。オーセンティケータ サーバ側で設定した場合は、内部マクロによってポートからこのコマンドが自動的に削除されます。

音声認識 802.1x セキュリティ

（注） 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにするようにスイッチを設定します。以前のリリースでは、セキュリティ違反の原因であるデータ クライアントを認証しようとすると、ポート全体がシャットダウンし、接続が完全に切断されます。

この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

関連トピック

音声認識 802.1x セキュリティの設定, （1615 ページ）

コモン セッション ID

認証マネージャは、使用された認証方式が何であれ、クライアントの単一のセッション ID（共通セッション ID）を使用します。この ID は、表示コマンドや MIB などのすべてのレポートに使用されます。セッション ID は、セッション単位のすべての Syslog メッセージに表示されます。

セッション ID には、次の情報が含まれます。

- ネットワーク アクセス デバイス（NAD）の IP アドレス
- 一意の 32 ビット整数（機械的に増加します）
- セッション開始タイム スタンプ（32 ビット整数）

次に、show authentication コマンドの出力に表示されたセッション ID の例を示します。この例では、セッション ID は 160000050000000B288508E5 です。

```
スイッチ# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

次に、Syslog 出力にセッション ID が表示される例を示します。この例でも、セッション ID は 160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

セッション ID は、NAD、AAA サーバ、その他のレポート分析アプリケーションでクライアントを識別するために使用されます。ID は自動的に表示されます。設定は必要ありません。

802.1x ポートベース認証の設定方法

802.1x 認証のデフォルト設定

表 *115* : *802.1x* 認証のデフォルト設定

機能	デフォルト設定
スイッチの 802.1x イネーブル ステート	ディセーブル

機能	デフォルト設定
ポート単位の 802.1x イネーブル ステート	ディセーブル（force-authorized） ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • デフォルトのアカウンティング ポート • キー	• 指定なし • 1645。 • 1646。 • 指定なし
ホスト モード	シングル ホスト モード
制御方向	双方向制御
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
再認証回数	2回（ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数）
待機時間	60 秒（スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数）
再送信時間	30 秒（スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数）
最大再送信回数	2 回（スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数）
クライアント タイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間）

機能	デフォルト設定
認証サーバ タイムアウト時間	30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間） dot1x timeout server-timeout インターフェイス コンフィギュレーション コマンドを使用して、このタイムアウト時間を変更できます。
無活動タイムアウト	ディセーブル
ゲスト VLAN	指定なし
アクセス不能認証バイパス	ディセーブル
制限付き VLAN	指定なし
オーセンティケータ（スイッチ）モード	指定なし
MAC 認証バイパス	ディセーブル
音声認識セキュリティ	ディセーブル

802.1x 認証設定時の注意事項

802.1X 認証

802.1x 認証を設定する場合の注意事項は、次のとおりです。

- 802.1x 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当ててられた VLAN に割り当てられ、再認証後に別のVLANに割り当てられた場合に、この変更が発生します。

  802.1xポートが割り当てられているVLANがシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセスVLANがシャットダウンまたは削除された後、ポートは無許可になります。
- 802.1x プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポート タイプではサポートされません。

- ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで802.1x認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x認証はイネーブルになりません。802.1x対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
- ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x認証はイネーブルになりません。802.1x対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
- EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。
- スイッチド ポート アナライザ（SPAN）およびリモート SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートの 802.1x 認証をイネーブルにすることができます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1x 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは 802.1x 認証をイネーブルにすることができます。

- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x 認証をグローバルにイネーブルにする前に、802.1x 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- Cisco IOS Release 12.2(55)SE 以降のリリースでは、802.1x 認証に関連するシステム メッセージのフィルタリングがサポートされています。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、およびアクセス不能認証バイパス設定時の注意事項は、次のとおりです。

- 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。
- DHCP クライアントが接続されている 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1x 認証プロセスを再起動する設定を変更できます。802.1x 認証プロセスの設定を

軽減します（**authentication timer inactivity** および **authentication timer reauthentication** インターフェイス コンフィギュレーション コマンド）。設定の減少量は、接続された 802.1x クライアントのタイプによって異なります。

- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
  - この機能はシングル ホスト モードおよびマルチホスト モードの 802.1x ポートでサポートされます。
  - Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステートの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
  - Windows XP クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。
  - アクセス不能認証バイパス機能および制限 VLAN を 802.1x ポート上に設定できます。スイッチが制限付き VLAN 内でクリティカル ポートを再認証しようとし、すべての RADIUS サーバが利用不可能な場合、スイッチはポート ステートをクリティカル認証ステートに変更し、制限付き VLAN に残ります。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。
- ワイヤレス ゲスト クライアントが固定クライアント VLAN の代わりに外部クライアント VLAN から IP を取得する際には、クライアントに新しい DHCP 要求を発行するために、WLAN 設定で **ip dhcp required** コマンドを使用する必要があります。これは、クライアントがアンカーで正しくない IP を取得することを防止します。

MAC 認証バイパス

MAC 認証バイパス設定時の注意事項は次のとおりです。

- 特に明記していないかぎり、MAC 認証バイパスの注意事項は 802.1x 認証のものと同じです。
- ポートが MAC アドレスで許可された後に、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバ データベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。
- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を設定できます。指定できる範囲は 1 ～ 65535 秒です。

ポートあたりのデバイスの最大数

802.1x 対応のポートに接続できるデバイスの最大数です。

- シングルホストモードの場合、アクセスVLANで接続できるデバイスは1台だけです。ポートが音声 VLAN でも設定されている場合、音声 VLAN を介して送受信できる Cisco IP Phone の数には制限はありません。
- マルチドメイン認証（MDA）モードの場合、アクセスVLANで1台のデバイス、音声VLANで 1 台の IP Phone が許可されます。
- マルチホスト モードでは、1 つの 802.1x サプリカントだけがポートで許可されますが、非 802.1x ホストは数に制限なく、アクセス VLAN で許可されます。音声 VLAN で許可されるデバイスの数には制限はありません。

802.1x 準備状態チェックの設定

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。

802.1x 準備状態チェックは、802.1x で設定できるすべてのポートで使用できます。準備状態チェックは、**dot1x force-unauthorized** として設定されるポートでは使用できません。

802.1x 準備状態チェックをスイッチでイネーブルにする場合には、次の手順に従ってください。

はじめる前に

準備状態チェックをスイッチでイネーブルにする場合、次の注意事項に従ってください。

- 準備状態チェックは通常、802.1x がスイッチでイネーブルにされる前に使用されます。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用すると、スイッチ スタックのすべてのポートがテストされます。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x 対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。Syslog メッセージは生成されません。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x 対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。Syslog メッセージは生成されません。

- 準備状態チェックは、複数のホスト（たとえば、IP Phone に接続される PC）を扱うポートに送信できます。Syslog メッセージは、タイマー時間内に準備状態チェックに応答する各クライアントに生成されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **dot1x test eapol-capable** [**interface***interface-id*]
4. **dot1x test timeout***timeout*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**dot1x test eapol-capable** [**interface***interface-id*] 例： スイッチ# **dot1x test eapol-capable interface gigabitethernet1/0/13** DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable	スイッチ上で 802.1x 準備状態チェックをイネーブルにします。 （任意）*interface-id* では、IEEE 802.1x の準備状態をチェックするポートを指定します。 （注） オプションの **interface** キーワードを省略した場合、スイッチのすべてのインターフェイスがテストされます。
ステップ 4	**dot1x test timeout***timeout*	（任意）EAPOL 応答の待機に使用するタイムアウトを設定します。範囲は 1 ～ 65535 秒です。デフォルトは 10 秒です。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

802.1x 準備状態チェック，（1586 ページ）

音声認識 802.1x セキュリティの設定

（注） 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能をスイッチで使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにします。この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

スイッチで音声認識 802.1x 音声セキュリティを設定する場合、次の注意事項に従ってください。

- **errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力して、音声認識 802.1x セキュリティをイネーブルにします。音声認識 802.1x セキュリティをディセーブルにするには、このコマンドの **no** バージョンを入力します。このコマンドは、スイッチの 802.1x 設定ポートのすべてに適用されます。

（注） **shutdown vlan** キーワードを指定しない場合、error-disabled ステートになったときにポート全体がシャットダウンされます。

- **errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して、error-disabled リカバリを設定すると、ポートは自動的に再びイネーブルにされます。error-disabled リカバリがポートで設定されていない場合、**shutdown** および **no-shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。
- 個々の VLAN を再びイネーブルにするには、**clear errdisable interface***interface-id***vlan** [*vlan-list*] 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルにされます。

音声認識 802.1x セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **errdisable detect cause security-violation shutdown vlan**
3. **errdisable recovery cause security-violation**
4. **clear errdisable interface***interface-id***vlan***[vlan-list]*
5. 次を入力します。
   - **shutdown**
   - **no shutdown**
6. **end**
7. **show errdisable detect**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**errdisable detect cause security-violation shutdown vlan**	セキュリティ違反エラーが発生したすべての VLAN をシャットダウンします。 （注） **shutdown vlan** キーワードを指定しない場合、すべてのポートが errdisable ステートになり、シャットダウンされます。
ステップ 3	**errdisable recovery cause security-violation**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**clear errdisable interface***interface-id***vlan***[vlan-list]*	（任意）errordisable になっている個々の VLAN を再びイネーブルにします。 • interface-id の場合、個々の VLAN を再びイネーブルにするポートを指定します。 • （任意）vlan-list の場合、再びイネーブルにする VLAN のリストを指定します。vlan-list を指定しない場合は、すべての VLAN が再びイネーブルになります。
ステップ 5	次を入力します。 • **shutdown** • **no shutdown**	（任意）errordisable の VLAN を再びイネーブルにして、すべての errordisable 指示をクリアします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show errdisable detect**	入力内容を確認します。

次に、セキュリティ違反エラーが発生した任意の VLAN をシャットダウンするようにスイッチを設定する例を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次に、ポート ギガビット イーサネット 40/2 で errdisable ステートであったすべての VLAN を再度イネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet4/0/2
vlan
```

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

関連トピック

音声認識 802.1x セキュリティ，（1607 ページ）

802.1x 違反モードの設定

次に示す状況で、シャットダウン、Syslog エラーを生成、または新しいデバイスからのパケットを廃棄するように 802.1x ポートを設定できます。

- デバイスが 802.1x 対応のポートに接続した
- ポートで認証されるデバイスの最大数に達した

スイッチ上にセキュリティ違反アクションを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **aaa new-model**
3. **aaa authentication dot1x** {**default**} *method1*
4. **interface***interface-id*
5. **switchport mode access**
6. **authentication violation** {**shutdown** | **restrict** | **protect** | **replace**}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model** 例： スイッチ(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1* 例： スイッチ(config)# **aaa authentication dot1x default group radius**	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。
ステップ 4	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/4**	IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**switchport mode access** 例： `スイッチ(config-if)# switchport mode access`	ポートをアクセス モードに設定します。
ステップ 6	**authentication violation** {**shutdown** | **restrict** | **protect** | **replace**} 例： `スイッチ(config-if)# authentication violation restrict`	違反モードを設定します。キーワードの意味は次のとおりです。 • **shutdown**：ポートを errordisable にします。 • **restrict**：syslog エラーを生成します。 • **protect**：トラフィックをポートに送信するすべての新しいデバイスからパケットをドロップします。 • **replace**：現在のセッションを削除し、新しいホストで認証します。
ステップ 7	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

802.1X 認証の設定

ユーザ単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1x の AAA プロセスを示します。

はじめる前に

802.1x ポートベース認証を設定するには、認証、許可、アカウンティング（AAA）をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

手順の概要

1. ユーザがスイッチのポートに接続します。
2. 認証が実行されます。
3. RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。
4. スイッチが開始メッセージをアカウンティング サーバに送信します。
5. 必要に応じて、再認証が実行されます。
6. スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバに送信します。
7. ユーザがポートから切断します。
8. スイッチが停止メッセージをアカウンティング サーバに送信します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ユーザがスイッチのポートに接続します。	
ステップ 2	認証が実行されます。	
ステップ 3	RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。	
ステップ 4	スイッチが開始メッセージをアカウンティング サーバに送信します。	
ステップ 5	必要に応じて、再認証が実行されます。	
ステップ 6	スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバに送信します。	
ステップ 7	ユーザがポートから切断します。	
ステップ 8	スイッチが停止メッセージをアカウンティング サーバに送信します。	

802.1x ポートベース認証の設定

802.1x ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **aaa new-model**
3. **aaa authentication dot1x** {**default**} *method1*
4. **dot1x system-auth-control**
5. **aaa authorization network** {**default**} **group radius**
6. **radius server***server name*
7. **key***string*
8. **interface***interface-id*
9. **switchport mode access**
10. **authentication port-control auto**
11. **dot1x pae authenticator**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**aaa new-model** 例： `スイッチ(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1* 例： `スイッチ(config)# aaa authentication dot1x default group radius`	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。 （注） **group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

	コマンドまたはアクション	目的
ステップ 4	**dot1x system-auth-control** 例： スイッチ(config)# **dot1x system-auth-control**	スイッチで 802.1x 認証をグローバルにイネーブルにします。
ステップ 5	**aaa authorization network** {**default**} **group radius** 例： スイッチ(config)# **aaa authorization network default group radius**	（任意）ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザRADIUS許可をスイッチに設定します。
ステップ 6	**radius server***server name* 例： スイッチ(config)# **radius server rsim address ipv4 124.2.2.12**	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 7	**key***string* 例： スイッチ(config-radius-server)# **key rad123**	（任意）RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。
ステップ 8	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**switchport mode access** 例： スイッチ(config-if)# **switchport mode access**	（任意）ステップ 6 および 7 で RADIUS サーバを設定した場合のみ、ポートをアクセス モードに設定します。
ステップ 10	**authentication port-control auto** 例： スイッチ(config-if)# **authentication port-control auto**	ポートでの 802.1x 認証をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**dot1x pae authenticator** 例： スイッチ(config-if)# **dot1x pae authenticator**	インターフェイスのポートアクセスエンティティを、オーセンティケータとしてのみ動作し、サプリカント用のメッセージは無視するように設定します。
ステップ 12	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

スイッチと RADIUS サーバ間の通信の設定

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチのIPアドレス、およびサーバとスイッチの双方で共有するキーストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

スイッチで RADIUS サーバのパラメータを設定するには、次の手順を実行します。この手順は必須です。

はじめる前に

認証、許可、およびアカウンティング（AAA）をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius server***server name***address ipv4***ip address***auth-port***port number***acct-port***port number***key***string*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server***server name***address ipv4***ip address***auth-port***port number***acct-port***port number***key***string* 例： スイッチ(config)# **radius server rsim address ipv4 124.2.2.12**	（任意）RADIUS サーバの IP アドレスを指定します。 **auth-port***port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1645 です。指定できる範囲は 0 ～ 65536 です。 **auth-port***port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1646 です。 （任意）**key***string* には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に **radius server** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

スイッチと RADIUS サーバ間の通信，（1586 ページ）

ホスト モードの設定

authentication port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている IEEE 802.1x 許可ポート上で、複数のホスト（クライアント）を許可するには、特権 EXEC モードで次の手順を実行します。MDA を設定してイネーブルにするには、**multi-domain** キーワードを使用します。これにより、ホスト デバイス、および IP Phone（シスコ製または他社製）など音声デバイスの両方が同じスイッチ ポートで許可されます。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] 例： スイッチ(config-if)# **authentication host-mode multi-host**	単一の 802.1x 許可ポートで複数のホスト（クライアント）を許可することができます。 キーワードの意味は次のとおりです。 • **multi-auth**：音声 VLAN で 1 クライアント、データ VLAN で複数の認証クライアントを許可します。 （注） **multi-auth** キーワードを使用できるのは、**authentication host-mode** コマンドだけです。 • **multi-host**：シングル ホストの認証後に 802.1x 許可ポートで複数のホストの接続を許可します。 • **multi-domain**：ホスト デバイスと IP Phone（シスコ製または他社製）など音声デバイスの両方が、IEEE 802.1x 許可ポートで認証されるようにします。

	コマンドまたはアクション	目的
		（注） ホストモードが **multi-domain** に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。 指定したインターフェイスで **authentication port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。
ステップ 4	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

定期的な再認証の設定

802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証を行う間隔（秒）を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **authentication periodic**
4. **authentication timer** {{[**inactivity** | **reauthenticate** | **restart**]} {*value*}}
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication periodic** 例： スイッチ(config-if)# **authentication periodic**	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。 （注） デフォルト値は 3600 秒です。再認証タイマーの値を変更するか、スイッチで RADIUS-provided セッション タイムアウトを使用するようにするには、**authentication timer reauthenticate** コマンドを入力します。
ステップ 4	**authentication timer** {{[**inactivity** | **reauthenticate** | **restart**]} {*value*}} 例： スイッチ(config-if)# **authentication timer reauthenticate 180**	再認証の試行の間隔（秒）を設定します。 **authentication timer** キーワードの意味は次のとおりです。 • **inactivity**：クライアントからのアクティビティがなくなり無許可になるまでの間隔（秒単位）。 • **reauthenticate**：自動再認証試行が開始されるまでの時間（秒） • **restart** *value*：無許可ポートの認証を試行するまでの間隔（秒単位）。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。**authentication timer inactivity** インターフェイス コンフィギュレーション コマンドは、アイドル状態の期間を制御します。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **authentication timer inactivity** *seconds*
4. **end**
5. **show authentication sessions interface** *interface-id*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication timer inactivity** *seconds* 例： スイッチ(config-if)# **authentication timer inactivity 30**	クライアントとの認証のやり取りに失敗した場合に、スイッチが待機状態のままでいる秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 60 秒です。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication sessions interface** *interface-id* 例： スイッチ# **show authentication sessions interface gigabitethernet2/0/1**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。スイッチがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、その後フレームを再送信します。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチがクライアントからの通知を待機する時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **authentication timer reauthenticate** *seconds*
4. **end**
5. **show authentication sessions interface** *interface-id*
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication timer reauthenticate** *seconds* 例： スイッチ(config-if)# **authentication timer reauthenticate 60**	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 5 秒です。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication sessions interface** *interface-id* 例： スイッチ# **show authentication sessions interface gigabitethernet2/0/1**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチからクライアントへのフレーム再送信回数の設定

スイッチからクライアントへの再送信時間を変更できるだけでなく、（クライアントから応答が得られなかった場合に）スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチからクライアントへのフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **dot1x max-reauth-req** *count*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-req** *count* 例： スイッチ(config-if)# **dot1x max-reauth-req 5**	スイッチが認証処理を再開するまでに、クライアントへ EAP 要求/アイデンティティ フレームを送信する回数を変更できます。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

再認証回数の設定

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **dot1x max-req** *count*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ# **interface gigabitethernet2/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： スイッチ(config-if)# **switchport mode access**	RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。

	コマンドまたはアクション	目的
ステップ 4	**dot1x max-req** *count* 例： `スイッチ(config-if)# dot1x max-req 4`	ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ～ 10 です。デフォルトは 2 です。
ステップ 5	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

MAC 移動のイネーブル化

MAC 移動を使用すると、認証されたホストをスイッチのポート間で移動できます。

スイッチで MAC 移動をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **authentication mac-move permit**
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**authentication mac-move permit** 例： `スイッチ(config)# authentication`	スイッチで MAC 移動をイネーブルにします。デフォルトは deny です。 セッション認識型ネットワーク モードでは、デフォルト CLI は **access-session mac-move deny** です。セッション認

	コマンドまたはアクション	目的
	mac-move permit	識型ネットワークでMAC移動をイネーブルにするには、**no access-session mac-move** グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MAC 置換のイネーブル化

MAC 置換を使用すると、ホストはポート上の認証ホストを置換できます。

インターフェイス上で MAC 置換をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **authentication violation** {**protect** | **replace** | **restrict** | **shutdown**}
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/2**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication violation** {**protect** | **replace** | **restrict** | **shutdown**} 例： スイッチ(config-if)# **authentication violation replace**	インターフェイス上でMAC置換をイネーブルにするには、**replace** キーワードを使用します。ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。 他のキーワードは、次のような機能があります。 • **protect**：ポートは、システム メッセージを生成せずに、予期しない MAC を使用するパケットをドロップします。 • **restrict**：違反パケットがCPUによってドロップされ、システム メッセージが生成されます。 • **shutdown**：ポートは、予期しない MAC アドレスを受信すると error disabled になります。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

IEEE 802.1x アカウンティングの設定

802.1xアカウンティングを使用して、AAAシステムアカウンティングをイネーブルにすると、ロギングのためにシステムリロードイベントをアカウンティングRADIUSサーバに送信できます。サーバは、アクティブな 802.1x セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップ メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

（注） ロギングの開始、停止、仮のアップデート メッセージ、タイム スタンプなどのアカウンティング タスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになった後、802.1x アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **aaa accounting dot1x default start-stop group radius**
4. **aaa accounting system default start-stop group radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/3**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting dot1x default start-stop group radius** 例： スイッチ(config-if)# **aaa accounting dot1x default start-stop group radius**	すべてのRADIUSサーバのリストを使用して802.1xアカウンティングをイネーブルにします。
ステップ 4	**aaa accounting system default start-stop group radius** 例： スイッチ(config-if)# **aaa accounting system default start-stop group radius**	（任意）システム アカウンティングをイネーブルにし（すべてのRADIUSサーバのリストを使用）、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的

ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1x 対応でないクライアントはゲスト VLAN に配置されます。802.1x 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングル ホスト モードまたはマルチ ホスト モードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. 次のいずれかを使用します。
   - **switchport mode access**
   - **switchport mode private-vlan host**
4. **authentication event no-response action authorize vlan***vlan-id*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/2**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。	• ポートをアクセス モードに設定します。

	コマンドまたはアクション	目的
	• **switchport mode access** • **switchport mode private-vlan host** 例： スイッチ(config-if)# **switchport mode private-vlan host**	• レイヤ2ポートをプライベートVLANホストポートとして設定します。
ステップ4	**authentication event no-response action authorize vlan***vlan-id* 例： スイッチ(config-if)# **authentication event no-response action authorize vlan 2**	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。
ステップ5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

制限付き VLAN の設定

スイッチ スタックまたはスイッチ上に制限付き VLAN を設定している場合、認証サーバが有効なユーザ名またはパスワードを受信できないと、IEEE 802.1x に準拠しているクライアントは制限付き VLAN に移されます。スイッチは、シングル ホスト モードでのみ制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. 次のいずれかを使用します。
   - **switchport mode access**
   - **switchport mode private-vlan host**
4. **authentication port-control auto**
5. **authentication event fail action authorize vlan***vlan-id*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet2/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **switchport mode access** • **switchport mode private-vlan host** 例： `スイッチ(config-if)# switchport mode access`	• ポートをアクセス モードに設定します。 • レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** 例： `スイッチ(config-if)# authentication port-control auto`	ポートでの 802.1x 認証をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**authentication event fail action authorize vlan***vlan-id* 例： スイッチ(config-if)# **authentication event fail action authorize vlan 2**	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。
ステップ 6	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

制限付き VLAN の認証試行回数の設定

ユーザを制限付き VLAN に割り当てる前に、**authentication event retry***retry count* インターフェイス コンフィギュレーション コマンドを使用して、認証試行の最大回数を設定できます。指定できる試行回数は 1 ～ 3 です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. 次のいずれかを使用します。
   - **switchport mode access**
   - **switchport mode private-vlan host**
4. **authentication port-control auto**
5. **authentication event fail action authorize vlan***vlan-id*
6. **authentication event retry***retry count*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/3**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **switchport mode access** • **switchport mode private-vlan host** 例： または スイッチ(config-if)# **switchport mode access**	• ポートをアクセス モードに設定します。 • レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** 例： スイッチ(config-if)# **authentication port-control auto**	ポートでの 802.1x 認証をイネーブルにします。
ステップ 5	**authentication event fail action authorize vlan***vlan-id* 例： スイッチ(config-if)# **authentication event fail action authorize vlan 8**	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。
ステップ 6	**authentication event retry***retry count* 例： スイッチ(config-if)# **authentication event retry 2**	ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は 1 ～ 3 秒です。デフォルトは 3 回に設定されています。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定

ポートにクリティカル音声 VLAN を設定し、アクセス不能認証バイパス機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **aaa new-model**
3. **radius-server dead-criteria**{**time** *seconds* } [**tries** *number*]
4. **radius-serverdeadtime***minutes*
5. **radius-server host ip-address** *address*[**acct-port** *udp-port*][**auth-port** *udp-port*] [**testusername** *name*[**idle-time** *time*] [**ignore-acct-port**][**ignore auth-port**]] [**key** *string*]
6. **dot1x critical** {**eapol** | **recovery delay** *milliseconds*}
7. **interface** *interface-id*
8. **authentication event server dead action** {**authorize** | **reinitialize**} **vlan** *vlan-id*]
9. **switchport voice vlan** *vlan-id*
10. **authentication event server dead action authorize voice**
11. **show authentication interface** *interface-id*
12. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**aaa new-model** 例： スイッチ(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 3	**radius-server dead-criteria**{**time** *seconds* } [**tries** *number*] 例： スイッチ(config)# **radius-server dead-criteria time 20 tries 10**	RADIUS サーバが使用不可またはダウン（切断）と見なされる条件を設定します。 • **time**：1 ～ 120 秒。スイッチは、デフォルトの *seconds* 値を 10 ～ 60 の間で動的に決定します。 • **number**：1 ～ 100 の試行回数。スイッチは、デフォルトの **tries***number* を 10 ～ 100 の間で動的に決定します。
ステップ 4	**radius-serverdeadtime***minutes* 例： スイッチ(config)# **radius-server deadtime 60**	（任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分（24 時間）です。デフォルト値は 0 分です。
ステップ 5	**radius-server host ip-address** *address*[**acct-port** *udp-port*][**auth-port** *udp-port*] [**testusername** *name*[**idle-time** *time*] [**ignore-acct-port**][**ignore auth-port**]] [**key** *string*] 例： スイッチ(config)# **radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username user1 idle-time 30 key abc1234**	（任意）次のキーワードを使用して RADIUS サーバパラメータを設定します。 • **acct-port***udp-port*：RADIUS アカウンティング サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルトは 1646 です。 • **auth-port***udp-port*：RADIUS 認証サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルトは 1645 です。 （注） RADIUS アカウンティング サーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。 • **test username***name*：RADIUS サーバ ステータスの自動テストをイネーブルにして、使用するユーザ名を指定します。 • **idle-time** time：スイッチがテスト パケットをサーバに送信した後の間隔を分数で設定します。範囲は 1 ～ 35791 分です。デフォルトは 60 分（1 時間）です。 • **ignore-acct-port**：RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。

	コマンドまたはアクション	目的
		• **ignore-auth-port**：RADIUS サーバ認証ポートのテストをディセーブルにします。 • **key***string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 （注） キーの先行スペースは無視されますが、途中および末尾のスペースは有効なので、キーは必ず **radius-server host** コマンド構文の最後の項目として設定してください。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 **radius-server key** {**0**string | **7***string* | *string*} グローバル コンフィギュレーション コマンドを使用しても認証および暗号キーを設定できます。
ステップ 6	**dot1x critical** {**eapol** | **recovery delay** *milliseconds*} 例： スイッチ(config)# **dot1x critical eapol** (config)# **dot1x critical recovery delay 2000**	（任意）アクセス不能認証バイパスのパラメータを設定します。 • **eapol**：スイッチがクリティカルポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。 • **recovery delay***milliseconds*：使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカルポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です（ポートは毎秒再初期化できます）。
ステップ 7	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**authentication event server dead action** {**authorize** | **reinitialize**} **vlan** *vlan-id*] 例： スイッチ(config-if)# **authentication**	これらのキーワードを使用して、RADIUS サーバが到達不能な場合にポートでホストを移動します。 • **authorize**：認証しようとする新しいホストをユーザ指定のクリティカル VLAN に移動します。

	コマンドまたはアクション	目的
	event server dead action reinitialicze vlan 20	• **reinitialize**：ポートのすべての許可済みホストをユーザ指定のクリティカル VLAN に移動します。
ステップ 9	**switchport voice vlan** *vlan-id* 例： スイッチ(config-if)# **switchport voice vlan**	ポートの音声 VLAN を指定します。音声 VLAN はステップ 6 で設定されたクリティカル データ VLAN と同じにはできません。
ステップ 10	**authentication event server dead action authorize voice** 例： スイッチ(config-if)# **authentication event server dead action authorize voice**	RADIUS サーバが到達不能な場合、ポートのデータ トラフィックを音声 VLAN に移動するために、クリティカル音声 VLAN を設定します。
ステップ 11	**show authentication interface** *interface-id* 例： スイッチ(config-if)# **do show authentication interface gigabit 1/0/1**	（任意）設定を確認します。
ステップ 12	**copy running-config startup-config** 例： スイッチ(config-if)# **do copy running-config startup-config**	（任意）設定を確認します。

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server host** グローバル コンフィギュレーション コマンドを使用します。アクセス不能な認証バイパスをディセーブルにするには、**no authentication event server dead action** インターフェイス コンフィギュレーション コマンドを使用します。クリティカル音声 VLAN をディセーブルにするには、**authentication event server dead action authorize voice** インターフェイス コンフィギュレーション コマンドを使用します。

アクセス不能認証バイパスの設定例

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
スイッチ(config)# radius-server dead-criteria time 30 tries 20
スイッチ(config)# radius-server deadtime 60
スイッチ(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username
user1 idle-time 30 key abc1234
スイッチ(config)# dot1x critical eapol
スイッチ(config)# dot1x critical recovery delay 2000
スイッチ(config)# interface gigabitethernet 1/0/1
スイッチ(config-if)# dot1x critical
スイッチ(config-if)# dot1x critical recovery action reinitialize
スイッチ(config-if)# dot1x critical vlan 20
スイッチ(config-if)# end
```

WoL を使用した 802.1x 認証の設定

WoL を使用した 802.1x 認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **authentication control-direction** {**both** | **in**}
4. **end**
5. **show authentication sessions interface** *interface-id*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `スイッチ(config)# interface gigabitethernet2/0/3`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**authentication control-direction** {**both** | **in**} 例： スイッチ(config-if)# **authentication control-direction both**	ポートで WoL を使用して 802.1x 認証をイネーブルにし、次のキーワードを使用してポートを双方向または単方向に設定します。 • **both**：ポートを双方向に設定します。ポートは、ホストにパケットを送受信できません。デフォルトでは、ポートは双方向です。 • **in**：ポートを単方向に設定します。ポートは、ホストにパケットを送信できますが、受信はできません。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication sessions interface** *interface-id* 例： スイッチ# **show authentication sessions interface gigabitethernet2/0/3**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MAC 認証バイパスの設定

MAC認証バイパスをイネーブルにするには、特権EXECモードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **authentication port-control auto**
4. **mab** [**eap**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication port-control auto** 例： スイッチ(config-if)# **authentication port-control auto**	ポートでの 802.1x 認証をイネーブルにします。
ステップ 4	**mab** [**eap**] 例： スイッチ(config-if)# **mab**	MAC 認証バイパスをイネーブルにします。 （任意）**eap** キーワードを使用して、スイッチが認可に EAP を使用するように設定します。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

802.1x ユーザ ディストリビューションの設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **vlan group** *vlan-group-name* **vlan-list** *vlan-list*
3. **end**
4. **no vlan group** *vlan-group-name* **vlan-list** *vlan-list*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan group** *vlan-group-name* **vlan-list** *vlan-list* 例： スイッチ(config)# **vlan group eng-dept vlan-list 10**	VLAN グループを設定し、単一の VLAN または VLANの範囲をそのグループにマッピングします。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	**no vlan group** *vlan-group-name* **vlan-list** *vlan-list* 例： スイッチ(config)# **no vlan group eng-dept vlan-list 10**	VLAN グループ コンフィギュレーションまたは VLAN グループ コンフィギュレーションの要素をクリアします。

VLAN グループの設定例

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ コンフィギュレーションおよび指定 VLAN とのマッピングを確認する例を示します。

```
スイッチ(config)# vlan group eng-dept vlan-list 10

スイッチ(config)# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10

スイッチ(config)# show dot1x vlan-group all
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10
hr-dept                         20
```

次に、VLAN を既存の VLAN グループに追加し、VLAN が追加されたことを確認する例を示します。

```
スイッチ(config)# vlan group eng-dept vlan-list 30
スイッチ(config)# show vlan group eng-dept
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10,30
```

次に、VLAN を VLAN グループから削除する例を示します。

```
スイッチ# no vlan group eng-dept vlan-list 10
```

次に、すべての VLAN が VLAN グループからクリアされたときに、その VLAN グループもクリアされる例を示します。

```
スイッチ(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

スイッチ(config)# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループをクリアする方法を示します。

```
スイッチ(config)# no vlan group end-dept vlan-list all
スイッチ(config)# show vlan-group all
```

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

NAC レイヤ 2 802.1x 検証の設定

NAC レイヤ 2 802.1x 検証を設定できます。これは、RADIUS サーバを使用した 802.1x 認証とも呼ばれます。

NAC レイヤ 2 802.1x 検証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **authentication event no-response action authorize vlan** *vlan-id*
5. **authentication periodic**
6. **authentication timer reauthenticate**
7. **end**
8. **show authentication sessions interface** *interface-id*
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `スイッチ(config)# interface gigabitethernet2/0/3`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： `スイッチ(config-if)# switchport mode access`	RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**authentication event no-response action authorize vlan** *vlan-id* 例： `スイッチ(config-if)# authentication event no-response action authorize vlan 8`	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。
ステップ 5	**authentication periodic** 例： `スイッチ(config-if)# authentication periodic`	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**authentication timer reauthenticate** 例： スイッチ(config-if)# **authentication timer reauthenticate**	クライアントに対する再認証試行を設定します（1時間に設定）。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 7	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show authentication sessions interface** *interface-id* 例： スイッチ# **show authentication sessions interface gigabitethernet2/0/3**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

NEAT を使用したオーセンティケータ スイッチの設定

この機能を設定するには、ワイヤリング クローゼット外の 1 つのスイッチがサプリカントとして設定され、オーセンティケータ スイッチに接続されている必要があります。

（注） *cisco-av-pairs* は、ACS で *device-traffic-class=switch* として設定されている必要があります。これは、サプリカントが正常に認証された後でトランクとしてインターフェイスを設定します。

スイッチをオーセンティケータに設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **cisp enable**
3. **interface** *interface-id*
4. **switchport mode access**
5. **authentication port-control auto**
6. **dot1x pae authenticator**
7. **spanning-tree portfast**
8. **end**
9. **show running-config interface** *interface-id*
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable** 例： `スイッチ(config)# cisp enable`	CISP をイネーブルにします。
ステップ 3	**interface** *interface-id* 例： `スイッチ(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access** 例： `スイッチ(config-if)# switchport mode access`	ポート モードを **access** に設定します。
ステップ 5	**authentication port-control auto** 例： `スイッチ(config-if)# authentication`	ポート認証モードを auto に設定します。

	コマンドまたはアクション	目的
	port-control auto	
ステップ 6	**dot1x pae authenticator** 例： スイッチ(config-if)# **dot1x pae authenticator**	インターフェイスをポート アクセス エンティティ（PAE）オーセンティケータとして設定します。
ステップ 7	**spanning-tree portfast** 例： スイッチ(config-if)# **spanning-tree portfast trunk**	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で Port Fast をイネーブルにします。
ステップ 8	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config interface** *interface-id* 例： スイッチ# **show running-config interface gigabitethernet2/0/1**	設定を確認します。
ステップ 10	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

NEAT を使用したサプリカント スイッチの設定

スイッチをサプリカントに設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **cisp enable**
3. **dot1x credentials** *profile*
4. **username** *suppswitch*
5. **password** *password*
6. **dot1x supplicant force-multicast**
7. **interface** *interface-id*
8. **switchport trunk encapsulation dot1q**
9. **switchport mode trunk**
10. **dot1x pae supplicant**
11. **dot1x credentials** *profile-name*
12. **end**
13. **show running-config interface** *interface-id*
14. **copy running-config startup-config**
15. Configuring NEAT with Auto Smartports Macros

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable** 例： `スイッチ(config)# cisp enable`	CISP をイネーブルにします。
ステップ 3	**dot1x credentials** *profile* 例： `スイッチ(config)# dot1x credentials test`	802.1x クレデンシャル プロファイルを作成します。これは、サプリカントとして設定されるポートに接続する必要があります。
ステップ 4	**username** *suppswitch* 例： `スイッチ(config)# username suppswitch`	ユーザ名を作成します。

	コマンドまたはアクション	目的
ステップ 5	**password** *password* 例： スイッチ(config)# **password myswitch**	新しいユーザ名のパスワードを作成します。
ステップ 6	**dot1x supplicant force-multicast** 例： スイッチ(config)# **dot1x supplicant force-multicast**	ユニキャストまたはマルチキャスト パケットのいずれかを受信した場合にスイッチに強制的にマルチキャスト EAPOL だけを送信させます。 これにより、NEAT がすべてのホスト モードでのサプリカントスイッチで機能できるようにもなります。
ステップ 7	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport trunk encapsulation dot1q** 例： スイッチ(config-if)# **switchport trunk encapsulation dot1q**	ポートをトランク モードに設定します。
ステップ 9	**switchport mode trunk** 例： スイッチ(config-if)# **switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	**dot1x pae supplicant** 例： スイッチ(config-if)# **dot1x pae supplicant**	インターフェイスをポート アクセス エンティティ（PAE）サプリカントとして設定します。
ステップ 11	**dot1x credentials** *profile-name* 例： スイッチ(config-if)# **dot1x credentials test**	802.1x クレデンシャル プロファイルをインターフェイスに対応付けます。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 13	**show running-config interface** *interface-id* 例： スイッチ# **show running-config interface gigabitethernet1/0/1**	設定を確認します。
ステップ 14	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 15	Configuring NEAT with Auto Smartports Macros	スイッチ VSA ではなく Auto Smartport ユーザ定義マクロを使用して、オーセンティケータ スイッチを設定することもできます。詳細については、このリリースに対応する『*Auto Smartports Configuration Guide*』を参照してください。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定

スイッチで 802.1x 認証を設定するほか、ACS を設定する必要があります。情報については、『*Configuration Guide for Cisco Secure ACS 4.2*』を参照してください。
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs_config.pdf

（注） スイッチにダウンロードする前に、ダウンロード可能な ACL を ACS で設定する必要があります。

ポートでの認証後、**show ip access-list** 特権 EXEC コマンドを使用して、ポートにダウンロードした ACL を表示できます。

ダウンロード可能な ACL の設定

これらのポリシーは、クライアントが認証され、クライアント IP アドレスが IP デバイス トラッキング テーブルに追加された後で有効になります。その後スイッチがダウンロード可能な ACL をポートに適用します。

特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **ip device tracking**
3. **aaa new-model**
4. **aaa authorization network default local group radius**
5. **radius-server vsa send authentication**
6. **interface** *interface-id*
7. **ip access-group** *acl-id* **in**
8. **show running-config interface** *interface-id*
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip device tracking** 例： スイッチ(config)# **ip device tracking**	IP デバイス トラッキング テーブルを設定します。
ステップ 3	**aaa new-model** 例： スイッチ(config)# **aaa new-model**	AAA をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaa authorization network default local group radius** 例： スイッチ(config)# **aaa authorization network default local group radius**	許可の方法をローカルに設定します。認証方法を削除するには、**no aaa authorization network default local group radius** コマンドを使用します。
ステップ 5	**radius-server vsa send authentication** 例： スイッチ(config)# **radius-server vsa send authentication**	RADIUS VSA 送信認証を設定します。
ステップ 6	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/4**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip access-group** *acl-id* **in** 例： スイッチ(config-if)# **ip access-group default_acl in**	ポートの入力方向のデフォルト ACL を設定します。 （注） *acl-id* はアクセス リストの名前または番号です。
ステップ 8	**show running-config interface** *interface-id* 例： スイッチ(config-if)# **show running-config interface gigabitethernet2/0/4**	設定を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ダウンロード ポリシーの設定

特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **access-list** *access-list-number* **{ deny | permit } { hostname | any | host } log**
3. **interface** *interface-id*
4. **ip access-group** *acl-id* **in**
5. **exit**
6. **aaa new-model**
7. **aaa authorization network default group radius**
8. **ip device tracking**
9. **ip device tracking probe** [**count** | **interval** | **use-svi**]
10. **radius-server vsa send authentication**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **{ deny | permit } { hostname | any | host } log** 例： スイッチ(config)# **access-list 1 deny any log**	デフォルト ポート ACL を定義します。 access-list-number には、1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。 条件が一致した場合にアクセスを拒否する場合は **deny**、許可する場合は **permit** を指定します。 source は、次のようなパケットを送信するネットワークまたはホストの送信元アドレスです。 • **hostname**：ドット付き 10 進表記による 32 ビット長の値。 • **any**：source および source-wildcard の値 0.0.0.0 255.255.255.255 の省略形を意味するキーワード any。source-wildcard 値を入力する必要はありません。 • **host**：source および source-wildcard の値 source 0.0.0.0 の省略形を意味するキーワード host。 （任意）source-wildcard ビットを送信元アドレスに適用します。 （任意）ログを入力して、エントリと一致するパケットに関する情報ロギング メッセージをコンソールに送信します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/2**	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip access-group** *acl-id* **in** 例： スイッチ(config-if)# **ip access-group default_acl in**	ポートの入力方向のデフォルト ACL を設定します。 （注） acl-id はアクセス リストの名前または番号です。
ステップ 5	**exit** 例： スイッチ(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**aaa new-model** 例： スイッチ(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 7	**aaa authorization network default group radius** 例： スイッチ(config)# **aaa authorization network default group radius**	許可の方法をローカルに設定します。許可の方法を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 8	**ip device tracking** 例： スイッチ(config)# **ip device tracking**	IP デバイス トラッキング テーブルをイネーブルにします。 IP デバイス トラッキング テーブルをディセーブルにするには、**no ip device tracking** グローバル コンフィギュレーション コマンドを使用します。
ステップ 9	**ip device tracking probe** [**count** | **interval** | **use-svi**] 例： スイッチ(config)# **ip device**	（任意）IP デバイス トラッキング テーブルを設定します。 • **count** *count*：スイッチが ARP プローブを送信する回数を設定します。指定できる範囲は 1 ～ 5 です。デフォルトは 3 です。

	コマンドまたはアクション	目的
	tracking probe count	• **interval** *interval*：スイッチが ARP プローブを再送信するまでに応答を待機する時間（秒単位）を設定します。範囲は 30 ～ 300 秒です。デフォルトは 30 秒です。 • **use-svi**：スイッチ仮想インターフェイス（SVI）の IP アドレスを ARP プローブの送信元として使用します。
ステップ 10	**radius-server vsa send authentication** 例： スイッチ(config)# **radius-server vsa send authentication**	ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。 （注） ダウンロード可能な ACL が機能する必要があります。
ステップ 11	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

VLAN ID ベース MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **mab request format attribute 32 vlan access-vlan**
3. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**mab request format attribute 32 vlan access-vlan** 例： `スイッチ(config)# mab request format attribute 32 vlan access-vlan`	VLAN ID ベース MAC 認証をイネーブルにします。
ステップ 3	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

柔軟な認証順序の設定

下の手順で使用される例は、MAB が IEEE 802.1x 認証（dot1x）の前に試行されるように柔軟な認証の順序設定の順序を変更します。MAB は最初の認証方式として設定されているため、MAB に他のすべての認証方式よりも優先されます。

（注） これらの認証方式のデフォルトの順序とプライオリティを変更する前に、これらの変更による潜在的な結果を理解する必要があります。詳細について、http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/application_note_c27-573287_ps6638_Products_White_Paper.html を参照してください。

特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **authentication order [dot1x | mab] | {webauth}**
5. **authentication priority [dot1x | mab] | {webauth}**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： スイッチ(config-if)# **switchport mode access**	RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**authentication order [dot1x | mab] | {webauth}** 例： スイッチ(config-if)# **authentication order mab dot1x**	（任意）ポート上で使用される認証方式の順序を設定します。
ステップ 5	**authentication priority [dot1x | mab] | {webauth}** 例： スイッチ(config-if)# **authentication priority mab dot1x**	（任意）認証方式をポート プライオリティ リストに追加します。
ステップ 6	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

関連トピック

柔軟な認証の順序設定，（1602 ページ）

Open1x の設定

ポートの許可ステートの手動制御をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **authentication control-direction** {**both** | **in**}
5. **authentication fallback** *name*
6. **authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]
7. **authentication open**
8. **authentication order** [**dot1x** | **mab**] | {**webauth**}
9. **authentication periodic**
10. **authentication port-control** {**auto** | **force-authorized** | **force-un authorized**}
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： スイッチ(config-if)# **switchport mode access**	RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。

	コマンドまたはアクション	目的
ステップ 4	**authentication control-direction** {**both** | **in**} 例： スイッチ(config-if)# **authentication control-direction both**	（任意）ポート制御を単一方向モードまたは双方向モードに設定します。
ステップ 5	**authentication fallback** *name* 例： スイッチ(config-if)# **authentication fallback profile1**	（任意）802.1x 認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。
ステップ 6	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] 例： スイッチ(config-if)# **authentication host-mode multi-auth**	（任意）ポート上で認証マネージャ モードを設定します。
ステップ 7	**authentication open** 例： スイッチ(config-if)# **authentication open**	（任意）ポート上でオープン アクセスをイネーブルまたはディセーブルにします。
ステップ 8	**authentication order** [**dot1x** | **mab**] | {**webauth**} 例： スイッチ(config-if)# **authentication order dot1x webauth**	（任意）ポート上で使用される認証方式の順序を設定します。
ステップ 9	**authentication periodic** 例： スイッチ(config-if)# **authentication periodic**	（任意）ポート上で再認証をイネーブルまたはディセーブルにします。
ステップ 10	**authentication port-control** {**auto** | **force-authorized** | **force-un authorized**} 例： スイッチ(config-if)# **authentication port-control auto**	（任意）ポートの許可ステートの手動制御をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

関連トピック

Open1x 認証, （1603 ページ）

ポート上での 802.1x 認証のディセーブル化

802.1x 認証をポートでディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで 802.1x 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **no dot1x pae authenticator**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**switchport mode access** 例： スイッチ(config-if)# **switchport mode access**	（任意）RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**no dot1x pae authenticator** 例： スイッチ(config-if)# **no dot1x pae authenticator**	ポートでの 802.1x 認証をディセーブルにします。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

802.1x 認証設定のデフォルト値へのリセット

802.1x 認証設定をデフォルト値に戻すには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **dot1x default**
4. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ 3	**dot1x default** 例： スイッチ(config-if)# **dot1x default**	設定可能な 802.1x のパラメータをデフォルト値へ戻します。
ステップ 4	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

802.1x の統計情報およびステータスのモニタリング

表 *116*：特権 *EXEC* 表示コマンド

コマンド	目的
show dot1x all statistics	すべてのポートの 802.1x 統計情報を表示します。
show dot1x interface *interface-id* **statistics**	指定されたポートの 802.1x 統計情報を表示します。
show dot1x all [**count** | **details** | **statistics** | **summary**]	スイッチの 802.1x 管理ステータスおよび動作ステータスを表示します。
show dot1x interface *interface-id*	指定されたポートの 802.1x 管理ステータスおよび動作ステータスを表示します。

表 *117*：グローバル コンフィギュレーション コマンド

コマンド	目的
no dot1x logging verbose	冗長な 802.1x 認証メッセージをフィルタに掛けます（Cisco IOS Release 12.2(55) SE 以降）

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セッション アウェアなネットワーキングに対するアイデンティティ コントロール ポリシーおよびアイデンティティ サービス テンプレートの設定。	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

第 70 章

Web ベース認証の設定

この章では、Webベースの認証を設定する方法について説明します。この章の内容は、次のとおりです。

- 機能情報の確認，1673 ページ
- Web ベース認証の概要，1673 ページ
- Web ベース認証の設定方法，1684 ページ
- Web ベース認証ステータスのモニタリング，1703 ページ

機能情報の確認

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

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

Web ベース認証の概要

IEEE 802.1x サプリカントが実行されていないホスト システムのエンド ユーザを認証するには、Web 認証プロキシと呼ばれる Web ベース認証機能を使用します。

（注） Web ベース認証は、レイヤ 2 およびレイヤ 3 インターフェイス上に設定できます。

HTTP セッションを開始すると、Web ベース認証は、ホストからの入力 HTTP パケットを代行受信し、ユーザに HTML ログイン ページを送信します。ユーザはクレデンシャルを入力します。このクレデンシャルは、Web ベース認証機能により、認証のために認証、許可、アカウンティング（AAA）サーバに送信されます。

認証が成功すると、Web ベース認証はログイン成功 HTML ページをホストに送信し、AAA サーバから返されたアクセス ポリシーを適用します。

認証に失敗した場合、Web ベース認証は、ログインの失敗を示す HTML ページをユーザに転送し、ログインを再試行するように、ユーザにプロンプトを表示します。最大試行回数を超過した場合、Web ベース認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザは待機期間中、ウォッチ リストに載せられます。

（注） 中央 Web 認証リダイレクト用の HTTPS トラフィック インターセプションはサポートされていません。

（注） グローバル パラメータ マップ（method-type、custom、redirect）は、すべてのクライアントおよび SSID で同じ Web 認証方式（consent、web consent、webauth など）を使用するときにのみ使用する必要があります。これにより、すべてのクライアントが同じ Web 認証方式になります。

要件により、1 つの SSID に consent、別の SSID に webauth を使用する場合、名前付きパラメータ マップを 2 つ使用する必要があります。1 番目のパラメータ マップには consent を設定し、2 番目のパラメータ マップには webauth を設定する必要があります。

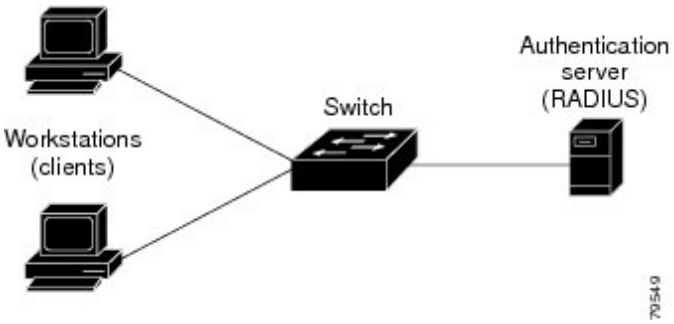
デバイスのロール

Web ベース認証では、ネットワーク上のデバイスに次のような固有の役割があります。

- クライアント：LAN およびサービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。このワークステーションでは、Java Script がイネーブルに設定された HTML ブラウザが実行されている必要があります。
- 認証サーバ：クライアントを認証します。認証サーバはクライアントの識別情報を確認し、そのクライアントが LAN およびスイッチのサービスへのアクセスを許可されたか、あるいはクライアントが拒否されたのかをスイッチに通知します。
- スイッチ：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。

次の図は、ネットワーク上でのこれらのデバイスの役割を示します。

図 *86*：*Web* ベース認証デバイスの役割



ホストの検出

スイッチは、検出されたホストに関する情報を格納するために、IPデバイストラッキングテーブルを維持します。

（注） デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

レイヤ 2 インターフェイスでは、Web ベース認証は、これらのメカニズムを使用して、IP ホストを検出します。

- ARP ベースのトリガー：ARP リダイレクト ACL により、Web ベース認証は、スタティック IP アドレス、またはダイナミック IP アドレスを持つホストを検出できます。
- ダイナミック ARP インスペクション
- DHCP スヌーピング：スイッチがホストの DHCP バインディング エントリを作成するときに Web ベース認証が通知されます。

セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストをレビューします。

  ホスト IP が例外リストに含まれている場合、この例外リスト エントリからポリシーが適用され、セッションが確立されます。

- 認証バイパスをレビューします。

  ホスト IP が例外リストに含まれていない場合、Web ベース認証は応答しないホスト（NRH）要求をサーバに送信します。

  サーバの応答が access accepted であった場合、認証はこのホストにバイパスされます。セッションが確立されます。

- HTTP インターセプト ACL を設定します。

  NRH 要求に対するサーバの応答が access rejected であった場合、HTTP インターセプト ACL がアクティブ化され、セッションはホストからの HTTP トラフィックを待機します。

認証プロセス

Web ベース認証をイネーブルにすると、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTP トラフィックが代行受信され、認証が開始されます。スイッチは、ユーザにログインページを送信します。ユーザはユーザ名とパスワードを入力します。スイッチはこのエントリを認証サーバに送信します。
- 認証に成功した場合、スイッチは認証サーバからこのユーザのアクセス ポリシーをダウンロードし、アクティブ化します。ログインの成功ページがユーザに送信されます
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザはログインを再試行します。失敗の回数が試行回数の最大値に達した場合、スイッチはログイン期限切れページを送信します。このホストはウォッチ リストに入れられます。ウォッチ リストのタイム アウト後、ユーザは認証プロセスを再試行することができます。
- 認証サーバがスイッチに応答せず、AAA 失敗ポリシーが設定されている場合、スイッチはホストに失敗アクセスポリシーを適用します。ログインの成功ページがユーザに送信されます
- ホストがレイヤ 2 インターフェイス上の ARP プローブに応答しなかった場合、またはホストがレイヤ 3 インターフェイスでアイドル タイムアウト内にトラフィックを送信しなかった場合、スイッチはクライアントを再認証します。
- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッション タイムアウトを適用します。
- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信します。Termination-Action は、サーバからの応答に含まれます。
- Termination-Action がデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除されます。

ローカル Web 認証バナー

Web 認証を使用して、デフォルトのカスタマイズ済み Web ブラウザ バナーを作成して、スイッチにログインしたときに表示するようにできます。

このバナーは、ログインページと認証結果ポップアップページの両方に表示されます。デフォルトのバナー メッセージは次のとおりです。

- 認証成功
- *Authentication Failed*

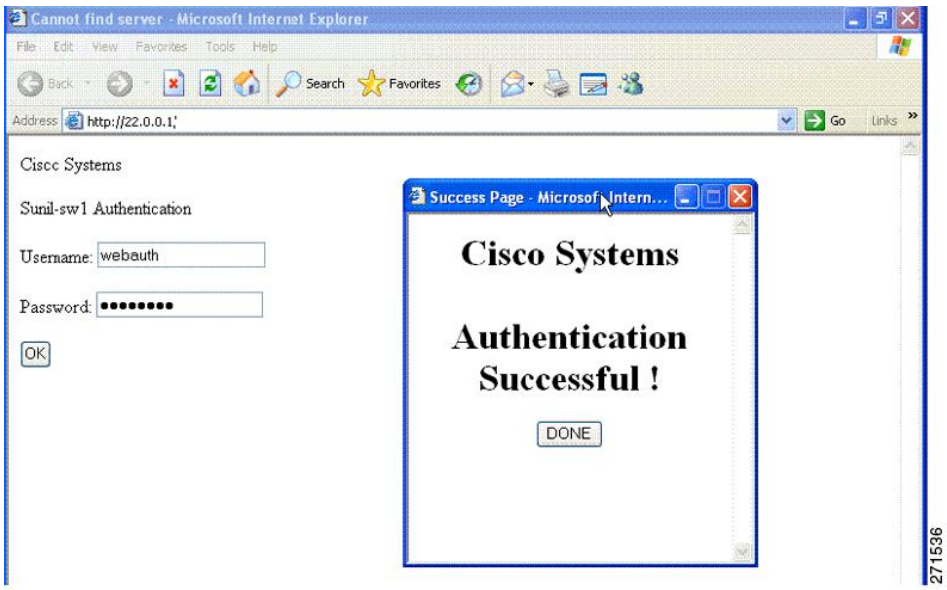
- 認証期限切れ

ローカル ネットワーク認証バナーは、レガシーおよび新スタイル（セッション アウェア）の CLI で次のように設定できます。

- レガシー モード：**ip admission auth-proxy-banner http** グローバル コンフィギュレーション コマンドを使用します。
- 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。

ログイン ページには、デフォルトのバナー、*Cisco Systems*、および *Switch host-name Authentication* が表示されます。*Cisco Systems* は認証結果ポップアップ ページに表示されます。

図 *87*：認証成功バナー

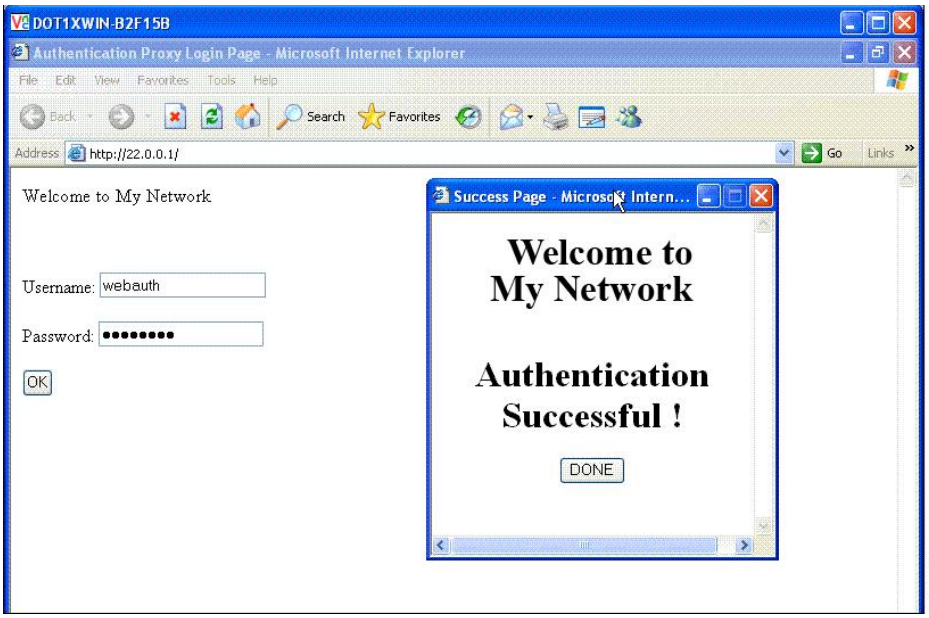


バナーは次のようにカスタマイズ可能です。

- スイッチ名、ルータ名、または会社名などのメッセージをバナーに追加する。
  - レガシー モード：**ip admission auth-proxy-banner http** *banner-text* グローバル コンフィギュレーション コマンドを使用します。
  - 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。
- ロゴまたはテキスト ファイルをバナーに追加する。
  - レガシー モード：**ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用します。

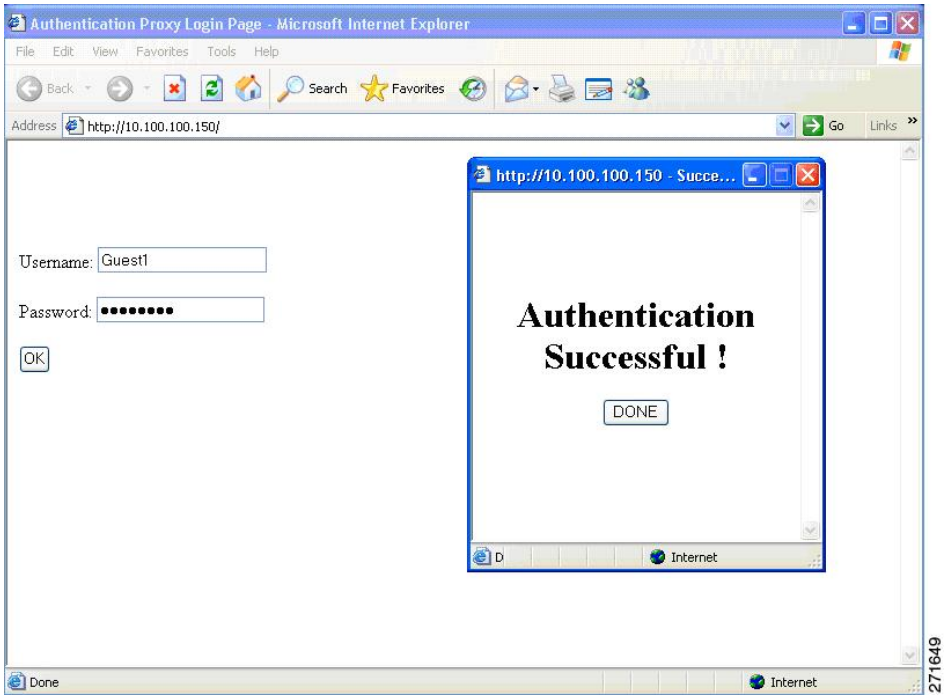
- 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。

図 *88*：カスタマイズされた *Web* バナー



バナーがイネーブルにされていない場合、Web 認証ログイン画面にはユーザ名とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはバナーは表示されません。

図 *89*：バナーが表示されていないログイン画面



詳細については、セッション対応『*Session Aware Networking Configuration Guide*』、『*Cisco IOS XE Release 3SE (Catalyst 3850 Switches) Session Aware Networking Configuration Guide*』、『*Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』、および『*Web Authentication Enhancements - Customizing Authentication Proxy*』 Web ページを参照してください。

Web 認証カスタマイズ可能な Web ページ

Web ベース認証プロセスでは、スイッチ内部の HTTP サーバは、認証中のクライアントに配信される 4 種類の HTML ページをホストします。サーバはこれらのページを使用して、ユーザに次の 4 種類の認証プロセス ステートを通知します。

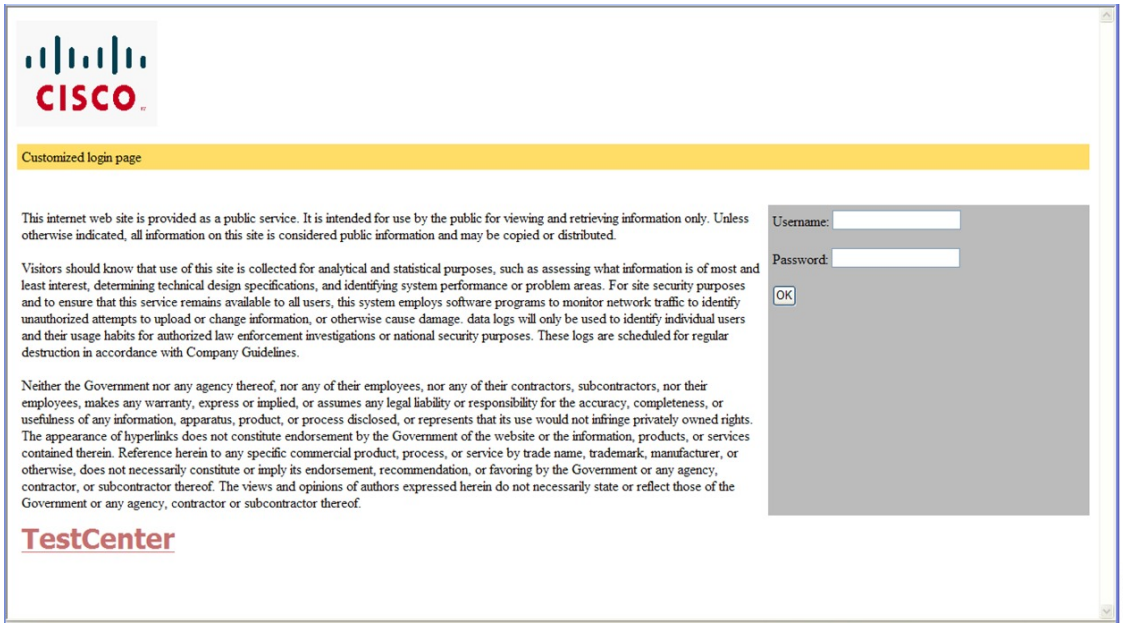
- ログイン：資格情報が要求されています。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：ログインの失敗回数が多すぎて、ログインセッションが期限切れになりました。

ガイドライン

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。
- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。
- バナー ページで、ログイン ページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。
- この URL 文字列は有効な URL（例：http://www.cisco.com）でなければなりません。不完全な URL は、Web ブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド（例：ページのタイム アウトを設定、暗号化されたパスワードの設定、同じページが 2 回送信されていないことの確認など）を記入する必要があります.
- 設定されたログイン フォームがイネーブルにされている場合、特定の URL にユーザをリダイレクトする CLI コマンドは使用できません。管理者は、Web ページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定の URL にユーザをリダイレクトする CLI コマンドを入力してから、Web ページを設定するコマンドを入力した場合、特定の URL にユーザをリダイレクトする CLI コマンドは効力を持ちません。
- 設定された Web ページは、スイッチのブート フラッシュ、またはフラッシュにコピーできます。
- スタック可能なスイッチでは、スタック マスターまたはスタック メンバーのフラッシュから設定済みのページにアクセスできます。
- ログイン ページを 1 つのフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、スタック マスター、またはメンバのフラッシュ）にすることができます。
- 4 ページすべてを設定する必要があります。
- Web ページを使ってバナー ページを設定した場合、このバナー ページには効果はありません。
- システム ディレクトリ（たとえば、flash、disk0、disk）に保存されていて、ログイン ページに表示する必要のあるロゴ ファイル（イメージ、フラッシュ、オーディオ、ビデオなど）すべてには、必ず、*web_auth_<filename>* の形式で名前をつけてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

デフォルトの内部HTMLページの代わりに、自分のHTMLページを使用することができます。認証後のユーザのリダイレクト先で、内部成功ページの代わりとなるURLを指定することもできます。

図 *90*：カスタマイズ可能な認証ページ



認証プロキシ Web ページの注意事項

カスタマイズされた認証プロキシ Web ページを設定する際には、次の注意事項に従ってください。

- カスタム Web ページ機能をイネーブルにするには、カスタム HTML ファイルを 4 個すべて指定します。指定したファイルの数が 4 個未満の場合、内部デフォルト HTML ページが使用されます。
- これら 4 個のカスタム HTML ファイルは、スイッチのフラッシュ メモリ内に存在しなければなりません。各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページ上のイメージはすべて、アクセス可能は HTTP サーバ上に存在しなければなりません。インターセプト ACL は、管理ルール内で設定します。
- カスタム ページからの外部リンクはすべて、管理ルール内でのインターセプト ACL の設定を必要とします。
- 有効な DNS サーバにアクセスするには、外部リンクまたはイメージに必要な名前解決で、管理ルール内にインターセプト ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルに設定されている場合、設定された auth-proxy-banner は使用されません。

- カスタム Web ページ機能がイネーブルに設定されている場合、ログインの成功に対するリダイレクション URL は使用できません。
- カスタム ファイルの指定を解除するには、このコマンドの **no** 形式を使用します。

カスタム ログイン ページはパブリック Web フォームであるため、このページについては、次の注意事項に従ってください。

- ログインフォームは、ユーザによるユーザ名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

関連トピック

認証プロキシ Web ページのカスタマイズ, （1693 ページ）

成功ログインに対するリダイレクト URL の注意事項

成功ログインに対するリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルに設定されている場合、リダイレクション URL 機能はディセーブルにされ、CLI では使用できません。リダイレクションは、カスタム ログイン成功ページで実行できます。
- リダイレクション URL 機能がイネーブルに設定されている場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの **no** 形式を使用します。
- Web ベースの認証クライアントが正常に認証された後にリダイレクション URL が必要な場合、URL 文字列は有効な URL（たとえば http://）で開始し、その後に URL 情報が続く必要があります。http:// を含まない URL が指定されると、正常に認証が行われても、そのリダイレクション URL によって Web ブラウザでページが見つからないまたは同様のエラーが生じる場合があります。

関連トピック

成功ログインに対するリダイレクション URL の指定, （1695 ページ）

その他の機能と Web ベース認証の相互作用

ポート セキュリティ

Web ベース認証とポート セキュリティは、同じポートに設定できます。Web ベース認証はポートを認証し、ポート セキュリティは、クライアントの MAC アドレスを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。この場合、このポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

関連トピック

ポート セキュリティのイネーブル化および設定, （1725 ページ）

LAN ポート IP

LAN ポート IP（LPIP）とレイヤ 2 Web ベース認証は、同じポートに設定できます。ホストは、まず Web ベース認証、次に LPIP ポスチャ検証を使用して認証されます。LPIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

Web ベース認証のアイドル時間が満了すると、NAC ポリシーは削除されます。ホストが認証され、ポスチャが再度検証されます。

Gateway IP

VLAN のいずれかのスイッチ ポートで Web ベース認証が設定されている場合、レイヤ 3 VLAN インターフェイス上にゲートウェイ IP（GWIP）を設定することはできません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェアで、両方の機能のホスト ポリシーが適用されます。GWIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

ACL

インターフェイスで VLAN ACL、または Cisco IOS ACL を設定した場合、ACL は、Web ベース認証のホスト ポリシーが適用された後だけ、ホスト トラフィックに適用されます。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの入力トラフィックについて、ポート ACL（PACL）をデフォルトのアクセス ポリシーとして設定することが、必須ではないですがより安全です。認証後、Web ベース認証のホスト ポリシーは、PACL に優先されます。ポートに設定された ACL がなくても、ポリシー ACL はセッションに適用されます。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN が VACL キャプチャ用に設定されているポートには Web ベース認証は設定できません。

コンテキストベース アクセス コントロール

コンテキストベース アクセス コントロール（CBAC）が、ポート VLAN のレイヤ 3 VLAN インターフェイスで設定されている場合、レイヤ 2 ポートで Web ベース認証は設定できません。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。Web ベース認証設定は、すべてのメンバ チャネルに適用されます。

Web ベース認証の設定方法

デフォルトの Web ベース認証の設定

次の表に、デフォルトの Web ベース認証の設定を示しています。

表 *118*：デフォルトの *Web* ベース認証の設定

機能	デフォルト設定
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	• 指定なし • 1645 • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

Web ベース認証の設定に関する注意事項と制約事項

- Web ベース認証は入力だけの機能です。
- Webベース認証は、アクセス ポートだけで設定できます。Webベース認証は、トランク ポート、EtherChannel メンバ ポート、またはダイナミック トランク ポートではサポートされていません。
- スタティックなARPキャッシュが割り当てられているレイヤ2インターフェイス上のホストは認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能では検出されません。
- デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IPデバイスのトラッキング機能をイネーブルにする必要があります。
- スイッチ HTTP サーバを実行するには、IP アドレスを少なくとも 1 つ設定する必要があります。また、各ホスト IP アドレスに到達するようにルートを設定する必要もあります。HTTP サーバは、ホストに HTTP ログイン ページを送信します。
- 2ホップ以上離れたところにあるホストでは、STP トポロジの変更により、ホストトラフィックの到着するポートが変わってしまった場合、トラフィックが停止する可能性があります。

これは、レイヤ 2（STP）トポロジの変更後に、ARP および DHCP の更新が送信されていない場合に発生します。

- Web ベース認証は、ダウンロード可能なホスト ポリシーとして、VLAN 割り当てをサポートしていません。
- Web ベース認証はセッション認識型ポリシー モードで IPv6 をサポートします。IPv6 Web 認証には、スイッチで設定された少なくても 1 つの IPv6 アドレスおよびスイッチ ポートに設定設定された IPv6 スヌーピングが必要です。
- Web ベース認証および Network Edge Access Topology（NEAT）は、相互に排他的です。インターフェイス上で NEAT がイネーブルの場合、Web ベース認証を使用できず、インターフェイス上で Web ベース認証が実行されている場合は、NEAT を使用できません。
- Web ベース認証 NRH（応答しないホスト）は、音声デバイスではサポートされません。
- パスワード認証プロトコル（PAP）のみがコントローラの Web ベースの RADIUS 認証でサポートされます。チャレンジ ハンドシェイク認証プロトコル（CHAP）は、コントローラの Web ベースの RADIUS 認証でサポートされません。
- スイッチから RADIUS サーバへの通信の設定に使用される次の RADIUS セキュリティ サーバ設定を確認します。
  - ホスト名
  - ホスト IP アドレス
  - ホスト名と特定の UDP ポート番号
  - IP アドレスと特定の UDP ポート番号

  IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って選択されます。
- RADIUS サーバ パラメータを設定する場合は、次の点に注意してください。
  - 別のコマンドラインに **key***string* を指定します。
  - **key***string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。
  - **key***string* を指定する場合、キーの中間、および末尾にスペースを使用します。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。
  - すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号キー値をグローバルに設定するには、**radius-server host** グローバル コンフィギュレーション コマ

ンドを使用します。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、radius-server transmit、および radius-server key グローバル コンフィギュレーション コマンドを使用します。詳細については、『*Cisco IOS Security Configuration Guide*, Release 12.4』および『*Cisco IOS Security Command Reference*, Release 12.4』を参照してください。

（注） RADIUS サーバでは、スイッチの IP アドレス、サーバとスイッチで共有される key string、およびダウンロード可能な ACL（DACL）などの設定を行う必要があります。詳細については、RADIUS サーバのマニュアルを参照してください。

認証ルールとインターフェイスの設定

この項での例は、レガシー スタイルの設定です。新しいスタイルの設定については、『*Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』を参照してください。

認証ルールおよびインターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admissionname***name***proxyhttp**
4. **interface***typeslot/port*
5. **ip access-group***name*
6. **ip admission***name*
7. **exit**
8. **ip device tracking**
9. **end**
10. **show ip admission status**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admissionname***name***proxyhttp** 例： スイッチ(config)# **ip admission name webauth1 proxy http**	Web ベース許可の認証ルールを設定します。
ステップ 4	**interface***typeslot/port* 例： スイッチ(config)# **interface gigabitEthernet1/0/1**	インターフェイス コンフィギュレーション モードを開始し、Webベース認証をイネーブルにする入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。 *type* には、fastethernet、gigabit ethernet、または tengigabitethernet を指定できます。
ステップ 5	**ip access-group***name* 例： スイッチ(config-if)# **ip access-group webauthag**	デフォルト ACL を適用します。
ステップ 6	**ip admission***name* 例： スイッチ(config-if)# **ip admission webauth1**	指定されたインターフェイスに Web ベース認証を設定します。
ステップ 7	**exit** 例： スイッチ(config-if)# **exit**	コンフィギュレーション モードに戻ります。
ステップ 8	**ip device tracking** 例： スイッチ(config)# **ip device tracking**	IP デバイス トラッキング テーブルをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 10	**show ip admission status** 例： スイッチ# **show ip admission *status***	設定を表示します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

AAA 認証の設定

AAA 認証を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa authentication login default group** {**tacacs+** | **radius**}
5. **aaa authorization auth-proxy default group** {**tacacs+** | **radius**}
6. **tacacs-server host** {*hostname* | *ip_address*}
7. **tacacs-server key** {*key-data*}
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**aaa new-model** 例： スイッチ(config)# **aaa new-model**	AAA 機能をイネーブルにします。
ステップ 4	**aaa authentication login default group** {**tacacs+** | **radius**} 例： スイッチ(config)# **aaa authentication login default group tacacs+**	ログイン時の認証方法のリストを定義します。
ステップ 5	**aaa authorization auth-proxy default group** {**tacacs+** | **radius**} 例： スイッチ(config)# **aaa authorization auth-proxy default group tacacs+**	Web ベース許可の許可方式リストを作成します。
ステップ 6	**tacacs-server host** {*hostname* | *ip_address*} 例： スイッチ(config)# **tacacs-server host 10.1.1.1**	AAA サーバを指定します。
ステップ 7	**tacacs-server key** {*key-data*} 例： スイッチ(config)# **tacacs-server key**	スイッチと TACACS サーバとの間で使用される許可および暗号キーを設定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ/RADIUS サーバ間通信の設定

RADIUS サーバのパラメータを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip radius source-interfacevlan***vlan interface number*
4. **radius-server host** {*hostname* | *ip-address*} **test username***username*
5. **radius-server key***string*
6. **radius-server dead-criteria tries***num-tries*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip radius source-interfacevlan***vlan interface number* 例： スイッチ(config)# **ip radius source-interface vlan 80**	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 4	**radius-server host** {*hostname* | *ip-address*} **test username***username* 例： スイッチ(config)# **radius-server host 172.120.39.46 test username user1**	リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **test username***username* は、RADIUS サーバ接続の自動テストをイネーブルにするオプションです。指定された *username* は有効なユーザ名である必要はありません。 **key** オプションは、スイッチと RADIUS サーバの間で使用される認証と暗号キーを指定します。 複数の RADIUS サーバを使用するには、それぞれのサーバでこのコマンドを入力してください。
ステップ 5	**radius-server key***string* 例： スイッチ(config)# **radius-server key rad123**	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。
ステップ 6	**radius-server dead-criteria tries***num-tries* 例： スイッチ(config)# **radius-server dead-criteria tries 30**	RADIUS サーバに送信されたメッセージへの応答がない場合に、このサーバが非アクティブであると見なすまでの送信回数を指定します。指定できる *num-tries* の範囲は 1 ～ 100 です。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

HTTP サーバの設定

Web ベース認証を使用するには、スイッチで HTTP サーバをイネーブルにする必要があります。このサーバは HTTP または HTTPS のいずれかについてイネーブルにできます。

（注） Apple の疑似ブラウザは、**ip http secure-server** コマンドだけを設定すると開きません。 **ip http server** コマンドも設定する必要があります。

HTTP または HTTPS のいずれかでサーバをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip http server**
4. **ip http secure-server**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http server** 例： `スイッチ(config)# ip http server`	HTTP サーバをイネーブルにします。Web ベース認証機能は、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。
ステップ 4	**ip http secure-server** 例： `スイッチ(config)# ip http`	HTTPS をイネーブルにします。 カスタム認証プロキシ Web ページを設定するか、成功ログインのリダイレクション URL を指定します。

	コマンドまたはアクション	目的
	secure-server	（注） **ip http secure-server** コマンドを入力したときに、セキュア認証が確実に行われるようにするには、ユーザが HTTP 要求を送信した場合でも、ログイン ページは必ずHTTPS（セキュア HTTP）形式になるようにします。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

認証プロキシ Web ページのカスタマイズ

Web ベースの認証中、スイッチのデフォルト HTML ページではなく、代わりの HTML ページがユーザに表示されるように、Web 認証を設定できます。

この機能のための同等のセッション認識型ネットワーク設定の例については、『*Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』マニュアルの「アイデンティティ制御ポリシーの設定」の章の「Web ベース認証のパラメータ マップの設定」の項を参照してください。

カスタム認証プロキシ Web ページの使用を指定するには、次の手順を実行してください。

はじめる前に

スイッチのフラッシュ メモリにカスタム HTML ファイルを保存します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admission proxy http login page file***device:login-filename*
4. **ip admission proxy http success page file***device:success-filename*
5. **ip admission proxy http failure page file***device:fail-filename*
6. **ip admission proxy http login expired page file***device:expired-filename*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admission proxy http login page file***device:login-filename* 例： スイッチ(config)# **ip admission proxy http login page file disk1:login.htm**	スイッチのメモリ ファイル システム内で、デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの場所を指定します。*device:* はフラッシュ メモリです。
ステップ 4	**ip admission proxy http success page file***device:success-filename* 例： スイッチ(config)# **ip admission proxy http success page file disk1:success.htm**	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 5	**ip admission proxy http failure page file***device:fail-filename* 例： スイッチ(config)# **ip admission proxy http fail page file disk1:fail.htm**	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 6	**ip admission proxy http login expired page file***device:expired-filename* 例： スイッチ(config)# **ip admission proxy http login expired page file disk1:expired.htm**	デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

認証プロキシ Web ページの注意事項, （1681 ページ）

成功ログインに対するリダイレクション URL の指定

認証後に内部成功 HTML ページを効果的に置き換えユーザのリダイレクト先となる URL を指定するためには、次の手順を実行してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admission proxy http success redirect***url-string*
4. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip admission proxy http success redirect***url-string* 例： `スイッチ(config)# ip admission proxy http success redirect www.example.com`	デフォルトのログイン成功ページの代わりにユーザをリダイレクトする URL を指定します。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

関連トピック

成功ログインに対するリダイレクト URL の注意事項, （1682 ページ）

Web ベース認証パラメータの設定

クライアントが待機時間中にウォッチ リストに掲載されるまで許容される失敗ログイン試行の最大回数を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admission max-login-attempts***number*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admission max-login-attempts***number* 例： スイッチ(config)# **ip admission max-login-attempts 10**	失敗ログイン試行の最大回数を設定します。指定できる範囲は 1 ～ 2147483647 回です。デフォルトは 5 分です。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Web ベース認証ローカル バナーの設定

Web 認証が設定されているスイッチにローカル バナーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admission auth-proxy-banner http** [*banner-text* | *file-path*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admission auth-proxy-banner http** [*banner-text*	*file-path*] 例： スイッチ(config)# **ip admission auth-proxy-banner http C My Switch C**	ローカル バナーをイネーブルにします。 （任意）*C banner-text C*（*C* は区切り文字）、またはバナーに表示されるファイル（たとえば、ロゴまたはテキスト ファイル）のファイル パスを入力して、カスタム バナーを作成します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SVI なしの Web ベース認証の設定

ルーティング テーブルに IP アドレスを作成せずに、HTML のログイン ページがクライアントにリダイレクトする SVI 機能なしの Web ベースの認証を設定します。これらの手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **parameter-map type webauth global**
4. **l2-webauth-enabled**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type webauth global** 例： スイッチ (config)# **parameter-map type webauth global**	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。グローバル キーワードで定義されたグローバル パラメータ マップでサポートされる特定のコンフィギュレーション コマンドは、parameter-map-name 引数で定義された名前付きパラメータ マップでサポートされるコマンドとは異なります。
ステップ 4	**l2-webauth-enabled** 例： スイッチ (config-params-parameter-map)# **l2-webauth-enabled**	SVI 機能なしの Web ベースの認証を有効にします
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VRF 認識による Web ベース認証の設定

HTML のログイン ページがクライアントにリダイレクトする VRF 認識による Web ベース認証を設定します。これらの手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **parameter-map type webauth global**
4. **webauth-vrf-aware**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type webauth global** 例： スイッチ (config)# **parameter-map type webauth global**	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。グローバル キーワードで定義されたグローバル パラメータ マップでサポートされる特定のコンフィギュレーション コマンドは、parameter-map-name 引数で定義された名前付きパラメータ マップでサポートされるコマンドとは異なります。
ステップ 4	**webauth-vrf-aware** 例： スイッチ (config-params-parameter-map)# **webauth-vrf-aware**	SVI で Web ベース認証の VRF 認識機能を有効にします。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

Web ベース認証キャッシュ エントリの削除

Web ベース認証キャッシュ エントリを削除するには、次の手順を実行します。

手順の概要

1. **enable**
2. **clear ip auth-proxy cache** {* | *host ip address*}
3. **clear ip admission cache** {* | *host ip address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**clear ip auth-proxy cache** {*	*host ip address*} 例： スイッチ# **clear ip auth-proxy cache 192.168.4.5**	Delete 認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。

	コマンドまたはアクション	目的
ステップ 3	**clear ip admission cache** {* | *host ip address*} 例： スイッチ# **clear ip admission cache 192.168.4.5**	Delete 認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングルホストのエントリを削除するには、具体的な IP アドレスを入力します。

Web ベース認証ステータスのモニタリング

すべてのインターフェイスまたは特定のポートに対する Web ベース認証設定を表示するには、このトピックのコマンドを使用します。

表 *119*：特権 *EXEC* 表示コマンド

コマンド	目的
show authentication sessions method webauth	FastEthernet、ギガビットイーサネット、または 10 ギガビットイーサネットのすべてのインターフェイスに対する Web ベースの認証設定を表示します。
show authentication sessions interface *type slot/port*[**details**]	FastEthernet、ギガビットイーサネット、または 10 ギガビット イーサネットの特定のインターフェイスに対する Web ベースの認証設定を表示します。 セッション認識型ネットワーク モードでは、**show access-session interface** コマンドを使用します。

第 71 章

ポート単位のトラフィック制御の設定

- ポートベースのトラフィック制御の概要，1705 ページ
- 機能情報の確認，1706 ページ
- ストーム制御に関する情報，1706 ページ
- ストーム制御の設定方法，1708 ページ
- 保護ポートに関する情報，1714 ページ
- 保護ポートの設定方法，1715 ページ
- 保護ポートのモニタリング，1716 ページ
- ポート ブロッキングに関する情報，1717 ページ
- ポート ブロッキングの設定方法，1717 ページ
- ポート ブロッキングのモニタリング，1719 ページ
- ポート セキュリティの前提条件，1719 ページ
- ポート セキュリティの制約事項，1719 ページ
- ポート セキュリティの概要，1720 ページ
- ポート セキュリティの設定方法，1725 ページ
- ポート セキュリティの設定例，1749 ページ

ポートベースのトラフィック制御の概要

ポートベースのトラフィック制御は、特定トラフィック状態に応じてポートレベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。次のポートベースのトラフィック制御機能が、このガイドの記述対象の Cisco IOS リリースでサポートされます。

- ストーム制御

- 保護ポート
- ポート ブロッキング
- ポート セキュリティ
- プロトコル ストーム プロテクション

機能情報の確認

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

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

ストーム制御に関する情報

ストーム制御

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム コントロール（またはトラフィック抑制）は、インターフェイスからスイッチング バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

トラフィック アクティビティの測定方法

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート

- 秒単位で受信するビット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 小さいフレームのトラフィック レートの秒単位のパケット数。この機能は、グローバルにイネーブルです。小さいフレームのしきい値は、各インターフェイスで設定されます。

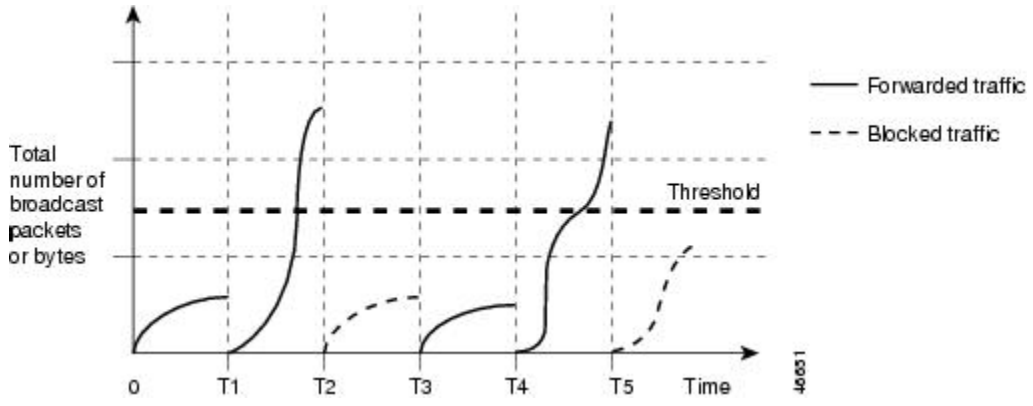
上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

（注） マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジ プロトコル データ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

トラフィック パターン

次の例は、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。

図 *91*：ブロードキャスト ストーム制御の例



T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。したがって、T2 と T5 の後のインターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル

（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過できるパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。

（注） パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御の設定方法

ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数 % の差異が生じる可能性があります。

（注） ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、次の手順を実行します。

はじめる前に

ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps***bps* [*bps-low*] | **pps***pps* [*pps-low*]}
5. **storm-control action** {**shutdown** | **trap**}
6. **end**
7. **show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps***bps* [*bps-low*] | **pps***pps* [*pps-low*]} 例： スイッチ(config-if)# **storm-control unicast level 87 65**	ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。 キーワードの意味は次のとおりです。 • *level* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ～ 100.00 です。 • （任意）*level-low* には、下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。この値は上限抑制値より小さ

	コマンドまたはアクション	目的
		いか、または等しくなければなりません。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ～ 100.00 です。 しきい値に最大値（100%）を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。 • **bps***bps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをビット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*bps-low* には、下限しきい値レベルをビット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ～ 10000000000.0 です。 • **pps***pps* には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low* には、下限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は **0.0 ～** 10000000000.0 です。 BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号（k、m、g など）を使用できます。
ステップ 5	**storm-control action** {**shutdown** | **trap**} 例： `スイッチ(config-if)#` **`storm-control action trap`**	ストーム検出時に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。 • ストーム中、ポートを error-disable の状態にするには、**shutdown** キーワードを選択します。 • ストームが検出された場合、SNMP（簡易ネットワーク管理プロトコル）トラップを生成するには、**trap** キーワードを選択します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**] 例： スイッチ# **show storm-control gigabitethernet1/0/1 unicast**	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御の設定が表示されます。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スモール フレーム到着レートの設定

67バイト未満の着信VLANタグ付きパケットは、小さいフレームと見なされます。このパケットはスイッチにより転送されますが、スイッチ ストーム制御カウンタを増加させません。

スイッチ上の小さいフレームの着信機能をグローバルにイネーブルにして、各インターフェイスのパケットの小さいフレームのしきい値を設定します。最小サイズよりも小さく、指定されたレート（しきい値）で着信するパケットは、ポートがディセーブルにされた後はドロップされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **errdisable detect cause small-frame**
4. **errdisable recovery interval***interval*
5. **errdisable recovery cause small-frame**
6. **interface***interface-id*
7. **small-frame violation-rate***pps*
8. **end**
9. **show interfaces***interface-id*
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**errdisable detect cause small-frame** 例： スイッチ(config)# **errdisable detect cause small-frame**	スイッチ上の小さいフレームの着信レート機能をイネーブルにします。
ステップ 4	**errdisable recovery interval***interval* 例： スイッチ(config)# **errdisable recovery interval 60**	（任意）指定された errdisable ステートから回復する時間を指定します。

	コマンドまたはアクション	目的
ステップ 5	**errdisable recovery cause small-frame** 例： スイッチ(config)# **errdisable recovery cause small-frame**	（任意）小さいフレームの着信によりポートが errdisable になった後、そのポートを自動的に再イネーブルにするリカバリ時間を設定します。 ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。
ステップ 6	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 7	**small-frame violation-rate***pps* 例： スイッチ(config-if)# **small-frame violation rate 10000**	インターフェイスが着信パケットをドロップしてポートを errdisable にするようにしきい値レートを設定します。範囲は、1 ～ 10,000 パケット/秒（pps）です。
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 9	**show interfaces***interface-id* 例： スイッチ# **show interfaces gigabitethernet1/0/2**	設定を確認します。
ステップ 10	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

保護ポートに関する情報

保護ポート

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ 2 トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータ トラフィックは、レイヤ 3 デバイスを介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

スイッチ スタックは論理的には 1 つのスイッチを表しているため、レイヤ 2 トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチ スタックの保護ポート間では転送されません。

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

保護ポートのガイドライン

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

保護ポートの設定方法

保護ポートの設定

はじめる前に

保護ポートは事前定義されていません。これは設定する必要があるタスクです。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport protected**
5. **end**
6. **show interfaces***interface-id***switchport**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**switchport protected** 例： `スイッチ(config-if)# switchport protected`	インターフェイスを保護ポートとして設定します。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces***interface-id***switchport** 例： `スイッチ# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。
ステップ 7	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

保護ポートのモニタリング

表 *120*：保護ポートの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

ポート ブロッキングに関する情報

ポート ブロッキング

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャスト トラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにします。

（注） マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

ポート ブロッキングの設定方法

インターフェイスでのフラッディング トラフィックのブロッキング

はじめる前に

インターフェイスは物理インターフェイスまたはEtherChannelグループのいずれも可能です。ポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport block multicast**
5. **switchport block unicast**
6. **end**
7. **show interfaces***interface-id***switchport**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport block multicast** 例： スイッチ(config-if)# **switchport block multicast**	ポートからの未知のマルチキャストの転送をブロックします。 （注） 純粋なレイヤ2マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。
ステップ 5	**switchport block unicast** 例： スイッチ(config-if)# **switchport block unicast**	ポートからの未知のユニキャストの転送をブロックします。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces***interface-id***switchport** 例： スイッチ# **show interfaces gigabitethernet1/0/1 switchport**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ポート ブロッキングのモニタリング

表 *121*：ポート ブロッキングの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

ポート セキュリティの前提条件

（注） 最大値をインターフェイス上ですでに設定されているセキュア アドレスの数より小さい値に設定しようとすると、コマンドが拒否されます。

ポート セキュリティの制約事項

スイッチまたはスイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数は、アクティブ スイッチ データベース管理（SDM）テンプレートによって決まります。この数は使用可能な MAC アドレ

スの合計で、他のレイヤ 2 機能で使用されるものや、インターフェイスで設定されたその他のセキュアな MAC アドレスが含まれています。

ポート セキュリティの概要

ポート セキュリティ

ポート セキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレス グループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュア ポートとしてポートを設定し、セキュア MAC アドレスが最大数に達した場合、ポートにアクセスを試みるステーションの MAC アドレスが識別されたセキュア MAC アドレスのいずれとも一致しないので、セキュリティ違反が発生します。また、あるセキュア ポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュア ポートにアクセスしようとしたときにも、違反のフラグが立てられます。

関連トピック

ポート セキュリティのイネーブル化および設定, （1725 ページ）
ポート セキュリティの設定例, （1749 ページ）

セキュア MAC アドレスのタイプ

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- スタティック セキュア MAC アドレス：**switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレス テーブルに保存されたのち、スイッチの実行コンフィギュレーションに追加されます。
- ダイナミック セキュア MAC アドレス：動的に設定されてアドレス テーブルにのみ保存され、スイッチの再起動時に削除されます。
- スティッキー セキュア MAC アドレス：動的に学習することも、手動で設定することもできます。アドレス テーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

スティッキ セキュア MAC アドレス

スティッキー ラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキー セキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイ

スを設定できます。インターフェイスはスティッキ ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキー セキュア MAC アドレスに変換します。すべてのスティッキー セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキー セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション）に、自動的には反映されません。スティッキー セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキ セキュア アドレスを保存しない場合、アドレスは失われます。

スティッキ ラーニングがディセーブルの場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレス テーブルに追加されている状態で、アドレス テーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。

違反が発生した場合の対処に基づいて、次の 3 種類の違反モードのいずれかにインターフェイスを設定できます。

- protect（保護）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。

（注） トランク ポートに protect 違反モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

- restrict（制限）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
- shutdown（シャットダウン）：ポート セキュリティ違反により、インターフェイスが error-disabled になり、ただちにシャットダウンされます。そのあと、ポートの LED が消灯します。セキュア ポートが error-disabled ステートの場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこのステートを解

除するか、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにできます。これは、デフォルトのモードです。

- shutdown vlan（VLAN シャットダウン）：VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。

次の表に、ポート セキュリティをインターフェイスに設定した場合の違反モードおよび対処について示します。

表 *122*：セキュリティ違反モードの処置

違反モード	トラフィックの転送 [18]	SNMP トラップの送信	Syslog メッセージの送信	エラー メッセージの表示 [19]	違反カウンタの増加	ポートのシャットダウン
protect	No	No	No	No	No	No
restrict	No	Yes	Yes	No	Yes	No
shutdown	No	No	No	No	Yes	Yes
shutdown vlan	No	No	Yes	No	Yes	No [20]

18 十分な数のセキュア MAC アドレスを削除するまで未知の送信元アドレスを持つパケットがドロップされます。
19 セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラー メッセージを返します。
20 違反が発生した VLAN のみシャットダウンします。

ポート セキュリティ エージング

ポート上のすべてのセキュア アドレスにエージング タイムを設定するには、ポート セキュリティ エージングを使用します。ポートごとに 2 つのタイプのエージングがサポートされています。

- absolute：指定されたエージング タイムの経過後に、ポート上のセキュア アドレスが削除されます。
- inactivity：指定されたエージング タイムの間、セキュア アドレスが非アクティブであった場合に限り、ポート上のセキュア アドレスが削除されます。

関連トピック

ポート セキュリティ エージングのイネーブル化および設定, （1730 ページ）

ポート セキュリティとスイッチ スタック

スタックに新規に加入したスイッチは、設定済みのセキュア アドレスを取得します。他のスタック メンバーから新しいスタック メンバーに、ダイナミック セキュア アドレスがすべてダウンロードされます。

スイッチ（アクティブ スイッチまたはスタック メンバのいずれか）がスタックから離れると、その他のスタック メンバに通知が行き、そのスイッチが設定または学習したセキュア MAC アドレスがセキュア MAC アドレス テーブルから削除されます。

デフォルトのポート セキュリティ設定

表 *123*：デフォルトのポート セキュリティ設定

機能	デフォルト設定
ポート セキュリティ	ポート上でディセーブル
スティッキー アドレス ラーニング	ディセーブル
ポートあたりのセキュア MAC アドレスの最大数	1。
違反モード	shutdown。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。
ポート セキュリティ エージング	ディセーブルエージング タイムは 0 スタティック エージングはディセーブル タイプは absolute

ポート セキュリティの設定時の注意事項

- ポート セキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートをダイナミック アクセス ポートにすることはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- （注） 音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。

- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュア アドレスを設定する必要があります。
- トランク ポートがポート セキュリティで設定され、データ トラフィックのアクセス VLAN および音声トラフィックのアクセス VLAN に割り当てられている場合は、**switchport voice** および **switchport priority extend** インターフェイス コンフィギュレーション コマンドを入力しても効果はありません。

  接続装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレス、音声 VLAN の IP アドレスの順に要求すると、アクセス VLAN だけが IP アドレスに割り当てられます。
- インターフェイスの最大セキュアアドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングをサポートしていません。

次の表に、他のポートベース機能と互換性のあるポート セキュリティについてまとめます。

表 *124*：ポート セキュリティと他のポートベース機能との互換性

ポート タイプまたはポートの機能	ポート セキュリティとの互換性
DTP [21] ポート[22]	No
トランク ポート	Yes
ダイナミックアクセス ポート[23]	No
ルーテッド ポート	No
SPAN 送信元ポート	Yes
SPAN 宛先ポート	No
EtherChannel	Yes
トンネリング ポート	Yes
保護ポート	Yes
IEEE 802.1x ポート	Yes

ポート タイプまたはポートの機能	ポート セキュリティとの互換性
音声 VLAN ポート[24]	Yes
IP ソース ガード	Yes
ダイナミック アドレス解決プロトコル（ARP）インスペクション	Yes
Flex リンク	Yes

21 DTP = Dynamic Trunking Protocol
22 **switchport mode dynamic** インターフェイス コンフィギュレーション コマンドで設定されたポート。
23 **switchport access vlan-dynamic** インターフェイス コンフィギュレーション コマンドで設定される Vlan Query Protocol（VQP）ポート。
24 ポートに最大限可能なセキュアなアドレスを設定します（アクセス VLAN で可能なセキュアなアドレスの最大数に 2 を加えた数）。

ポートベースのトラフィック制御の概要

ポートベースのトラフィック制御は、特定トラフィック状態に応じてポートレベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。次のポートベースのトラフィック制御機能が、このガイドの記述対象の Cisco IOS リリースでサポートされます。

- ストーム制御
- 保護ポート
- ポート ブロッキング
- ポート セキュリティ
- プロトコル ストーム プロテクション

ポート セキュリティの設定方法

ポート セキュリティのイネーブル化および設定

はじめる前に

このタスクは、ポートにアクセスできるステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制約します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode** {**access** | **trunk**}
5. **switchport voice vlan***vlan-id*
6. **switchport port-security**
7. **switchport port-security [maximum***value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]
8. **switchport port-security violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}
9. **switchport port-security [mac-address***mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}]
10. **switchport port-security mac-address sticky**
11. **switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]
12. **end**
13. **show port-security**
14. **show running-config**
15. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode** {**access**	**trunk**} 例： スイッチ(config-if)# **switchport**	インターフェイス スイッチポート モードを access または trunk に設定します。デフォルト モード（dynamic auto）のインターフェイスは、セキュア ポートとして設定できません。

	コマンドまたはアクション	目的
	mode access	
ステップ 5	**switchport voice vlan***vlan-id* 例： スイッチ(config-if)# **switchport voice vlan 22**	ポート上で音声 VLAN をイネーブルにします。 vlan-id：音声トラフィックに使用する VLAN を指定します。
ステップ 6	**switchport port-security** 例： スイッチ(config-if)# **switchport port-security**	インターフェイス上でポート セキュリティをイネーブルにします。
ステップ 7	**switchport port-security [maximum***value* **[vlan** {*vlan-list* | {**access** | **voice**}}]] 例： スイッチ(config-if)# **switchport port-security maximum 20**	（任意）インターフェイスの最大セキュア MAC アドレス数を設定します。スイッチまたはスイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、アクティブなスイッチング データベース管理（SDM）テンプレートによって決まります。この値は、使用可能な MAC アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数を表します。 （任意）**vlan**：VLAN 当たりの最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-list*：トランク ポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、VLAN 単位の最大値を設定できます。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。
ステップ 8	**switchport port-security violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}	（任意）違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。

	コマンドまたはアクション	目的
	例： スイッチ(config-if)# **switchport port-security violation restrict**	• **protect**：ポート セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MACアドレスを削除するか、または許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。 （注） トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。 • **restrict**：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。 • **shutdown**：違反が発生すると、インターフェイスが error-disabled になり、ポートの LED が消灯します。SNMP トラップが送信されます。Syslogメッセージがロギングされ、違反カウンタが増加します。 • **shutdown vlan**：VLAN単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。 （注） セキュア ポートが error-disabled ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力して、このステートから回復させることができます。手動で再びイネーブルにするには、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface vlan** 特権 EXEC コマンドを入力します。
ステップ 9	**switchport port-security [mac-address***mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}]	（任意）インターフェイスのセキュアMACアドレスを入力します。このコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。 （注） このコマンドの入力後にスティッキーラーニングをイネーブルにすると、動的に学習されたセキュアアドレスがスティッキーセキュアMACアドレスに変換されて実行コンフィギュレーションに追加されます。 （任意）**vlan**：VLAN 当たりの最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。
	例： スイッチ(config-if)# **switchport port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice**	

	コマンドまたはアクション	目的
		• *vlan-id*：トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。
ステップ 10	**switchport port-security mac-address sticky** 例： `スイッチ(config-if)# switchport port-security mac-address sticky`	（任意）インターフェイス上でスティッキ ラーニングをイネーブルにします。
ステップ 11	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}] 例： `スイッチ(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice`	（任意）スティッキー セキュア MAC アドレスを入力し、必要な回数だけコマンドを繰り返します。設定したセキュア MAC アドレスの数が最大数より少ない場合、残りの MAC アドレスは動的に学習されてスティッキー セキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。 （注） このコマンドの入力前にスティッキー ラーニングをイネーブルにしないと、エラー メッセージが表示されてスティッキー セキュア MAC アドレスを入力できません。 （任意）**vlan**：VLAN 当たりの最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 13	**show port-security** 例： スイッチ# **show port-security**	入力を確認します。
ステップ 14	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 15	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ポート セキュリティ，（1682 ページ）
ポート セキュリティ，（1720 ページ）
ポート セキュリティの設定例，（1749 ページ）

ポート セキュリティ エージングのイネーブル化および設定

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュア ポート上のデバイスを削除および追加し、なおかつポート上のセキュア アドレス数を制限できます。セキュア アドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport port-security aging** {**static** | **time***time* | **type** {**absolute** | **inactivity**}}
5. **end**
6. **show port-security** [**interface***interface-id*] [**address**]
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport port-security aging** {**static** | **time***time* | **type** {**absolute** | **inactivity**}} 例： スイッチ(config-if)# **switchport port-security aging time 120**	セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにします。またはエージング タイムやタイプを設定します。 （注） スイッチは、スティッキー セキュア アドレスのポート セキュリティ エージングをサポートしていません。 このポートに、スタティックに設定されたセキュアアドレスのエージングをイネーブルにする場合は、**static** を入力します。 *time* には、このポートのエージング タイムを指定します。有効な範囲は、0 ～ 1440 分です。 **type** には、次のキーワードのいずれか 1 つを選択します。

	コマンドまたはアクション	目的
		• **absolute**：エージング タイプを絶対エージングとして設定します。このポートのセキュア アドレスはすべて、指定した時間（分単位）が経過すると期限切れになり、セキュア アドレス リストから削除されます。 • **inactivity**：エージング タイプを非アクティブ エージングとして設定します。指定された time 期間中にセキュア送信元アドレスからのデータ トラフィックがない場合に限り、このポートのセキュア アドレスが期限切れになります。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show port-security** [**interface***interface-id*] [**address**] 例： `スイッチ# show port-security interface gigabitethernet1/0/1`	入力を確認します。
ステップ 7	**show running-config** 例： `スイッチ# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ポート セキュリティ エージング，（1722 ページ）

機能情報の確認

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

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

ストーム制御に関する情報

ストーム制御

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム コントロール（またはトラフィック抑制）は、インターフェイスからスイッチング バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

トラフィック アクティビティの測定方法

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 秒単位で受信するビット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 小さいフレームのトラフィック レートの秒単位のパケット数。この機能は、グローバルにイネーブルです。小さいフレームのしきい値は、各インターフェイスで設定されます。

上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されて

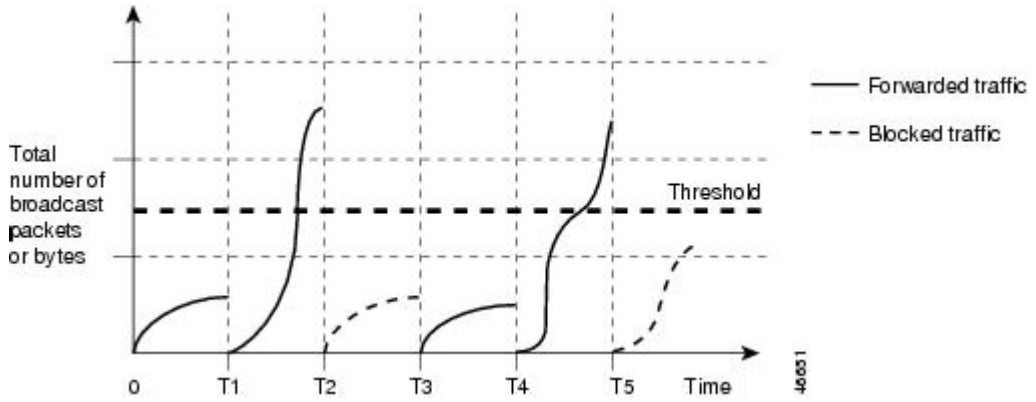
いない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

（注） マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジ プロトコル データ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

トラフィック パターン

次の例は、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。

図 *92*：ブロードキャスト ストーム制御の例



T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。したがって、T2 と T5 の後のインターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過できるパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。

（注） パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control**インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御の設定方法

ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数 % の差異が生じる可能性があります。

（注） ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、次の手順を実行します。

はじめる前に

ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps***bps* [*bps-low*] | **pps***pps* [*pps-low*]}
5. **storm-control action** {**shutdown** | **trap**}
6. **end**
7. **show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps***bps* [*bps-low*] | **pps***pps* [*pps-low*]} 例： スイッチ(config-if)# **storm-control unicast level 87 65**	ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。 キーワードの意味は次のとおりです。 • *level* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ～ 100.00 です。 • （任意）*level-low* には、下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。この値は上限抑制値より小さいか、または等しくなければなりません。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ～ 100.00 です。 しきい値に最大値（100%）を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。 • **bps***bps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをビット/秒で指定します（小

	コマンドまたはアクション	目的
		数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*bps-low* には、下限しきい値レベルをビット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ～ 10000000000.0 です。 • **pps***pps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low* には、下限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は **0.0 ～** 10000000000.0 です。 BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号（k、m、g など）を使用できます。
ステップ 5	**storm-control action** {**shutdown** | **trap**} 例： `スイッチ(config-if)# storm-control action trap`	ストーム検出時に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。 • ストーム中、ポートを error-disable の状態にするには、**shutdown** キーワードを選択します。 • ストームが検出された場合、SNMP（簡易ネットワーク管理プロトコル）トラップを生成するには、**trap** キーワードを選択します。
ステップ 6	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**] 例： `スイッチ# show storm-control gigabitethernet1/0/1 unicast`	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御の設定が表示されます。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スモール フレーム到着レートの設定

67バイト未満の着信VLANタグ付きパケットは、小さいフレームと見なされます。このパケットはスイッチにより転送されますが、スイッチ ストーム制御カウンタを増加させません。

スイッチ上の小さいフレームの着信機能をグローバルにイネーブルにして、各インターフェイスのパケットの小さいフレームのしきい値を設定します。最小サイズよりも小さく、指定されたレート（しきい値）で着信するパケットは、ポートがディセーブルにされた後はドロップされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **errdisable detect cause small-frame**
4. **errdisable recovery interval***interval*
5. **errdisable recovery cause small-frame**
6. **interface***interface-id*
7. **small-frame violation-rate***pps*
8. **end**
9. **show interfaces***interface-id*
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**errdisable detect cause small-frame** 例： スイッチ(config)# **errdisable detect cause small-frame**	スイッチ上の小さいフレームの着信レート機能をイネーブルにします。
ステップ 4	**errdisable recovery interval***interval* 例： スイッチ(config)# **errdisable recovery interval 60**	（任意）指定された errdisable ステートから回復する時間を指定します。
ステップ 5	**errdisable recovery cause small-frame** 例： スイッチ(config)# **errdisable recovery cause small-frame**	（任意）小さいフレームの着信によりポートが errdisable になった後、そのポートを自動的に再イネーブルにするリカバリ時間を設定します。 ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。
ステップ 6	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 7	**small-frame violation-rate***pps* 例： スイッチ(config-if)# **small-frame violation rate 10000**	インターフェイスが着信パケットをドロップしてポートを errdisable にするようにしきい値レートを設定します。範囲は、1 ～ 10,000 パケット/秒（pps）です。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 9	**show interfaces***interface-id* 例： スイッチ# **show interfaces gigabitethernet1/0/2**	設定を確認します。
ステップ 10	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

機能情報の確認

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

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

保護ポートに関する情報

保護ポート

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ 2 トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータ トラフィックは、レイヤ 3 デバイスを介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

スイッチ スタックは論理的には 1 つのスイッチを表しているため、レイヤ 2 トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチ スタックの保護ポート間では転送されません。

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

保護ポートのガイドライン

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

保護ポートの設定方法

保護ポートの設定

はじめる前に

保護ポートは事前定義されていません。これは設定する必要があるタスクです。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport protected**
5. **end**
6. **show interfaces***interface-id***switchport**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `スイッチ(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport protected** 例： `スイッチ(config-if)# switchport protected`	インターフェイスを保護ポートとして設定します。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show interfaces***interface-id***switchport** 例： スイッチ# **show interfaces gigabitethernet1/0/1 switchport**	入力を確認します。
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

保護ポートのモニタリング

表 *125*：保護ポートの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

次の作業

-

その他の参考資料

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

機能情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

機能情報の確認

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

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

ポート ブロッキングに関する情報

ポート ブロッキング

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャスト トラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにします。

（注） マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

ポート ブロッキングの設定方法

インターフェイスでのフラッディング トラフィックのブロッキング

はじめる前に

インターフェイスは物理インターフェイスまたはEtherChannelグループのいずれも可能です。ポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport block multicast**
5. **switchport block unicast**
6. **end**
7. **show interfaces***interface-id***switchport**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**switchport block multicast** 例： スイッチ(config-if)# **switchport block multicast**	ポートからの未知のマルチキャストの転送をブロックします。 （注） 純粋なレイヤ2マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。
ステップ 5	**switchport block unicast** 例： スイッチ(config-if)# **switchport block unicast**	ポートからの未知のユニキャストの転送をブロックします。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces***interface-id***switchport** 例： スイッチ# **show interfaces gigabitethernet1/0/1 switchport**	入力を確認します。
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ポート ブロッキングのモニタリング

表 *126* : ポート ブロッキングの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

次の作業

-

その他の参考資料

関連資料

関連項目	マニュアル タイトル

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル

MIB

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

シスコのテクニカル サポート

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

機能情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

ポート セキュリティの設定例

次に、ポート上でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する例を示します。違反モードはデフォルトです。スタティック セキュア MAC アドレスは設定せず、スティッキー ラーニングはイネーブルです。

```
スイッチ(config)# interface gigabitethernet1/0/1
```

```
スイッチ(config-if)# switchport mode access
スイッチ(config-if)# switchport port-security
スイッチ(config-if)# switchport port-security maximum 50
スイッチ(config-if)# switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 上にスタティック セキュア MAC アドレスを設定する例を示します。

```
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# switchport mode trunk
スイッチ(config-if)# switchport port-security
スイッチ(config-if)# switchport port-security mac-address 0000.0200.0004 vlan 3
```

次に、ポートのスティッキー ポート セキュリティをイネーブルにする例を示します。データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュア アドレスの総数を 20 に設定します（データ VLAN に 10、音声 VLAN に 10 を割り当てます）。

```
スイッチ(config)# interface tengigabitethernet1/0/1
スイッチ(config-if)# switchport access vlan 21
スイッチ(config-if)# switchport mode access
スイッチ(config-if)# switchport voice vlan 22
スイッチ(config-if)# switchport port-security
スイッチ(config-if)# switchport port-security maximum 20
スイッチ(config-if)# switchport port-security violation restrict
スイッチ(config-if)# switchport port-security mac-address sticky
スイッチ(config-if)# switchport port-security mac-address sticky 0000.0000.0002
スイッチ(config-if)# switchport port-security mac-address 0000.0000.0003
スイッチ(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
スイッチ(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
スイッチ(config-if)# switchport port-security maximum 10 vlan access
スイッチ(config-if)# switchport port-security maximum 10 vlan voice
```

関連トピック

ポート セキュリティ, （1720 ページ）
ポート セキュリティのイネーブル化および設定, （1725 ページ）

第 72 章

IPv6 ファーストホップセキュリティの設定

- 機能情報の確認，1751 ページ
- IPv6 でのファーストホップセキュリティの前提条件，1752 ページ
- IPv6 でのファーストホップセキュリティの制約事項，1752 ページ
- IPv6 でのファーストホップセキュリティに関する情報，1752 ページ
- SISF ベースの IPv4 および IPv6 デバイストラッキングに関する情報，1755 ページ
- SISF ベースの IP デバイストラッキングおよびスヌーピングポリシーを作成する方法，1758 ページ
- IPv6 スヌーピングポリシーの設定方法，1763 ページ
- IPv6 バインディングテーブルの内容を設定する方法，1770 ページ
- IPv6 ネイバー探索インスペクションポリシーの設定方法，1771 ページ
- IPv6 ルータアドバタイズメントガードポリシーの設定方法，1777 ページ
- IPv6 DHCP ガードポリシーの設定方法，1783 ページ
- IPv6 ソースガードの設定方法，1790 ページ
- IPv6 プレフィックスガードの設定方法，1794 ページ
- IPv6 ファーストホップセキュリティの設定例，1798 ページ
- その他の参考資料，1799 ページ

機能情報の確認

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

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

IPv6 でのファースト ホップ セキュリティの前提条件

- IPv6 がイネーブルになった必要な SDM テンプレートが設定されていること。
- IPv6 ネイバー探索機能についての知識が必要です。

IPv6 でのファースト ホップ セキュリティの制約事項

- 次の制限は、FHS ポリシーを EtherChannel インターフェイスに適用する場合に該当します（ポート チャネル）。
  - FHS ポリシーがアタッチされた物理ポートは EtherChannel グループに参加することができません。
  - FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。

IPv6 でのファースト ホップ セキュリティに関する情報

IPv6 のファーストホップ セキュリティ（FHS IPv6）は、ポリシーを物理インターフェイス、または VLAN にアタッチできる一連の IPv6 セキュリティ機能です。IPv6 ソフトウェア ポリシー データベース サービスは、これらのポリシーを保存しアクセスします。ポリシーを設定または変更すると、ポリシー属性はソフトウェア ポリシーデータベースに保存または更新され、その後指定したとおりに適用されます。次の IPv6 ポリシーが現在サポートされています。

- IPv6 スヌーピング ポリシー：IPv6 スヌーピング ポリシーは、IPv6 内の FHS で使用できるほとんどの機能をイネーブルにできるコンテナ ポリシーとして機能します。
- IPv6 FHS バインディング テーブルの内容：スイッチに接続された IPv6 ネイバーのデータベース テーブルはネイバー探索（ND）プロトコル スヌーピングなどの情報ソースから作成されます。このデータベースまたはバインディング テーブルは、リンク層アドレス（LLA）、IPv4 または IPv6 アドレス、およびスプーフィングやリダイレクト攻撃を防止するためにネイバーのプレフィックス バインディングを検証するために、さまざまな IPv6 ガード機能（IPv6 ND インスペクションなど）によって使用されます。
- IPv6 ネイバー探索インスペクション：IPv6 ND インスペクションは、レイヤ 2 ネイバー テーブル内のステートレス自動設定アドレスのバインディングを学習し、保護します。IPv6 ND 検査は、信頼できるバインディング テーブル データベースを構築するためにネイバー探索メッセージを分析します。準拠していない IPv6 ネイバー探索メッセージはドロップされま

す。ND メッセージは、その IPv6 からメディア アクセス コントロール（MAC）へのマッピングが検証可能な場合に信頼できると見なされます。
この機能によって、DAD、アドレス解決、ルータ ディスカバリ、ネイバー キャッシュに対する攻撃などの、ND メカニズムに固有の脆弱性のいくつかが軽減されます。

- IPv6 ルータ アドバタイズメント ガード：IPv6 ルータ アドバタイズメント（RA）ガード機能を使用すると、ネットワーク管理者は、ネットワーク スイッチ プラットフォームに到着した不要または不正な RA ガード メッセージをブロックまたは拒否できます。RA は、リンクで自身をアナウンスするためにルータによって使用されます。RA ガード機能は、これらの RA を分析して、未承認のルータによって送信された偽の RA をフィルタリングして除外します。ホスト モードでは、ポートではルータ アドバタイズメントとルータ リダイレクト メッセージはすべて許可されません。RA ガード機能は、レイヤ 2 デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。レイヤ 2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます。

- IPv6 DHCP ガード：IPv6 DHCP ガード機能は、承認されない DHCPv6 サーバおよびリレー エージェントからの返信およびアドバタイズメント メッセージをブロックします。IPv6 DHCP ガードは、偽造されたメッセージがバインディング テーブルに入るのを防ぎ、DHCPv6 サーバまたは DHCP リレーからデータを受信することが明示的に設定されていないポートで受信された DHCPv6 サーバ メッセージをブロックできます。この機能を使用するには、ポリシーを設定してインターフェイスまたは VLAN にアタッチします。DHCP ガード パケットをデバッグするには、**debug ipv6 snooping dhcp-guard** 特権 EXEC コマンドを使用します。

- IPv6 ソース ガード：IPv4 ソース ガードと同様、IPv6 ソース ガードは送信元アドレス スプーフィングを防ぐために、送信元アドレスまたはプレフィックスを検証します。

  ソース ガードでは、送信元または宛先アドレスに基づいてトラフィックを許可または拒否するようにハードウェアをプログラムします。ここでは、データ パケットのトラフィックのみを処理します。

  IPv6 ソース ガード機能は、ハードウェア TCAM テーブルにエントリを格納し、ホストが無効な IPv6 送信元アドレスでパケットを送信しないようにします。

  ソース ガード パケットをデバッグするには、debug ipv6 snooping source-guard 特権 EXEC コマンドを使用します。

  （注） IPv6 ソース ガード機能およびプレフィックス ガード機能は、入力方向でのみサポートされています。つまり、出力方法ではサポートされていません。

  次の制約事項が適用されます。

  - FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。
  - IPv6 ソース ガードがスイッチ ポートでイネーブルになっている場合は、そのスイッチ ポートが属するインターフェイスで NDP または DHCP スヌーピングをイネーブルにす

る必要があります。そうしないと、このポートからのすべてのデータ トラフィックがブロックされます。

- IPv6 ソース ガード ポリシーを VLAN に適用することはできません。インターフェイス レベルのみでサポートされています。
- IPv6 ソース ガードとプレフィックス ガードは同時に使用できません。ポリシーをインターフェイスに付加する際は、「アドレスを確認」するか「プレフィックスを確認」する必要はありますが、両方を確認する必要はありません。
- PVLAN と送信元/プレフィックス ガードは同時に適用できません。
- IPv6 送信元ガードとプレフィックス ガードは EtherChannel でサポートされています。

IPv6 送信元ガードの詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Source Guard」の章を参照してください。

- IPv6 プレフィックス ガード：IPv6 プレフィックス ガードは、IPv6 送信元ガード機能内で動作し、デバイスがトポロジに不正なアドレスから発信されたトラフィックを拒否できるようにします。IPv6 プレフィックス ガードは、IPv6 プレフィックスが DHCP プレフィックス委任を使用してデバイス（ホーム ゲートウェイなど）に委任される場合によく使用されています。この機能は、リンクに割り当てられたアドレスの範囲を検出し、この範囲に入っていないアドレスを発信元とするトラフィックをブロックします。

  IPv6 プレフィックス ガードの詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Prefix Guard」の章を参照してください。

- IPv6 宛先ガード：IPv6 宛先ガード機能は、IPv6 ネイバー探索で動作し、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決します。アドレス グリーニング機能に依存して、リンク上でアクティブなすべての宛先をバインディング テーブルに挿入してから、バインディング テーブルで宛先が見つからなかったときに実行される解決をブロックします。

  （注） IPv6 宛先ガードは、設定された SVI のレイヤ 2 VLAN に適用することをお勧めします。

  IPv6 宛先ガードに関する詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Destination Guard」の章を参照してください。

関連トピック

IPv6 スヌーピング ポリシーの設定方法, （1763 ページ）

IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法, （1765 ページ）

IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法, （1767 ページ）

IPv6 スヌーピング ポリシーを全体的に VLAN にアタッチする方法 , （1769 ページ）

IPv6 バインディング テーブルの内容を設定する方法 , （1770 ページ）

IPv6 ネイバー探索インスペクション ポリシーの設定方法, （1771 ページ）

IPv6 ネイバー探索インスペクション ポリシーをインターフェイスにアタッチする方法, （1773 ページ）

IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法, （1767 ページ）

IPv6 ネイバー探索インスペクション ポリシーを全体的に VLAN にアタッチする方法 , （1776 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法, （1777 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法, （1780 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法, （1781 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法, （1782 ページ）

IPv6 DHCP ガード ポリシーの設定方法 , （1783 ページ）

IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法, （1786 ページ）

IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法, （1787 ページ）

IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法 , （1789 ページ）

IPv6 ソース ガードの設定方法, （1790 ページ）

IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法, （1791 ページ）

IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法, （1793 ページ）

IPv6 プレフィックス ガードの設定方法, （1794 ページ）

IPv6 プレフィックス ガード ポリシーをインターフェイスにアタッチする方法, （1795 ページ）

IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法, （1797 ページ）

SISF ベースの IPv4 および IPv6 デバイス トラッキングに関する情報

Cisco IOS XE Denali 16.1.1 以降、新しいスイッチ統合セキュリティ機能（SISF）ベースの IP デバイス トラッキング機能は、IP に依存しない CLI コマンドを使用して、IPv4 と IPv6 の両方で FHS が使用可能なスヌーピングおよびデバイス トラッキング機能を有効にするコンテナ ポリシーとして機能します。

既存のすべての IPv6 スヌーピング コマンド（Cisco IOS XE Denali 16.1.1 以前）は、現在 IPv4 および IPv6 アドレス ファミリ両方に設定を適用できる SISF ベース デバイス トラッキング コマンドに対応します。

デバイスに既存の IP デバイス トラッキングおよび IPv6 スヌーピング設定では、新しい device-tracking upgrade-cli によって、既存の構成を Cisco IOS XE Denali 16.1.1 の新しい SISF ベース デバイス トラッキング CLI コマンドに移行することができます。詳細については、新しい SISF ベースのデバイス トラッキング CLI への移行を参照してください。

SISF ベース デバイス トラッキング CLI への移行時の制限

- デバイスにレガシー IP デバイス トラッキング（IPDT）または IPv6 スヌーピング CLI 設定がない場合、以降すべての設定に対して新しい SISF ベース デバイス トラッキング CLI コマンドのみ使用できます。古い IP デバイス トラッキング CLI および Ipv6 スヌーピング CLI は使用できません。
- 既存の IPv6 スヌーピング設定がデバイスにある場合、以降の設定にはレガシーIPv6 スヌーピング CLI を使用するか、既存の設定をすべて新しい SISF ベース デバイス トラッキング CLIに移行するために、**デバイス トラッキング アップグレード CLI** コマンドを使用できます。すべての従来の CLI が変換された後は、新しい CLI コマンドのみがデバイスで動作します。**デバイス トラッキング アップグレード CLI** コマンドを使用していなければ、レガシー IPv6 スヌーピング CLI のみがデバイスで使用できます。
- 既存の IP デバイス トラッキング設定がデバイスにあれば、レガシー IPDT コマンドまたは IPv6 スヌーピングの CLI コマンドが使用できます。このオプションは、レガシー モードがレガシーIPDT と IPv6 スヌーピング CLI のみがデバイスで使用可能に制限されます。しかし、既存の設定を新しいデバイス トラッキング コマンドに移行することを推奨します。
- すべての設定を新しい SISF ベース デバイス トラッキング CLIに移行するため、**デバイス トラッキングアップグレード CLI コマンドを実行すると、新しいデバイス トラッキング CLI の使用が許可されます。**デバイス トラッキング アップグレード CLI**コマンドを実行した後は**、新しいデバイス トラッキング CLI のみがデバイスで利用でき、レガシーIPDT または IPv6 スヌーピング コマンドはサポートされません。
- 古い IPDT IPv6 スヌーピング CLI と新しい SISF ベース デバイス トラッキング CLI の両方を設定することはできません。
- 従来の設定が新しい SISF ベース デバイス トラッキング設定に移行するとき、**ip DHCP スヌーピング VLAN** コマンドがレガシー モードで有効であれば、WL-DEV-TRACK-DHCP と呼ばれるデバイス トラッキング ポリシーが自動的に IPv4 および有効な IP デバイス トラッキングのある IPv6 クライアントの両方をトラックするため作成されます。ip DHCP スヌーピング VLAN が有効でなければ、デバイス トラッキングに左右される追加機能をサポートするため、特別にデバイス トラッキングを有効にしたことを確認してください。

新しい SISF ベースのデバイス トラッキング CLI への移行

device-tracking upgrade-cli コマンドを使用して、レガシー IP デバイス トラッキング（IPv4 用）と IPv6 スヌーピング CLI 設定を、新しいデバイス トラッキング CLI コマンドに移行しておくことをお勧めします。

設定シナリオと移行の結果

Cisco IOS XE Denali 16.1.1 より前のレガシー設定に基づいて、**device-tracking upgrade-cli** コマンドは CLI を異なる方法でアップグレードします。既存の設定を移行する前に、次のシナリオ、および対応する移行情報を検討します。

IP デバイス トラッキング設定のみがデバイスに存在

既存の IP デバイス トラッキング設定があるデバイスで **device-tracking upgrade-cli** コマンドを実行すると、内部で設定が解釈され、新しく作成されてインターフェイスで割り当てられる SISF ポリシーが使用されます。これにより、この SISF ポリシーを更新できます。

IPv6 スヌーピング設定のみがデバイスに存在

既存の IPv6 スヌーピング設定があるデバイスで、古い IPv6 スヌーピング CLI を以降の設定に使用できます。2 つのオプションが使用できます。

- （推奨）**device-tracking upgrade-cli** コマンドを使用して、既存の設定をすべて、新しい SISF ベースの device-tracking CLI に移行。レガシー CLI がすべて変換されたら、新しい CLI コマンドのみがデバイスで動作します。
- レガシー IPv6 スヌーピング CLI を今後の設定に使用し、**device-tracking upgrade-cli** コマンドは実行しない。このオプションでは、デバイスで使用可能なのはレガシー IPv6 スヌーピング CLI のみであり、新しい SISF ベースの device-tracking CLI コマンドは使用できません。

Default という名前の SISF ポリシーが、変換プロセスによって作成されます。このポリシーを他のインターフェイスに手動で割り当てることはできません。

IP デバイス トラッキングと IPv6 スヌーピング設定の両方がデバイスに存在

レガシー IP デバイス トラッキング設定と IPv6 スヌーピング設定があるデバイスでは、**device-tracking upgrade-cli** コマンドを使用して、新しい CLI に変換できます。ただし、インターフェイスに割り当てることができるスヌーピング ポリシーは 1 つだけであり、IPv6 スヌーピング ポリシー パラメータは IP デバイス トラッキング設定よりも優先される、ということに注意してください。

（注） 新しい SISF ベースの設定に移行しておらず、レガシー IPv6 スヌーピングや IPDT 構文を使用し続けている場合、IPv4 デバイス トラッキング設定情報が IPv6 スヌーピング コマンドに表示される可能性があります。統合された機能では、設定や操作に使用する構文に関係なく、IPv4 と IPv6 の両方を扱うためです。これを回避するには、レガシー設定を移行して新しい device-tracking コマンドを使用するようお勧めします。

IP デバイス トラッキングも IPv6 スヌーピング設定もデバイスに存在しない

デバイスに IP デバイス トラッキングも IPv6 スヌーピング CLI 設定もない場合、今後の設定に使用できるのは新しい SISF ベースの **device-tracking CLI** コマンドのみです。レガシー IP デバイス トラッキング コマンドと IPv6 スヌーピング コマンドは使用できません。

IPDT、IPv6 スヌーピング、およびデバイス トラッキング CLI の互換性

次の表に、IP デバイス トラッキング コマンドおよび IPv6 スヌーピング CLI コマンドの、新しい SISF ベースのデバイス トラッキング CLI および対応する CLI を表示します。

IP デバイス トラッキング（IPDT）	IPv6 スヌーピング	SISF ベースのデバイス トラッキング
ip device tracking probe count	サポート対象外	サポート対象外
ip device tracking probe delay	ipv6 neighbor binding reachable-lifetime	device-tracking policy reachable-lifetime
ip device tracking probe interval	ipv6 snooping tracking retry-interval	device-tracking policy retry-interval
ip device tracking probe use-svi	**ip device tracking probe auto-source override** として受け付け/解釈	**ip device tracking probe auto-source override** として受け付け/解釈
ip device tracking probe auto-source fallback	サポート対象外	サポート対象外
ip device tracking probe auto-source override	サポート対象外	サポート対象外
ip device tracking tracebuffer	サポート対象外	サポート対象外
ip device tracking maximum	ipv6 snooping policy <name> limit	device-tracking snooping policy <name> limit
ip device tracking probe count	サポート対象外	サポート対象外
ip device tracking probe interval	サポート対象外	サポート対象外
clear ip device tracking all	サポート対象外	サポート対象外

SISF ベースの IP デバイス トラッキングおよびスヌーピング ポリシーを作成する方法

デバイス トラッキング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **device-tracking policy***policy-name*
3. {[**device-role** {**node**| **switch**}] | [**limit address-count***value*] | [**no**] | [**destination-glean**{**recovery**|**log-only**[**dhcp**]] | [**data-glean**{**recovery**|**log-only**{**dhcp** | **ndp**}] | **prefix-glean**] | [**security-level** {**glean**| **guard**| **inspect**}] | [**tracking** {**disable**[**stale-lifetime**[*seconds* | **infinite**] | **enable**[**reachable-lifetime**[*seconds* | **infinite**] }] | [**trusted-port**] }
4. **end**
5. **show device-tracking policy** *policy-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ2	**device-tracking policy***policy-name* 例： スイッチ(config)# **device-tracking policy example_policy**	デバイス トラッキング コンフィギュレーション モードを開始します。
ステップ3	{[**device-role** {**node**| **switch**}]	[**limit address-count***value*]	[**no**]	[**destination-glean**{**recovery**|**log-only**[**dhcp**]]	[**data-glean**{**recovery**|**log-only**{**dhcp**	**ndp**}]	**prefix-glean**]	[**security-level** {**glean**| **guard**| **inspect**}]	[**tracking** {**disable**[**stale-lifetime**[*seconds*	**infinite**]	**enable**[**reachable-lifetime**[*seconds*	**infinite**] }]	[**trusted-port**] } 例： スイッチ(config-device-tracking)# security-level inspect 例： スイッチ(config-device-tracking)# trusted-port	IPv4 と IPv6 の両方で次のオプションを有効にします。 • （任意）**device-role**{**node**]	**switch**}：ポートに接続されたデバイスのロールを指定します。デフォルトは **node** です。 • （任意）**limit address-count***value*：ターゲットごとに許可されるアドレス数を制限します。 • （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。 • （任意）**destination-glean**{**recovery**| **log-only**}[**dhcp**]}：データ トラフィックの送信元アドレス グリーニングによるバインディング テーブルの回復をイネーブルにします。 • （任意）**data-glean**{**recovery**| **log-only**}[**dhcp**	**ndp**]}：送信元アドレスまたはデータ アドレスのグリーニングを使用したバインディング テーブルの回復をイネーブルにします。 • （任意）**security-level**{**glean**|**guard**|**inspect**}：この機能によって適用されるセキュリティのレベルを指定します。デフォルトは **guard** です。

	コマンドまたはアクション	目的
		glean：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。 **guard**：アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバ メッセージを拒否します。これがデフォルトのオプションです。 **inspect**：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。 • （任意）**tracking** {**disable** | **enable**}：トラッキング オプションを指定します。 • （任意）**trusted-port**：信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。
ステップ 4	**end** 例： スイッチ(config-device-tracking)# **exit**	設定モードを終了します。
ステップ 5	**show device-tracking policy** *policy-name* 例： スイッチ#**show device-tracking policy example_policy**	デバイス トラッキング ポリシー設定を表示します。

デバイス トラッキング ポリシーをインターフェイスにアタッチする方法

デバイス トラッキング ポリシーをインターフェイスにアタッチするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface***interface*
3. **device-trackingattach-policy***policy_name*
4. **show device-tracking policies** [**interface***interface*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface* 例： スイッチ(config)# **interface gigabitethernet 1/1/4**	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**device-trackingattach-policy***policy_name* 例： スイッチ(config-if)# **device-tracking attach-policy example_policy**	デバイス トラッキング ポリシーをインターフェイスまたはそのインターフェイス上で指定されたVLANにアタッチします。
ステップ 4	**show device-tracking policies** [**interface***interface*] 例： スイッチ#(config-if)# **do show running-config**	指定されたインターフェイスの種類と番号に一致するポリシーを表示します。

デバイス トラッキング ポリシーを VLAN にアタッチする方法

複数のインターフェイスでデバイス トラッキング ポリシーを VLAN にアタッチするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **vlan configuration***vlan_list*
3. **device-tracking** [**attach-policy***policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration***vlan_list* 例： スイッチ(config)# **vlan configuration 333**	デバイス トラッキング ポリシーをアタッチする VLAN を指定し、そのVLANインターフェイスのコンフィギュレーション モードを開始します。
ステップ 3	**device-tracking** [**attach-policy***policy_name*] 例： スイッチ (config-vlan-config)#**device-tracking attach-policy example_policy**	すべてのスイッチインターフェイスで、デバイストラッキングポリシーを指定されたVLANにアタッチします。
ステップ 4	**do show running-config** 例： スイッチ#(config-if)# **do show running-config**	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

デバイス全体のエントリをバインディング テーブルに追加する方法

バインディング テーブルの内容を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. [**no**] **device-trackingDefault**| [**down-lifetime***value*] | [**logging**] | [**max entries***value*] | [**reachable-lifetime***seconds* | **retry-interval***seconds*] | [**stale-lifetime**[*seconds*]
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **device-trackingDefault**| [**down-lifetime***value*] | [**logging**] | [**max entries***value*] | [**reachable-lifetime***seconds* | **retry-interval***seconds*] | [**stale-lifetime**[*seconds*] 例： スイッチ(config)# **device-tracking Default**	デバイス全体のデフォルト デバイス トラッキング ポリシーを作成し、エントリを次のオプションと共にバインディング テーブルに追加します。 • down-lifetime：エントリが削除される前に DOWN 状態で保持されるデフォルトの最長時間を設定します。 • logging：バインディング テーブル イベントを記録する syslog ロギングを有効にします。 • max-entries：バインディング テーブル内の最大エントリ数を定義します。 • reachable-lifetime：到達可能なエントリが到達可能性の証拠なしに直接的または間接的に到達可能であると見なされる最長時間を定義します。 • retry-interval：2 つのプローブの間隔を定義します。 • stale-lifetime：エントリが削除される前に Slate 状態で保持される最長時間を定義します。
ステップ 3	**exit** 例： スイッチ(config)# **exit**	グローバル コンフィギュレーション モードを終了して、ルータを特権 EXEC モードにします。

IPv6 スヌーピング ポリシーの設定方法

IPv6 スヌーピング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **ipv6 snooping policy***policy-name*
3. {[**default**] | [**device-role** {**node**| **switch**}] | [**limit address-count***value*] | [**no**] | [**protocol**{**dhcp** | **ndp**}] | [**security-level** {**glean**| **guard**| **inspect**}] | [**tracking** {**disable**[**stale-lifetime**[*seconds* | **infinite**] | **enable**[**reachable-lifetime**[*seconds* | **infinite**] }] | [**trusted-port**] }
4. **end**
5. **show ipv6 snooping policy** *policy-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 snooping policy***policy-name* 例： スイッチ(config)# **ipv6 snooping policy example_policy**	スヌーピング ポリシーを作成し、IPv6 スヌーピング ポリシー コンフィギュレーション モードに移行します。
ステップ 3	{[**default**]	[**device-role** {**node**| **switch**}]	[**limit address-count***value*]	[**no**]	[**protocol**{**dhcp**	**ndp**}]	[**security-level** {**glean**| **guard**| **inspect**}]	[**tracking** {**disable**[**stale-lifetime**[*seconds*	**infinite**]	**enable**[**reachable-lifetime**[*seconds*	**infinite**] }]	[**trusted-port**] } 例： スイッチ(config-ipv6-snooping)# security-level inspect 例： スイッチ(config-ipv6-snooping)# trusted-port	データ アドレス グリーニングをイネーブルにし、さまざまな条件に対してメッセージを検証し、メッセージのセキュリティ レベルを指定します。 • （任意）**default**：すべてをデフォルト オプションに設定します。 • （任意）**device-role**{**node**]	**switch**}：ポートに接続されたデバイスのロールを指定します。デフォルトは **node** です。 • （任意）**limit address-count***value*：ターゲットごとに許可されるアドレス数を制限します。 • （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。 • （任意）**protocol**{**dhcp**	**ndp**}：分析のために、スヌーピング機能にどのプロトコルをリダイレクトするかを指定します。デフォルトは、**dhcp** および **ndp** です。デフォルトを変更するには、**no protocol** コマンドを使用します。 • （任意）**security-level**{**glean**|**guard**|**inspect**}：この機能によって適用されるセキュリティのレベルを指定します。デフォルトは **guard** です。

	コマンドまたはアクション	目的
		glean：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。 **guard**：アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバ メッセージを拒否します。これがデフォルトのオプションです。 **inspect**：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。 • （任意）**tracking** {**disable** | **enable**}：デフォルトのトラッキング動作を上書きし、トラッキング オプションを指定します。 • （任意）**trusted-port**：信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。
ステップ 4	**end** 例： スイッチ(config-ipv6-snooping)# **exit**	コンフィギュレーション モードから特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 snooping policy** *policy-name* 例： スイッチ#**show ipv6 snooping policy example_policy**	スヌーピング ポリシー設定を表示します。

次の作業

IPv6 スヌーピング ポリシーをインターフェイスまたは VLAN にアタッチします。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法

インターフェイスまたは VLAN に IPv6 ルータスヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **switchport**
4. **ipv6 snooping** [**attach-policy** *policy_name* [**vlan** {*vlan_id* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids*}] | **vlan** {*vlan_id* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
5. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： スイッチ(config)# **interface gigabitethernet 1/1/4**	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport** 例： スイッチ(config-if)# **switchport**	switchport モードを開始します。 （注） インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに switchport インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。switchport コンフィギュレーション モードではコマンド プロンプトは（config-if）# と表示されます。
ステップ 4	**ipv6 snooping** [**attach-policy** *policy_name* [**vlan** {*vlan_id*	**add** *vlan_ids*	**except***vlan_ids*	**none**	**remove** *vlan_ids*}]	**vlan** {*vlan_id*	**add** *vlan_ids*	**except***vlan_ids*	**none**	**remove** *vlan_ids*	**all**}]	インターフェイスまたはそのインターフェイス上の特定の VLAN にカスタム IPv6 スヌーピング ポリシーをアタッチします。デフォルト ポリシーをインターフェイスにアタッチするには、**attach-policy** キーワードを指定せずに **ipv6 snooping** コマンドを使用します。デフォルト ポリシーをインターフェイス上の VLAN にアタッチするには、**ipv6 snooping vlan** コマンドを使用します。

	コマンドまたはアクション	目的
	例： スイッチ(config-if)# **ipv6 snooping** or スイッチ(config-if)# **ipv6 snooping attach-policy example_policy** or スイッチ(config-if)# **ipv6 snooping vlan 111,112** or スイッチ(config-if)# **ipv6 snooping attach-policy example_policy vlan 111,112**	デフォルト ポリシーは、セキュリティ レベル **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。
ステップ 5	**do show running-config** 例： スイッチ#(config-if)# **do show running-config**	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range***Interface_name*
3. **ipv6snooping** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
4. **do show running-configinterface***portchannel_interface_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range***Interface_name* 例： スイッチ(config)# **interface Po11**	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。
ステップ 3	**ipv6snooping** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}] 例： スイッチ(config-if-range)# **ipv6 snooping attach-policy example_policy** or スイッチ(config-if-range)# **ipv6 snooping attach-policy example_policy vlan 222,223,224** **or** スイッチ(config-if-range)#**ipv6 snooping vlan 222, 223,224**	IPv6 スヌーピング ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： スイッチ#(config-if-range)# **do show running-config int po11**	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 スヌーピング ポリシーを全体的に VLAN にアタッチする方法

複数のインターフェイス上の VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 snooping** [**attach-policy** *policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： `スイッチ(config)# vlan configuration 333`	VLANインターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6 snooping** [**attach-policy** *policy_name*] 例： `スイッチ(config-vlan-config)#ipv6 snooping attach-policy example_policy`	すべてのスイッチおよびスタック インターフェイスで、IPv6 スヌーピング ポリシーを指定したVLANにアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。デフォルト ポリシーは、セキュリティ レベル **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。
ステップ 4	**do show running-config** 例： `スイッチ#(config-if)# do show running-config`	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のVLANにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 バインディング テーブルの内容を設定する方法

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. [**no**] **ipv6 neighbor binding** [**vlan***vlan-id*{*ipv6-address***interface** interface_type *stack/module/porthw_address* [**reachable-lifetimevalue**[*seconds* | **default** | **infinite**] | [**tracking**{ [default | disable] [**reachable-lifetimevalue**[*seconds* | **default** | **infinite**] | [**enable** [**reachable-lifetimevalue**[*seconds* | **default** | **infinite**] | [**retry-interval** {*seconds*| **default** [**reachable-lifetimevalue**[*seconds* | **default** | **infinite**] }]
3. [**no**] **ipv6 neighbor binding max-entries***number* [**mac-limit***number* | **port-limit***number* [**mac-limit***number*] | **vlan-limit***number* [[**mac-limit***number*] | [**port-limit***number* [**mac-limit***number*]]]]
4. **ipv6 neighbor bindinglogging**
5. **exit**
6. **show ipv6 neighbor binding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ipv6 neighbor binding** [**vlan***vlan-id*{*ipv6-address***interface** interface_type *stack/module/porthw_address* [**reachable-lifetimevalue**[*seconds*	**default**	**infinite**]	[**tracking**{ [default	disable] [**reachable-lifetimevalue**[*seconds*	**default**	**infinite**]	[**enable** [**reachable-lifetimevalue**[*seconds*	**default**	**infinite**]	[**retry-interval** {*seconds*| **default** [**reachable-lifetimevalue**[*seconds*	**default**	**infinite**] }] 例： スイッチ(config)# **ipv6 neighbor binding**	バインディング テーブル データベースにスタティック エントリを追加します。
ステップ 3	[**no**] **ipv6 neighbor binding max-entries***number* [**mac-limit***number*	**port-limit***number* [**mac-limit***number*]	**vlan-limit***number* [[**mac-limit***number*]	[**port-limit***number* [**mac-limit***number*]]]] 例： スイッチ(config)# **ipv6 neighbor binding max-entries 30000**	バインディング テーブル キャッシュに挿入できるエントリの最大数を指定します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 neighbor bindinglogging** 例： スイッチ(config)# **ipv6 neighbor binding logging**	バインディング テーブル メイン イベントのロギングをイネーブルにします。
ステップ 5	**exit** 例： スイッチ(config)# **exit**	グローバル コンフィギュレーション モードを終了して、ルータを特権 EXEC モードにします。
ステップ 6	**show ipv6 neighbor binding** 例： スイッチ# **show ipv6 neighbor binding**	バインディング テーブルの内容を表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 ネイバー探索インスペクション ポリシーの設定方法

特権 EXEC モードから、IPv6 ND インスペクション ポリシーを設定するには、次の手順に従ってください。

手順の概要

1. **configure terminal**
2. **[no]ipv6 nd inspectionpolicy***policy-name*
3. **device-role** {**host** | **monitor** | **router** | **switch**}
4. **drop-unsecure**
5. **limit address-count***value*
6. **sec-level minimum***value*
7. **tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}
8. **trusted-port**
9. **validate source-mac**
10. **no** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**}
11. **default** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**}
12. **do show ipv6 nd inspection policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**]**ipv6 nd inspectionpolicy***policy-name* 例： スイッチ(config)# **ipv6 nd inspection policy example_policy**	ND インスペクション ポリシー名を指定し、ND インスペクション ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**device-role** {**host** | **monitor** | **router** | **switch**} 例： スイッチ(config-nd-inspection)# **device-role switch**	ポートに接続されているデバイスのロールを指定します。デフォルトは **host** です。
ステップ 4	**drop-unsecure** 例： スイッチ(config-nd-inspection)# **drop-unsecure**	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
ステップ 5	**limit address-count***value* 例： スイッチ(config-nd-inspection)# **limit address-count 1000**	1 ～ 10,000 を入力します。
ステップ 6	**sec-level minimum***value* 例： スイッチ(config-nd-inspection)# **limit address-count 1000**	暗号化生成アドレス（CGA）オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
ステップ 7	**tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]} 例： スイッチ(config-nd-inspection)# **tracking disable stale-lifetime infinite**	ポートでデフォルトのトラッキング ポリシーを上書きします。
ステップ 8	**trusted-port** 例： スイッチ(config-nd-inspection)# **trusted-port**	信頼できるポートにするポートを設定します。

	コマンドまたはアクション	目的
ステップ 9	**validate source-mac** 例： スイッチ(config-nd-inspection)# **validate source-mac**	送信元 Media Access Control（MAC）アドレスをリンク層アドレスと照合します。
ステップ 10	**no** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**} 例： スイッチ(config-nd-inspection)# **no validate source-mac**	このコマンドの **no** 形式を使用してパラメータの現在の設定を削除します。
ステップ 11	**default** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**} 例： スイッチ(config-nd-inspection)# **default limit address-count**	設定をデフォルト値に戻します。
ステップ 12	**do show ipv6 nd inspection policy***policy_name* 例： スイッチ(config-nd-inspection)# **do show ipv6 nd inspection policy example_policy**	ND インスペクション コンフィギュレーション モードを終了しないで ND インスペクションの設定を確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 ネイバー探索インスペクション ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェース上の VLAN に IPv6 ND 検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： スイッチ(config)# **interface gigabitethernet 1/1/4**	インターフェイスのタイプおよびIDを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] 例： スイッチ(config-if)# **ipv6 nd inspection attach-policy example_policy** or スイッチ(config-if)# **ipv6 nd inspection attach-policy example_policy vlan 222,223,224** **or** スイッチ(config-if)# **ipv6 nd inspection vlan 222, 223,224**	ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルトポリシーがアタッチされます。
ステップ 4	**do show running-config** 例： スイッチ#(config-if)# **do show running-config**	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 ネイバー探索インスペクション ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ネイバー探索検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range***Interface_name*
3. **ipv6ndinspection** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_id*s | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
4. **do show running-configinterface***portchannel_interface_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range***Interface_name* 例： スイッチ(config)# **interface Po11**	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。
ステップ 3	**ipv6ndinspection** [**attach-policy***policy_name* [**vlan** {*vlan_ids*	**add** *vlan_ids*	**except** *vlan_ids*	**none**	**remove***vlan_ids*	**all**}]	**vlan** [{*vlan_id*s	**add** *vlan_ids*	**except***vlan_ids*	**none**	**remove***vlan_ids*	**all**}] 例： スイッチ(config-if-range)# **ipv6 nd inspection attach-policy example_policy** or スイッチ(config-if-range)# **ipv6 nd inspection attach-policy example_policy vlan 222,223,224** **or** スイッチ(config-if-range)#**ipv6 nd inspection vlan 222, 223,224**	NDインスペクションポリシーをインターフェイスまたはそのインターフェイス上の特定のVLANにアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

	コマンドまたはアクション	目的
ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： スイッチ#(config-if-range)# **do show running-config int po11**	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 ネイバー探索インスペクション ポリシーを全体的に VLAN にアタッチする方法

複数のインターフェイス上の VLAN に IPv6 ND 探索ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 nd inspection** [**attach-policy** *policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： スイッチ(config)# **vlan configuration 334**	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6 nd inspection** [**attach-policy** *policy_name*] 例： スイッチ(config-vlan-config)#**ipv6 nd inspection attach-policy example_policy**	すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 デフォルトのポリシーは、device-role **host**、no drop-unsecure、limit address-count disabled、sec-level minimum is disabled、tracking is disabled、no trusted-port、no validate source-mac です。

	コマンドまたはアクション	目的
ステップ 4	**do show running-config** 例： スイッチ#(config-if)# **do show running-config**	コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法

IPv6 ルータ アドバタイズメント ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. [**no**]**ipv6 nd raguardpolicy***policy-name*
3. [**no**]**device-role** {**host** | **monitor** | **router** | **switch**}
4. [**no**]**hop-limit** {**maximum** | **minimum**} *value*
5. [**no**]**managed-config-flag** {**off** | **on**}
6. [**no**]**match** {**ipv6 access-list***list* | **ra prefix-list***list*}
7. [**no**]**other-config-flag** {**on** | **off**}
8. [**no**]**router-preference maximum** {**high** | **medium** | **low**}
9. [**no**]**trusted-port**
10. **default** {**device-role** | **hop-limit** {**maximum** | **minimum**} | **managed-config-flag** | **match** {**ipv6 access-list** | **ra prefix-list** } | **other-config-flag** | **router-preference maximum**| **trusted-port**}
11. **do show ipv6 nd raguard policy***policy_name*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	[**no**]**ipv6 nd raguardpolicy***policy-name* 例： スイッチ(config)# **ipv6 nd raguard policy example_policy**	RA ガード ポリシー名を指定し、RA ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 3	[**no**]**device-role** {**host** | **monitor** | **router** | **switch**} 例： スイッチ(config-nd-raguard)# **device-role switch**	ポートに接続されているデバイスのロールを指定します。デフォルトは **host** です。
ステップ 4	[**no**]**hop-limit** {**maximum** | **minimum**} *value* 例： スイッチ(config-nd-raguard)# **hop-limit maximum 33**	（1 ～ 255）最大および最小のホップ制限値の範囲。 ホップ制限値によるルータアドバタイズメントメッセージのフィルタリングをイネーブルにします。不正 RA メッセージは低いホップ制限値（IPv4 の Time to Live と同じ）を持つ可能性があるため、ホストによって受け入れられると、ホストが不正 RA メッセージジェネレータを超えて宛先にトラフィックを生成することができなくなります。指定されていないホップ制限値を持つ RA メッセージはブロックされます。 設定されていない場合、このフィルタはディセーブルになります。「**minimum**」を設定して、指定する値より低いホップ制限値を持つRA メッセージをブロックします。「**maximum**」を設定して、指定する値より高いホップ制限値を持つ RA メッセージをブロックします。
ステップ 5	[**no**]**managed-config-flag** {**off** | **on**} 例： スイッチ(config-nd-raguard)# **managed-config-flag on**	管理アドレス設定（「M」フラグ）フィールドに基づいてルータアドバタイズメントメッセージのフィルタリングをイネーブルにします。「M」フィールドが 1 の不正 RA メッセージの結果としてホストが不正DHCPv6サーバを使用する場合があります。設定されていない場合、このフィルタはディセーブルになります。 **On**：「M」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。 **Off**：「M」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。
ステップ 6	[**no**]**match** {**ipv6 access-list***list* | **ra prefix-list***list*} 例： スイッチ(config-nd-raguard)# **match ipv6 access-list example_list**	指定したプレフィックス リストまたはアクセス リストと照合します。

	コマンドまたはアクション	目的
ステップ 7	[**no**]**other-config-flag** {**on** | **off**} 例： スイッチ(config-nd-raguard)# **other-config-flag on**	その他の設定（「O」フラグ）フィールドに基づくルータ アドバタイズメント メッセージのフィルタリングをイネーブルにします。「O」フィールドが 1 の不正 RA メッセージの結果としてホストが不正DHCPv6サーバを使用する場合があります。設定されていない場合、このフィルタはディセーブルになります。 **On**：「O」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。 **Off**：「O」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。
ステップ 8	[**no**]**router-preference maximum** {**high** | **medium** | **low**} 例： スイッチ(config-nd-raguard)# **router-preference maximum high**	「Router Preference」フラグを使用したルータ アドバタイズメント メッセージのフィルタリングをイネーブルにします。設定されていない場合、このフィルタはディセーブルになります。 • **high**：「Router Preference」が「high」、「medium」、または「low」に設定された RA メッセージを受け入れます。 • **medium**：「Router Preference」が「high」に設定された RA メッセージをブロックします。 • **low**：「Router Preference」が「medium」または「high」に設定された RA メッセージをブロックします。
ステップ 9	[**no**]**trusted-port** 例： スイッチ(config-nd-raguard)# **trusted-port**	信頼できるポートとして設定すると、すべての接続デバイスが信頼され、より詳細なメッセージ検証は実行されません。
ステップ 10	**default** {**device-role** | **hop-limit** {**maximum** | **minimum**} | **managed-config-flag** | **match** {**ipv6 access-list** | **ra prefix-list** } | **other-config-flag** | **router-preference maximum**| **trusted-port**} 例： スイッチ(config-nd-raguard)# **default hop-limit**	コマンドをデフォルト値に戻します。
ステップ 11	**do show ipv6 nd raguard policy***policy_name* 例： スイッチ(config-nd-raguard)# **do show ipv6 nd raguard policy example_policy**	（任意）：RA ガード ポリシー コンフィギュレーション モードを終了しないで ND ガード ポリシー設定を表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェース上の VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 nd raguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `スイッチ(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよびIDを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd raguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids*	**add** *vlan_ids*	**except** *vlan_ids*	**none**	**remove** *vlan_ids*	**all**}]	**vlan** [{*vlan_ids*	**add** *vlan_ids*	**except***vlan_ids*	**none**	**remove** *vlan_ids*	**all**}] 例： `スイッチ(config-if)# ipv6 nd raguard attach-policy example_policy` or `スイッチ(config-if)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`	ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

	コマンドまたはアクション	目的
	or スイッチ(config-if)# **ipv6 nd raguard vlan 222, 223,224**	
ステップ 4	**do show running-config** 例： スイッチ#(config-if)# **do show running-config**	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ルータ アドバタイズメント ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range***Interface_name*
3. **ipv6ndraguard** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
4. **do show running-configinterface***portchannel_interface_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range***Interface_name* 例： スイッチ(config)# **interface Po11**	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
		ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。
ステップ 3	**ipv6ndraguard** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}] 例： スイッチ(config-if-range)# **ipv6 nd raguard attach-policy example_policy** or スイッチ(config-if-range)# **ipv6 nd raguard attach-policy example_policy vlan 222,223,224** **or** スイッチ(config-if-range)#**ipv6 nd raguard vlan 222, 223,224**	RA ガードポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： スイッチ#(config-if-range)# **do show running-config int po11**	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法

インターフェイスに関係なく VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **vlan configuration***vlan_list*
3. **ipv6dhcp guard** [**attach-policy***policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration***vlan_list* 例： スイッチ(config)# **vlan configuration 335**	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 RA ガード ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6dhcp guard** [**attach-policy***policy_name*] 例： スイッチ(config-vlan-config)#**ipv6 nd raguard attach-policy example_policy**	すべてのスイッチおよびスタック インターフェイスで、IPv6 RA ガード ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	**do show running-config** 例： スイッチ#(config-if)# **do show running-config**	コンフィギュレーションモードを終了しないで、ポリシーが特定のVLANにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 DHCP ガード ポリシーの設定方法

IPv6 DHCP（DHCPv6）ガード ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. [**no**]**ipv6 dhcp guardpolicy***policy-name*
3. [**no**]**device-role** {**client** | **server**}
4. [**no**] **matchserveraccess-list***ipv6-access-list-name*
5. [**no**] **matchreplyprefix-list***ipv6-prefix-list-name*
6. [**no**]**preference**{ **max***limit* | **min***limit* }
7. [**no**] **trusted-port**
8. **default** {**device-role** | **trusted-port**}
9. **do show ipv6 dhcp guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**]**ipv6 dhcp guardpolicy***policy-name* 例： スイッチ(config)# **ipv6 dhcp guard policy example_policy**	DHCPv6 ガードポリシー名を指定し、DHCPv6 ガードポリシー コンフィギュレーション モードを開始します。
ステップ 3	[**no**]**device-role** {**client**	**server**} 例： スイッチ(config-dhcp-guard)# **device-role server**	（任意）特定のロールのデバイスからのものではないポート上の DHCPv6 応答および DHCPv6 アドバタイズメントをフィルタします。デフォルトは **client** です。 • **client**：デフォルト値。アタッチされたデバイスがクライアントであることを指定します。サーバ メッセージにはこのポートでドロップされます。 • **server**：適用されたデバイスが DHCPv6 サーバであることを指定します。このポートでは、サーバ メッセージが許可されます。
ステップ 4	[**no**] **matchserveraccess-list***ipv6-access-list-name* 例： ;;Assume a preconfigured IPv6 Access List as follows: スイッチ(config)# **ipv6 access-list my_acls** スイッチ(config-ipv6-acl)# **permit host**	（任意）。アドバタイズされた DHCPv6 サーバまたはリレー アドレスが認証されたサーバのアクセスリストからのものであることの確認をイネーブルにします（アクセス リストの宛先アドレスは「any」です）。設定されていない場合、このチェックは回避されます。空のアクセス リストは、permit all として処理されます。

	コマンドまたはアクション	目的
	FE80::A8BB:CCFF:FE01:F700 any ;;configure DCHPv6 Guard to match approved access list. スイッチ(config-dhcp-guard)# **match server access-list my_acls**	
ステップ 5	[**no**] **matchreplyprefix-list***ipv6-prefix-list-name* 例： ;;Assume a preconfigured IPv6 prefix list as follows: スイッチ(config)# **ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128** ;; Configure DCHPv6 Guard to match prefix スイッチ(config-dhcp-guard)# **match reply prefix-list my_prefix**	（任意）DHCPv6応答メッセージ内のアドバタイズされたプレフィクスが設定された承認プレフィクス リストからのものであることの確認をイネーブルにします。設定されていない場合、このチェックは回避されます。空のプレフィクス リストは、permit として処理されます。
ステップ 6	[**no**]**preference**{ **max***limit* | **min***limit* } 例： スイッチ(config-dhcp-guard)# **preference max 250** スイッチ(config-dhcp-guard)#**preference min 150**	**device-role** が **server** である場合に **max** および **min** を設定して、DHCPv6 サーバアドバタイズメント値をサーバ優先度値に基づいてフィルタします。デフォルトではすべてのアドバタイズメントが許可されます。 **max***limit*：（0 ～ 255）（任意）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限未満であるかどうかの検証をイネーブルにします。デフォルトは 255 です。設定されていない場合、このチェックは回避されます。 **min***limit*：（0 ～ 255）（任意）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限を超過しているかどうかの検証をイネーブルにします。デフォルトは 0 です。設定されていない場合、このチェックは回避されます。
ステップ 7	[**no**] **trusted-port** 例： スイッチ(config-dhcp-guard)# **trusted-port**	（任意）**trusted-port**：ポートを信頼モードに設定します。このポートでは、これ以上のポリシングは実行されません。 （注） 信頼できるポートを設定した場合、device-role オプションは使用できません。
ステップ 8	**default** {**device-role** | **trusted-port**} 例： スイッチ(config-dhcp-guard)# **default device-role**	（任意）**default**：コマンドをデフォルトに設定します。
ステップ 9	**do show ipv6 dhcp guard policy***policy_name* 例： スイッチ(config-dhcp-guard)# **do show ipv6 dhcp guard policy example_policy**	（任意）コンフィギュレーション サブモードを終了せずに IPv6 DHCP のガード ポリシーの設定を表示します。*policy_name* 変数を省略すると、すべての DHCPv6 ポリシーが表示されます。

DHCPv6 ガード設定の例

```
enable
configure terminal
ipv6 access-list acl1
 permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy pol1
 device-role server
 match server access-list acl1
 match reply prefix-list abc
 preference min 0
 preference max 255
 trusted-port
interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy pol1 vlan add 1
 vlan 1
  ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
4. **do show running-config interface** Interface_type *stack/module/port*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** Interface_type *stack/module/port* 例： `スイッチ(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**ipv6 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	
	例：
	`スイッチ(config-if)# ipv6 dhcp guard attach-policy example_policy`
	
	or
	
	`スイッチ(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	
	or
	
	`スイッチ(config-if)# ipv6 dhcp guard vlan 222, 223,224`
		DHCP ガードポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-config interface** Interface_type *stack/module/port* 例： `スイッチ#(config-if)# do show running-config gig 1/1/4`	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 DHCP ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range***Interface_name*
3. **ipv6dhcpguard** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_id*s | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
4. **do show running-configinterface***portchannel_interface_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range***Interface_name* 例： スイッチ(config)# **interface Po11**	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。
ステップ 3	**ipv6dhcpguard** [**attach-policy***policy_name* [**vlan** {*vlan_ids*	**add** *vlan_ids*	**except** *vlan_ids*	**none**	**remove***vlan_ids*	**all**}]	**vlan** [{*vlan_id*s	**add** *vlan_ids*	**except***vlan_ids*	**none**	**remove***vlan_ids*	**all**}] 例： スイッチ(config-if-range)# **ipv6 dhcp guard attach-policy example_policy** or スイッチ(config-if-range)# **ipv6 dhcp guard attach-policy example_policy vlan 222,223,224** **or** スイッチ(config-if-range)#**ipv6 dhcp guard vlan 222, 223,224**	DHCP ガードポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

	コマンドまたはアクション	目的
ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： スイッチ#(config-if-range)# **do show running-config int po11**	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法

複数のインターフェイス上の VLAN に IPv6 DHCP のガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 dhcp guard** [**attach-policy** *policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： スイッチ(config)# **vlan configuration 334**	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6 dhcp guard** [**attach-policy** *policy_name*] 例： スイッチ(config-vlan-config)#**ipv6 dhcp guard attach-policy example_policy**	すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。デフォルト ポリシーは、device-role **client**、**no** trusted-port です。

	コマンドまたはアクション	目的
ステップ 4	**do show running-config** 例： スイッチ#(config-if)# **do show running-config**	コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 ソース ガードの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. [**no**] **ipv6 source-guard policy***policy_name*
4. [**deny global-autoconf**] [**permit link-local**] [**default**{...}] [**exit**] [**no**{...}]
5. **end**
6. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**] **ipv6 source-guard policy***policy_name* 例： スイッチ(config)# **ipv6 source-guard policy example_policy**	IPv6 ソース ガード ポリシー名を指定し、IPv6 ソース ガード ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**[deny global-autoconf] [permit link-local] [default**{...}**] [exit] [no**{...}**]** 例： スイッチ(config-sisf-sourceguard)# **deny global-autoconf**	（任意）IPv6 ソース ガード ポリシーを定義します。 • **deny global-autoconf**：自動設定されたグローバル アドレスからのデータ トラフィックを拒否します。これは、リンク上のすべてのグローバル アドレスが DHCP によって割り当てられているときに、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。 • **permit link-local**：リンクローカル アドレスから送信されたすべてのデータ トラフィックを許可します。 （注） ソース ガード ポリシーに基づく信頼できるオプションはサポートされません。
ステップ 5	**end** 例： スイッチ(config-sisf-sourceguard)# **end**	IPv6 ソース ガード ポリシー コンフィギュレーション モードを終了します。
ステップ 6	**show ipv6 source-guard policy***policy_name* 例： スイッチ# **show ipv6 source-guard policy example_policy**	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

次の作業

インターフェイスに IPv6 ソース ガード ポリシーを適用します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** Interface_type *stack/module/port*
4. **ipv6 source-guard**[**attach-policy**<*policy_name*>]
5. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** Interface_type *stack/module/port* 例： スイッチ(config)# **interface gigabitethernet 1/1/4**	インターフェイスのタイプおよびIDを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 source-guard**[**attach-policy**<*policy_name*>] 例： スイッチ(config-if)# **ipv6 source-guard attach-policy example_policy**	インターフェイスにIPv6 ソース ガード ポリシーをアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy***policy_name* 例： スイッチ#(config-if)# **show ipv6 source-guard policy example_policy**	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel***port-channel-number*
4. **ipv6 source-guard**[**attach-policy**<*policy_name*>]
5. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel***port-channel-number* 例： `スイッチ (config)# interface Po4`	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。
ステップ 4	**ipv6 source-guard**[**attach-policy**<*policy_name*>] 例： `スイッチ(config-if) # ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy***policy_name* 例： `スイッチ(config-if) #show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法，（1798 ページ）

IPv6 プレフィックス ガードの設定方法

（注） プレフィックス ガードが適用されている場合にリンクローカル アドレスから送信されたルーティング プロトコル制御パケットを許可するには、ソースガード ポリシー コンフィギュレーション モードで permit link-local コマンドをイネーブルにします。

手順の概要

1. **enable**
2. **configureterminal**
3. **[no]ipv6 source-guard policy***source-guard-policy*
4. **[no]validate address**
5. **validate prefix**
6. **exit**
7. **show ipv6 source-guard policy**[*source-guard-policy*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**[no]ipv6 source-guard policy***source-guard-policy* 例： スイッチ (config)# **ipv6 source-guard policy my_snooping_policy**	IPv6 ソースガード ポリシー名を定義して、スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**[no]validate address** 例： スイッチ（config-sisf-sourceguard）# **no validate address**	アドレス検証機能をディセーブルにし、IPv6プレフィックス ガード機能を設定できるようにします。
ステップ 5	**validate prefix** 例： スイッチ（config-sisf-sourceguard）# **validate prefix**	IPv6 ソース ガードをイネーブルにし、IPv6プレフィックスガード動作を実行します。
ステップ 6	**exit** 例： スイッチ（config-sisf-sourceguard）# **exit**	スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 source-guard policy**[*source-guard-policy*] 例： スイッチ # **show ipv6 source-guard policy policy1**	IPv6 ソースガード ポリシー設定を表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 プレフィックス ガード ポリシーをインターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** Interface_type *stack/module/port*
4. **ipv6 source-guard attach-policy***policy_name*
5. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** Interface_type *stack/module/port* 例： スイッチ(config)# **interface gigabitethernet 1/1/4**	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 source-guard attach-policy***policy_name* 例： スイッチ(config-if)# **ipv6 source-guard attach-policy example_policy**	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy***policy_name* 例： スイッチ(config-if)# **show ipv6 source-guard policy example_policy**	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel***port-channel-number*
4. **ipv6 source-guard**[**attach-policy**<*policy_name*>]
5. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel***port-channel-number* 例： `スイッチ (config)# interface Po4`	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。
ステップ 4	**ipv6 source-guard**[**attach-policy**<*policy_name*>] 例： `スイッチ(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy***policy_name* 例： `スイッチ(config-if)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

関連トピック

IPv6 でのファースト ホップ セキュリティに関する情報, （1752 ページ）

例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法, （1798 ページ）

IPv6 ファースト ホップ セキュリティの設定例

例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

次の例は、IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch(config-sisf-sourceguard) # validate address
switch(config-sisf-sourceguard)# exit
Switch(config)# interface Po4
Switch(config)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
Switch(config-if)# exit
switch(config)#
```

関連トピック

IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法, （1793 ページ）

例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

次の例は、IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch (config-sisf-sourceguard)# no validate address
Switch((config-sisf-sourceguard)# validate prefix
Switch(config)# interface Po4
Switch(config-if)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
```

関連トピック

IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法, （1797 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
『Implementing IPv6 Addressing and Basic Connectivity』	http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-0sy/ip6-addrg-bsc-con.html
IPv6 ネットワーク管理とセキュリティのトピック	『IPv6 Configuration Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』 http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/xe-3se/3850/ipv6-xe-3se-3850-library.html
IPv6 コマンド リファレンス	『IPv6 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』 http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-xe-3se-3850-cr-book.html

エラー メッセージ デコーダ

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

シスコのテクニカル サポート

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

第 73 章

Cisco TrustSec の設定

- Cisco TrustSec の概要，1801 ページ
- 機能情報の確認，1801 ページ
- Cisco TrustSec の機能，1802 ページ
- Cisco TrustSec の機能情報，1805 ページ

Cisco TrustSec の概要

Cisco TrustSec は、ネットワーク内のユーザ、ホスト、およびネットワーク デバイスを強力に識別する機能に基づいた、シスコ ネットワーク デバイスのセキュリティを改善します。TrustSec は、特定のロールについてデータ トラフィックを一意に分類することで、トポロジに依存しない、スケーラブルなアクセス コントロールを実現します。TrustSec は、認証されたピアおよびこれらのピアとの暗号化リンク間で信頼を確立することで、データの機密保持および整合性を保証します。

Cisco TrustSec の主要コンポーネントは、Cisco Identity Services Engine（ISE）です。スイッチ上で手動で設定することもできますが、Cisco ISE は TrustSec ID およびセキュリティ グループ ACL（SGACL）でスイッチをプロビジョニングできます。

機能情報の確認

スイッチ上で Cisco TrustSec を設定するには、次の URL にある『Cisco TrustSec Switch Configuration Guide』を参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec.html

Cisco TrustSec General Availability リリースのリリース ノートについては、次の URL を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

概要、データ シート、プラットフォーム マトリクスごとの機能、およびケース スタディを含む Cisco TrustSec ソリューションの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/netsol/ns1051/index.html

Cisco TrustSec の機能

次の表に、TrustSec がイネーブルになった Cisco スイッチで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability リリースによって、サポートされるスイッチの数および各スイッチでサポートされる TrustSec 機能の数は増加しています。

Cisco TrustSec の機能	説明
802.1AE タギング（MACSec）	IEEE 802.1AE に基づくワイヤレート ホップ単位レイヤ 2 暗号化のプロトコル。 MACSec 対応デバイス間において、パケットは送信デバイスからの出力で暗号化され、受信デバイスへの入力で復号化されます。デバイス内では平文です。 この機能は、TrustSec ハードウェア対応デバイス間だけで利用できます。 （注） この機能は、Cisco IOS XE Denali 16.1.1の Catalyst 3850 および Catalyst 3650 スイッチではサポートされていません。 （注） この機能は 2960x ではサポートされていません。
エンドポイント アドミッション コントロール（EAC）	EAC は、TrustSec ドメインに接続しているエンドポイントユーザまたはデバイスの認証プロセスです。通常、EAC はアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可に成功すると、ユーザまたはデバイスに対してセキュリティ グループ タグが割り当てられます。現在、EAC は 802.1X、MAC 認証バイパス（MAB）、および Web 認証プロキシ（WebAuth）とすることができます。

Cisco TrustSec の機能	説明
ネットワーク デバイス アドミッション コントロール（NDAC）	NDAC は、TrustSec ドメイン内の各ネットワーク デバイスがピア デバイスのクレデンシャルおよび信頼性を確認できる認証プロセスです。NDAC は、IEEE 802.1X ポート ベースの認証に基づく認証フレームワークを利用し、EAP 方式として EAP-FAST を使用します。NDAC プロセスの認証および許可に成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションとなります。 （注） この機能は 2960x ではサポートされません。
セキュリティ グループ アクセス コントロール リスト（SGACL）	セキュリティ グループ アクセス コントロール リスト（SGACL）は、セキュリティ グループ タグをポリシーと関連付けます。ポリシーは、TrustSec ドメインから出力される SGT タグ付きトラフィックに対して適用されます。
セキュリティ アソシエーション プロトコル（SAP）	NDAC 認証のあと、セキュリティ アソシエーションプロトコル（SAP）は、その後の TrustSec ピア間の MACSec リンク暗号化のキーおよび暗号スイートについて、自動的にネゴシエーションを行います。SAP は IEEE 802.11i で定義されます。 （注） この機能は、Cisco IOS XE Denali 16.1.1の Catalyst 3850 および Catalyst 3650 スイッチではサポートされていません。 （注） この機能は 2960x ではサポートされていません。
セキュリティ グループ タグ（SGT）	SGT は、TrustSec ドメイン内の送信元のセキュリティ分類を示す 16 ビットの単一ラベルです。イーサネット フレームまたは IP パケットに追加されます。

Cisco TrustSec の機能	説明
SGT Exchange Protocol（SXP）（）	Security Group Tag Exchange Protocol（SXP）。SXP を使用すると、TrustSec にハードウェアで対応していないデバイスが Cisco Identity Services Engine（ISE）または Cisco Secure アクセス コントロール システム（ACS）から認証されたユーザとデバイスの SGT 属性を受信できます。デバイスは、次にセキュリティ グループ アクセス コントロール リスト（SGACL）強制のために、送信元トラフィックをタグ付けする TrustSec にハードウェアで対応しているデバイスに、sourceIP-to-SGT バインディングを転送できます。

リンクの両端で 802.1AE MACsec をサポートしている場合、SAP ネゴシエーションが実行されます。サプリカントとオーセンティケータの間で EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティ パラメータの交換、およびキーの管理が実行されます。これらの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョンとライセンスおよびリンク ハードウェア サポートに応じて、SAP ネゴシエーションは次の動作モードの 1 つを使用できます。

- Galois Counter Mode（GCM）：認証と暗号化
- GCM authentication（GMAC）：GCM 認証、暗号化なし
- No Encapsulation：カプセル化なし（クリア テキスト）
- null：カプセル化、認証または暗号化なし

Cisco TrustSec の機能情報

表 *127* : *Cisco TrustSec* の機能情報

機能名	リリース	機能情報
• NDAC • SXPv1、SXPv2 • SGT • SGACL レイヤ 2 の適用 • SGT および VLAN から SGT へのマッピングのインターフェイス • サブネットと SGT のマッピング • レイヤ 3 ポート マッピング（PM） • レイヤ 3 アイデンティティ ポート マッピング（IPM） • セキュリティグループ名のダウンロード • SXP ループ検出 • ポリシーベースの CoA	Cisco IOS XE 3.3SE	これらの機能は、Catalyst 3850 および 3650 スイッチ、Cisco 5700 シリーズ Wireless LAN コントローラで追加されました。
SXPv1 および SXPv2	Cisco IOS XE 15.0(2)EX	SXP は Catalyst 2960-X スイッチで追加されています。
SXPv1 および SXPv2	Cisco IOS XE 15.0(2)EX1	SXP は Catalyst 2960-XR スイッチで追加されています。

第 74 章

ワイヤレス ゲスト アクセスの設定

- 機能情報の確認，1807 ページ
- ゲスト アクセスの前提条件，1807 ページ
- ゲスト アクセスの制約事項，1808 ページ
- ワイヤレス ゲスト アクセスについて，1808 ページ
- 高速安全ローミング，1808 ページ
- ゲスト アクセスを設定する方法，1809 ページ
- ゲスト アクセスの設定例，1827 ページ
- ゲスト アクセスに関する追加情報，1833 ページ
- ゲスト アクセスの機能履歴と情報，1834 ページ

機能情報の確認

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

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

ゲスト アクセスの前提条件

- すべてのモビリティ ピアは、階層モビリティ アーキテクチャに対して設定されている必要があります。

- WLAN 上のゲスト コントローラ モビリティ アンカーの設定は、モビリティ エージェントおよびゲスト コントローラ上である必要があります。
- ゲスト アクセスは、3 ボックス ソリューションまたは 2 ボックス ソリューションが可能です。モビリティ トンネルのリンク ステータスは、以下の間で適用される必要があります。
  - モビリティ エージェント、モビリティ コントローラおよびゲスト コントローラ。

  または
  - モビリティ エージェント/モビリティ コントローラおよびゲスト コントローラ。

ゲスト アクセスの制約事項

ゲスト コントローラの機能は、Catalyst 3850 スイッチでサポートされていませんが、Catalyst 3850 はモビリティ エージェントとして機能できます。

ワイヤレス ゲスト アクセスについて

理想としては、ワイヤレス ゲスト ネットワークの実装で、企業の既存のワイヤレスおよび有線インフラストラクチャを最大限活用して、物理オーバーレイ ネットワークを構築する際のコストや複雑さを回避します。この場合は、次の要素と機能の追加が必要になります。

- 専用のゲスト WLAN/SSID：ゲスト アクセスを必要とするあらゆる場所で、キャンパス ワイヤレス ネットワークを介して実装されます。ゲスト WLAN は、モビリティ アンカー（ゲスト コントローラ）が設定された WLAN で識別されます。
- ゲスト トラフィックのセグメンテーション：ゲストの移動場所を制限するために、キャンパス ネットワーク上のレイヤ 2 またはレイヤ 3 での実装テクニックを必要とします。
- アクセス コントロール：キャンパス ネットワーク内に組み込まれたアクセス コントロール機能の使用、または企業ネットワークからインターネットへのゲスト アクセスを制御する外部プラットフォームの実装を伴います。
- ゲスト ユーザ資格情報の管理：スポンサーまたは Lobby 管理者がゲストの代わりに仮の資格情報を作成できるプロセス。この機能は、アクセス コントロール プラットフォーム内に常駐している場合と、AAA などの管理システムのコンポーネントになっている場合とがあります。

高速安全ローミング

高速セキュア ローミングは、Cisco Centralized Key Management（CCKM）、および 802.11i クライアントの Pairwise Master Key（PMK）情報をキャッシュすることで実現できます。Cisco Centralized

Key Management（CCKM）はローミングの向上に役立ちます。クライアントのみがローミング プロセスを開始できますが、以下のような要因に影響されます。

- AP 間のオーバーラップ
- AP 間の距離
- チャネル、シグナル強度、および AP 上のロード
- データ レートと出力電力

高速ローミング クライアント（802.11i、[CCKM]）が新しいデバイスにローミングする場合は常に、クライアントは高速ローミング後にモビリティ「ハンドオフ」手順を実行します。また、モビリティ「ハンドオフ」手順後に学習した AAA 属性が再適用されます。

クライアントが 802.11i WPA2、CCKM、を使用している場合、高速セキュア ローミングの要件をすべて満たすために、ローミング中の完全な L2 認証を避ける必要があります。完全な L2 認証を避けるため、認証およびローミング クライアントのキーの継承に PMK キャッシュ（802.11i、CCKM、）が使用されます。これには、モビリティ グループ内のモビリティ アンカー（MA）およびモビリティ コントローラ（MC）が同じ PMK キャッシュ値を持つことが必要です。

セッションタイムアウトは、PMK キャッシュの有効期限を定義します。クライアントが再認証に失敗した場合、または CLI から手動で削除された場合、PMK キャッシュも削除される場合があります。オリジナルのコントローラまたはスイッチの削除は、同じモビリティ グループ内の他のコントローラまたはスイッチにも影響します。

ゲスト アクセスを設定する方法

ロビー管理者アカウントの作成

手順の概要

1. **configure terminal**
2. **user-name** *user-name*
3. **type lobby-admin**
4. **password 0** *password*
5. **end**
6. **show running-config | section** *user-name* (or) **show running-config | section** *configured lobby admin username*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ # **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**user-name** *user-name* 例： スイッチ (config)# **user-name** lobby	ユーザ アカウントを作成します。
ステップ 3	**type lobby-admin** 例： スイッチ (config-user-name)# **type lobby-admin**	ロビー管理者としてアカウント タイプを指定します。
ステップ 4	**password 0** *password* 例： スイッチ(config-user-name)# **password 0** lobby	ロビー管理者アカウントのパスワードを作成します。
ステップ 5	**end** 例： スイッチ (config-user-name)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config | section** *user-name* (or) **show running-config | section** *configured lobby admin username* 例： スイッチ # **show running-config | section** lobby	設定の詳細を表示します。

ゲスト ユーザ アカウントの設定

手順の概要

1. **configure terminal**
2. **user-name** *user-name*
3. **password** *unencrypted/hidden-password password*
4. **type network-user description** *description* **guest-user lifetime year** *0-1* **month** *0-11* **day** *0-30* **hour** *0-23* **minute** *0-59* **second** *0-59*
5. **end**
6. **show aaa local netuser all**
7. **show running-config | section***user-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**user-name** *user-name* 例： `スイッチ (config)# user-name guest`	Lobby Ambassador アカウントのユーザ名を作成します。
ステップ 3	**password** *unencrypted/hidden-password password* 例： `スイッチ (config-user-name)# password 0 guest`	ユーザのパスワードを指定します。
ステップ 4	**type network-user description** *description* **guest-user lifetime year** *0-1* **month** *0-11* **day** *0-30* **hour** *0-23* **minute** *0-59* **second** *0-59* 例： `スイッチ (config-user-name)# type network-user description guest guest-user lifetime year 1 month 10 day 3 hour 1 minute 5 second 30`	ユーザのタイプを指定します。
ステップ 5	**end** 例： `スイッチ (config-user-name)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show aaa local netuser all** 例： スイッチ # **show aaa local netuser all**	設定の詳細を表示します。有効期間後に、ゲスト タイプとユーザ名は削除され、ゲスト ユーザ名と関連付けられるクライアントは認証解除されます。
ステップ 7	**show running-config | section***user-name* 例： スイッチ # **show running-config | section** guest	設定の詳細を表示します。

モビリティ エージェント（MA）の設定

手順の概要

1. **configure terminal**
2. **wireless mobility controller ip***mc-ipaddress* **public-ip** *mc-publicipaddress*
3. **wlan** *wlan-name wlan-id ssid*
4. **client vlan id***vlan-group name/vlan-id*
5. **no security wpa**
6. **mobility anchor** *ipaddress*
7. **aaa-override**
8. **no shutdown**
9. **end**
10. **show wireless mobility summary**
11. **show wlan name** *wlan-name/id*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**wireless mobility controller ip***mc-ipaddress* **public-ip** *mc-publicipaddress* 例： スイッチ（config）# **wireless mobility controller ip**27.0.0.1 **public-ip** 27.0.0.1	MA が関連付けられるモビリティ コントローラを設定します。
ステップ 3	**wlan** *wlan-name wlan-id ssid* 例： スイッチ（config）# **wlan** mywlan 34 mywlan-ssid	• *wlan-name* には、プロファイル名を入力します。範囲は 1 ～ 32 文字です。 • *wlan-id* には WLAN ID を入力します。範囲は 1 ～ 512 です。 • *ssid* では、この WLAN に対する Service Set Identifier（SSID）を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。
ステップ 4	**client vlan id***vlan-group name/vlan-id* 例： スイッチ（config-wlan）# **client vlan VLAN0136**	WLAN の VLAN ID またはグループを設定します。
ステップ 5	**no security wpa** 例： スイッチ（config-wlan）# **no security wpa**	セキュリティ設定は GC で作成された WLAN で同じである必要があります。この例はオープン認証を対象としています。オープンおよび webauth などの他のセキュリティ タイプに対して、適切なコマンドを提供する必要があります。
ステップ 6	**mobility anchor** *ipaddress* 例： スイッチ（config-wlan）# **mobility anchor** 9.3.32.2	ゲスト コントローラをモビリティ アンカーとして設定します。
ステップ 7	**aaa-override** 例： スイッチ（config-wlan）# **aaa-override**	（任意）AAA オーバーライドをイネーブルにします。AAA オーバーライドは、AAA 属性を優先する必要が生じたときのために、非オープン認証で要求されます。ゲスト ユーザを有効期限が切れた後に認証解除する必要があるか、AAA オーバーライド属性をユーザに与える必要がある場合にのみ必要です。
ステップ 8	**no shutdown** 例： スイッチ(config-wlan) # **no shutdown**	WLAN をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： スイッチ (config) # **end**	特権 EXEC モードに戻ります。
ステップ 10	**show wireless mobility summary** 例： スイッチ # **show wireless mobility summary**	モビリティ コントローラの IP アドレス、およびモビリティ トンネルのステータスを確認します。
ステップ 11	**show wlan name** *wlan-name/id* 例： スイッチ # **show wlan name** mywlan	モビリティ アンカーの設定を表示します。

モビリティ コントローラの設定

モビリティ コントローラ モードは **wireless mobility controller** コマンドを使用してイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **wireless mobility group member ip***ip-address***public-ip***ip-address***group***group-name*
3. **wireless mobility controller peer-group***peer-group-name*
4. **wireless mobility controller peer-group***peer-group-name***member ip***ipaddress***public-ip***ipaddress*
5. **end**
6. **show wireless mobility summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ # **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless mobility group member ip***ip-address***public-ip***ip-address***group***group-name* 例： スイッチ (config) # **wireless mobility group member ip** 27.0.0.1 **public-ip** 23.0.0.1 **group** test	MC グループ内のすべてのピアを追加します。*ip-address* は、ゲスト コントローラの IP アドレスである必要があります。

	コマンドまたはアクション	目的
ステップ 3	**wireless mobility controller peer-group***peer-group-name* 例： スイッチ (config) # **wireless mobility controller peer-group** pg	スイッチのピア グループを作成します。
ステップ 4	**wireless mobility controller peer-group***peer-group-name***member ip***ipaddress***public-ip***ipaddress* 例： スイッチ (config) # **wireless mobility controller peer-group** pg **member ip** 9.7.136.10 **public-ip** 9.7.136.10	スイッチのピア グループにMAを追加します。
ステップ 5	**end** 例： スイッチ (config) # **end**	特権 EXEC モードに戻ります。
ステップ 6	**show wireless mobility summary** 例： スイッチ # **show wireless mobility summary**	設定の詳細を表示します。

Web 認証証明書の入手

手順の概要

1. **configure terminal**
2. **crypto pki import** *trustpoint name* **pkcs12 tftp:** *passphrase*
3. **end**
4. **show crypto pki** *trustpoints cert*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**crypto pki import** *trustpoint name* **pkcs12 tftp:** *passphrase* 例： スイッチ（config）# **crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco**	証明書をインポートします。
ステップ 3	**end** 例： スイッチ（config）# **end**	特権 EXEC モードに戻ります。
ステップ 4	**show crypto pki** *trustpoints cert* 例： スイッチ # **show crypto pki trustpoints cert**	設定の詳細を表示します。

Web 認証証明書の表示

手順の概要

1. **show crypto ca certificate verb**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show crypto ca certificate verb** 例： スイッチ # **show crypto ca certificate verb**	現在の Web 認証証明書の詳細を表示します。

デフォルトの Web 認証ログイン ページの選択

AAA オーバーライド フラグは、ローカルまたはリモート AAA サーバを使用した Web 認証のために、WLAN でイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **parameter-map type webauth***parameter-map name*
3. **wlan***wlan-name*
4. **shutdown**
5. **security web-auth**
6. **security web-auth authentication-list** *authentication list name*
7. **security web-auth parameter-map***parameter-map name*
8. **no shutdown**
9. **end**
10. **show running-config | section***wlan-name*
11. **show running-config | section parameter-map type webauth***parameter-map*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map type webauth***parameter-map name* 例： `スイッチ (config) # parameter-map type webauth test`	web-auth パラメータ マップを設定します。
ステップ 3	**wlan***wlan-name* 例： `スイッチ (config) # wlan wlan10`	wlan-name に、プロファイル名を入力します。範囲は 1 ～ 32 文字です。
ステップ 4	**shutdown** 例： `スイッチ (config) # shutdown`	WLAN をディセーブルにします。
ステップ 5	**security web-auth** 例： `Controller (config-wlan) # security web-auth`	WLAN の Web 認証をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**security web-auth authentication-list** *authentication list name* 例： `Controller (config-wlan) # security web-auth authentication-list test`	認証リスト名と Web 認証 WLAN のマップを可能にします。
ステップ 7	**security web-auth parameter-map***parameter-map name* 例： `スイッチ (config) # security web-auth parameter-map test`	パラメータ マップ名と Web 認証 WLAN のマップを可能にします。
ステップ 8	**no shutdown** 例： `スイッチ (config) # no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `スイッチ (config) # end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config | section***wlan-name* 例： `スイッチ# show running-config | section mywlan`	設定の詳細を表示します。
ステップ 11	**show running-config | section parameter-map type webauth***parameter-map* 例： `スイッチ# show running-config | section parameter-map type webauth test`	設定の詳細を表示します。

外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択

AAA オーバーライド フラグは、ローカルまたはリモート AAA サーバを使用した Web 認証のために、WLAN でイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **parameter-map type webauth global**
3. **virtual-ip {ipv4 | ipv6}***ip-address*
4. **parameter-map type webauth***parameter-map name*
5. **type {authbypass | consent | webauth | webconsent}**
6. **redirect [for-login|on-success|on-failure]***URL*
7. **redirect portal {ipv4 | ipv6}***ip-address*
8. **end**
9. show running-config | section parameter-map

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map type webauth global** 例： `スイッチ (config) # parameter-map type webauth global`	グローバル webauth タイプ パラメータを設定します。
ステップ 3	**virtual-ip {ipv4 | ipv6}***ip-address* 例： `スイッチ (config-params-parameter-map) # virtual-ip ipv4 1.1.1.1`	仮想 IP アドレスを設定します。
ステップ 4	**parameter-map type webauth***parameter-map name* 例： `スイッチ (config-params-parameter-map) # parameter-map type webauth test`	webauth タイプ パラメータを設定します。
ステップ 5	**type {authbypass | consent | webauth | webconsent}** 例： `スイッチ (config-params-parameter-map) # type webauth`	consent、passthru、webauth、または webconsent など WebAuth のサブタイプを設定します。
ステップ 6	**redirect [for-login|on-success|on-failure]***URL* 例： `スイッチ (config-params-parameter-map) # redirect for-login http://9.1.0.100/login.html`	ログイン ページ、成功ページおよび失敗ページのリダイレクト URL を設定します。

	コマンドまたはアクション	目的
ステップ 7	**redirect portal {ipv4 | ipv6}***ip-address* 例： スイッチ (config-params-parameter-map) # **redirect portal ipv4** 23.0.0.1	外部ポータルの IPv4 アドレスを設定します。
ステップ 8	**end** 例： スイッチ (config-params-parameter-map) # **end**	特権 EXEC モードに戻ります。
ステップ 9	show running-config | section parameter-map 例： スイッチ # **show running-config | section parameter-map**	設定の詳細を表示します。

WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て

手順の概要

1. **configure terminal**
2. **parameter-map type webauth** *parameter-map-name*
3. **custom-page login device** *html-filename*
4. **custom-page login expired** *html-filename*
5. **custom-page failure device** *html-filename*
6. **custom-page success device** *html-filename*
7. **end**
8. **show running-config | section parameter-map type webauth** *parameter-map*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**parameter-map type webauth** *parameter-map-name* 例： `スイッチ (config) # parameter-map type webauth test`	webauth タイプ パラメータを設定します。
ステップ 3	**custom-page login device** *html-filename* 例： `スイッチ (config-params-parameter-map)# custom-page login device device flash:login.html`	Web 認証カスタマイズ ログイン ページに対するファイル名を指定できます。
ステップ 4	**custom-page login expired** *html-filename* 例： `スイッチ (config-params-parameter-map)# custom-page login expired device flash:loginexpired.html`	Web認証カスタマイズログイン期限切れページのファイル名を指定することを可能にします。
ステップ 5	**custom-page failure device** *html-filename* 例： `スイッチ (config-params-parameter-map)# custom-page failure device device flash:loginfail.html`	Web 認証カスタマイズ ログイン失敗ページに対するファイル名を指定できます。
ステップ 6	**custom-page success device** *html-filename* 例： `スイッチ (config-params-parameter-map)# custom-page success device device flash:loginsuccess.html`	Web 認証カスタマイズ ログイン成功ページに対するファイル名を指定できます。
ステップ 7	**end** 例： `スイッチ (config-params-parameter-map)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config | section parameter-map type webauth** *parameter-map* 例： `スイッチ (config) # show running-config | section parameter-map type webauth test`	設定の詳細を表示します。

AAA-Override の設定

手順の概要

1. **configure terminal**
2. **wlan***wlan-name*
3. **aaa-override**
4. **end**
5. **show running-config | section***wlan-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ # **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan***wlan-name* 例： スイッチ (config) # **wlan** ramban	*wlan-name* にはプロファイル名を入力します。範囲は 1 ～ 32 文字です。
ステップ 3	**aaa-override** 例： スイッチ (config-wlan) # **aaa-override**	WLAN の AAA オーバーライドをイネーブルにします。
ステップ 4	**end** 例： スイッチ (config-wlan) # **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config	section***wlan-name* 例： スイッチ # **show running-config	section** ramban	設定の詳細を表示します。

クライアントの負荷分散の設定

手順の概要

1. **configure terminal**
2. **wlan** *wlan-name*
3. **shutdown**
4. **mobility anchor** *ip-address1*
5. **mobility anchor** *ip-address2*
6. **no shutdown wlan**
7. **end**
8. **show running-config | section** *wlan-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan-name* 例： `スイッチ (config)# wlan ramban`	*wlan-name* にはプロファイル名を入力します。
ステップ 3	**shutdown** 例： `スイッチ (config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 4	**mobility anchor** *ip-address1* 例： `スイッチ (config-wlan) # mobility anchor 9.7.136.15`	ゲスト コントローラをモビリティ アンカーとして設定します。
ステップ 5	**mobility anchor** *ip-address2* 例： `スイッチ (config-wlan) # mobility anchor 9.7.136.16`	ゲスト コントローラをモビリティ アンカーとして設定します。
ステップ 6	**no shutdown wlan** 例： `スイッチ (config-wlan) # no shutdown wlan`	WLAN をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： スイッチ (config-wlan) # **end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config | section** *wlan-name* 例： スイッチ # **show running-config | section** ramban	設定の詳細を表示します。

事前認証 ACL の設定

手順の概要

1. **configure terminal**
2. **wlan** *wlan-name*
3. **shutdown**
4. **ip access-group web** *preauthrule*
5. **no shutdown**
6. **end**
7. **show wlan name** *wlan-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan-name* 例： スイッチ (config)# **wlan** ramban	*wlan-name* にはプロファイル名を入力します。
ステップ 3	**shutdown** 例： スイッチ (config-wlan)# **shutdown**	WLAN をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**ip access-group web** *preauthrule* 例： スイッチ (config-wlan)# **ip access-group web** preauthrule	認証前に適用する必要のある ACL を設定します。
ステップ 5	**no shutdown** 例： スイッチ (config)# **no shutdown**	WLAN をイネーブルにします。
ステップ 6	**end** 例： スイッチ (config-wlan)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show wlan name** *wlan-name* 例： スイッチ# **show wlan name** ramban	設定の詳細を表示します。

IOS ACL 定義の設定

手順の概要

1. **configure terminal**
2. **ip access-list extended** *access-list number*
3. **permit udp any eq** *port number* **any**
4. **end**
5. **show access-lists** *ACL number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ # **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip access-list extended** *access-list number* 例： スイッチ (config) # **ip access-list extended** 102	拡張 IP アクセス リストを設定します。

	コマンドまたはアクション	目的
ステップ 3	**permit udp any eq** *port number* **any** 例： スイッチ (config-ext-nacl) # **permit udp any eq** 8080 **any**	宛先ホストを設定します。
ステップ 4	**end** 例： スイッチ (config-wlan) # **end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** *ACL number* 例： スイッチ # **show access-lists** 102	設定の詳細を表示します。

Webpassthrough の設定

手順の概要

1. **configure terminal**
2. **parameter-map type webauth** *parameter-map name*
3. **type consent**
4. **end**
5. **show running-config | section parameter-map type webauth** *parameter-map*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ # **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map type webauth** *parameter-map name* 例： スイッチ (config) # **parameter-map type webauth** webparalocal	webauth タイプ パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 3	**type consent** 例： スイッチ (config-params-parameter-map) # **type consent**	WebAuth タイプを同意として設定します。
ステップ 4	**end** 例： スイッチ (config-params-parameter-map) # **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config | section parameter-map type webauth** *parameter-map* 例： スイッチ (config) # **show running-config | section parameter-map type webauth** test	設定の詳細を表示します。

ゲスト アクセスの設定例

例：Lobby Ambassador アカウントの作成

次の例は、Lobby Ambassador アカウントを設定する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# user-name lobby
スイッチ(config)# type lobby-admin
スイッチ(config)# password 0 lobby
スイッチ(config)# end
スイッチ#  show running-config | section lobby
    user-name lobby
    creation-time 1351118727
    password 0 lobby
    type lobby-admin
```

例：Web 認証証明書の入手

次の例は、Web 認証証明書を取得する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco
スイッチ(config)# end
スイッチ# show crypto pki trustpoints cert
 Trustpoint cert:
    Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
```

```
    st=California
    c=US
          Serial Number (hex): 00
    Certificate configured.
スイッチ# show  crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    Name: ldapserver
    e=rkannajr@cisco.com
    cn=ldapserver
    ou=WNBU
    o=Cisco
    st=California
    c=US
  Validity Date:
    start date: 07:35:23 UTC Jan 31 2012
    end   date: 07:35:23 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12
  Storage: nvram:rkannajrcisc#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Validity Date:
    start date: 07:27:56 UTC Jan 31 2012
    end   date: 07:27:56 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12 ldap
  Storage: nvram:rkannajrcisc#0CA.cer
```

例：Web 認証証明書の表示

次の例は、Web 認証証明書を表示する方法を示しています。

```
スイッチ# show crypto ca certificate verb
     Certificate
     Status: Available
     Version: 3
     Certificate Serial Number (hex): 2A9636AC00000000858B
     Certificate Usage: General Purpose
     Issuer:
```

```
cn=Cisco Manufacturing CA
o=Cisco Systems
Subject:
Name: WS-C3780-6DS-S-2037064C0E80
Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
cn=WS-C3780-6DS-S-2037064C0E80
serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca.crl
Validity Date:
start date: 15:43:22 UTC Aug 21 2011
end   date: 15:53:22 UTC Aug 21 2021
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
X509v3 extensions:
X509v3 Key Usage: F0000000
  Digital Signature
  Non Repudiation
  Key Encipherment
  Data Encipherment
X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
Authority Info Access:
Associated Trustpoints: CISCO_IDEVID_SUDI
Key Label: CISCO_IDEVID_SUDI
```

例：ゲスト ユーザ アカウントの設定

次の例は、ゲスト ユーザ アカウントを設定する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# user-name guest
スイッチ(config-user-name)# password 0 guest
スイッチ(config-user-name)# type network-user description guest guest-user lifetime year 1
month 10 day 3 hour 1 minute 5 second 30
スイッチ(config-user-name)# end
スイッチ# show aaa local netuser all
User-Name           : guest
Type                : guest
Password            : guest
Is_passwd_encrypted : No
Descriptio          : guest
Attribute-List      : Not-Configured
First-Login-Time    : Not-Logged-In
Num-Login           : 0
Lifetime            : 1 years 10 months 3 days 1 hours 5 mins 30 secs
Start-Time          : 20:47:37 chennai Dec 21 2012
```

例：モビリティ コントローラの設定

次の例は、モビリティ コントローラを設定する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test
スイッチ(config)# wireless mobility controller peer-group pg
スイッチ(config)# wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip
 9.7.136.10
スイッチ(config)# end
スイッチ# show wireless mobility summary
```

```
Mobility Controller Summary:

Mobility Role                                  : Mobility Controller
Mobility Protocol Port                         : 16666
Mobility Group Name                            : default
Mobility Oracle                                : Enabled
DTLS Mode                                      : Enabled

Mobility Keepalive Interval                    : 10
Mobility Keepalive Count                       : 3
Mobility Control Message DSCP Value            : 7
Mobility Domain Member Count                   : 3

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

IP              Public IP        Group Name       Multicast IP     Link Status
-----------------------------------------------------------------------------
9.9.9.2         -                default          0.0.0.0          UP   : UP
12.12.11.11     12.13.12.12      rasagna-grp                       DOWN : DOWN
27.0.0.1        23.0.0.1         test                              DOWN : DOWN

Switch Peer Group Name            : spg1
Switch Peer Group Member Count    : 0
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0

Switch Peer Group Name            : pg
Switch Peer Group Member Count    : 1
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0

IP              Public IP             Link Status
-------------------------------------------------
9.7.136.10      9.7.136.10            DOWN : DOWN
```

例：デフォルトの Web 認証ログイン ページの選択

次の例は、デフォルトの Web 認証ログイン ページを選択する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their CPL
control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly
advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
スイッチ(config)# wlan wlan50
スイッチ(config-wlan)# shutdown
スイッチ(config-wlan)# security web-auth authentication-list test
スイッチ(config-wlan)# security web-auth parameter-map test
スイッチ(config-wlan)# no shutdown
スイッチ(config-wlan)# end
スイッチ# show running-config | section wlan50
wlan wlan50 50 wlan50
 security wpa akm cckm
 security wpa wpa1
 security wpa wpa1 ciphers aes
 security wpa wpa1 ciphers tkip
 security web-auth authentication-list test
 security web-auth parameter-map test
 session-timeout 1800
 no shutdown

スイッチ# show running-config | section parameter-map type webauth test
```

```
parameter-map type webauth test
 type webauth
```

例：外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択

次の例は、外部 Web サーバからカスタマイズされた Web 認証ログイン ページを選択する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# parameter-map type webauth global
スイッチ(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
スイッチ(config-params-parameter-map)# parameter-map type webauth test
スイッチ(config-params-parameter-map)# type webauth
スイッチ(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
スイッチ(config-params-parameter-map)# redirect portal ipv4 23.0.0.1
スイッチ(config-params-parameter-map)# end
スイッチ# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 23.0.0.1
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

例：WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て

次の例は、WLANごとのログイン割り当て、ログイン失敗、およびログアウトページを割り当てる方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# parameter-map type webauth test
スイッチ(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
スイッチ(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html

スイッチ(config-params-parameter-map)# custom-page failure device flash:loginfail.html
スイッチ(config-params-parameter-map)# custom-page success device flash:loginsucess.html
スイッチ(config-params-parameter-map)# end
スイッチ# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 23.0.0.1
 custom-page login device flash:loginsantosh.html
 custom-page success device flash:loginsucess.html
 custom-page failure device flash:loginfail.html
 custom-page login expired device flash:loginexpire.html
```

例：AAA-Override の設定

次の例は、AAA-Override を設定する例を示しています。

```
スイッチ# configure terminal
スイッチ(config)# wlan fff
```

```
スイッチ(config-wlan)# aaa-override
スイッチ(config-wlan)# end
スイッチ# show running-config | section fff
 wlan fff 44 fff
 aaa-override
 shutdown
```

例：クライアントの負荷分散の設定

次の例は、クライアントの負荷分散を設定する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# wlan fff
スイッチ(config-wlan)# shutdown
スイッチ(config-wlan)# mobility anchor 9.7.136.15
スイッチ(config-wlan)# mobility anchor 9.7.136.16
スイッチ(config-wlan)# no shutdown wlan
スイッチ(config-wlan)# end
スイッチ# show running-config | section fff
wlan fff 44 fff
 aaa-override
 shutdown
```

例：事前認証 ACL の設定

次の例は、事前認証 ACL を設定する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# wlan fff
スイッチ(config-wlan)# shutdown
スイッチ(config-wlan)# ip access-group web preauthrule
スイッチ(config-wlan)# no shutdown
スイッチ(config-wlan)# end
スイッチ# show wlan name fff
```

例：IOS ACL 定義の設定

次に、IOS ACL 定義を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ip access-list extended 102
スイッチ(config-ext-nacl)# permit udp any eq 8080 any
スイッチ(config-ext-nacl)# end
スイッチ# show access-lists 102
 Extended IP access list 102
    10 permit udp any eq 8080 any
```

例：Webpassthrough の設定

次の例は、Webpassthrough を設定する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# parameter-map type webauth webparalocal
スイッチ(config-params-parameter-map)# type consent
```

```
スイッチ(config-params-parameter-map)# end
スイッチ# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 23.0.0.1
```

ゲスト アクセスに関する追加情報

関連資料

関連項目	マニュアル タイトル
モビリティ CLI コマンド	*Mobility Command Reference, Cisco IOS XE 3SE (Cisco WLC 5700 Series)*
モビリティ設定	*Mobility Configuration Guide, Cisco IOS XE 3SE (Cisco WLC 5700 Series)*
セキュリティ CLI コマンド	*Security Command Reference, Cisco IOS Release 3SE (Cisco WLC 5700 Series)*
Catalyst 5700 シリーズ ワイヤレス コントローラの Web ベースの認証	*Security Configuration Guide, Cisco IOS Release 3SE (Cisco WLC 5700 Series)*
有線ゲスト アクセス設定およびコマンド	*Identity Based Networking Services*

標準および RFC

標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

ゲスト アクセスの機能履歴と情報

リリース	機能情報
Cisco IOS XE Release 3.2SE	この機能が導入されました。

第 75 章

不正なデバイスの管理

- 機能情報の確認，1835 ページ
- 不正なデバイスについて，1835 ページ
- 不正検出の設定方法，1841 ページ
- 不正検出のモニタリング，1844 ページ
- 例：不正検出の設定，1844 ページ
- 不正検出に関する追加情報，1845 ページ
- 不正検出設定の機能履歴と情報，1846 ページ

機能情報の確認

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

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

不正なデバイスについて

不正なアクセス ポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセス ポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連のクリア ツー センド（CTS）フレームを送信できるようになります。アクセス ポイントになりすまして、特定のクライアントに

は送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。無線 LAN サービス プロバイダーは、空間からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、認可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正アクセス ポイントは、企業のファイアウォールの内側にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正なアクセスポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアントセッションをハイジャックすることは簡単です。さらに警戒すべきことは、セキュリティで保護されていないアクセス ポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

次に、不正なデバイスの管理に関する注意事項を示します。

- 許可とアソシエーションの検出後、ただちに阻止フレームが送信されます。強化された不正阻止アルゴリズムを使用すると、アドホック クライアントをより効果的に阻止することができます。
- ローカル モード アクセス ポイントは、関連付けられたクライアントに対応するように設計されています。これらのアクセス ポイントは比較的短時間でオフチャネル スキャンを実行します（各チャネル約 50 ミリ秒）。高度な不正検出を実行するには、監視モードのアクセス ポイントを使用する必要があります。あるいは、スキャン間隔を 180 秒から 120 または 60 秒などに短縮して、無線がオフチャネルになる頻度を増やします。これにより、不正が検出される可能性は増加します。ただしこの場合も、アクセスポイントが各チャネルに費やす時間は約 50 ミリ秒です。
- 家庭の環境で展開されるアクセスポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。
- クライアント カードの実装により、アド ホックの抑制の効果が低下することがあります。
- 不正なアクセス ポイントの分類および報告は、不正の状態と、不正なアクセス ポイントの状態を自動的に移行できるようにする、ユーザ定義の分類規則に従って行うことができます。
- 各コントローラは、不正アクセス ポイントの封じ込めを無線チャンネルごとに 3 台（監視モード アクセス ポイントの場合、無線チャネルごとに 6 台）に制限します。
- Rogue Location Discovery Protocol（RLDP）は、オープン認証に設定されている不正なアクセス ポイントを検出します。
- RLDP はブロードキャスト Basic Service Set Identifier（BSSID）を使用する不正なアクセス ポイント（つまり Service Set Identifier をビーコンでブロードキャストするアクセス ポイント）を検出します。
- RLDP は、同じネットワークにある不正なアクセス ポイントのみを検出します。ネットワークのアクセス リストによって不正なアクセス ポイントからコントローラへの RLDP のトラフィックの送信が阻止されている場合は、RLDP は機能しません。

- RLDP は 5 GHz の動的周波数選択（DFS）チャネルでは機能しません。ただし RLDP は、管理対象のアクセス ポイントが DFS チャネルの監視モードである場合には機能します。
- メッシュ AP で RLDP が有効にされていて、その AP が RLDP タスクを実行すると、そのメッシュ AP のアソシエーションはコントローラから解除されます。回避策は、メッシュ AP で RLDP を無効にすることです。
- RLDP が監視モードではない AP で有効になっている場合、RLDP の処理中にクライアント接続の中断が発生します。
- 不正を手動で阻止すると、不正なエントリは期限切れになった後でも保持されます。
- 不正を自動、ルール、AwIPS などの他の防御方法で阻止すると、不正なエントリは期限切れになると削除されます。
- コントローラは、不正なクライアントの検証を AAA サーバに一度だけ要求します。その結果、不正なクライアント検証が最初の試行で失敗すると、不正なクライアントは今後脅威として検出されなくなります。これを回避するには、[Validate Rogue Clients Against AAA] を有効にする前に、認証サーバに有効なクライアント エントリを追加します。
- 7.4 以前のリリースでは、ルールによってすでに分類された不正は再分類されませんでした。7.5 リリースでは、不正ルールの優先順位に基づいて不正を再分類できるようにこの動作が強化されました。優先順位は、コントローラが受信する不正レポートを使用して決定されます。
- WLAN、LAN、11a 無線および 11bg 無線の不正な AP の MAC アドレスは、不正 BSSID の +/- 1 の差異で設定されているので、不正検出 AP は、5Mhz チャネルの不正な有線 AP の関連付けおよび阻止に失敗します。8.0 リリースでは、MAC アドレスの範囲を広げることによって、この動作が強化されました。不正検出 AP は有線 ARP MAC と不正 BSSID を +/- 3 の差異で関連付けます。
- オープン認証を使用する不正アクセス ポイントはネットワーク上で検出できます。NAT 有線または不正有線検出は、WLC（RLDP と不正検出 AP の両方）ではサポートされません。非隣接 MAC アドレスは、RLDP ではなく AP の不正検出モードでサポートされます。

（注） 不正AP、不正クライアント、または一時的な封じ込めの設定は、リロード時に破棄されます。リロード後にすべての不正を再設定する必要があります。

（注） 不正クライアントのトラップを制御する別個のコマンドはありません。ただし、不正な AP に使用される config trapflags rogueap {enable | disable} コマンドを使用して、不正クライアントのトラップを有効または無効にすることもできます。さらに、GUI設定では、不正クライアントを制御するために、[Management] -> [SNMP] -> [TrapControl] -> [Security] -> [Rogue AP] で不正クライアント AP フラグを使用する必要があります。

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol（RLDP）は、不正 AP で認証が設定されていない（オープン認証）場合に使用される積極的なアプローチです。このモードは、デフォルトで無効になっており、不正チャネルに移動して、クライアントとして不正に接続するようにアクティブ AP に指示します。この間に、アクティブ AP は、接続されたすべてのクライアントに認証解除メッセージを送信してから、無線インターフェイスをシャットダウンします。次に、クライアントとして不正 AP にアソシエートします。その後で、AP は、不正 AP から IP アドレスの取得を試み、ローカル AP と不正接続情報を含む User Datagram Protocol（UDP）パケット（ポート 6352）を不正 AP を介してコントローラに転送します。コントローラがこのパケットを受信すると、不正 AP が RLDP 機能を使用して有線ネットワークで検出されたことをネットワーク管理者に通知するためのアラームが設定されます。

RLDP の不正 AP の検出精度は 100% です。オープン AP と NAT AP を検出します。

（注） Lightweight AP が不正 AP とアソシエートして DHCP アドレスを受信するかどうかを確認するには、**debug dot11 rldp enable** コマンドを使用します。このコマンドは、Lightweight AP からコントローラに送信された UDP パケットも表示します。

ここで、Lightweight AP から送信される UDP （宛先ポート 6352）パケットのサンプルを示します。0020 0a 01 01 0d 0a 01 .....(.*.....0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00 .....x.....0040 00 00 00 00 00 00 00 00 00 00

最初の 5 バイトのデータには、不正 AP によってローカル モード AP に割り当てられた DHCP アドレスが含まれています。次の 5 バイトはコントローラの IP アドレスで、その後に不正 AP MAC アドレスを表す 6 バイトが続きます。その後に、18 バイトの 0 が続きます。

ここで、RLDP の動作手順を示します。

1. 信号強度値を使用して不正に最も近い統合 AP を特定します。
2. その後で、この AP が WLAN クライアントとして不正に接続します。3 回のアソシエーションを試みて、成功しない場合はタイムアウトします。
3. アソシエーションが成功すると、AP が DHCP を使用して IP アドレスを取得します。
4. IP アドレスが取得されたら、AP（WLAN クライアントとして機能している）は、コントローラの IP アドレスのそれぞれに UDP パケットを送信します。
5. コントローラがクライアントから RLDP パケットの 1 つでも受信すると、その不正が重大度が critical の on-wire としてマークされます。

（注） コントローラのネットワークと不正デバイスが設置されたネットワークの間にフィルタリングルールが設定されている場合は、RLDP パケットがコントローラに到達できません。

RLDP の注意事項：

- RLDP は、認証と暗号化が無効になっている SSID をブロードキャストするオープン不正 AP でのみ動作します。
- RLDP では、クライアントとして機能しているマネージド AP が不正ネットワーク上で DHCP を介して IP アドレスを取得できる必要があります。
- 手動 RLDP を使用して、不正上で RLDP トレースを複数回試すことができます。
- RLDP プロセス中は、AP がクライアントにサービスを提供できません。これがローカル モード AP のパフォーマンスと接続に悪影響を及ぼします。この問題を回避するために、RLDP はモニタ モード AP に対してのみ選択的に有効にできます。
- RLDP は、5GHz DFS チャネルで動作する不正 AP への接続は試行しません。

（注） RLDP は、シスコの Atonomous 不正アクセス ポイントではサポートされていません。これらのアクセス ポイントは、RLDP クライアントによって送信された DHCP 検出要求をドロップします。また不正なアクセスポイントチャネルが動的周波数選択（DFS）を必要とする場合、RLDP はサポートされません。自動 RLDP 試行で不正（ノイズの多い RF 環境などが原因）が検出されなかった場合は、コントローラが再試行しません。ただし、不正デバイス上で RLDP を手動で開始できます。

不正なデバイスの検出

コントローラは、近くにあるすべてのアクセスポイントを継続的に監視し、不正なアクセスポイントとクライアントに関する情報を自動的に検出および収集します。コントローラは不正なアクセス ポイントを検出すると、Rogue Location Discovery Protocol（RLDP）を使用し、不正検出モードのアクセス ポイントが接続されて、不正がネットワークに接続されているかどうかを特定します。

コントローラは、オープン認証および設定された不正デバイスで RLDP を開始します。RLDP が Flexconnect またはローカル モードのアクセス ポイントを使用すると、クライアントはその時点で接続を解除されます。RLDP のサイクルが終了すると、クライアントはアクセス ポイントに再接続します。不正なアクセス ポイントが検出された時点で（自動設定）、RLDP のプロセスが開始されます。

すべてのアクセスポイント、または監視（リッスン専用）モードに設定されたアクセスポイントでのみ RLDP を使用するようにコントローラを設定できます。後者のオプションでは、混雑した無線周波数（RF）空間での自動不正アクセスポイント検出が実現され、不要な干渉を生じさせたり、正規のデータアクセスポイント機能に影響を与えずにモニタリングを実行できます。すべてのアクセス ポイントで RLDP を使用するようにコントローラを設定した場合、モニタ アクセス ポイントとローカル（データ）アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 動作に対してモニタ アクセスポイントを選択します。ネットワーク上に不正があると RLDP が判断した場合、検出された不正を手動または自動で阻止することを選択できます。

RLDP は、オープン認証に設定されている不正なアクセス ポイントの存在をネットワーク上で一度だけ（デフォルト設定の再試行回数）検出します。再試行は **config rogue ap rldp retries** コマンドを使用して設定できます。

3 種類の方法でコントローラから RLDP を開始またはトリガーできます。

1. コントローラの CLI から RLDP 開始コマンドを手動で入力します。RLDP を開始するための同等の GUI オプションはサポートされていません。
   config rogue ap rldp initiate*mac-address*
2. コントローラの CLI から RLDP をスケジュールします。RLDP をスケジュールするための同等の GUI オプションはサポートされていません。
   config rogue ap rldp schedule
3. 自動 RLDP。コントローラの CLI または GUI から自動 RLDP を設定できますが、次の注意事項を考慮してください。
   - 不正検出のセキュリティ レベルが custom に設定されている場合にのみ、自動 RLDP オプションを設定できます。
   - 自動 RLDP および RLDP のスケジュールを同時に有効にすることはできません。

不正なアクセス ポイントは、自動または手動で Contained 状態に変更されます。コントローラは、不正の阻止に最も効果的なアクセスポイントを選択し、そのアクセスポイントに情報を提供します。アクセス ポイントは、無線あたりの不正阻止数のリストを保存します。自動阻止の場合は、監視モードのアクセス ポイントだけを使用するようにコントローラを設定できます。阻止動作は次の 2 つの方法で開始されます。

- コンテナ アクセスポイントが定期的に不正阻止のリストを確認し、ユニキャスト阻止フレームを送信します。不正なアクセス ポイントの阻止の場合、フレームは不正なクライアントがアソシエートされている場合にのみ送信されます。
- 阻止された不正アクティビティが検出されると、阻止フレームが送信されます。

個々の不正阻止には、一連のユニキャスト アソシエーション解除フレームおよび認証解除フレームの送信が含まれます。

Cisco Prime Infrastructure のインタラクションと不正検出

Cisco Prime Infrastructure ではルール ベースの分類がサポートされ、コントローラで設定された分類ルールが使用されます。コントローラは、次のイベント後に Cisco Prime Infrastructure にトラップを送信します。

- 不明なアクセス ポイントが Friendly 状態に初めて移行すると、コントローラは、不正の状態が Alert の場合にのみ Cisco Prime Infrastructure にトラップを送信します。不正の状態が Internal または External であると、トラップは送信されません。
- タイムアウトの経過後に不正なエントリが削除されると、Malicious（Alert、Threat）または Unclassified（Alert）に分類された不正なアクセス ポイントに関して、コントローラから Cisco Prime Infrastructure にトラップが送信されます。コントローラでは、不正の状態が Contained、Contained Pending、Internal、および External である不正なエントリは削除されません。

不正検出の設定方法

不正検出の設定（CLI）

手順の概要

1. **configure terminal**
2. **wireless wpsroguedetectionmin-rssi***rssi in dBm*
3. **wireless wpsroguedetectionmin-transient-time** *time in seconds*
4. **wireless wpsrogueclient** {**aaa** | **mse**}
5. **wireless wpsrogue apvalid-clientauto-contain**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless wpsroguedetectionmin-rssi***rssi in dBm* 例： スイッチ(config)# **wireless wps rogue detection min-rssi 100**	不正に必要な最小 RSSI 値を指定します。これは、AP が不正を検出し、スイッチで不正エントリが作成されるために必要な値です。 rssi in dBm パラメータの有効範囲は –128 ～ –70 dBm で、デフォルト値は –128 dBm です。 （注） この機能は、すべての AP モードに適用できます。RSSI 値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、AP が不正を検出する最小 RSSI 値を指定することで、このオプションを使用して不正をフィルタリングすることができます。
ステップ 3	**wireless wpsroguedetectionmin-transient-time** *time in seconds* 例： スイッチ(config)# **wireless wps rogue detection min-transient-time**	不正が初めてスキャンされた後、AP で不正スキャンを連続的に実行する間隔を入力します。 time in sec パラメータの有効範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。

	コマンドまたはアクション	目的
		（注） この機能は、モニタ モードの AP のみに適用されます。 一時的な間隔値を使用して、AP が不正をスキャンする間隔を制御できます。AP では、それぞれの一時的間隔値に基づいて、不正のフィルタリングも実行できます。 この機能には次の利点があります。 • AP からコントローラへの不正レポートが短くなる • 一時的な不正エントリをコントローラで回避できる • 一時的な不正への不要なメモリ割り当てを回避できる

ステップ 4	**wireless wpsrogueclient** {**aaa** | **mse**}
	例：
	`スイッチ(config)# wireless wps rogue client aaa`
	`スイッチ(config)# wireless wps rogue client mse`
		不正なクライアントが有効なクライアントかどうかを検証するために、AAA サーバまたはローカル データベース、または MSE を設定します。

ステップ 5	**wireless wpsrogue apvalid-clientauto-contain** 例： `スイッチ(config)# wireless wps rogue ap valid-client auto-contain`	信頼できるクライアントが関連付けられる不正なアクセス ポイントを自動的に阻止するように指定します。
ステップ 6	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

不正検出の設定（GUI）

ステップ 1 該当するアクセス ポイントで不正検出が有効になっていることを確認します。コントローラに join されたすべてのアクセス ポイントに対し、不正の検出がデフォルトで有効にされます（OfficeExtend アクセス ポイントを除く）。ただし、[Configuration] > [Wireless] > [Access Policies] > [All APs] を選択して [Edit AP] ページを開き、このページの [General] エリアの [Rogue Detector] チェックボックスを選択または選択解除して、個別のアクセス ポイントの不正検出をイネーブルまたはディセーブルにすることができます。

ステップ 2 [Configuration] > [Security] > [Wireless Protection Policies] > [Rogue Policies] を選択します。

[Rogue Policies] ページが表示されます。

ステップ 3 [Rogue Location Discovery Protocol] ドロップダウン リストから、次のオプションのいずれかを選択します。

- Disable：すべてのアクセス ポイントで RLDP を無効にします。これはデフォルト値です。
- All APs：すべてのアクセス ポイントで RLDP を有効にします。
- Monitor Mode APs：監視モードのアクセス ポイントでのみ RLDP を有効にします。

ステップ 4 [Expiration Timeout for Rogue AP and Rogue Client Entries] テキスト ボックスに、不正なアクセス ポイントとクライアント エントリの期限が切れてリストから削除されるまでの秒数を入力します。有効な範囲は 240 ～ 3600 秒で、デフォルト値は 1200 秒です。

（注） 不正なアクセス ポイントまたはクライアントのエントリがタイムアウトすると、その不正の状態がいずれの分類タイプに対しても Alert または Threat である場合には、コントローラから削除されます。

ステップ 5 AAA サーバまたはローカル データベースを使用して、不正なクライアントが有効なクライアントであるかどうかを検証するには、[Validate Rogue Clients Against AAA] チェックボックスをオンにします。デフォルトでは、チェックボックスはオフになっています。

ステップ 6 必要に応じて、アドホックの不正検出およびレポートを有効にするには、[Detect and report Adhoc networks] チェックボックスを選択します。デフォルトでは、チェックボックスはオンになっています。

ステップ 7 [Rogue Detection Report Interval] テキスト ボックスに、AP が不正検出レポートをコントローラに送信する間隔を秒単位で入力します。有効な範囲は 10 ～ 300 秒で、デフォルト値は 10 秒です。

ステップ 8 コントローラに自動的に特定の不正デバイスを阻止させる場合は、次のパラメータを有効にします。デフォルトでは、これらのパラメータは無効の状態です。

注意 Auto Contain パラメータのいずれかを選択して [Apply] をクリックすると、「`Using this feature may have legal consequences.Do you want to continue?`」というメッセージが表示されます。産業科学医療（ISM）帯域の 2.4 GHz および 5 GHz の周波数は一般に公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

- Auto Containment Level：自動阻止レベルを設定します。デフォルトで、自動阻止レベルは 1 に設定されています。
- Auto Containment only for Monitor mode APs：自動阻止用のモニタ モード アクセス ポイントを設定します。
- Rogue on Wire：有線ネットワークで検出される不正の自動阻止を設定します。
- Using Our SSID：ネットワークの SSID をアドバタイズする不正の自動阻止を設定します。このパラメータをオフにしておくと、該当する不正が検出されても警告が生成されるだけです。
- Valid Client on Rogue AP：信頼できるクライアントが関連付けられている不正なアクセス ポイントの自動阻止を設定します。このパラメータをオフにしておくと、該当する不正が検出されても警告が生成されるだけです。

- AdHoc Rogue AP：コントローラによって検出されたアドホック ネットワークの自動阻止を設定します。このパラメータをオフにしておくと、該当するネットワークが検出されても警告が生成されるだけです。

ステップ 9 [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

不正検出のモニタリング

この項では、不正検出の新しいコマンドについて説明します。

次のコマンドは、スイッチ上で不正検出をモニタするために使用できます。

表 *128*：不正検出モニタリングのコマンド

コマンド	目的
show wireless wps rogue ap summary	スイッチによって検出されたすべての不正アクセス ポイントのリストを表示します。
show wireless wps rogue client detailed*client-mac*	特定の不正クライアントの詳細情報を表示します。
show wireless wps rogue client summary	スイッチで検出されたすべての不正なクライアントのリストを表示します。
show nmsp capability	NMSP 機能を表示します。

例：不正検出の設定

この例は、検出された不正 AP が存在する必要がある最小 RSSI を、スイッチで作成されたエントリを持つように設定する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# wireless wps rogue detection min-rssi -100
スイッチ(config)# end
スイッチ# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

次に、分類インターバルを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wireless wps rogue detection min-transient-time 500
```

```
スイッチ(config)# end
スイッチ# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

次に、不正なクライアントが有効なクライアントかどうかを検証するためにMSEを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wireless wps rogue client mse
スイッチ(config)# end
スイッチ# show wireless wps rogue client summary
```

次に、信頼できるクライアントが関連付けられる不正なアクセス ポイントを自動的に阻止する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wireless wps rogue ap valid-client auto-contain
スイッチ(config)# end
スイッチ# show wireless wps rogue ap summary
スイッチ# show nmsp capability
```

不正検出に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

不正検出設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。
Cisco IOS XE 3E	MSE に対する不正な検証。

第 76 章

不正なアクセス ポイントの分類

- 機能情報の確認，1847 ページ
- 不正なアクセス ポイントの分類について，1847 ページ
- 不正なアクセス ポイントの分類の制限，1850 ページ
- 不正なアクセス ポイントの分類方法，1851 ページ
- 不正なデバイスの表示および分類（GUI），1857 ページ
- 例：不正なアクセス ポイントの分類，1859 ページ
- 不正なアクセス ポイントの分類に関する追加情報，1860 ページ
- 不正なアクセス ポイントの分類の機能履歴および情報，1861 ページ

機能情報の確認

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

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

不正なアクセス ポイントの分類について

コントローラ ソフトウェアでは、不正なアクセス ポイントを Friendly、Malicious、または Unclassified に分類して表示するルールを作成できます。

デフォルトでは、いずれの分類ルールも有効になっていません。したがって、すべての未知（管理対象外）のアクセス ポイントは Unclassified に分類されます。ルールを作成し、その条件を設

定して、ルールを有効にすると、未分類のアクセス ポイントは分類し直されます。ルールを変更するたびに、Alert状態にあるすべてのアクセス ポイント（Friendly、Malicious、およびUnclassified）にそのルールが適用されます。

（注） ルール ベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。

（注） 1 台のコントローラにつき最大 64 の不正分類ルールを設定できます。

コントローラは、管理対象のアクセス ポイントの 1 つから不正レポートを受信すると、次のように応答します。

1. コントローラは未知（管理対象外）のアクセス ポイントが危険性のないMACアドレスのリストに含まれているか確認します。そのリストに含まれている場合、コントローラはそのアクセス ポイントを Friendly として分類します。
2. 未知（管理対象外）のアクセス ポイントが危険性のないMACアドレスのリストに含まれていない場合、コントローラは、不正状態の分類ルール適用処理を開始します。
3. 不正なアクセス ポイントが Malicious、Alert または Friendly、Internal または External にすでに分類されている場合は、コントローラはそのアクセス ポイントを自動的に分類しません。不正なアクセス ポイントがそれ以外に分類されており、Alert 状態にある場合に限り、コントローラはそのアクセス ポイントを自動的に分類し直します。
4. コントローラは、優先度の一番高いルールを適用します。不正なアクセス ポイントがルールで指定された条件に一致すると、コントローラはそのアクセス ポイントをルールに設定された分類タイプに基づいて分類します。
5. 不正なアクセス ポイントが設定されたルールのいずれにも一致しないと、コントローラはそのアクセス ポイントを Unclassified に分類します。
6. コントローラは、すべての不正なアクセス ポイントに対して上記の手順を繰り返します。
7. 不正なアクセス ポイントが社内ネットワーク上にあると RLDP で判断されると、ルールが設定されていない場合でも、コントローラは不正の状態を Threat とマークし、そのアクセス ポイントを自動的に Malicious に分類します。その後、不正なアクセス ポイントに対して手動で封じ込め処理を行うことができますが（不正を自動的に封じ込めるようRLDPが設定されていない限り）、その場合は不正の状態が Contained に変更されます。不正なアクセス ポイントがネットワーク上にないと、コントローラによって不正の状態が Alert とマークされ、そのアクセス ポイントを手動で封じ込め処理を行うことができるようになります。
8. 必要に応じて、各アクセスポイントを本来とは異なる分類タイプや不正の状態に手動で変更することも可能です。

表 *129*：分類マッピング

ルール ベースの分類タイプ	不正の状態
Friendly	• Internal：不明なアクセス ポイントがネットワーク内に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、Internal に設定します。たとえば、ラボ ネットワーク内のアクセス ポイントなどです。 • External：不明なアクセス ポイントがネットワーク外に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、External に設定します。たとえば、近隣のコーヒー ショップに属するアクセス ポイントなどです。 • Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。
Malicious	• Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • Threat：未知（管理対象外）のアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。 • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。 • Contained Pending：不明なアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。
未分類	• Pending：最初の検出で、不明なアクセス ポイントは 3 分間 Pending 状態に置かれます。この間に、管理対象のアクセス ポイントでは、不明なアクセス ポイントがネイバー アクセス ポイントであるかどうかが判定されます。 • Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。 • Contained Pending：不明なアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。

分類および不正アクセス ポイントのステータスは以下のように設定されています。

- Known から Friendly、Internal
- Acknowledged から Friendly、External
- Contained から Malicious、Contained

前述のように、コントローラでは、ユーザ定義のルールに基づいて未知（管理対象外）のアクセス ポイントの分類タイプと不正の状態が自動的に変更されます。もしくは、未知（管理対象外）のアクセス ポイントを本来とは異なる分類タイプと不正の状態に手動で変更することができます。

表 *130*：設定可能な分類タイプ/不正の状態の推移

遷移元	目的
Friendly（Internal、External、Alert）	Malicious（Alert）
Friendly（Internal、External、Alert）	Unclassified（Alert）
Friendly（Alert）	Friendly（Internal、External）
Malicious（Alert、Threat）	Friendly（Internal、External）
Malicious（Contained、Contained Pending）	Malicious（Alert）
Unclassified（Alert、Threat）	Friendly（Internal、External）
Unclassified（Contained、Contained Pending）	Unclassified（Alert）
Unclassified（Alert）	Malicious（Alert）

不正の状態が Contained の場合、不正なアクセス ポイントの分類タイプを変更する前に、そのアクセス ポイントが封じ込められないようにする必要があります。不正なアクセス ポイントを Malicious から Unclassified に変更する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

不正なアクセス ポイントの分類の制限

いくつかの不正なルールがあります。その内容は次のとおりです。

- カスタム タイプの不正の分類は、不正ルールに関連付けられています。このため、不正を手動で Custom として分類することはできません。カスタム クラスの変更は不正ルールを使用する場合にのみ行えます。
- 不正分類の変更に対して、ルールによって 30 分ごとに阻止用のトラップが送信されます。カスタム分類の場合、最初のトラップはカスタム分類よりも前に存在していたため、そのト

ラップに重大度スコアは含まれません。不正が分類されると、30分後に生成される後続のトラップから重大度スコアが取得されます。

- 不正ルールは、優先順位に従って、コントローラ内の新しい着信不正レポートごとに適用されます。
- 不正がより高い優先度ルールを満たし、分類されると、同じレポートの優先順位リスト内で下位に下がることはありません。
- 以前に分類された不正は、次の制限に従って、新しい不正レポートが作成されるたびに、再分類されます。
  - ルールによって Friendly に分類され、状態が ALERT に設定されている不正は、新しい不正レポートを受け取ると再分類が開始されます。
  - 不正が管理者によって Friendly に手動で分類されると、状態は INTERNAL になり、次に続く不正レポートで再分類されません。
  - 不正が Malicious に分類されると、その状態に関係なく、後続の不正レポートで再分類されません。
- 一部の属性が新しい不正レポートで欠落している場合、複数の不正ルールによって、Friendly から Malicious に不正の状態が遷移する可能性があります。
- どの不正ルールによっても、Maliciousから他の分類に不正の状態が遷移することはありません。

不正なアクセス ポイントの分類方法

不正分類ルールの設定（CLI）

手順の概要

1. **configure terminal**
2. **wireless wps rogue rule***rule-name***priority***priority*
3. **classify** {**friendly** | **malicious**}
4. **condition** {**client-count**|**duration**|**encryption**|**infrastructure**|**rssi**|**ssid**}
5. **match** {**all** | **any**}
6. **default**
7. **exit**
8. **shutdown**
9. **end**
10. **configure terminal**
11. **wireless wps rogue ruleshutdown**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless wps rogue rule***rule-name***priority***priority* 例： スイッチ(config)# **wireless wps rogue rule rule_3 priority 3** スイッチ(config-rule)#	ルールを作成またはイネーブルにします。ルールを作成する場合、ルールのプライオリティを入力する必要があります。 （注） ルールを作成した後、ルールを編集する場合、ディセーブルになった不正ルールに対してのみプライオリティを変更できます。有効にされた不正ルールのプライオリティは変更できません。編集時の不正ルールのプライオリティ変更は任意です。
ステップ 3	**classify** {**friendly** | **malicious**} 例： スイッチ(config)# **wireless wps rogue rule rule_3 priority 3** スイッチ(config-rule)# **classify friendly**	ルールを分類します。
ステップ 4	**condition** {**client-count**|**duration**|**encryption**|**infrastructure**|**rssi**|**ssid**} 例： スイッチ(config)# **wireless wps rogue rule rule_3 priority 3** スイッチ(config-rule)# **condition client-count 5**	不正アクセス ポイントが満たす必要のあるルールに以下の条件を追加することを指定します。 • **client-count**：不正なアクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正なアクセス ポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセス ポイントはMaliciousに分類されます。このオプションを選択する場合は、*condition_value*パラメータに、不正なアクセス ポイントにアソシエートされたクライアントの最小数を入力します。有効な値の範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。 • **duration**：不正なアクセス ポイントが最小期間検出される必要があります。このオプションを選択する場合は、*condition_value*パラメータに最小検出期間の値を入力します。有効な値の範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。

	コマンドまたはアクション	目的
		• **encryption**：アドバタイズされた WLAN で暗号化が無効になっている必要があります。 • **infrastructure**：SSID がコントローラで認識される必要があります。 • **rssi**：不正なアクセス ポイントには、最小の RSSI 値が必要です。たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、*condition_value* パラメータに最小 RSSI 値を入力します。有効な値の範囲は -95 ～ -50 dBm（両端の値を含む）で、デフォルト値は 0 dBm です。 • **ssid**：不正なアクセス ポイントには、特定の SSID が必要です。コントローラによって管理されない SSID を追加する必要があります。このオプションを選択する場合は、*condition_value* パラメータに SSID を入力します。SSID はユーザ設定の SSID リストに追加されます。

ステップ 5	**match** {**all** | **any**}
	
	例：
	`スイッチ(config)# wireless wps rogue rule rule_3 priority 3`
	`スイッチ(config-rule)# match all`
		検出された不正なアクセス ポイントがルールに一致していると見なされ、そのルールの分類タイプが適用されるためには、ルールで定義されているすべての条件を満たす必要があるか、一部の条件を満たす必要があるかを指定します。

ステップ 6	**default**
	
	例：
	`スイッチ(config)# wireless wps rogue rule rule_3 priority 3`
	`スイッチ(config-rule)# default`
		コマンドをデフォルトに設定するように指定します。

ステップ 7	**exit**
	
	例：
	`スイッチ(config)# wireless wps rogue rule rule_3 priority 3`
	`スイッチ(config-rule)# exit`
	`スイッチ(config)#`
		サブモードの終了を指定します。

	コマンドまたはアクション	目的
ステップ 8	**shutdown** 例： スイッチ(config)# **wireless wps rogue rule rule_3 priority 3** スイッチ(config-rule)# **shutdown**	特定の不正ルールをディセーブルにすることを指定します。たとえば、ルール **rule_3** はディセーブルです。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 10	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 11	**wireless wps rogue ruleshutdown** 例： スイッチ(config)# **wireless wps rogue rule shutdown**	すべての不正ルールをディセーブルにすることを指定します。
ステップ 12	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

不正分類ルールの設定（GUI）

ステップ 1 [Security] > [Wireless Protection Policies] > [Rogue Policies] > [Rogue Rules] を選択して、[Rogue Rules] ページを開きます。
すでに作成されているすべてのルールが優先順位に従って一覧表示されます。各ルールの名前、タイプ、およびステータスが表示されます。

（注） ルールを削除するには、そのルールの青いドロップダウンの矢印の上にマウス カーソルを置いて、[Remove] をクリックします。

ステップ 2 次の手順を実行して、新しいルールを作成します。

a) [Add Rule] をクリックします。[Add Rule] セクションがページ上部に表示されます。
b) [Rule Name] テキスト ボックスに、新しいルールの名前を入力します。名前にはスペースを含めないでください。
c) [Rule Type] ドロップダウン リストで、以下のオプションから選択してこのルールと一致する不正アクセス ポイントを [Friendly] または [Malicious] として分類します。

- Friendly
- Malicious

d) [Add] をクリックして既存のルール リストにこのルールを追加するか、[Cancel] をクリックしてこの新しいルールを破棄します。

ステップ 3 次の手順を実行して、ルールを編集します。

a) 編集するルールの名前をクリックします。[Rogue Rule] > [Edit] ページが表示されます。

b) [Type] ドロップダウン リストで、以下のオプションから選択してこのルールと一致する不正アクセス ポイントを分類します。

- Friendly
- Malicious

c) [Match Operation] テキスト ボックスから、次のいずれかを選択します。
[All]：このルールが有効な場合、検出された不正なアクセス ポイントは、ルールで指定されたすべての条件を満たしている場合にルールと一致し、その不正に対してルールの分類タイプが適用されます。

[Any]：このルールが有効な場合、検出された不正なアクセス ポイントは、ルールで指定された条件のいずれかを満たす場合にルールと一致し、その不正に対してルールの分類タイプが適用されます。これはデフォルト値です。

d) このルールを有効にするには、[Enable Rule] チェックボックスをオンにします。デフォルト値はオフです。

e) この特定のルールをディセーブルにするには、[Enable Rule] チェックボックスをオフにします。

（注） GUI から一度にすべての不正ルールをディセーブルにすることはできませんが、**wireless wps rogue ruleshutdown** コマンドを使用すると、CLI からすべての不正ルールをディセーブルにできます。

f) [Add Condition] ドロップダウン リストで、不正なアクセス ポイントが満たす必要がある次の条件から 1 つまたは複数を選択し、[Add Condition] をクリックします。

- [SSID]：不正なアクセス ポイントには、特定のユーザ設定 SSID が必要です。このオプションを選択する場合は、[User Configured SSID] テキスト ボックスに SSID を入力し、[Add SSID] をクリックします。ユーザ設定の SSID が追加され、リストされます。

  （注） SSID を削除するには、SSID を強調表示して [Remove] をクリックします。WLAN に適用された SSID は不正ルールには適用できません。

- [RSSI]：不正なアクセス ポイントには、最小の受信信号強度表示（RSSI）値が必要です。たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、[Minimum RSSI] テキスト ボックスに最小 RSSI 値を入力します。有効な値の範囲は -95 ～ -50 dBm（両端の値を含む）で、デフォルト値は 0 dBm です。

- [Duration]：不正なアクセス ポイントが最小期間検出される必要があります。このオプションを選択する場合は、[Time Duration] テキスト ボックスに最小検出期間の値を入力します。有効な値の範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。

- [Client Count]：不正なアクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正なアクセス ポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、[Minimum Number of Rogue Clients] テキスト ボックスに、不正なアクセス ポイントにアソシエートされたクライアントの最小数を入力します。有効な値の範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。
- [No Encryption]：不正なアクセス ポイントのアドバタイズされた WLAN で暗号化が無効になっている必要があります。不正なアクセス ポイントの暗号化が無効になっている場合、より多くのクライアントがそのアクセス ポイントに対してアソシエートを試行します。このオプションに関して、これ以外の設定を行う必要はありません。

  （注） Cisco Prime Infrastructure は、このオプションを「Open Authentication（オープンな認証）」と呼んでいます。

- [Managed SSID]：不正なアクセス ポイントの管理対象 SSID（WLAN に設定された SSID）がコントローラで認識される必要があります。このオプションに関して、これ以外の設定を行う必要はありません。

  （注） SSID および管理対象 SSID の 2 つのリストは相互に排他的であるため、[SSID] および [Managed SSID] の条件を [All] 操作で使用することはできません。[Match All] を使用してルールを定義し、これら2つの条件を設定した場合は、いずれかの条件が満たされないので、不正なアクセス ポイントが Friendly または Malicious に分類されることはありません。

  1 つのルールにつき最大 6 つの条件を追加できます。条件を追加すると、[Conditions] セクションにその条件が表示されます。

  （注） このルールから条件を削除するには、条件付近の [Remove] をクリックします。

- [User configured SSID]：不正アクセス ポイントが特定のユーザ設定 SSID のサブ文字列を持つ必要があります。コントローラは同じ発生パターン内でサブ文字列を検索し、サブ文字列が SSID の文字列全体で見つかった場合はその一致を返します。

g) [Apply] をクリックします。

ステップ 4 不正分類ルールを適用する優先順位を変更する場合の手順は、次のとおりです。

1. [Change Priority] をクリックして、[Rogue Rules > Priority] ページにアクセスします。

   不正ルールが優先順位に従って [Change Rules Priority] テキスト ボックスに表示されます。

2. 優先順位を変更する特定のルールをクリックし、[Up] をクリックしてリスト内の順位を上げるか、[Down] をクリックしてリスト内の順位を下げます。

   （注） ディセーブルのルールだけの優先順位を変更することが可能です。イネーブルのルールだけの優先順位を変更することはできません。

3. [Apply] をクリックします。

不正なデバイスの表示および分類（GUI）

ステップ 1 [Monitor] > [Rogues] の順に選択します。

ステップ 2 次のオプションを選択すると、コントローラで検出された各タイプの不正なアクセス ポイントを表示できます。

- Friendly APs
- Malicious APs
- Unclassified APs

対応する不正な AP ページが、不正アクセス ポイントの MAC アドレス、不正アクセス ポイントを検出した無線の数、不正アクセスポイントに接続されたクライアント数、不正アクセスポイントの現在のステータス、および最後のコンタクトに関する情報を提供します。

ステップ 3 不正なアクセス ポイントの詳細を取得するには、アクセスポイントのMACアドレスをクリックします。[Rogue AP Detail] ページが表示されます。
このページには、不正なデバイスのMACアドレス、不正なデバイスのタイプ（アクセスポイントなど）、不正なデバイスが有線ネットワーク上にあるかどうか、不正なデバイスが最初および最後に報告された日時、デバイスの現在のステータスといった情報が表示されます。

[Class Type] テキスト ボックスには、この不正なアクセス ポイントの現在の分類が表示されます。

- [Friendly]：ユーザ定義の Friendly ルールと一致した不明なアクセス ポイント、または既知の不正なアクセス ポイント。危険性のないアクセス ポイントは阻止することができません。
- [Malicious]：ユーザ定義の Malicious ルールと一致した不明なアクセス ポイント、またはユーザが Friendly または Unclassified 分類タイプから手動で移動した不明なアクセス ポイント。

  （注） アクセス ポイントが Malicious に分類されると、その後でそのアクセス ポイントにルールを適用することはできなくなります。また、別の分類タイプに移動することもできません。危険性のあるアクセス ポイントを Unclassified 分類タイプに移動する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

- [Unclassified]：ユーザ定義の Friendly または Malicious ルールと一致しない不明なアクセス ポイント。未分類のアクセス ポイントは阻止することができます。また、このアクセス ポイントは、ユーザ定義のルールに従って自動的に、またはユーザが手動で、Friendly または Malicious 分類タイプに移動できます。

ステップ 4 このデバイスの分類を変更するには、[Class Type] ドロップダウン リストから別の分類を選択します。

（注） 不正なアクセスポイントの現在の状態が [Contain] である場合、そのアクセスポイントは移動できません。

ステップ 5 [Update Status] ドロップダウン リストから次のオプションのいずれかを選択して、この不正なアクセス ポイントに対するコントローラの応答方法を指定します。

- [Internal]：コントローラはこの不正なアクセス ポイントを信頼します。このオプションは、[Class Type] が [Friendly] に設定されている場合に使用できます。
- [External]：コントローラはこの不正なアクセス ポイントの存在を認識します。このオプションは、[Class Type] が [Friendly] に設定されている場合に使用できます。
- [Contain]：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。このオプションは、[Class Type] が [Malicious] または [Unclassified] に設定されている場合に使用できます。
- [Alert]：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。このオプションは、[Class Type] が [Malicious] または [Unclassified] に設定されている場合に使用できます。

ページの下部には、この不正なアクセス ポイントが検出されたアクセス ポイントと、不正なアクセス ポイントにアソシエートされたすべてのクライアントの両方に関する情報が提供されます。クライアントの詳細を表示するには、[Edit] をクリックして [Rogue Client Detail] ページを開きます。

ステップ 6 [Apply] をクリックします。

ステップ 7 [Save Configuration] をクリックします。

ステップ 8 コントローラで検出されたアドホック不正を確認するには、[Adhoc Rogues] を選択します。[Adhoc Rogues] ページが表示されます。
このページには、MAC アドレス、BSSID、アドホック不正の SSID、アドホック不正が検出された無線の数、アドホック不正の現在のステータスといった情報が表示されます。

ステップ 9 アドホック不正の詳細情報を取得するには、その不正の MAC アドレスをクリックします。[Adhoc Rogue Detail] ページが表示されます。
このページには、アドホック不正の MAC アドレスおよび BSSID、不正が最初および最後に報告された日時、不正の現在のステータスといった情報が表示されます。

ステップ 10 [Update Status] ドロップダウン リストから次のオプションのいずれかを選択して、このアドホック不正に対するコントローラの応答方法を指定します。

- [Contain]：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
- [Alert]：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。
- [Internal]：コントローラはこの不正なアクセス ポイントを信頼します。
- [External]：コントローラはこの不正なアクセス ポイントの存在を認識します。

ステップ 11 [Maximum Number of APs to Contain the Rogue] ドロップダウン リストから、[1]、[2]、[3]、[4] のオプションのいずれかを選択して、このアドホック不正を阻止するために使用するアクセス ポイントの最大数を指定します。

ページの下部には、このアドホック不正が検出されたアクセス ポイントに関する情報が提供されます。

ステップ 12 [Apply] をクリックします。

ステップ 13 [Save Configuration] をクリックします。

ステップ 14 無視するように設定されている任意のアクセス ポイントを表示するには、[Rogue AP Ignore-List] を選択します。[Rogue AP Ignore-List] ページが表示されます。
このページには、無視するように設定されている任意のアクセス ポイントの MAC アドレスが表示されます。不正無視リストには、ユーザが Cisco Prime Infrastructure マップに手動で追加した任意の自律アクセス ポイントのリストが含まれています。コントローラでは、これらの自律アクセス ポイントが、Prime Infrastructure によって管理されていても不正と見なされます。不正無視リストを使用すると、コントローラでこれらのアクセス ポイントを無視できます。このリストは次のように更新されます。

- コントローラは、不正レポートを受信すると、不明なアクセス ポイントが不正無視アクセス ポイント リストに存在するかどうかを確認します。
- 不明なアクセス ポイントが不正無視リストに存在する場合、コントローラはこのアクセス ポイントを無視して他の不正なアクセス ポイントの処理を続けます。
- 不明なアクセス ポイントが不正無視リストにない場合、コントローラは Prime Infrastructure にトラップを送信します。Prime Infrastructure が自律アクセス ポイントにこのアクセス ポイントを検出した場合、Prime Infrastructure はこのアクセス ポイントを不正無視リストに追加するためのコマンドをコントローラに送信します。このアクセス ポイントは、今後の不正レポートで無視されるようになります。
- ユーザが Prime Infrastructure から自律アクセス ポイントを削除した場合、Prime Infrastructure はこのアクセス ポイントを不正無視リストから削除するコマンドをコントローラに送信します。

例：不正なアクセス ポイントの分類

次の例は、不正アクセス ポイントを Friendly として組織および表示できるルールを作成する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# wireless wps rogue rule ap1 priority 1
スイッチ(config-rule)# classify friendly
スイッチ(config-rule)# end
```

この例は、不正アクセス ポイントが満たす必要のある条件を適用する方法を示しています。

```
スイッチ# configure terminal
スイッチ(config)# wireless wps rogue rule ap1 priority 1
スイッチ(config-rule)# condition client-count 5
スイッチ(config-rule)# condition duration 1000
スイッチ(config-rule)# end
```

不正なアクセス ポイントの分類に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

不正なアクセス ポイントの分類の機能履歴および情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 77 章

wIPS の設定

- 機能情報の確認，1863 ページ
- wIPS について，1863 ページ
- アクセス ポイントで wIPS を設定する方法，1871 ページ
- wIPS 情報のモニタリング，1872 ページ
- 例：wIPS の設定，1873 ページ
- wIPS の設定に関する追加情報，1873 ページ
- wIPS 設定実行の機能履歴，1874 ページ

機能情報の確認

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

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

wIPS について

Cisco Adaptive Wireless Intrusion Prevention System（wIPS）（Cisco 適応型ワイヤレス侵入防御システム）では、ワイヤレスでの脅威検出およびパフォーマンス管理のための高度な手法が使用されます。この手法では、ネットワーク トラフィック分析、ネットワーク デバイス/トポロジに関する情報、シグニチャベースの技法、および異常検出を組み合わせることにより、非常に正確で全面的な無線の脅威防御を実現できます。インフラストラクチャに完全に統合されたソリューショ

ンで、有線ネットワークとワイヤレス ネットワークの両方でワイヤレス トラフィックを継続的にモニタし、ネットワーク インテリジェンスを使用してさまざまな原因による攻撃を分析することにより、損害または漏洩が発生する前に、攻撃を正確に特定し事前に防止することができます。

Cisco Adaptive wIPS は、Cisco 3300 シリーズ Mobility Services Engine（MSE）の一部です。MSE は、Cisco Aironet アクセス ポイントを継続的にモニタすることによって収集される情報の処理を一元化します。Cisco Adaptive wIPS の機能と、MSE への Cisco Prime Infrastructure の統合により、wIPS は wIPS のポリシーとアラームの設定/モニタ、脅威の報告を行うことができます。

（注） ご使用の wIPS が Cisco WLC、アクセス ポイント、および Cisco MSE で構成されている場合、これら 3 つのエンティティはすべて UTC タイム ゾーンに設定する必要があります。

Cisco Adaptive wIPS は、Cisco WLC では設定されていません。代わりに、プロファイル設定が Cisco Prime Infrastructure から wIPS サービスに転送され、wIPS サービスによってそのプロファイルが Cisco WLC に転送されます。プロファイルは Cisco WLC のフラッシュメモリに格納され、AP が Cisco WLC に接続すると、その AP へ送信されます。アクセス ポイントの関連付けが解除され、別の Cisco WLC に接続すると、そのアクセス ポイントは新たな Cisco WLC から wIPS プロファイルを受信します。

ローカル モードの AP で、wIPS 機能のサブセットを備えたものは、拡張ローカル モード アクセス ポイント、または ELM AP と呼ばれます。AP が次のいずれかのモードであれば、その AP が wIPS モードで機能するよう設定できます。

- Monitor
- Local

通常のローカル モードの AP は、wIPS 機能のサブセットによって拡張されています。この機能を使用すると、別途のオーバーレイ ネットワークがなくても、AP を展開して保護機能を実現できます。

wIPS ELM では、オフチャネルのアラームを検出する機能が制限されます。AP は定期的にオフチャネルになり、短い期間内での動作していないチャネルをモニタし、そのチャネルで攻撃を検出した場合はアラームをトリガーします。ただし、オフチャネルのアラーム検出はベストエフォートであり、攻撃を検出してアラームをトリガーするのは、これよりも時間がかかります。これが原因となって、ELM AP が断続的にアラームを検出しては（確認できないため）クリアする、という場合があります。上記のいずれのモードの AP も、ポリシー プロファイルに基づくアラームを Cisco WLC 経由で定期的に wIPS サービスに送信できます。wIPS サービスはアラームを格納および処理して、SNMP トラップを生成します。Cisco Prime Infrastructure は自身の IP アドレスをトラップの宛先として設定し、SNMP トラップを Cisco MSE から受信します。

次の表に SNMP トラップ制御とそれに対応するトラップを示します。トラップ制御が有効な場合、そのトラップ制御のトラップもすべて有効です。

（注） Cisco WLC は SNMP トラップの送信に SNMPv2 のみを使用します。

表 *131*：*SNMP* トラップ制御と対応トラップ

タブ名	トラップ制御	トラップ
General	Link (Port) Up/Down	linkUp、linkDown
	Spanning Tree	newRoot、topologyChange、stpInstanceNewRootTrap、stpInstanceTopologyChangeTrap
	Config Save	bsnDot11EssCreated、bsnDot11EssDeleted、bsnConfigSaved、ciscoLwappScheduledResetNotif、ciscoLwappClearResetNotif、ciscoLwappResetFailedNotif、ciscoLwappSysInvalidXmlConfig
AP	AP Register	bsnAPDisassociated、bsnAPAssociated
	AP Interface Up/Down	bsnAPIfUp、bsnAPIfDown
Client Traps	802.11 Association	bsnDot11StationAssociate
	802.11 Disassociation	bsnDot11StationDisassociate
	802.11 Deauthentication	bsnDot11StationDeauthenticate
	802.11 Failed Authentication	bsnDot11StationAuthenticateFail
	802.11 Failed Association	bsnDot11StationAssociateFail
	Exclusion	bsnDot11StationBlacklisted
	NAC Alert	cldcClientWlanProfileName、cldcClientIPAddress、cldcApMacAddress、cldcClientQuarantineVLAN、cldcClientAccessVLAN

タブ名	トラップ制御	トラップ
Security Traps	User Authentication	bsnTooManyUnsuccessLoginAttempts、cLWAGuestUserLoggedIn、cLWAGuestUserLoggedOut
	RADIUS Servers Not Responding	bsnRADIUSServerNotResponding、ciscoLwappAAARadiusReqTimedOut
	WEP Decrypt Error	bsnWepKeyDecryptError
	Rogue AP	bsnAdhocRogueAutoContained、bsnRogueApAutoContained、bsnTrustedApHasInvalidEncryption、bsnMaxRogueCountExceeded、bsnMaxRogueCountClear、bsnApMaxRogueCountExceeded、bsnApMaxRogueCountClear、bsnTrustedApHasInvalidRadioPolicy、bsnTrustedApHasInvalidSsid、bsnTrustedApIsMissing
	SNMP Authentication	agentSnmpAuthenticationTrapFlag
	Multiple Users	multipleUsersTrap
Auto RF Profile Traps	Load Profile	bsnAPLoadProfileFailed
	Noise Profile	bsnAPNoiseProfileFailed
	Interference Profile	bsnAPInterferenceProfileFailed
	Coverage Profile	bsnAPCoverageProfileFailed
Auto RF Update Traps	channel update	bsnAPCurrentChannelChanged
	Tx Power Update	bsnAPCurrentTxPowerChanged

タブ名	トラップ制御	トラップ
Mesh Traps	Child Excluded Parent	ciscoLwappMeshChildExcludedParent
	Parent Change	ciscoLwappMeshParentChange
	Authfailure Mesh	ciscoLwappMeshAuthorizationFailure
	Child Moved	ciscoLwappMeshChildMoved
	Excessive Parent Change	ciscoLwappMeshExcessiveParentChange
	Excessive Children	ciscoLwappMeshExcessiveChildren
	Poor SNR	ciscoLwappMeshAbateSNR、ciscoLwappMeshOnsetSNR
	Console Login	ciscoLwappMeshConsoleLogin
	Excessive Association	ciscoLwappMeshExcessiveAssociation
	Default Bridge Group Name	ciscoLwappMeshDefaultBridgeGroupName

次に、表「*SNMP* トラップ制御と対応トラップ」に記載されているトラップについて説明します。

- General トラップ
  - [SNMP Authentication]：SNMPv2 エンティティが、適切に認証されていないプロトコル メッセージを受信しました。

    （注） SNMP V3 モードで設定されているユーザが正しくないパスワードで Cisco WLC にアクセスを試みると、認証は失敗し、エラー メッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。

  - [Link (Port) Up/Down]：リンクのステータスは、アップまたはダウンから変更されます。
  - [Link (Port) Up/Down]：リンクのステータスは、アップまたはダウンから変更されます。
  - [Multiple Users]：2 人のユーザが同じ ID でログインします。
  - [Rogue AP]：不正アクセス ポイントが検出されるたびに、このトラップが MAC アドレスとともに送信されます。また、以前に検出された不正アクセス ポイントが存在しなくなっている場合にこのトラップが送信されます。
  - [Config Save]：Cisco WLC 設定が変更されると送信される通知。
- Cisco AP トラップ

- [AP Register]：アクセス ポイントが Cisco WLC と関連付けられるか関連付けが解除されると送信される通知。
- [AP Interface Up/Down]：アクセス ポイント インターフェイス（802.11X）の状態がアップまたはダウンになると送信される通知です。

- Client 関連トラップ
  - [802.11 Association]：クライアントが関連付けフレームを送信すると送信される関連付け通知。
  - [802.11 Disassociation]：クライアントが関連付け解除フレームを送信すると送信される関連付け解除通知。
  - [802.11 Deauthentication]：クライアントが認証解除フレームを送信すると送信される認証解除通知。
  - [802.11 Failed Authentication]：クライアントが成功以外のステータス コードの認証フレームを送信すると送信される認証エラー通知。
  - [802.11 Failed Association]：クライアントが成功以外のステータス コードのアソシエーション フレームを送信すると送信されるアソシエーション エラー通知。
  - [Exclusion]：クライアントが除外リスト（ブラックリスト）にある場合に送信される関連付け失敗通知。
  - [Authentication]：クライアントが正常に認証されると送信される認証通知。
  - [Max Clients Limit Reached]：[Threshold] フィールドに定義されていて Cisco WLC と関連付けられたクライアントが最大数に達すると送信される通知。
  - [NAC Alert]：クライアントが SNMP NAC 対応 WLAN に join する場合に送信されるアラート。

    この通知は、NAC 対応 SSID 上のクライアントがそのプレゼンスに関する情報を NAC アプライアンスに通知するための Layer2 認証を完了したときに生成されます。cldcClientWlanProfileName は、802.11 ワイヤレス クライアントが接続されている WLAN のプロファイル名を表します。cldcClientIPAddress は、クライアントの一意の IP アドレスを表します。cldcApMacAddress は、クライアントが関連付けられている AP の MAC アドレスを表します。cldcClientQuarantineVLAN は、クライアントの隔離 VLAN を表します。cldcClientAccessVLAN は、クライアントのアクセス VLAN を表します。
  - [Association with Stats]：クライアントが Cisco WLC と関連付けられる、またはローミングする場合に、データの統計情報とともに送信される関連付け通知。データの統計情報には、送受信されたパケット数およびバイト数が含まれます。
  - [Disassociation with Stats]：クライアントが Cisco WLC との関連付けを解除されるときに、データの統計情報とともに送信される関連付け解除通知。データの統計情報には、送受信されたパケット数およびバイト数、SSID、およびセッション ID が含まれます。

（注） 以降のリリースからリリース 7.4 にダウングレードする場合、リリース 7.4 でサポートされないトラップ（たとえば、NAC Alert トラップ）がダウングレード前に有効になっていると、すべてのトラップは無効になります。ダウングレードが終了したら、ダウングレード前に有効であったすべてのトラップを有効にする必要があります。他のすべてのトラップが無効にならないように、ダウングレードする前に新しいトラップを無効にすることをお勧めします。

- Security Traps
  - [User Auth Failure]：このトラップは、クライアントの RADIUS 認証の失敗が発生したことを通知します。
  - [RADIUS Server No Response]：このトラップは、RADIUS クライアントが送信した認証要求に応答する RADIUS サーバがないことを示します。
  - [WEP Decrypt Error]：Cisco WLC が WEP 復号化エラーを検出すると送信される通知。
  - [Rogue AP]：不正アクセス ポイントが検出されるたびに、このトラップが MAC アドレスとともに送信されます。また、以前に検出された不正アクセス ポイントが存在しなくなっている場合にこのトラップが送信されます。
  - [SNMP Authentication]：SNMPv2 エンティティが、適切に認証されていないプロトコル メッセージを受信しました。

    （注） SNMP V3 モードで設定されているユーザが正しくないパスワードで Cisco WLC にアクセスを試みると、認証は失敗し、エラー メッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。

  - [Multiple Users]：2 人のユーザが同じ ID でログインします。
- SNMP Authentication
  - [Load Profile]：[Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Noise Profile]：[Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Interference Profie]：[Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Coverage Profile]：[Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- Auto RF Profile Traps
  - [Load Profile]：[Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。

- [Noise Profile]：[Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Interference Profie]：[Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Coverage Profile]：[Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。

• Auto RF Update Traps

- [Channel Update]：アクセス ポイントの動的チャネル アルゴリズムが更新されると送信される通知。
- [Tx Power Update]：アクセス ポイントの動的送信電力アルゴリズムが更新されると送信される通知。

• Mesh Traps

- Child Excluded Parent：親メッシュ ノード経由での Cisco WLC に対する関連付けの失敗数が定義された回数に達すると送信される通知。
- 子メッシュ ノード数が検出応答タイムアウトのしきい値制限を超えると送信される通知。子メッシュ ノードが、定義された間隔で除外された親メッシュ ノードのアソシエーションを試行することはありません。子メッシュ ノードは、ネットワークに接続するときに、除外された親 MAC アドレスを記憶し、Cisco WLC に通知します。
- Parent Change：子メッシュ ノードがその親を変更すると、通知がエージェントによって送信されます。子メッシュ ノードは以前の親を記憶し、ネットワークに再度接続する際に、親の変更について Cisco WLC に通知します。
- Child Moved：親メッシュ ノードが子メッシュ ノードとの接続を失うと送信される通知。
- Excessive Parent Change：子メッシュ ノードが親を頻繁に変更すると送信される通知です。各メッシュ ノードは一定期間の親の変更回数のカウントを保持します。定義されたしきい値を超えると、子メッシュ ノードが Cisco WLC に通知します。
- Excessive Children：子の数が RAP および MAP に関して超過すると送信される通知。
- Poor SNR：子メッシュ ノードが、バックホール リンクでより低い SNR を検出すると送信される通知です。他のトラップの場合、子メッシュ ノードが、「clMeshSNRThresholdAbate」によって定義されるオブジェクトより高い SNR をバックホール リンクで検出すると、通知をクリアするための通知が送信されます。
- Console Login：MAP コンソールへのログインが成功するか、3 回の試行の後に失敗すると、エージェントによって通知が送信されます。
- Default Bridge Group Name：MAP メッシュ ノードがその親にデフォルトのブリッジ グループ名を使用して接続すると送信される通知。

（注） 上記以外のトラップにトラップ制御機能はありません。これらのトラップは、頻繁に生成されないので、トラップ制御は必要ありません。Cisco WLC によって生成される他のトラップは、オフにすることはできません。

（注） 上記のすべてのケースで、Cisco WLC は単なる転送デバイスとして機能します。

（注） MIB をダウンロードするには、ここをクリックしてください。

アクセス ポイントで wIPS を設定する方法

アクセス ポイントでの wIPS の設定（CLI）

手順の概要

1. **apname***name***mode***submodewips*
2. **end**
3. **showwirelesswpswipssummary**
4. **showwirelesswpswipsstatistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**apname***name***mode***submodewips* 例： スイッチ# **ap name ap1 mode local wips**	ローカルまたはモニタ モードに対してアクセス ポイントを設定し、wIPS にサブモードを設定します。
ステップ 2	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 3	**showwirelesswpswipssummary** 例： スイッチ# **show wireless wps wips summary**	アクセス ポイントで wIPS 設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	**showwirelesswpswipsstatistics** 例： スイッチ# **show wireless wps wips statistics**	wIPS 設定の現在のステートを表示します。

アクセス ポイントでの wIPS の設定（GUI）

ステップ 1 [Configuration] > [Wireless] > [Access Points] > [All APs] を選択します。
[All APs] ページおよび スイッチ と関連付けられたすべてのアクセス ポイントのリストが表示されます。

ステップ 2 wIPS を設定するアクセス ポイントの名前をクリックします。
[AP] > [Edit] ページが表示されます。

ステップ 3 [General] 領域で、[AP Mode] パラメータを設定します。wIPS 用のアクセス ポイントを設定するには、[AP Mode] ドロップダウン リストから次のモードのいずれかを選択します。

- Local
- Monitor

ステップ 4 [AP Sub Mode] ドロップダウン リストから [wIPS] を選択して、[AP Sub Mode] を wIPS に設定します。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save] をクリックします。

wIPS 情報のモニタリング

このセクションは、wIPS の新しいコマンドについて説明します。

以下のコマンドは、アクセス ポイント上で設定された wIPS をモニタするために使用できます。

表 *132*：*wIPS* コマンドのモニタリング

コマンド	目的
show wireless wps wips summary	アクセス ポイントで wIPS 設定を表示します。
show wireless wps wips statistics	wIPS 設定の現在のステートを表示します。

例：wIPS の設定

次に、AP1 上で wIPS を設定する例を示します。

```
スイッチ# ap name ap1 mode local submode wips
スイッチ# end
スイッチ# show wireless wps wips summary
```

wIPS の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
wIPS コマンド	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

wIPS 設定実行の機能履歴

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 78 章

侵入検知システムの設定

- 機能情報の確認，1875 ページ
- Intrusion Detection System について，1875 ページ
- 侵入検知システムを設定する方法，1876 ページ
- 侵入検知システムのモニタリング，1877 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

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

Intrusion Detection System について

Cisco Intrusion Detection System/Intrusion Prevention System（CIDS/IPS）は、特定のクライアントに関わる攻撃がレイヤ 3 ～ レイヤ 7 で検出されたとき、これらのクライアントによるワイヤレスネットワークへのアクセスをブロックするようスイッチに指示します。このシステムは、ワーム、スパイウェア/アドウェア、ネットワーク ウイルス、およびアプリケーションの不正使用などの脅威の検出、分類、阻止を支援することにより、強力なネットワーク保護を提供します。潜在的な攻撃を検出するには 2 つの方法があります。

- IDS センサー
- IDS シグニチャ

IDS センサーは、ネットワーク内のさまざまなタイプの IP レベルの攻撃を検出するように設定できます。センサーで攻撃が特定されたら、違反クライアントを回避（shun）するようスイッチに警告することができます。新規 IDS センサーが追加される場合、回避するクライアントのリストを取得するために スイッチ がセンサにクエリを発行できるように、IDS センサーを スイッチ と登録する必要があります。

IDS センサーは、疑わしいクライアントを検出すると、スイッチ にこのクライアントを回避するよう警告します。回避エントリは、同じモビリティ グループ内のすべての スイッチ に配信されます。回避すべきクライアントが現在、このモビリティ グループ内の スイッチ に join している場合、アンカー スイッチ はこのクライアントを動的除外リストに追加し、外部 スイッチ はクライアントを切り離します。次回、このクライアントが スイッチ に接続を試みた場合、アンカー スイッチ はハンドオフを拒否し、外部 スイッチ にクライアントを除外することを通知します。

侵入検知システムを設定する方法

IDS センサーの設定

手順の概要

1. **configure terminal**
2. **wireless wps cids-sensor** *index* [**ip-address** *ip-addr* **username** *username* **password** *password_type password*]
3. **wireless wps cids-sensor** *index*
4. [**default exit fingerprint interval no port shutdown**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless wps cids-sensor** *index* [**ip-address** *ip-addr* **username** *username* **password** *password_type password*] 例： `スイッチ(config)# wireless wps cids-sensor 2 231.1.1.1 admin pwd123`	内部インデックス番号を保持する IDS センサーを設定します。index パラメータは、コントローラで IDS センサーが検索される順序を決定します。コントローラでは最大 5 つの IDS センサーをサポートします。 • **ip-address**：（任意）IDS に IP アドレスを提供します。 • **username**：（任意）IDS のユーザ名を設定します。 • **password**：（任意）対応するユーザ名のパスワードを設定します。

	コマンドまたはアクション	目的
ステップ 3	**wireless wps cids-sensor** *index* 例： スイッチ(config)# **wireless wps cids-sensor 1**	IDS コンフィギュレーション サブモードを開始します。
ステップ 4	[**default exit fingerprint interval no port shutdown**] 例： スイッチ(config-cids-index)# **default**	さまざまな IDS パラメータを設定します。 • **default**：（任意）コマンドをデフォルトに設定します。 • **exit**：（任意）サブモードを終了します。 • **fingerprint**：（任意）センサーの TLS フィンガープリントを設定します。 • **interval**：（任意）センサーのクエリ間隔を設定します。範囲は 10 ～ 3600 秒です。 • **no**：（任意）コマンドを解除するか、デフォルトを設定します。 • **port**：（任意）センサーのポート番号を設定します。 • **shutdown**：（任意）侵入検知センサーをシャット ダウンします。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

侵入検知システムのモニタリング

表 *133*：ワイヤレス マルチキャストをモニタリングするためのコマンド

コマンド	説明
show wireless wps cids-sensor *index*	指摘されたインデックス値で IDS センサーの IDS 設定を表示します。
show wireless wps cids-sensor summary	すべての設定された IDS のリストを、インデックス、IP アドレス、ポート番号、インターバル値、ステータスおよびクエリなどの対応する値とともに表示します。

コマンド	説明
show wireless wps shun-list	IDS 回避リストを表示します。

第 XIII 部

スタック マネージャおよびハイ アベイラビリティ

- スイッチ スタックの管理，1881 ページ
- Cisco NSF with SSO の設定，1921 ページ
- ワイヤレスハイ アベイラビリティの設定，1937 ページ

第 79 章

スイッチ スタックの管理

- 機能情報の確認，1881 ページ
- スイッチ スタックの前提条件，1882 ページ
- スイッチ スタックの制約事項，1882 ページ
- スイッチ スタックに関する情報，1882 ページ
- スイッチ スタックの設定方法，1897 ページ
- スイッチ スタックのトラブルシューティング，1906 ページ
- スイッチ スタックのモニタリング，1908 ページ
- スイッチ スタックの設定例，1909 ページ
- スイッチ スタックに関する追加情報，1918 ページ

機能情報の確認

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

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

スイッチ スタックの前提条件

スイッチ スタック内のすべてのスイッチがアクティブ スイッチと同じライセンス レベルを実行している必要があります。ライセンス レベルについては、*System Management Configuration Guide*（*Catalyst 3650 Switches*）を参照してください。

スイッチスタック内のすべてのスイッチが互換性のあるソフトウェアバージョンを実行している必要があります。

スタック構成をイネーブルにするには、StackWise アダプタがスタッキング ポートに取り付けられている必要があります。スイッチ スタックのハードウェア要件については、*Catalyst 3650 Switch Hardware Installation Guide*を参照してください。

スイッチ スタックの制約事項

スイッチ スタック設定の制約事項を以下に示します。

- LAN Base ライセンス レベルを実行しているスイッチ スタックは、レイヤ 3 機能をサポートしません。
- スイッチ スタックは、StackWise-160 ポート経由で接続された最大 9 つのスタック対応スイッチで構成できます。
- スイッチ スタックに Catalyst 3850 スイッチと Catalyst 3650 スイッチを組み合わせて含めることはできません。
- スイッチスタックには、異なるライセンス レベルの組み合わせを含めることはできません。

スイッチ スタックに関する情報

スイッチ スタックの概要

スイッチ スタックは、StackWise-160 ポート経由で接続された最大 9 つのスタック対応スイッチで構成できます。スタック メンバーは 1 つの統合システムとして連携します。レイヤ 2 プロトコルとレイヤ 3 プロトコルが、スイッチ スタック全体を単一のエンティティとしてネットワークに提示します。

スイッチ スタックには、必ず 1 個のアクティブ スイッチおよび 1 個のスタンバイ スイッチがあります。アクティブ スイッチが使用不可能になった場合、スタンバイ スイッチがアクティブ スイッチの役割を担い、スタックは継続して動作します。

アクティブ スイッチがスイッチ スタックの動作を制御し、スタック全体の単一管理点になります。アクティブ スイッチから、以下を設定します。

- すべてのスタック メンバーに適用されるシステム レベル（グローバル）の機能
- スタック メンバーごとのインターフェイス レベルの機能

アクティブ スイッチには、スイッチ スタックの保存済みの実行コンフィギュレーション ファイルが格納されています。コンフィギュレーション ファイルには、スイッチ スタックのシステム レベルの設定と、スタック メンバーごとのインターフェイス レベルの設定が含まれます。各スタック メンバーは、バックアップ目的で、これらのファイルの現在のコピーを保持します。

スイッチ スタックでサポートされる機能

アクティブ スイッチ上でサポートされるシステムレベルの機能は、スイッチ スタック全体でサポートされます。

暗号化機能

アクティブ スイッチが暗号化ユニバーサル ソフトウェア イメージ（暗号化対応）を実行している場合は、スイッチ スタック上で暗号化機能を使用できます。

StackWise-160

スタック メンバーは、StackWise-160 テクノロジーを使用して、1 つの統合システムとして連携します。レイヤ 2 プロトコルとレイヤ 3 プロトコルは、スイッチ スタック全体をネットワーク内の単一のエンティティとしてサポートします。

（注） LAN Base イメージを実行しているスイッチ スタックは、レイヤ 3 機能をサポートしません。

StackWise-160 は、160 Gbps のスタック帯域幅で、ステートフル スイッチオーバー（SSO）を使用してスタック内に復元力を提供します。スタックは、メンバー スイッチが選出したアクティブ スイッチによって管理される単一のスイッチングユニットとして動作します。アクティブ スイッチによって、スタック内のスタンバイ スイッチが自動的に選出されます。アクティブ スイッチは、すべてのスイッチング、ルーティング、およびワイヤレスに関する情報を作成して更新し、この情報を継続的にスタンバイ スイッチと同期します。アクセス ポイントは、アクティブ スイッチに直接接続されていなければ、アクティブからスタンバイへのスイッチオーバー中に切断されることはありません。この場合、アクセス ポイントは電源がオフになって、リブートします。動作中のスタックは、サービスを中断せずに、新しいメンバーを追加したり、既存のメンバーを削除することができます。

スイッチ スタックのメンバーシップ

スタンドアロン スイッチは、アクティブ スイッチとしても動作するスタック メンバーを 1 つだけ持つスイッチ スタックです。スタンドアロン スイッチを別のスタンドアロン スイッチと接続すると、2 つのスタック メンバーで構成され、一方がアクティブ スイッチであるスイッチ スタックを構築できます。スタンドアロン スイッチを既存のスイッチ スタックに接続すると、スタック メンバーシップを増やすことができます。

すべてのスタック メンバーで hello メッセージが送受信されます。

- スタック メンバーが応答しない場合は、そのメンバーがスタックから削除されます。
- スタンバイ スイッチが応答しない場合は、新しいスタンバイ スイッチが選択されます。

- アクティブ スイッチが応答しない場合は、スタンバイ スイッチがアクティブ スイッチになります。

加えて、アクティブ スイッチとスタンバイ スイッチとの間でキープアライブ メッセージが送受信されます。

- スタンバイ スイッチが応答しない場合は、新しいスタンバイ スイッチが選択されます。
- アクティブ スイッチが応答しない場合は、スタンバイ スイッチがアクティブ スイッチになります。

スイッチ スタック メンバーシップの変更

スタック メンバを同一のモデルと交換した場合、新たなスイッチ（プロビジョニングされるスイッチとも呼びます）は交換されたスイッチと同じメンバ番号を使用すると、交換されたスイッチとまったく同じ設定で機能します。

アクティブ スイッチを削除したり、電源の入ったスタンドアロン スイッチまたはスイッチ スタックを追加したりしないかぎり、メンバーシップの変更中も、スイッチ スタックの動作は間断なく継続されます。

- 電源の入ったスイッチの追加（マージ）により、すべてのスイッチはリロードし、その中から新しいアクティブ スイッチを選定します。新しく選定されたアクティブ スイッチは、その役割と設定を保持します。他のすべてのスイッチは、個別のスタック メンバー番号を保持し、新しく選択されたアクティブ スイッチのスタック設定を使用します。
- 電源が入った状態のスタック メンバを取り外すと、スイッチ スタックが、それぞれ同じ設定を持つ2つ以上のスイッチ スタックに分割（パーティション化）されます。これにより、以下の現象が発生する可能性があります。
  - ネットワーク内での IP アドレスの競合。スイッチ スタックを分離されたままにしておきたい場合は、新しく作成されたスイッチ スタックの IP アドレス（複数の場合あり）を変更してください。
  - スタック内の 2 つのメンバー間の MAC アドレスの競合。**stack-mac update force** コマンドを使用すると、この競合を解消できます。

新しく作成されたスイッチ スタックにアクティブ スイッチまたはスタンバイ スイッチがない場合、スイッチ スタックはリロードし、新しいアクティブ スイッチを選定します。

（注） スイッチ スタックに追加または削除するスイッチの電源がオフであることを確認します。

スタック メンバーを追加または削除したら、スイッチ スタックがすべての帯域幅（160 Gbps）で動作していることを確認します。スタック モード LED が点灯するまで、スタック メンバの Mode ボタンを押します。スタック内のすべてのスイッチでは、右側の最後の 2 つのポート LED がグリーンに点灯します。スイッチ モデルに応じて、右側の最後の 2 つのポートは 10 ギガビット イーサネット ポートまたは Small Form-Factor Pluggable（SFP）モジュール ポート（10/100/1000 ポート）になります。スイッチの一方または両方の LED がグリーンでない場合、スタックは全帯域幅で稼働していません。

スタックを分割しないで、電源が入ったスタック メンバを取り外す場合、次の手順を実行します。

- 新規に作成されたスイッチ スタックのスイッチの電源をオフにします。
- それをそのスタック ポートを介して元のスイッチ スタックに再接続します。
- スイッチの電源を入れます。

スイッチ スタックに影響するケーブル配線と電源の考慮事項については、*Catalyst 3650 Switch Hardware Installation Guide* を参照してください。

スタック メンバー番号

スタック メンバー番号（1 ～ 9）は、スイッチ スタック内の各メンバーを識別します。また、メンバー番号によって、スタック メンバーが使用するインターフェイス レベルの設定が決定します。**show switch** EXEC コマンドを使用すると、スタック メンバー番号を表示できます。

新しい初期設定状態の スイッチ（スイッチ スタックに参加していないスイッチまたはスタック メンバー番号が手動で割り当てられていないスイッチ）は、デフォルト スタック メンバー番号 1 で出荷されます。そのスイッチがスイッチ スタックに参加すると、そのデフォルト スタック メンバー番号がスタック内で使用可能な最小メンバー番号に変更されます。

同じスイッチ スタック内のスタック メンバーが同じスタック メンバー番号を持つことはできません。スタンドアロン スイッチを含むすべてのスタック メンバーは、番号が手動で変更されるまで、または、その番号がスタック内の他のメンバーによってすでに使用されていないかぎり、独自のメンバー番号を保持します。

- **switch***current-stack-member-number***renumber***new-stack-member-number* コマンドを使用して手動でスタック メンバー番号を変更した場合は、その番号がスタック内の他のメンバーに割り当てられていないときにだけ、そのスタック メンバーのリセット後（または、**reload slot** *stack-member-number* 特権 EXEC コマンドの使用後）に、新たな番号が有効となります。スタック メンバー番号を変更するもう 1 つの方法は、スイッチ_NUMBER 環境変数を変更することです。

  番号がスタック内の他のメンバーによって使用されている場合は、スイッチがスタック内で使用可能な最小番号を選択します。

手動でスタック メンバーの番号を変更し、新たなメンバー番号にインターフェイス レベルの設定が関連付けられていない場合は、スタック メンバーをデフォルト設定にリセットします。

プロビジョニングされたスイッチ上では、**switch***current-stack-member-number***renumber***new-stack-member-number* コマンドを使用できません。使用すると、コマンドは拒否されます。

- スタック メンバーを別のスイッチ スタックに移動した場合、そのスタック メンバーは、自分の番号がスタック内の他のメンバーによって使用されていない場合にだけ、その番号を保持します。その番号が使用されている場合は、スイッチがスタック内で使用可能な最小番号を選択します。
- スイッチ スタックをマージした場合は、新しいアクティブ スイッチのスイッチ スタックに参加しているスイッチがスタック内で使用可能な最小番号を選択します。

ハードウェア インストレーション ガイドに記載されているように、スイッチ ポート LED をスタック モードで使用すれば、各スタック メンバーのスタック メンバー番号を目視で確認できます。

デフォルト モードでは、スタック マスターのスタック LED だけが緑色に点滅します。ただし、[MODE] ボタンを **[Stack]** オプションまでスクロールすると、すべてのスタック メンバのスタック LED が緑色に点灯します。

[MODE] ボタンが [Stack] オプションまでスクロールすると、各スタック メンバのスイッチ番号が、そのスイッチの最初の 5 つのポートの LED で表示されます。スイッチ番号は、すべてのスタック メンバで、バイナリ形式で表示されます。スイッチでは、オレンジ色の LED は値 0、緑の LED は値 1 を示します。

スイッチ番号 5（バイナリ 00101）の例：

スイッチ番号 5 のスタック メンバについては、最初の 5 つの LED が以下の色の組み合わせで点灯します。

- ポート 1：オレンジ
- ポート 2：オレンジ
- ポート 3：緑
- ポート 4：オレンジ
- ポート 5：緑

同様に、スイッチ番号に基づき、すべてのスタック メンバーで、最初の 5 つの LED がオレンジ色か緑色に点灯します。

（注）
- 水平スタック ポートを相手側の通常のネットワーク ポートに接続した場合、相手側から受信した SDP パケットがないと、スタック ポートの送受信は 30 秒以内に無効になります。
- スタック ポートはダウンしませんが、送受信だけ無効になります。次に示すログ メッセージがコンソールに表示されます。ピア側のネットワーク ポートがスタック ポートに変換されると、このスタック ポートの送受信が有効になります。

```
%STACKMGR-4-HSTACK_LINK_CONFIG: Verify peer stack port setting for
hstack StackPort-1 switch 5 (hostname-switchnumber)
```

スタック メンバーのプライオリティ値

スタック メンバのプライオリティ値が高いほど、アクティブ スイッチ として選択され、自分のスタック メンバ番号を保持できる可能性が高くなります。プライオリティ値は 1 ～ 15 の範囲で指定できます。デフォルトのプライオリティ値は 1 です。**show switch** EXEC コマンドを使用すると、スタック メンバーのプライオリティ値を表示できます。

（注） アクティブ スイッチにするスイッチには、最大プライオリティ値を割り当てることをお勧めします。これにより、再選択が実施されたときにそのスイッチがアクティブ スイッチとして再選択されることが保証されます。

スタック メンバのプライオリティ値を変更するには、**switch***stack-member-number***priority***new priority-value* コマンドを使用します。詳細については、「スタック メンバー プライオリティ値の設定」のセクションを参照してください。

新しいプライオリティ値はすぐに有効となりますが、現在の アクティブ スイッチ には影響しません。新たなプライオリティ値は、現在のアクティブ スイッチまたはスイッチ スタックのリセット時に、どのスタック メンバが新たな アクティブ スイッチ として選択されるかを決定する場合に影響を及ぼします。

スイッチ スタック ブリッジ ID と MAC アドレス

スイッチ スタックは、そのブリッジ *ID* によって、または、レイヤ 3 デバイスとして動作している場合はそのルータ MAC アドレスによって、ネットワーク内で識別されます。ブリッジ ID とルータ MAC アドレスは、アクティブ スイッチの MAC アドレスによって決定されます。

アクティブ スイッチが変わった場合は、新しいアクティブ スイッチの MAC アドレスによって、新しいブリッジ ID とルータ MAC アドレスが決定されます。

スイッチ スタック全体がリロードした場合は、スイッチ スタックがアクティブ スイッチの MAC アドレスを使用します。

スイッチ スタック上の永続的 MAC アドレス

永続的MACアドレス機能を使用すれば、スタックMACアドレスが変更されるまでの時間遅延を設定できます。この期間に、前のアクティブ スイッチがスタックに再参加すると、スイッチが現在はスタック メンバーで、アクティブ スイッチではない場合でも、スタックはその MAC アドレスをスタックMACアドレスとして使用し続けます。この期間に前のアクティブ スイッチがスタックに再参加しなかった場合は、スイッチ スタックが新しいアクティブ スイッチの MAC アドレスをスタック MAC アドレスとして取得します。デフォルトでは、新しいアクティブ スイッチが引き継ぐ場合でも、スタック MAC アドレスは最初のアクティブ スイッチの MAC アドレスになります。

また、スタック MAC アドレスが新しいアクティブ スイッチ MAC アドレスに変更されないように、スタック MAC の永続性を設定することもできます。

アクティブ スイッチとスタンバイ スイッチの選択と再選択

すべてのスタック メンバは、アクティブ スイッチまたはスタンバイ スイッチにすることができます。アクティブ スイッチが使用できなくなった場合、スタンバイ スイッチがアクティブ スイッチになります。

アクティブ スイッチは、次のイベントのいずれかが発生しないかぎり、役割を維持します。

- スイッチ スタックがリセットされた。
- アクティブ スイッチがスイッチ スタックから削除された。
- アクティブ スイッチがリセットされたか、電源が切れた。
- アクティブ スイッチに障害が発生した。
- 電源の入ったスタンドアロン スイッチまたはスイッチ スタックが追加され、スイッチ スタック メンバーシップが増えた。

アクティブスイッチは、次にリストした順番で、いずれかのファクタに基づいて選択または再選択されます。

1. 現在 アクティブ スイッチ であるスイッチ。
2. 最高のスタック メンバ プライオリティ値を持つスイッチ

（注） アクティブ スイッチ にしたいスイッチには、最高のプライオリティ値を割り当てることを推奨します。これにより、再選択が発生したときにそのスイッチを アクティブ スイッチ として選択させられます。

3. 起動時間が最短のスイッチ。
4. MAC アドレスが最小のスイッチ

（注） 新しいスタンバイ スイッチを選択または再選択する場合の要素は、アクティブ スイッチの選択または再選択の場合と同様で、アクティブ スイッチを除くすべての参加スイッチに適用されます。

選択後、新しいアクティブスイッチは数秒後に使用可能になります。その間、スイッチスタックはメモリ内の転送テーブルを使用してネットワークの中断を最小限に抑えます。新たなアクティブ スイッチが選択され、リセットされている間、他の使用可能なスタック メンバーの物理インターフェイスには何も影響はありません。

以前のアクティブスイッチが使用可能になっても、アクティブスイッチとしての役割を継続することはありません。

スイッチスタック全体の電源を入れるかリセットした場合、一部のスタックメンバがアクティブスイッチ選択に参加しない場合があります。同じ 2 分の間に電源が投入されたスタック メンバは、アクティブスイッチの選択に参加し、アクティブスイッチとして選択される可能性があります。120 秒間経過後に電源が投入されたスタック メンバは、この初回の選択には参加しないで、スタックメンバになります。アクティブスイッチの選択に影響する電源の注意事項については、スイッチのハードウェア インストレーション ガイドを参照してください。

ハードウェア インストレーション ガイドに記載されているとおり、スイッチの ACTV LED を使用して、そのスイッチがアクティブ スイッチかどうかを確認できます。

スイッチ スタックのコンフィギュレーション ファイル

アクティブ スイッチは、スイッチ スタックの保存された実行コンフィギュレーション ファイルを保持します。スタンバイスイッチは、自動的に、同期された実行コンフィギュレーションファイルを受け取ります。スタック メンバーは、実行コンフィギュレーション ファイルがスタートアップコンフィギュレーションファイルに保存された時点で同期されたコピーを受け取ります。アクティブスイッチが使用できなくなると、スタンバイスイッチが現行の実行コンフィギュレーションを引き継ぎます。

コンフィギュレーション ファイルには、次の設定情報が格納されています。

- すべてのスタック メンバーに適用される IP 設定、STP 設定、VLAN 設定、SNMP 設定などのシステム レベル（グローバル）のコンフィギュレーション設定
- スタック メンバーのインターフェイス固有のコンフィギュレーション設定：各スタック メンバーに固有

（注） 実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存せずにアクティブ スイッチを交換した場合は、アクティブ スイッチのインターフェイス固有の設定が保存されます。

スイッチ スタックに参加している新しい初期設定のままの スイッチは、そのスイッチ スタックのシステム レベルの設定を使用します。スイッチが電源をオンにする前に別のスイッチ スタック

に移動された場合、そのスイッチは保存されたコンフィギュレーション ファイルを失って、新しいスイッチ スタックのシステム レベルの設定を使用します。スイッチが新しいスイッチ スタックに参加する前にスタンドアロン スイッチとして電源をオンにされた場合は、スタックがリロードされます。スタックがリロードすると、新しいスイッチがアクティブ スイッチになって、そのコンフィグレーションを保持し、他のスタック メンバーのコンフィギュレーションファイルを上書きする可能性があります。

各スタック メンバーのインターフェイス固有のコンフィギュレーションには、スタック メンバー番号が関連付けられます。スタック メンバーは、番号が手動で変更された場合、または同じスイッチ スタック内の他のメンバーによってすでに使用されている場合以外は、自分の番号を保持します。スタック メンバーの番号を変更した場合は、そのスタック メンバーのリセット後に新しい番号が有効になります。

- そのメンバー番号に対応するインターフェイス固有のコンフィギュレーションが存在しない場合は、スタック メンバーはデフォルトのインターフェイス固有のコンフィギュレーションを使用します。
- そのメンバー番号に対応するインターフェイス固有のコンフィギュレーションが存在する場合は、スタック メンバーはそのメンバー番号に関連付けられたインターフェイス固有のコンフィギュレーションを使用します。

故障したメンバーを同一のモデルに交換すると、交換後のメンバーが、自動的に、故障したスイッチと同じインターフェイス固有のコンフィギュレーションを使用します。インターフェイス設定を再設定する必要はありません。交換後のスイッチ（プロビジョニングされたスイッチとも呼ばれる）には、故障したスイッチと同じスタック メンバー番号を割り当てる必要があります。

スタンドアロン スイッチのコンフィギュレーションの場合と同様に、スタック コンフィギュレーションをバックアップして復元します。

スタック メンバーを割り当てるためのオフライン設定

オフライン設定機能を使用すると、新しいスイッチがスイッチ スタックに参加する前に、スイッチに割り当て（設定を割り当て）できます。現在スタックに属していないスイッチに関連付けられたスタック メンバー番号、スイッチ タイプ、およびインターフェイスを設定できます。スイッチ スタックで作成した設定を割り当てられた設定と呼びます。スイッチ スタックに追加され、この設定を受信するスイッチを割り当てられたスイッチと呼びます。

switch *stack-member-number* **provision** *type* グローバル コンフィギュレーション コマンドにより、手動で設定を作成しプロビジョニングします。*stack-member-number* は、スタックに追加する前に、プロビジョニングされたスイッチ上で変更する必要があり、スイッチ スタック上の新しいスイッチ用に作成したスタック メンバー番号と一致する必要があります。割り当てられた設定内のスイッチ タイプは新しく追加したスイッチのスイッチ タイプと一致する必要があります。スイッチ スタックにスイッチを追加する場合に、割り当てられた設定が存在しないときは、割り当てられる設定が自動的に作成されます。

プロビジョニングされたスイッチに関連付けられているインターフェイスを設定すると、スイッチ スタックがその設定を受け入れ、実行コンフィギュレーションにその情報が表示されます。ただし、スイッチがアクティブでないため、インターフェイス上の設定が機能しないうえ、割り当

てられたスイッチに関連付けられたインターフェイスが特定の機能の表示には現れません。たとえば、プロビジョニングされたスイッチに関連付けられている VLAN 設定情報は、スイッチ スタック上の **show vlan** ユーザ EXEC コマンド出力に表示されません。

スイッチ スタックは、割り当てられたスイッチがスタックに属するかどうかに関係なく、実行コンフィギュレーションに割り当てられた設定を保持します。**copy running-config startup-config** 特権 EXEC コマンドを入力すると、プロビジョニングされた設定をスタートアップ コンフィギュレーション ファイルに保存できます。スタートアップ コンフィギュレーション ファイルでは、割り当てられたスイッチがスタックに属するかどうかに関係なく、スイッチ スタックは保存した情報をリロードして使用できます。

割り当てられたスイッチのスイッチ スタックへの追加による影響

プロビジョニングされたスイッチをスイッチ スタックに追加すると、スタックはプロビジョニングされた設定かデフォルト設定のどちらかを適用します。下の表に、スイッチ スタックが、プロビジョニングされた設定とプロビジョニングされたスイッチを比較するときに発生するイベントを示します。

表 *134*：プロビジョニングされた設定とプロビジョニングされたスイッチの比較結果

シナリオ		結果
スタック メンバー番号とスイッチ タイプが一致する場合。	**1** プロビジョニングされたスイッチのスタック メンバ番号と、スタックのプロビジョニングされた設定のスタック メンバ番号が一致する場合、かつ **2** プロビジョニングされたスイッチのスイッチ タイプと、スタック上でプロビジョニングされた設定内のスイッチ タイプが一致する場合。	スイッチ スタックは、プロビジョニングされた設定をプロビジョニングされたスイッチに適用し、スタックに追加します。

シナリオ		結果
スタック メンバー番号は一致するが、スイッチ タイプが一致しない場合。	1 プロビジョニングされたスイッチのスタック メンバ番号と、スタックのプロビジョニングされた設定のスタック メンバ番号が一致する場合、ただし 2 プロビジョニングされたスイッチのスイッチ タイプと、スタック上でプロビジョニングされた設定内のスイッチ タイプが一致しない場合。	スイッチ スタックは、デフォルト設定をプロビジョニングされたスイッチに適用し、スタックに追加します。 プロビジョニングされた設定は、新しい情報を反映するために変更されます。
プロビジョニングされた設定でスタック メンバ番号が検出されない		スイッチ スタックは、デフォルト設定をプロビジョニングされたスイッチに適用し、スタックに追加します。 プロビジョニングされた設定は、新しい情報を反映するために変更されます。
プロビジョニングされたスイッチのスタック メンバ番号が、プロビジョニングされた設定で検出されない		スイッチ スタックは、デフォルト設定をプロビジョニングされたスイッチに適用し、スタックに追加します。

プロビジョニングされた設定で指定されたのとは異なるタイプの、プロビジョニングされたスイッチを、電源が切られたスイッチ スタックに追加してから電源を供給すると、スイッチ スタックは、スタートアップ コンフィギュレーション ファイル内の（現在は不正な）**switch** *stack-member-number* **provision** *type* グローバル コンフィギュレーション コマンドを拒否します。ただし、スタックの初期化中は、スタートアップコンフィギュレーションファイルのデフォルトでないインターフェイス コンフィギュレーション情報が、（間違ったタイプの可能性がある）割り当てられたインターフェイス向けに実行されます。実際のスイッチ タイプと前にプロビジョニングされたスイッチ タイプの違いによって、拒否されるコマンドと、受け入れられるコマンドがあります。

（注） スイッチスタックに新しいスイッチのプロビジョニングされた設定が含まれていない場合は、スイッチがデフォルトのインターフェイス設定でスタックに参加します。その後で、スイッチスタックが、新しいスイッチと一致する **switch** *stack-member-number* **provision** *type* グローバル コンフィギュレーション コマンドで、その実行コンフィギュレーションに追加されます。設定情報については、「スイッチスタックへの新しいメンバーのプロビジョニング」のセクションを参照してください。

スイッチ スタックの割り当てられたスイッチの交換による影響

スイッチ スタック内の割り当てられたスイッチに障害が発生し、スタックから削除して別のスイッチと交換すると、スタックが割り当てられた設定またはデフォルト設定をそのスイッチに適用します。スイッチ スタックが割り当てられた設定と割り当てられたスイッチを比較するときに発生するイベントは、割り当てられたスイッチをスタックに追加するときに発生するものと同じです。

割り当てられたスイッチのスイッチ スタックからの削除による影響

割り当てられたスイッチをスイッチスタックから削除すると、削除されたスタック メンバーに関連付けられた設定は、割り当てられた情報として実行コンフィギュレーション内に残ります。設定を完全に削除するには、**no switch***stack-member-number* **provision** グローバル コンフィギュレーション コマンドを使用します。

互換性のないソフトウェアを実行しているスイッチのアップグレード

自動アップグレード機能と自動アドバイス機能を使用すれば、スイッチ スタックと互換性のないソフトウェア パッケージがインストールされたスイッチを互換性のあるバージョンのソフトウェアにアップグレードしてスイッチ スタックに参加できるようにすることができます。

自動アップグレード

自動アップグレード機能の目的は、スイッチを互換性のあるソフトウェア イメージにアップグレードしてスイッチ スタックに参加できるようにすることです。

新しいスイッチがスイッチスタックに参加しようとすると、各スタック メンバーがそれ自体と新しいスイッチの互換性チェックを実行します。各スタック メンバーは、アクティブ スイッチに互換性チェックの結果を送信し、その結果に基づいてスイッチがスイッチ スタックに参加できるかどうかが判断されます。新しいスイッチ上のソフトウェアがスイッチ スタックと互換性がない場合は、新しいスイッチがバージョン不一致（VM）モードに入ります。

新しいスイッチ上の自動アップグレード機能がイネーブルになっている場合は、アクティブ スイッチが、自動的に、互換性のあるスタック メンバー上で実行されているものと同じソフトウェア イメージで新しいスイッチをアップグレードします。自動アップグレードは、一致しないソフトウェアが検出された数分後に起動します。

自動アップグレードはデフォルトでディセーブルになっています。

自動アップグレードには自動コピー プロセスと自動抽出プロセスが含まれます。

- 自動コピーは、スタック メンバー上で実行しているソフトウェア イメージを新しいスイッチに自動的にコピーして、そのスイッチをアップグレードします。また、自動コピーは、自動アップグレードがイネーブルになっている場合、新しいスイッチ上に十分なフラッシュ メモリが存在する場合、およびスイッチ スタック上で実行しているソフトウェア イメージが新しいスイッチに適合する場合に実行されます。

（注） VMモードのスイッチでは、すべてのリリース済みのソフトウェアが稼働するとは限りません。たとえば、新しいスイッチ ハードウェアは以前のバージョンのソフトウェアでは認識されません。

- 自動抽出（auto-extract）は、自動アップグレード プロセスがスタック内で新しいスイッチにコピーする適切なソフトウェアを見つけられなかった場合に実行されます。この場合、自動抽出プロセスは、スイッチ スタックまたは新しいスイッチをアップグレードするために必要なbinファイルを、スタック内のすべてのスイッチで検索します。binファイルは、スイッチ スタックまたは新しいスイッチ内の任意のフラッシュ ファイル システムに配置できます。スタック メンバー上で新しいスイッチに適したbin ファイルが見つかった場合は、このプロセスがファイルを抽出して自動的に新しいスイッチをアップグレードします。

自動アップグレード機能は、バンドル モードで使用することはできません。スイッチ スタックは、インストール済みモードで実行する必要があります。スイッチスタックがバンドルモードになっている場合は、**software expand** 特権 EXEC コマンドを使用してインストール済みモードに変更します。

自動アップグレードをイネーブルにするには、新しいスイッチ上で **software auto-upgrade enable** グローバル コンフィギュレーション コマンドを使用します。自動アップグレードのステータスをチェックするには、**show running-config** 特権 EXEC コマンドを使用して表示された *Auto upgrade* 行を確認します。

新しいスイッチを特定のソフトウェア バンドルでアップグレードするように自動アップグレードを設定するには、**software auto-upgrade source url** グローバル コンフィギュレーション コマンドを使用します。ソフトウェア バンドルが無効になっている場合は、新しいスイッチは、互換性のあるスタック メンバー上で実行しているものと同じソフトウェア イメージでアップグレードされます。

自動アップグレード プロセスが完了すると、新しいスイッチがリロードして、完全に機能するメンバーとしてスタックに参加します。リロード時に両方のスタック ケーブルが接続されていれば、スイッチ スタックが 2 つのリング上で動作するため、ネットワークのダウンタイムが発生しません。

互換性のないソフトウェアを実行しているスイッチのアップグレードの詳細については、『*Cisco IOS File System, Configuration Files, and Bundle Files Appendix, Cisco IOS XE Release 3SE（Catalyst 3650 Switches）*』を参照してください。

自動アドバイス

自動アドバイス機能は次の場合に起動されます。

- 自動アップグレード機能がディセーブルになっている。
- 新しいスイッチがバンドルモードで、スタックがインストール済みモードになっている。自動アドバイスは、新しいスイッチをインストール済みモードに変更するための **software auto-upgrade** 特権 EXEC コマンドの使用に関する syslog メッセージを表示します。
- スタックがバンドルモードになっている。自動アドバイスは、新しいスイッチがスタックに参加できるようにするためのバンドルモードでの起動に関する syslog メッセージを表示します。
- 新しいスイッチが互換性のないソフトウェアを実行しているために、自動アップグレードの試みが失敗した。スイッチ スタックが新しいスイッチとの互換性チェックを実行した後に、自動アドバイスが、新しいスイッチが自動アップグレードできるかどうかに関する syslog メッセージを表示します。

自動アドバイスはディセーブルにできません。また、スイッチ スタック ソフトウェアと、バージョン不一致（VM）モードのスイッチのソフトウェアに同じライセンス レベルが含まれていない場合は提案を表示しません。

自動アドバイス メッセージの例

自動アップグレードがディセーブルになっており、互換性のないスイッチが参加しようとしている：例

この自動アドバイスのサンプル出力は、自動アップグレード機能がディセーブルになっており、互換性のないスイッチ 1 がスイッチ スタックに参加しようとした場合に表示されるシステム メッセージを示しています。

```
*Oct 18 08:36:19.379: %INSTALLER-6-AUTO_ADVISE_SW_INITIATED: 2 installer:  Auto advise
initiated for switch 1
*Oct 18 08:36:19.380: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  Searching stack for software
 to upgrade switch 1
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  Switch 1 with incompatible
 software has been
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  added to the stack. The
software running on
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  all stack members was
scanned and it has been
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  determined that the 'software
 auto-upgrade'
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  command can be used to
install compatible
*Oct 18 08:36:19.382: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  software on switch 1.
```

自動アップグレードがディセーブルになっており、新しいスイッチがバンドル モードで動作している：例

この自動アドバイスのサンプル出力は、自動アップグレードがディセーブルになっており、バンドル モードで動作しているスイッチがインストール済みモードで動作しているスタックに参加しようとした場合に表示されるシステム メッセージを示しています。

```
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW_INITIATED: 2 installer:  Auto advise
initiated for switch 1
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  Switch 1 running bundled
software has been added
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  to the stack that is running
 installed software.
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  The 'software auto-upgrade'
 command can be used to
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  convert switch 1 to the
installed running mode by
*Oct 18 11:09:47.005: %INSTALLER-6-AUTO_ADVISE_SW: 2 installer:  installing its running
software.
```

スイッチ スタックの管理接続

スイッチ スタックおよびスタック メンバ インターフェイスは、アクティブ スイッチを経由して管理します。CLI、SNMP、およびサポートされているネットワーク管理アプリケーション（CiscoWorks など）を使用できます。個別の スイッチ ごとにスタック メンバーを管理することはできません。

（注） SNMP を使用して、サポートされる MIB によって定義されるスタック全体のネットワーク機能を管理します。スイッチは、スタックのメンバーシップや選択などのスタック構成固有の機能を管理するための MIB をサポートしません。

特定のスタック メンバーへの接続

特定のスタック メンバ ポートを設定する場合は、CLI コマンド インターフェイス表記にスタック メンバ番号を含めてください。

スタンバイ スイッチをデバッグするには、**session standby ios** 特権 EXEC コマンドを使用してアクティブ スイッチからアクセスします。特定のスタック メンバをデバッグするには、アクティブなスイッチから **session switch***stack-member-number* 特権 EXEC コマンドを使用して、スタック メンバの診断シェルにアクセスします。特定のスタック メンバへの CLI セッションで使用できるのは、**show** コマンドと **debug** コマンドに限ります。

IP アドレスによるスイッチ スタックへの接続

スイッチ スタックは、単一 IP アドレスを介して管理されます。IP アドレスは、システムレベル設定であり、アクティブ スイッチやその他のスタック メンバー固有ではありません。スタックからアクティブ スイッチまたはその他のスタック メンバーを削除しても IP 接続があれば、そのまま同じ IP アドレスを使用してスタックを管理できます。

（注） スイッチ スタックからスタック メンバーを削除した場合、各スタック メンバーは自身の IP アドレスを保持します。したがって、ネットワーク内で同じ IP アドレスを持つ 2 つのデバイスが競合するのを避けるため、スイッチ スタックから削除したスイッチの IP アドレスを変更しておきます。

スイッチ スタック設定の関連情報については、「スイッチ スタックのコンフィギュレーション ファイル」のセクションを参照してください。

コンソール ポートまたはイーサネット管理ポートによるスイッチ スタックへの接続

アクティブ スイッチに接続するには、次のいずれかの方法を使用します。

- 1 つまたは複数のスタック メンバーのコンソール ポートを経由して、端末または PC をアクティブ スイッチに接続できます。
- 1 つまたは複数の スタック メンバーのイーサネット管理ポートを経由して、PC をアクティブ スイッチに接続できます。イーサネット管理ポート経由でスイッチ スタックに接続する方法については、「イーサネット管理ポートの使用」のセクションを参照してください。

1つまたは複数のスタック メンバのコンソール ポートを経由して、ターミナルまたはPCをスタック マスターに接続することで、アクティブ スイッチに接続できます。

アクティブ スイッチに複数の CLI セッションを使用する場合は注意が必要です。1 つのセッションで入力したコマンドは、別のセッションには表示されません。そのため、コマンドを入力したセッションを識別できなくなることがあります。

スイッチ スタックを管理する場合は、1 つの CLI セッションだけを使用することを推奨します。

スイッチ スタックの設定方法

永続的 MAC アドレス機能のイネーブル化

（注） この機能を設定するためにコマンドを入力すると、設定の結果を記述した警告メッセージが表示されます。この機能は慎重に使用してください。古い アクティブ スイッチ の MAC アドレスを同じドメイン内で使用すると、トラフィックが失われることがあります。

永続 MAC アドレスをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **stack-mac persistent timer** [**0** | *time-value*]
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**stack-mac persistent timer** [**0**	*time-value*] 例： スイッチ(config)# **stack-mac persistent timer 7**	アクティブ スイッチ変更からスタック MAC アドレスが新しいアクティブ スイッチのものに変更されるまでの遅延をイネーブルにします。この間に以前のアクティブ スイッチがスタックに再加入した場合、スタックはその MAC アドレスをスタック MAC アドレスとして使用します。 • 現在アクティブなスイッチの MAC アドレスを無期限に使用継続するには、値なしまたは値 **0** でコマンドを入力します。 • スタック MAC アドレスが新しいアクティブ スイッチの MAC アドレスに変更されるまでの時間を設定するには、*time-value* に 1 ～ 60 分の範囲内の値を入力します。 設定した時間が経過するまで、以前のアクティブ スイッチのスタック MAC アドレスが使用されます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

永続的 MAC アドレス機能をディセーブルにするには、**no stack-mac persistent timer** グローバル コンフィギュレーション コマンドを使用します。

スタック メンバー番号の割り当て

この任意の作業は、アクティブ スイッチ からのみ使用できます。

メンバー番号をスタック メンバーに割り当てるには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **switch***current-stack-member-number***renumber***new-stack-member-number*
4. **end**
5. **reload slot***stack-member-number*
6. **show switch**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**switch***current-stack-member-number***renumber***new-stack-member-number* 例： スイッチ(config)# **switch 3 renumber 4**	スタック メンバの現在のスタック メンバ番号と新たなスタック メンバ番号を指定します。指定できる範囲は 1 ～ 9 です。 スタック メンバの現在のスタック メンバ番号と新たなメンバ番号を指定します。指定できる範囲は 1 ～ 2 です。 **show switch** ユーザ EXEC コマンドを使用すると、現在のスタック メンバ番号を表示できます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**reload slot***stack-member-number* 例： スイッチ# **reload slot 4**	スタック メンバをリセットします。
ステップ 6	**show switch** 例： **show**スイッチ	スタック メンバ番号を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スタック メンバー プライオリティ値の設定

この任意の作業は、アクティブ スイッチ からのみ使用できます。

プライオリティ値をスタック メンバーに割り当てるには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **switch***stack-member-number***priority***new-priority-number*
4. **end**
5. **show switch** *stack-member-number*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**switch***stack-member-number***priority***new-priority-number* 例： スイッチ(config)# **switch 3 priority 2**	スタック メンバのスタック メンバ番号と、新しいプライオリティを指定します。スタック メンバ番号の有効範囲は 1 ～ 9 です。プライオリティ値の範囲は 1 ～ 15 です。 **show switch** ユーザ EXEC コマンドを使用して、現在のプライオリティ値を表示できます。 新しいプライオリティ値はすぐに有効となりますが、現在の アクティブ スイッチ には影響しません。新たなプライオリティ値は、現在の アクティブ スイッチ またはスイッチ スタックのリセット時に、どのスタック メンバが新たな アクティブ スイッチ として選択されるかを決定する場合に影響を及ぼします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show switch** *stack-member-number* 例： スイッチ(config)# **show switch**	スタック メンバー プライオリティ値を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ スタックへの新しいメンバーのプロビジョニング

この任意の作業は、アクティブ スイッチ からのみ使用できます。

手順の概要

1. **show switch**
2. **configure terminal**
3. **switch***stack-member-number***provision** *type*
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show switch** 例： スイッチ# **show switch**	スイッチ スタックに関する要約情報を表示します。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**switch***stack-member-number***provision** *type* 例： スイッチ(config)# **switch 3 provision WS-xxxx**	事前に設定されたスイッチのスタック メンバー番号を指定します。デフォルトでは、スイッチはプロビジョニングされません。 *Stack-member-number* の範囲は 1 ～ 9 です。スイッチ スタック内でまだ使用されていないスタック メンバー番号を指定します。ステップ 1 を参照してください。 *Type* には、コマンドライン ヘルプ ストリングに示されたサポート対象のスイッチのモデル番号を入力します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

割り当てられたスイッチ情報の削除

開始する前に、スタックから割り当てられたスイッチを削除する必要があります。この任意の作業は、アクティブ スイッチ からのみ使用できます。

手順の概要

1. **configure terminal**
2. **no switch** *stack-member-number* **provision**
3. **end**
4. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no switch** *stack-member-number* **provision** 例： スイッチ(config)# **no switch 3 provision**	指定されたメンバーの割り当て情報を削除します。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のように設定されたスタック内の割り当てられたスイッチを削除する場合：

- スタックは 4 つのメンバーを持つ
- スタック メンバー 1 がアクティブ スイッチである
- スタック メンバー 3 が割り当てられたスイッチである

さらに、割り当てられた情報を削除し、エラー メッセージを受信しないようにするには、スタック メンバー 3 の電源を切り、スタック メンバー 3 とそれが接続されているスイッチとの間の StackWise-160 ケーブルを抜き、そのケーブルを別のメンバー間に再接続して、**no switch** *stack-member-number* **provision** グローバル コンフィギュレーション コマンドを入力します。

スイッチ スタック内の非互換スイッチの表示

手順の概要

1. **show switch**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show switch** 例： スイッチ# **show switch**	スイッチ スタック内の非互換スイッチを表示します（[Current State] が [V-Mismatch] で表示されます）。[V-Mismatch] 状態は、非互換ソフトウェアのスイッチを示します。アクティブ スイッチ と同じライセンス レベルで実行されていないスイッチには、[Lic-Mismatch] と出力表示されます ライセンス レベルの管理については、*System Management Configuration Guide*（*Catalyst 3650 Switches*）を参照してください。

スイッチ スタックでの互換性のないスイッチのアップグレード

手順の概要

1. **software auto-upgrade**
2. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**software auto-upgrade** 例： スイッチ# **software auto-upgrade**	スイッチ スタック内の互換性のないスイッチをアップグレードします。または、バンドル モードのスイッチをインストール済みモードに変更します。
ステップ 2	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ スタックのトラブルシューティング

スタック メンバーの診断コンソールへのアクセス

はじめる前に

このオプション タスクは、アクティブ スイッチのみから使用できます。

手順の概要

1. **session switch** *stack-member-number*
2. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**session switch** *stack-member-number* 例： スイッチ# **session switch 2**	アクティブ スイッチからスタック メンバーの診断シェルにアクセスします。
ステップ 2	**exit** 例： スイッチ(diag)> **exit**	アクティブ スイッチ上の CLI セッションに戻ります。

スタック ポートの一時的なディセーブル化

スタック ポートでフラッピングが発生し、スタック リングが不安定になっている場合に、そのポートをディセーブルにするには、**switch** *stack-member-number* **stack port** *port-number* **disable** 特権 EXEC コマンドを入力します。ポートを再びイネーブルにするには、**switch** *stack-member-number* **stack port** *port-number* **enable** コマンドを入力します。

（注） **switch** *stack-member-number* **stack port** *port-number* **disable** コマンドの使用には注意が必要です。スタック ポートをディセーブルにすると、スタックは半分の帯域幅で稼働します。

スタック ポートを通じてすべてのメンバーが接続されており、準備完了状態であれば、スタックはフルリング状態です。

次の現象が発生すると、スタックが部分リング状態になります。

- すべてのメンバがスタック ポートを通じて接続されたが、一部が ready ステートではない。
- スタック ポートを通じて接続されていないメンバーがある。

手順の概要

1. **switch***stack-member-number* **stack port** *port-number* **disable**
2. **switch***stack-member-number* **stack port** *port-number* **enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**switch***stack-member-number* **stack port** *port-number* **disable** 例： スイッチ# **switch 2 stack port 1 disable**	指定されたポートをディセーブルにします。
ステップ 2	**switch***stack-member-number* **stack port** *port-number* **enable** 例： スイッチ# **switch 2 stack port 1 enable**	スタック ポートを再びイネーブルにします。

スタックがフルリング状態のときにスタック ポートをディセーブルにしようとする場合は、1 つのスタック ポートしかディセーブルにすることができません。次のメッセージが表示されます。

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

スタックが部分リング状態のときにスタック ポートをディセーブルにしようとしても、そのポートをディセーブルにすることができません。次のメッセージが表示されます。

```
Disabling stack port not allowed with current stack configuration.
```

他のメンバーの起動中のスタック ポートの再イネーブル化

スイッチ 1 のポート 1 がスイッチ 4 のポート 2 に接続されています。ポート 1 でフラッピングが発生した場合は、**switch 1 stack port 1 disable** 特権 EXEC コマンドを使用してポート 1 をディセーブルにすることができます。スイッチ 1 のポート 1 がディセーブルになっており、スイッチ 1 の

電源がまだオンになっている状態でスタック ポートを再びイネーブルにするには、次の手順を実行します。

ステップ 1 スイッチ 1 のポート 1 とスイッチ 4 のポート 2 の間のスタック ケーブルを取り外します。

ステップ 2 スタックからスイッチ 4 を取り外します。

ステップ 3 スイッチを追加してスイッチ 4 を交換し、スイッチ番号 4 を割り当てます。

ステップ 4 スイッチ 1 のポート 1 とスイッチ 4（交換後のスイッチ）のポート 2 の間のケーブルを再接続します。

ステップ 5 スイッチ間のリンクを再びイネーブルにします。**switch 1 stack port 1 enable** 特権 EXEC コマンドを入力して、スイッチ 1 のポート 1 をイネーブルにします。

ステップ 6 スイッチ 4 の電源を入れます。

注意 スイッチ 1 のポート 1 をイネーブルにする前にスイッチ 4 の電源を入れると、スイッチのいずれかがリロードされる場合があります。

最初にスイッチ 4 の電源を入れると、リンクを起動するために **switch 1 stack port 1 enable** および **switch 4 stack port 2 enable** 特権 EXEC コマンドを入力する必要がある場合があります。

スイッチ スタックのモニタリング

表 *135*：スタック情報を表示するコマンド

コマンド	説明
show switch	割り当てられたスイッチやバージョン不一致モードのスイッチのステータスなど、スタックに関するサマリー情報を表示します。
show switch*stack-member-number*	特定のメンバーに関する情報を表示します。
show switch detail	スタックに関する詳細情報を表示します。
show switch neighbors	スタック ネイバーを表示します。
show switch stack-ports [**summary**]	スタックのポート情報を表示します。

コマンド	説明
show redundancy	冗長システムと現在のプロセッサ情報を表示します。冗長システムの情報にはシステム稼働時間、スタンバイ失敗、スイッチオーバー理由、ハードウェア、設定冗長モードおよび動作冗長モードが含まれます。表示される現在のプロセッサ情報にはアクティブ位置、ソフトウェアの状態、現在の状態での稼働時間などが含まれます。
show redundancy state	アクティブおよびスタンバイ スイッチの冗長状態をすべて表示します。

スイッチ スタックの設定例

スイッチ スタックの設定のシナリオ

これらのスイッチ スタック設定シナリオのほとんどが、少なくとも2つのスイッチがStackWise-160ポート経由で接続されていることを前提とします。

表 *136*：設定シナリオ

シナリオ		結果
既存のアクティブ スイッチによって明確に決定されるアクティブ スイッチ選択	StackWise-160 ポート経由で 2 つの電源の入ったスイッチ スタックを接続します。	2つのアクティブ スイッチのうち1つだけが新しいアクティブ スイッチになります。
スタック メンバーのプライオリティ値によって明確に決定されるアクティブ スイッチ選択	**1** StackWise-160 ポート経由で 2 つのスイッチを接続します。 **2** **switch***stack-member-number* **priority** *new-priority-number* グローバル コンフィギュレーション コマンドを使用して、一方のスタック メンバにより高いメンバ プライオリティ値を設定します。 **3** 両方のスタック メンバーを同時に再起動します。	より高いプライオリティ値を持つスタック メンバーがアクティブ スイッチに選択されます。

シナリオ		結果
コンフィギュレーション ファイルによって明確に決定されるアクティブ スイッチ選択	両方のスタック メンバーが同じプライオリティ値を持つものと仮定します。 **1** 一方つのスタック メンバーがデフォルトのコンフィギュレーションを持ち、他方のスタック メンバーが保存済み（デフォルトでない）のコンフィギュレーション ファイルを持つことを確認します。 **2** 両方のスタック メンバーを同時に再起動します。	保存済みのコンフィギュレーション ファイルを持つスタック メンバーがアクティブ スイッチに選択されます。
MAC アドレスによって明確に決定されるアクティブ スイッチ選択	両方のスタック メンバーが同じプライオリティ値、コンフィギュレーション ファイル、フィーチャ セットを持っていると仮定して、両方のスタック メンバーを同時に再起動します。	MAC アドレスが小さい方のスタック メンバーがアクティブ スイッチに選択されます。
スタック メンバー番号の競合	一方のスタック メンバーが他方のスタック メンバーより高いプライオリティ値を持つものと仮定します。 **1** 両方のスタック メンバーが同じスタック メンバー番号を持つように確認します。必要に応じて、*switch current-number renumber new-number* グローバル コンフィギュレーション コマンドを使用します。 **2** 両方のスタック メンバーを同時に再起動します。	より高いプライオリティ値を持つスタック メンバーが、自分のスタック メンバー番号を保持します。もう一方のスタック メンバーは、新たなスタック メンバー番号を持ちます。

シナリオ		結果
スタック メンバーの追加	1 新しいスイッチの電源を切ります。 2 StackWise-160 ポート経由で、新しいスイッチを電源の入ったスイッチ スタックに接続します。 3 新しいスイッチの電源を入れます。	アクティブ スイッチが保持されます。新たなスイッチがスイッチ スタックに追加されます。
アクティブ スイッチの障害	アクティブ スイッチを取り外します（または電源をオフにします）。	残りのスタック メンバーのいずれかが新しいスタック マスターになります。スタック内の他のすべてのスタック メンバーは、スタック メンバーのままで、再起動はされません。
9台を超えるスタック メンバーの追加	1 StackWise-160 ポート経由で、10スイッチ を接続します。 2 すべてのスイッチの電源をオンにします。	2台のスイッチがアクティブ スイッチになります。1台のアクティブ スイッチが9台のスタック メンバーで構成されます。その他のアクティブ スイッチはスタンドアロン スイッチとして残ります。 アクティブ スイッチのスイッチとそれぞれのアクティブ スイッチに属しているスイッチを識別するには、スイッチ上のModeボタンとポートLEDを使用します。

永続的 MAC アドレス機能のイネーブル化：例

次に、永続的 MAC アドレス機能に 7 分の遅延時間を設定し、設定を確認する例を示します。

```
スイッチ(config)# stack-mac persistent timer 7
  WARNING: The stack continues to use the base MAC of the old Master
  WARNING: as the stack MAC after a master switchover until the MAC
  WARNING: persistency timer expires. During this time the Network
  WARNING: Administrators must make sure that the old stack-mac does
  WARNING: not appear elsewhere in this network domain. If it does,
  WARNING: user traffic may be blackholed.
  スイッチ(config)# end
  スイッチ# show switch
```

```
Switch/Stack Mac Address : 0016.4727.a900
Mac persistency wait time: 7 mins
                                             H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Active 0016.4727.a900     1      P2B     Ready
```

スイッチ スタックへの新しいメンバーのプロビジョニング：例

次に、スタック メンバー番号2が設定されたスイッチをスイッチ スタックに割り当てる例を示します。 **show running-config** コマンドの出力は、プロビジョニングされたスイッチに関連付けられたインターフェイスを示します。

```
スイッチ(config)# switch 2 provision switch_PID
  スイッチ(config)# end
  スイッチ# show running-config | include switch 2
  !
  interface GigabitEthernet2/0/1
  !
  interface GigabitEthernet2/0/2
  !
  interface GigabitEthernet2/0/3
  <output truncated>
```

show switch stack-ports summary コマンドの出力：例

スタック メンバ2のポート1だけがディセーブルです。

```
スイッチ# show switch stack-ports summary
  スイッチ#/  Stack   Neighbor   Cable     Link   Link   Sync      #         In
   Port#     Port               Length     OK   Active   OK    Changes   Loopback
             Status                                          To LinkOK
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1     OK         3      50 cm     Yes    Yes    Yes        1        No
    1/2     Down      None    3 m       Yes    No     Yes        1        No
    2/1     Down      None    3 m       Yes    No     Yes        1        No
    2/2     OK         3      50 cm     Yes    Yes    Yes        1        No
    3/1     OK         2      50 cm     Yes    Yes    Yes        1        No
    3/2     OK         1      50 cm     Yes    Yes    Yes        1        No
```

表 *137*：*show switch stack-ports summary* コマンドの出力

フィールド	説明
Switch#/Port#	メンバー番号と、そのスタック ポート番号

フィールド	説明
Stack Port Status	スタック ポートのステータス。 • Absent：スタック ポートにケーブルが検出されません。 • Down：ケーブルは検出されましたが、接続されたネイバーがアップになっていないか、スタック ポートがディセーブルになっています。 • OK：ケーブルが検出され、接続済みのネイバーが起動しています。
Neighbor	スタック ケーブルの接続先の、アクティブなメンバーのスイッチの数。
Cable Length	有効な長さは 50 cm、1 m、または 3 m です。 スイッチがケーブルの長さを検出できない場合は、値は *no cable* になります。ケーブルが接続されていないか、リンクが信頼できない可能性があります。
Link OK	スタック ケーブルが接続され機能しているかどうか。相手側には、接続されたネイバーが存在する場合も、そうでない場合もあります。 リンク パートナーは、ネイバー スイッチ上のスタック ポートのことです。 • No：このポートに接続されているスタック ケーブルがないか、スタック ケーブルが機能していません。 • Yes：このポートには正常に機能するスタック ケーブルが接続されています。
Link Active	スタック ケーブル相手側にネイバーが接続されているかどうか。 • No：相手側にネイバーが検出されません。ポートは、このリンクからトラフィックを送信できません。 • Yes：相手側にネイバーが検出されました。ポートは、このリンクからトラフィックを送信できます。

フィールド	説明
Sync OK	リンク パートナーが、スタック ポートに有効なプロトコル メッセージを送信するかどうか。 • No：リンク パートナーからスタック ポートに有効なプロトコル メッセージが送信されません。 • Yes：リンクの相手側は、ポートに有効なプロトコル メッセージを送信します。
# Changes to LinkOK	リンクの相対的安定性。 短期間で多数の変更が行われた場合は、リンクのフラップが発生することがあります。
In Loopback	スタック ケーブルがメンバのスタック ポートに接続されているかどうか。 • No：メンバーの 1 つ以上のスタック ポートに、スタック ケーブルが接続されています。 • Yes：メンバーのどのスタック ポートにも、スタック ケーブルが接続されていません。

ソフトウェア ループバック：例

メンバーが 3 つのスタックでは、スタック ケーブルですべてのメンバーが接続されます。

```
スイッチ# show switch stack-ports summary
  スイッチ#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync   #Changes   In
            Status            Length    OK    Active  OK     To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------   --------
    1/1     OK         3      50 cm     Yes    Yes    Yes        1        No
    1/2     OK         2      3 m       Yes    Yes    Yes        1        No
    2/1     OK         1      3 m       Yes    Yes    Yes        1        No
    2/2     OK         3      50 cm     Yes    Yes    Yes        1        No
    3/1     OK         2      50 cm     Yes    Yes    Yes        1        No
    3/2     OK         1      50 cm     Yes    Yes    Yes        1        No
```

スイッチ 1 のポート 1 からスタック ケーブルを切断すると、次のメッセージが表示されます。

```
01:09:55: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 3 has changed to state DOWN
  01:09:56: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 1 has changed to state DOWN

  スイッチ# show switch stack-ports summary
  スイッチ#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
```

```
          Status            Length    OK    Active  OK    To LinkOK  Loopback

--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     Absent    None    No cable  No     No     No         1        No
  1/2     OK          2     3 m       Yes    Yes    Yes        1        No
  2/1     OK          1     3 m       Yes    Yes    Yes        1        No
  2/2     OK          3     50 cm     Yes    Yes    Yes        1        No
  3/1     OK          2     50 cm     Yes    Yes    Yes        1        No
  3/2     Down      None    50 cm     No     No     No         1        No
```

スイッチ 1 のポート 2 からスタック ケーブルを切断すると、スタックが分割されます。

スイッチ 2 とスイッチ 3 がスタック ケーブルで接続された 2 メンバー スタックのメンバーになります。

```
スイッチ# show sw stack-ports summary
  スイッチ#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    2/1     Down      None    3 m       No     No     No         1        No
    2/2     OK          3     50 cm     Yes    Yes    Yes        1        No
    3/1     OK          2     50 cm     Yes    Yes    Yes        1        No
    3/2     Down      None    50 cm     No     No     No         1        No
```

スイッチ 1 はスタンドアロン スイッチです。

```
スイッチ# show switch stack-ports summary
  スイッチ#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1     Absent    None    No cable  No     No     No         1        Yes
    1/2     Absent    None    No cable  No     No     No         1        Yes
```

スタック ケーブルが接続されたソフトウェア ループバック：例

- スイッチ 1 のポート 1 のポート ステータスが *Down* で、ケーブルが接続されています。

  スイッチ 1 のポート 2 のポート ステータスが *Absent* で、ケーブルが接続されていません。

  ```
  スイッチ# show switch stack-ports summary
    スイッチ#
   Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
              Status            Length    OK    Active  OK    To LinkOK  Loopback
    --------  ------  --------  --------  ----  ------  ----  ---------  --------
      1/1     Down      None    50 Cm     No     No     No         1        No
      1/2     Absent    None    No cable  No     No     No         1        No
  ```

- 物理ループバックでは、ケーブルはスタック ポートとスイッチの両方に接続されています。この設定を使用して、次のテストを行えます。

  - 正常に稼働しているスイッチのケーブル
  - 正常なケーブルを使用したスタック ポート

  ```
  スイッチ# show switch stack-ports summary
    スイッチ#
   Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
              Status            Length    OK    Active  OK    To LinkOK  Loopback
    --------  ------  --------  --------  ----  ------  ----  ---------  --------
  ```

```
  2/1       OK       2      50 cm     Yes    Yes    Yes       1         No
  2/2       OK       2      50 cm     Yes    Yes    Yes       1         No
```

ポート ステータスを見ると、次のことがわかります。

- スイッチ 2 はスタンドアロン スイッチである。
- ポートはトラフィックを送受信できる。

スタック ケーブルが接続されていないソフトウェア ループバック：例

```
スイッチ# show switch stack-ports summary
  スイッチ#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1     Absent    None    No cable   No     No     No       1         Yes
    1/2     Absent    None    No cable   No     No     No       1         Yes
```

切断されたスタック ケーブルの特定：例

すべてのスタック メンバーは、スタック ケーブルで接続されます。スイッチ 1 のポート 2 と、スイッチ 2 のポート 1 が接続されます。

次に、メンバーのポート ステータスを示します。

```
スイッチ# show switch stack-ports summary
  スイッチ#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1     OK         2      50 cm     Yes    Yes    Yes       0         No
    1/2     OK         2      50 cm     Yes    Yes    Yes       0         No
    2/1     OK         1      50 cm     Yes    Yes    Yes       0         No
    2/2     OK         1      50 cm     Yes    Yes    Yes       0         No
```

スイッチ 1 のポート 2 からケーブルを切断すると、次のメッセージが表示されます。

```
%STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 2 has changed to state DOWN

  %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 1 has changed to state DOWN
```

ポート ステータスは以下の通りです。

```
  スイッチ# show switch stack-ports summary
  スイッチ#
 Sw#/Port#  Port    Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status            Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1       OK       2      50 cm     Yes    Yes    Yes       1         No
    1/2     Absent    None    No cable   No     No     No       2         No
    2/1      Down     None    50 cm      No     No     No       2         No
    2/2       OK       1      50 cm     Yes    Yes    Yes       1         No
```

ケーブルの片方だけが、スタック ポート（スイッチ 2 のポート 1）に接続されます。

- スイッチ 1 のポート 2 の *Stack Port Status* 値は *Absent* で、スイッチ 2 のポート 1 の値は *Down* です。
- *Cable Length* 値は *No cable* です。

問題の診断

- スイッチ 1 のポート 2 のケーブル接続を確認します。
- スイッチ 1 のポート 2 が次の状態であれば、ポートまたはケーブルに問題があります。
  - *In Loopback* 値が *Yes* である。

  または
  - *Link OK*、*Link Active*、または *Sync OK* 値が *No* である。

スタック ポート間の不安定な接続の修正：例

すべてのメンバーは、スタック ケーブルで接続されます。スイッチ 1 のポート 2 と、スイッチ 2 のポート 1 が接続されます。

ポート ステータスは次のとおりです。

```
スイッチ# show switch stack-ports summary
  スイッチ#
 Sw#/Port#  Port     Neighbor  Cable     Link  Link    Sync  #Changes   In
            Status             Length    OK    Active  OK    To LinkOK  Loopback
  --------  ------  --------  --------  ----  ------  ----  ---------  --------
    1/1       OK       2      50 cm     Yes    Yes    Yes       1          No
    1/2      Down     None    50 cm      No     No     No       2          No
    2/1      Down     None    50 cm      No     No     No       2          No
    2/2       OK       1      50 cm     Yes    Yes    Yes       1          No
```

問題の診断

- Stack Port Status の値が *Down* になっています。
- Link OK、Link Active、および Sync OK の値が *No* になっています。
- Cable Length の値が *50 cm* になっています。スイッチがケーブルを検出し、正しく識別しています。

スイッチ 1 のポート 2 と、スイッチ 2 のポート 1 との接続は、少なくとも 1 つのコネクタ ピンで不安定になっています。

スイッチ スタックに関する追加情報

関連資料

関連項目	マニュアル タイトル
スイッチ スタックのケーブル配線と電源供給。	*Catalyst 3650 Switch Hardware Installation Guide* http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960cx_3650cx/hardware/installation/guide/b_2960cx-3560cx_hig.html

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

第 80 章

Cisco NSF with SSO の設定

- 機能情報の確認，1921 ページ
- NSF with SSO の前提条件，1921 ページ
- NSF with SSO の制約事項，1922 ページ
- NSF with SSO に関する情報，1922 ページ
- Cisco NSF with SSO の設定方法，1929 ページ

機能情報の確認

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

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

NSF with SSO の前提条件

NSF with SSO の前提条件と考慮事項を次に示します。

- ルーティング プロトコルの使用には IP Services ライセンス レベルが必要です。ルーティング用 EIGRP スタブおよび OSPF は、IP Base ライセンス レベルでサポートされます。
- NSF の BGP サポートでは、ネイバー ネットワーキング デバイスが NSF 認識である必要があります。つまり、デバイスにはグレースフル リスタート機能があり、セッション確立中に OPEN メッセージ内でこの機能をアドバタイズする必要があります。NSF 対応ルータが特定の BGP ネイバーにグレースフル リスタート機能がないことを検出すると、NSF 対応セッショ

ンをそのネイバーと確立しません。グレースフル リスタート機能のある他のすべてのネイバーは、この NSF 対応ネットワーキング デバイスと NSF 対応セッションを継続します。

- OSPF NSF では、すべてのネイバー ネットワーキング デバイスが NSF を認識する必要があります。NSF 対応ルータが特定のネットワーク セグメントで NSF 非認識ネイバーを検出すると、そのセグメントで NSF 機能をディセーブルにします。NSF 対応または NSF 認識ルータで完全に構成された他のネットワーク セグメントに対しては、継続して NSF 機能を提供します。

NSF with SSO の制約事項

NSF with SSO の制約事項を次に示します。

- NSF 機能は、IPv4 ルーティング プロトコルに対してのみサポートされます。NSF 機能は、IPv6 ルーティング プロトコルに対してはサポートされません。
- IP マルチキャスト ルーティングは SSO を認識しないため、NSF はサポートされません。
- NSF は、IOS-XE ソフトウェアが LAN Base モードで動作している場合は、サポートされません。
- NSF が動作するには、SSO をデバイス上に設定する必要があります。
- NSF/SSO は、IP バージョン 4 トラフィックおよびプロトコルのみをサポートします。IPv6 トラフィックはサポートしていません。
- グレースフル リスタート機能をサポートするためには、すべてのレイヤ 3 のネイバー デバイスが NSF Helper または NSF 対応である必要があります。
- IETF の場合、すべてのネイバー デバイスで NSF 認識ソフトウェア イメージが実行されている必要があります。

NSF with SSO に関する情報

NSF with SSO の概要

スイッチでは、アクティブ スイッチが使用できなくなった場合にスタンバイ スイッチが処理を引き継ぐようにすることで、障害耐性をサポートします。Cisco Nonstop Forwarding（NSF）は、ステートフル スイッチオーバー（SSO）と連動して、ネットワークを使用できない時間を最小限に抑えます。

NSF には次の利点があります。

- ネットワークのアベイラビリティの向上：NSF は、ユーザのセッション情報がスイッチオーバー後も維持されるように、ネットワーク トラフィックとアプリケーションのステート情報を転送し続けます。

- ネットワーク全体の安定性：ネットワークの安定性は、ネットワーク内でルータに障害が発生し、ルーティング テーブルが失われたときに作成されるルート フラップの数を減らすことで改善できます。
- 隣接ルータはリンク フラップを検出しません。インターフェイスはスイッチオーバーの間アップ状態のままなので、隣接ルータはリンク フラップを検出しません（リンクがダウンして、アップに戻ることはありません）。
- ルーティング フラップの回避：SSO がスイッチオーバー時にネットワーク トラフィックを転送し続けるので、ルーティング フラップが回避されます。
- スイッチオーバーの前に確立したユーザ セッションを維持します。

アクティブ スイッチとスタンバイ スイッチ間でキープアライブ メッセージが送受信されます。

- スタンバイ スイッチが応答しない場合は、新しいスタンバイ スイッチが選択されます。
- アクティブ スイッチが応答しない場合は、スタンバイ スイッチがアクティブ スイッチになります。

加えて、すべてのスタック メンバーで hello メッセージが送受信されます。

- スタック メンバーが応答しない場合は、そのメンバーがスタックから削除されます。
- スタンバイ スイッチが応答しない場合は、新しいスタンバイ スイッチが選択されます。
- アクティブ スイッチが応答しない場合は、スタンバイ スイッチがアクティブ スイッチになります。

SSO の動作

スタンバイ スイッチは、SSO モードで稼働する場合、完全に初期化されたステートで起動し、アクティブ スイッチの固定コンフィギュレーションおよび実行コンフィギュレーションと同期化します。そのあと、スタンバイ スーパーバイザエンジンは、次のプロトコルのステートを維持し、ステートフル スイッチオーバーをサポートする機能に関するハードウェアおよびソフトウェア ステートの変更すべてを同期化して維持します。そのため、冗長アクティブ スイッチ構成内のレイヤ 2 セッションへの割り込みは最小限になります。

アクティブ スイッチに障害が発生した場合、スタンバイ スイッチがアクティブ スイッチになります。この新しいアクティブ スイッチは既存のレイヤ2スイッチング情報を使用して、トラフィック転送を続けます。ルーティングテーブルが新しいアクティブ スイッチに追加されるまで、レイヤ 3 の転送は延期されます。

（注） SSO は、IOS-XE ソフトウェアが LAN Base ライセンス レベルで動作している場合は、サポートされません。

次の機能のステートは、アクティブ スイッチとスタンバイ スイッチの間で保存されます。

- 802.3

- 802.3u
- 802.3x（フロー制御）
- 802.3ab（GE）
- 802.3z（CWDM を含めたギガビット イーサネット）
- 802.3ad（LACP）
- 802.1p（レイヤ 2 QoS）
- 802.1q
- 802.1X（認証）
- 802.1D（スパニングツリー プロトコル）
- 802.3af（インライン パワー）
- PAgP
- VTP
- ダイナミック ARP インスペクション
- DHCP スヌーピング
- IP ソース ガード
- IGMP スヌーピング（バージョン 1 および 2）
- DTP（802.1Q および ISL）
- MST
- PVST+
- Rapid PVST
- PortFast/UplinkFast/BackboneFast
- BPDU ガードおよびフィルタリング
- 音声 VLAN
- ポート セキュリティ
- ユニキャスト MAC フィルタリング
- ACL（VACL、PACL、RACLS）
- QoS（DBL）
- マルチキャスト ストーム制御/ブロードキャストストーム制御

SSO は、次の機能と互換性があります。ただし、次の機能のプロトコル データベースはスタンバイ スイッチとアクティブ スイッチの間で同期されません。

- レイヤ 2 プロトコル トンネリング（L2PT）を備えた 802.1Q トンネリング

- ベビー ジャイアント
- ジャンボ フレーム サポート
- CDP
- フラッディング ブロック
- UDLD
- SPAN/RSPAN
- NetFlow

スイッチ上のすべてのレイヤ 3 プロトコルは、SSO がイネーブルにされている場合、スタンバイ スイッチで学習されます。

NSF の動作

Cisco IOS ノンストップ フォワーディング（NSF）は常にステートフル スイッチオーバー（SSO）とともに実行され、レイヤ 3 トラフィックの冗長性を確保します。NSF は、ルーティングについては BGP、OSPF、EIGRP ルーティング プロトコルでサポートされ、転送についてはシスコ エクスプレス フォワーディング（CEF）でサポートされています。ルーティング プロトコルでは NSF 機能および認識機能が拡張されました。これは、プロトコルを稼働するルータがスイッチオーバーを検出でき、ネットワーク トラフィックを転送し続け、ピアデバイスからのルート情報を回復するのに必要なアクションを実行できることを意味します。

ルーティング プロトコルがルーティング情報ベース（RIB）テーブルを再作成している間、それぞれのプロトコルは、CEF に依存してスイッチオーバー中にパケットの転送を続行します。ルーティング プロトコルが収束したあと、CEF は FIB テーブルを更新し、失効したルート エントリを削除します。次に、CEF は新しい FIB 情報でハードウェアを更新します。

アクティブ スイッチが BGP（**graceful-restart** コマンドを使用）、OSPF、または EIGRP ルーティング プロトコル用に設定されている場合、ルーティング更新は、アクティブ スイッチが選択されている間、自動的に送信されます。

スイッチは、IP Services ライセンス レベルでは BGP、OSPF および EIGRP プロトコルについて NSF 認識および NSF 機能をサポートし、IP Base ライセンス レベルでは EIGRP スタブについて NSF 認識をサポートします。

NSF は 2 つの主要な要素で構成されています。

- NSF 認識

  ネットワーキング デバイスが NSF 互換ソフトウェアを実行している場合、このデバイスは NSF 認識です。アクティブ スイッチ選択が発生していても NSF ルータがまだパケットを転送可能なことを隣接ルータ デバイスが検出する機能を NSF 認識といいます。レイヤ 3 ルーティング プロトコル（BGP、OSPF、EIGRP）に対する Cisco IOS 拡張機能は、CEF ルーティング テーブルが時間切れにならないように、または NSF ルータがルートをドロップしないように、ルート フラッピングを防ぐよう設計されています。NSF 認識ルータは、ルーティング プロトコル情報をネイバー NSF ルータに送信します。NSF 認識は、EIGRP スタブ、EIGRP、

OSPF プロトコルに対してはデフォルトでイネーブルになります。NSF 認識は BGP に対してデフォルトではディセーブルに設定されています。

- NSF 機能

  NSF をサポートするようにデバイスを設定した場合にデバイスは NSF 対応になります。NSF 認識ネイバーまたは NSF 対応ネイバーからルーティング情報を再構築します。NSF は SSO と連動して IP パケットを転送し続けることにより、アクティブ スイッチ選択のあとのレイヤ 3 ネットワークを利用できない時間を最小限にします。レイヤ 3 ルーティング プロトコル（BGP、OSPFv2、EIGRP）の再コンバージェンスは、ユーザが意識する必要がなく、バックグラウンドで自動的に実行されます。ルーティング プロトコルはネイバー デバイスから情報を回復し、シスコ エクスプレス フォワーディング（CEF）テーブルを再構築します。

（注） NSF は IPv6 をサポートしておらず、サポートしているのは IPv4 ユニキャストだけです。

Cisco Express Forwarding; シスコ エクスプレス フォワーディング

Cisco IOS ノンストップ フォワーディング（NSF）の重要な要素は、パケット転送です。シスコ製のネットワーキング デバイスでは、パケット転送はシスコ エクスプレス フォワーディング（CEF）によって実行されます。CEF は FIB を維持し、スイッチオーバー時に最新だった FIB 情報を使用して、スイッチオーバー中のパケットの転送を続行します。この機能により、スイッチオーバー中のトラフィックの中断を短くします。

通常の NSF 操作中に、アクティブなスーパバイザ スイッチ上の CEF は、現在の FIB と隣接データベースを、スタンバイ スイッチ上の FIB と隣接データベースと同期させます。スイッチオーバー時に、スタンバイ スイッチは最初 FIB と、アクティブ スイッチでカレントだったもののミラーイメージである隣接データベースを備えています。CEF はスタンバイ スイッチ上の転送エンジンに、アクティブ スイッチの CEF によって送信される変更を維持します。転送エンジンは、インターフェイスおよびデータ パスが使用可能になりしだい、スイッチオーバー後も転送を継続できます。

ルーティング プロトコルがプレフィックス単位で RIB を再び読み込み始めるため、CEF に対してプレフィックス単位のアップデートが行われます。CEF はこれを使用して FIB と隣接データベースを更新します。既存エントリと新規エントリには、最新であることを示す新しいバージョン（「エポック」）番号が付けられます。転送エンジンでは、コンバージェンス中に転送情報が更新されます。RIB が収束すると、スイッチが信号通知を行います。ソフトウェアは、現在のスイッチオーバー エポックよりも前のエポックを持った FIB および隣接エントリをすべて削除します。これで FIB は最新のルーティング プロトコル転送情報を表示するようになります。

BGP の動作

NSF 対応ルータは BGP ピアで BGP セッションを開始し、OPEN メッセージをピアへ送信します。メッセージに含まれるものは、NSF 対応デバイスに「グレースフル」リスタート機能があるステートメントです。グレースフル リスタートは、BGP ルーティング ピアがスイッチオーバーのあとに

ルーティング フラップが発生するのを防ぐメカニズムです。BGP ピアがこの機能を受信した場合、メッセージを送信するデバイスがNSF対応であることを認識しています。NSF対応ルータ ピアおよびBGP ピアは両方ともセッションの確立時に、OPEN メッセージ内でグレースフル リスタート機能を交換する必要があります。両方のピアがグレースフル リスタート機能を示すステートメントを交換しない場合、このセッションでグレースフル リスタートは行われません。

BGP セッションがアクティブ スイッチのスイッチオーバー中に中断された場合、NSF 認識 BGP ピアがNSF 対応ルータに関連するルートすべてを失効としてマーキングしますが、一定期間の転送先を決定するためにこれらのルートを使用し続けます。この機能は、新しいアクティブ スイッチがBGP ピアでルーティング情報のコンバージェンスを待っている間に、パケットが失われないようにします。

アクティブ スイッチのスイッチオーバーが発生した後、NSF対応ルータはBGPピアとのセッションを再確立します。新しいセッションの確立時に、NSF 対応ルータが再起動したことを識別する新しいグレースフル リスタート メッセージを送信します。

この時点で、ルーティング情報は 2 つの BGP ピアの間で交換されます。交換が完了すると、NSF対応デバイスはルーティング情報を使用して新しい転送情報を持った RIB および FIB で更新されます。NSF認識デバイスはネットワーク情報を使用して、失効ルートをBGPテーブルから削除します。その後 BGP プロトコルが完全に収束されます。

BGP ピアがグレースフル リスタート機能をサポートしていない場合、OPEN メッセージ内のグレースフル リスタート機能は無視されますが、NSF 対応デバイスとの BGP セッションは確立します。この機能により、NSF非認識（つまりNSF機能のない）BGP ピアとの相互運用が可能になりますが、NSF 非認識 BGP ピアとの BGP セッションではグレースフル リスタートは使用できません。

（注） NSF の BGP サポートでは、ネイバー ネットワーキング デバイスが NSF 認識である必要があります。つまり、デバイスにはグレースフル リスタート機能があり、セッション確立中にOPENメッセージ内でこの機能をアドバタイズする必要があります。NSF対応ルータが特定のBGP ネイバーにグレースフル リスタート機能がないことを検出すると、NSF 対応セッションをそのネイバーと確立しません。グレースフル リスタート機能のある他のすべてのネイバーは、この NSF 対応ネットワーキング デバイスと NSF 対応セッションを継続します。

OSPF の動作

OSPFNSF対応ルータがアクティブ スイッチのスイッチオーバーを実行する場合、ルータはOSPFネイバーとリンク ステートデータベースを再同期化するため、次の作業を行う必要があります。

- ネイバー関係をリセットしないで、ネットワーク上で利用できる OSPF ネイバーを再学習します。
- ネットワークのリンク ステート データベース内容を再取得します。

NSF 対応ルータは、アクティブ スイッチのスイッチオーバーの後できるだけ迅速に、ネイバーNSF 認識デバイスに OSPF NSF 信号を送信します。ネイバー ネットワーキング デバイスは、このルータとのネイバー関係をリセットしてはならないインジケータとしてこの信号を認識します。

NSF 対応ルータがネットワーク上の他のルータから信号を受信すると、ネイバー リストの再構築を始めます。

ネイバー関係が再構築されると、NSF 対応ルータはすべての NSF 認識ネイバーとデータベースの再同期化を始めます。この時点でルーティング情報は OSPF ネイバーの間で交換されます。交換が完了すると、NSF 対応デバイスはルーティング情報を使用して、失効ルートを削除し、RIB を更新して、新しい転送情報で FIB を更新します。その後、OSPF プロトコルは完全に収束されます。

（注） OSPF NSF では、すべてのネイバー ネットワーキング デバイスが NSF を認識する必要があります。NSF 対応ルータが特定のネットワーク セグメントで NSF 非認識ネイバーを検出すると、そのセグメントで NSF 機能をディセーブルにします。NSF 対応または NSF 認識ルータで完全に構成された他のネットワーク セグメントに対しては、継続して NSF 機能を提供します。

EIGRP の動作

EIGRP NSF 対応ルータが NSF 再起動後に最初に再起動したときには、ネイバーはなくトポロジ テーブルは空です。ルータはインターフェイスを確立してネイバーを再取得し、トポロジとルーティング テーブルを再構築する必要があるときに、スタンバイ（今はアクティブ）スイッチから通知を受けます。再起動ルータおよびピアは、再起動ルータへのデータ トラフィック転送を中断することなく、次の作業を実行する必要があります。EIGRP ピア ルータは再起動ルータから学習したルートを維持し、NSF 再起動プロセスを介してトラフィックを転送し続けます。

ネイバーによって隣接関係がリセットされないように、再起動するルータは再起動を示すために EIGRP パケット ヘッダーの新しい再起動（RS）ビットを使用します。RS ビットは、NSF 再起動中に hello パケットと初期 INIT アップデート パケットに設定されます。Hello パケットの RS ビットを使用すると、ネイバーにすばやく NSF 再起動を通知できます。RS ビットを参照しない場合、ネイバーは INIT アップデートの受信、または Hello ホールド タイマーの期限切れによってリセットされた隣接関係を検出します。RS ビットを使用しない場合、ネイバーは、リセットされた隣接関係を NSF または通常の起動方法を使用して処理する必要があるかどうか認識できません。

hello パケットまたは INIT パケットを受信することでネイバーが再起動の知らせを受信すると、ピア リスト内で再起動したピアを見つけ、再起動しているルータとの隣接関係を維持します。ネイバーはトポロジー テーブルを、最初のアップデート パケットに設定された RS ビットのある再起動ルータに送信します。このパケットは NSF 認識であり、再起動ルータに役立つことを示しています。ネイバーは NSF 再起動ネイバーでない場合、Hello パケットに RS ビットを設定しません。

（注） ルータが NSF を認識できていても、コールド スタートで起動されたために NSF 再起動ネイバーを支援しない場合もあります。

1 つ以上のピア ルータが NSF 認識の場合、再起動ルータはアップデートを受信してからデータベースを再構築します。再起動ルータは Routing Information Base（RIB）に通知できるように収束したかどうかを認識する必要があります。各 NSF 認識ルータは、End of Table（EOT）内容を表示

するために、最新アップデートパケットのEOTマーカーを送信する必要があります。再起動ルータはEOTマーカーを受信すると、収束したことを認識します。再起動ルータはアップデートの送信を開始できます。

NSF認識ピアは、再起動ルータからEOT表示を受信したときに再起動ルータが収束した時間を認識します。その後ピアはトポロジー テーブルをスキャンして、送信元として再起動されたネイバーを持ったルートを検索します。ピアはルートタイムスタンプと再起動イベントタイムスタンプを比較し、ルートがまだ利用できるかどうかを判断します。ピアはアクティブになり、再起動したルータを介して利用できなくなったルート用に代替パスを検索します。

再起動ルータがすべてのEOT表示をネイバーから受信した場合、またはNSF収束タイマーが満了した場合、EIGRPはRIBにコンバージェンスを通知します。EIGRPはRIBコンバージェンス信号を待ってから、トポロジーテーブルを待機中のNSF認識ピアすべてにフラッディングします。

Cisco NSF with SSO の設定方法

SSO の設定

あらゆるサポート対象プロトコルを持ったNSFを使用するには、SSOを設定する必要があります。

手順の概要

1. **redundancy**
2. **mode sso**
3. **end**
4. **show running-config**
5. **show redundancy states**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**redundancy** 例： `スイッチ(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ2	**mode sso** 例： `スイッチ(config-red)# mode sso`	SSOを設定します。このコマンドにより、スタンバイ スイッチが再起動され、SSOモードで機能を開始します。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： スイッチ(config-red)# **end**	EXEC モードに戻ります。
ステップ 4	**show running-config** 例： スイッチ# **show running-config**	SSOがイネーブルになっていることを確認します。
ステップ 5	**show redundancy states** 例： スイッチ# **show redundancy states**	動作中の冗長モードを表示します。

SSO の設定例

次に、SSO 対応としてシステムを設定し、冗長ステートを表示する例を示します。

```
スイッチ(config)# redundancy
  スイッチ(config)# mode sso
  スイッチ(config)# end
  スイッチ# show redundancy states
  my state = 13 -ACTIVE
  peer state = 8 -STANDBY HOT
  Mode = Duplex
  Unit = Primary
  Unit ID = 5
  Redundancy Mode (Operational) = sso
  Redundancy Mode (Configured) = sso
  Split Mode = Disabled
  Manual Swact = Enabled
  Communications = Up
  client count = 29
  client_notification_TMR = 30000 milliseconds
  keep_alive TMR = 9000 milliseconds
  keep_alive count = 1
  keep_alive threshold = 18
  RF debug mask = 0x0
```

CEF NSF の確認

CEF NSF を確認するには、**show cef state** 特権 EXEX コマンドを使用します。

```
スイッチ# show cef state
CEF Status:
RP instance
common CEF enabled
IPv4 CEF Status:
CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
universal per-destination load sharing algorithm, id DEA83012
```

```
IPv6 CEF Status:
CEF disabled/not running
dCEF disabled/not running
universal per-destination load sharing algorithm, id DEA83012
RRP state:
I am standby RRP: no
RF Peer Presence: yes
RF PeerComm reached: yes
RF Progression blocked: never
Redundancy mode: rpr(1)
CEF NSF sync: disabled/not running
CEF ISSU Status:
FIBHWIDB broker
No slots are ISSU capable.
FIBIDB broker
No slots are ISSU capable.
FIBHWIDB Subblock broker
No slots are ISSU capable.
FIBIDB Subblock broker
No slots are ISSU capable.
Adjacency update
No slots are ISSU capable.
IPv4 table broker
No slots are ISSU capable.
CEF push
No slots are ISSU capable.
```

NSF の BGP の設定

BGP NSF に参加しているピア デバイスすべてに BGP グレースフル リスタートを設定する必要があります。

手順の概要

1. **configure terminal**
2. **router bgp as-number**
3. **bgp graceful-restart**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp as-number** 例： `スイッチ(config)# router bgp 300`	BGP ルーティング プロセスをイネーブルにして、スイッチをスイッチ コンフィギュレーション モードにします。
ステップ 3	**bgp graceful-restart** 例： `スイッチ(config)# bgp graceful-restart`	BGP グレースフル リスタート機能をイネーブルにし、BGP NSF を開始します。BGP セッションが確立されたあとでこのコマンドを入力した場合、BGP ネイバーと交換する機能のセッ

	コマンドまたはアクション	目的
		ションを再開する必要があります。再起動スイッチとすべてのピアでこのコマンドを入力します。

BGP NSF の確認

BGP の NSF を確認するには、BGP のグレースフル リスタートが SSO 対応ネットワーキング デバイスとネイバー デバイスに設定されているかどうかを確認する必要があります。確認する手順は、次のとおりです。

ステップ 1 **show running-config** コマンドを入力して、「bgp graceful-restart」が SSO 対応スイッチの BGP 設定に表示されていることを確認します。

例：

```
スイッチ# show running-config
.
.
.
router bgp 120
.
.
.
bgp graceful-restart
neighbor 192.0.2.0 remote-as 300
.
.
.
```

ステップ 2 各 BGP ネイバーでステップ 1 を繰り返します。

ステップ 3 SSO デバイスおよびネイバー デバイスで、グレースフル リスタート機能がアドバタイズおよび受信されたことを示していることを確認し、グレースフル リスタート機能を備えたアドレス ファミリであることを確認します。アドレス ファミリが表示されていない場合、BGP NSF も発生しません。

例：

```
スイッチ# show ip bgp neighbors
BGP neighbor is 192.0.2.3, remote AS 1, internal link
BGP version 4, remote router ID 192.0.2.4
BGP state = Established, up for 00:02:38
Last read 00:00:38, last write 00:00:35, hold time is 180, keepalive interval is 60
seconds
Neighbor capabilities:
Route refresh: advertised and received(new)
Address family IPv4 Unicast: advertised and received
Message statistics:
InQ depth is 0
OutQ depth is 0
Sent Rcvd
Opens: 1 1
Notifications: 0 0
Updates: 0 0
Keepalives: 4 4
```

```
Route Refresh: 0 0
Total: 5 5
Default minimum time between advertisement runs is 0 seconds
.....................................................
(Remaining output deleted)
```

OSPF NSF の設定

OSPF NSF に参加しているすべてのピア デバイスは OSPF NSF を認識できるようにする必要があります。NSF ソフトウェア イメージをデバイスにインストールすれば自動的に認識するようになります。

手順の概要

1. **configure terminal**
2. **router ospf***processID*
3. **nsf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ(config)# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf***processID* 例： スイッチ(config)# **router ospf *processID***	OSPF ルーティング プロセスをイネーブルにして、スイッチをルータ コンフィギュレーション モードにします。
ステップ 3	**nsf** 例： スイッチ(config)# **nsf**	OSPF 用に NSF 動作をイネーブルにします。

OSPF NSF の確認

ステップ 1 show running-config コマンドを入力して、「nsf」が SSO 対応デバイスの OSPF 設定に表示されていることを確認します。

例：

```
スイッチ(config)#show running-config
route ospf 120
log-adjacency-changes
nsf
network 192.0.2.0 192.0.2.255 area 0
network 192.0.2.1 192.0.2.255 area 1
network 192.0.2.2 192.0.2.255 area 2
.
.
.
```

ステップ 2 **show ip ospf** コマンドを入力して、デバイス上で NSF がイネーブルであることを確認します。

例：

```
スイッチ show ip ospf
Routing Process "ospf 1" with ID 192.0.2.1
Start time: 00:02:07.532, Time elapsed: 00:39:05.052
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
transit capable is 0
External flood list length 0
IETF Non-Stop Forwarding enabled
restart-interval limit: 120 sec
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
Number of interfaces in this area is 3 (1 loopback)
Area has no authentication
SPF algorithm last executed 00:08:53.760 ago
SPF algorithm executed 2 times
Area ranges are
Number of LSA 3. Checksum Sum 0x025BE0
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

EIGRP NSF の設定

手順の概要

1. **configure terminal**
2. **router eigrp***as-number*
3. **nsf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp***as-number* 例： スイッチ(config)# **router eigrp** *as-number*	EIGRP ルーティング プロセスをイネーブルにして、スイッチをルータ コンフィギュレーション モードにします。
ステップ 3	**nsf** 例： スイッチ(config-router)# **nsf**	EIGRP NSF をイネーブルにします。 「再起動」スイッチとすべてのピアでこのコマンドを入力します。

EIGRP NSF の確認

ステップ 1 **show running-config** コマンドを入力して、「nsf」が SSO 対応デバイスの EIGRP 設定に表示されていることを確認します。

例：

```
スイッチ show running-config
..
.
router eigrp 100
auto-summary
nsf
..
.
```

ステップ 2 **show ip protocols** コマンドを入力して、デバイス上で NSF がイネーブルであることを確認します。

例：

```
スイッチ show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.0.2.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 1
Routing for Networks:
Routing on Interfaces Configured Explicitly (Area 0):
Loopback0
GigabitEthernet5/3
```

```
TenGigabitEthernet3/1
Routing Information Sources:
Gateway Distance Last Update
192.0.2.1 110 00:01:02
Distance: (default is 110)
Routing Protocol is "bgp 601"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
IGP synchronization is disabled
Automatic route summarization is disabled
Neighbor(s):
Address FiltIn FiltOut DistIn DistOut Weight RouteMap
192.0.2.0
Maximum path: 1
Routing Information Sources:
Gateway Distance Last Update
192.0.2.0 20 00:01:03
Distance: external 20 internal 200 local 200
```

第 81 章

ワイヤレスハイ アベイラビリティの設定

- 機能情報の確認，1937 ページ
- ハイ アベイラビリティに関する情報，1937 ページ
- 冗長性に関する情報，1938 ページ
- アクセス ポイントのステートフル スイッチオーバーに関する情報，1940 ページ
- グレースフル スイッチオーバーの開始，1941 ページ
- ハイ アベイラビリティ用の EtherChannel の設定，1941 ページ
- LACP の設定，1942 ページ
- ハイ アベイラビリティのトラブルシューティング，1943 ページ

機能情報の確認

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

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

ハイ アベイラビリティに関する情報

ハイ アベイラビリティ機能は、スイッチがスタック ケーブルで接続され、Cisco StackWise-160 テクノロジーがイネーブルの場合、デフォルトでイネーブルになります。これをディセーブルにはできません。ただし、コマンドラインインターフェイスを使用して手動のグレースフル スイッチオーバーを開始して、スイッチでイネーブルのハイ アベイラビリティ機能を使用することができます。

Cisco ワイヤレス LAN コントローラでは、ハイ アベイラビリティは冗長性とともに実現されます。

Cisco ワイヤレス LAN コントローラでは、冗長性は 2 通りの方法（n+1 と AP SSO 冗長性）で実現されます。

アクティブ コントローラとスタンバイ コントローラ間でキープアライブ メッセージが送受信されます。

- スタンバイ コントローラが応答しない場合は、新しいスタンバイ コントローラが選択されます。
- アクティブ コントローラが応答しない場合は、スタンバイ コントローラがアクティブ コントローラになります。

加えて、すべてのスタック メンバーで hello メッセージが送受信されます。

- スタック メンバーが応答しない場合は、そのメンバーがスタックから削除されます。
- スタンバイ コントローラが応答しない場合は、新しいスタンバイ コントローラが選択されます。
- アクティブ コントローラが応答しない場合は、スタンバイ コントローラがアクティブ コントローラになります。

冗長性に関する情報

N+1 冗長性の場合、アクセス ポイントは、第 1、第 2、および第 3 コントローラで設定されます。1 台のコントローラで管理されるアクセス ポイント数が原因で第 1 コントローラに障害が発生した場合、アクセス ポイントは第 2 コントローラにフェール オーバーします。AP SSO 冗長性の場合、第 1 コントローラが使用できない場合、アクセス ポイントはそのコントローラを再検出し、第 2 コントローラで CAPWAP トンネルを再確立します。ただし、コントローラに再度参加させるには、すべてのクライアントを切断して、再認証を実行する必要があります。

選択したアクセス ポイントおよび選択したコントローラ用の第 1、第 2、および第 3 コントローラを設定できます。

理想的なハイ アベイラビリティ展開では、第 1 および第 2 コントローラに接続されたアクセス ポイントを持つことができ、1 台のコントローラは、アクセス ポイントへ接続せずに維持できます。このように、アクセス ポイントを持たないコントローラは障害発生時に引き継ぐことができ、アクティブなコントローラのサービスを再開できます。

アクセス ポイントの冗長性の設定

選択したアクセス ポイントの第 1、第 2、または第 3 コントローラを設定するには、この項に説明されているコマンドを使用する必要があります。

はじめる前に

手順の概要

1. conf t
2. ap capwap backup primary
3. **ap capwap backup secondary**
4. ap capwap backup tertiary

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	conf t 例： `Controller # conf t`	端末を設定します。
ステップ 2	ap capwap backup primary 例： `Controller # ap capwap backup primary WLAN-Controller-A`	選択したアクセス ポイントの第 1 コントローラを設定します。
ステップ 3	**ap capwap backup secondary** 例： `Controller # ap capwap backup secondary WLAN-Controller-B`	選択したアクセス ポイントの第 2 コントローラを設定します。
ステップ 4	ap capwap backup tertiary 例： `Controller # ap capwap backup tertiary WLAN-Controller-C`	選択したアクセス ポイントの第 3 コントローラを設定します。

次の作業

指定されたアクセス ポイントの第 1、第 2、第 3 コントローラの設定を完了したら、**show ap name***AP-NAME* コマンドを使用して、その設定を確認する必要があります。**show ap name***AP-NAME* コマンドに関する詳細については、『Lightweight Access Point Configuration Guide for Cisco Wireless LAN Controller』を参照してください。

-

ハートビート メッセージの設定

ハートビート メッセージを使用して、コントローラの障害検出時間を短縮することができます。障害が発生すると、コントローラがハートビート タイマーを待機した後にアクティブからホットスタンバイへのスイッチオーバーが発生します。コントローラがハートビート時間内に動作しない場合は、スタンバイがアクティブ コントローラとして引き継ぎます。理想的には、アクセスポイントが指定されたタイムアウト値以内に 3 つのハートビート メッセージを生成し、コントローラがタイムアウト値以内に応答しない場合、スタンバイ コントローラがアクティブ コントローラを引き継ぎます。ネットワークに応じてタイムアウト値を指定できます。理想的には、スイッチオーバーの実行時に混乱が生じるためタイマー値は高くない値にします。この項では、コントローラの障害検出時間を短縮するために、タイムアウト値を使用してコントローラとアクセス ポイント間のハートビート間隔を設定する方法について説明します。

はじめる前に

手順の概要

1. conf t
2. ap capwap timers heartbeat-timeout

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	conf t 例： `controller # conf t`	端末を設定します。
ステップ 2	ap capwap timers heartbeat-timeout 例： `controller #  ap capwap timers heartbeat-timeout`	コントローラとアクセス ポイント間のハートビート間隔を設定します。タイムアウト値の範囲は 1 ～ 30 です。

アクセス ポイントのステートフル スイッチオーバーに関する情報

アクセス ポイント ステートフル スイッチオーバー（AP SSO）とは、すべてのアクセス ポイントがステートフルにスイッチオーバーし、ユーザ セッション情報がスイッチオーバー中も維持され、アクセス ポイントがネットワーク内でセッションを失うことなく動作継続することで、ネットワークの可用性が高まることを意味します。スタックのアクティブ スイッチは、IP 機能やルーティング情報交換を含め、すべてのネットワーク機能を実行するよう装備されます。スイッチは、1000 アクセス ポイントと 12000 クライアントをサポートします。

ただし、スイッチオーバー発生時にFlexConnectモードでローカルにスイッチされるクライアントを除き、すべてのクライアントが認証解除され新しいアクティブ スイッチに再度関連付けられる必要があります。

スタック内で冗長ペアが形成されると、ハイ アベイラビリティが実現します。これには、アクティブからスタンバイへのスイッチオーバーの間もアクセスポイントが接続された状態を維持することが含まれます。

（注） スイッチが冗長ペアを形成した後は、スイッチ スタック内でAP SSOをディセーブルにできません。

（注） スイッチオーバーの後、新しいスタンバイがスタック構成時にリロードされた場合は、一括同期できないことが理由です。これは正常にスタック構成をするための2回目の試行で、リロード後にみられます。これを回避するためには、コマンド *exception dump device second flash* を実行します。これはクラッシュ情報ディレクトリがフルの場合に、クラッシュファイルをフラッシュにダンプするために使用されます。クラッシュが発生し、クラッシュ情報に領域が残されていない場合には、fullcore/crash ファイルをフラッシュに保存します。

グレースフル スイッチオーバーの開始

手動スイッチオーバーを実行し、スイッチで有効なハイ アベイラビリティ機能を使用するには、**redundancy force-switchover** コマンドを実行します。このコマンドは、アクティブからスタンバイ スイッチへのグレースフル スイッチオーバーを開始します。

```
スイッチ# redundancy force-switchover
System configuration has been modified. Save ? [yes/no] : yes
Building configuration …
Preparing for switchover …
Compressed configuration from 14977 bytes to 6592 bytes[OK]This will reload the active unit
 and force switchover to standby[confirm] : y
```

ハイ アベイラビリティ用の EtherChannel の設定

LAG または EtherChannel は、スタンバイ装置とアクティブ装置の両方の既存のポートすべてを単一の論理ポートにバンドルし、60 Gbps の集約帯域幅を実現します。EtherChannel の作成は、障害に対する保護を可能にします。作成された Etherchannel または LAG は、アクセス ポイントのハイ アベイラビリティを確保するための冗長リンクに使用されます。

EtherChannel の設定と EtherChannel モードの詳細については、『Layer 2 (Link Aggregation) Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)』を参照してください。

ステップ 1 スタック ケーブルを使用して、電力がダウン状態の 2 台のスイッチを接続します。

ステップ 2 両方のスイッチに同時に電源投入して起動するか、1 台のスイッチに電源投入して起動します。スイッチが正常起動し、ハイ アベイラビリティ ペアを形成します。

ステップ 3 装置で EtherChannel または LAG を設定します。

ステップ 4 設定した EtherChannel のステータスを表示するには、**show etherchannel summary** コマンドを使用します。設定が完了すると、指定されたすべてのポートは単一のチャネルにバンドルされ、**show etherchannel summary** コマンドの出力に表示されます。

ステップ 5 **show ap uptime** コマンドを実行して、接続されたアクセス ポイントを確認します。

LACP の設定

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **lacp max-bundle** *number*
4. **lacp port-priority** *number*
5. **switchport backup interface** *po2*
6. **end**
7. **show etherchannel summary**
8. **show interfaces switchport backup**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *number* 例： `スイッチ(config)# interface Port-channel Po2`	ポートチャネル インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**lacp max-bundle** *number* 例： スイッチ(config-if)# **lacp max-bundle 6**	ポート チャネルで許可される、アクティブなバンドルされた LACP ポートの最大数を定義します。値の範囲は 1 ～ 8 です。
ステップ 4	**lacp port-priority** *number* 例： スイッチ(config-if)# **lacp port-priority 4**	LACP を使用するポートに設定するポート プライオリティを指定します。値の範囲は 0 ～ 65535 です。
ステップ 5	**switchport backup interface** *po2* 例： スイッチ(config-if)# **switchport backup interface Po2**	バックアップ インターフェイスとしてインターフェイスを指定します。
ステップ 6	**end**	インターフェイスとコンフィギュレーション モードを終了します。
ステップ 7	**show etherchannel summary** 例： スイッチ# **show etherchannel summary**	EtherChannel プロパティの概要を表示します。
ステップ 8	**show interfaces switchport backup** 例： スイッチ# **show interfaces switchport backup**	バックアップ EtherChannel のプロパティの概要を表示します。

ハイ アベイラビリティのトラブルシューティング

スタンバイ コンソールへのアクセス

スタック内のアクティブ スイッチのコンソールにのみアクセスできます。スタンバイ スイッチにアクセスするには、次のコマンドを使用します。

はじめる前に

シスコ サポートの管理下でのみこの機能を使用します。

手順の概要

1. **configure terminal**
2. **service internal**
3. **redundancy**
4. **main-cpu**
5. **standby console enable**
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service internal** 例： スイッチ(config)# **service internal**	Cisco IOS デバッグ コマンドをイネーブルにします。
ステップ 3	**redundancy** 例： スイッチ(config)# **redundancy**	冗長コンフィギュレーション モードを開始します。
ステップ 4	**main-cpu** 例： スイッチ(config)# **main-cpu**	冗長メイン コンフィギュレーション サブモードを開始します。
ステップ 5	**standby console enable** 例： スイッチ(config)# **standby console enable**	スタンバイ コンソールをイネーブルにします。
ステップ 6	**exit** 例： スイッチ(config)# **exit**	コンフィギュレーション モードを終了します。

スイッチオーバー前

スイッチオーバーはスイッチ に障害が発生した場合に発生します。ただし、手動スイッチオーバーの実行時は、次のコマンドを実行して正常なスイッチオーバーを開始することができます。

手順の概要

1. **show redundancy states**
2. **show switch detail**
3. **show platform ses states**
4. **show ap summary**
5. **show capwap detail**
6. **show dtls database-brief**
7. **show power inline**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show redundancy states** 例： スイッチ# **show redundancy states**	アクティブおよびスタンバイ スイッチのハイ アベイラビリティ ロールを表示します。
ステップ 2	**show switch detail** 例： スイッチ# **show switch detail**	スタックの物理特性を表示します。スタックの物理状態が「Ready」または「Port」かどうか確認します。
ステップ 3	**show platform ses states** 例： スイッチ# **show platform ses states**	スタック マネージャのシーケンスを表示します。
ステップ 4	**show ap summary** 例： スイッチ# **show ap summary**	アクティブおよびスタンバイ スイッチのすべてのアクセス ポイントを表示します。
ステップ 5	**show capwap detail** 例： スイッチ# **show capwap detail**	アクティブおよびスタンバイ スイッチの CAPWAP トンネルの詳細を表示します。
ステップ 6	**show dtls database-brief** 例： スイッチ# **show dtls database-brief**	アクティブおよびスタンバイ スイッチの DTLS の詳細を表示します。
ステップ 7	**show power inline** 例： スイッチ# **show power inline**	イーサネットの電源状態を表示します。 （注） フェールオーバーが発生時した場合、正常なスイッチオーバーのために、SSO では、スタンバイ コントローラはスタンバイホット状態、冗長ポートはターミナル状態である必要があります。

	コマンドまたはアクション	目的

スイッチオーバー後

ここでは、アクティブからスタンバイ スイッチへのスイッチオーバーが実行されるのを保障するため、ユーザが実行する必要のある手順を定義します。スタンバイ スイッチからアクティブへのスイッチオーバー成功後、アクティブへ接続されたすべてのアクセス ポイントはスタンバイ（その後アクティブ）スイッチに再参加する必要があります。

手順の概要

1. **show ap uptime**
2. **show wireless summary**
3. **show wcdb database all**
4. **show power inline**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ap uptime** 例： スイッチ# **show ap uptime**	スイッチオーバー後のアクセスポイントのアップタイムが十分に大きいかどうかを確認します。
ステップ 2	**show wireless summary** 例： スイッチ# **show wireless summary**	アクティブ スイッチに接続されているクライアントを表示します。
ステップ 3	**show wcdb database all** 例： スイッチ# **show wcdb database all**	クライアントがアップタイムに達したかを表示します。
ステップ 4	**show power inline** 例： スイッチ# **show power inline**	Power over Ethernet の電源状態を表示します。

スイッチ スタックのモニタリング

表 *138*：スタック情報を表示するコマンド

コマンド	説明
show switch	割り当てられたスイッチやバージョン不一致モードのスイッチのステータスなど、スタックに関するサマリー情報を表示します。
show switch*stack-member-number*	特定のメンバーに関する情報を表示します。
show switch detail	スタックに関する詳細情報を表示します。
show switch neighbors	スタック ネイバーを表示します。
show switch stack-ports [**summary**]	スタックのポート情報を表示します。
show redundancy	冗長システムと現在のプロセッサ情報を表示します。冗長システムの情報にはシステム稼働時間、スタンバイ失敗、スイッチオーバー理由、ハードウェア、設定冗長モードおよび動作冗長モードが含まれます。表示される現在のプロセッサ情報にはアクティブ位置、ソフトウェアの状態、現在の状態での稼働時間などが含まれます。
show redundancy state	アクティブおよびスタンバイ スイッチの冗長状態をすべて表示します。

LACP の設定：例

次に、LACP を設定して LACP バンドルの作成と状態を確認する例を示します。

```
スイッチ(config)# !
interface TenGigabitEthernet1/0/1
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/2
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/3
 switchport mode trunk
 channel-group 1 mode active
```

```
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/4
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/5
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/6
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/1
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/2
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/3
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/4
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/5
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/6
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface Vlan1
 no ip address
 ip igmp version 1
 shutdown
!
```

スイッチ# **show etherchannel summary**

```
  Flags:  D - down        P - bundled in port-channel
          I - stand-alone s - suspended
          H - Hot-standby (LACP only)
          R - Layer3      S - Layer2
          U - in use      f - failed to allocate aggregator

          M - not in use, minimum links not met
          u - unsuitable for bundling
          w - waiting to be aggregated
          d - default port


Number of channel-groups in use: 1
Number of aggregators:           1
```

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Te1/0/1(P)  Te1/0/2(P)  Te1/0/3(P)
                                 Te1/0/4(H)  Te1/0/5(H)  Te1/0/6(H)
                                 Te2/0/1(P)  Te2/0/2(P)  Te2/0/3(P)
                                 Te2/0/4(H)  Te2/0/5(H)  Te2/0/6(H)
```

次に、スイッチのバックアップ インターフェイス ペアの例を示します。

```
スイッチ# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Port-channel1             Port-channel2             Active Standby/Backup Up
```

次に、スイッチに設定された EtherChannel の概要の例を示します。

```
スイッチ# show ethernet summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Te1/0/1(P)  Te1/0/2(P)  Te1/0/3(P)
                                 Te1/0/4(P)  Te1/0/5(P)  Te1/0/6(P)
2      Po2(SU)         LACP      Te2/0/1(P)  Te2/0/2(P)  Te2/0/3(P)
                                 Te2/0/4(P)  Te2/0/5(P)  Te2/0/6(P)
```

第 XIV 部

システム管理

- システムの管理，1953 ページ
- スイッチのセットアップ設定の実行，1995 ページ
- Right-To-Use ライセンスの設定，2041 ページ
- 管理者のユーザ名とパスワードの設定，2059 ページ
- 802.11 パラメータおよび帯域選択の設定，2065 ページ
- アグレッシブ ロード バランシングの設定，2085 ページ
- クライアント ローミングの設定，2093 ページ
- Application Visibility and Control の設定，2109 ページ
- 音声パラメータとビデオ パラメータの設定，2145 ページ
- RFID タグ追跡の設定，2171 ページ
- ロケーションの設定，2175 ページ
- フロー制御のモニタリング，2185 ページ
- SDM テンプレートの設定，2189 ページ
- システム メッセージ ログの設定，2197 ページ
- オンライン診断の設定，2215 ページ
- コンフィギュレーション ファイルの管理，2227 ページ

- コンフィギュレーションの置換とロールバック，2273 ページ
- フラッシュ ファイル システムの操作，2289 ページ
- Cisco IOS XE ソフトウェア バンドルの使用，2303 ページ
- 条件付きデバッグおよび放射線トレース，2315 ページ
- ソフトウェア設定のトラブルシューティング，2323 ページ

第 82 章

システムの管理

- 機能情報の確認，1953 ページ
- スイッチの管理に関する情報，1954 ページ
- スイッチを管理する方法，1963 ページ
- スイッチのモニタリングおよび保守の管理，1987 ページ
- スイッチ管理の設定例，1988 ページ
- スイッチ管理に関する追加情報，1991 ページ
- スイッチ管理に関する追加情報，1992 ページ
- スイッチ管理の機能履歴と情報，1994 ページ

機能情報の確認

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

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

スイッチの管理に関する情報

システム日時の管理

スイッチのシステム日時は自動設定方式（RTC および NTP）または手動設定方式を使用して管理できます。

（注） ここで使用するコマンドの構文および使用方法の詳細については、*Cisco.com* で、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

システム クロック

時刻サービスの基本となるのはシステム クロックです。このクロックはシステムがスタートアップした瞬間から稼働し、日時を常時トラッキングします。

システム クロックは、次のソースにより設定できます。

- NTP
- 手動設定

システム クロックは、次のサービスに時刻を提供します。

- ユーザの **show** コマンド
- ログおよびデバッグ メッセージ

システム クロックは、グリニッジ標準時（GMT）とも呼ばれる協定世界時（UTC）に基づいて内部的に時刻を追跡します。ローカルのタイム ゾーンおよび夏時間に関する情報を設定することにより、時刻がローカルのタイム ゾーンに応じて正確に表示されるようにできます。

システム クロックは、時刻に信頼性があるかどうか（つまり、信頼できると見なされるタイム ソースによって時刻が設定されているか）を常時トラッキングします。信頼性のない場合は、時刻は表示目的でのみ使用され、再配信されません。

ネットワーク タイム プロトコル

NTP は、ネットワーク上のデバイス間の時刻の同期化を目的に設計されています。NTP はユーザ データグラム プロトコル（UDP）で稼働し、UDP は IP 上で稼働します。NTP は RFC 1305 で規定されています。

NTP ネットワークは通常、タイム サーバに接続されたラジオ クロックやアトミック クロックなど、正規の時刻源から時刻を取得します。NTP は、ネットワークにこの時刻を分配します。NTP はきわめて効率的で、1 分間に 1 パケットを使用するだけで、2 台のデバイスを 1 ミリ秒以内に同期化できます。

NTP では、信頼できるタイム ソースから各マシンが何NTP「ホップ」隔たっているかを表すために、ストラタムという概念が使用されます。ストラタム 1 タイム サーバには、ラジオ クロックまたは原子時計が直接接続されており、ストラタム 2 タイム サーバは、NTP を使用してストラタム 1 タイム サーバから時刻を取得します（以降のストラタムも同様です）。NTP が稼働するデバイスは、タイム ソースとして、NTP を使用して通信するストラタム番号が最小のデバイスを自動的に選択します。この方法によって、NTP 時刻配信の自動編成型ツリーが効率的に構築されます。

NTP では、同期化されていないデバイスと同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

NTP が稼働するデバイス間の通信（アソシエーション）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間でNTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するようにNTP を設定できます。各デバイスを、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られます。

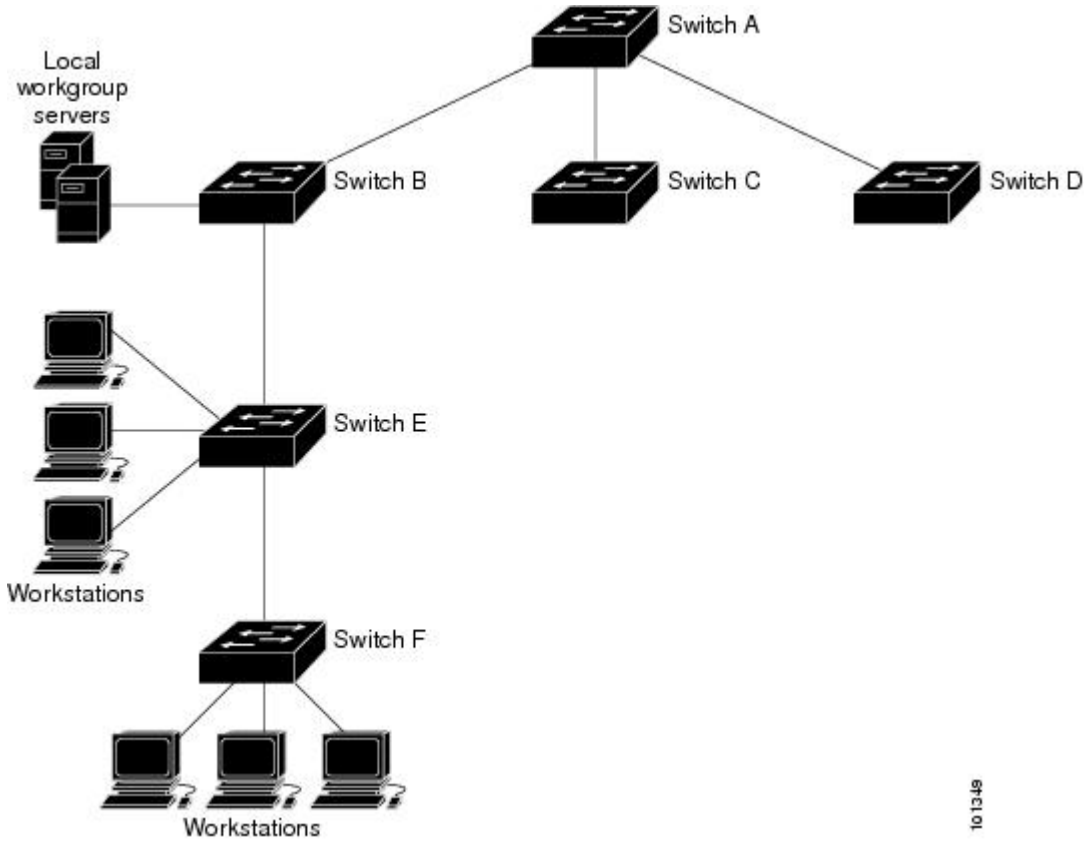
デバイス上で維持される時刻は、重要なリソースです。NTP のセキュリティ機能を使用して、不正確な時刻が誤って、あるいは意図的に設定されることがないようにしてください。その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

シスコによるNTP の実装では、ストラタム 1 サービスをサポートしていないため、ラジオ クロックまたは原子時計に接続できません。ネットワークの時刻サービスは、IP インターネット上のパブリック NTP サーバから取得することを推奨します。

次の図にNTP を使用した一般的なネットワークの例を示します。スイッチ A は、NTP サーバ モードで設定した**スイッチ** B、C、D の NTP マスターです。スイッチ B、C、D とスイッチ A の間に

はサーバ アソシエーションが設定されています。スイッチ E はアップストリームおよびダウンストリーム スイッチ、スイッチ B およびスイッチ F それぞれの NTP ピアとして設定されます。

図 *93*：一般的な *NTP* ネットワークの構成



ネットワークがインターネットから切り離されている場合、シスコの NTP によって、実際には、他の方法で時刻を学習しているにもかかわらず、デバイスが NTP を使用して同期化しているように動作を設定できます。他のデバイスは、NTP によりこのデバイスと同期化されます。

複数のタイム ソースがある場合は、NTP は常に、より信頼性があると見なされます。NTP の時刻は、他の方法による時刻に優先します。

自社のホスト システムに NTP ソフトウェアを組み込んでいるメーカーが数社あり、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホスト システムも時間が同期化されます。

NTP ストラタム

NTP では、信頼できるタイム ソースから各マシンが何 NTP「ホップ」隔たっているかを表すために、ストラタムという概念が使用されます。ストラタム 1 タイム サーバには、ラジオ クロックまたは原子時計が直接接続されており、ストラタム 2 タイム サーバは、NTP を使用してストラタム 1 タイム サーバから時刻を取得します（以降のストラタムも同様です）。NTP が稼働するデバイ

スは、タイム ソースとして、NTP を使用して通信するストラタム番号が最小のデバイスを自動的に選択します。この方法によって、NTP 時刻配信の自動編成型ツリーが効率的に構築されます。

NTP では、同期化されていないデバイスと同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

NTP アソシエーション

NTP が稼働するデバイス間の通信（アソシエーション）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られます。

NTP セキュリティ

デバイス上で維持される時刻は、重要なリソースです。NTP のセキュリティ機能を使用して、不正確な時刻が誤って、あるいは意図的に設定されることがないようにしてください。その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

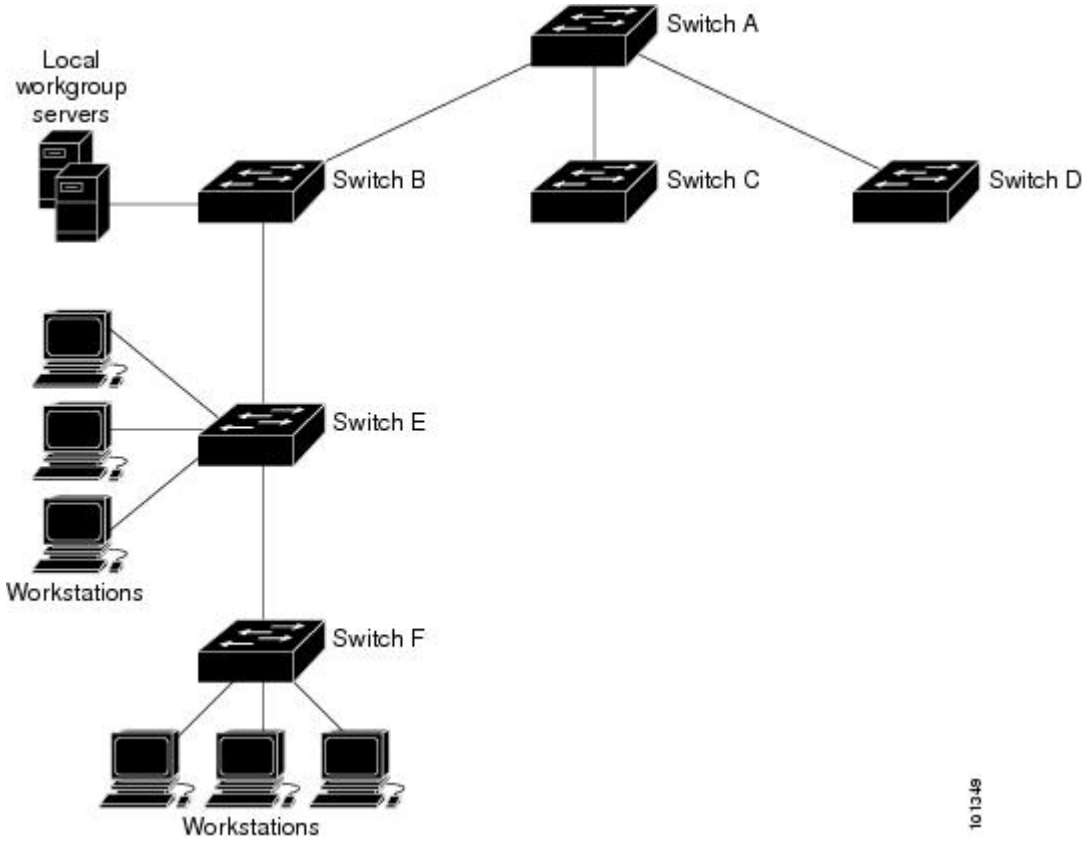
NTP の実装

NTP の実装では、ストラタム 1 サービスがサポートされないため、ラジオ クロックまたは原子時計に接続できません。ネットワークの時刻サービスは、IP インターネット上のパブリック NTP サーバから取得することを推奨します。

次の図は NTP を使用した一般的なネットワークの例を示します。スイッチ A は、スイッチ B、C、D が NTP サーバ モードに設定されている（スイッチ A との間にサーバ アソシエーションが

設定されている）場合のNTPマスターです。スイッチEは、アップストリーム スイッチ（スイッチ B）とダウンストリーム スイッチ（スイッチ F）の NTP ピアとして設定されます。

図 *94*：一般的な *NTP* ネットワークの構成



ネットワークがインターネットから切り離されている場合、NTP によって、実際には、他の方法で時刻を取得している場合でも、NTPを使用した同期化と同様にデバイスの動作を設定できます。他のデバイスは、NTP によりこのデバイスと同期化されます。

複数のタイム ソースがある場合は、NTPは常に、より信頼性があると見なされます。NTPの時刻は、他の方法による時刻に優先します。

自社のホスト システムにNTP ソフトウェアを組み込んでいるメーカーが数社あり、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホスト システムも時間が同期化されます。

NTP バージョン 4

スイッチには、NTP バージョン 4 が実装されています。NTPv4 は NTP バージョン 3 の拡張版です。NTPv4 は IPv4 と IPv6 の両方をサポートし、NTPv3 との下位互換性があります。

NTPv4 は次の互換性を提供します。

- IPv6 のサポート。

- NTPv3 よりさらに向上したセキュリティ。NTPv4 プロトコルは、公開キー暗号化および標準 X509 認証に基づくセキュリティ フレームワークを提供します。
- ネットワークに対する時間分布ヒエラルキーの自動計算。特定のマルチキャスト グループを使用して、NTPv4 は、最も低い帯域幅コストで最高の時間精度を達成するサーバのヒエラルキーを自動的に設定します。この機能では、サイトローカル IPv6 マルチキャスト アドレスが活用されます。

NTPv4 の設定の詳細については、『*Cisco IOS IPv6 Configuration Guide, Release 12.4T*』の「*Implementing NTPv4 in IPv6*」の章を参照してください。

システム名およびシステム プロンプト

スイッチを識別するシステム名を設定します。デフォルトでは、システム名およびシステム プロンプトは スイッチ です。

システム プロンプトを設定していない場合は、システム名の最初の 20 文字がシステム プロンプトとして使用されます。大なり記号（>）が付加されます。システム名が変更されると、プロンプトは更新されます。

ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*, *Release 12.4*』および『*Cisco IOS IP Command Reference*, *Volume 2 of 3: Routing Protocols*, *Release 12.4*』を参照してください。

スタックのシステム名およびシステム プロンプト

アクティブ スイッチを介してスタック メンバにアクセスする場合は、**session***stack-member-number* 特権 EXEC コマンドを使用する必要があります。スタック メンバ番号の有効範囲は です。このコマンドを使用すると、スタック メンバの番号がシステム プロンプトの末尾に追加されます。たとえば、Switch-2# はスタック メンバ 2 の特権 EXEC モードのプロンプトであり、スイッチ スタックのシステム プロンプトは Switch です。

デフォルトのシステム名とプロンプトの設定

デフォルトのスイッチのシステム名およびプロンプトは *Switch* です。

DNS

DNS プロトコルは、ドメイン ネーム システム（DNS）を制御します。DNS とは分散型データベースであり、ホスト名を IP アドレスにマッピングできます。スイッチに DNS を設定すると、**ping**、**telnet**、**connect** などのすべての IP コマンドおよび関連する Telnet サポート操作で IP アドレスの代わりにホスト名を使用できます。

IP によって定義される階層型の命名方式では、デバイスを場所またはドメインで特定できます。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。たとえば、シスコは、IP で *com* というドメイン名に分類される商業組織なので、ドメイン名は *cisco.com* となりま

す。このドメイン内の特定のデバイス、たとえばファイル転送プロトコル（FTP）システムは、*ftp.cisco.com* で表されます。

IPではドメイン名をトラッキングするために、ドメインネームサーバという概念が定義されています。ドメイン ネーム サーバの役割は、名前から IP アドレスへのマッピングをキャッシュ（またはデータベース）に保存することです。ドメイン名を IP アドレスにマッピングするには、まず、ホスト名を明示し、ネットワーク上に存在するネームサーバを指定し、DNSをイネーブルにします。

DNS のデフォルト設定値

表 *139* : *DNS* のデフォルト設定値

機能	デフォルト設定
DNS イネーブル ステート	イネーブル
DNS デフォルト ドメイン名	未設定
DNS サーバ	ネーム サーバのアドレスが未設定

ログイン バナー

Message-of-The-Day（MoTD）バナーおよびログイン バナーを作成できます。MOTD バナーはログイン時に、接続されたすべての端末に表示されます。すべてのネットワーク ユーザに影響するメッセージ（差し迫ったシステム シャットダウンの通知など）を送信する場合に便利です。

ログイン バナーも接続されたすべての端末に表示されます。表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

（注） ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*』を参照してください。

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

MAC Address Table

MAC アドレス テーブルには、スイッチがポート間のトラフィック転送に使用するアドレス情報が含まれています。このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応しています。アドレステーブルに含まれるアドレスタイプには、次のものがあります。

- ダイナミックアドレス：スイッチが取得し、使用されなくなった時点で期限切れとなる送信元の MAC アドレス
- スタティックアドレス：手動で入力され、期限切れにならず、スイッチのリセット時にも消去されないユニキャスト アドレス

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN（仮想 LAN）ID、アドレスに対応付けられたポート番号、およびタイプ（スタティックまたはダイナミック）のリストです。

（注） ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

MAC アドレス テーブルの作成

すべてのポートでサポートされる複数の MAC アドレスを使用して、他のネットワーク デバイスにスイッチ上のすべてのポートを接続できます。スイッチは、各ポートで受信するパケットの送信元アドレスを取得し、アドレス テーブルにアドレスとそれに関連付けられたポート番号を追加することによって、動的なアドレス指定を行います。ネットワークでデバイスの追加または削除が行われると、スイッチによってアドレステーブルが更新され、新しいダイナミック アドレスが追加され、使用されていないアドレスは期限切れになります。

エージング インターバルは、グローバルに設定されています。ただし、スイッチは VLAN ごとにアドレス テーブルを維持し、STP によって VLAN 単位で有効期間を短縮できます。

スイッチは、受信したパケットの宛先アドレスに基づいて、任意の組み合わせのポート間でパケットを送信します。スイッチは、MAC アドレス テーブルを使用することによって、宛先アドレスに関連付けられたポートに限定してパケットを転送します。宛先アドレスがパケットを送信したポート上にある場合は、パケットはフィルタリング処理され、転送されません。スイッチは、常にストアアンドフォワード方式を使用します。このため、完全なパケットをいったん保存してエラーがないか検査してから転送します。

MAC アドレスおよび VLAN

すべてのアドレスは VLAN と関連付けされます。1 つのアドレスを複数の VLAN に対応付け、それぞれで異なる宛先を設定できます。たとえば、ユニキャスト アドレスを VLAN 1 のポート 1 および VLAN 5 のポート 9、10、1 に転送するといったことが可能です。

VLAN ごとに、独自の論理アドレス テーブルが維持されます。ある VLAN で認識されているアドレスが別の VLAN で認識されるには、別の VLAN 内のポートによって学習されるか、または別の VLAN 内のポートにスタティックに対応付けられる必要があります。

MAC アドレスおよびスイッチのスタック

すべてのスタック メンバにある MAC アドレス テーブルでは、同期が取られます。いかなる時点でも、各スタック メンバには、各 VLAN のアドレス テーブルの同じコピーがあります。アドレスがエージング アウトすると、アドレスは、すべてのスタック メンバにあるアドレス テーブル

から削除されます。スイッチがスイッチ スタックに参加すると、そのスイッチでは、他のスタック メンバでラーニングされた各 VLAN のアドレスを受信します。スタック メンバがスイッチ スタックに残っているときには、残りのスタック メンバは、エージングアウトするか、前のスタック メンバによってラーニングされたすべてのアドレスが削除されます。

MAC アドレス テーブルのデフォルト設定

次の表に、MAC アドレス テーブルのデフォルト設定を示します。

表 *140*： *MAC* アドレスのデフォルト設定

機能	デフォルト設定
エージング タイム	300 秒
ダイナミック アドレス	自動学習
スタティック アドレス	未設定

ARP テーブルの管理

デバイスと通信するには（イーサネット上のデバイスなど）、ソフトウェアは最初にそのデバイスの 48 ビット MAC アドレスまたはローカルデータ リンク アドレスを学習する必要があります。IP アドレスからローカル データ リンク アドレスを学習するプロセスを、アドレス解決といいます。

アドレス解決プロトコル（ARP）は、ホスト IP アドレスを、該当するメディアまたは MAC アドレスおよび VLAN ID に対応付けます。IP アドレスを使用して、ARP は対応する MAC アドレスを見つけます。MAC アドレスが見つかると、IP と MAC アドレスとの対応を ARP キャッシュに格納し、すばやく検索できるようにします。その後、IP データグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化および ARP 要求/応答については、サブネットワーク アクセス プロトコル（SNAP）で規定されています。IP インターフェイスでは、標準的なイーサネット形式の ARP カプセル化（**arpa** キーワードで表される）がデフォルトでイネーブルに設定されています。

手動でテーブルに追加された ARP エントリは期限切れにならないので、手動で削除する必要があります。

CLI（コマンドライン インターフェイス）の手順については、*Cisco.com* で Cisco IOS Release 12.4 のマニュアルを参照してください。

スイッチを管理する方法

手動による日付と時刻の設定

正確なシステム時刻は再開と再起動により保持されますが、日付と時刻はシステムが再開してから手動で設定できます。

手動設定は必要な場合にのみ使用することを推奨します。スイッチが同期できる外部ソースがある場合は、システム クロックを手動で設定する必要はありません。

（注） アクティブ スイッチに障害が発生し、別のスタック メンバがアクティブ スイッチの役割を引き継ぐ前に手動でシステム クロックを設定している場合は、この設定を再設定する必要があります。

システム クロックの設定

ネットワーク上に、NTP サーバなどの時刻サービスを提供する外部ソースがある場合、手動でシステム クロックを設定する必要はありません。

システム クロックを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. 次のいずれかを使用します。
   - **clock set***hh:mm:ss day month year*
   - **clock set** *hh:mm:ss month day year*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかを使用します。 • **clock set***hh:mm:ss day month year*	次のいずれかの書式を使ってシステム クロックを手動で設定します。

	コマンドまたはアクション	目的
	• **clock set** *hh:mm:ss month day year* 例： スイッチ# **clock set 13:32:00 23 March 2013**	• *hh:mm:ss*：時間（24 時間形式）、分、秒を指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • *day*：月の日で日付を指定します。 • *month*：月を名前で指定します。 • *year*：年を指定します（略式表記で指定しないでください）。

タイム ゾーンの設定

タイム ゾーンを手動で設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **clock timezone***zone hours-offset* [*minutes-offset*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**clock timezone***zone hours-offset* [*minutes-offset*]	時間帯を設定します。

	コマンドまたはアクション	目的
	例： スイッチ(config)# **clock timezone AST -3 30**	内部時間は、協定世界時（UTC）で維持されるため、このコマンドは表示専用で、時刻を手動で設定するときだけに使用されます。 • *zone*：標準時が適用されているときに表示されるタイムゾーンの名前を入力します。デフォルトはUTC です。 • *hours-offset*：UTC からのオフセット時間数を入力します。 •（任意）*minutes-offset*：UTCからのオフセット分数を入力します。ローカル タイム ゾーンが UTC と 1 時間の差の割合である場合に指定できます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

夏時間の設定

毎年特定の日に夏時間が開始および終了する地域に夏時間を設定するには、次の作業を行います。

手順の概要

1. **enable**
2. **configureterminal**
3. **clock summer-time***zone***date***date month year hh:mm date month year hh:mm* [*offset*]]
4. **clock summer-time***zone***recurring** [*week day month hh:mm week day month hh:mm* [*offset*]]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**clock summer-time***zone***date***date month year hh:mm date month year hh:mm* [*offset*]] 例： スイッチ(config)# **clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00**	毎年指定された日に開始および終了する夏時間を設定します。
ステップ 4	**clock summer-time***zone***recurring** [*week day month hh:mm week day month hh:mm* [*offset*]] 例： スイッチ(config)# **clock summer-time PDT recurring 10 March 2013 2:00 3 November 2013 2:00**	毎年指定された日に開始および終了する夏時間を設定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。 終了時間は夏時間を基準にしています。夏時間はデフォルトでディセーブルに設定されています。パラメータなしで **clock summer-time***zone***recurring** を指定すると、夏時間のルールはデフォルトにより米国のルールになります。 開始月が終了月より後の場合は、システムでは南半球にいると見なされます。

	コマンドまたはアクション	目的
		• *zone*：夏時間が有効な場合に表示される時間帯名（PDT など）を指定します。 • （任意）*week*：月の週（1 ～ 4、**first**、または **last**）を指定します。 • （任意）*day*：曜日（Sunday、Monday など）を指定します。 • （任意）*month*：月（January、February など）を指定します。 • （任意）*hh:mm*：時および分単位で時間（24 時間形式）を指定します。 • （任意）*offset*：夏時間中に追加する分数を指定します。デフォルトは 60 です。
ステップ 5	**end** **例**： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** **例**： `スイッチ# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** **例**： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ユーザの居住地域の夏時間が定期的なパターンに従わない（次の夏時間のイベントの正確な日時を設定する）場合は、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **clock summer-time***zone***date**[*month date year hh:mm month date year hh:mm* [*offset*]]or**clock summer-time***zone***date** [*date month year hh:mm date month year hh:mm* [*offset*]]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**clock summer-time***zone***date**[*month date year hh:mm month date year hh:mm* [*offset*]]or**clock summer-time***zone***date** [*date month year hh:mm date month year hh:mm* [*offset*]]	最初の日付で夏時間開始の日付を、2 番めの日付で終了の日付を設定します。 夏時間はデフォルトでディセーブルに設定されています。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前（たとえば PDT）を入力します。 • （任意）*week* には、月の何週目かを指定します（1 ～ 5、または last）。 • （任意）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh:mm* には、時刻を時間（24 時間形式）と分で指定します。 • （任意）*offset* には、夏時間の間、追加する分数を指定します。デフォルトは 60 です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

システム名の設定

システム名を手動で設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **hostname***name*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname***name* 例： スイッチ(config)# **hostname remote-users**	システム名を設定します。システム名を設定すると、システム プロンプトとしても使用されます。 デフォルト設定はスイッチです。 名前は ARPANET ホスト名のルールに従う必要があります。このルールではホスト名は文字で始まり、文字または数字で終わり、その間には文字、数字、またはハイフンしか使用できません。名前には 63 文字まで使用できます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DNS の設定

スイッチのIPアドレスをホスト名として使用する場合、このIPアドレスが使用されるため、DNS クエリは発生しません。ピリオド（.）なしでホスト名を設定すると、ピリオドと、それに続くデフォルトのドメイン名がホスト名に追加され、その後で DNS クエリーが行われ、名前を IP アドレスにマッピングします。デフォルトのドメイン名は、グローバル コンフィギュレーション コマンド **ip domain-name** で設定される値です。ホスト名にピリオド（.）がある場合は、Cisco IOS ソフトウェアは、ホスト名にデフォルトのドメイン名を追加せずに IP アドレスを検索します。

DNS を使用するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip domain-name***name*
4. **ip name-server***server-address1* [*server-address2 ... server-address6*]
5. **ip domain-lookup** [**nsap** | **source-interface***interface*]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip domain-name***name* 例： スイッチ(config)# **ip domain-name Cisco.com**	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 ブート時にはドメイン名は設定されていませんが、スイッチの設定が BOOTP または Dynamic Host Configuration Protocol（DHCP）サーバから行われている場合、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（この情報がサーバに設定されている場合）。
ステップ 4	**ip name-server***server-address1* [*server-address2 ... server-address6*] 例： スイッチ(config)# **ip name-server 192.168.1.100**	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバ アドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。スイッチは、最初にプライマリ サーバへ DNS クエ

	コマンドまたはアクション	目的
	192.168.1.200 192.168.1.300	リを送信します。そのクエリが失敗した場合は、バックアップサーバにクエリが送信されます。
ステップ 5	**ip domain-lookup** [**nsap** | **source-interface***interface*] 例： スイッチ(config)# **ip domain-lookup**	（任意）スイッチ上で、DNSに基づくホスト名からアドレスへの変換をイネーブルにします。この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

Message-of-the-Day ログイン バナーの設定

スイッチにログインしたときに画面に表示される 1 行以上のメッセージ バナーを作成できます。

MOTD ログイン バナーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **banner motd***cmessage c*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**banner motd***cmessage c* 例： スイッチ(config)# **banner motd #** This is a secure site. Only authorized users are allowed. For access, contact technical support. #	MoTD を指定します。 *c*：ポンド記号（#）など、目的のデリミタを入力して **Return** キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 *message*：255 文字までのバナー メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ログイン バナーの設定

接続されたすべての端末でログイン バナーが表示されるように設定できます。バナーが表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

ログイン バナーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **banner login***c message c*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**banner login***c message c* 例： スイッチ(config)# **banner login $** Access for authorized users only. Please enter your username and password. $	ログイン メッセージを指定します。 *c*：ポンド記号（#）など、目的のデリミタを入力して **Return** キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 *message*：255 文字までのログイン メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MAC アドレス テーブルの管理

アドレス エージング タイムの変更

ダイナミック アドレス テーブルのエージング タイムを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **mac address-table aging-time** [*0* | *10-1000000*] [**routed-mac** | **vlan***vlan-id*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mac address-table aging-time** [*0* | *10-1000000*] [**routed-mac** | **vlan***vlan-id*] 例： スイッチ(config)# **mac address-table aging-time 500 vlan 2**	ダイナミック エントリが使用または更新された後、MAC アドレス テーブル内に保持される時間を設定します。 指定できる範囲は 10 ～ 1000000 秒です。デフォルトは 300 です。0 を入力して期限切れをディセーブルにすることもできます。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。 *vlan-id*：有効な ID は 1 ～ 4094 です。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MAC アドレス変更通知トラップの設定

NMS ホストに MAC アドレス変更通知トラップを送信するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server host***host-addrcommunity-string notification-type* { **informs** | **traps** } {**version** {**1** | **2c** | **3**}} {**vrf***vrf instance name*}
4. **snmp-server enable traps mac-notification change**
5. **mac address-table notification change**
6. **mac address-table notification change** [**interval***value*] [**history-size***value*]
7. **interface***interface-id*
8. **snmp trap mac-notification change** {**added** | **removed**}
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server host***host-addrcommunity-string notification-type* { **informs**	**traps** } {**version** {**1**	**2c**	**3**}} {**vrf***vrf instance name*} 例： スイッチ(config)# **snmp-server host 172.20.10.10 traps private mac-notification**	トラップ メッセージの受信側を指定します。 • *host-addr*：NMS の名前またはアドレスを指定します。 • **traps**（デフォルト）：ホストに SNMP トラップを送信します。 • **informs**：ホストに SNMP インフォームを送信します。

	コマンドまたはアクション	目的
		• **version**：サポートするSNMPバージョンを指定します。informsにはバージョン1（デフォルト）を使用できません。 • *community-string*：通知処理で送信する文字列を指定します。**snmp-server host** コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、**snmp-server community** コマンドを使用し、次に**snmp-server host**コマンドを使用することを推奨します。 • *notification-type*：**mac-notification** キーワードを使用します。 • **vrf***vrf instance name*：ホストのVPNルーティング/転送インスタンスを指定します。
ステップ4	**snmp-server enable traps mac-notification change** 例： `スイッチ(config)# snmp-server enable traps mac-notification change`	スイッチがMACアドレス変更通知トラップを送信できるようにします。
ステップ5	**mac address-table notification change** 例： `スイッチ(config)# mac address-table notification change`	MACアドレス変更通知機能をイネーブルにします。

ステップ6	**mac address-table notification change** [**interval***value*] [**history-size***value*]
	
	例：
	
	`スイッチ(config)# mac address-table notification change interval 123`
	`スイッチ(config)#mac address-table notification change history-size 100`
		トラップ インターバル タイムと履歴テーブルのサイズを入力します。
		• （任意）**interval***value*：NMSに生成されるトラップの各セット間の通知トラップ インターバルを秒単位で指定します。指定できる範囲は0 ～ 2147483647秒です。デフォルトは1秒です。
		• （任意）**history-size***value*：MAC通知履歴テーブルの最大エントリ数を指定します。指定できる範囲は0 ～ 500です。デフォルトは1です。

	コマンドまたはアクション	目的
ステップ 7	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。
ステップ 8	**snmp trap mac-notification change** {**added** | **removed**} 例： スイッチ(config-if)# **snmp trap mac-notification change added**	インターフェイス上で MAC アドレス変更通知トラップをイネーブルにします。 • MAC アドレスがインターフェイスに追加された（**added**）場合にトラップをイネーブルにします。 • MAC アドレスがインターフェイスから削除された（**removed**）場合に MAC 通知トラップをイネーブルにします。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MAC アドレス移動通知トラップの設定

MAC 移動通知を設定する場合は、MAC アドレスが、同じ VLAN 内のあるポートから別のポートに移動すると常に、SNMP 通知が生成されてネットワーク管理システムに送信されます。

NMS ホストに MAC アドレス移動通知トラップを送信するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server host***host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*
4. **snmp-server enable traps mac-notification move**
5. **mac address-table notification mac-move**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**snmp-server host***host-addr* {**traps**	**informs**} {**version** {**1**	**2c**	**3**}} *community-string notification-type* 例： スイッチ(config)# **snmp-server host 172.20.10.10 traps private mac-notification**	トラップ メッセージの受信側を指定します。 • *host-addr*：NMSの名前またはアドレスを指定します。 • **traps**（デフォルト）：ホストにSNMPトラップを送信します。 • **informs**：ホストにSNMPインフォームを送信します。 • **version**：サポートするSNMPバージョンを指定します。informsにはバージョン1（デフォルト）を使用できません。 • *community-string*：通知処理で送信する文字列を指定します。**snmp-server host** コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。

	コマンドまたはアクション	目的
		• *notification-type*：**mac-notification** キーワードを使用します。
ステップ 4	**snmp-server enable traps mac-notification move** 例： スイッチ(config)# **snmp-server enable traps mac-notification move**	スイッチが NMS に MAC アドレス移動通知トラップを送信できるようにします。
ステップ 5	**mac address-table notification mac-move** 例： スイッチ(config)# **mac address-table notification mac-move**	MAC アドレス移動通知機能をイネーブルにします。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

スイッチによるMACアドレス移動通知トラップの送信をディセーブルにするには、**no snmp-server enable traps mac-notification move** グローバル コンフィギュレーション コマンドを使用します。MACアドレス変更通知機能をディセーブルにするには、**no mac address-table notification mac-move** グローバル コンフィギュレーション コマンドを使用します。

show mac address-table notification mac-move 特権 EXEC コマンドを入力して、設定を確認することができます。

MAC しきい値通知トラップの設定

MAC しきい値通知を設定する場合は、MAC アドレス テーブルのしきい値の制限値に達するか、その値を超えると、SNMP 通知が生成されてネットワーク管理システムに送信されます。

NMS ホストに MAC アドレス テーブルしきい値通知トラップを送信するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server host***host-addr* {**traps**|**informs**} {**version** {**1** | **2c**| **3**}} *community-string notification-type*
4. **snmp-server enable traps mac-notification threshold**
5. **mac address-table notification threshold**
6. **mac address-table notification threshold** [**limit***percentage*] | [**interval***time*]
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server host***host-addr* {**traps**|**informs**} {**version** {**1**	**2c**| **3**}} *community-string notification-type* 例： スイッチ(config)# **snmp-server host 172.20.10.10 traps private**	トラップ メッセージの受信側を指定します。 • *host-addr*：NMS の名前またはアドレスを指定します。 • **traps**（デフォルト）：ホストに SNMP トラップを送信します。 • **informs**：ホストに SNMP インフォームを送信します。

	コマンドまたはアクション	目的
	mac-notification	• **version**：サポートする SNMP バージョンを指定します。informs にはバージョン 1（デフォルト）を使用できません。 • *community-string*：通知処理で送信する文字列を指定します。**snmp-server host** コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type*：**mac-notification** キーワードを使用します。
ステップ 4	**snmp-server enable traps mac-notification threshold** 例： `スイッチ(config)# snmp-server enable traps mac-notification threshold`	NMS への MAC しきい値通知トラップをイネーブルにします。
ステップ 5	**mac address-table notification threshold** 例： `スイッチ(config)# mac address-table notification threshold`	MAC アドレスしきい値通知機能をイネーブルにします。

ステップ 6	**mac address-table notification threshold** [**limit***percentage*]	[**interval***time*]
		
		例：
		
		`スイッチ(config)# mac address-table notification threshold interval 123`
		`スイッチ(config)# mac address-table notification threshold limit 78`
			MAC アドレスしきい値使用状況モニタリングのしきい値を入力します。
			• （任意）**limit***percentage*：MAC アドレス テーブルの使用率を指定します。有効値は 1 ～ 100 % です。デフォルト値は 50% です。
			• （任意）**interval***time*：通知の間隔を指定します。有効値は 120 秒以上です。デフォルトは 120 秒です。

ステップ 7	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

スタティック アドレス エントリの追加および削除

スタティック アドレスを追加するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **mac address-table static***mac-addr***vlan***vlan-id***interface***interface-id*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mac address-table static***mac-addr***vlan***vlan-id***interface***interface-id* 例： スイッチ(config)# **mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1**	MAC アドレス テーブルにスタティック アドレスを追加します。 • *mac-addr*：アドレス テーブルに追加する宛先 MAC ユニキャストアドレスを指定します。この宛先アドレスを持つパケットが指定したVLANに着信すると、指定したインターフェイスに転送されます。 • *vlan-id*：指定された MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4094 です。 • *interface-id*：受信パケットが転送されるインターフェイスを指定します。有効なインターフェイスは、物理ポートまたはポートチャネルです。スタティック マルチキャストアドレスの場合、複数のインターフェイス ID を入力できます。スタティック ユニキャスト アドレスの場合、インターフェイスは同時に 1 つしか入力できません。ただし、同じMACアドレスおよびVLAN ID を指定すると、コマンドを複数回入力できます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ユニキャスト MAC アドレス フィルタリングの設定

スイッチが送信元または宛先ユニキャストスタティックアドレスをドロップするよう設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **mac address-table static***mac-addr***vlan***vlan-id***drop**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mac address-table static***mac-addr***vlan***vlan-id***drop** 例： スイッチ(config)# **mac address-table static c2f3.220a.12f4 vlan 4 drop**	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、スイッチが指定した送信元または宛先ユニキャスト スタティック アドレスを持つパケットをドロップするように設定します。 • *mac-addr*：送信元または宛先ユニキャスト MAC アドレス（48 ビット）を指定します。この MAC アドレスを持つパケットはドロップされます。 • *vlan-id*：指定された MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4094 です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチのモニタリングおよび保守の管理

コマンド	目的
clear mac address-table dynamic	すべてのダイナミック エントリを削除します。
clear mac address-table dynamic address *mac-address*	特定の MAC アドレスを削除します。
clear mac address-table dynamic interface *interface-id*	指定された物理ポートまたはポート チャネル上のすべてのアドレスを削除します。
clear mac address-table dynamic vlan *vlan-id*	指定されたVLAN上のすべてのアドレスを削除します。
show clock [*detail*]	時刻と日付の設定を表示します。
show ip igmp snooping groups	すべての VLAN または指定された VLAN に対するレイヤ2マルチキャスト エントリを表示します。
show mac address-table address *mac-address*	指定されたMACアドレスのMACアドレステーブル情報を表示します。

コマンド	目的
show mac address-table aging-time	すべてのVLANまたは指定されたVLANのエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミックMACアドレステーブルエントリのみを表示します。
show mac address-table interface *interface-name*	指定されたインターフェイスの MAC アドレステーブル情報を表示します。
show mac address-table move update	MAC アドレス テーブル移動更新情報を表示します。
show mac address-table multicast	マルチキャストの MAC アドレスのリストを表示します。
show mac address-table notification {change | mac-move | threshold}	MAC 通知パラメータおよび履歴テーブルを表示します。
show mac address-table secure	セキュア MAC アドレスを表示します。
show mac address-table static	スタティックMACアドレステーブルエントリだけを表示します。
show mac address-table vlan *vlan-id*	指定されたVLANのMACアドレステーブル情報を表示します。

スイッチ管理の設定例

例：システム クロックの設定

次の例は、システム クロックを手動で設定する方法を示しています。

```
スイッチ# clock set 13:32:00 23 July 2013
```

例：サマー タイムの設定

次に、サマータイムが 3 月 10 日の 02:00 に開始し、11 月 3 日の 02:00 に終了する場合の設定を例として示します。

```
スイッチ(config)# clock summer-time PDT recurring PST date
10 March 2013 2:00 3 November 2013 2:00
```

次に、サマータイムの開始日と終了日を設定する例を示します。

```
スイッチ(config)#clock summer-time PST date
20 March 2013 2:00 20 November 2013 2:00
```

例：MOTD バナーの設定

次の例は、開始および終了デリミタにポンド記号（#）を使用して、MOTDバナーを設定する方法を示しています。

```
スイッチ(config)# banner motd #

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

#

スイッチ(config)#
```

次に、前の設定により表示されたバナーの例を示します。

```
Unix> telnet 192.0.2.15

Trying 192.0.2.15...

Connected to 192.0.2.15.

Escape character is '^]'.

This is a secure site. Only authorized users are allowed.

For access, contact technical support.

User Access Verification

Password:
```

例：ログイン バナーの設定

次の例は、開始および終了デリミタにドル記号（$）を使用して、にログイン バナーを設定する方法を示しています。

```
スイッチ(config)# banner login $

Access for authorized users only. Please enter your username and password.

$
```

```
スイッチ(config)#
```

例：MAC アドレス変更通知トラップの設定

次に、NMS として 172.20.10.10 を指定し、NMS への MAC アドレス通知トラップの送信をイネーブルにし、MAC アドレス変更通知機能をイネーブルにし、インターバル タイムを 123 秒に設定し、履歴サイズを 100 エントリに設定し、特定のポートで MAC アドレスが追加された場合のトラップをイネーブルにする例を示します。

```
スイッチ(config)# snmp-server host 172.20.10.10 traps private mac-notification
スイッチ(config)# snmp-server enable traps mac-notification change
スイッチ(config)# mac address-table notification change
スイッチ(config)# mac address-table notification change interval 123
スイッチ(config)# mac address-table notification change history-size 100
スイッチ(config)# interface gigabitethernet1/2/1
スイッチ(config-if)# snmp trap mac-notification change added
```

例：MAC しきい値通知トラップの設定

次に、NMS として 172.20.10.10 を指定し、MAC アドレスしきい値通知機能をイネーブルにし、インターバル タイムを 123 秒に設定し、制限を 78% に設定する例を示します。

```
スイッチ(config)# snmp-server host 172.20.10.10 traps private mac-notification
スイッチ(config)# snmp-server enable traps mac-notification threshold
スイッチ(config)# mac address-table notification threshold
スイッチ(config)# mac address-table notification threshold interval 123
スイッチ(config)# mac address-table notification threshold limit 78
```

例：MAC アドレス テーブルへのスタティック アドレスの追加

次の例では、MAC アドレス テーブルにスタティック アドレス c2f3.220a.12f4 を追加する方法を示します。VLAN 4 でこの MAC アドレスを宛先アドレスとして持つパケットを受信すると、パケットは指定されたポートに転送されます。

```
スイッチ(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet1/1/1
```

例：ユニキャスト MAC アドレス フィルタリングの設定

次に、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つドロップ パケットを設定する例を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

```
スイッチ(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

スイッチ管理に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference (Catalyst 3650 Switches)*
ネットワーク管理の設定	*Network Management Configuration Guide (Catalyst 3650 Switches)*
レイヤ 2 の設定	*Layer 2/3 Configuration Guide (Catalyst 3650 Switches)*
VLAN コンフィギュレーション	*VLAN Configuration Guide (Catalyst 3650 Switches)*
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S（Catalyst 3850 Switches）*
プラットフォームに依存しない設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S（Catalyst 3850 Switches）* *IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S（Catalyst 3850 Switches）*

標準および **RFC**

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

スイッチ管理に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference (Catalyst 3650 Switches)*
ネットワーク管理の設定	*Network Management Configuration Guide (Catalyst 3650 Switches)*
レイヤ 2 の設定	*Layer 2/3 Configuration Guide (Catalyst 3650 Switches)*

関連項目	マニュアル タイトル
VLAN コンフィギュレーション	*VLAN Configuration Guide (Catalyst 3650 Switches)*
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S*（*Catalyst 3650 Switches*）
プラットフォームに依存しない設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S*（*Catalyst 3650 Switches*） *IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S*（*Catalyst 3650 Switches*）

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

スイッチ管理の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 83 章

スイッチのセットアップ設定の実行

- 機能情報の確認，1995 ページ
- スイッチセットアップ設定の実行に関する情報，1995 ページ
- スイッチ設定コンフィギュレーションの実行方法，2011 ページ
- スイッチのセットアップ設定のモニタリング，2030 ページ
- スイッチ のセットアップを実行する場合の設定例，2034 ページ
- スイッチのセットアップの実行に関する追加情報，2035 ページ
- WCM サブパッケージのインストール，2037 ページ
- スイッチセットアップ設定の機能履歴と情報，2039 ページ

機能情報の確認

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

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

スイッチセットアップ設定の実行に関する情報

IP アドレスの割り当ておよび DHCP 自動設定を含む初期スイッチ設定タスクを実行する前に、このモジュールのセクションを確認します。

スイッチブート プロセス

スイッチを起動するには、ハードウェアインストレーションガイドの手順にしたがって、スイッチを設置して電源をオンにし、スイッチの初期設定（IP アドレス、サブネットマスク、デフォルト ゲートウェイ、シークレット、Telnet パスワードなど）を行う必要があります。

通常の起動プロセスにはブートローダ ソフトウェアの動作が含まれ、以下のアクティビティが実行されます。

- 下位レベルの CPU 初期化を行います。CPU レジスタを初期化することにより、物理メモリがマッピングされる場所、容量、速度などを制御します。
- CPU サブシステムの電源投入時セルフ テスト（POST）を実行し、システム DRAM をテストします。
- システム ボード上のファイル システムを初期化します。
- デフォルトのオペレーティング システム ソフトウェア イメージをメモリにロードし、スイッチを起動します。

ブート ローダにより、オペレーティング システムがロードされる前に、ファイル システムにアクセスすることができます。ブートローダの使用目的は通常、オペレーティング システムのロード、展開、および起動に限定されます。オペレーティング システムが CPU を制御できるようになると、ブートローダは、次にシステムがリセットされるか電源が投入されるまでは非アクティブになります。

また、オペレーティング システムが使用不可能になるほどの重大な障害が発生した場合は、ブートローダはシステムにトラップドアからアクセスします。トラップドア メカニズムによりシステムへのアクセスを十分に行うことで、必要に応じて、XMODEM プロトコルを使用してオペレーティング システムのソフトウェア イメージを再インストールし、失われたパスワードを回復し、最終的にオペレーティング システムを再起動できます。

スイッチ情報を割り当てるには、PC または端末をコンソール ポートに接続するか、PC をイーサネット管理ポートに接続して、PC または端末エミュレーション ソフトウェアのボーレートおよびキャラクタ フォーマットをスイッチのコンソール ポートの設定と一致させておく必要があります。

- デフォルトのボーレートは 9600 です。
- デフォルトのデータ ビットは 8 です。

（注） データ ビット オプションを 8 に設定した場合、パリティ オプションは「なし」に設定します。

- デフォルトのストップ ビットは 2（マイナー）です。
- デフォルトのパリティ設定は「なし」です。

ソフトウェア インストーラ機能

次のスイッチでソフトウェア インストーラ機能がサポートされます。

- スタンドアロン スイッチ、スイッチ スタック、またはスタック内のスイッチのサブセットでのソフトウェア バンドルのインストール。デフォルトでは、スイッチ スタックが設定されている場合、すべてのスイッチでインストールが行われます。
- スイッチのスタックでは、すべてのスイッチをインストール モードすることが推奨されます。
- 以前にインストールしたパッケージ セットへのソフトウェア ロールバック。
- 有効なインストール済みパッケージがブート フラッシュに存在しない場合の緊急インストール。
- 互換性のないソフトウェアを持つスイッチ スタックに参加しているスイッチの自動アップグレード。
- スイッチ スタック内の別のスイッチにパッケージをインストールするための供給元として 1 台のスイッチのパッケージを使用してのインストール。

（注） ソフトウェア インストールおよびロールバックは、インストール モードのみで実行しているときに行う必要があります。**software expand** EXEC コマンドを使用すると、ブートのバンドル モードをインストール モードに変換できます。

ソフトウェアのブート モード

スイッチでは、ソフトウェア パッケージを起動するための次の 2 種類のモードがサポートされています。

- インストール モード
- バンドル モード

関連トピック

例 : インストール モードでのソフトウェアブートアップ ディスプレイ, （2031 ページ）
例 : 緊急インストール, （2032 ページ）

インストール モードでのブート

以下のフラッシュ内のソフトウェア パッケージのプロビジョニング ファイルを起動して、インストール モードでスイッチを起動できます:

```
スイッチ: boot flash:packages.conf
```

プロビジョニングファイルには、起動、マウント、実行するソフトウェアパッケージのリストが含まれます。インストールされている各パッケージの ISO ファイル システムは、フラッシュからルート ファイル システムに直接マウントされます。

（注） インストール モードで起動するために使用するパッケージとプロビジョニング ファイルは、フラッシュに保存する必要があります。usbflash0 または tftp: からインストール モードで起動することはサポートされていません。

関連トピック

例 : インストール モードでのソフトウェアブートアップ ディスプレイ，（2031 ページ）

例：緊急インストール，（2032 ページ）

バンドル モードでのブート

バンドル（.bin）ファイルを使用して、スイッチ をバンドル モードでブートできます：

```
switch:  boot flash:cat3850-universalk9.SSA.03.08.83.EMD.150-8.83.EMD.bin
```

バンドルに含まれるプロビジョニング ファイルは、どのパッケージを起動、マウント、および実行するかを判断するために使用されます。パッケージはバンドルから取得され、RAM にコピーされます。各パッケージの ISO ファイル システムは、ルート ファイル システムにマウントされます。

インストールモードでの起動とは異なり、バンドルモードでの起動では、バンドルのサイズに対応するサイズの追加メモリが使用されます。

インストールモードでの起動とは異なり、バンドルモードでの起動は複数のメディアから利用できます：

- flash:
- usbflash0:
- tftp:

（注） バンドル モードでの起動では、自動インストールおよびスマート インストール機能はサポートされません。

（注） バンドル モードでの起動では、AP イメージのプレダウンロード機能はサポートされません。プレダウンロード機能の詳細については、Cisco WLC 5700 シリーズの「*Preloading an Image to Access Points*（アクセス ポイントへのイメージのダウンロード）」の章を参照してください。

関連トピック

例 : インストール モードでのソフトウェアブートアップ ディスプレイ，（2031 ページ）
例：緊急インストール，（2032 ページ）

スイッチ スタックのブート モード

スタック内のすべてのスイッチは、インストールモードまたはブートモードで実行している必要があります。混合モードのスタックはサポートされません。新しいスイッチが、別のブート モードのスタックに参加する場合、新しいスイッチは、V 不一致状態となります。

混合モードのスイッチ スタックが同時に起動する場合、アクティブ スイッチを除くすべてのスイッチは、V 不一致状態となります。ブート モードが自動アップグレードをサポートしない場合、スイッチ スタック メンバはアクティブ スイッチと同じブート モードで再起動する必要があります。

スタックがインストールモードで実行されている場合、スイッチスタックに参加しようとしている新しいスイッチを自動的にアップグレードするために、自動アップグレード機能が使用できます。

自動アップグレード機能により新しいスイッチのブートモードがインストールモードに変更されます。スタックがバンドル モードでのブートで実行されている場合、自動アップグレード機能は使用できなくなります。スイッチスタックに参加できるように、バンドルモードを使用して新しいスイッチを起動する必要があります。

次の例では、ブート モードがアクティブ スイッチと互換性がない場合に、スイッチ スタックに参加しようとするスイッチの状態を示します。

```
スイッチ# show switch

Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch#   Role   Mac Address     Priority Version   State
-----------------------------------------------------------
 1       Member 6400 f125.1a00   1        0         V-Mismatch
*2       Active 6400.f125.1100   1        V01       Ready
スイッチ
```

スイッチ情報の割り当て

IP 情報を割り当てるには、スイッチのセットアップ プログラムを使用する方法、Dynamic Host Configuration Protocol（DHCP）サーバを使用する方法、または手動で実行する方法があります。

特定のIP情報の設定が必要な場合、スイッチのセットアッププログラムを使用してください。このプログラムを使用すると、ホスト名とイネーブルシークレットパスワードを設定することもできます。

また、任意で、Telnetパスワードを割り当てたり（リモート管理中のセキュリティ確保のため）、スイッチをクラスタのコマンドまたはメンバスイッチとして、あるいはスタンドアロンスイッチとして設定したりできます。

サーバの設定後は DHCP サーバを使用して、IP 情報の集中管理と自動割り当てを行います。

（注） DHCP を使用している場合は、スイッチが動的に割り当てられた IP アドレスを受信してコンフィギュレーション ファイルを読み込むまでは、セットアップ プログラムからの質問に応答しないでください。

スイッチの設定手順を熟知している経験豊富なユーザの場合は、スイッチを手動で設定してください。それ以外のユーザは、「ブートプロセス」で説明したセットアッププログラムを使用してください。

デフォルトのスイッチ情報

表 *141*：デフォルトのスイッチ情報

機能	デフォルト設定
IP アドレスおよびサブネット マスク	IP アドレスまたはサブネット マスクは定義されていません。
デフォルト ゲートウェイ	デフォルト ゲートウェイは定義されていません。
イネーブル シークレット パスワード	パスワードは定義されていません。
ホスト名	出荷時に割り当てられるデフォルトのホスト名は、スイッチ です。
Telnet パスワード	パスワードは定義されていません。
クラスタ コマンド スイッチ機能	ディセーブル
クラスタ名	クラスタ名は定義されません。

DHCP ベースの自動設定の概要

DHCP は、インターネットホストおよびインターネットワーキング デバイスに設定情報を提供します。このプロトコルには、2つのコンポーネントがあります。1つはDHCPサーバからデバイスにコンフィギュレーション パラメータを提供するコンポーネント、もう 1 つはデバイスにネットワーク アドレスを割り当てるコンポーネントです。DHCPはクライアント/サーバモデルに基づい

ています。指定されたDHCPサーバが、動的に設定されるデバイスに対して、ネットワーク アドレスを割り当て、コンフィギュレーション パラメータを提供します。スイッチは、DHCP クライアントおよびDHCP サーバとして機能できます。

DHCP ベースの自動設定では、スイッチ（DHCP クライアント）は起動時に、IP アドレス情報およびコンフィギュレーション ファイルを使用して自動的に設定されます。

DHCP ベースの自動設定を使用すると、スイッチ上でDHCP クライアント側の設定を行う必要はありません。ただし、DHCP サーバで、IP アドレスに関連した各種リース オプションを設定する必要があります。

DHCPを使用してネットワーク上のコンフィギュレーションファイルの場所をリレーする場合は、TFTPサーバおよびドメイン ネーム システム（DNS）サーバの設定が必要になることがあります。

（注） スイッチ スタックとDHCP、DNS、TFTP サーバとの間では冗長接続を確立することを推奨します。接続されているスタック メンバーがスイッチ スタックから削除された場合でも、これらのサーバがアクセス可能なまま維持されるように保証するうえで役立ちます。

スイッチのDHCP サーバは、スイッチと同じLAN 上に配置することも、そのスイッチとは別のLAN 上に配置することもできます。DHCP サーバが異なるLAN 上で動作している場合、スイッチとDHCP サーバ間に、DHCP のリレー デバイスを設定する必要があります。リレー デバイスは、直接接続されている2 つのLAN 間でブロードキャスト トラフィックを転送します。ルータはブロードキャストパケットを転送しませんが、受信したパケットの宛先IPアドレスに基づいてパケットを転送します。

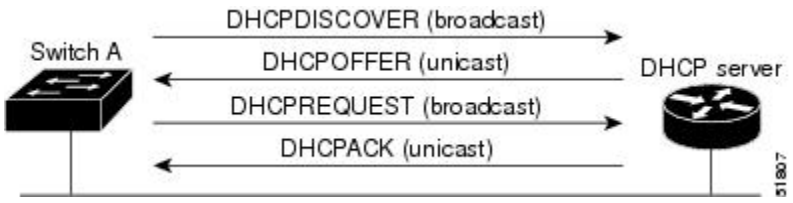
DHCP ベースの自動設定は、スイッチのBOOTP クライアント機能に代わるものです。

DHCP クライアントの要求プロセス

スイッチを起動したときに、スイッチにコンフィギュレーション ファイルがない場合、DHCP クライアントが呼び出され、DHCPクライアントがDHCPサーバに設定情報を要求します。コンフィギュレーション ファイルが存在し、その設定に特定のルーテッド インターフェイスの **ip address dhcp** インターフェイス コンフィギュレーション コマンドが含まれる場合、DHCP クライアントが呼び出され、DHCP クライアントがインターフェイスにIP アドレス情報を要求します。

次は、DHCP クライアントとDHCP サーバの間で交換される一連のメッセージです。

図 *95*：*DHCP* クライアント/サーバ間のメッセージ交換



クライアントであるスイッチAは、DHCPサーバの場所を特定するために、DHCPDISCOVERメッセージをブロードキャストします。DHCPサーバは、DHCPOFFERユニキャストメッセージによっ

て、使用可能なコンフィギュレーション パラメータ（IP アドレス、サブネット マスク、ゲートウェイ IP アドレス、DNS IP アドレス、IP アドレス用のリースなど）をクライアントに提示します。

DHCPREQUESTブロードキャストメッセージでは、クライアントは、提示された設定情報に対して、DHCP サーバに正式な要求を戻します。この正式な要求はブロードキャストされるため、クライアントから DHCPDISCOVER ブロードキャスト メッセージを受信した他のすべての DHCP サーバは、クライアントに提示した IP アドレスを再利用できます。

DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに戻すことで、IP アドレスがクライアントに割り当てられたことを確認します。このメッセージによって、クライアントとサーバはバウンドされ、クライアントはサーバから受信した設定情報を使用します。スイッチの受信する情報量は、DHCP サーバの設定方法によって異なります。

DHCPOFFERユニキャストメッセージによって送信されたコンフィギュレーションパラメータが無効である（コンフィギュレーション エラーがある）場合、クライアントは DHCP サーバに、DHCPDECLINE ブロードキャスト メッセージを戻します。

DHCP サーバはクライアントに、提示されたコンフィギュレーション パラメータが割り当てられていない、パラメータのネゴシエーション中にエラーが発生した、または DHCPOFFER メッセージに対するクライアントの応答が遅れている（DHCP サーバがパラメータを別のクライアントに割り当てた）という意味の DHCPNAK 拒否ブロードキャスト メッセージを送信します。

DHCP クライアントは、複数の DHCP サーバまたは BOOTP サーバから提示を受け取り、そのうちの任意の 1 つを受け入れることができますが、通常は最初に受け取った提示を受け入れます。DHCP サーバから提示された IP アドレスが必ずしもクライアントに割り当てられるわけではありません。ただし、サーバは通常、クライアントが正式にアドレスを要求するまではアドレスを確保しておきます。スイッチがBOOTPサーバからの応答を受け入れ、自身を設定する場合、スイッチはスイッチ コンフィギュレーション ファイルを取得するために、TFTP 要求をユニキャストするのではなくブロードキャストします。

DHCP ホスト名オプションにより、スイッチのグループはホスト名および標準コンフィギュレーションを集中管理型DHCPサーバから取得できます。クライアント（スイッチ）はDCHPDISCOVERメッセージ内に、DHCP サーバからのホスト名および他のコンフィギュレーション パラメータの要求に使用される Option 12 フィールドを加えます。すべてのクライアントのコンフィギュレーション ファイルは、DHCP から取得したホスト名を除き、まったく同じです。

クライアントにデフォルトのホスト名がある場合（**hostname***name* グローバル コンフィギュレーション コマンドを設定していないか、**no hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を削除していない場合）は、**ip address dhcp** インターフェイス コンフィギュレーション コマンドを入力すると、DHCP のホスト名オプションがパケットに含まれません。この場合、インターフェイスの IP アドレスを取得中にクライアントが DHCP との相互作用で DHCP ホスト名オプションを受信した場合、クライアントは DHCP ホスト名オプションを受け入れて、システムに設定済みのホスト名があることを示すフラグが設定されます。

DHCP ベースの自動設定およびイメージ アップデート

DHCP イメージ アップグレード機能を使用すると、ネットワーク内の 1 つ以上のスイッチに新しいイメージ ファイルおよび新しいコンフィギュレーション ファイルをダウンロードするように

DHCP サーバを設定できます。ネットワーク内のすべてのスイッチでのイメージおよびコンフィギュレーションの同時アップグレードによって、ネットワークに加えられたそれぞれの新しいスイッチが、同じイメージとコンフィギュレーションを確実に受信するようになります。

DHCP イメージ アップグレードには、自動設定およびイメージ アップデートの 2 つのタイプがあります。

DHCP ベースの自動設定の制約事項

- ネットワーク内に割り当てられた IP アドレスがなく、1 つ以上のレイヤ 3 インターフェイスが起動してない場合は、設定プロセスが保存された DHCP ベースの自動設定は停止します。
- タイムアウトを設定しない限り、設定機能を備えている DHCP ベースの自動設定は IP アドレスのダウンロードを無期限に繰り返します。
- コンフィギュレーション ファイルをダウンロードできないか破損している場合は、自動インストールプロセスが停止します。
- TFTP からダウンロードされたコンフィギュレーション ファイルは、実行コンフィギュレーション内の既存コンフィギュレーションとマージされますが、**write memory** または **copy running-configuration startup-configuration** 特権 EXEC コマンドを入力しない限り、NVRAM に保存されません。ダウンロードされたコンフィギュレーションがスタートアップコンフィギュレーションに保存された場合、後続のシステム再起動中にこの機能はトリガーされません。

DHCP 自動設定

DHCP 自動設定は、コンフィギュレーション ファイルを DHCP サーバからネットワーク内の 1 つ以上のスイッチにダウンロードします。ダウンロードされたコンフィギュレーション ファイルは、スイッチの実行コンフィギュレーション ファイルになります。このファイルは、スイッチがリロードされるまで、フラッシュ メモリに保存されたブートアップ コンフィギュレーションを上書きしません。

DHCP 自動イメージ アップデート

DHCP 自動設定とともに DHCP 自動イメージ アップグレードを使用すると、コンフィギュレーションおよび新しいイメージをネットワーク内の 1 つ以上のスイッチにダウンロードできます。新しいコンフィギュレーションおよび新しいイメージをダウンロードしている 1 つのスイッチスイッチ（または複数のスイッチ）は、ブランク（つまり、出荷時のデフォルト設定がロードされている状態）にできます。

コンフィギュレーションをすでに持っているスイッチに新しいコンフィギュレーションをダウンロードすると、ダウンロードされたコンフィギュレーションは、スイッチに保存されているコンフィギュレーションファイルに追加されます（どの既存のコンフィギュレーションファイルも、ダウンロードされたファイルに上書きされません）。

スイッチの DHCP 自動イメージアップデートをイネーブルにするには、イメージ ファイルおよびコンフィギュレーション ファイルがある TFTP サーバを、正しいオプション 67（コンフィギュ

レーションファイル名）、オプション66（DHCPサーバホスト名）、オプション150（TFTPサーバアドレス）、およびオプション125（Cisco IOSイメージファイルの説明）の設定で設定する必要があります。

スイッチをネットワークに設置すると、自動イメージアップデート機能が開始します。ダウンロードされたコンフィギュレーションファイルはスイッチの実行コンフィギュレーションに保存され、新しいイメージがダウンロードされてスイッチにインストールされます。スイッチを再起動すると、このコンフィギュレーションがスイッチのコンフィギュレーションに保存されます。

DHCP サーバ設定時の注意事項

デバイスを DHCP サーバとして設定する場合、次の注意事項に従ってください。

- DHCPサーバには、スイッチのハードウェアアドレスによって各スイッチと結び付けられている予約済みのリースを設定する必要があります。
- スイッチに IP アドレス情報を受信させるには、DHCP サーバに次のリース オプションを設定する必要があります。
  - クライアントの IP アドレス（必須）
  - クライアントのサブネット マスク（必須）
  - DNS サーバの IP アドレス（任意）
  - ルータの IP アドレス（スイッチで使用するデフォルト ゲートウェイ アドレス）（必須）
- スイッチに TFTP サーバからコンフィギュレーション ファイルを受信させる場合は、DHCP サーバに次のリース オプションを設定する必要があります。
  - TFTP サーバ名（必須）
  - ブート ファイル名（クライアントが必要とするコンフィギュレーション ファイル名）（推奨）
  - ホスト名（任意）
- DHCPサーバの設定によっては、スイッチはIPアドレス情報またはコンフィギュレーションファイル、あるいはその両方を受信できます。
- 前述のリースオプションを設定しなかった場合、DHCPサーバは、設定されたパラメータのみを使用してクライアントの要求に応答します。IPアドレスおよびサブネットマスクが応答に含まれていないと、スイッチは設定されません。ルータのIPアドレスまたはTFTPサーバ名が見つからなかった場合、スイッチはTFTP要求をユニキャストしないでブロードキャストする場合があります。その他のリースオプションは、使用できなくても自動設定には影響しません。
- スイッチはDHCPサーバとして動作可能です。デフォルトでは、Cisco IOS DHCPサーバおよびDHCPリレーエージェント機能はスイッチ上でイネーブルにされていますが、設定されていません。（これらの機能は動作しません。）

TFTP サーバの目的

DHCP サーバの設定に基づいて、スイッチは TFTP サーバから 1 つまたは複数のコンフィギュレーション ファイルをダウンロードしようとします。TFTP サーバへの IP 接続に必要なすべてのオプションについてスイッチに応答するよう DHCP を設定している場合で、なおかつ、TFTP サーバ名、アドレス、およびコンフィギュレーション ファイル名を指定して DHCP サーバを設定している場合、スイッチは指定された TFTP サーバから指定されたコンフィギュレーション ファイルをダウンロードしようとします。

コンフィギュレーション ファイル名、および TFTP サーバを指定しなかった場合、またはコンフィギュレーション ファイルをダウンロードできなかった場合は、スイッチはファイル名と TFTP サーバアドレスをさまざまに組み合わせてコンフィギュレーション ファイルをダウンロードしようとします。ファイルには、特定のコンフィギュレーション ファイル名（存在する場合）と次のファイルが指定されています。network-config、cisconet.cfg、*hostname*.config、または *hostname*.cfg です。この場合、*hostname* はスイッチの現在のホスト名です。使用される TFTP サーバアドレスには、（存在する場合）指定された TFTP サーバのアドレス、およびブロードキャスト アドレス（255.255.255.255）が含まれています。

スイッチが正常にコンフィギュレーション ファイルをダウンロードするには、TFTP サーバのベース ディレクトリに 1 つまたは複数のコンフィギュレーション ファイルが含まれていなければなりません。含めることのできるファイルは、次のとおりです。

- DHCP 応答で指定されているコンフィギュレーション ファイル（実際のスイッチ コンフィギュレーション ファイル）。
- network-confg または cisconet.cfg ファイル（デフォルトのコンフィギュレーション ファイル）
- router-confg または ciscortr.cfg ファイル（これらのファイルには、すべてのスイッチに共通のコマンドが含まれています。通常、DHCP および TFTP サーバが適切に設定されていれば、これらのファイルはアクセスされません）

DHCP サーバ リース データベースに TFTP サーバ名を指定する場合は、DNS サーバのデータベースに TFTP サーバ名と IP アドレスのマッピングを設定することも必要です。

使用する TFTP サーバが、スイッチとは異なる LAN 上にある場合、またはスイッチがブロードキャスト アドレスを使用してアクセスした場合（前述のすべての必須情報が DHCP サーバの応答に含まれていない場合に発生）は、リレーを設定して TFTP サーバに TFTP パケットを転送する必要があります。適切な解決方法は、必要なすべての情報を使用して DHCP サーバを設定することです。

DNS サーバの目的

DHCP サーバは、DNS サーバを使用して TFTP サーバ名を IP アドレスに変換します。DNS サーバ上で、TFTP サーバ名から IP アドレスへのマッピングを設定する必要があります。TFTP サーバには、スイッチのコンフィギュレーション ファイルが存在します。

DHCP の応答時に IP アドレスを取得する DHCP サーバのリース データベースに、DNS サーバの IP アドレスを設定できます。リース データベースには、DNS サーバの IP アドレスを 2 つまで入力できます。

DNS サーバは、スイッチと同じ LAN 上に配置することも、別の LAN 上に配置することもできます。DNS サーバが別の LAN 上に存在する場合、スイッチはルータを介して DNS サーバにアクセスできなければなりません。

コンフィギュレーション ファイルの入手方法

IP アドレスおよびコンフィギュレーション ファイル名が DHCP で専用のリースとして取得できるかどうかに応じて、スイッチは次の方法で設定情報を入手します。

- IP アドレスおよびコンフィギュレーション ファイル名が、スイッチ用に予約され、DHCP 応答（1 ファイル読み込み方式）で提供されている場合

  スイッチは DHCP サーバから、IP アドレス、サブネット マスク、TFTP サーバ アドレス、およびコンフィギュレーション ファイル名を受信します。スイッチは、TFTP サーバにユニキャスト メッセージを送信し、指定されたコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、ブートアップ プロセスを完了します。

- スイッチの IP アドレスおよびコンフィギュレーション ファイル名が予約されているが、DHCP 応答に TFTP サーバ アドレスが含まれていない場合（1 ファイル読み込み方式）。

  スイッチは DHCP サーバから、IP アドレス、サブネット マスク、およびコンフィギュレーション ファイル名を受信します。スイッチは、TFTP サーバにブロードキャスト メッセージを送信し、指定されたコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、ブートアップ プロセスを完了します。

- IP アドレスだけがスイッチ用に予約され、DHCP 応答で提供されており、コンフィギュレーション ファイル名は提供されない場合（2 ファイル読み込み方式）

  スイッチ は DHCP サーバから、IP アドレス、サブネット マスク、および TFTP サーバ アドレスを受信します。スイッチは、TFTP サーバにユニキャストメッセージを送信し、network-confg または cisconet.cfg のデフォルト コンフィギュレーション ファイルを取得します（network-confg ファイルが読み込めない場合、スイッチは cisconet.cfg ファイルを読み込みます）。

  デフォルト コンフィギュレーション ファイルには、スイッチのホスト名から IP アドレスへのマッピングが含まれています。スイッチは、ファイルの情報をホスト テーブルに書き込み、ホスト名を入手します。ファイルにホスト名がない場合、スイッチは DHCP 応答で指定されたホスト名を使用します。DHCP 応答でホスト名が指定されていない場合、スイッチはデフォルトのスイッチをホスト名として使用します。

  デフォルトのコンフィギュレーション ファイルまたは DHCP 応答からホスト名を入手した後、スイッチはホスト名と同じ名前のコンフィギュレーション ファイル（network-confg または cisconet.cfg のどちらが先に読み込まれたかに応じて、*hostname*-confg または *hostname*.cfg）を TFTP サーバから読み込みます。cisconet.cfg ファイルが読み込まれている場合は、ホストのファイル名は 8 文字に切り捨てられます。

  network-confg、cisconet.cfg、またはホスト名と同じ名前のファイルを読み込むことができない場合、スイッチは router-confg ファイルを読み込みます。router-confg ファイルを読み込むことができない場合、スイッチは ciscortr.cfg ファイルを読み込みます。

（注） DHCP 応答から TFTP サーバを入手できなかった場合、ユニキャスト伝送によるコンフィギュレーション ファイルの読み込みにすべて失敗した場合、または TFTP サーバ名を IP アドレスに変換できない場合には、スイッチは TFTP サーバ要求をブロードキャストします。

環境変数の制御方法

通常動作スイッチでは、9600 bps に設定されているコンソール接続のみを通じてブート ローダ モードを開始します。電源コードを再接続中にスイッチ電源コードを取り外し、[Mode] ボタンを押します。すべてのオレンジのシステム LED が点灯したままになったら、[Mode] ボタンを放してもかまいません。ブートローダの スイッチ プロンプトが表示されます。

スイッチのブート ローダ ソフトウェアは不揮発性の環境変数をサポートするため、これらの環境変数を使用して、ブート ローダまたはシステムで稼働する他のソフトウェアの動作を制御できます。ブートローダの環境変数は、UNIX または DOS システムで設定できる環境変数と類似しています。

値を持つ環境変数は、フラッシュ ファイル システムの外にあるフラッシュ メモリに保存されます。

ファイルの各行には、環境変数名と等号に続いて、その変数の値が指定されます。変数が存在しない場合は、変数の値はありません。値がヌル ストリングと表示された場合は、変数に値が設定されています。ヌル ストリング（たとえば""）が設定されている変数は、値が設定された変数です。多くの環境変数は事前に定義されており、デフォルト値が設定されています。

環境変数の設定を変更するには、ブートローダにアクセスするか、Cisco IOS コマンドを使用します。通常の環境では、環境変数の設定を変更する必要はありません。

一般的な環境変数

この表では、最も一般的な環境変数の機能について説明します。

表 *142*：一般的な環境変数

変数	ブートローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
BOOT	**set BOOT***filesystem***:/***file-url* ... 自動起動時にロードして実行を試みる、セミコロンで区切られた実行可能ファイルのリスト。	**boot system** {*filesystem***:/***file-url* ...| **switch** {*number* | **all**}} 次の起動時にロードする Cisco IOS イメージと、イメージがロードされるスタック メンバーを指定します。このコマンドは、BOOT 環境変数の設定を変更します。 パッケージプロビジョニング ファイルは、*packages.conf* ファイルとも呼ばれ、起動時にどのソフトウェア パッケージをアクティブ化するかを判断するために、システムが使用するものです。 • インストールモードで起動する場合、アクティブ化するパッケージを指定するために、**boot** コマンドで指定されたパッケージプロビジョニング ファイルが使用されます。例：**boot flash:packages.conf**。 • バンドルモードで起動する場合、起動したバンドルに含まれているパッケージのプロビジョニング ファイルがバンドルに含まれているパッケージのアクティブ化に使用されます。例：**boot flash:image.bin**。

変数	ブートローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
MANUAL_BOOT	**set MANUAL_BOOT yes** スイッチの起動を自動で行うか手動で行うかを決定します。 有効な値は 1、yes、0、および no です。no または 0 に設定されている場合、ブートローダはシステムを自動的に起動しようとします。それ以外の値に設定されている場合は、ブートローダ モードから手動でスイッチを起動する必要があります。	**boot manual** 次回の起動時にスイッチを手動で起動できるようにします。MANUAL_BOOT 環境変数の設定が変更されます。 次回のシステム再起動時には、スイッチはブートローダ モードになります。システムを起動するには、**boot flash:***filesystem*:/*file-url* ブートローダ コマンドを使用し、起動可能イメージの名前を指定します。
CONFIG_FILE	**set CONFIG_FILE flash:**/*file-url* Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を変更します。	**boot config-file flash:**/*file-url* Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。このコマンドによって、CONFIG_FILE 環境変数が変更されます。
SWITCH_NUMBER	**set SWITCH_NUMBER***stack-member-number* スタック メンバのメンバ番号を変更します。	**switch***current-stack-member-number***renumber***new-stack-member-number* スタック メンバのメンバ番号を変更します。
SWITCH_PRIORITY	**set SWITCH_PRIORITY***stack-member-number* スタック メンバのプライオリティ値を変更します。	**switch***stack-member-number***priority***priority-number* スタック メンバのプライオリティ値を変更します。
BAUD	**set BAUD** *baud-rate*	**line console 0** **speed***speed-value* ボー レートを設定します。
ENABLE_BREAK	**set ENABLE_BREAK yes/no**	**boot enable-break switch yes/no** 自動起動時の break をイネーブルにします。**break** コマンドの入力に与えられた時間は 5 秒です。

TFTP の環境変数

イーサネット管理ポートを通してスイッチに PC を接続していると、TFTP でブートローダに対してコンフィギュレーション ファイルのアップロードまたはダウンロードができます。このテーブルの環境変数が設定されていることを確認します。

表 *143* : *TFTP* の環境変数

変数	説明
MAC_ADDR	スイッチの MAC アドレスを指定します。 （注） 変数は変更しないことを推奨します。 ただし、ブートローダを稼働した後に変数を変更した場合、またはこの変数が保存されている値と異なる場合は、TFTP を使用する前にこのコマンドを入力します。
IP_ADDR	スイッチの関連付けられた IP サブネットに IP アドレスおよびサブネット マスクを指定します。
DEFAULT_ROUTER	デフォルト ゲートウェイに IP アドレスおよびサブネット マスクを指定します。

ソフトウェア イメージのリロードのスケジューリング

スイッチ上でソフトウェア イメージのリロードを後で（深夜や週末など、スイッチをあまり使用しないときに）行うよう、スケジュールを設定できます。または（ネットワーク内のすべてのスイッチでソフトウェアのアップグレードを実行する場合などに）ネットワーク全体でリロードを同時に行うことができます。

（注） リロードのスケジュールは、約 24 日以内に設定する必要があります。

リロード オプションには以下のものがあります。

- 指定した分数、または時間および分数が経過したときに、ソフトウェアがリロードされます。リロードは、約 24 時間以内に実行する必要があります。最大 255 文字で、リロードの理由を指定できます。

- ソフトウェアのリロードが（24時間制で）指定された時間に有効になります。月日を指定すると、指定された日時にリロードが行われるようにスケジュールが設定されます。月日を指定しなかった場合、リロードは当日の指定時刻に行われます（指定時刻が現時刻より後の場合）。または翌日の指定時刻に行われます（指定時刻が現在時刻よりも前の場合）。00:00を指定すると、深夜0時のリロードが設定されます。

reload コマンドはシステムを停止させます。手動で起動することが設定されていない限り、システムは自動的に再起動します。

手動で起動するようにスイッチが設定されている場合、仮想端末からリロードを実行しないでください。これは、スイッチがブート ローダ モードになることでリモート ユーザが制御を失う、ということを防止するための制約です。

コンフィギュレーション ファイルを変更すると、リロードの前にコンフィギュレーションを保存するように指示するプロンプトがスイッチにより表示されます。保存操作時に、CONFIG_FILE環境変数がすでに存在しないスタートアップコンフィギュレーションファイルを示していた場合、保存を続行するかどうかという問い合わせがシステムから出されます。その状況のまま続けると、リロード時にセットアップ モードが開始されます。

スケジュールがすでに設定されたリロードを取り消すには、**reload cancel** 特権 EXEC コマンドを使用します。

スイッチ設定コンフィギュレーションの実行方法

DHCP を使用してスイッチに新しいイメージおよび新しいコンフィギュレーションをダウンロードするには、少なくとも 2 つのスイッチ を設定する必要があります。1 つ目のスイッチは DHCP サーバおよびTFTPサーバと同じように機能し、2つ目のスイッチ（クライアント）は新しいコンフィギュレーション ファイル、または新しいコンフィギュレーション ファイルおよび新しいイメージ ファイルをダウンロードするように設定されています。

DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定

このタスクでは、新しい スイッチ。の自動設定をサポートできるように、ネットワーク内の既存のスイッチで TFTP や DHCP 設定の DHCP 自動設定を行う方法を示します。

手順の概要

1. **configure terminal**
2. **ip dhcp pool***poolname*
3. **boot***filename*
4. **network***network-number mask prefix-length*
5. **default-router***address*
6. **option 150***address*
7. **exit**
8. **tftp-server flash**:*filename.text*
9. **interface***interface-id*
10. **no switchport**
11. **ip address***address mask*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool***poolname* 例： スイッチ(config)# **ip dhcp pool pool**	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**boot***filename* 例： スイッチ(dhcp-config)# **boot config-boot.text**	ブート イメージとして使用されるコンフィギュレーション ファイルの名前を指定します。
ステップ 4	**network***network-number mask prefix-length* 例： スイッチ(dhcp-config)# **network 10.10.10.0**	DHCPアドレス プールのサブネット ネットワーク番号およびマスクを指定します。 （注） プレフィックス長は、アドレス プレフィックスを構成するビット数を指定します。プレフィックスは、クライアントのネットワーク マスクを指定する二者択一の方法です。プレフィックス長は、スラッシュ（/）で開始する必要があります。

	コマンドまたはアクション	目的
	255.255.255.0	
ステップ 5	**default-router***address* 例： スイッチ(dhcp-config)# **default-router 10.10.10.1**	DHCP クライアントのデフォルト ルータの IP アドレスを指定します。
ステップ 6	**option 150***address* 例： スイッチ(dhcp-config)# **option 150 10.10.10.1**	TFTP サーバの IP アドレスを指定します。
ステップ 7	**exit** 例： スイッチ(dhcp-config)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**tftp-server flash**:*filename.text* 例： スイッチ(config)# **tftp-server flash:config-boot.text**	TFTP サーバ上のコンフィギュレーション ファイルを指定します。
ステップ 9	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/4**	コンフィギュレーション ファイルを受信するクライアントのアドレスを指定します。
ステップ 10	**no switchport** 例： スイッチ(config-if)# **no switchport**	インターフェイスをレイヤ 3 モードにします。
ステップ 11	**ip address***address mask* 例： スイッチ(config-if)# **ip address 10.10.10.1 255.255.255.0**	IP アドレスとインターフェイスのマスクを指定します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

例：DHCP サーバとしてのスイッチの設定，（2034 ページ）

DHCP 自動イメージ アップデート（コンフィギュレーション ファイルおよびイメージ）の設定

このタスクでは、新しいスイッチのインストールをサポートするように既存のスイッチで TFTP および DHCP を設定する DHCP 自動設定について説明します。

はじめる前に

最初にスイッチにアップロードするテキスト ファイル（たとえば、autoinstall_dhcp）を作成します。テキスト ファイルに、ダウンロードするイメージの名前を指定します（たとえば、c3750e-ipservices-mz.122-44.3.SE.tarc3750x-ipservices-mz.122-53.3.SE2.tar）。このイメージは、bin ファイルでなく、tar ファイルである必要があります。

手順の概要

1. **configure terminal**
2. **ip dhcp pool***poolname*
3. **boot***filename*
4. **network***network-number mask prefix-length*
5. **default-router***address*
6. **option 150***address*
7. **option 125***hex*
8. **copy tftp flash***filename.txt*
9. **copy tftp flash***imagename.bin*
10. **exit**
11. **tftp-server flash:***config.text*
12. **tftp-server flash:***imagename.bin*
13. **tftp-server flash:***filename.txt*
14. **interface***interface-id*
15. **no switchport**
16. **ip address***address mask*
17. **end**
18. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool***poolname* 例： `スイッチ(config)# ip dhcp pool pool1`	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**boot***filename* 例： `スイッチ(dhcp-config)# boot config-boot.text`	ブート イメージとして使用されるファイルの名前を指定します。

	コマンドまたはアクション	目的
ステップ 4	**network***network-number mask prefix-length* 例： スイッチ(dhcp-config)# **network 10.10.10.0 255.255.255.0**	DHCPアドレスプールのサブネットネットワーク番号およびマスクを指定します。 （注） プレフィックス長は、アドレス プレフィックスを構成するビット数を指定します。プレフィックスは、クライアントのネットワーク マスクを指定する二者択一の方法です。プレフィックス長は、スラッシュ（/）で開始する必要があります。
ステップ 5	**default-router***address* 例： スイッチ(dhcp-config)# **default-router 10.10.10.1**	DHCP クライアントのデフォルト ルータの IPアドレスを指定します。
ステップ 6	**option 150***address* 例： スイッチ(dhcp-config)# **option 150 10.10.10.1**	TFTP サーバの IP アドレスを指定します。
ステップ 7	**option 125***hex* 例： スイッチ(dhcp-config)# **option 125 hex 0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370**	イメージ ファイルのパスを記述したテキスト ファイルのパスを指定します。
ステップ 8	**copy tftp flash***filename.txt* 例： スイッチ(config)# **copy tftp flash image.bin**	スイッチに、テキスト ファイルをアップロードします。
ステップ 9	**copy tftp flash***imagename.bin* 例： スイッチ(config)# **copy tftp flash image.bin**	スイッチに、新しいイメージの tar ファイルをアップロードします。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： スイッチ(dhcp-config)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**tftp-server flash:***config.text* 例： スイッチ(config)# **tftp-server flash:config-boot.text**	TFTP サーバ上の Cisco IOS コンフィギュレーション ファイルを指定します。
ステップ 12	**tftp-server flash:***imagename.bin* 例： スイッチ(config)# **tftp-server flash:image.bin**	TFTP サーバ上のイメージ名を指定します。
ステップ 13	**tftp-server flash:***filename.txt* 例： スイッチ(config)# **tftp-server flash:boot-config.text**	ダウンロードするイメージ ファイルの名前を記述したテキスト ファイルを指定します。
ステップ 14	**interface***interface-id* 例： スイッチ(config)# **interface gigabitEthernet1/0/4**	コンフィギュレーション ファイルを受信するクライアントのアドレスを指定します。
ステップ 15	**no switchport** 例： スイッチ(config-if)# **no switchport**	インターフェイスをレイヤ3モードにします。
ステップ 16	**ip address***address mask* 例： スイッチ(config-if)# **ip address 10.10.10.1 255.255.255.0**	IP アドレスとインターフェイスのマスクを指定します。
ステップ 17	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 18	**copyrunning-configstartup-config** 例： スイッチ(config-if)# **end**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：DHCP 自動イメージ アップデートの設定, （2034 ページ）

DHCP サーバからファイルをダウンロードするクライアントの設定

（注） レイヤ3インターフェイスだけを設定してイネーブルにする必要があります。保存されているコンフィギュレーションのDHCPベースの自動設定にIPアドレスを割り当てないでください。

手順の概要

1. **configure terminal**
2. **boot host dhcp**
3. **boot host retry timeout***timeout-value*
4. **banner config-save ^C***warning-message***^C**
5. **end**
6. **show boot**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot host dhcp** 例： スイッチ(conf)# **boot host dhcp**	保存されているコンフィギュレーションで自動設定をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**boot host retry timeout***timeout-value* 例： スイッチ(conf)# **boot host retry timeout 300**	（任意）システムがコンフィギュレーション ファイルをダウンロードしようとする時間を設定します。 （注） タイムアウトを設定しないと、システムは無期限に DHCP サーバから IP アドレスを取得しようとします。
ステップ 4	**banner config-save ^C***warning-message***^C** 例： スイッチ(conf)# **banner config-save ^C** **Caution - Saving Configuration File** **to NVRAM May Cause You to No longer** **Automatically Download Configuration Files** **at Reboot^C**	（任意）コンフィギュレーション ファイルをNVRAMに保存しようとするときに表示される警告メッセージを作成します。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show boot** 例： スイッチ# **show boot**	設定を確認します。

関連トピック

例：DHCP サーバから設定をダウンロードするためのスイッチの設定, （2034 ページ）

複数の SVI への IP 情報の手動割り当て

このタスクでは、複数のスイッチ仮想インターフェイス（SVI）に IP 情報を手動で割り当てる方法について説明します。

手順の概要

1. **configure terminal**
2. **interface vlan***vlan-id*
3. **ip address***ip-address subnet-mask*
4. **exit**
5. **ip default-gateway***ip-address*
6. **end**
7. **show interfaces vlan***vlan-id*
8. **show ip redirects**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan***vlan-id* 例： `スイッチ(config)# interface vlan 99`	インターフェイス コンフィギュレーション モードを開始して、IP 情報が割り当てられている VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
ステップ 3	**ip address***ip-address subnet-mask* 例： `スイッチ(config-vlan)# ip address 10.10.10.2 255.255.255.0`	IP アドレスとサブネット マスクを入力します。
ステップ 4	**exit** 例： `スイッチ(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip default-gateway***ip-address* 例： `スイッチ(config)# ip default-gateway 10.10.10.1`	スイッチに直接接続しているネクストホップのルータインターフェイスのIPアドレスを入力します。このスイッチにはデフォルトゲートウェイが設定されています。デフォルトゲートウェイは、スイッチスイッチから宛先 IP アドレスを取得していない IP パケットを受信します。

	コマンドまたはアクション	目的
		デフォルト ゲートウェイが設定されると、スイッチは、ホストが接続する必要のあるリモート ネットワークに接続できます。 （注） IP でルーティングするようにスイッチを設定した場合、デフォルト ゲートウェイの設定は不要です。 （注） デフォルトゲートウェイの構成に基づいて、スイッチの CAPWAP は中継を行い、ルーティングされたアクセスポイントとスイッチの接続をサポートします。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces vlan***vlan-id* 例： スイッチ# **show interfaces vlan 99**	設定された IP アドレスを確認します。
ステップ 8	**show ip redirects** 例： スイッチ# **show ip redirects**	設定されたデフォルト ゲートウェイを確認します。

スイッチのスタートアップ コンフィギュレーションの変更

システム コンフィギュレーションを読み書きするためのファイル名の指定

Cisco IOS ソフトウェアは、デフォルトで config.text ファイルを使用して、システム コンフィギュレーションの不揮発性コピーを読み書きします。別のファイル名を指定することもできます。次回の起動時には、その名前のファイルが読み込まれます。

はじめる前に

このタスクではスタンドアロンの スイッチ を使用します。

手順の概要

1. **configure terminal**
2. **boot flash**:*/file-url*
3. **end**
4. **show boot**
5. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot flash**:*/file-url* 例： `スイッチ(config)# boot flash:config.text`	次回の起動時に読み込むコンフィギュレーション ファイルを指定します。 *file-url*：パス（ディレクトリ）およびコンフィギュレーション ファイル名。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show boot** 例： `スイッチ# show boot`	入力を確認します。 **boot** グローバル コンフィギュレーション コマンドによって、CONFIG_FILE 環境変数の設定が変更されます。
ステップ 5	**copyrunning-configstartup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチの手動による起動

スイッチはデフォルトで自動的に起動しますが、手動で起動するように設定することもできます。

はじめる前に

このタスクのスタンドアロン スイッチを使用します。

手順の概要

1. **configure terminal**
2. **boot manual**
3. **end**
4. **show boot**
5. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot manual** 例： `スイッチ(config)# boot manual`	次回の起動時に、スイッチを手動で起動できるようにします。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show boot** 例： `スイッチ# show boot`	入力を確認します。 **boot manual** グローバル コンフィギュレーション コマンドによって、MANUAL_BOOT 環境変数の設定が変更されます。 次回、システムを再起動したときには、スイッチはブートローダ モードになり、ブートローダ モードであることが *switch:* プロンプトによって示されます。システムを起動するには、**boot***filesystem:/file-url* ブート ローダ コマンドを使用します。

	コマンドまたはアクション	目的
		• *filesystem*：システム ボードのフラッシュ デバイスに flash: を使用します。 スイッチ: **boot flash:** • *file-url*：パス（ディレクトリ）および起動可能なイメージの名前を指定します。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ステップ 5	**copyrunning-configstartup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インストール モードでスイッチ の起動

手順の概要

1. **cp***source_file_pathdestination_file_path*
2. **software expand file***source_file_path*
3. **reload**
4. **boot flash: packages.conf**
5. **show version**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**cp***source_file_pathdestination_file_path* 例： スイッチ# **copy tftp://10.0.0.6/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash:**	（任意）FTP または TFTP サーバから、bin ファイル（image.bin）をフラッシュまたはUSB フラッシュにコピーします。
ステップ 2	**software expand file***source_file_path* 例：	フラッシュ、FTP、TFTP、HTTP、または HTTPS サーバに保存さ

	コマンドまたはアクション	目的

	TFTP からの bin ファイルの解凍：
	`Switch# software expand file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to flash:`
	`Preparing expand operation ...`
	`[1]: Downloading file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to active switch 1`
	`[1]: Finished downloading file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to active switch 1`
	`[1]: Copying software from active switch 1 to switch 2`
	`[1]: Finished copying software to switch 2`
	`[1 2]: Expanding bundle cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin`
	`[1 2]: Copying package files`
	`[1 2]: Package files copied`
	`[1 2]: Finished expanding bundle cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin`
	
	`18 -rw- 74387812 Dec 7 2012 05:55:43 +00:00 cat3k_caa-base.SSA.03.09.37.EXP.pkg`
	`19 -rw- 2738868 Dec 7 2012 05:55:44 +00:00 cat3k_caa-drivers.SSA.03.09.37.EXP.pkg`
	`20 -rw- 32465772 Dec 7 2012 05:55:44 +00:00 cat3k_caa-infra.SSA.03.09.37.EXP.pkg`
	`21 -rw- 30389036 Dec 7 2012 05:55:44 +00:00 cat3k_caa-iosd-universalk9.SSA.150-9.37.EXP.pkg`
	`22 -rw- 18342624 Dec 7 2012 05:55:44 +00:00 cat3k_caa-platform.SSA.03.09.37.EXP.pkg`
	`23 -rw- 63374028 Dec 7 2012 05:55:44 +00:00 cat3k_caa-wcm.SSA.10.0.10.14.pkg`
	
	`17 -rw- 1239 Dec 7 2012 05:56:29 +00:00 packages.conf`
		れたbinファイルを、起動したスイッチに解凍します。
		（注） packages.conf ファイルが拡張されたファイル内に含まれていることを確認します。

ステップ 3	**reload** 例： `スイッチ: reload`	スイッチをリロードします。 （注） packages.conf スイッチ ファイルを使用して手動または自動で起動できます。手動で起動した場合、ステップ 4 に進むことができます。それ以外の場合、スイッチは自動的に起動します。
ステップ 4	**boot flash: packages.conf** 例： `switch: boot flash:packages.conf`	packages.conf ファイルでスイッチをブートします。

	コマンドまたはアクション	目的

ステップ 5	**show version**
	
	例：
	`switch# show version`
	
	`Switch Ports Model SW Version SW Image Mode`
	`------ ----- ----- ---------- ---------- ----`
	`1 6 WS-C3850-6DS-S 03.09.26.EXP ct3850-ipservicesk9 INSTALL`
		スイッチが**インストール** モードであることを確認します。

バンドル モードでスイッチの起動

スイッチを起動するにはいくつかの方法があります。ビン ファイルを TFTP サーバからコピーしてからスイッチを起動する、あるいは **boot flash:<image.bin>** または **boot usbflash0:<image.bin>** コマンドを使用して、直接フラッシュあるいは USB フラッシュからスイッチを起動します。

以下の手順は、バンドルモードで TFTP サーバからスイッチを起動する方法を示します。

手順の概要

1. **cp***source_file_pathdestination_file_path*
2. **switch:BOOT=<source path of .bin file>**
3. **boot**
4. **show version**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**cp***source_file_pathdestination_file_path* 例： スイッチ# **copy tftp://10.0.0.6/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash:**	（任意）FTP または TFTP サーバから、bin ファイル（image.bin）をフラッシュまたは USB フラッシュにコピーします。
ステップ 2	**switch:BOOT=<source path of .bin file>** 例： スイッチ: **switch:BOOT=tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin**	ブート パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 3	**boot** 例： `switch: boot`	スイッチをブートします。

ステップ 4	**show version**
	
	例：
	`switch# show version`
	`Switch Ports Model SW Version SW Image Mode`
	`------ ----- ----- ---------- ---------- ----`
	`1 6 WS-C3850-6DS-S 03.09.40.EXP ct3850-ipservicesk9 BUNDLE`
		スイッチが**バンドル** モードであることを確認します。

スイッチ スタックで特定のソフトウェア イメージを起動する場合

スイッチはデフォルトで、BOOT 環境変数の情報を使用して、システムを自動的に起動しようとします。この変数が設定されていない場合、スイッチは、フラッシュ ファイルシステム全体に再帰的に縦型検索し、最初の実行可能イメージをロードして実行しようとします。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。起動する具体的なイメージを指定することもできます。

手順の概要

1. **configure terminal**
2. **boot system switch** {*number* | **all**}
3. **end**
4. **show boot system**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot system switch** {*number*	**all**} 例： `Switch(config)# boot system switch 2`	（任意）スタックのスイッチについては、次回起動時にシステムイメージをロードするスイッチ メンバを指定します。

	コマンドまたはアクション	目的
	flash:cat3850-universalk9.SSA.03.08.83.EMD.150-8.83.EMD.bin	• スタック メンバを指定するには、*number* を使用します（1 つのスタック メンバのみを指定）。 • すべてのスタック メンバを指定するには、**all** を使用します。 Catalyst 3750-X スタック マスターまたはスタック メンバーを開始する場合、他の Catalyst 3750-X スタック メンバーにスイッチ イメージを指定できます。 Catalyst 3750-E スタック マスターまたはスタック メンバーを開始する場合、他の Catalyst 3750-E スタック メンバーにスイッチ イメージを指定できます。 Catalyst 3750 スイッチを指定する場合、Catalyst 3750 スタック メンバーでこのコマンドを入力します。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show boot system** 例： `スイッチ# show boot system`	入力を確認します。 **boot system** グローバル コマンドは、BOOT 環境変数の設定を変更します。 次回の起動時に、スイッチは BOOT 環境変数の情報を使用して、システムを自動的に起動しようとします。
ステップ 5	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ソフトウェア イメージのリロードのスケジュール設定

このタスクでは、ソフトウェア イメージを後でリロードするようにスイッチを設定する方法について説明します。

手順の概要

1. **configure terminal**
2. **copy running-config startup-config**
3. **reload in** [*hh*:]*mm* [*text*]
4. **reload at** *hh*: *mm* [*month day* | *day month*] [*text*]
5. **reload cancel**
6. **show reload**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**copy running-config startup-config** 例： `copy running-config startup-config`	**reload** コマンドを使用する前に、スイッチの設定情報をスタートアップ コンフィギュレーションに保存します。

ステップ 3	**reload in** [*hh*:]*mm* [*text*]
	
	例：
	
	`スイッチ(config)# reload in 12`
	
	`System configuration has been modified. Save? [yes/no]: y`
		指定した分数、または時間および分数が経過したときに、ソフトウェアがリロードされるようにスケジュールを設定します。リロードは、約 24 日以内に実行する必要があります。最大 255 文字で、リロードの理由を指定できます。

ステップ 4	**reload at** *hh*: *mm* [*month day* | *day month*] [*text*] 例： `スイッチ(config)# reload at 14:00`	リロードを実行する時間を、時間数と分数で指定します。 （注） スイッチのシステム クロックが（ネットワーク タイム プロトコル（NTP）、ハードウェア カレンダー、または手動で）設定されている場合にのみ、**at** キーワードを使用します。時刻は、スイッチに設定されたタイムゾーンに基づきます。リロードが複数のスイッチで同時に行われるようにスケジューリングするには、各スイッチの時間が NTP と同期している必要があります。

	コマンドまたはアクション	目的
ステップ5	**reload cancel** 例： スイッチ(config)# **reload cancel**	以前にスケジューリングされたリロードをキャンセルします。
ステップ6	**show reload** 例： **show reload**	以前スイッチにスケジューリングされたリロードに関する情報、またはリロードがスケジューリングされているかを表示します。

スイッチのセットアップ設定のモニタリング

例：スイッチ実行コンフィギュレーションの確認

```
スイッチ# show running-config
Building configuration...

Current configuration: 1363 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Stack1
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxE0
!
.
<output truncated>
.
interface gigabitethernet6/0/2
mvr type source

<output truncated>

...!
interface VLAN1
 ip address 172.20.137.50 255.255.255.0
 no ip directed-broadcast
!
ip default-gateway 172.20.137.1 !
!
snmp-server community private RW
snmp-server community public RO
snmp-server community private@es0 RW
snmp-server community public@es0 RO
snmp-server chassis-id 0x12
!
end
```

例：インストール モードでのソフトウェアブートアップ ディスプレイ

この例では、インストール モードでのソフトウェア ブートアップの表示を示します。

```
switch: boot flash:packages.conf

Getting rest of image
Reading full image into memory....done
Reading full base package into memory...: done = 74596432
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042f354
Kernel Size : 0x318412/3245074
Initramfs Address : 0x60747768
Initramfs Size : 0xdc08e8/14420200
Compression Format: .mzip

Bootable image at @ ram:0x6042f354
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@
```

```
---------------------------------------
Kernel Address : 0x6042ff38
Kernel Size : 0x318412/3245074
Initramfs Address : 0x6074834c
Initramfs Size : 0xdc08e8/14420200
Compression Format: .mzip

Bootable image at @ ram:0x6042ff38
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@
```

```
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin)...
Reading full image into memory.....................done
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@
```

スイッチ のセットアップを実行する場合の設定例

例：DHCP サーバとしてのスイッチの設定

```
スイッチ# configure terminal
スイッチ(config)# ip dhcp pool pool1
スイッチ(dhcp-config)# network 10.10.10.0 255.255.255.0
スイッチ(dhcp-config)# boot config-boot.text
スイッチ(dhcp-config)# default-router 10.10.10.1
スイッチ(dhcp-config)# option 150 10.10.10.1
スイッチ(dhcp-config)# exit
スイッチ(config)# tftp-server flash:config-boot.text
スイッチ(config)# interface gigabitethernet1/0/4
スイッチ(config-if)# no switchport
スイッチ(config-if)# ip address 10.10.10.1 255.255.255.0
スイッチ(config-if)# end
```

関連トピック

DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定, （2011 ページ）

例：DHCP 自動イメージ アップデートの設定

関連トピック

DHCP 自動イメージ アップデート（コンフィギュレーション ファイルおよびイメージ）の設定, （2014 ページ）

例：DHCP サーバから設定をダウンロードするためのスイッチの設定

次に、VLAN 99 上のレイヤ 3 SVI インターフェイスを使用し、保存されているコンフィギュレーションで DHCP ベースの自動設定をイネーブルにする例を示します。

```
スイッチ# configure terminal
スイッチ(config)# boot host dhcp
スイッチ(config)# boot host retry timeout 300
スイッチ(config)# banner config-save ^C Caution - Saving Configuration File to NVRAM May
Cause You to No longer Automatically Download Configuration Files at Reboot^C
スイッチ(config)# vlan 99
スイッチ(config-vlan)# interface vlan 99
スイッチ(config-if)# no shutdown
スイッチ(config-if)# end
スイッチ# show boot
BOOT path-list:
Config file:          flash:/config.text
Private Config file:  flash:/private-config.text
Enable Break:         no
Manual Boot:          no
HELPER path-list:
```

```
NVRAM/Config file
      buffer size:    32768
Timeout for Config
          Download:    300 seconds
Config Download
       via DHCP:       enabled (next boot: enabled)
スイッチ#
```

関連トピック

DHCP サーバからファイルをダウンロードするクライアントの設定, （2018 ページ）

例：ソフトウェア イメージのリロードのスケジューリング

次に、当日の午後 7 時 30 分に、ソフトウェアをスイッチにリロードする例を示します。

```
スイッチ# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 2013 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

次に、未来の日時を指定して、ソフトウェアをスイッチにリロードする例を示します。

```
スイッチ# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 2013 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```

スイッチのセットアップの実行に関する追加情報

関連資料

関連項目	マニュアル タイトル
スイッチ セットアップ コマンド ブート ローダ コマンド	*System Management Command Reference (Catalyst 3650 Switches)*
プレダウンロード機能	*System Management Configuration Guide*（*Cisco WLC 5700 Series*）
IOS XE DHCP 設定	*IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S*（*Catalyst 3650 Switches*）
ハードウェアの設置	*Catalyst 3650 Switch Hardware Installation Guide*
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S*（*Catalyst 3650 Switches*）

関連項目	マニュアル タイトル
プラットフォームに依存しない設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S*（*Catalyst 3650 Switches*） *IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S*（*Catalyst 3650 Switches*）

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

WCM サブパッケージのインストール

このドキュメントでは、Cisco Catalyst 3850 および 3650 シリーズ スイッチでのワイヤレス コントロール モジュール（WCM）サブパッケージをインストールする手順について説明します。

WCM モジュールおよび AP イメージから成る WCM サブパッケージは、機能をアップグレードし、新しい AP をサポートし、既知の問題を解決します。これはイメージの WCM の部分だけをアップグレードするので、イメージ全体のアップグレードは不要で、それによるネットワーク ダウンタイムはありません。たとえば、WCM が、イメージのバージョンの不一致により、新しい AP をネットワークに接続させることができなかった場合は、イメージの WCM の部分だけをアップグレードして、新しい AP のサポートを追加します。WCM がアップグレードされると、ネットワーク内のすべての AP は、新しいイメージに自動的にアップグレードされます。

利点

- WCM のバグを修正
- 新しい AP をサポート
- WCM で使用可能な機能を更新

前提条件

- コントローラは、インストール モードで起動する必要があります。

- WCM サブパッケージは、インストーラがサポートする送信元で使用可能である必要があります。たとえば、フラッシュ、TFTP、USB などです。

制約事項

- WCM サブパッケージは、イメージ 16.1 の以前のマイナー バージョンにのみインストールできます（たとえば、16.01.YY の WCM パッケージ（cat3k_caa-wcm.16.01.YY.SS A.pkg）をインストールできるのは、16.01.01 ～ 16.01.YY のスーパー パッケージ（cat3k_caa-universalk9.16.01.[01-to-YY].SSA.bin）です）。
- アップグレードしたら、スイッチを再起動する必要があります。

WCM サブパッケージのインストール

ステップ 1 コントローラの WCM パッケージをアップグレードします。
request platform software package install switch all file flash: wcm_sub_package.pkg auto-copy

ステップ 2 （任意）APイメージをダウンロードしてインストールします。この手順では、APを新しいイメージで事前にダウンロードおよびプログラミングすることで、ネットワークのダウンタイムを減少させます。そうしないと、コントローラがリロードしたとき、コントローラと AP 間のバージョンに不一致が発生し、その AP は新しい AP イメージを使用して自身のアップグレードを開始するため、ネットワークのダウンタイムがさらに長くなる可能性があります。

（注） ダウンロードおよびインストール後に、CLI が AP に達したことを確認するために 30 秒間待機します。

a) 接続されているすべての AP に新しいイメージをプッシュします。
ap image predownload
b) ダウンロードの経過表示をモニタします。
show ap image
c) すべての AP のブート変数を新しいイメージを指すように指定します。
ap image swap
d) AP をリセットします。
ap image reset

ステップ 3 コントローラをリロードします。リロード後、新しいWCMパッケージのコントローラがリロードし、新しい AP イメージの AP がリロードすると、アップグレードしたコントローラに接続を開始します。
reload

スイッチセットアップ設定の機能履歴と情報

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 84 章

Right-To-Use ライセンスの設定

- 機能情報の確認，2041 ページ
- RTU ライセンスの設定に関する制約事項，2041 ページ
- RTU ライセンスの設定に関する情報，2042 ページ
- RTU ライセンスの設定方法，2046 ページ
- RTU ライセンスのモニタリングおよびメンテナンス，2051 ページ
- RTU ライセンスの設定例，2052 ページ
- RTU ライセンスに関する追加情報，2057 ページ
- RTU ライセンスの機能履歴と情報，2058 ページ

機能情報の確認

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

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

RTU ライセンスの設定に関する制約事項

次に、RTU ライセンスの設定および使用に関する制約事項を示します。

- AP-Count ライセンスは注文が可能で、スイッチ上で事前にアクティブ化できます。

- イメージ ベースのライセンスは、アップグレードできます。AP-Count ライセンスは非アクティブ化したり、スイッチとコントローラとの間で移動したりできます。
- 永久ライセンスをアクティブ化するには、新しいイメージ レベルを設定した後にスイッチを再起動する必要があります。AP-Count ライセンスをアクティブ化するために再起動する必要はありません。
- 期限切れのイメージ ベースの評価ライセンスは、再起動後は再アクティブ化できません。
- スイッチ スタックのスタック メンバは同一のライセンス レベルを実行する必要があります。
- 混合スイッチ スタックのライセンスはサポートされていません。
- スイッチは、注文したイメージとともに事前にインストールされています。イメージを事前に注文していなかった場合、スイッチはデフォルトで LAN ベース イメージで起動します。
- 追加 AP-Count ライセンスは、工場出荷時にインストールされます。

関連トピック

イメージ ベース ライセンスのアクティブ化, （2046 ページ）

例：RTU イメージ ベースのライセンスのアクティブ化, （2052 ページ）

RTU ライセンスの設定に関する情報

Right-To-Use ライセンス

Right-To-Use（RTU）ライセンスでは、特定のライセンス タイプおよびレベルを注文してアクティブ化し、ライセンスの使用状況をスイッチで管理することができます。注文できるライセンスは次のとおりです。

- 永久ライセンス：特定の機能を備え、有効期限のないライセンスを購入できます。
- 評価ライセンス：スイッチに事前にインストールされています。使用有効期間は90日です。

永久ライセンスまたは評価ライセンスをアクティブ化するには、エンドユーザ ライセンス契約（EULA）を承認する必要があります。評価ライセンスの場合は、90 日の期限が切れる前に永久ライセンスを購入するか、ライセンスを非アクティブ化するように通知されます。

永久ライセンスは 1 つのデバイスから別のデバイスに移動できます。ライセンスをアクティブ化するには、スイッチを再起動する必要があります。

評価ライセンスはスイッチのマニュファクチャリング イメージであり、別のスイッチに移動できません。このタイプのライセンスは、再起動後は再アクティブ化できません。

関連トピック

イメージ ベース ライセンスのアクティブ化, （2046 ページ）

例：RTU イメージ ベースのライセンスのアクティブ化, （2052 ページ）

Right-To-Use イメージ ベースのライセンス

Right-To-Use イメージ ライセンスは、特定のイメージ ベースに基づき、次の一連の機能をサポートします。

- LAN Base：レイヤ 2 の機能。
- IP Base：レイヤ 2 およびレイヤ 3 の機能。
- IP Services：レイヤ 2、レイヤ 3、IPv6 の機能（スイッチにのみ適用され、コントローラには適用されません）。

デフォルトのイメージ ベースのライセンスは LAN Base です。

Right-To-Use ライセンスの状態

特定のライセンス タイプとレベルを設定した後は、ライセンスの状態をモニタすることでライセンスを管理できます。

表 *144*： *RTU* ライセンスの状態

ライセンスの状態	説明
Active, In Use	EULA が承認され、デバイス再起動後にライセンスが使用されています。
Active, Not In Use	EULA が承認され、ライセンスが有効になった時点で、スイッチを使用する準備が整っています。
非アクティブ化	EULA が承認されませんでした。

イメージ ベースのライセンスの状態をモニタする場合のガイドラインは次のとおりです。

- 購入した永久ライセンスは、スイッチの再起動後のみに *Active, In Use* 状態に設定されます。
- 複数のライセンスを購入した場合は、再起動すると最も高い機能セットのライセンスがアクティブ化されます。たとえば、IP Services ライセンスがアクティブ化され、LAN Base ライセンスはアクティブ化されません。
- スイッチの再起動後も、購入済みの残りのライセンスは **Active, Not In Use** 状態のままです。

（注） AP-Count ライセンスの場合に状態を「Active, In Use」に変更するには、まず、評価 AP-Count ライセンスが非アクティブ化されているようにする必要があります。

スイッチ スタックのライセンスのアクティブ化

Right-To-Use ライセンスはスイッチ スタックでサポートされます。スイッチは、StackWise 160ポートを介して接続された最大9個のスタッキング対応スイッチのセットです。接続できるのはスタック内の 1 つのタイプのスイッチのみです。スタック内の 1 個のスイッチはアクティブなスイッチとして識別され、残りのスイッチはスタンバイ スイッチになります。アクティブなスイッチは、RTU ライセンスを使用し、アクティブなコンソールからアクティブ化されたスイッチです。スタック内のスタンバイ スイッチのライセンス レベルは、同時にアクティブ化できます。

ライセンス レベルが一致している場合は、新しいスイッチはスイッチ スタックに参加できます。不一致がある場合は、アクティブ スイッチがライセンス レベルを再設定してスタックに参加するようにリブートします。

モビリティ コントローラ モード

AP-Count ライセンスは、スイッチがモビリティ コントローラ モードになっている場合にのみ使用します。MC は、AP-CountAP-Count ライセンスをトラッキングするゲートキーパであり、アクセス ポイント参加を許可または拒否できます。

AP-Count ライセンスはスイッチを、CLI で設定可能なモビリティ コントローラ モードで実行して管理します。

関連トピック

モビリティ モードの変更, （2050 ページ）

Right-To-Use AP-Count ライセンス

Right-To-Use（RTU）ライセンスにより、特定のライセンス タイプを注文およびアクティブ化してライセンスの使用状況をスイッチで管理することができます。

特定の数の追加アクセス ポイント数ライセンスとともにスイッチを注文できますが、注文するライセンスの総数は 25 を超えることはできません。スイッチを受け取った後でも追加アクセス ポイント数のライセンスを注文できます。

たとえば、25 の新しい追加ライセンスを注文した場合、それらの注文した追加ライセンスのみをスイッチに追加できます。ライセンスの追加単位は 1 です。ただし、スイッチに追加するライセンスの総数が 25 を超えないようにします。

アクセス ポイント数ライセンスを管理し、CLI で現在使用中のアクセス ポイント数を確認できるようにスイッチを設定できます。

以下では、2 種類のアクセス ポイント ライセンスについて説明します。

1 アクセス ポイントの永久ライセンス

- 追加アクセス ポイント数ライセンス：後でスイッチのキャパシティを増やすために追加ライセンスを購入できます。追加アクセス ポイント数ライセンスをあるスイッチから別のコントローラに換えることができます。

2 アクセス ポイントの評価ライセンス

- ライセンスを購入する前に、評価ライセンスをアクティブ化して、多くのアクセス ポイントを評価できます。
- 評価できるアクセス ポイントの最大数は 25 です。
- アクセス ポイント ライセンスを使用した評価期間は 90 日です。
- CLI から評価ライセンスのアクティブ化と非アクティブ化が行えます。

関連トピック

ap-count ライセンスのアクティブ化, （2047 ページ）
アップグレード ライセンスまたはキャパシティ Adder ライセンスの取得, （2048 ページ）
ライセンスの再ホスト, （2049 ページ）

Right-to-Use AP-Count 評価ライセンス

アクセス ポイント数の多いライセンスにアップグレードする場合は、永久バージョンのライセンスにアップグレードする前に評価ライセンスを試すことができます。たとえば、50アクセスポイント数の永久ライセンスを使用して、100 アクセス ポイント数の評価ライセンスを試す場合は 90 日間の評価ライセンスを試すことができます。たとえば、10アクセスポイント数の永久ライセンスを使用して、15 アクセス ポイント数の評価ライセンスを試す場合は 90 日間の評価ライセンスを試すことができます。

評価ライセンスがアクティブ化されると、AP-Count 永久ライセンスは無視されます。最大でサポート対象の1,000 のアクセス ポイントのライセンスを 90 日間利用できます最大でサポート対象の 25 のアクセス ポイントのライセンスを 90 日間利用できます。

操作の中断を避けるために、スイッチは、評価ライセンスの有効期限が切れてもライセンスを変更しません。期限切れ警告メッセージは有効期限日の 5 日前から毎日表示されます。90 日後に、評価ライセンスは期限切れになり、警告メッセージが表示されます。評価ライセンスをディセーブルにし、永久ライセンスを購入する必要があります。

評価ライセンスの期限が切れた後にスイッチを再起動すると、ライセンスのデフォルトが永久ライセンスに設定されます。

関連トピック

ap-count ライセンスのアクティブ化, （2047 ページ）
アップグレード ライセンスまたはキャパシティ Adder ライセンスの取得, （2048 ページ）
ライセンスの再ホスト, （2049 ページ）

Right-To-Use Adder AP-Count 再ホスト ライセンス

あるデバイスのライセンスを無効にして、別のデバイスにインストールする操作を再ホストと呼びます。デバイスの目的を変更するために、ライセンスのリホストが必要になる場合があります。

たとえば、Office Extend または屋内アクセス ポイントを別のスイッチに移動する場合、あるスイッチから別のコントローラに基本ライセンスを移行できます。

ライセンスを再ホストするには、あるデバイスの Adder AP-Count ライセンスを非アクティブ化し、別のデバイスで同じライセンスをアクティブ化します。

評価ライセンスを再ホストすることはできません。

RTU ライセンスの設定方法

イメージ ベース ライセンスのアクティブ化

手順の概要

1. **license right-to-use activate**{**ipbase** |**ipservices** | **lanbase**} {**all** | **evaluation all** } [**slot** *slot-number*] [**acceptEULA**]
2. **reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]
3. **show license right-to-use usage** [**slot** *slot-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use activate**{**ipbase**	**ipservices**	**lanbase**} {**all**	**evaluation all** } [**slot** *slot-number*] [**acceptEULA**] 例： スイッチ# **license right-to-use activate ipservices all acceptEULA**	イメージ ベース ライセンスのタイプをアクティブ化します。すべてのスイッチ上でアクティブ化され、EULA への同意が含まれることもあります。 （注） EULA に同意しない場合は、変更した設定はリロード後に反映されません。デフォルトのライセンス（または非アクティブ化されたライセンス）がリロード後にアクティブになります。
ステップ 2	**reload** [*LINE*	**at**	**cancel**	**in**	**slot** *stack-member-number*	**standby-cpu**] 例： スイッチ# **reload slot 1** Proceed with reload? [confirm] **y**	特定のスタック メンバをリロードし、RTU 追加 AP-Count ライセンスのアクティブ化プロセスを完了します。

	コマンドまたはアクション	目的
		（注） これまでに同意していなかった場合は、リロード後に同意を促すメッセージが表示されます。
ステップ 3	**show license right-to-use usage** [**slot** *slot-number*] 例： スイッチ# **show license right-to-use usage** Slot# License Name Type usage-duration(y:m:d) In-Use EULA --- 1 ipservices permanent 0 :10 :0 yes yes 1 ipbase permanent 0 :0 :0 no no 1 ipbase evaluation 0 :0 :0 no no 1 lanbase permanent 0 :0 :7 no yes 1 apcount evaluation 0 :0 :0 no no 1 apcount base 0 :0 :0 no no 1 apcount adder 0 :0 :0 no no Switch#	詳細な使用状況に関する情報を表示します。

関連トピック

RTU ライセンスの設定に関する制約事項，（2041 ページ）
Right-To-Use ライセンス，（2042 ページ）
RTU ライセンスのモニタリングおよびメンテナンス，（2051 ページ）
例：RTU イメージ ベースのライセンスのアクティブ化，（2052 ページ）

ap-count ライセンスのアクティブ化

手順の概要

1. **license right-to-use activate**{**apcount** *ap-number* **slot** *slot-num*} | **evaluation**} [**acceptEULA**]
2. **show license right-to-use usage** [**slot** *slot-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use activate**{**apcount** *ap-number* **slot** *slot-num*} | **evaluation**} [**acceptEULA**] 例： スイッチ# **license right to use activate apcount 5 slot 1 acceptEULA**	1 つ以上の追加 AP-Count ライセンスをアクティブ化し、ただちに EULA に同意します。
ステップ 2	**show license right-to-use usage** [**slot** *slot-number*] 例： スイッチ# **show license right-to-use usage** Slot# License Name Type usage-duration(y:m:d) In-Use EULA --- 1 ipservices permanent 0 :3 :29 yes yes 1 ipservices evaluation 0 :0 :0 no no 1 ipbase permanent 0 :0 :0 no no 1 ipbase evaluation 0 :0 :0 no no 1 lanbase permanent 0 :0 :0 no no 1 apcount evaluation 0 :3 :11 no no 1 apcount base 0 :0 :0 no yes 1 apcount adder 0 :0 :17 yes yes Switch#	詳細な使用状況に関する情報を表示します。

関連トピック

RTU ライセンスのモニタリングおよびメンテナンス，（2051 ページ）

Right-To-Use AP-Count ライセンス，（2044 ページ）

Right-to-Use AP-Count 評価ライセンス，（2045 ページ）

アップグレード ライセンスまたはキャパシティ Adder ライセンスの取得

キャパシティ Adder ライセンスを使用して、スイッチがサポートするアクセス ポイントの数を増やすことができます。

手順の概要

1. **license right-to-use** {**activate** | **deactivate**} **apcount** {*ap-number* | **evaluation** } **slot** *slot-num* [**acceptEULA**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use** {**activate** | **deactivate**} **apcount** {*ap-number* | **evaluation** } **slot** *slot-num* [**acceptEULA**] 例： スイッチ# **license right to use activate apcount 5 slot 2 acceptEULA**	Adder Ap-count ライセンスを 1 つ以上アクティブ化して、EULA を許可します。

関連トピック

Right-to-Use AP-Count 評価ライセンス, （2045 ページ）

Right-To-Use AP-Count ライセンス, （2044 ページ）

ライセンスの再ホスト

ライセンスを再ホストするには、1 つの スイッチ のライセンスを非アクティブ化し、別の スイッチ で同じライセンスをアクティブ化します。

手順の概要

1. **license right-to-use deactivate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**]
2. **license right-to-use activate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use deactivate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**] 例： スイッチ# **license right to use deactivate apcount 1 slot 1 acceptEULA**	1 つのスイッチのライセンスを非アクティブ化します。
ステップ 2	**license right-to-use activate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**] 例： スイッチ# **license right to use activate apcount 2 slot 2 acceptEULA**	別のスイッチのライセンスを非アクティブ化します。

関連トピック

Right-To-Use AP-Count ライセンス，（2044 ページ）
Right-to-Use AP-Count 評価ライセンス，（2045 ページ）

モビリティ モードの変更

手順の概要

1. **wireless mobility controller**
2. **write memory**
3. **reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]
4. **no wireless mobility controller**
5. **write memory**
6. **reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**wireless mobility controller**
	
	例：
	`スイッチ(config)# wireless mobility controller`
	`%`
	`Mobility role changed to Mobility Controller.`
	`Please save config and reboot the whole stack.`
		モビリティ エージェント モードのスイッチをモビリティ コントローラ モードに変更します。

ステップ 2	**write memory**
	
	例：
	`スイッチ# write memory`
	
	`Building configuration...`
	`Compressed configuration from 13870 bytes to 5390 bytes[OK]`
	
	`スイッチ#`	

ステップ 3	**reload** [*LINE*	**at**	**cancel**	**in**	**slot** *stack-member-number*	**standby-cpu**]
						
						例：
						`スイッチ# reload slot 3`
						`Proceed with reload? [confirm] y`	

	コマンドまたはアクション	目的
ステップ 4	**no wireless mobility controller** 例： スイッチ(config)# **no wireless mobility controller** % Mobility role changed to Mobility Agent. Please save config and reboot the whole stack. Switch(config)#	モビリティ コントローラ モードのスイッチをモビリティ エージェント モードに変更します。
ステップ 5	**write memory** 例： スイッチ# **write memory** Building configuration... Compressed configuration from 13870 bytes to 5390 bytes[OK] スイッチ#	
ステップ 6	**reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**] 例： スイッチ# **reload slot 3** Proceed with reload? [confirm] **y**	

関連トピック

モビリティ コントローラ モード, （2044 ページ）

RTU ライセンスのモニタリングおよびメンテナンス

コマンド	目的
show license right-to-use default	デフォルトのライセンス情報を表示します。
show license right-to-use detail	スイッチ スタック内のすべてのライセンスの詳細情報を表示します。
show license right-to-use eula {adder | evaluation | permanent}	エンドユーザ ライセンス契約を表示します。
show license right-to-use mismatch	一致しないライセンス情報を表示します。

コマンド	目的
show license right-to-use slot *slot-number*	スイッチスタック内の特定のスロットのライセンス情報を表示します。
show license right-to-use summary	スイッチスタック全体のライセンス情報の要約を表示します。
show license right-to-use usage [**slot** *slot-number*]	スイッチスタック内のすべてのライセンスの使用状況に関する詳細情報を表示します。
show switch	ライセンスのステータスを含むスイッチスタック内のすべてのメンバの詳細情報を表示します。

関連トピック

イメージ ベース ライセンスのアクティブ化, （2046 ページ）
例：RTU イメージ ベースのライセンスのアクティブ化, （2052 ページ）
ap-count ライセンスのアクティブ化, （2047 ページ）

RTU ライセンスの設定例

例：RTU イメージ ベースのライセンスのアクティブ化

次に、IP Services イメージ ライセンスをアクティブ化し、特定のスロットの EULA を受け入れる例を示します。

```
Switch# license right-to-use activate ipservices slot 1 acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

次に、評価用ライセンスをアクティブ化する例を示します。

```
Switch# license right-to-use activate ipservices evaluation acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

関連トピック

イメージ ベース ライセンスのアクティブ化, （2046 ページ）
RTU ライセンスの設定に関する制約事項, （2041 ページ）
Right-To-Use ライセンス, （2042 ページ）
RTU ライセンスのモニタリングおよびメンテナンス, （2051 ページ）

例：RTU ライセンス情報の表示

次に、スイッチ スタックのアクティブ スイッチからの統合RTU ライセンス情報の例を示します。スタック内のすべてのメンバのライセンス レベルは同じです。評価 AP-Count ライセンスをアクティブ化すると、追加 AP-Count ライセンスは無視されます。Ap-Count ライセンスの最大数は、評価がイネーブルの場合に使用できます。

```
Switch# show license right-to-use summary

 License Name    Type           Count   Period left
--------------------------------------------------------
  ipservices     permanent        10      Lifetime
  apcount        evaluation       15       90

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

License Level In Use: ipservices
License Level on Reboot: ipbase
Evaluation AP-Count: Enabled
Total AP Count Licenses: 25
AP Count Licenses In-use: 10
AP Count Licenses Remaining: 15
```

次に、永久ライセンスと追加ライセンスのサマリーを示します。評価 AP-Count ライセンスはディセーブルで、スイッチ スタック内でアクティブ化された追加 AP-Count ライセンスの総数が示されています。使用中の AP-Count ライセンスは、それらのライセンスが接続されていることを意味します。

```
Switch# show license right-to-use summary

  License Name    Type           Count      Period left
------------------------------------------------------------
  ipservices     permanent      N/A         Lifetime
  apcount        base           0
  apcount        adder          25          Lifetime

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

License Level In Use: ipservices
License Level on Reboot: ipservices eval
Evaluation AP-Count: Disabled
Total AP Count Licenses: 25
AP Count Licenses In-use: 10
AP Count Licenses Remaining: 15
```

次に、RTU のデフォルトのライセンスを示します。デフォルトのライセンスは事前にインストールされており、削除したり、移動したりできません。アクティブ化されているライセンスがない場合、スイッチは再起動後にデフォルトのライセンスを使用します。

```
Switch# show license right-to-use default

 Slot#    License Name    Type            Count
-----------------------------------------------------
 1        ipservices      permanent      N/A
 1        apcount         base           0
 1        apcount         adder          10

 Slot#    License Name    Type            Count
-----------------------------------------------------
 2        ipservices      permanent      N/A
 2        apcount         base           0
 2        apcount         adder          10
```

```
 Slot#    License Name    Type           Count
------------------------------------------------------
 3        ipservices      permanent     N/A
 3        apcount         base          0
 3        apcount         adder         10
```

次に、コントローラの統合 RTU ライセンス情報の例を示します。評価 AP-Count ライセンスがアクティブ化されると、基本および追加の AP-Count ライセンスは無視されます。AP-Count ライセンスの最大数は、評価がイネーブルの場合に使用できます。

```
controller# show license right-to-use summary
 License Name    Type     Count   Period left
------------------------------------------------
 apcount      evaluation  25    Expired

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

Evaluation AP-Count: Enabled
Total AP Count Licenses: 25
AP Count Licenses In-use: 2
AP Count Licenses Remaining: 23
```

次に、RTU のデフォルトのライセンスを示します。デフォルトのライセンスは事前にインストールされており、削除したり、移動したりできません。アクティブ化されているライセンスがない場合、コントローラは再起動後にデフォルトのライセンスを使用します。

```
controller# show license right-to-use  default
Slot#    License Name    Type           Count
------------------------------------------------------
  1        apcount         base          10
```

例：RTU ライセンスの詳細の表示

次に、スロット 1 の RTU ライセンスのすべての詳細情報の例を示します。

```
Switch# show license right-to-use detail slot 1

Index 1:  License Name: ipservices
           Period left: Lifetime
           License Type: permanent
           License State: Active, In use
           License Count: Non-Counted
           License Location: Slot 1
Index 2:  License Name: ipservices
           Period left: 90
           License Type: evaluation
           License State: Not Activated
           License Count: Non-Counted
           License Location: Slot 1
Index 3:  License Name: ipbase
           Period left: Lifetime
           License Type: permanent
           License State: Active, Not In use
           License Count: Non-Counted
           License Location: Slot 1
Index 4:  License Name: ipbase
           Period left: 90
           License Type: evaluation
           License State: Not Activated
           License Count: Non-Counted
           License Location: Slot 1
           License Location: Standby Switch 1
Index 5:  License Name: lanbase
           Period left: Lifetime
```

```
           License Type: permanent
           License State: Not Activated
           License Count: Non-Counted
           License Location: Slot 1
Index 6:  License Name: apcount
           Period left: 90
           License Type: evaluation
           License State: Active, In use
           License Count: 50
           License Location: Slot 1
Index 7:  License Name: apcount
           Period left: Lifetime
           License Type: base
           License State: Active, Not In use
           License Count: 0
           License Location: Slot 1
Index 8:  License Name: apcount
           Period left: Lifetime
           License Type: adder
           License State: Active, Not In use
           License Count: 10
           License Location: Slot 1


Controller# show license right-to-use detail slot 1
Index 6:  License Name: apcount
          Period left: Expired
          License Type: evaluation
          License State: Active, In use
          License Count: 1000
          License Location: Slot 1
Index 7:  License Name: apcount
          Period left: Lifetime
          License Type: base
          License State: Active, Not In use
          License Count: 0
          License Location: Slot 1
Index 8:  License Name: apcount
          Period left: Lifetime
          License Type: adder
          License State: Not Activated
          License Count: 0
          License Location: Slot 1
```

例：RTU ライセンスの不一致の表示

この例では、スタック内のスイッチのライセンス情報と、メンバ スイッチの不一致ステータスを示します。メンバ スイッチがアクティブ スイッチと一致している必要があります。

```
Switch# show switch

Switch/Stack Mac Address : 6400.f125.0c80
                                                     H/W   Current
Switch#   Role        Mac Address     Priority Version  State
-----------------------------------------------------------------------------
 1       Standby     6400.f125.1b00     1      0        Ready
*2       Active      6400.f125.0c80     1      V01      Ready
 3       Member      6400.f125.1780     1      0        Lic-Mismatch
```

（注） ライセンスの不一致を解決するには、まず、RTU ライセンスのサマリーを確認します。

```
Switch# show switch right-to-use summary
```

次に、アクティブ スイッチと同じライセンス レベルとなるように、一致していないスイッチのライセンス レベルを変更します。この例では、アクティブ スイッチと一致するように IP Base ライセンスをメンバ スイッチに対してアクティブ化したことを示します。

```
Switch# license right-to-use activate ipbase slot 1 acceptEULA
```

例：RTU ライセンス使用状況の表示

次に、スイッチ スタックの詳細なライセンス使用状況の例を示します。スロット 1 の IP Services ライセンスは永久ライセンスで、1 日使用しています。スロット 2 の AP-Count ライセンスは、評価に使用できる状態です。EULA に同意しており、使用中の状態であることが示されていますが、再起動後に評価ライセンスは非アクティブ化されます。

```
Switch# show license right-to-use usage

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-------------------------------------------------------------------------------

 1      ipservices     permanent      0 :0 :1            yes     yes
 1      ipservices     evaluation     0 :0 :0            no      no
 1      ipbase         permanent      0 :0 :0            no      yes
 1      ipbase         evaluation     0 :0 :0            no      no
 1      lanbase        permanent      0 :0 :0            no      no
 1      apcount        evaluation     0 :0 :0            yes     yes
 1      apcount        base           0 :0 :0            no      yes
 1      apcount        adder          0 :0 :0            no      yes

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-------------------------------------------------------------------------------

 2      ipservices     permanent       0 :0 :1           yes     no
 2      ipservices     evaluation      0 :0 :0           no      yes
 2      ipbase         permanent       0 :0 :0           no      yes
 2      ipbase         evaluation      0 :0 :0           no      no
 2      lanbase        permanent       0 :0 :0           no      no
 2      apcount        evaluation      0 :0 :0           yes     yes
 2      apcount        base            0 :0 :0           no      yes
 2      apcount        adder           0 :0 :0           no      no

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-------------------------------------------------------------------------------

 3      ipservices     permanent       0 :0 :1           yes     yes
 3      ipservices     evaluation      0 :0 :0           no      no
 3      ipbase         permanent       0 :0 :0           no      no
 3      ipbase         evaluation      0 :0 :0           no      no
 3      lanbase        permanent       0 :0 :0           no      no
 3      apcount        evaluation      0 :0 :0           yes     yes
 3      apcount        base            0 :0 :0           no      yes
 3      apcount        adder           0 :0 :0           no      no
```

次に、コントローラの詳細なライセンス使用状況の例を示します。

```
Controller# show license right-to-use usage
Slot#  License Name     Type      usage-duration(y:m:d)  In-Use  EULA
-------------------------------------------------------------------------
1      apcount        evaluation   0 :3 :3                yes    yes
1      apcount        base         0 :0 :0                no     yes
1      apcount        adder        0 :0 :0                no     no
```

RTU ライセンスに関する追加情報

関連資料

関連項目	マニュアル タイトル
RTU コマンド	*System Management Command Reference (Catalyst 3650 Switches)*
RTU AP イメージ プレロード機能	*System Management Configuration Guide*（*Cisco WLC 5700 Series*）

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

RTU ライセンスの機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 85 章

管理者のユーザ名とパスワードの設定

- 機能情報の確認，2059 ページ
- 管理者のユーザ名とパスワードの設定について，2059 ページ
- 管理者のユーザ名とパスワードの設定，2061 ページ
- 例：管理者のユーザ名とパスワードの設定，2063 ページ
- 管理者のユーザ名とパスワードに関する追加情報，2063 ページ
- 管理者のユーザ名とパスワードの設定の機能履歴と情報，2064 ページ

機能情報の確認

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

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

管理者のユーザ名とパスワードの設定について

管理者のユーザ名とパスワードを設定しておくと、権限のないユーザによるスイッチの設定変更や設定情報の表示を防ぐことができます。この項では、初期設定とパスワード リカバリの手順を説明します。

スイッチに関連付けられた一つ以上のアクセス ポイントを管理および設定する管理者のユーザ名とパスワードを設定することもできます。

強力なパスワード

管理者ユーザがアクセス ポイントを管理するため、ASCII キーによる暗号化パスワードなどの強力な管理者パスワードを設定できます。

強力なパスワードを作成する場合は、次のガイドラインに従ってください。

- 次のカテゴリ（小文字、大文字、数字、特殊文字）のうち、少なくとも 3 つが必要です。

（注） GUI のログインでは、ユーザ名とパスワードでの特殊文字の使用はサポートされません。

- 新しいパスワードは、関連付けられているユーザ名と同じにしたり、ユーザ名を反転させたりすることはできません。
- パスワードの文字を 4 回以上連続して繰り返すことはできません。
- パスワードに **cisco**、**ocsic**、**admin**、**nimda** を使用することはできません。また、これらの文字のいくつかを大文字にしたり、i を「1」、「|」、または「!」に、「o」を「0」に、または「s」を「$」に置き換たりすることもできません。
- ユーザ名およびパスワードで許容される最大文字数は 32 文字です。

暗号化パスワード

パスワードには 3 種類のキーを設定できます。

- ランダムに生成されたキー：このキーはランダムに生成され、最も安全なオプションです。1 台のシステムから別のシステムへコンフィギュレーション ファイルをエクスポートするには、キーもエクスポートする必要があります。
- 静的キー：最も単純なオプションは固定（静的）暗号キーを使用することです。固定キーを使用すれば、キー管理は必要ありませんが、キーが何らかの方法で検出されると、データはそのキーの知識を持つ任意のユーザによって復号化できます。これは、セキュアなオプションではなく、CLI では難読化と呼ばれます。
- ユーザによって定義されたキー：ユーザ自身がキーを定義できます。1 台のシステムから別のシステムへコンフィギュレーション ファイルをエクスポートするには、双方のシステムで同じキー設定する必要があります。

管理者のユーザ名とパスワードの設定

手順の概要

1. **configure terminal**
2. **wireless security strong-password**
3. **username***admin-username***password{0***unencrypted_password*| **7***hidden_password*|*unencrypted_text***}**
4. **username***admin-username***secret{0***unencrypted_secret_text*| **4***SHA256 encrypted_secret_text*| **5***MD5 encrypted_secret_text*| **LINE}**
5. **ap mgmtuser username***username***password{0***unencrypted password* | **8***AES encrypted password***}secret{0***unencrypted password* | **8***AES encrypted password***}**
6. **ap dot1x username***username***password{0***unencrypted password* | **8***AES encrypted password***}**
7. **end**
8. **ap nameapnamemgmtuser username***username***password***password***secret***secret _text*
9. **apnameapnamedot1x-user***username***password***password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless security strong-password** 例： スイッチ(config)# **wireless security strong-password**	管理者ユーザのための強力なパスワード ポリシーをイネーブルにします。
ステップ 3	**username***admin-username***password{0***unencrypted_password*| **7***hidden_password*|*unencrypted_text***}** 例： スイッチ(config)# **username adminuser1 password 0 QZsek239@**	管理者のユーザ名とパスワードを指定します。 管理者は、スイッチを設定し、設定情報を表示できます。
ステップ 4	**username***admin-username***secret{0***unencrypted_secret_text*| **4***SHA256 encrypted_secret_text*| **5***MD5 encrypted_secret_text*| **LINE}** 例： スイッチ(config)# **username adminuser1 secret 0 QZsek239@**	管理者のシークレットを指定します。

	コマンドまたはアクション	目的
ステップ 5	**ap mgmtuser username***username***password{0***unencrypted password* **| 8***AES encrypted password***}secret{0***unencrypted password* **| 8***AES encrypted password***}** 例： スイッチ(config)# **ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!**	スイッチへ設定されたすべてのアクセス ポイントを管理するため、システムの管理者のユーザ名とパスワードを指定します。 特権アクセスポイント管理のためのシークレット テキストを含めることもできます。 （注） パスワードが強力なパスワード ポリシーを満たしていない場合、パスワードは有効なエラー メッセージとともに拒否されます。たとえば、次のパスワードは、強力なパスワードでないため、拒否されます。 スイッチ# **ap mgmtuser username cisco password 0 abcd secret 0 1234**
ステップ 6	**ap dot1x username***username***password{0***unencrypted password* **| 8***AES encrypted password***}** 例： スイッチ(config)# **ap dot1x username cisco password 0 Qwci12@**	スイッチへ設定されたすべてのアクセス ポイントを管理するため、802.1X のユーザ名とパスワードを指定します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**ap nameapnamemgmtuser username***username***password***password***secret***secret _text* 例： スイッチ# **ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qne35! secret Nzep592$**	スイッチに設定された特定のアクセス ポイントを管理するための管理者のユーザ名、パスワード、およびシークレット テキストを設定します。
ステップ 9	**apnameapnamedot1x-user***username***password***password* 例： スイッチ# **ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qne35!**	特定のアクセス ポイントの 802.1X ユーザ名とパスワードを設定します。

例：管理者のユーザ名とパスワードの設定

次に、コンフィギュレーション モードで、管理者のユーザ名と、厳格なパスワード ポリシーに則ったパスワードを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wireless security strong-password
スイッチ(config)# username adminuser1 password 0 QZsek239@
スイッチ(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!
スイッチ(config)# ap dot1x username cisco password 0 Qwci12@
スイッチ# end
```

次に、グローバル EXEC モードで、管理者のユーザ名およびパスワードをアクセス ポイントに設定する例を示します。

```
スイッチ# wireless security strong-password
スイッチ# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qwci12@ secret Qwci14@
スイッチ# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qwci12@
スイッチ# end
```

管理者のユーザ名とパスワードに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*SSystem Management Command Reference Guide (Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

管理者のユーザ名とパスワードの設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 86 章

802.11 パラメータおよび帯域選択の設定

- 機能情報の確認，2065 ページ
- 帯域選択の制約事項、802.11 帯域とパラメータ，2065 ページ
- 帯域選択、802.11 帯およびパラメータに関する情報，2066 ページ
- 802.11 帯とそのパラメータを設定する方法，2068 ページ
- 帯域選択、802.11 帯およびパラメータの設定のモニタリング，2076 ページ
- 帯域選択、802.11 帯およびパラメータの設定例，2080 ページ
- 802.11 パラメータおよび帯域選択に関する追加情報，2082 ページ
- 802.11 パラメータおよび帯域選択設定の機能履歴と情報，2083 ページ

機能情報の確認

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

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

帯域選択の制約事項、802.11 帯域とパラメータ

- 帯域選択が有効になっている WLAN では、ローミングの遅延が発生するので、音声やビデオのような、遅延に敏感なアプリケーションはサポートされません。
- 帯域選択は、Cisco Aironet 1040、1140、1250、1260、 1550、 2600、 3500、 3600、 シリーズ アクセス ポイントでのみ使用できます。

- 帯域選択が動作するのは、コントローラに接続されたアクセス ポイントに対してのみです。コントローラに接続しない FlexConnect アクセス ポイントは、リブート後に帯域選択を実行しません。
- 帯域選択アルゴリズムによるデュアル バンド クライアントの誘導は、同じアクセス ポイントの 2.4 GHz 無線から 5 GHz 無線へに限られます。このアルゴリズムが機能するのは、アクセス ポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。
- コントローラ上で帯域選択とアグレッシブ ロード バランシングの両方を有効にすることができます。これらは独立して動作し、相互に影響を与えることはありません。
- コントローラ GUI またはコントローラ CLI を使用して、帯域選択とクライアント ロード バランシングをグローバルで有効または無効にすることはできません。ただし、特定の WLAN の帯域選択とクライアント ロード バランシングを有効または無効にできます。帯域選択とクライアント ロード バランシングは、デフォルトではグローバルで有効になっています。

帯域選択、802.11 帯およびパラメータに関する情報

帯域選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、混雑の少ない 5 GHz アクセス ポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセス ポイントからの同一チャネル干渉も発生します。802.11b/g では、重複しないチャネルが 3 つしかないからです。このような原因による干渉を防ぎ、ネットワーク全体のパフォーマンスを向上させるには、スイッチで帯域選択を設定します。

帯域選択は、デフォルトではグローバルで有効になっています。

帯域選択のしくみは、クライアントへのプローブ応答を規制するというものです。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。

（注） クライアント RSSI値（sh cont d0|RSSI と表示される）が受信されたクライアントパケットの平均で、midRSSI 機能はプローブ パケットの即時 RSSI 値です。その結果、クライアント RSSI 値は、設定された midRSSI 値（7 dB デルタ）より弱いと見なされます。クライアントからのプローブ 802.11b は、802.11a バンドに関連付けるためクライアントをプッシュするように抑制されます。

802.11 帯域

自国の法的な規制基準を遵守するために、コントローラの 802.11b/g/n（2.4GHz）帯域と 802.11a/n（5GHz）帯域を設定できます。デフォルトでは、802.11b/g/n と 802.11a/n の両方がイネーブルになっています。

コントローラが 802.11g トラフィックだけを許可するように設定されている場合、802.11b クライアントデバイスはアクセスポイントに正常に接続できますが、トラフィックを送信できません。802.11g トラフィック専用にコントローラを設定する場合、必須として 11g レートをマークする必要があります。

802.11n パラメータ

この項では、ネットワーク上の 802.11n デバイス（Cisco Aironet 1140 および 3600 シリーズ アクセス ポイントなど）を管理する手順を説明します。802.11n デバイスでは、2.4GHz 帯域と 5GHz 帯域をサポートしており、高スループット データ レートを提供します。

802.11n の高スループット データ レートは、すべての 802.11n アクセス ポイントで使用できます。この場合、WLAN で WMM が使用されていることと、レイヤ 2 暗号化なしであるか WPA2/AES 暗号化が有効化されていることが必要です。

（注） Cisco 802.11n AP は、偽の wIPS アラームをトリガーする可能性がある誤ったビーコン フレームを断続的に送信する場合があります。これらのアラームを無視することをお勧めします。この問題は Cisco 802.11n AP の 1140、1250、2600、3500、および 3600 で確認されています。

802.11h パラメータ

802.11h では、チャネルの変更がクライアント デバイスに通知されます。また、クライアント デバイスの送信電力を制限できるようになっています。

802.11 帯とそのパラメータを設定する方法

帯域選択の設定（CLI）

手順の概要

1. **configure terminal**
2. **wireless client band-select cycle-count** *cycle_count*
3. **wireless client band-select cycle-threshold** *milliseconds*
4. **wireless client band-select expire suppression** *seconds*
5. **wireless client band-select expire dual-band** *seconds*
6. **wireless client band-select client-rssi** *client_rssi*
7. **end**
8. **wlan** *wlan_profile_name wlan_ID SSID_network_name* **band-select**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless client band-select cycle-count** *cycle_count* 例： スイッチ(config)# **wireless client band-select cycle-count 3**	帯域選択のプローブ サイクル カウントを設定します。 *cycle_count* パラメータには、1 ～ 10 の範囲内の値を入力できます。
ステップ 3	**wireless client band-select cycle-threshold** *milliseconds* 例： スイッチ(config)# **wireless client band-select cycle-threshold 5000**	新規スキャン周期の時間のしきい値を設定します。 *milliseconds* パラメータには、しきい値として 1 ～ 1000 の範囲内の値を入力できます。
ステップ 4	**wireless client band-select expire suppression** *seconds* 例： スイッチ(config)# **wireless client band-select expire suppression 100**	抑制の期限切れを帯域幅選択に設定します。 *seconds* パラメータには、抑制期間として 10 ～ 200 の範囲内の値を入力できます。

	コマンドまたはアクション	目的
ステップ 5	**wireless client band-select expire dual-band** *seconds* 例： スイッチ(config)# **wireless client band-select expire dual-band 100**	デュアル バンドの期限を設定します。 *seconds* パラメータには、デュアル バンド用に 10 ～ 300 の範囲内の値を入力できます。
ステップ 6	**wireless client band-select client-rssi** *client_rssi* 例： スイッチ(config)# **wireless client band-select client-rssi 40**	クライアント RSSI しきい値を設定します。 *client_rssi* パラメータには、プローブに応答するクライアント RSSI の最小 dBm として 20 ～ 90 の範囲内の値を入力できます。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **band-select** 例： スイッチ(config)# **wlan wlan1 25 ssid12** スイッチ(config-wlan)# **band-select**	特定の WLAN で帯域選択を設定します。 *wlan_ID* パラメータには、1 ～ 512 の範囲内の値を入力できます。 *SSID_network_name* パラメータには、最大 32 文字の英数字を入力できます。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 帯域の設定（CLI）

802.11 帯およびパラメータを設定できます。

手順の概要

1. **configure terminal**
2. **ap dot11 5ghz shutdown**
3. **ap dot11 24ghz shutdown**
4. **ap dot11 {5ghz | 24ghz} beaconperiod** *time_unit*
5. **ap dot11 {5ghz | 24ghz} fragmentation** *threshold*
6. **ap dot11 {5ghz | 24ghz} dtpc**
7. **wireless client association limit** *number* **interval** *milliseconds*
8. **ap dot11 {5ghz | 24ghz} rate** *rate {disable | mandatory | supported}*
9. **no ap dot11 5ghz shutdown**
10. **no ap dot11 24ghz shutdown**
11. **ap dot11 24ghz dot11g**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 5ghz shutdown** 例： スイッチ(config)# **ap dot11 5ghz shutdown**	802.11a 帯域をディセーブルにします。 （注） 802.11a ネットワーク パラメータを設定する前に、802.11a 帯域をディセーブルにする必要があります。
ステップ 3	**ap dot11 24ghz shutdown** 例： スイッチ(config)# **ap dot11 24ghz shutdown**	802.11b 帯域をディセーブルにします。 （注） 802.11b ネットワーク パラメータを設定する前に、802.11b 帯域をディセーブルにする必要があります。
ステップ 4	**ap dot11 {5ghz | 24ghz} beaconperiod** *time_unit* 例： スイッチ(config)# **ap dot11 5ghz beaconperiod 500**	アクセス ポイントによる SSID のブロードキャスト レートを指定します。 ビーコン間隔は時間単位（TU）で測定されます。1 TU は 1024 マイクロ秒です。20 ～ 1000 ミリ秒ごとにビーコンを送信するように、アクセス ポイントを設定できます。
ステップ 5	**ap dot11 {5ghz | 24ghz} fragmentation** *threshold*	パケットを断片化するサイズを指定します。 しきい値は、256 ～ 2346 バイト（両端の値を含む）です。接続不良や多くの無線干渉が発生している領域では、この値を小さくします。

	コマンドまたはアクション	目的
	例： スイッチ(config)# **ap dot11 5ghz fragmentation 300**	
ステップ 6	**ap dot11 {5ghz | 24ghz} dtpc** 例： スイッチ(config)# **ap dot11 5ghz dtpc** スイッチ(config)# **no ap dot11 24ghz dtpc**	アクセスポイントによる、チャネルのアドバタイズ、ビーコンの電力レベル送信、応答プローブをイネーブルにします。 デフォルト値はイネーブルです。Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）を使用するクライアント デバイスは、アクセス ポイントからチャネルおよび電力レベル情報を受信して、自身の設定を自動的に調整します。たとえば、主に日本で使用されているクライアント デバイスをイタリアに移送し、そこのネットワークに追加した場合、チャネルと電力設定の自動調整を DTPC に任せることができます。 （注） Cisco IOS ソフトウェアを実行するアクセス ポイントでは、この機能はワールド モードと呼ばれます。 このコマンドの **no** 形式は、802.11a または 802.11b DTPC 設定をディセーブルにします。
ステップ 7	**wireless client association limit** *number* **interval** *milliseconds* 例： スイッチ(config)# **wireless client association limit 50 interval 1000**	設定できるクライアントの最大数を指定します。 単一アクセス ポイント スロットの、所定の間隔内におけるアソシエーション要求の最大数を設定できます。設定できるアソシエーション制限の範囲は 1 ～ 100 です。 アソシエーション要求制限間隔は 100 ～ 10000 ミリ秒です。
ステップ 8	**ap dot11 {5ghz | 24ghz} rate** *rate {disable | mandatory | supported}* 例： スイッチ(config)# **ap dot11 5ghz rate 36 mandatory**	データをコントローラとクライアント間で送信できる速度を指定します。 • *disabled*：クライアントが通信に使用するデータ レートを指定するように定義します。 • *mandatory*：クライアントがコントローラのアクセス ポイントにアソシエートするにはこのデータ レートをサポートする必要があると定義します。 • *supported*：アソシエートしたクライアントは、このデータ レートをサポートしていれば、このレートを使用してアクセス ポイントと通信することができます。ただし、クライアントがこのレートを使用できなくても、アソシエートは可能です。 • *rate*：データが送信されるレートを指定します。802.11a、802.11b 帯域では、データは 1、2、5.5、6、9、11、12、18、24、36、48、または 54 Mbps のレートで送信されます。

	コマンドまたはアクション	目的
ステップ 9	**no ap dot11 5ghz shutdown** 例： スイッチ(config)# **no ap dot11 5ghz shutdown**	802.11a 帯域をイネーブルにします。 （注） デフォルト値はイネーブルです。
ステップ 10	**no ap dot11 24ghz shutdown** 例： スイッチ(config)# **no ap dot11 24ghz shutdown**	802.11b 帯域をイネーブルにします。 （注） デフォルト値はイネーブルです。
ステップ 11	**ap dot11 24ghz dot11g** 例： スイッチ(config)# **ap dot11 24ghz dot11g**	802.11g ネットワークのサポートをイネーブルまたはディセーブルにします。 デフォルト値はイネーブルです。このコマンドは、802.11b 帯域が有効になっている場合のみ使用できます。この機能を無効にすると、802.11b 帯域は 802.11g をサポートせずに有効になります。
ステップ 12	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

802.11n のパラメータの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 {5ghz | 24ghz} dot11n**
3. **ap dot11 {5ghz | 24ghz} dot11n mcs tx** *rtu*
4. **wlan***wlan_profile_name wlan_ID SSID_network_name* **wmm require**
5. **ap dot11 {5ghz | 24ghz} shutdown**
6. **{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}**
7. **no ap dot11 {5ghz | 24ghz} shutdown**
8. **ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}**
9. **ap dot11 {5ghz | 24ghz} dot11n rifs rx**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 {5ghz | 24ghz} dot11n** 例： スイッチ(config)# **ap dot11 5ghz dot11n**	ネットワークで 802.11n サポートをイネーブルします。 このコマンドの **no** 形式は、ネットワーク上の 802.11n サポートをディセーブルにします。
ステップ 3	**ap dot11 {5ghz | 24ghz} dot11n mcs tx** *rtu* 例： スイッチ(config)# **ap dot11 5ghz dot11n mcs tx 20**	データをアクセス ポイントとクライアント間で送信できる変調および符号化方式（MCS）レートを指定します。**mcs tx** パラメータには、0 ～ 23 の値が設定できます。 このコマンドの **no** 形式は、設定された MCS レートをディセーブルに設定します。
ステップ 4	**wlan***wlan_profile_name wlan_ID SSID_network_name* **wmm require** 例： スイッチ(config)# **wlan wlan1 25 ssid12** スイッチ(config-wlan)# **wmm require**	WLAN で WMM をイネーブルにし、設定した 802.11n データ レートを使用します。 **require** パラメータは、クライアント デバイスに WMM の使用を要求します。WMM をサポートしていないデバイスは WLAN に接続できません。
ステップ 5	**ap dot11 {5ghz | 24ghz} shutdown** 例： スイッチ(config)# **ap dot11 5ghz shutdown**	ネットワークをディセーブルにします。
ステップ 6	**{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}** 例： スイッチ(config)# **ap dot11 5ghz dot11n a-mpdu tx priority all**	802.11n パケットに使用する集約方法を指定します。 集約は、パケット データ フレームを個別に伝送するのではなく、グループにまとめるプロセスです。集約方法には、Aggregated MAC Protocol Data Unit（A-MPDU）と Aggregated MAC Service Data Unit（A-MSDU）の 2 種類があります。A-MPDU と A-MSDU は、両方ともソフトウェアで実行されます。 集約方法は、アクセス ポイントからクライアントへのトラフィックのタイプごとに指定できます。 次の表は、トラフィック タイプごとに割り当てられる優先レベル（0 ～ 7）の説明です。

	コマンドまたはアクション	目的
		表 *145*：トラフィック タイプの優先レベル **ユーザ優先度** / **トラフィック タイプ** 0 / ベスト エフォート 1 / バックグラウンド 2 / 予備 3 / エクセレント エフォート 4 / 制御された負荷 5 / ビデオ、遅延およびジッタは100ミリ秒未満 6 / 音声、遅延およびジッタは 100 ミリ秒未満 7 / ネットワーク制御 各優先レベルを個別に設定するか、all パラメータを使用して一度にすべての優先レベルを設定できます。トラフィックが A-MPDU 送信または A-MSDU 伝送を使用するよう、プライオリティ レベルを設定できます。 • 他のオプションとともに **ap** コマンドを使用すると、そのプライオリティ レベルに関連付けられたトラフィックは、A-MPDU 送信に関連付けらます。 • 他のオプションとともに **no ap** コマンドを使用すると、そのプライオリティ レベルに関連付けられたトラフィックは、A-MSDU 送信に関連付けられます。 クライアントが使用する集約方法に合わせて優先度を設定します。デフォルトでは、A-MPDU は、優先レベル 0、4、および 5 に対して有効になっており、それ以外は無効になっています。デフォルトでは、A-MPDU は、6 と 7 以外のすべての優先度に対して有効になっています。

	コマンドまたはアクション	目的
ステップ 7	**no ap dot11 {5ghz | 24ghz} shutdown** 例： スイッチ(config)# **no ap dot11 5ghz shutdown**	ネットワークを再度イネーブルにします。
ステップ 8	**ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}** 例： スイッチ(config)# **ap dot11 5ghz dot11n guard-interval long**	ネットワークのガード間隔を設定します。
ステップ 9	**ap dot11 {5ghz | 24ghz} dot11n rifs rx** 例： スイッチ(config)# **ap dot11 5ghz dot11n rifs rx**	ネットワークの Reduced Interframe Space（RIFS）を設定します。
ステップ 10	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11h のパラメータの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 5ghz shutdown**
3. **{ap \| no ap} dot11 5ghz channelswitch mode** *switch_mode*
4. **ap dot11 5ghz power-constraint** *value*
5. **no ap dot11 5ghz shutdown**
6. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ap dot11 5ghz shutdown** 例： スイッチ(config)# **ap dot11 5ghz shutdown**	802.11a ネットワークをディセーブルにします。
ステップ 3	**{ap | no ap} dot11 5ghz channelswitch mode** *switch_mode* 例： スイッチ(config)# **ap dot11 5ghz channelswitch mode 0**	アクセス ポイントの、新しいチャネルに切り替わった際のアナウンス機能をイネーブルまたはディセーブルにします。 **channelswitch** パラメータには 0 または 1 を入力できます。チャネルが実際に切り替えられるまで送信を制限する場合は 0 を入力し、制限しない場合は 1 を入力します。デフォルト値は [disabled] です。
ステップ 4	**ap dot11 5ghz power-constraint** *value* 例： スイッチ(config)# **ap dot11 5ghz power-constraint 200**	802.11h 電力制限値を 0 から 255 の範囲で設定します。 value パラメータのデフォルト値は 3 dB です。
ステップ 5	**no ap dot11 5ghz shutdown** 例： スイッチ(config)# **no ap dot11 5ghz shutdown**	802.11a ネットワークを再度イネーブルします。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

帯域選択、802.11 帯およびパラメータの設定のモニタリング

帯域選択と 802.11 帯を使用した設定のモニタリング コマンド

このセクションでは、帯域選択および 802.11 帯の新しいコマンドについて説明します。

次のコマンドは、スイッチの帯域選択と 802.11 帯、およびパラメータのモニタリングに使用できます。

表 *146*：帯域選択と *802.11* 帯を使用した設定のモニタリング コマンド

コマンド	目的

show ap dot11 5ghz network	802.11a 帯域ネットワーク パラメータ、802.11a 運用率、802.11n MCS 設定および 802.11n ステータス情報を表示します。
show ap dot11 24ghz network	802.11b 帯域ネットワーク パラメータ、802.11b/g 運用率、802.11n MCS 設定および 802.11n ステータス情報を表示します。
show wireless dot11h	802.11h 設定パラメータを表示します。
show wireless band-select	帯域選択設定を表示します。

例：5 GHz 帯域の設定の確認

```
スイッチ# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
```

```
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

例：24 GHz 帯域の設定の確認

```
スイッチ# show ap dot11 24ghz network
802.11b Network : Enabled
11gSupport : Enabled
11nSupport : Enabled

  802.11b/g Operational Rates
  802.11b 1M : Mandatory
  802.11b 2M : Mandatory
  802.11b 5.5M : Mandatory
  802.11g 6M : Supported
  802.11g 9M : Supported
  802.11b 11M : Mandatory
  802.11g 12M : Supported
  802.11g 18M : Supported
  802.11g 24M : Supported
```

```
  802.11g 36M : Supported
  802.11g 48M : Supported
  802.11g 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
  Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable Mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 11
Default Tx Power Level : 1
DTPC Status : true
Call Admission Limit : 105
G711 CU Quantum : 15
ED Threshold : -50
Fragmentation Threshold : 2346
PBCC Mandatory : Disabled
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type : default-wmm
Call Admision Control (CAC) configuration
Voice AC
```

```
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

例：802.11h パラメータの状態の確認

```
スイッチ# show wireless dot11h
Power Constraint: 0
Channel Switch: 0
Channel Switch Mode: 0
```

例：帯域選択設定の確認

```
スイッチ# show wireless band-select
Band Select Probe Response    : per WLAN enabling
Cycle Count                   : 2
Cycle Threshold (millisec)    : 200
Age Out Suppression (sec)     : 20
Age Out Dual Band (sec)       : 60
Client RSSI (dBm)             : 80
```

帯域選択、802.11 帯およびパラメータの設定例

例：帯域選択の設定

次に、帯域選択の新規スキャン周期のプローブサイクルカウントおよび時間しきい値を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wireless client band-select cycle-count 3
スイッチ(config)# wireless client band-select cycle-threshold 5000
スイッチ(config)# end
```

次に、抑制の期限を帯域選択に設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wireless client band-select expire suppression 100
スイッチ(config)# end
```

次に、デュアル バンドの期限を帯域選択に設定する例を示します。

```
スイッチ# configure terminal
```

```
スイッチ(config)# wireless client band-select expire dual-band 100
スイッチ(config)# end
```

次に、クライアント RSSI しきい値を帯域選択に設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wireless client band-select client-rssi 40
スイッチ(config)# end
```

次に、特定の WLAN 上で帯域選択を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wlan wlan1 25 ssid12
スイッチ(config-wlan)# band-select
スイッチ(config)# end
```

例：802.11 帯設定

次に、ビーコン間隔、フラグメンテーション、および動的な送信電力コントロールを使用して 802.11 帯を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ap dot11 5ghz shutdown
スイッチ(config)# ap dot11 24ghz shutdown
スイッチ(config)# ap dot11 5ghz beaconperiod 500
スイッチ(config)# ap dot11 5ghz fragmentation 300
スイッチ(config)# ap dot11 5ghz dtpc
スイッチ(config)# wireless client association limit 50 interval 1000
スイッチ(config)# ap dot11 5ghz rate 36 mandatory
スイッチ(config)# no ap dot11 5ghz shutdown
スイッチ(config)# no ap dot11 24ghz shutdown
スイッチ(config)# ap dot11 24ghz dot11g
スイッチ(config)#end
```

例：802.11n 設定

次に、集約方法を使って 5 GHz 帯域の802.11n パラメータを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ap dot11 5ghz dot11n
スイッチ(config)# ap dot11 5ghz dot11n mcs tx 20
スイッチ(config)# wlan wlan1 25 ssid12
スイッチ(config-wlan)# wmm require\
スイッチ(config-wlan)# exit
スイッチ(config)# ap dot11 5ghz shutdown
スイッチ(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
スイッチ(config)# no ap dot11 5ghz shutdown
スイッチ(config)#exit
```

次に、5 GHz 帯域でガード インターバルを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ap dot11 5ghz dot11n
スイッチ(config)# ap dot11 5ghz dot11n mcs tx 20
スイッチ(config)# wlan wlan1 25 ssid12
```

```
スイッチ(config-wlan)# wmm require\
スイッチ(config-wlan)# exit
スイッチ(config)# no ap dot11 5ghz shutdown
スイッチ(config)# ap dot11 5ghz dot11n guard-interval long
スイッチ(config)#end
```

次に、5 GHz 帯域で RIFS を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ap dot11 5ghz dot11n
スイッチ(config)# ap dot11 5ghz dot11n mcs tx 20
スイッチ(config)# wlan wlan1 25 ssid12
スイッチ(config-wlan)# wmm require\
スイッチ(config-wlan)# exit
スイッチ(config)# ap dot11 5ghz shutdown
スイッチ(config)# ap dot11 5ghz dot11n rifs rx
スイッチ(config)#end
```

例：802.11h 設定

次に、制限伝送を使用して、アクセス ポイントをいつ新しいチャネルに切り替えるかをアナウンスするために、そのアクセスポイントを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ap dot11 5ghz shutdown
スイッチ(config)# ap dot11 5ghz channelswitch mode 0
スイッチ(config)# no ap dot11 5ghz shutdown
スイッチ(config)#end
```

次に、5 GHz 帯域で 802.11h 電力制限を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ap dot11 5ghz shutdown
スイッチ(config)# ap dot11 5ghz power-constraint 200
スイッチ(config)# no ap dot11 5ghz shutdown
スイッチ(config)#end
```

802.11 パラメータおよび帯域選択に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

802.11 パラメータおよび帯域選択設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 87 章

アグレッシブ ロード バランシングの設定

- 機能情報の確認，2085 ページ
- アグレッシブ ロード バランシングの制約事項，2085 ページ
- アグレッシブ ロード バランシング パラメータの設定情報，2086 ページ
- アグレッシブ ロード バランシングの設定方法，2088 ページ
- アグレッシブ ロード バランシングのモニタリング，2090 ページ
- アグレッシブ ロード バランシングに関する追加情報，2090 ページ
- アグレッシブ ロード バランシングの設定の機能履歴と情報，2091 ページ

機能情報の確認

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

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

アグレッシブ ロード バランシングの制約事項

- コマンドライン インターフェイスからのみアグレッシブ ロード バランシングを設定できます。
- アグレッシブ ロード バランシングは、手動で有効にしなければなりません。デフォルトでは無効になっています。
- 帯域選択設定と別にでも一緒にでもロード バランシングをイネーブルにできます。

- 帯域選択がデュアル バンド クライアントでイネーブルの場合、ロード バランシング パラメータは 5 GHz 無線から、無線の負荷が最小のもののみ選択します。2.4 GHz クライアントでは、5 GHz クライアントのプローブ情報がないため、ロードバランシング アルゴリズムは 2.4 GHz 無線でのみ選択できます。
- 同じスイッチのアクセス ポイント間でクライアントのロード バランシングを実行できますが、異なるスイッチのアクセス ポイント間のクライアントでは実行できません。
- ロードバランシングは無線クライアントの数に基づいて既存の関連付け拒否メカニズムを使用し、帯域選択はアクセス ポイントでのプローブ応答分散の抑制によってのみ実装されます。

アグレッシブ ロード バランシング パラメータの設定情報

アグレッシブ ロード バランシング

コントローラ上でアグレッシブ ロード バランシングを有効にすると、ワイヤレス クライアントの負荷を Lightweight アクセス ポイント間で分散することができます。アグレッシブ ロード バランシングはコントローラを使用して有効にできます。

ワイヤレス クライアントが Lightweight アクセス ポイントへのアソシエートを試みると、アソシエーション応答パケットとともに 802.11 応答パケットがクライアントに送信されます。この 802.11 応答パケットの中にステータス コード 17 があります。コード 17 は AP がビジー状態であることを示します。AP のしきい値が満たされていない場合、AP は「success」を示すアソシエーション応答で応答します。AP 使用率のしきい値に達した、またはしきい値を超過した場合は、コード 17（AP ビジー）で応答し、よりビジー状態の度合いが低い別の AP がクライアント要求を受け取ります。

たとえば、AP1 上のクライアント数が、AP2 のクライアント数とロードバランシング ウィンドウの和を上回っている場合は、AP1 の負荷は AP2 よりも高いと判断されます。クライアントが AP1 にアソシエートしようとすると、ステータス コード 17 が含まれている 802.11 応答パケットがクライアントに送信されます。アクセスポイントの負荷が高いことがこのステータス コードからわかるので、クライアントは別のアクセス ポイントへのアソシエーションを試みます。

コントローラは、クライアント アソシエーションを 10 回まで拒否するように設定できます（クライアントがアソシエーションを 11 回試みた場合、11 回目の試行時にアソシエーションが許可されます）。また、特定の WLAN 上でロード バランシングを有効にするか、無効にするかも指定できます。これは、特定のクライアント グループ（遅延に敏感な音声クライアントなど）に対してロード バランシングを無効にする場合に便利です。

（注） 音声クライアントは、遅延が 300 ミリ秒に設定されている場合には認証されません。これを回避するには、中央認証、ローカル スイッチング WLAN を CCKM に設定します。AP と WLC の間の Pagent ルータを 600 ミリ秒の遅延に設定してください（300 ms UP と 300 msDOWN そして音声クライアントの関連付けを行います）

アクセスポイントがサポートできるクライアントアソシエーションの最大数は、次の要因に依存しています。

- Lightweight アクセス ポイントと Autonomous Cisco IOS アクセス ポイントの場合、クライアント アソシエーションの最大数は異なります。
- 無線単位の制限と、AP 単位の全体的な制限が存在する場合があります。
- AP ハードウェア（16 MB の AP では、32 MB 以上の AP よりも制限が厳しくなります）

Lightweight アクセス ポイントのクライアント アソシエーションの制限は次のとおりです。

- 16 MB の AP の場合、AP ごとに 128 台のクライアントに制限されます。この制限は、1100 および 1200 シリーズ AP に適用されます。
- 32 MB 以上の AP の場合、AP 単位の制限は存在しません。

すべての Cisco IOS AP の最大クライアント アソシエーションの制限は、1 無線につき 200 アソシエーションです。

（注） 32 MB 以上の Lightweight Cisco IOS AP では、無線が 2 つの場合、最大で 200 + 200 = 400 アソシエーションがサポートされます。

Autonomous Cisco IOS アクセス ポイントあたりの最大クライアント アソシエーションの制限は、AP あたり約 80 ～ 127 クライアントです。この数は、次の要因に応じて変化します。

- AP モデル（16 MB か、32 MB 以上か）
- Cisco IOS ソフトウェア リリース
- ハードウェア構成（無線が 2 つの場合、1 つの場合よりも多くのメモリを使用します）
- 有効にしている機能（特に WDS 機能）

無線単位の制限は、およそ200アソシエーションです。アソシエーションは、多くの場合、AP単位の制限に先に達します。Cisco Unified Wireless Network とは異なり、Autonomous Cisco IOS では、SSID 単位/AP 単位のアソシエーション制限がサポートされています。この制限は、dot11 SSID の下で、max-associations CLI を使用して設定されます。最大数は 255 アソシエーションです（これはデフォルト値でもあります）。

（注） FlexConnect APの場合は、アソシエーションがローカルに処理されます。ロードバランシングの判断は、Cisco WLC で行われます。FlexConnect AP は、Cisco WLC の計算結果を確認する前に、まず、クライアントに応答を返します。FlexConnect AP がスタンドアロン モードの場合は、ロード バランシングが適用されません。

FlexConnect AP は、ローカル モードの AP と同様にロード バランシング用のステータス 17 で（再）アソシエーション応答を送信しません。代わりに、ステータス 0（成功）で（再）アソシエーションを送信してから、理由 5 で認証解除を送信します。

アグレッシブ ロード バランシングの設定方法

アグレッシブなロード バランシングの設定（CLI）

手順の概要

1. 次のコマンドを入力して、アグレッシブ ロード バランシング用のクライアント ウィンドウを設定します。
2. 次のコマンドを入力して、ロード バランシング用の拒否回数を設定します。
3. 次のコマンドを入力して、変更を保存します。
4. 次のコマンドを入力して、WLAN コンフィギュレーション モードを開始します。
5. 特定の WLAN 上でロード バランシングを有効にするには、次のコマンドを入力します。
6. 次のコマンドを入力して、設定を確認します。
7. 次のコマンドを入力して、変更を保存します。

手順の詳細

ステップ 1 次のコマンドを入力して、アグレッシブ ロードバランシング用のクライアント ウィンドウを設定します。
wireless load-balancing window*client_count*

client_count パラメータには、0 ～ 20 の範囲内の値を入力できます。

ステップ 2 次のコマンドを入力して、ロード バランシング用の拒否回数を設定します。
wireless load-balancing denial*denial_count*

denial_count パラメータには、1 ～ 10 の値を入力できます。

ステップ 3 次のコマンドを入力して、変更を保存します。
write memory

ステップ 4 次のコマンドを入力して、WLAN コンフィギュレーション モードを開始します。
wlan*profile-namewlan_IDSSID*

profile-name には、32 文字以内の英数字のプロファイル名を入力することができます。*wlan_ID* パラメータには、1 ～ 512 の値を入力できます。*SSID* パラメータには、32 文字以内の英数字のネットワーク名を入力できます。

ステップ 5 特定の WLAN 上でロード バランシングを有効にするには、次のコマンドを入力します。
load-balance

ロード バランシングを無効にするには、**no load-balance** コマンドを使用します。

ステップ 6 次のコマンドを入力して、設定を確認します。
show wireless load-balancing

```
Aggressive Load Balancing.........................: per WLAN enabling
```

```
Aggressive Load Balancing Window (clients).................:: 5
Aggressive Load Balancing Denial Count.....................:: 3

Statistics
Total Denied Count (clients)...............................:: 0
Total Denial Sent (messages)...............................:: 0
Exceeded Denial Max Limit Count (times)....................:: 0
None 5G Candidate Count (times)............................:: 0
None 2.4G Candidate Count (times)..........................:: 0
```

ステップ 7 次のコマンドを入力して、変更を保存します。
write memory

アグレッシブなロード バランシングの設定（GUI）

ステップ 1 [Load Balancing] ページを開くには、[Configure] > [Advanced] > [Load Balancing] の順に選択します。

ステップ 2 クライアントの [Aggressive Load Balancing] ウィンドウに、0 ～ 20 の値を入力します。
このウィンドウ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。

ロード バランシング ウィンドウ + 最も負荷が低いアクセス ポイント上のクライアント アソシエーション数 = ロード バランシングしきい値

特定のクライアント デバイスからアクセス可能なアクセス ポイントが複数ある場合に、アクセス ポイントはそれぞれ、アソシエートしているクライアントの数が異なります。クライアントの数が最も少ないアクセス ポイントは、負荷が最も低くなります。クライアント ウィンドウ サイズと、負荷が最も低いアクセス ポイント上のクライアント数の合計がしきい値となります。クライアント アソシエーションの数がこの閾値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントがアソシエートできるのは、クライアント数が閾値を下回るアクセス ポイントだけとなります。

ステップ 3 [Aggressive Load Balancing Denial Count] テキスト ボックスに、1 ～ 10 の値を入力します。
拒否数は、ロード バランシング中のアソシエーション拒否の最大数を設定します。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Save Configuration] をクリックします。

ステップ 6 特定の WLAN 上でアグレッシブ ロード バランシングを有効または無効にするには、次の手順を実行します。

a) [WLANs] > [WLAN ID] を選択します。[Wireless Networks Details] ページが表示されます。
b) [Advanced] タブで、[Load Balance] および [Band Select] チェックボックスをオンまたはオフにします。
c) [Done] をクリックします。
d) [Apply] をクリックします。設定が正常に適用されたメッセージが表示されます。

アグレッシブ ロード バランシングのモニタリング

ここでは、アグレッシブ ロード バランシング用の新しいコマンドについて説明します。

次のコマンドがスイッチ上でアグレッシブ ロード バランシングをモニタするために使用できます。

表 *147*：アグレッシブ ロード バランシング コマンドの監視

コマンド	目的
show wireless load-balancing	ロードバランシング機能のステータスを表示します。

アグレッシブ ロード バランシングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

アグレッシブ ロード バランシングの設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 88 章

クライアント ローミングの設定

- 機能情報の確認，2093 ページ
- クライアント ローミングの設定の制約事項，2093 ページ
- クライアント ローミングについて，2094 ページ
- レイヤ 2 またはレイヤ 3 のローミング設定方法，2097 ページ
- クライアントのローミング パラメータのモニタリング，2104 ページ
- モビリティ設定のモニタ，2105 ページ
- クライアント ローミング設定に関する追加情報，2106 ページ
- クライアント ローミング設定の機能履歴と情報，2107 ページ

機能情報の確認

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

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

クライアント ローミングの設定の制約事項

以下は、クライアント ローミングを設定する際に注意が必要な制約事項です。

- Cisco Compatible Extensions（CCX）サポートは、スイッチ上の各 WLAN について自動的にイネーブルになり、ディセーブルにできません。スイッチは、クライアントの CCX バージョンを自身のクライアント データベースに格納します。この情報に基づいて、CCX フレームを生成するとともに、CCX フレームに応答します。これらのローミング拡張機能を使用する

には、クライアントで CCXv4 か CCXv5（または、アクセス ポイント経由ローミングの場合 CCXv2）がサポートされている必要があります。

- 600 シリーズ アクセス ポイント間のクライアント ローミングはサポートされません。

クライアント ローミングについて

コントローラは、ワイヤレス ネットワークをローミングするクライアントにハイエンドのワイヤレスサービスを提供します。今では、ワイヤレスサービスはスイッチと統合され、付加価値が高く新しい、シスコの統合されたモビリティ アーキテクチャを提供します。この統合されたアーキテクチャにより、ワイヤレスおよび有線クライアントの両方に対して、シームレスで高速なクライアント ローミング サービスが可能になります。

新しいモビリティアーキテクチャは、モビリティドメイン（MD）、モビリティグループ（MG）、モビリティサブドメイン（MSD）にネットワークの論理分類を使用して高速なクライアント ローミング サービスをサポートし、モビリティ Oracle（MO）、モビリティ コントローラ（MC）、モビリティエージェント（MA）などのシステムを使用してスイッチ ピア グループ（SPG）をサポートします。

- **モビリティ ドメイン**は、クライアント ローミングがサポートされているすべてのドメインです。モビリティ ドメインはモビリティ グループの集合です。たとえば、キャンパス ネットワークは、モビリティ ドメインと見なすことができます。
- **モビリティ グループ**は、高速ローミングがサポートされるモビリティ サブドメインの集合です。モビリティ グループは、頻繁にローミングがサポートされているキャンパス内の複数の建物である可能性があります。
- **モビリティ サブドメイン**は、モビリティ ドメイン ネットワークの自律的な部分です。それぞれのモビリティ サブドメインには、1 台のモビリティ コントローラおよび SPG の集合があります。サブドメインは 802.11r キーのドメインと同じです。
- **スイッチ ピア グループ**はモビリティ エージェントの集合です。
- **モビリティ Oracle** はモビリティ サブドメインで発生したモビリティ イベントの接続ポイントとして機能します。モビリティ Oracle は、モビリティ ドメイン全体、自宅、および現在のサブドメインの各クライアントのローカルデータベースも管理します。MO はモビリティ ドメイン全体に対して 1 つだけです。Cisco WLC の 5700 シリーズ コントローラまたは Cisco Unified Wireless Network ソリューション コントローラは、MO として機能します。
- **モビリティ コントローラ**は、SPG 間の ローミング イベントにモビリティ管理サービスを提供します。MC は、そのサブドメインに属するすべてのモビリティ エージェントに、SPG 名や SPG ピア メンバ リストなどの設定を送信します。Cisco WLC 5700 シリーズ コントローラ、Cisco Catalyst 3850 スイッチ、または Cisco Unified Wireless Network ソリューション コントローラは、MC として機能します。MC には、その中で内部的に実行されている MC 機能および MA 機能があります。
- **モビリティ エージェント**は、モバイル クライアント用のクライアント モビリティのステートマシンを維持するコンポーネントです。すべての AP は、モビリティ エージェントに接続されます。

新しいモビリティ アーキテクチャは、次のようなシナリオでのシームレスなローミングをサポートします。

- スイッチ内のローミング：同じモビリティ エージェントが管理する AP 間でのクライアント ローミング。
- SPG内のローミング：同じSPGのモビリティ エージェント間でのクライアント ローミング。
- SPG内、サブドメイン内のローミング：同じサブドメイン内の異なるSPGのモビリティ エージェント間でのクライアント ローミング。
- サブドメイン内のローミング：サブドメインでのモビリティ エージェント間のクライアント ローミング。

高速ローミング

新しいモビリティ アーキテクチャは、完全な認証の必要性を排除することによって、クライアントがモビリティ グループ内でローミングするときの高速なローミングをサポートします。セキュリティ ポリシーは、高速ローミングのためのスイッチ間で同じである必要があります。

ローカル、アンカー、外部 MA および MC

クライアントが MA に最初に参加し、接続ポイントが変更されていない場合、その MA はローカル MA または関連 MA と呼ばれます。この MA が関連づけられている MC は、ローカル MC または関連 MC と呼ばれます。

クライアントが 2 つの MA 間をローミングすると、クライアントが以前関連付けられていた MA は、アンカー MA（接続ポイント）になり、クライアントが現在関連付けられている MA は、外部 MA または関連 MA（プレゼンス ポイント）になります。これらの MA が関連づけられている MC は、アンカー、外部、または関連 MC とそれぞれ呼ばれます。

サブネット間ローミング

同様に、マルチコントローラ展開では、異なるサブネット上の同一モビリティ グループ内のコントローラによって管理されるアクセスポイント間のクライアントローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、クライアントは同じDHCP割り当てまたはクライアント割り当てIPアドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。IP アドレス 0.0.0.0、または自動 IP アドレス 169.254.*.* のクライアントが DHCP Discover を送信するか、オペレータが設定した時間が経過してタイムアウトになると、トンネルが切断され、クライアントの再認証が必要になります。

VoIP による通話ローミング

802.11 Voice-over-IP（VoIP）通話は、RF 信号が最も強いアソシエーションを見つけ出すことで、最適な Quality of Service（QoS）と最高のスループットを実現します。VoIP 通話には、ローミング ハンドオーバーの遅延時間が 20 ミリ秒以下という最小要件がありますが、シスコ ワイヤレス ソリューションならばこの要件を容易に満たすことができます。このソリューションでは、オープン認証が使用されていれば、平均ハンドオーバー遅延時間は 5 ミリ秒以下です。この短い遅延

時間は、個々のアクセスポイントにローミングハンドオーバーのネゴシエートを許可せずにコントローラによって制御されます。

シスコ ワイヤレス ソリューションでは、コントローラが同一のモビリティ グループに属している場合、異なるサブネット上のコントローラによって管理される lightweight アクセス ポイント間での 802.11 VoIP 通話ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、VoIP 通話は同じ DHCP 割り当て IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。VoIP クライアントが VoIP 通話 IP アドレス 0.0.0.0 を使用して DHCP Discover を送信するか、VoIP 通話自動 IP アドレス 169.254.*.* を使用するか、またはオペレータが設定した時間が経過してタイムアウトになると、トンネルが切断され、VoIP クライアントの再認証が必要になります。

CCX レイヤ 2 クライアント ローミング

コントローラでは、次の 5 つの CCX レイヤ 2 クライアント ローミング拡張機能がサポートされています。

- アクセス ポイント経由ローミング：この機能により、クライアントはスキャン時間を節約できます。CCXv2 クライアントがアクセス ポイントにアソシエートする際、新しいアクセス ポイントに以前のアクセスポイントの特徴をリストする情報パケットを送信します。各クライアントがアソシエートされていた以前のアクセスポイントと、アソシエーション直後にクライアントに送信（ユニキャスト）されていた以前のアクセスポイントをすべてまとめて作成したアクセスポイントのリストがクライアントによって認識および使用されると、ローミング時間が短縮します。アクセスポイントのリストには、チャネル、クライアントの現在の SSID をサポートしているネイバー アクセス ポイントの BSSID、およびアソシエーション解除以来の経過時間が含まれています。
- 拡張ネイバー リスト：特に音声アプリケーションを提供する際に、CCXv4 クライアントのローミング能力とネットワーク エッジのパフォーマンスを向上させるための機能です。アクセス ポイントは、ネイバー リストのユニキャスト更新メッセージを使用して、アソシエートされたクライアントのネイバーに関する情報を提供します。
- 拡張ネイバー リスト要求（E2E）：End-2-End 仕様は、音声/ローミング能力の全体的向上のために新しいプロトコルとインターフェイスを定義する、Cisco と Intel の共同プログラムです。これは、CCX 環境の Intel クライアントにのみ適用されます。これにより、Intel クライアントは自由にネイバー リストを要求できるようになります。要求すると、アクセス ポイントはコントローラに要求を転送します。コントローラは要求を受信し、クライアントがアソシエートされているアクセス ポイントに対するネイバーの現在の CCX ローミング サブリストで応答します。

（注） 特定のクライアントが E2E をサポートするかどうかを調べるには、コントローラの GUI で [Wireless] > [Clients] の順に選択し、そのクライアントの [Detail] リンクをクリックして、[Client Properties] 領域の [E2E Version] テキスト ボックスを確認します。

- ローミング理由レポート：CCXv4 クライアントが新しいアクセス ポイントにローミングした理由を報告するための機能です。また、ネットワーク管理者はローミング履歴を作成およびモニタできるようになります。
- ダイレクトされたローミング要求：クライアントがアソシエートしているアクセスポイントよりもサービス能力が高いアクセス ポイントが他にある場合に、ローミング要求をコントローラからクライアントに送信できるようになります。この場合、コントローラはクライアントに join できる最適なアクセスポイントの一覧を送信します。クライアントはダイレクトされたローミング要求を受け入れることも、無視することもできます。CCX 以外のクライアントおよびCCXv3 以下を実行するクライアントは、どちらの操作も行う必要がありません。この機能を使用するために設定する必要はありません。

レイヤ 2 またはレイヤ 3 のローミング設定方法

レイヤ 2 またはレイヤ 3 のローミング設定

はじめる前に

レイヤ 2 またはレイヤ 3 ローミングをモビリティ エージェントに設定するには、次の必要条件を考慮する必要があります。

- レイヤ 2 とレイヤ 3 ローミングのための SSID およびセキュリティ ポリシーは、MA 全体で同じである必要があります。
- クライアント VLAN ID は、レイヤ 2 ローミングでは同じで、レイヤ 3 ローミングでは異なっている必要があります。
- ブリッジ ドメイン ID とクライアント VLAN ID は、レイヤ 2 ローミングで同じである必要があります。ブリッジ ドメイン ID とクライアント VLAN ID のうち、一方または両方が、レイヤ 3 ローミングで異なる必要があります。

手順の概要

1. **configure terminal**
2. **wlan***wlan_profile_namewlan_IDSSID_network_name*
3. **no mobility anchor sticky**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan***wlan_profile_namewlan_IDSSID_network_name* 例： スイッチ(config)#**wlan wlan1**	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**no mobility anchor sticky** 例： スイッチ(config-wlan)#**no mobility anchor sticky**	（任意）レイヤ2アンカーをディセーブルにします。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権EXECモードに戻ります。また、Ctrl+Zキーを押しても、グローバル コンフィギュレーション モードを終了できます。

CCX クライアント ローミング パラメータの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 {5ghz | 24ghz} l2roam rf-params**{**default | custom***min-rssiroam-hystscan-threshtrans-time*}
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 {5ghz | 24ghz} l2roam rf-params**{**default | custom***min-rssiroam-hystscan-threshtrans-time*}	CCX レイヤ2クライアント ローミング パラメータを設定します。 デフォルト RF パラメータを選択するには、**default** オプションを入力します。

	コマンドまたはアクション	目的
	例： スイッチ#**ap dot11 5ghz l2roam rf-params custom -80**	クライアント ローミングに影響を与える RF パラメータを最適化するには、**custom** オプションを入力してから、次のオプションのいずれかを入力してください： • [Minimum RSSI]：クライアントがアクセス ポイントにアソシエートするために必要な最小の受信信号強度インジケータ（RSSI）を示します。 クライアントの平均の受信信号の強度がこのしきい値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。 最小の RSSI 値を -50 ～ -90 dBm の範囲で設定できます。また、デフォルト値は -85 dBm です。 • [Hysteresis]：クライアントが近隣のアクセス ポイントにローミングするときに必要な信号強度の値を示します。 このパラメータは、クライアントが 2 つのアクセス ポイント間のボーダー近くに物理的に存在している場合に、アクセス ポイント間のローミングの量を減らすことを意図しています。 [Hysteresis] は、3 ～ 20 dB の範囲で設定できます。デフォルトは 3 dB です。 • [Scan Threshold]：クライアントがより適切なアクセス ポイントにローミングするまでに許可される最小 RSSI を示します。 RSSI が指定された値より低い場合、クライアントは指定遷移時間内により強い信号のあるアクセス ポイントへローミングできる必要があります。このパラメータはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。 RSSI 値を -50 ～ -90 dBm の範囲で設定できます。また、デフォルト値は -72 dBm です。 • [Transition Time]：クライアントのアソシエートされたアクセス ポイントからの RSSI がスキャンしきい値より低くなった場合に、クライアントがローミングに適した近傍のアクセス ポイントの検出およびローミングにかけられる最大許容時間を示します。

	コマンドまたはアクション	目的
		[Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミングパフォーマンスの最低レベルを保証します。これらのパラメータを使用すると、最も高いクライアント速度とローミングヒステリシスが得られるだけでなく、アクセスポイント間の一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。 1 ～ 5 秒の範囲で時間を設定できます。デフォルトの時間は 5 秒です。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

モビリティ Oracle の設定

手順の概要

1. **configure terminal**
2. **wireless mobility oracle**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless mobility oracle** 例： `スイッチ(config)# wireless mobility oracle`	コントローラのモビリティ Oracle をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

モビリティ コントローラの設定

手順の概要

1. **configure terminal**
2. **wireless mobility controller**
3. **wireless mobility controller peer-group** *switch-peer-group-name*
4. **wireless mobility controller peer-group** *switch-peer-group-name* **member ip** *ip-address* {**public-ip** *public-ip-address*}
5. **wireless mobility controller peer-group** *switch-peer-group-name* **multicast**
6. **wireless mobility controller peer-group** *switch-peer-group-name* **multicast ip** *peer-group-multicast-ip-addr*
7. **wireless mobility controller peer-group***switch-peer-group-name* **bridge-domain-id** *id*
8. **wireless mobility group member ip** *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*]
9. **wireless mobility dscp** *value*
10. **wireless mobility group keepalive** {*count* | *interval*}
11. **wireless mobility group name** *name*
12. **wireless mobility oracle ip***mo-ip-address*
13. **wireless management interface** *interface-name*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless mobility controller** 例： スイッチ(config)# wireless mobility controller	ワイヤレス モビリティ コントローラをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**wireless mobility controller peer-group** *switch-peer-group-name* 例： `スイッチ(config)# wireless mobility controller peer-group SPG1`	スイッチ ピア グループ名を設定します。グループ名には、最大 31 文字の印字可能な ASCII 文字（大文字小文字が区別されます）を入力できます。モビリティ グループ名には、スペースは使用できません。 （注） このコマンドの **No** 形式を使用すると、スイッチ ピア グループを削除します。
ステップ 4	**wireless mobility controller peer-group** *switch-peer-group-name* **member ip** *ip-address* {**public-ip** *public-ip-address*} 例： `スイッチ(config)# wireless mobility controller peer-group SPG1 member ip 10.0.0.1`	スイッチ ピア グループにモビリティ グループ メンバを追加します。 （注） このコマンドの **No** 形式を使用すると、スイッチ ピア グループからメンバを削除します。
ステップ 5	**wireless mobility controller peer-group** *switch-peer-group-name* **multicast** 例： `スイッチ(config)# wireless mobility controller peer-group SPG1 multicast`	スイッチ ピア グループ内でマルチキャスト モードを設定します。
ステップ 6	**wireless mobility controller peer-group** *switch-peer-group-name* **multicast ip** *peer-group-multicast-ip-addr* 例： `スイッチ(config)# wireless mobility controller peer-group SPG1 multicast ip 10.0.0.4`	スイッチ ピア グループのマルチキャスト IP アドレスを設定します。 （注） このコマンドの **No** 形式を使用すると、スイッチ ピア グループからマルチキャスト IP を削除します。
ステップ 7	**wireless mobility controller peer-group***switch-peer-group-name* **bridge-domain-id** *id* 例： `スイッチ(config)# wireless mobility controller peer-group SPG bridge-domain-id 10.0.0.5`	スイッチ ピア グループのブリッジ ドメイン ID を設定します。デフォルトは 0 です。 （注） このコマンドの **No** 形式を使用すると、ブリッジ ドメイン ID をデフォルトの値に設定します。
ステップ 8	**wireless mobility group member ip** *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*] 例： `スイッチ(config)# wireless mobility group member ip 10.0.0.1`	モビリティ グループ メンバを追加します。 （注） このコマンドの **No** 形式を使用すると、グループからメンバを削除します。デフォルトのグループ名は MC のグループ名です。

	コマンドまたはアクション	目的
ステップ 9	**wireless mobility dscp** *value* 例： スイッチ(config)# wireless mobility dscp 46	モビリティ制御パケットの DSCP 値を設定します。 DSCP 値に指定できる範囲は 0 ～ 63 です。デフォルト値は 46 です。
ステップ 10	**wireless mobility group keepalive** {*count* | *interval*} 例： スイッチ(config)# wireless mobility group keepalive count	ワイヤレス モビリティ グループのキープアライブ数（メンバのステータスが DOWN するまでのキープアライブの試行回数、および 2 つのキープアライブ間の間隔であるキープアライブ インターバル）を設定します。
ステップ 11	**wireless mobility group name** *name* 例： スイッチ(config)# wireless mobility group name group1	最大 31 文字の印字可能な ASCII 文字（大文字小文字が区別されます）で、ワイヤレスモビリティ グループ名を指定します。
ステップ 12	**wireless mobility oracle ip***mo-ip-address* 例： スイッチ(config)# wireless mobility oracle ip 10.0.0.5	モビリティ oracle に IP アドレスを設定します。
ステップ 13	**wireless management interface** *interface-name* 例： スイッチ(config)# wireless management interface Vlan21	ワイヤレス管理インターフェイスを設定します。
ステップ 14	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

モビリティ エージェントの設定

手順の概要

1. **configure terminal**
2. **wireless mobility controller ip** *ip-address*
3. **wireless mobility load-balance**
4. **wireless mobility load-balance threshold** *threshold -value*
5. **wireless management interface** *interface-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless mobility controller ip** *ip-address* 例： スイッチ(config)# wireless mobility controller ip 10.10.10.20	モビリティ コントローラの IPアドレスを設定します。
ステップ 3	**wireless mobility load-balance** 例： スイッチ(config)# wireless mobility load-balance	ワイヤレス モビリティ ロード バランシングを設定します。
ステップ 4	**wireless mobility load-balance threshold** *threshold -value* 例： スイッチ(config)# wireless mobility load-balance threshold 100	ローカル、またはMA にアンカーできるクライアント数を設定します。100～2000 の範囲でしきい値を設定できます。デフォルト値は 1000 です。
ステップ 5	**wireless management interface** *interface-name* 例： スイッチ(config)# wireless management interface Vlan21	モビリティ エージェントのワイヤレス管理インターフェイスを設定します。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

クライアントのローミング パラメータのモニタリング

このセクションでは、クライアント パラメータ用の新しいコマンドについて説明します。

次のコマンドがスイッチ のクライアント ローミング パラメータをモニタするために使用できます。

表 *148*：クライアント ローミング パラメータ モニタリング コマンド

コマンド	目的

show ap dot11 {5ghz | 24ghz} l2roam rf-param	802.11a または 802.11b/g ネットワーク上でクライアント ローミングに設定されている現在の RF パラメータを表示します。
show ap dot11 {5ghz | 24ghz} l2roam statistics	802.11a または 802.11b/g ネットワークの CCX レイヤ2クライアント ローミング統計を表示します。
show ap dot11 {5ghz | 24ghz} l2roam mac-address *mac-address* **statistics**	特定のアクセス ポイントの CCX レイヤ 2 クライアント ローミング統計を表示します。

モビリティ設定のモニタ

このセクションでは、モビリティ設定をモニタするための新しいコマンドについて説明します。

次のコマンドは、モビリティ Oracle、モビリティ コントローラとモビリティ エージェントのモビリティ設定のモニタリングに使用できます。

表 ***149*** : モビリティ コントローラおよびモビリティ エージェント用モビリティ設定モニタリング コマンド

コマンド	目的
show wireless mobility summary	モビリティ コントローラとモビリティ エージェントのサマリー情報を表示します。
show wireless mobility statistics	モビリティの統計情報を表示します。
show wireless mobility dtls connections	確立した DTLS 接続を表示します。

表 ***150*** : モビリティ ***Oracle*** 用モビリティ設定モニタリング コマンド

コマンド	目的
show wireless mobility oracle summary	モビリティ Oracle が認識するモビリティ コントローラの状態を表示します。
show wireless mobility oracle client summary	モビリティ Oracle データベース内クライアントの情報を表示します。
show wireless mobility oracle client detail*client -mac-address*	モビリティ Oracle データベース内の、特定のクライアントの詳細情報を表示します。

show wireless mobility oracle*mc-ip*	指定のモビリティ コントローラにアンカーされている、または関連付けられているモビリティ Oracle データベース内クライアント一覧の情報を表示します。

表 *151* : モビリティ コントローラ用モビリティ設定モニタリング コマンド

コマンド	目的
show wireless mobility controller client summary	サブドメインのクライアントのリストを表示します。
show wireless mobility controller client*mac-address***detail**	サブドメインのクライアントに関する詳細情報を表示します。
show wireless mobility agent*ma-ip***client summary**	指定のモビリティ エージェントにアンカーされている、または関連付けられているクライアントのリストを表示します。
show wireless mobility ap-list	モビリティ グループに認識される Cisco AP のリストを表示します。

表 *152* : モビリティ エージェント用モビリティ設定モニタリング コマンド

コマンド	目的
show wireless mobility load-balance summary	モビリティ ロード バランス プロパティの概要を表示します。

クライアント ローミング設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
モビリティ設定	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
モビリティ関連のコマンド	*Mobility Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

クライアント ローミング設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 89 章

Application Visibility and Control の設定

- 機能情報の確認，2109 ページ
- Application Visibility and Control について，2110 ページ
- サポートされる AVC クラス マップおよびポリシー マップのフォーマット，2111 ページ
- アプリケーションの可視性およびコントロールの前提条件，2114 ページ
- Application Visibility and Control によるスイッチ間ローミングに関するガイドライン，2114 ページ
- Application Visibility and Control の制限，2115 ページ
- Application Visibility and Control の設定方法，2115 ページ
- Application Visibility and Control のモニタリング，2137 ページ
- 例：Application Visibility and Control，2140 ページ
- Application Visibility and Control に関する追加情報，2143 ページ
- Application Visibility and Control の機能履歴および情報，2144 ページ

機能情報の確認

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

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

Application Visibility and Control について

Application Visibility and Control（AVC）は、ネットワークベースのアプリケーション認識エンジンによるディープ パケット インスペクション技術を使用してアプリケーションを分類し、無線ネットワークにアプリケーション レベルの可視性と制御（QoS）を提供します。アプリケーションの認識後は、AVC機能によってデータ トラフィックをドロップ、マーク、またはポリシングできます。

AVC はプロトコルと一致するように QoS クライアント ポリシー内のクラス マップを定義することによって設定されます。

AVC を使用して、1000 以上のアプリケーションを検出できます。AVC により、リアルタイム分析を実施し、ネットワークの輻輳、コストの掛かるネットワーク リンクの使用、およびインフラストラクチャの更新を削減するためのポリシーを作成することができるようになります。

（注） UI の [Monitor Summary] セクションで、[Top Applications] に 30 のアプリケーションのリストを表示できます。

トラフィック フローは、アクセス ポイントの NBAR2 エンジンを通して分析および認識されます。NBAR2 対応プロトコルまたはアプリケーションについて、8.0 プロトコル パックを参照してください。特定のフローが WebEx などの認識されたプロトコルまたはアプリケーションでマークされます。このフロー単位の情報は Flexible NetFlow（FNF）によるアプリケーションの可視化に使用できます。FNF の詳細については、『*Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*』を参照してください。QoS を使用したトラフィックの制御にも同じアプリケーション名を使用できます。QoS の詳細については、『*QoS Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*』を参照してください。

AVC QoS アクションは、AVC フィルタを通してアップストリームとダウンストリームの両方向に適用されます。アップストリーム フローに対してサポートされる QoS アクションはドロップ、マーク、およびポリシングで、ダウンストリーム フローに対してサポートされるアクションはマークとポリシングです。AVC QoS は、アプリケーションが正しく分類され、ポリシーマップ内のクラスマップ フィルタに一致する場合にだけ適用できます。たとえば、ポリシーにアプリケーション名に基づくフィルタが含まれており、トラフィックも同じアプリケーション名に分類されている場合は、ポリシー内でこの一致に対して指定されたアクションが適用されます。すべての QoS アクションについては、サポートされる AVC クラス マップおよびポリシー マップのフォーマット，（2111 ページ）を参照してください。

Application Visibility and Control プロトコル パック

プロトコル パックとは、コントローラ ソフトウェアのリリース トレーニング以外のプロトコル アップデートを配布する方法です。コントローラ ソフトウェアを交換せずにコントローラにロードできます。

Application Visibility and Control プロトコル パック（AVC プロトコル パック）は、複数のプロトコル記述言語（PDL）ファイルとマニフェスト ファイルを含む単一の圧縮ファイルです。必要なプロトコルのセットをロードすることができ、ネットワークでの分類のために追加プロトコルを

認識する際に役立ちます。マニフェストファイルは、プロトコルパックの名前、バージョン、およびプロトコル パック内の利用可能な PDL の情報など、プロトコル パックに関する情報を提供します。

AVC プロトコル パックは、特定の AVC エンジン バージョン向けにリリースされています。コントローラ プラットフォームのエンジン バージョンがプロトコル パックに必要なバージョン以降であれば、プロトコル パックをロードできます。

サポートされるAVCクラスマップおよびポリシーマップのフォーマット

サポートされる AVC クラス マップのフォーマット

クラス マップのフォーマット	クラスマップの例	方向
match protocol*protocol name*	`class-map match-any webex-class match protocol webex-media`	アップストリームおよびダウンストリームの両方で
match protocolattribute category*category-name*	`class-map match-any IM match protocol attribute category instant-messaging`	アップストリームおよびダウンストリームの両方で
match protocolattribute sub-category*sub-category-name*	`class-map match-any realtimeconferencing match protocol attribute sub-category voice-video-chat-collaboration`	アップストリームおよびダウンストリームの両方で
match protocolattribute application-group*application-group-name*	`class-map match-any skype match protocol attribute application-group skype-group`	アップストリームおよびダウンストリームの両方で
組み合わせフィルタ	`class-map match-any webex-class match protocol webex match dscp 45 match wlan user-priority 6`	アップストリームのみ

サポートされる AVC ポリシーのフォーマット

ポリシーのフォーマット	QoS 処理
match protocol フィルタに基づいてクライアントポリシーをアップストリーム	マーク、ポリシー、およびドロップ
match protocol フィルタに基づいてクライアントポリシーをダウンストリーム	マークおよびポリシー

次の表で、AVC ポリシーの詳細なフォーマット、および例について説明します。

AVC ポリシーのフォーマット	AVC ポリシーの例	方向

ベーシック セット	`policy-map webex-policy`
	` class webex-class`
	` set dscp ef //or set up,cos`
		アップストリームおよびダウンストリーム

ベーシック ポリシー	`policy-map webex-policy`
	` class webex-class`
	` police 5000000`
		アップストリームおよびダウンストリーム

ベーシック セットおよびポリシー	`policy-map webex-policy`
	` class webex-class`
	` set dscp ef //or set up,cos`
	` police 5000000`
		アップストリームおよびダウンストリーム

デフォルトを含む複数のセットおよびポリシー	`policy-map webex-policy`
	` class webex-class`
	` set dscp af31 //or set up,cos`
	` police 4000000`
	` class class-webex-category`
	` set dscp ef //or set up,cos`
	` police 6000000`
	` class class-default`
	` set dscp <>`
		アップストリームおよびダウンストリーム

階層型ポリシー	`policy-map webex-policy`
	` class webex-class`
	` police 5000000`
	` service-policy client-in-police-only`
	
	` policy-map client-in-police-only`
	` class webex-class`
	` police 100000`
	` class class-webex-category`
	` set dscp ef //or set up,cos`
	` police 6000000`
	` police 200000`
		アップストリームおよびダウンストリーム

階層型セットおよびポリシー	`policy-map webex-policy`
	` class class-default`
	` police 1500000`
	` service policy client-up-child`
	` policy-map webex-policy`
	` class webex-class`
	` police 100000`
	` set dscp ef`
	` class class-webex-category`
	` police 200000`
	` set dscp af31`	

ドロップ アクション		アップストリームのみ

AVC ポリシーのフォーマット	AVC ポリシーの例	方向

	上記のいずれかの例を、この追加例とともにこのフォーマットに適用します。
	`policy-map webex-policy`
	` class webex-class`
	` drop`
	` class netflix`
	` set dscp ef //or set up,cos`
	` police 6000000`
	` class class-default`
	` set dscp <>`	

アプリケーションの可視性およびコントロールの前提条件

- アクセスポイントは、AVC 対応である必要があります
- AVC（QoS）の制御部分を機能させるには、FNF 付きのアプリケーションの可視化機能を設定する必要があります。

Application Visibility and Control によるスイッチ間ローミングに関するガイドライン

不正な形式の QoS ポリシーによりクライアントが除外されるのを防ぐには、次のガイドラインに従います。

- 新しい QoS ポリシーをスイッチに追加する場合、同じ名前の QoS ポリシーは、同じローミングまたはモビリティ ドメイン内の他のスイッチに追加する必要があります。
- スイッチに新しいリリースのソフトウェアイメージがロードされると、新しいポリシー形式がサポートされます。以前のリリースから新しいリリースにソフトウェアイメージをアップグレードした場合は、設定を別々に保存する必要があります。以前のリリースのイメージがロードされると、一部の QoS ポリシーがサポートされていないと表示される場合があり、それらの QoS ポリシーをサポートされるポリシー形式に復元する必要があります。

Application Visibility and Control の制限

Application Visibility and Control の設定方法

アプリケーションの可視性およびコントロールの設定（CLI）

アプリケーションの可視性を設定するには、次の手順を実行します。

1. フローにキーフィールドおよび非キーフィールドを指定して、フロー レコードを作成します。
2. オプションとしてフロー レコードを指定して、任意のフロー エクスポータを作成します。
3. フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを作成します。
4. Ipv4 入力または出力方向にフロー モニタを適用するように WLAN を設定します。

アプリケーションの制御を設定するには、次の手順を実行します。

1. AVC QoS ポリシーを作成します。
2. 次の 3 つの方法のいずれかを使用してクライアントに AVC QoS ポリシーを接続します。WLAN の設定、ACS または ISE の使用、またはローカル ポリシーの追加。

フロー レコードの作成

デフォルトでは、**wireless avc basic**（フロー レコード）の使用が可能です。GUI から [Apply] をクリックすると、レコードはフロー モニタにマッピングされます。

デフォルトのフロー レコードは、編集も削除もできません。新しいフロー レコードが必要な場合、1 つを作成し、CLI からのフロー モニタにマップする必要があります。

手順の概要

1. **configure terminal**
2. **flowrecord***flow_record_name*
3. **description***string*
4. **matchipv4protocol**
5. **matchipv4sourceaddress**
6. **matchipv4destinationaddress**
7. **matchtransportsource-port**
8. **matchtransportdestination-port**
9. **matchflowdirection**
10. **matchapplicationname**
11. **matchwirelessssid**
12. **collectcounterbyteslong**
13. **collectcounterpacketslong**
14. **collectwirelessapmacaddress**
15. **collectwirelessclientmacaddress**
16. **end**

手順の詳細

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

ステップ 2	**flowrecord***flow_record_name*
	
	例：
	`スイッチ(config)# flow record record1`
	`スイッチ (config-flow-record)#`
		フロー レコード コンフィギュレーション モードを開始します。

ステップ 3	**description***string* 例： `スイッチ(config-flow-record)# description IPv4flow`	（任意）最大 63 文字で、このフロー レコードの説明を指定します。
ステップ 4	**matchipv4protocol** 例： `スイッチ (config-flow-record)# match ipv4 protocol`	IPv4 プロトコルとの一致を指定します。

	コマンドまたはアクション	目的
ステップ 5	**matchipv4sourceaddress** 例： スイッチ (config-flow-record)# **match ipv4 source address**	IPv4 送信元アドレス ベースのフィールドとの一致を指定します。
ステップ 6	**matchipv4destinationaddress** 例： スイッチ (config-flow-record)# **match ipv4 destination address**	IPv4 宛先アドレス ベースのフィールドとの一致を指定します。
ステップ 7	**matchtransportsource-port** 例： スイッチ (config-flow-record)# **match transport source-port**	トランスポート層の発信元ポートのフィールドとの一致を指定します。
ステップ 8	**matchtransportdestination-port** 例： スイッチ (config-flow-record)# **match transport destination-port**	トランスポート層の宛先ポートのフィールドとの一致を指定します。
ステップ 9	**matchflowdirection** 例： スイッチ (config-flow-record)# **match flow direction**	フローがモニタされる方向との一致を指定します。
ステップ 10	**matchapplicationname** 例： スイッチ (config-flow-record)# **match application name**	アプリケーション名との一致を指定します。 （注） この操作は、AVC サポートでは必須です。フローがアプリケーションと一致することが可能になるためです。
ステップ 11	**matchwirelessssid** 例： スイッチ (config-flow-record)# **match wireless ssid**	ワイヤレス ネットワークを特定するSSID名との一致を指定します。
ステップ 12	**collectcounterbyteslong** 例： スイッチ (config-flow-record)# **collect counter bytes long**	カウンタ フィールドの合計バイトを収集するように指定します。
ステップ 13	**collectcounterpacketslong** 例： スイッチ (config-flow-record)# **collect counter bytes long**	カウンタ フィールドの合計パケットを収集するように指定します。

	コマンドまたはアクション	目的
ステップ 14	**collectwirelessapmacaddress** 例： スイッチ (config-flow-record)# **collect wireless ap mac address**	ワイヤレス クライアントが関連付けられているアクセス ポイントの MAC アドレスの BSSID を収集するように指定します。
ステップ 15	**collectwirelessclientmacaddress** 例： スイッチ (config-flow-record)# **collect wireless client mac address**	ワイヤレス ネットワークのクライアントの MAC アドレスを収集するように指定します。
ステップ 16	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

フロー エクスポータの作成（オプション）

フローエクスポートを作成すると、フローのエクスポートパラメータを定義できます。これは、フロー パラメータを設定するためのオプションの手順です。

手順の概要

1. **configure terminal**
2. **flowexporter***flow_exporter_name*
3. **description***string*
4. **destination***{hostname | ip-address}*
5. **transport udp***port-value*
6. **optionapplication-tabletimeout***seconds***(optional)**
7. **optionusermac-tabletimeout***seconds***(optional)**
8. **end**
9. **show flow exporter**
10. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**flowexporter***flow_exporter_name* 例： スイッチ(config)# **flow exporter record1** スイッチ (config-flow-exporter)#	フロー エクスポータ コンフィギュレーション モードを開始します。
ステップ 3	**description***string* 例： スイッチ(config-flow-exporter)# **description IPv4flow**	最大 63 文字で、フロー レコードの説明を示します。
ステップ 4	**destination***{hostname | ip-address}* 例： スイッチ (config-flow-exporter) # **destination** 10.99.1.4	エクスポータでデータを送信する宛先システムのホスト名または IPv4 アドレスを指定します。
ステップ 5	**transport udp***port-value* 例： スイッチ (config-flow-exporter) # **transport udp** 2	UDP プロトコルのポートの値を設定します。
ステップ 6	**optionapplication-tabletimeout***seconds***(optional)** 例： スイッチ (config-flow-exporter)# **option application-table timeout 500**	（任意）application table timeout オプションを指定します。有効な範囲は 1 ～ 86400 秒です。
ステップ 7	**optionusermac-tabletimeout***seconds***(optional)** 例： スイッチ (config-flow-exporter)# **option usermac-table timeout 1000**	（任意）wireless usermac-to-username table オプションを指定します。有効な範囲は 1 ～ 86400 秒です。
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 9	**show flow exporter** 例： スイッチ # **show flow exporter**	設定を確認します。
ステップ 10	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

フロー モニタの作成

フロー モニタを作成して、フロー レコードおよびフロー エクスポータと関連付けることができます。

手順の概要

1. **configure terminal**
2. **flow monitor***monitor-name*
3. **description***description*
4. **record***record-name*
5. **exporter***exporter-name*
6. **cachetimeout**{**active**|**inactive**}**(Optional)**
7. **end**
8. **show flow monitor**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flow monitor***monitor-name* 例： `スイッチ (config)# flow monitor flow-monitor-1`	フローモニタを作成し、フローモニタ コンフィギュレーション モードを開始します。
ステップ 3	**description***description* 例： `スイッチ (config-flow-monitor)# description flow-monitor-1`	フロー モニタの説明を作成します。
ステップ 4	**record***record-name* 例： `スイッチ (config-flow-monitor)# record flow-record-1`	事前に作成されたレコーダの名前を指定します。
ステップ 5	**exporter***exporter-name* 例： `スイッチ (config-flow-monitor)# exporter flow-exporter-1`	事前に作成されたエクスポータの名前を指定します。

	コマンドまたはアクション	目的
ステップ 6	**cachetimeout{active|inactive}(Optional)** 例： スイッチ (config-flow-monitor)# **cache timeout active 1800** スイッチ (config-flow-monitor)# **cache timeout inactive 200**	フロー キャッシュ パラメータを設定するように指定します。1 ～ 604800 秒の時間範囲で設定できます（任意）。 （注） AVC フロー モニタで最適な結果を得るためには、非アクティブなキャッシュのタイムアウト値を 90 秒よりも長く設定することをお勧めします。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show flow monitor** 例： スイッチ # **show flow monitor**	設定を確認します。

AVC QoS ポリシーの作成

AVC QoS ポリシーを作成するには、次の一般的な手順を実行します。

1. match protocol フィルタでクラス マップを作成します。
2. ポリシー マップを作成します。
3. 次のいずれかの方法でクライアントにポリシー マップを適用します。
   a. CLI または GUI から WLAN 上にポリシー マップを適用します。
   b. CLI から AAA サーバ（ACS サーバまたは ISE）を使用してポリシー マップを適用します。

      詳細については、『*Cisco Identity Services Engine User Guide*』および『*Cisco Secure Access Control System User Guide*』を参照してください。
   c. CLI または GUI からローカル ポリシーを適用します。

クラス マップの作成

match protocol フィルタを設定する前に、クラスマップを作成する必要があります。マーキング、ポリシング、ドロップなどの QoS アクションがトラフィックに適用できます。AVC の match protocol フィルタはワイヤレス クライアントにのみ適用されます。サポートされているプロトコルについては、「8.0 protocol pack」 を参照してください。

手順の概要

1. **configure terminal**
2. **class-map***class-map-name*
3. **match protocol**{*application-name*|**attribute category***category-name*|**attribute sub-category***sub-category-name*|**attribute application-group***application-group-name*}
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map***class-map-name* 例： スイッチ(config)# **class-map webex-class**	クラス マップを作成します。
ステップ 3	**match protocol**{*application-name*|**attribute category***category-name*|**attribute sub-category***sub-category-name*|**attribute application-group***application-group-name*} 例： スイッチ(config)# **class-map webex-class** スイッチ(config-cmap)# **match protocol webex-media** スイッチ(config)# **class-map class-webex-category** スイッチ(config-cmap)# **match protocol attribute category webex-media** スイッチ# **class-map class-webex-sub-category** スイッチ(config-cmap)# **match protocol attribute sub-category webex-media** スイッチ# **class-map class-webex-application-group** スイッチ(config-cmap)# **match protocol attribute application-group webex-media**	アプリケーション名、カテゴリ名、サブカテゴリの名前、またはアプリケーショングループに一致するものを指定します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権EXECモードに戻ります。また、Ctrl+Zキーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシー マップの作成

手順の概要

1. **configure terminal**
2. **policy-map***policy-map-name*
3. **class** [*class-map-name* | **class-default**]
4. **police***rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]
5. **set**{**dscp***new-dscp*|**cos***cos-value*}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map***policy-map-name* 例： スイッチ(config)# **policy-map webex-policy** スイッチ(config-pmap)#	ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。 （注） 既存のポリシー マップを削除するには、**no policy-map***policy-map-name* グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**class** [*class-map-name*	**class-default**] 例： スイッチ(config-pmap)# **class-map webex-class** スイッチ(config-pmap-c)#	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップおよびクラス マップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **class-default** トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシー マップの最後に配置されます。暗黙の **match any** が **class-default** クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは **class-default** と一致します。 （注） 既存のクラス マップを削除するには、**no class***class-map-name* ポリシーマップ コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	**police***rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] 例： スイッチ(config-pmap-c)# **police 100000 80000 drop**	分類したトラフィックにポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。指定できる範囲は 8000 ～ 10000000000 です • *burst-byte* には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ～ 1000000 です。 •（任意）レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。（ポリシング済み DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。
ステップ 5	**set**{**dscp***new-dscp*|**cos***cos-value*} 例： スイッチ(config-pmap-c)# **set dscp 45**	パケットに新しい値を設定することによって、IP トラフィックを分類します。 • **dscp***new-dscp* には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

次の作業

ポリシーマップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーまたはポリシーをインターフェイスに付加します。

ローカル ポリシーの設定（*CLI*）

ローカル ポリシーの設定（CLI）

ローカル ポリシーを設定するには、次の手順を実行します。

1. サービス テンプレートを作成します。
2. インターフェイス テンプレートを作成します。
3. パラメータ マップを作成します。
4. ポリシー マップを作成します。
5. WLAN 上でローカル ポリシーを適用します。

サービス テンプレートの作成（CLI）

手順の概要

1. **configure terminal**
2. **service-template***service-template-name*
3. **access-group***acl_list*
4. **vlan***vlan_id*
5. **absolute-timer***seconds*
6. **service-policy qos**{**input**|**output**}
7. **end**

手順の詳細

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

ステップ 2	**service-template***service-template-name*
	
	例：
	
	`スイッチ(config)# service-template cisco-phone-template`
	`スイッチ(config-service-template)#`
		サービス テンプレート コンフィギュレーション モードを開始します。

ステップ 3	**access-group***acl_list* 例： `スイッチ(config-service-template)# access-group foo-acl`	適用するアクセス リストを指定します。
ステップ 4	**vlan***vlan_id* 例： `スイッチ(config-service-template)# vlan 100`	VLAN ID を指定します。1 ～ 4094 の値を指定できます。
ステップ 5	**absolute-timer***seconds* 例： `スイッチ(config-service-template)# absolute-timer 20`	サービステンプレートのセッション タイムアウト値を指定します。1 ～ 65535 の値を指定できます。

	コマンドまたはアクション	目的
ステップ 6	**service-policy qos**{**input**|**output**} 例： スイッチ(config-service-template)# **service-policy qos input foo-qos**	クライアントの QoS ポリシーを設定します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

パラメータ マップの作成（CLI）

クラス マップよりパラメータ マップを使用することをお勧めします。

手順の概要

1. **configure terminal**
2. **parameter-map typesubscriberattribute-to-service***parameter-map-name*
3. *map-index***map**{**device-type**|**mac-address**|**oui**|**user-role**|**username**}{**eq**|**not-eq**|**regex***filter-name*}
4. **interface-template***interface-template-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map typesubscriberattribute-to-service***parameter-map-name* 例： スイッチ(config)# **parameter-map type subscriber attribute-to-service Aironet-Policy-para**	パラメータ マップのタイプと名前を指定します。
ステップ 3	*map-index***map**{**device-type**|**mac-address**|**oui**|**user-role**|**username**}{**eq**|**not-eq**|**regex***filter-name*} 例： スイッチ(config-parameter-map-filter)# **10 map device-type eq "WindowsXP-Workstation"**	パラメータ マップ属性フィルタ基準を指定します。

	コマンドまたはアクション	目的
ステップ 4	**interface-template***interface-template-name* 例： スイッチ(config-parameter-map-filter-submode)# **interface-template cisco-phone-template** スイッチ(config-parameter-map-filter-submode)#	サービステンプレートコンフィギュレーション モードを開始します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報，（776 ページ）
ローカル ポリシーの設定に関する制限，（775 ページ）
ローカル ポリシーの監視，（784 ページ）
例：ローカル ポリシーの設定，（785 ページ）

ポリシー マップの作成（CLI）

手順の概要

1. **configure terminal**
2. **policy-map typecontrolsubscriber***policy-map-name*
3. **eventidentity-update**{**match-all**|**match-first**}
4. *class_number***class** {*class_map_name*|**always** }{**do-all**| **do-until-failure**| **do-until-success**}
5. *action-index***mapattribute-to-servicetable***parameter-map-name*
6. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**policy-map typecontrolsubscriber***policy-map-name* 例： スイッチ(config)# **policy-map type control subscriber Aironet-Policy**	ポリシー マップ タイプを指定します。
ステップ 3	**eventidentity-update**{**match-all**|**match-first**} 例： スイッチ(config-policy-map)# **event identity-update match-all**	ポリシーマップに対する一致基準を指定します。
ステップ 4	*class_number***class** {*class_map_name*|**always** }{**do-all**| **do-until-failure**| **do-until-success**} 例： スイッチ(config-class-control-policymap)# **1 class local_policy1_class do-until-success**	ローカル プロファイリング ポリシー クラスマップ番号を設定し、処理の実行方法を指定します。クラスマップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • **always**：照合を行わずに実行しますが、成功を返します。 • **do-all**：すべての処理を実行します。 • **do-until-failure**：照合が失敗するまですべての処理を実行します。これはデフォルト値です。 • **do-until-success**：照合が成功するまですべての処理を実行します。
ステップ 5	*action-index***mapattribute-to-servicetable***parameter-map-name* 例： スイッチ(config-policy-map)# **10 map attribute-to-service table Aironet-Policy-para**	使用するパラメータ マップ テーブルを指定します。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報，（776 ページ）
ローカル ポリシーの設定に関する制限，（775 ページ）

ローカル ポリシーの監視，（784 ページ）
例：ローカル ポリシーの設定，（785 ページ）

WLAN 上のデバイスのローカル ポリシーの適用（CLI）

はじめる前に

パラメータ マップのサービス ポリシーにデバイス タイプ ベースのルールが含まれる場合、デバイス分類子がイネーブルになっていることを確認します。

（注） **device classification** コマンドを使用して、show コマンドの出力で正しく表示されるようにデバイスを分類する必要があります。

手順の概要

1. **configure terminal**
2. **wlan***wlan-name*
3. **service-policy type controlsubscriber***policymapname*
4. **profiling local http**（任意）
5. **profiling radius http**（任意）
6. **no shutdown**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan***wlan-name* 例： `スイッチ(config)# wlan wlan1`	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**service-policy type controlsubscriber***policymapname* 例： `スイッチ(config-wlan)# service-policy type control subscriber Aironet-Policy`	WLAN にローカル ポリシーを適用します。

	コマンドまたはアクション	目的
ステップ 4	**profiling local http**（任意） 例： スイッチ(config-wlan)# **profiling local http**	HTTP プロトコルに基づいて、デバイスのプロファイリングのみをイネーブルにします（任意）。
ステップ 5	**profiling radius http**（任意） 例： スイッチ(config-wlan)# **profiling radius http**	ISE でデバイスのプロファイリングをイネーブルにします（任意）。
ステップ 6	**no shutdown** 例： スイッチ(config-wlan)# **no shutdown**	WLAN をシャットダウンしないように指定します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

ローカル ポリシーの設定に関する情報，（776 ページ）
ローカル ポリシーの設定に関する制限，（775 ページ）
ローカル ポリシーの監視，（784 ページ）
例：ローカル ポリシーの設定，（785 ページ）

ローカル ポリシーの設定（*GUI*）

ローカル ポリシーの設定（*GUI*）

ローカル ポリシーを設定するには、次の手順を実行します。

1. サービス テンプレートを作成します。
2. ポリシー マップを作成します。
3. 作成したローカル ポリシーを WLAN に適用します。

サービス テンプレートの作成（*GUI*）

ステップ 1 [Configuration] > [Security] > [Local Policies] > [Service Template] の順に選択して、[Service Template] ページを開きます。

ステップ 2 次のように、新しいテンプレートを作成します。

a) [New] をクリックして、[Service Template] > [New] ページを開きます。
b) [Service Template name] テキスト ボックスに、新しいサービス テンプレートの名前を入力します。

c) [VLAN ID] テキスト ボックスに、ポリシーに関連付ける必要のある VLAN ID を入力します。値の範囲は 1 ～ 4094 です。
d) [Session timeout] テキスト ボックスに、クライアントが再認証を強制されるまでの最大時間を秒単位で入力します。値の範囲は、1 ～ 65535 秒です。
e) [Access control list] ドロップダウン リストから、ポリシーにマップするアクセス コントロール リストを選択します。
f) [Ingress QoS] ドロップダウン リストから、適用する入力 QoS ポリシーを選択します。
g) [Egress QoS] ドロップダウン リストから、適用する出力 QoS ポリシーを選択します。
h) [Apply] をクリックして、設定を保存します

ステップ 3 次のように、サービス テンプレートを編集します。

a) [Service Template] ページで、サービス テンプレートをクリックして、[Service Template] > [Edit] ページを開きます。
b) [VLAN ID] テキスト ボックスに、ポリシーに関連付ける必要のある VLAN ID を入力します。値の範囲は 1 ～ 4094 です。
c) [Session timeout] テキスト ボックスに、クライアントが再認証を強制されるまでの最大時間を秒単位で入力します。値の範囲は、1 ～ 65535 秒です。
d) [Access control list] ドロップダウン リストから、ポリシーにマップするアクセス コントロール リストを選択します。
e) [Ingress QoS] ドロップダウン リストから、適用する入力 QoS ポリシーを選択します。
f) [Egress QoS] ドロップダウン リストから、適用する出力 QoS ポリシーを選択します。
g) [Apply] をクリックして、設定を保存します

ステップ 4 次のように、サービス テンプレートを削除します。

a) [Service Template] ページでサービス テンプレートを選択します。
b) [Remove] をクリックします。
c) [Apply] をクリックして、設定を保存します

ポリシー マップの作成（*GUI*）

ステップ 1 [Configuration] > [Security] > [Local Policies] > [Policy Map] の順に選択して、[Policy Map] ページを開きます。

ステップ 2 新しいポリシー マップを作成するには、次の手順を実行します。

a) [New] をクリックして、[Policy Map] > [New] ページを開きます。
b) [Policy Map name] テキスト ボックスに、新しいポリシー マップの名前を入力します。
c) [Add] をクリックして、[Match Criteria] エリアを開きます。
d) [Device Type] ドロップダウン リストから、デバイス タイプを選択します。デバイス タイプの一致基準は、選択したデバイス タイプに合わせて eq、not-eq、または regex にすることができます。

e) [User Role] ドロップダウン リストから、eq、not-eq、または regex として一致基準を選択し、ユーザのユーザ タイプまたはユーザ グループ（学生や教員など）を入力します。
f) [Service Template] ドロップダウン リストから、ポリシーにマップするサービス テンプレートを選択します。
g) [Add] をクリックします。一致基準が [Match Criteria Lists] に追加されます。
h) [Match Criteria Lists] エリアで、[Add] をクリックして、一致基準をポリシーに追加します。
i) [Apply] をクリックして、設定を保存します

ステップ 3 ポリシー マップを編集するには、次の手順を実行します。

a) [Policy Map] ページで、編集するポリシー マップを選択して、[Edit] をクリックし、[Policy Map] > [Edit] ページを開きます。
b) [Match Criteria] エリアで、[Device Type] ドロップダウン リストから、デバイス タイプを選択します。デバイス タイプの一致基準は、選択したデバイス タイプに合わせて eq、not-eq、または regex にすることができます。
c) [Match Criteria] エリアで、[User Role] ドロップダウン リストから、ユーザ ロールを選択します。eq、not-eq、または regex として一致基準を選択し、ユーザのユーザ タイプまたはユーザ グループを入力します。
d) [Service Template] ドロップダウン リストから、ポリシーにマップするサービス テンプレートを選択します。
e) [OK] をクリックして設定を保存するか、[Cancel] をクリックして設定を破棄します。
f) [Add] をクリックして、デバイス タイプ、ユーザ ロール、およびサービス テンプレートに基づく新しい一致基準をポリシーに追加します。
g) [Match Criteria Lists] エリアで、一致基準を選択して、[Move to] をクリックし、行テキスト ボックスに入力した値に基づいて一致基準を移動します。
h) 一致基準を選択して、[Move up] をクリックし、一致基準をリストの上方に移動します。
i) 一致基準を選択して、[Move down] をクリックし、一致基準をリストの下方に移動します。
j) 一致基準を選択して、[Remove] をクリックし、ポリシー マップのリストから一致基準を削除します。
k) [Apply] をクリックして、設定を保存します

ステップ 4 ポリシー マップを削除するには、次の手順を実行します。

a) [Policy Map] ページで、ポリシー マップを選択します。
b) [Remove] をクリックします。
c) [Apply] をクリックして、設定を保存します

WLAN へのローカル ポリシーの適用（*GUI*）

ステップ 1 [Configuration] > [Wireless] > [WLAN] を選択して、[WLANs] ページを開きます。

ステップ 2 対応する WLAN プロファイルをクリックします。[WLANs > Edit] ページが表示されます。

ステップ 3 [Policy-Mapping] タブをクリックします。

ステップ 4 [Device Classification] チェックボックスをオンにして、デバイス タイプに基づく分類をイネーブルにします。

ステップ 5 [Local Subscriber Policy] ドロップダウン リストから、WLAN に適用する必要があるポリシーを選択します。

ステップ 6 [Local HTTP Profiling] を選択して、HTTP に基づくデバイスのプロファイリングをイネーブルにします（任意）。

ステップ 7 [Radius HTTP Profiling] を選択して、RADIUS に基づくデバイスのプロファイリングをイネーブルにします（任意）。

ステップ 8 [Apply] をクリックして、設定を保存します

IPV4 の入出力方向にフロー モニタを適用する WLAN の設定

手順の概要

1. **configure terminal**
2. **wlan***wlan-id*
3. **ip flow monitor***monitor-name***{input | output}**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan***wlan-id* 例： `スイッチ (config) # wlan 1`	WLAN コンフィギュレーション サブモードを開始します。*wlan-id* には WLAN ID を入力します。指定できる範囲は 1 ～ 64 です。

	コマンドまたはアクション	目的
ステップ 3	**ip flow monitor***monitor-name*{**input** | **output**} 例： スイッチ (config-wlan) # **ip flow monitor flow-monitor-1 input**	入力または出力パケットに対応する WLAN にフロー モニタを関連付けます。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Application Visibility and Control の設定（GUI）

アプリケーションの可視性の設定（GUI）

デフォルトのフロー モニタ（**wireless-avc-basic**）にデフォルトのフロー レコード（**wireless avc basic**）を適用できます。

作成したフロー レコードおよびフローモニタを使用する場合、レコード名およびモニタ名は同じである必要があります。これは、GUI からの AVC を設定する場合のみで、CLI 設定には適用されません。

アップストリームまたはダウンストリーム、あるいはその両方で、作成したフロー モニタを使用できますが、フロー モニタでマッピングする際に同じレコード名を使用していることを確認してください。

ステップ 1 [Configuration] > [Wireless] > [WLAN] の順に選択します。
[WLAN] ページが表示されます。

ステップ 2 対応する WLAN ID をクリックして、[WLAN] > [Edit] ページを開き、[AVC] をクリックします。
[Application Visibility] ページが表示されます。

a) WLAN の AVC をイネーブルにするには、[Application Visibility Enabled] チェックボックスをオンにします。
b) [Upstream Profile] テキスト ボックスに、AVC プロファイルの名前を入力します。
c) [Downstream Profile] テキスト ボックスに、AVC プロファイルの名前を入力します。

AVC をイネーブルにするには、アップストリームとダウンストリームのプロファイルのプロファイル名を入力する必要があります。プロファイル名は、フロー モニタの名前です。デフォルトでは、フロー モニタの名前（**wireless-avc-basic**）が [Upstream Profile] および [Downstream Profile] テキスト ボックスに表示

されます。デフォルトのフロー モニタでは、デフォルトのフロー レコード（**wireless avc basic**）を使用します。デフォルトのフロー レコードがシステムによって生成され、使用可能です。

アップストリームおよびダウンストリームのプロファイルのプロファイル名は変更可能ですが、フローモニタに同じフロー レコードが使用できることを確認してください。

アップストリームおよびダウンストリームのプロファイルは異なるプロファイル名を持つことができますが、フロー モニタにフロー レコードが使用できるようにする必要があります。

ステップ 3 WLAN の AVC を適用するには、[Apply] をクリックします。

ステップ 4 特定の WLAN で AVC を無効にするには、次の手順を実行してください。

- [Configuration] > [Wireless] > [WLAN] を選択して、[WLAN] ページを開きます。
- 対応する WLAN ID をクリックして、[WLAN] > [Edit] ページを開きます。
- [Application Visibility] ページを開くには、[AVC] をクリックします。
- [Application Visibility Enabled] チェックボックスをオフにします。
- 特定の WLAN で AVC を無効にするには、[Apply] をクリックします。

Application Visibility and Control の設定（GUI）

ステップ 1 [Configuration] > [Wireless] を選択します。

ステップ 2 左側のペインをクリックして [QOS-Policy] を選択すると、[QoS] ノードが開きます。
[QOS-Policy] ページが表示されます。

ステップ 3 [Add New] をクリックして、新しい QoS ポリシーを作成します。
[Create QoS Policy] ページが表示されます。

ステップ 4 [Policy Type] ドロップダウン リストから [Client] を選択します。

ステップ 5 [Policy Direction] ドロップダウン リストからポリシーが適用される必要のある方向を選択します。
次のオプションを使用できます。

- 入力
- Egress

ステップ 6 [Policy Name] テキスト ボックスに、ポリシー名を入力します。

ステップ 7 [Description] テキスト ボックスに、ポリシーの説明を入力します。

ステップ 8 クライアント ポリシーに対する AVC のクラス マップを設定するには、[Enable Application Recognition] チェックボックスをオンにします。

（注） 出力クライアント ポリシーで、[Application Recognition] をイネーブルにすると、[Voice]、[Video] および [User Defined] チェックボックスがイネーブルになります。

次のオプションを使用できます。

- [Trust]：このポリシーの分類タイプを指定します。
  - [Protocol]：プロトコルを選択し、パケットのマーキングおよびポリシングを設定できます。
  - [Category]：アプリケーションのカテゴリを選択できます。例えば、ブラウザ。
  - [Subcategory]：アプリケーションのサブカテゴリを選択できます。例えば、ファイル共有。
  - [Application-Group]：アプリケーション グループを選択できます。例えば、ftp グループ。
- [Protocol Choice]：[Available Protocols] リストから、プロトコル、カテゴリ、サブカテゴリ、アプリケーション グループを [Assigned Protocols] として選択し、パケットのマーキングおよびポリシングを適用します。
- [Mark]：各パケットにマーキング ラベルを指定します。次のオプションを使用できます。
  - [DSCP]：特定の QoS を示すラベルを割り当てます。範囲は 0 ～ 63 です。
  - [CoS]：IEEE 802.1Q サービス クラスと一致します。有効な範囲は 0 ～ 7 です。
  - [None]：パケットはマークされません。
- [Police (kbps)]：ポリシング レートを kbps 単位で指定します。このオプションは、[Policy Direction] が出力の場合に使用できます。
- [Drop]：選択したプロトコルに対応する入力パケットをドロップするように指定します。

（注） 各クライアント ポリシーに最大 5 つまで AVC クラスを追加できます。

ステップ 9 [Add] をクリックして、新しい AVC クラス マップを作成します。新しいクラス マップは、表形式で表示されます。

ステップ 10 AVC QoS ポリシーを作成するには、[Apply] をクリックします。

ステップ 11 QoS ポリシーを編集するには、[QOS-Policy] ページの QoS ポリシーのリンクをクリックします。[QOS-Policy] > [Edit] ページが表示されます。[Apply] を選択して、変更を確定します。

ステップ 12 QoS ポリシーから AVC クラス マップを削除するには、AVC のクラス マップ テーブルから対応する AVC クラス マップの行に移動して [Remove] をクリックします。[Apply] をクリックして、変更を確定します。

Application Visibility and Control のモニタリング

Application Visibility and Control のモニタリング（CLI）

このセクションでは、アプリケーションの可視性に関する新しいコマンドについて説明します。

次のコマンドは、スイッチおよびアクセスポイントのアプリケーションの可視性をモニタするために使用できます。

表 *153*：スイッチ のアプリケーションの可視性モニタリング コマンド

コマンド	目的
show avc client*client-mac***top***n***application**[**aggregate**|**upstream**|**downstream**]	指定されたクライアント MAC の上位「N」アプリケーションに関する情報を表示します。
show avc wlan*ssid***top***n***application**[**aggregate**|**upstream**|**downstream**]	指定された SSID の上位「N」アプリケーションに関する情報を表示します。
avc top user[enable | disable]	上位「N」アプリケーションに関する情報を有効または無効にします。
show avc wlan*wlan-id***application***app name***top***N*[**aggregate**|**upstream**|**downstream**]	アプリケーション内のユーザごとのネットワーク利用状況が表示されます。
show wlanid*wlan-id*	AVC が特定の WLAN で有効または無効になっているかどうかについての情報が表示されます。
show flow monitor*flow_monitor_name***cache**	フロー モニタに関する情報を表示します。
show wireless client mac-address*mac-address***service-policy**{**input**|**output**}	ワイヤレスクライアントにマッピングされたポリシーに関する情報が表示されます。

show ip nbar protocol-discovery[**interface***interface-type interface-number*] [**stats**{**byte-count** | **bit-rate** | **packet-count** | **max-bit-rate**}] [**protocol***protocol-name* | **top-n***number*]	NBAR Protocol Discovery 機能によって収集された統計情報を表示します。 • （任意）表示される統計情報を最適化するには、キーワードおよび引数を入力します。キーワードのそれぞれの詳細については、『Cisco IOS Quality of Service Solutions Command Reference』の**show ip nbar protocol-discovery** コマンドを参照してください。 （注） NBARを設定する場合、インターフェイスのプロトコル検出を有効にする必要があります。
show policy-map target **show policy-map** **show policy-map***policy-name* **show policy-map interface***interface-type interface-number*	ポリシー マップに関する情報を表示します。

表 *154*：アプリケーションの可視性統計情報コマンドのクリア

コマンド	目的
clearavcclient*mac***stats**	クライアントごとの統計情報をクリアします。
clearavcwlan*wlan-name***stats**	WLAN ごとの統計情報をクリアします。

アプリケーションの可視性およびコントロールのモニタリング（GUI）

スイッチの [Home] ページにある [AVC on WLAN] の円グラフを使用して、WLAN の AVC 情報を一度に表示できます。円グラフには、最初の WLAN の AVC データ（集約：アプリケーション累積使用率 %）が表示されます。さらに、クライアントに基づく上位 5 つの WLAN が最初に表示されます。対応する円グラフ情報を表示するには、WLANのいずれかをクリックします。AVCが最初の WLAN で無効の場合、[Home] ページには AVC の円グラフが表示されません。

ステップ 1 [Monitor] > [Controller] > [AVC} > [WLANs] の順に選択します。
[WLANs] ページが表示されます。

ステップ 2 対応する WLAN プロファイルをクリックします。

[Application Statistics] ページが表示されます。

[Top Application] ドロップダウン リストから、表示したい上位アプリケーションの数を選択し、[Apply] をクリックします。有効範囲は 5 ～ 30 の 5 の倍数です。

a) [Aggregate]、[Upstream]、[Downstream] タブで、次のフィールドを含むアプリケーションの累積、直近の 90 秒の統計情報、ならびに使用率を確認できます。

- アプリケーション名
- パケット数
- バイト数
- 平均パケット サイズ
- 使用率 (%)

ステップ 3 [Monitor] > [Clients] > [Client Details] > [Clients] の順に選択します。
[Clients] ページが表示されます。

ステップ 4 [Client MAC Address] をクリックして、[AVC Statistics] をクリックします。
[Application Visibility] ページが表示されます。

a) [Aggregate]、[Upstream]、[Downstream] タブで、次のフィールドを含むアプリケーションの累積、直近の 90 秒の統計情報、ならびに使用率を確認できます。

- アプリケーション名
- パケット数
- バイト数
- 平均パケット サイズ
- 使用率(%)

SSID およびクライアント ポリシーの統計情報の監視（GUI）

統計情報は、ワイヤレス ターゲットの入力ポリシー（最大 5 クラス）でのみサポートされます。非常に大規模なポリシーの場合、入力ポリシーの統計情報はスイッチに表示されません。統計情報の頻度は、アクセス ポイントに関連付けられているクライアントの数によって異なります。

統計情報の種類	方式	詳細
SSID ポリシー	[Monitor] > [Controller] > [Statistics] > [QoS] の順に選択します。	[QoS] ページには、SSID ポリシー、無線の種類、および AP の一覧が表示されます。 SSID ポリシー、無線、およびアクセス ポイントをドロップダウン リストから選択し、[Apply] をクリックして、選択された SSID ポリシーの統計情報を表示します。 一致基準、確認済みバイト数、適合レート、超過レートなどの詳細を表示できます。
クライアント ポリシー	[Monitor] > [Clients] > [Client Details] の順に選択します。	[Clients] ページには、クライアントの MAC アドレスの一覧、AP、およびその他の項目が表示されます。 クライアントの MAC アドレスをクリックし、[QoS Statistics] タブをクリックします。 一致基準、確認済みバイト数、適合レート、超過レートなどの詳細を表示できます。

例：Application Visibility and Control

例:アプリケーションの可視性設定

この例では、フロー レコードとフロー モニタの作成方法、フロー レコードをフロー モニタに適用する方法、およびフロー モニタを WLAN に適用する方法を示します。

```
スイッチ# configure terminal
スイッチ(config)# flow record fr_v4
スイッチ(config-flow-record)# match ipv4 protocol
スイッチ(config-flow-record)# match ipv4 source address
スイッチ(config-flow-record)# match ipv4 destination address
スイッチ(config-flow-record)# match transport destination-port
スイッチ(config-flow-record)# match flow direction
スイッチ(config-flow-record)# match application name
スイッチ(config-flow-record)# match wireless ssid
スイッチ(config-flow-record)# collect counter bytes long
```

```
スイッチ(config-flow-record)# collect counter packets long
スイッチ(config-flow-record)# collect wireless ap mac address
スイッチ(config-flow-record)# collect wireless client mac address
スイッチ(config)#end

スイッチ# configure terminal
スイッチ# flow monitor fm_v4
スイッチ(config-flow-monitor)# record fr_v4
スイッチ(config-flow-monitor)# cache timeout active 1800
スイッチ(config)#end

スイッチ(config)#wlan wlan1
スイッチ(config-wlan)#ip flow monitor fm_v4 input
スイッチ(config-wlan)#ip flow mon fm-v4 output
スイッチ(config)#end
```

例：Application Visibility and Control の QoS 設定

次に、match protocol でアプリケーション名、カテゴリ、およびサブカテゴリのフィルタを適用してクラス マップを作成する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# class-map cat-browsing
スイッチ(config-cmap)# match protocol attribute category browsing
スイッチ(config-cmap)#end

スイッチ# configure terminal
スイッチ(config)# class-map cat-fileshare
スイッチ(config-cmap)# match protocol attribute category file-sharing
スイッチ(config-cmap)#end

スイッチ# configure terminal
スイッチ(config)# class-map match-any subcat-terminal
スイッチ(config-cmap)# match protocol attribute sub-category terminal
スイッチ(config-cmap)#end

スイッチ# configure terminal
スイッチ(config)# class-map match-any webex-meeting
スイッチ(config-cmap)# match protocol webex-meeting
スイッチ(config-cmap)#end
```

次に、ポリシー マップを作成し、アップストリーム QoS の既存のクラス マップを定義する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# policy-map test-avc-up
スイッチ(config-pmap)# class cat-browsing
スイッチ(config-pmap-c)# police 150000
スイッチ(config-pmap-c)# set dscp 12
スイッチ(config-pmap-c)#end

スイッチ# configure terminal
スイッチ(config)# policy-map test-avc-up
スイッチ(config-pmap)# class cat-fileshare
スイッチ(config-pmap-c)# police 1000000
```

```
スイッチ(config-pmap-c)# set dscp 20
スイッチ(config-pmap-c)#end
```

```
スイッチ# configure terminal
スイッチ(config)# policy-map test-avc-up
スイッチ(config-pmap)# class subcat-terminal
スイッチ(config-pmap-c)# police 120000
スイッチ(config-pmap-c)# set dscp 15
スイッチ(config-pmap-c)#end
```

```
スイッチ# configure terminal
スイッチ(config)# policy-map test-avc-up
スイッチ(config-pmap)# class webex-meeting
スイッチ(config-pmap-c)# police 50000000
スイッチ(config-pmap-c)# set dscp 21
スイッチ(config-pmap-c)#end
```

次に、ポリシー マップを作成し、ダウンストリーム QoS の既存のクラス マップを定義する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# policy-map test-avc-down
スイッチ(config-pmap)# class cat-browsing
スイッチ(config-pmap-c)# police 200000
スイッチ(config-pmap-c)# set dscp 10
スイッチ(config-pmap-c)#end
```

```
スイッチ# configure terminal
スイッチ(config)# policy-map test-avc-up
スイッチ(config-pmap)# class cat-fileshare
スイッチ(config-pmap-c)# police 300000
スイッチ(config-pmap-c)# set wlan user-priority 2
スイッチ(config-pmap-c)# set dscp 20
スイッチ(config-pmap-c)#end
```

```
スイッチ# configure terminal
スイッチ(config)# policy-map test-avc-up
スイッチ(config-pmap)# class subcat-terminal
スイッチ(config-pmap-c)# police 100000
スイッチ(config-pmap-c)# set dscp 25
スイッチ(config-pmap-c)#end
```

```
スイッチ# configure terminal
スイッチ(config)# policy-map test-avc-up
スイッチ(config-pmap)# class webex-meeting
スイッチ(config-pmap-c)# police 60000000
スイッチ(config-pmap-c)# set dscp 41
スイッチ(config-pmap-c)#end
```

次に、定義された QoS ポリシーを WLAN に適用する例を示します。

```
スイッチ# configure terminal
スイッチ(config)#wlan  alpha
スイッチ(config-wlan)#shut
スイッチ(config-wlan)#end
スイッチ(config-wlan)#service-policy client input test-avc-up
```

```
スイッチ(config-wlan)#service-policy client output test-avc-down
スイッチ(config-wlan)#no shut
スイッチ(config-wlan)#end
```

例 :ローカル プロファイリング ポリシーのための QoS の属性設定

次の例は、ローカル プロファイリング ポリシーのための QoS の属性を設定する方法です :

```
スイッチ(config)# class-map type control subscriber match-all local_policy1_class
スイッチ(config-filter-control-classmap)# match device-type android
スイッチ(config)# service-template local_policy1_template
スイッチ(config-service-template)# vlan 40
スイッチ(config-service-template)# service-policy qos output local_policy1
スイッチ(config)# policy-map type control subscriber local_policy1
スイッチ(config-event-control-policymap)# event identity-update match-all
スイッチ(config-class-control-policymap)# 1 class local_policy1_class do-until-success
スイッチ(config-action-control-policymap)# 1 activate service-template local_policy1_template

スイッチ(config)# wlan open_auth 9
スイッチ(config-wlan)# client vlan VLAN40
スイッチ(config-wlan)# service-policy type control subscriber local_policy1
```

Application Visibility and Control に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
Flexible NetFlow 設定	*Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
Flexible NetFlow コマンド	*Flexible NetFlow Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
QoS の設定	*QoS Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*
QoS コマンド	*QoS Command Reference, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

Application Visibility and Control の機能履歴および情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。
Cisco IOS XE 3E	QoS を使用した AVC 制御が導入されました。

第 90 章

音声パラメータとビデオ パラメータの設定

- 機能情報の確認，2145 ページ
- 音声およびビデオのパラメータの前提条件，2145 ページ
- 音声およびビデオのパラメータの制約事項，2146 ページ
- 音声パラメータとビデオ パラメータの設定について，2146 ページ
- 音声パラメータとビデオ パラメータの設定方法，2151 ページ
- 音声およびビデオ パラメータのモニタリング，2164 ページ
- 音声およびビデオ パラメータの設定例，2166 ページ
- 音声およびビデオ パラメータに関する追加情報，2168 ページ
- 音声およびビデオ パラメータ設定の機能履歴と情報，2169 ページ

機能情報の確認

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

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

音声およびビデオのパラメータの前提条件

音声およびビデオのパラメータを設定する前に、次のポイントをご確認ください。

- スイッチに接続するアクセス ポイントが設定されていることを確認します。
- SSID を設定します。

音声およびビデオのパラメータの制約事項

以下は、音声およびビデオについてのパラメータを設定する際に考慮する必要のある制限事項です。

- SIP CAC は TSPEC ベースのアドミッション コントロールをサポートする Cisco Phone 9971 を使用できます。また、ステータス コード 17 をサポートする電話を使用できます。
- 非 TSPEC SIP 電話に音声優先対応を提供するために、SIP スヌーピングがサポートされています。
- ビデオ CAC 用 TSPEC はサポートされません。
- Cisco 792x IP Phone は、11K が有効な非 WMM デバイスとして許可されると、電話での音声の問題が発生します。

（注） 11K が有効な非 WMM デバイスとして許可されているすべての Cisco 792x IP Phone の音声 WLAN の 11K を無効にします。この問題を解決するには、Cisco Unified Call Manager のファームウェアを 1.4.5 にアップグレードします。詳細については、『Cisco Unified Call Manager Configuration Guide』を参照してください。

音声パラメータとビデオ パラメータの設定について

スイッチには、音声またはビデオ、あるいはその両方の品質に影響を及ぼす次の 3 つのパラメータがあります。

- Call Admission Control（コール アドミッション制御）
- Expedited bandwidth requests
- Unscheduled automatic power save delivery

コール アドミッション制御（CAC）および UAPSD は Cisco Compatible Extensions（CCX）v4 および v5 でサポートされますが、これらのパラメータは、CCX がなくても、（802.1e をサポートする）WMM を実装するデバイスであればサポートされます。Expedited Bandwidth Requests は、CCXv5 でのみサポートされます。

音声の品質に関する問題の監視およびレポートには、Traffic Stream Metrics（TSM）を使用します。

コール アドミッション制御

コール アドミッション制御（CAC）を使用すると、ワイヤレス LAN で輻輳が発生したときに、アクセス ポイントは制御された Quality of Service（QoS）を維持できます。CCXv4 に展開された WMM プロトコルは異なるネットワーク負荷の下で QoS を維持します。

Over-the-Air（OTA）という 2 種類の CAC（静的ベースの CAC および負荷ベースの CAC）が使用可能です。

スイッチは次の QoS ポリシーをサポートします。

- ユーザ定義のポリシー：独自のQoSポリシーを定義できます。こうしたポリシーを既存のメタル ポリシーより細かく制御できます。
- システム定義の重要なメタル ポリシー：下位互換性をサポートします。
  - Platinum：VoIP クライアントに使用されます。
  - Gold：ビデオ クライアント用に使用されます。
  - Silver：ベスト エフォート型トラフィックに使用されます。
  - Bronze：NRT トラフィックに使用されます。

静的ベースの CAC

WMM および TSPEC をサポートする Voice over WLAN アプリケーションでは、コールを開始するために必要になる帯域幅または共有メディア時間を指定できます。帯域幅ベースまたは静的なCACによりアクセス ポイントは、特定のコールに対応できるかどうかを判断できます。アクセス ポイントでは、許容される品質でコールの最大数を維持するために、必要であればコールを拒否します。

WLANのQoS設定により、帯域幅ベースのCACサポートのレベルが決定します。音声アプリケーションで帯域幅ベースの CAC を使用するには、WLAN を Platinum QoS に対して設定する必要があります。帯域幅ベースの CAC により、アクセス ポイントの帯域幅のアベイラビリティは、アクセス ポイント クライアントによる帯域幅の現使用量に基づいて決定され、Voice over WLAN アプリケーションによって要求された帯域幅がアクセスポイントクライアントに追加されます。この合計が設定された帯域幅しきい値を超えると、新しいコールは拒否されます。

（注） WMM が有効化されている CCX v4 クライアントに対して Admission Control（ACM; アドミッション コントロール）を有効にする必要があります。そうしない場合、帯域幅ベースの CAC はこれらの CCXv4 クライアントに対して正しく動作しません。

load-based の CAC

load-based の CAC では、音声アプリケーションまたはビデオ アプリケーションに対し、すべての種類のトラフィック（クライアントからのトラフィックなど）、共通チャネルアクセスポイントの負荷、および共通割り当てチャネルの干渉などによる帯域幅の消費を考慮した測定方法を利用できるようになります。load-based の CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。

負荷ベースCACでは、アクセスポイントではRFチャネルの使用率（消費された帯域幅の割合）、チャネル干渉、およびアクセス ポイントで許可される追加のコールが継続的に測定、更新されま

す。アクセス ポイントは、コールをサポートするのに十分なだけの未使用帯域幅がチャネルにある場合に限り、新規のコールを許可します。このようにすることで、load-based の CAC は、チャネルのオーバーサブスクリプションを防ぎ、WLAN の負荷および干渉のあらゆる状況下で QoS を維持します。

（注） load-based の CAC を無効にすると、アクセス ポイントが帯域幅ベースの CAC を使用するようになります。

IOSd コール アドミッション制御

IOSd コール アドミッション制御（CAC）は、スイッチからアクセス ポイントの間の帯域幅のアベイラビリティを制御します。

スイッチにクラスベースの無条件パケット マーキング機能を設定し、CAC を管理できます。

CAC は、音声およびビデオ トラフィックのみに適用される概念で、データ トラフィックには適用されません。データ トラフィックが増加すると、ネットワーク、キューイング、バッファリングの特定のリンクでオーバーサブスクリプションが発生し、パケット ドロップの決定によって輻輳状態が解消されます。増加したトラフィックは、トラフィックを送信するインターフェイスが使用可能になるまで遅延するか、またはトラフィックがドロップされた場合、プロトコル、またはエンド ユーザがタイムアウトを開始し、情報の再送信を要求するまで遅延状態となります。

遅延とパケット損失の両方の影響を受けやすいリアルタイムのトラフィックの場合、この方法では、このトラフィックのユーザが要求する Quality of Service（QoS）を維持しながらネットワークの輻輳を解決することはできません。音声など、リアルタイムの遅延の影響を受けやすいトラフィックの場合、ネットワークのドロップや遅延が発生し、QoS が損なわれたり、お客様の不満を引き起こすよりも、輻輳状態でのネットワーク アクセスを拒否することをお勧めします。

したがって CAC では、音声コールの確立前に行われ、必要なネットワーク リソースが新しいコールに適した QoS を実現できるかどうかによる、情報に基づく決定と安定性がもたらされます。

既存の CAC アルゴリズムおよび許可 CAC CLI 設定に基づいて、スイッチにより、TSPEC のビデオ再生または SIP スヌーピングを利用できるようになります。**admit cac** CLI は、音声コールのパススルーに必須です。

BSSID のポリサーが音声またはビデオのトラフィック用に設定されている場合、パケットで追加チェックが実行されます。

Expedited Bandwidth Requests

Expedited Bandwidth Request 機能を使用すると、CCXv5 クライアントは WLAN への緊急の WMM Traffic Specifications（TSPEC）要求（e911 コールなど）を示すことができるようになります。コントローラがこの要求を受信すると、コントローラは、処理中の他の TSPEC コールの質を変えることなく、緊急のコールに対応しようとします。

Expedited Bandwidth Requests は、帯域幅ベースの CAC と load-based の CAC の両方に適用できます。Expedited Bandwidth Requests はデフォルトでは無効になっています。この機能が無効の場合、

コントローラはすべての緊急の要求を無視し、TSPEC 要求は通常の TSPEC 要求として処理します。

次の表に、通常の TSPEC 要求と Expedited Bandwidth Requests についての、TSPEC 要求処理の例を示します。

表 *155*：*TSPEC* 要求処理の例

CAC モード	音声コール用に予約されている帯域幅[25]	使用率[26]	通常の TSPEC 要求	Expedited Bandwidth Request を 使用した TSPEC
帯域幅ベースの CAC	75%（デフォルト設定）	75% 未満	許可	許可
		75% ～ 90%（音声コール用に予約された帯域幅が消費される）	却下	許可
		90% 以上	却下	却下
load-based の CAC		75% 未満	許可	許可
		75% ～ 85%（音声コール用に予約された帯域幅が消費される）	却下	許可
		85% 以上	却下	却下

25 帯域幅ベースの CAC では、音声コールの帯域幅利用率はアクセス ポイント無線単位であり、共通チャネル アクセス ポイントは考慮されません。load-based の CAC の場合、音声コールの帯域幅利用率は、チャネル全体に対して測定されます。

26 帯域幅ベースの CAC（消費された音声帯域幅とビデオ帯域幅）または load-based の CAC（チャネル使用率 [Pb]）

（注） TSPEC G711-20 ms および G711-40 ms のコーデック タイプのアドミッション制御がサポートされます。

U-APSD

Unscheduled automatic power save delivery（U-APSD）は、モバイル クライアントのバッテリ寿命を延ばす IEEE 802.11e で定義されている QoS 機能です。バッテリ寿命を延ばすだけでなく、この機能は無線メディアで配送されるトラフィック フローの遅延時間を短縮します。U-APSD は、アクセス ポイントでバッファされる個々のパケットをポーリングするようにクライアントに要求しな

いため、単一のアップリンク トリガー パケットを送信することにより、複数のダウンリンク パケットの送信が許可されます。WMM が有効化されると、U-APSD は自動的に有効化されます。

Traffic Stream Metrics

voice-over-wireless LAN（VoWLAN）展開では、クライアントとアクセス ポイント間のエア インターフェイスでの音声関連のメトリクスの測定には、Traffic Stream Metrics（TSM）が使用されます。TSM ではパケット遅延とパケット損失の両方がレポートされます。これらのレポートを調べることにより、劣悪な音声品質の問題を分離できます。

このメトリクスは、CCX v4 以降のリリースをサポートするアクセス ポイントとクライアント デバイス間のアップリンク（クライアント側）統計とダウンリンク（アクセス ポイント側）統計の集合から成ります。クライアントが CCX v4 または CCXv5 に準拠していない場合、ダウンリンク統計のみが取得されます。クライアントとアクセス ポイントで、これらのメトリクスが測定されます。アクセス ポイントではまた、5 秒おきに測定値が収集されて、90 秒のレポートが作成された後、レポートがコントローラに送信されます。コントローラは、アップリンクの測定値はクライアント単位で保持し、ダウンリンクの測定値はアクセス ポイント単位で保持します。履歴データは 1 時間分を保持します。このデータを格納するには、アップリンク メトリクス用に 32MB、ダウンリンク メトリクス用に 4.8MB の追加のメモリがコントローラに必要です。

無線帯域別ベースで（たとえば、すべての 802.11a ラジオ）、GUI または CLI により TSM を設定できます。コントローラは、リブート後も持続するように、フラッシュ メモリに設定を保存します。アクセス ポイントにより、コントローラからの設定が受信された後、指定された無線帯域で TSM が有効化されます。

この表に、別のコントローラ シリーズでの TSM エントリの上限を示します。

TSM エントリ	**5700**
最大 AP TSM エントリ数	100
最大クライアント TSM エントリ数	250
最大 TSM エントリ数	100*250=25000

（注） 上限に到達すると、追加の TSM エントリを保存し、WCS または NCS に送信することができなくなります。クライアント TSM エントリが満杯で、AP TSM エントリにまだ空きがある場合、AP エントリのみが保存されます（逆もまた同様）。これにより、出力が不完全になります。TSM クリーンアップは、1 時間ごとに行われます。エントリは、対応する AP とクライアントがシステム内に存在しない場合にのみ削除されます。

優先コール番号を使用した音声優先制御の設定について

TSPEC ベースのコールをサポートしない VoWLAN クライアントからの SIP コールをサポートするようにスイッチを設定できます。この機能は、SIP CAC サポートと呼ばれます。帯域幅が、設定された voice プールで使用可能な場合は、SIP コールが通常のフローを使用し、スイッチがこれらのコールに帯域幅を割り当てます。

また、最大 6 つの優先コール番号に順位を設定できます。コールが、設定された優先番号の 1 つに送信された場合、スイッチは設定された最大音声帯域幅を検査しません。スイッチは、音声 CAC に設定されている音声の最大帯域幅を超えてもコールに必要な帯域幅を割り当てます。優先コールは、帯域幅割り当てが無線の帯域幅の 85% を超えた場合、拒否されます。帯域割り当ては、帯域幅プール全体（設定された最大音声プールからだけではない）の 85% になります。帯域割り当ては、ローミング コールの場合であっても同じです。

音声優先制御を設定する前に、次のパラメータを設定しておく必要があります。

- 音声コールがパススルーできるように WLAN QoS を設定します。
- 無線の ACM を有効にします。
- WLAN 上で SIP コール スヌーピングを有効にします。

EDCA パラメータについて

拡張型分散チャネル アクセス（EDCA）パラメータは、音声、ビデオ、およびその他の Quality of Service（QoS）トラフィックのために優先的な無線チャネル アクセスを提供するように設計されています。

音声パラメータとビデオ パラメータの設定方法

音声パラメータの設定（CLI）

はじめる前に

SIP ベースの CAC が設定されていることを確認します。

この手順を開始する前に CAC のクラス マップを作成する必要があります。

手順の概要

1. **show wlan summary**
2. **show wlan***wlan_id*
3. **configure terminal**
4. **policy-map***policy-map name*
5. **class** {*class-name* | **class-default**}
6. **admitcacwmm-tspec**
7. **service-policy***policy-map name*
8. **end**
9. **wlan***wlan_profile_namewlan_IDSSID_network_name***wlan shutdown**
10. **wlan***wlan_profile_namewlan_IDSSID_network_name*
11. **wlan***wlan_name***call-snoop**
12. **wlan***wlan_name***service-policy input***input_policy_name*
13. **wlan***wlan_name***service-policy output***ouput_policy_name*
14. **wlan***wlan_name***service-policy input***ingress_policy_name*
15. **wlan***wlan_name***service-policy output***egress_policy_name*
16. **ap dot11 {5ghz | 24ghz} shutdown**
17. **ap dot11 {5ghz | 24ghz} cac voice sip**
18. **ap dot11 {5ghz | 24ghz} cac voice acm**
19. **ap dot11 {5ghz | 24ghz} cac voice max-bandwidth***bandwidth*
20. **ap dot11 {5ghz | 24ghz} cac voice roam-bandwidth***bandwidth*
21. **no wlan shutdown**
22. **no ap dot11 {5ghz | 24ghz} shutdown**
23. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show wlan summary** 例： スイッチ# **show wlan summary**	スイッチに設定されているすべての WLAN を指定します。
ステップ 2	**show wlan***wlan_id* 例： スイッチ# **show wlan 25**	変更する WLAN を指定します。Voice over WLAN の場合、WLAN が WMM に対して設定されており、QoS レベルが Platinum に設定されていることを確認します。
ステップ 3	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**policy-map***policy-map name* 例： スイッチ(config)# **policy-map test_2000** スイッチ(config-pmap)#	ポリシーマップ コンフィギュレーション モードを開始します。 1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。 WLAN では、これらのコマンドを有効にするには、service-policy を設定する必要があります。
ステップ 5	**class** {*class-name* | **class-default**} 例： スイッチ(config-pmap)# **class test_1000** スイッチ(config-pmap-c)#	ポリシー クラスマップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。 ポリシーを作成または変更するクラスの名前を指定します。 未分類のパケットのシステムデフォルト クラスも作成できます。
ステップ 6	**admitcacwmm-tspec** 例： スイッチ(config-pmap-c)# **admit cac wmm-tspec** スイッチ(config-pmap-c)#	（任意）ポリシーマップのコールアドミッション制御（CAC）の要求を許可します。
ステップ 7	**service-policy***policy-map name* 例： スイッチ(config-pmap-c)# **service-policy test_2000** スイッチ(config-pmap-c)#	QoS サービス ポリシーを設定します。
ステップ 8	**end** 例： スイッチ(config)# **end**	特権EXECモードに戻ります。また、Ctrl+Zキーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 9	**wlan***wlan_profile_namewlan_IDSSID_network_name***wlan shutdown** 例： スイッチ(config)# **wlan wlan1** スイッチ(config-wlan)# **wlan shutdown**	ビデオ パラメータの変更前に、WMM がイネーブルになっているWLANをすべてディセーブルにします。
ステップ 10	**wlan***wlan_profile_namewlan_IDSSID_network_name* 例： スイッチ(config)# **wlan wlan1** スイッチ(config-wlan)# **wlan shutdown**	音声パラメータの変更前に、WMM がイネーブルになっているWLANをすべてディセーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**wlan***wlan_name***call-snoop** 例： スイッチ(config)# **wlan wlan1 call-snoop**	特定の WLAN のコール スヌーピングをイネーブルにします。
ステップ 12	**wlan***wlan_name***service-policy input***input_policy_name* 例： スイッチ(config)# **wlan wlan1** スイッチ(config-wlan)# **service-policy input platinum-up**	特定の WLAN の入力 SSID ポリシーを音声に設定します。
ステップ 13	**wlan***wlan_name***service-policy output***ouput_policy_name* 例： スイッチ(config)# **wlan wlan1** スイッチ(config-wlan)# **service-policy output platinum**	特定の WLAN の出力 SSID ポリシーを音声に設定します。
ステップ 14	**wlan***wlan_name***service-policy input***ingress_policy_name* 例： スイッチ(config)# **wlan wlan1** スイッチ(config-wlan)# **service-policy input policy1**	特定の WLAN の入力 SSID ポリシーをユーザ定義ポリシーとして設定します。
ステップ 15	**wlan***wlan_name***service-policy output***egress_policy_name* 例： スイッチ(config)# **wlan wlan1** スイッチ(config-wlan)# **service-policy output policy2**	特定の WLAN の出力 SSID ポリシーをユーザ定義ポリシーとして設定します。
ステップ 16	**ap dot11 {5ghz | 24ghz} shutdown** 例：	無線ネットワークをディセーブルにします。 スイッチ(config)# **ap dot11 5ghz shutdown**
ステップ 17	**ap dot11 {5ghz | 24ghz} cac voice sip** 例： スイッチ(config)# **ap dot11 5ghz cac voice sip**	802.11a または 802.11b/g ネットワークについて、SIP IOSd CAC をイネーブルまたはディセーブルにします。
ステップ 18	**ap dot11 {5ghz | 24ghz} cac voice acm** 例： スイッチ(config)# **ap dot11 5ghz cac voice acm**	802.11a または 802.11b/g ネットワークについて、帯域幅ベースの音声 CAC をイネーブルまたはディセーブルにします。
ステップ 19	**ap dot11 {5ghz | 24ghz} cac voice max-bandwidth***bandwidth* 例： スイッチ(config)# **ap dot11 5ghz cac voice max-bandwidth 85**	802.11a または 802.11b/g ネットワーク上で音声アプリケーション用にクライアントに割り当てられている最大帯域幅の割合を設定します。 帯域幅の範囲は 5 ～ 85 % で、デフォルト値は 75% です。クライアントが指定値に達すると、

	コマンドまたはアクション	目的
		このネットワーク上での新しいビデオはアクセス ポイントで拒否されます。
ステップ 20	**ap dot11 {5ghz | 24ghz} cac voice roam-bandwidth***bandwidth* 例： スイッチ(config)# **ap dot11 5ghz cac voice roam-bandwidth 10**	割り当てられた最大帯域幅のうち、ローミングする音声クライアント用に予約する割合を設定します。 帯域幅の範囲は0～25%で、デフォルト値は6%です。スイッチは、割り当てられた最大帯域幅のうち、この割合の帯域幅をローミングする音声クライアント用に予約します。
ステップ 21	**no wlan shutdown** 例： スイッチ(config-wlan)# **no wlan shutdown**	WMMがイネーブルになっているすべてのWLANを再度イネーブルにします。
ステップ 22	**no ap dot11 {5ghz | 24ghz} shutdown** 例： スイッチ(config)# **no ap dot11 5ghz shutdown**	無線ネットワークを再度イネーブルにします。
ステップ 23	**end** 例： スイッチ(config)# **end**	特権EXECモードに戻ります。また、Ctrl+Zキーを押しても、グローバル コンフィギュレーション モードを終了できます。

ビデオ パラメータの設定（CLI）

手順の概要

1. **show wlan summary**
2. **show wlan***wlan_id*
3. **configure terminal**
4. **policy-map***policy-map name*
5. **class** {*class-name* | **class-default**}
6. **admitcacwmm-tspec**
7. **service-policy***policy-map name*
8. **end**
9. **wlan***wlan_profile_name*
10. **ap dot11 {5ghz | 24ghz} shutdown**
11. **ap dot11 {5ghz | 24ghz} cac video acm**
12. **ap dot11 {5ghz | 24ghz} cac video load-based**
13. **ap dot11 {5ghz | 24ghz} cac video max-bandwidth***bandwidth*
14. **ap dot11 {5ghz | 24ghz} cac video roam-bandwidth***bandwidth*
15. **no wlan shutdown***wlan_id*
16. **no ap dot11 {5ghz | 24ghz} shutdown**
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show wlan summary** 例： スイッチ# **show wlan summary**	スイッチに設定されているすべてのWLANを指定します。
ステップ 2	**show wlan***wlan_id* 例： スイッチ# **show wlan 25**	変更する WLAN を指定します。
ステップ 3	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**policy-map***policy-map name* 例： スイッチ(config)# **policy-map test_2000** スイッチ(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。 WLAN では、これらのコマンドを有効にするには、service-policy を設定する必要があります。
ステップ 5	**class** {*class-name* | **class-default**} 例： スイッチ(config-pmap)# **class test_1000** スイッチ(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。 ポリシーを作成または変更するクラスの名前を指定します。 未分類のパケットのシステム デフォルト クラスも作成できます。
ステップ 6	**admitcacwmm-tspec** 例： スイッチ(config-pmap-c)# **admit cac wmm-tspec** スイッチ(config-pmap-c)#	（任意）ポリシー マップのコール アドミッション制御（CAC）の要求を許可します。
ステップ 7	**service-policy***policy-map name* 例： スイッチ(config-pmap-c)# **service-policy test_2000** スイッチ(config-pmap-c)#	QoS サービス ポリシーを設定します。
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 9	**wlan***wlan_profile_name* 例： スイッチ(config)# **wlan wlan1** スイッチ(config-wlan)# **wlan shutdown**	ビデオパラメータの変更前に、WMMがイネーブルになっている WLAN をすべてディセーブルにします。
ステップ 10	**ap dot11 {5ghz | 24ghz} shutdown** 例： スイッチ(config)# **ap dot11 5ghz shutdown**	無線ネットワークをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**ap dot11 {5ghz | 24ghz} cac video acm** 例： スイッチ(config)# **ap dot11 5ghz cac video acm**	802.11a または 802.11b/g ネットワークについて、帯域幅ベースのビデオ CAC をイネーブルまたはディセーブルにします。
ステップ 12	**ap dot11 {5ghz | 24ghz} cac video load-based** 例： スイッチ(config)# **ap dot11 5ghz cac video load-based**	負荷ベース CAC の方式を設定します。 このコマンドを入力しない場合は、デフォルトのスタティック CAC が適用されます。
ステップ 13	**ap dot11 {5ghz | 24ghz} cac video max-bandwidth***bandwidth* 例： スイッチ(config)# **ap dot11 5ghz cac video max-bandwidth 20**	802.11a または 802.11b/g ネットワーク上でビデオ アプリケーション用にクライアントに割り当てられている最大帯域幅の割合を設定します。 帯域幅の範囲は 5 ～ 85 % で、デフォルト値は 75% です。デフォルト値は 0 で、帯域幅の要求は制御されません。音声帯域幅とビデオ帯域幅の合計が、85% または設定した最大メディア帯域幅を超えないようにする必要があります。
ステップ 14	**ap dot11 {5ghz | 24ghz} cac video roam-bandwidth***bandwidth* 例： スイッチ(config)# **ap dot11 5ghz cac video roam-bandwidth 9**	割り当てられた最大帯域幅のうち、ローミングするビデオ クライアント用に予約する割合を設定します。 bandwidth の範囲は 0 ～ 25% で、デフォルト値は 0% です。
ステップ 15	**no wlan shutdown***wlan_id* 例： スイッチ(config-wlan)# **no wlan shutdown 25**	WMM がイネーブルになっているすべての WLAN を再度イネーブルにします。
ステップ 16	**no ap dot11 {5ghz | 24ghz} shutdown** 例： スイッチ(config)# **no ap dot11 5ghz shutdown**	無線ネットワークを再度イネーブルにします。
ステップ 17	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

SIP ベースの CAC の設定（CLI）

SIP CAC は、実行できる SIP 呼び出しの総数を制御します。

手順の概要

1. **configure terminal**
2. **wlan***wlan-name*
3. **call-snoop**
4. **service-policy** [**client**] **input***policy-map name*
5. **service-policy** [**client**] **output***policy-map name*
6. **end**
7. **show wlan** {*wlan-id* | *wlan-name*}
8. **configure terminal**
9. **ap dot11 {5ghz | 24ghz} cac {voice | video} acm**
10. **ap dot11 {5ghz | 24ghz} cac voice sip**
11. **end**

手順の詳細

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

ステップ 2	**wlan***wlan-name*
	
	例：
	`スイッチ(config)# wlan qos-wlan`
	`スイッチ(config-wlan)#`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	**call-snoop** 例： `スイッチ(config-wlan)# call-snoop`	特定の WLAN のコール スヌーピング機能をイネーブルにします。
ステップ 4	**service-policy** [**client**] **input***policy-map name* 例： `スイッチ(config-wlan)# service-policy input platinum-up`	WLAN 入力トラフィックにポリシー マップを割り当てます。入力トラフィックの音声に QoS ポリシーを指定していることを確認します。

	コマンドまたはアクション	目的
ステップ 5	**service-policy** [**client**] **output***policy-map name* 例： スイッチ(config-wlan)# **service-policy output platinum**	WLAN出力トラフィックにポリシーマップを割り当てます。出力トラフィックに音声にQoSポリシーを指定していることを確認します。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコンフィギュレーションモードを終了できます。
ステップ 7	**show wlan** {*wlan-id* | *wlan-name*} 例： スイッチ# **show wlan qos-wlan**	WLAN の設定済みの QoS ポリシーを検証します。
ステップ 8	**configure terminal** 例： スイッチ# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 9	**ap dot11 {5ghz | 24ghz} cac {voice | video} acm** 例： スイッチ(config)# **ap dot11 5ghz cac voice acm**	無線の静的 ACM をイネーブルにします。 SIP スヌーピングをイネーブルにする場合、静的 CAC ではなく、負荷ベースの CAC を使用します。
ステップ 10	**ap dot11 {5ghz | 24ghz} cac voice sip** 例： スイッチ(config)# **ap dot11 5ghz cac voice sip**	SIP-Based CAC を設定します。
ステップ 11	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコンフィギュレーションモードを終了できます。

優先コール番号の設定（CLI）

はじめる前に

優先コール番号を設定する前に、次のパラメータを設定する必要があります。

- WLAN QoS を音声に設定します。
- 無線の ACM を有効にします。

- WLAN 上で SIP コール スヌーピングを有効にします。
- SIP ベース CAC をイネーブルにします。

手順の概要

1. **configure terminal**
2. **wlan** *wlan-name* **qos platinum**
3. **ap dot11 {5ghz | 24ghz} cac {voice | video} acm**
4. **wlan** *wlan-name*
5. **wireless sip preferred-call-no** *call_index call_number*
6. **no wireless sip preferred-call-no** *call_index*
7. **end**

手順の詳細

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

ステップ 2	**wlan** *wlan-name* **qos platinum**
	
	例：
	`スイッチ(config)# wlan wlan1`
	`スイッチ(config-wlan)# qos platinum`
		特定の WLAN の QoS を音声に設定します。

ステップ 3	**ap dot11 {5ghz | 24ghz} cac {voice | video} acm** 例： `スイッチ(config)# ap dot11 5ghz cac voice acm`	無線の静的 ACM をイネーブルにします。 SIP スヌーピングをイネーブルにする場合、静的 CAC ではなく、負荷ベースの CAC を使用します。

ステップ 4	**wlan** *wlan-name*
	
	例：
	`スイッチ(config)# wlan wlan1`
	`スイッチ(config-wlan)# call-snoop`
		特定の WLAN のコール スヌーピング機能をイネーブルにします。

ステップ 5	**wireless sip preferred-call-no** *call_index call_number* 例： `スイッチ(config)# wireless sip preferred-call-no 1 555333`	新しい優先コールを追加します。

	コマンドまたはアクション	目的
ステップ 6	**no wireless sip preferred-call-no** *call_index* 例： スイッチ(config)# **no wireless sip preferred-call-no 1**	優先コールを削除します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

EDCA パラメータの設定（CLI）

手順の概要

1. **configure terminal**
2. **ap dot11 {5ghz | 24ghz } shutdown**
3. **ap dot11 {5ghz | 24ghz} edca-parameters {custom-voice | optimized-video-voice | optimized-voice | svp-voice | wmm-default}**
4. **show ap dot11 {5ghz | 24ghz} network**
5. **no ap dot11 {5ghz | 24ghz} shutdown**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 {5ghz	24ghz } shutdown** 例： スイッチ(config)# **ap dot11 5ghz shutdown**	無線ネットワークをディセーブルにします。
ステップ 3	**ap dot11 {5ghz	24ghz} edca-parameters {custom-voice	optimized-video-voice	optimized-voice	svp-voice	wmm-default}**	802.11a または 802.11b/g ネットワークに対する特定の EDCA パラメータをイネーブルにします。 • [custom-voice]：802.11a または 802.11b/g ネットワーク用のカスタム音声パラメータをイネーブルにします。

	コマンドまたはアクション	目的
	例： スイッチ(config)# **ap dot11 5ghz edca-parameters optimized-voice**	• [optimized-video-voice]：802.11a または 802.11b/g ネットワークに対する EDCA 音声およびビデオ最適化パラメータをイネーブルにします。 ネットワーク上で音声サービスとビデオ サービスを両方とも展開する場合に、このオプションを選択します。 • [optimized-voice]：SpectraLink 以外の音声用に最適化された 802.11a または 802.11b/g ネットワークに対するプロファイル パラメータをイネーブルにします。 ネットワーク上で SpectraLink 以外の音声サービスを展開する場合に、このオプションを選択します。 • [svp-voice]：802.11a または 802.11b/g ネットワークに対する SpectraLink 音声優先パラメータをイネーブルにします。 コールの品質を向上させるためにネットワーク上で SpectraLink の電話を展開する場合に、このオプションを選択します。 • [wmm-default]：802.11a または 802.11b/g ネットワークに対する Wi-Fi Multimedia（WMM）デフォルト パラメータをイネーブルにします。 これはデフォルト値です。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。
ステップ 4	**show ap dot11 {5ghz | 24ghz} network** 例： スイッチ(config)# **show ap dot11 5ghz network**	音声用の MAC 最適化の現在のステータスを表示します。
ステップ 5	**no ap dot11 {5ghz | 24ghz} shutdown** 例： スイッチ(config)# **no ap dot11 5ghz shutdown**	無線ネットワークを再度イネーブルにします。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

音声およびビデオ パラメータのモニタリング

このセクションでは、音声およびビデオ パラメータに関する新しいコマンドについて説明します。

次のコマンドは、音声およびビデオ パラメータをモニタするために使用できます。

表 *156*：音声およびビデオ パラメータ コマンド

コマンド	目的
show ap dot11 {5ghz | 24ghz} network	無線ベースの音声統計情報を表示します。
show ap name*ap_name***dot11 24ghz tsm all**	TSM の音質メトリックと、音声用の MAC 最適化の現在のステータスを表示します。
show ap name*apname***cac voice**	特定アクセス ポイントの CAC に関する情報を表示します。
show client detail*client_mac*	特定のクライアントの U-APSD 状態を表示します。
show policy-map interface wireless client	ビデオ クライアント ポリシーの詳細を表示します。
show access-list	スイッチ由来のビデオクライアントダイナミック アクセス リストを表示します。
show wireless client voice diag status	音声診断がイネーブルになっているかディセーブルになっているかについて表示します。イネーブルになっている場合は、ウォッチリスト内のクライアントに関する情報とボイスコール診断の残り時間も表示します。 （注） 音声診断 CLI で機能するためには、次のコマンドを入力する必要があります。 **debug voice-diagnostic mac-addr***client_mac_01client_mac_02*
show wireless client voice diag tspec	音声診断が有効になっているクライアントから送信された TSPEC 情報が表示されます。
show wireless client voice diag qos-map	QoS/DSCP マッピングに関する情報と 4 つのキュー（VO、VI、BE、BK）それぞれのパケット統計が表示されます。各種 DSCP 値も表示されます。

show wireless client voice diag rssi	音声診断が有効になっている場合、クライアントの過去 5 秒間の RSSI 値が表示されます。
show client voice-diag roam-history	過去3回のローミング コールに関する情報が表示されます。出力には、タイムスタンプ、ローミングに関連したアクセス ポイント、およびローミングの理由が含まれ、ローミングに失敗した場合にはその理由も含まれます。
show policy-map interface wireless mac*mac-address*	音声およびビデオデータのパケット統計情報を表示します。
show wireless media-stream client summary	メディア ストリームおよびビデオ クライアント情報のサマリーを表示します。
show controllers d0 | b queue	アクセスポイントにおいて、パケットが通過するキューを表示します。
show platform qos queue stats*interface*	スイッチからのパケットが通過するキューを表示します。

次のコマンドを使用してビデオ パラメータをモニタできます。

表 *157*：ビデオ パラメータ モニタリング コマンド

コマンド	目的
show ap join stats summary*ap_mac*	特定のアクセス ポイントにおける、最後の接続エラーの詳細を表示します。
show ip igmp snooping wireless mgid	TSM の音質メトリックと、音声用の MAC 最適化の現在のステータスを表示します。
show wireless media-stream multicast-direct state	メディア ストリーム マルチキャストダイレクト パラメータを表示します。
show wireless media-stream group summary	メディアストリームとクライアント情報のサマリーを表示します。
show wireless media-stream group detail*group_name*	特定のメディアストリーム グループの詳細を表示します。
show wireless media-stream client summary	メディア ストリーム クライアント セットの詳細を表示します。

show wireless media-stream client detail*group_name*	メディア ストリーム クライアント セットの詳細を表示します。
show ap dot11 {5ghz | 24ghz) media-stream rrc	メディア ストリームの詳細を表示します。
show wireless media-stream message details	メッセージ設定に関する情報を表示します。
show ap name*ap-name***auto-rf dot11 5ghz | i Util**	チャネル使用率の詳細を表示します。
show controllers d0 | b queue	2.4 GHz、5 GHz 帯域ベースのアクセス ポイントにおいて、パケットがどのキューを通過しているかを表示します。
show controllers d1 | b queue	2.4 GHz、5 GHz 帯域ベースのアクセス ポイントにおいて、パケットがどのキューを通過しているかを表示します。
show cont d1 | b Media	帯域 A または B のビデオ メトリックの詳細を表示します。
show capwap mcast mgid all	アクセスポイントに関連付けられたすべてのマルチキャスト グループとそれらに対応するマルチキャスト グループ ID（MGIDs）に関する情報を表示します。
show capwap mcast mgid id*id*	特定の MGID のマルチキャスト グループに属するすべてのビデオ クライアントに関する情報を表示します。

音声およびビデオ パラメータの設定例

例：音声およびビデオの設定

音声およびビデオ用の出力 SSID ポリシーの設定

次に、音声およびビデオ用の出力 SSID ポリシー を作成して設定する例を示します。

```
table-map egress_ssid_tb
 map from 24 to 24
 map from 34 to 34
 map from 46 to 46
 default copy

class-map match-any voice
  match  dscp ef
class-map match-any video
  match  dscp af41
```

```
policy-map ssid-cac
class class-default
    shape average 25000000
   set dscp dscp table egress_ssid_tb
   queue-buffers ratio 0
   service-policy ssid-child-cac

policy-map ssid-child-cac
 class voice
    priority level 1
    police 5000000
     conform-action transmit
     exceed-action drop
    admit cac wmm-tspec
      rate 1000
      wlan-up  6 7
 class video
    priority level 2
    police 10000000
      conform-action transmit
      exceed-action drop
    admit cac wmm-tspec
      rate 3000
      wlan-up  4 5
```

音声およびビデオ用の入力 SSID ポリシーの設定

次に、音声およびビデオ用の入力 SSID ポリシー を作成して設定する例を示します。

```
table-map up_to_dscp
 map from 0 to 0
 map from 1 to 8
 map from 2 to 8
 map from 3 to 0
 map from 4 to 34
 map from 5 to 34
 map from 6 to 46
 map from 7 to 48
 default copy

policy-map ingress_ssid
 class class-default
   set dscp wlan user-priority table up_to_dscp
```

音声およびビデオ用の出力ポート ポリシーの設定

次に、音声およびビデオ用の出力ポート ポリシー を作成して設定する例を示します。

```
policy-map port_child_policy
 class non-client-nrt-class
 bandwidth remaining ratio 10

 class voice
 priority level 1
 police rate 3000000

 class video
 priority level 2
 police rate 4000000
```

WLAN の音声とビデオに関する入出力 SSID ポリシーの適用

次に、WLAN の音声とビデオに関する入出力 SSID ポリシーを適用する例を示します。

```
wlan voice_video 1 voice_video
```

```
service-policy input ingress_ssid
service-policy output ssid-cac
```

音声およびビデオ パラメータに関する追加情報

関連資料

関連項目	マニュアル タイトル
マルチキャストの設定	*Multicast Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
VideoStream 設定	*VideoStream Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

音声およびビデオ パラメータ設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 91 章

RFID タグ追跡の設定

- 機能情報の確認，2171 ページ
- RFID タグ追跡の設定について，2171 ページ
- RFID タグ トラッキングの設定方法，2172 ページ
- RFID タグ トラッキング情報のモニタリング，2173 ページ
- RFID タグ トラッキングに関する追加情報，2173 ページ
- RFID タグ トラッキング設定の機能履歴と情報，2174 ページ

機能情報の確認

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

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

RFID タグ追跡の設定について

スイッチでは、Radio-Frequency Identification（RFID）タグ トラッキングを設定できます。RFID タグは、資産の位置をリアルタイムで追跡するために取り付けられる、小型の無線装置です。タグは、その位置を専用の 802.11 パケットを使用してアドバタイズします。このパケットは、アクセス ポイント、コントローラ、およびロケーション アプライアンスで処理されます。

RFID タグ トラッキングの設定方法

RFID タグ追跡の設定（CLI）

手順の概要

1. **location rfid status**
2. （任意）**no location rfid status**
3. **location rfid timeout** *seconds*
4. **location rfid mobility vendor-name** *name*
5. （任意）**no location rfid mobility** *name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**location rfid status** 例： スイッチ(config)# **location rfid status**	RFID タグ追跡をイネーブルにします。 デフォルトでは、RFID タグ トラッキングはイネーブルになっています。
ステップ 2	（任意）**no location rfid status** 例： スイッチ(config)# **no location rfid status**	RFID タグ トラッキングをディセーブルにします。
ステップ 3	**location rfid timeout** *seconds* 例： スイッチ(config)# **location rfid timeout 1500**	静的なタイムアウト値（60 ～ 7200 秒）を指定します。 静的なタイムアウト値は、タグを失効させずにスイッチが保持する期間です。たとえば、タグが 30 秒ごとにビーコンするよう設定されている場合は、タイムアウト値を 90 秒（ビーコン値の約 3 倍）に設定することをお勧めします。デフォルト値は 1200 秒です。
ステップ 4	**location rfid mobility vendor-name** *name* 例： スイッチ(config)# **location rfid mobility vendor-name Aerosct**	特定のタグについて RFID タグモビリティをイネーブルにします。**location rfid mobility vendor-name** コマンドを入力すると、タグが設定を選択および/またはダウンロードしようとするとき、クライアント モードの DHCP アドレスを取得できません。 （注） これらのコマンドは Pango タグに対してのみ使用できます。したがって、**vendor_name** に指定できる値は、すべて小文字の「pango」のみとなります。

	コマンドまたはアクション	目的
ステップ 5	（任意）**no location rfid mobility** *name* 例： スイッチ(config)# **no location rfid mobility test**	特定のタグについて RFID タグ モビリティをディセーブルにします。**no location rfid mobility** コマンドを入力すると、タグは DHCP アドレスを取得できます。タグがあるサブネットから別のサブネットへ移動すると、タグは、アンカー状態を維持するのではなく、新しいアドレスを取得します。

RFID タグ トラッキング情報のモニタリング

このセクションでは、RFIDタグ トラッキング情報に関する新しいコマンドについて説明します。

次のコマンドはスイッチの RFID タグ トラッキング情報をモニタするために使用できます。

表 *158*：*RFID* タグ トラッキング情報モニタリング コマンド

コマンド	目的
show location rfid config	RFID タグ トラッキングの現在の設定を表示します。
show location rfid detail*mac_address*	特定の RFID タグの詳細情報を表示します。
show location rfid summary	現在スイッチ に接続されているすべての RFID タグのリストを表示します。
show location rfid client	クライアントとしてスイッチに関連付けられている RFID タグのリストを表示します。

RFID タグ トラッキングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

RFID タグ トラッキング設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 92 章

ロケーションの設定

- 機能情報の確認，2175 ページ
- ロケーションの設定に関する情報，2175 ページ
- ロケーションの設定方法，2176 ページ
- ロケーション設定および NMSP 設定のモニタリング，2180 ページ
- 例：ロケーションの設定，2182 ページ
- 例：NMSP の設定，2182 ページ
- ロケーション設定に関する追加情報，2182 ページ
- ロケーション設定の機能履歴と情報，2183 ページ

機能情報の確認

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

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

ロケーションの設定に関する情報

スイッチは、対象クライアントデバイス周辺のアクセス ポイントから受信信号強度表示（RSSI）測定値を収集し、このクライアントのロケーションを特定します。スイッチは、最大16台のアクセス ポイントから、クライアント、RFID タグ、および不正なアクセス ポイントのロケーション レポートを取得できます。

通常のクライアントまたは調整クライアントのパス損失測定（S60）要求を設定すると、ロケーションの精度を向上させることができます。

ロケーションの設定方法

ロケーションの設定（CLI）

手順の概要

1. **configure terminal**
2. **location plm** {**calibrating** [**multiband** | **uniband**] | **client** *burst_interval*
3. **location rssi-half-life** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *seconds*
4. **location expiry** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *timeout*
5. **location algorithm** {**rssi-average** | **simple**}
6. **location admin-tag** *string*
7. **location civic-location identifier** {*identifier* | **host**}
8. **location custom-location identifier** {*identifier* | **host**}
9. **location geo-location identifier** {*identifier* | **host**}
10. **location prefer** {**cdp** | **lldp-med** | **static**} **weight** *priority_value*
11. **location rfid** {**status** | **timeout** | **vendor-name**}
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**location plm** {**calibrating** [**multiband**	**uniband**]	**client** *burst_interval* 例： `スイッチ(config)# location plm client 100`	調整または非調整クライアントのパス損失測定（S60）要求を設定します。 パス損失測定要求で、位置精度が向上します。標準の非調整クライアントに対して、0 ～ 3600 秒の範囲で **burst_interval** パラメータを設定できます。デフォルト値は 60 秒です。 関連付けされた 802.11a または 802.11b/g 無線、関連付けされた 802.11a/b/g 無線の調整クライアントにパス損失測定要求を設定できます。 クライアントからプローブが送信される頻度が低い場合や、少数のチャネルに対してしか送信されない場合は、クライアントのロケーションが更新不可能になるか、精度が低下します。**location plm** コマンドを実行すると、クライアントは強制的に、すべてのチャネルに対してパケットを送信するようになります。CCXv4 以上のクライアントがアソシエートすると、スイッチはそのクライアントにパス損失測

	コマンドまたはアクション	目的
		定要求を送信します。これは、アクセスポイントが使用している帯域とチャネル（2.4 GHz のみのアクセス ポイントの場合は一般にチャネル 1、6、および 11）で無期限に送信するようクライアントに指示するものです。送信する間隔は設定可能です（たとえば 60 秒）。
ステップ 3	**location rssi-half-life** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *seconds* 例： スイッチ(config)# **location rssi-half-life calibrating-client 60**	クライアント、調整クライアント、RFID タグ、不正アクセス ポイントの RSSI 半減期を設定します。 クライアント、調整クライアント、RFID タグ、不正アクセス ポイントの **location rssi-half-life** パラメータ値を入力できます。指定可能な値は、0、1、2、5、10、20、30、60、90、120、180、または 300 秒です。デフォルト値は 0 秒です。 クライアントデバイスの中には、チャネル変更直後は送信電力を下げるものがあるのと、RF は変動しやすいことから、RSSI の値がパケットごとに大きく異なることもあります。**location rssi-half-life** コマンドを実行すると、精度を向上させるために、均一でない状態で受信したデータを平均化するための半減期（ハーフ ライフ）を設定することができます。 （注） **location rssi-half-life** コマンドを使用したり、変更したりしないことをお勧めします。
ステップ 4	**location expiry** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *timeout* 例： スイッチ(config)# **location expiry calibrating-client 50**	クライアント、調整クライアント、RFID タグ、不正アクセス ポイントの RSSI タイムアウト値を設定します。 クライアント、RFID タグ、不正アクセス ポイントの RSSI タイムアウト値を入力できます。範囲は 5 ～ 3600 秒で、デフォルト値は 5 秒です。 調整クライアントには 0 ～ 3600 秒の範囲で RSSI タイムアウト値を入力でき、デフォルト値は 5 秒です。 ロケーションを正確に特定するには、CPU が保持する RSSI が最近のものであることと、その値が大きいことが必要です。**location expiry** コマンドを使用すると、古い RSSI 平均が失効するまでの時間を指定できます。 （注） **location expiry** コマンドを使用したり、変更したりしないことをお勧めします。
ステップ 5	**location algorithm** {**rssi-average** | **simple**} 例： スイッチ(config)# **location algorithm rssi-average**	RSSI および信号対雑音比（SNR）値の平均の算出に使用されるアルゴリズムを設定します。 **location algorithm rssi-average** コマンドを入力することで、より正確な、しかしより CPU オーバーヘッドの高いアルゴリズムを指定できます。または、**location algorithm simple** コマンドを入力することで、

	コマンドまたはアクション	目的
		高速で CPU のオーバーヘッドが低い、しかし精度に欠けるアルゴリズムを指定することもできます。 （注） **location algorithm** コマンドは、使用したり、変更したりしないことをお勧めします。
ステップ 6	**location admin-tag** *string* 例： `スイッチ(config)# location admin-tag`	クライアントデバイスの場所の管理タグまたはサイト情報を設定します。
ステップ 7	**location civic-location identifier** {*identifier* | **host**} 例： `スイッチ(config)# location civic-location identifier host`	都市ロケーション情報を指定します。 文字列またはホストとして都市ロケーション識別子を設定できます。
ステップ 8	**location custom-location identifier** {*identifier* | **host**} 例： `スイッチ(config)# location custom-location identifier host`	カスタム ロケーション情報を指定します。 文字列またはホストとしてカスタムロケーション識別子を設定できます。
ステップ 9	**location geo-location identifier** {*identifier* | **host**} 例： `スイッチ(config)# location geo-location identifier host`	クライアントデバイスの地理的なロケーション情報を指定します。 文字列またはホストとしてロケーション識別子を設定できます。
ステップ 10	**location prefer** {**cdp** | **lldp-med** | **static**} **weight** *priority_value* 例： `スイッチ(config)# location prefer weight cdp 50`	ロケーション情報のソースのプライオリティを設定します。 優先順位のウェイトは、0 から 255 の範囲で入力できます。
ステップ 11	**location rfid** {**status** | **timeout** | **vendor-name**} 例： `スイッチ(config)# location rfid timeout 100`	RFID タグ ステータス、RFID タイムアウト値、RFID タグ ベンダー名などの RFID タグ トラッキング オプションを設定します。 60 ～ 7200 秒の範囲で RFID タイムアウト値を入力できます。
ステップ 12	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

クライアント、RFID タグ、および不正デバイスの NMSP 通知間隔の変更（CLI）

ネットワーク モビリティ サービス プロトコル（NMSP）によって、Mobility Services Engine とコントローラの間の発信/着信トラフィックに関する通信の管理が行われます。高い頻度でのロケーション更新を必要とするアプリケーションがある場合は、クライアント、アクティブな RFID タグ、および不正なアクセス ポイント/クライアントの NMSP 通知間隔を 1 ～ 180 秒の範囲内で変更できます。

（注） コントローラと Mobility Services Engine との通信には、TCP ポート 16113 が使用されます。コントローラと Mobility Services Engine の間にファイアウォールがある場合は、NMSP を機能させるにはこのポートが開いている（ブロックされていない）ことが必要です。

手順の概要

1. **configure terminal**
2. **nmsp notification interval** {**attachment** *seconds* | **location** *seconds* | **rssi** [**clients** *interval* | **rfid** *interval* | **rogues** [**ap** | **client**] *interval*]}
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**nmsp notification interval** {**attachment** *seconds*	**location** *seconds*	**rssi** [**clients** *interval*	**rfid** *interval*	**rogues** [**ap**	**client**] *interval*]} 例： スイッチ(config)# **nmsp notification interval rssi rfid 50**	クライアント、RFID タグ、不正クライアント、不正アクセス ポイントの NMSP 通知間隔を設定します。 1 ～ 180 秒の範囲で RSSI 測定値の NMSP 通知間隔の値を入力できます。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

クライアント、RFIDタグ、および不正デバイスのNMSP通知しきい値の変更（CLI）

手順の概要

1. **configure terminal**
2. **location notify-threshold** {**clients** | **rogues ap** | **tags** } *threshold*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**location notify-threshold** {**clients**	**rogues ap**	**tags** } *threshold* 例： スイッチ(config)# **location notify-threshold clients 5**	クライアント、RFIDタグ、不正なクライアント、不正なアクセス ポイントの NMSP 通知しきい値を設定します。 RSSI しきい値は、0 ～ 10 db の範囲で入力できます。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ロケーション設定および NMSP 設定のモニタリング

ロケーション設定のモニタリング（CLI）

このセクションでは、ロケーション設定に関する新しいコマンドについて説明します。

次のコマンドは、スイッチ のロケーション設定のモニタリングに使用できます。

表 *159*：ロケーション設定モニタリング コマンド

コマンド	目的
show location summary	現在のロケーション設定値を表示します。

show location statistics rfid	ロケーション ベースの RFID 統計情報を表示します。
show location detail*client_mac_addr*	特定のクライアントの RSSI テーブルを表示します。

NMSP 設定のモニタリング（CLI）

このセクションでは、NMSP 設定に関する新しいコマンドについて説明します。

次のコマンドがスイッチ の NMSP 設定のモニタリングに使用できます。

表 *160*：*NMSP* 設定モニタリング コマンド

コマンド	目的
show nmsp attachment suppress interfaces	アタッチメント抑制インターフェイスを表示します。
show nmsp capability	NMSP 機能を表示します。
show nmsp notification interval	NMSP 通知間隔を表示します。
show nmsp statistics connection	接続固有の NMSP カウンタを表示します。
show nmsp statistics summary	一般的な NMSP カウンタを表示します。
show nmsp status	アクティブな NMSP 接続の状態を表示します。
show nmsp subscription detail	スイッチ がサブスクライブされているモビリティ サービスをすべて表示します。
show nmsp subscription detail*ip_addr*	特定の IP アドレスにサブスクライブされたモビリティ サービスについてのみ詳細を表示します。
show nmsp subscription summary	スイッチがサブスクライブされているすべてのモビリティ サービスの詳細を表示します。

例：ロケーションの設定

次に、関連付けされた 802.11a または 802.11b/g 無線の調整クライアント用パス損失測定（S60）要求を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# location plm calibrating uniband
スイッチ(config)# end
スイッチ# show location summary
```

次に、不正アクセス ポイントの RSSI 半減期を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# location rssi-half-life rogue-aps 20
スイッチ(config)# end
スイッチ# show location summary
```

例：NMSP の設定

次に、RFID タグの NMSP 通知間隔を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# nmsp notification interval rssi rfid 50
スイッチ(config)# end
スイッチ# show nmsp notification interval
```

次に、クライアントの NMSP 通知しきい値を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# nmsp notify-threshold 5
スイッチ(config)# end
スイッチ# show nmsp statistics summary
```

ロケーション設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

ロケーション設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 93 章

フロー制御のモニタリング

- 機能情報の確認，2185 ページ
- フロー制御の概要，2185 ページ
- フロー制御のモニタリング，2186 ページ
- 例：フロー制御のモニタリング，2186 ページ
- フロー制御のモニタリングに関する追加情報，2187 ページ
- フロー制御のモニタリングに関する機能履歴および情報，2188 ページ

機能情報の確認

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

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

フロー制御の概要

デフォルトでは、スイッチでフロー制御がイネーブルになっています。

フロー制御は信頼できる IPC に WCM と Cisco IOS のシム レイヤを提供します。WCM のすべてのコンポーネントに専用チャネルがあります。フロー制御を利用する WCM のコンポーネントはわずかです。CLI からのフロー制御の設定はありません。すべてのチャネルのフロー制御をモニタできます。

フロー制御のモニタリング

このセクションでは、フロー制御の新しいコマンドについて説明します。

次のコマンドがスイッチフロー制御のモニタに使用できます。

表 *161*：フロー制御のモニタリング

コマンド	目的
show wireless flow-control *channel -id*	特定のチャネルのフロー制御に関する情報を表示します。
show wireless flow-control *channel-id* **statistics**	特定のチャネルのフロー制御に関する統計情報を表示します。

例：フロー制御のモニタリング

次に、チャネルに関する情報を表示する例を示します。

```
スイッチ# show wireless flow-control 3
スイッチ#

Channel Name         : CAPWAP
FC State             : Disabled
Remote Server State  : Enabled
Pass-thru Mode       : Disabled
EnQ Disabled         : Disabled
Queue Depth          : 2048
Max Retries          : 5
Min Retry Gap (mSec): 3
```

次に、特定チャネルのフロー制御を表示する例を示します。

```
スイッチ# show wireless flow-control 3
スイッチ#

Channel Name                                 : CAPWAP
# of times channel went into FC              : 0
# of times channel came out of FC            : 0
Total msg count received by the FC Infra     : 1
Pass-thru msgs send count                    : 0
Pass-thru msgs fail count                    : 0
# of msgs successfully queued                : 0
# of msgs for which queuing failed           : 0
# of msgs sent thru after queuing            : 0
# of msgs sent w/o queuing                   : 1
# of msgs for which send failed              : 0
# of invalid EAGAINS received                : 0
Highest watermark reached                    : 0
# of times Q hit max capacity                : 0
Avg time channel stays in FC (mSec)          : 0
```

フロー制御のモニタリングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

フロー制御のモニタリングに関する機能履歴および情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。

第 94 章

SDM テンプレートの設定

- 機能情報の確認，2189 ページ
- SDM テンプレートの設定に関する情報，2190 ページ
- SDM テンプレートの設定方法，2192 ページ
- SDM テンプレートのモニタリングおよびメンテナンス，2193 ページ
- SDM テンプレートの設定例，2194 ページ
- Additional References for SDM Templates，2195 ページ
- SDM テンプレートの設定の機能履歴と情報，2196 ページ

機能情報の確認

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

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

SDM テンプレートの設定に関する情報

SDM テンプレート

SDM テンプレートを使用してシステム リソースを設定すると、特定の機能に対するサポートをネットワーク内でのデバイスの使用方法に応じて最適化することができます。一部の機能に最大システム使用率を提供するようにテンプレートを選択できます。

デバイスでサポートされているテンプレートは次のとおりです。

- Advanced：Advancedテンプレートはこのリリースでサポートされているすべてのイメージで利用できます。これは、NetFlow、マルチキャスト グループ、セキュリティ ACE、QoS ACE などの機能のシステム リソースを最大化します。
- VLAN：VLANテンプレートはLAN Baseライセンスでのみ使用できます。VLANテンプレートは、ルーティングを無効にし、最大数のユニキャスト MAC アドレスをサポートします。通常は、レイヤ 2 デバイス用に選択されます。

テンプレートを変更し、システムを再起動したら、**show sdm prefer** 特権 EXEC コマンドを使用して、新しいテンプレート設定を確認できます。**reload** 特権 EXEC コマンドを入力する前に、**show sdm prefer** コマンドを入力すると、**show sdm prefer** コマンドにより、現在使用しているテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。

デフォルトは Advanced テンプレートです。

表 *162*：テンプレートで許容される機能リソースの概算

リソース	**Advanced**	**VLAN**
Number of VLANs	4094	4094
ユニキャスト MAC アドレス	32 K	32 K
オーバーフロー ユニキャスト MAC アドレス	512	512
IGMP グループとマルチキャスト ルート	4 K	4 K
オーバーフローIGMP グループおよびマルチキャスト ルート	512	512
• 直接接続ルート	32 K	32 K
• 間接接続 IP ホスト	8 K	8 K

リソース	Advanced	VLAN
ポリシーベース ルーティング ACE	1024	0
QoS 分類 ACE	3 K	3 K
セキュリティの ACE	1.5 K	1.5 K
NetFlow ACE	1024	1024
入力マイクロフロー ポリサーの ACE:	256 K	0
出力マイクロフロー ポリサーの ACE：	256 K	0
FSPAN ACE	256	256
Tunnels：	256	0
コントロール プレーン エントリ：	512	512
入力 NetFlow フロー：	8 K	8 K
出力 NetFlow フロー：	16 K	16 K
SGT/DGT エントリ：	4 K	4 K
SGT/DGT オーバーフロー エントリ：	0	512

（注） スイッチがワイヤレスモビリティエージェントとして使用される場合、許可されるテンプレートは Advanced テンプレートのみです。

表には、テンプレートが選択されたときに設定される、おおよそのハードウェア上限が示されています。ハードウェア リソースのある部分がいっぱいの場合は、処理のオーバーフローはすべて CPU に送られ、スイッチのパフォーマンスに重大な影響が出ます。

SDM テンプレートとスイッチ スタック

1 つのスイッチ スタックで、すべてのスタック メンバにより、アクティブなスイッチに保存された同一の SDM テンプレートを使用する必要があります。新規スイッチがスタックに追加される

と、アクティブ スイッチに保存された SDM コンフィギュレーションは、個々のスイッチに設定されているテンプレートを上書きします。

show switch 特権 EXEC コマンドを使用すると、スタック メンバが SDM 不一致モードになっているかどうかを確認できます。

SDM テンプレートの設定方法

SDM テンプレートの設定

スイッチ SDM テンプレートの設定

SDM テンプレートの設定

SDM テンプレートを使用して機能動作を最適にサポートするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **sdm prefer** {**advanced**|**vlan**}
4. **end**
5. **reload**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**sdm prefer** {**advanced**|**vlan**} 例： `スイッチ(config)# sdm prefer`	スイッチで使用する SDM テンプレートを指定します。キーワードの意味は次のとおりです。 • **advanced**：NetFlow などの高度な機能をサポートします。

	コマンドまたはアクション	目的
	advanced	• **vlan**：ハードウェアでのルーティングをサポートしないスイッチでの VLAN 設定を最大化します。 （注） **no sdm prefer** コマンドとデフォルト テンプレートはサポートされません。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**reload** 例： スイッチ# **reload**	オペレーティング システムをリロードします。

SDM テンプレートのモニタリングおよびメンテナンス

コマンド	目的
show sdm prefer	使用中の SDM テンプレートを表示します。
reload	スイッチをリロードして、新しく設定した SDM テンプレートをアクティブにします。
no sdm prefer	デフォルトの SDM テンプレートを設定します。

SDM テンプレートの設定例

例：SDM テンプレートの設定

例：SDM テンプレートの表示

次に、詳細なテンプレート情報を表示した出力例を示します。

```
スイッチ# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
  Number of VLANs:                                4094
  Unicast MAC addresses:                          32768
  Overflow Unicast MAC addresses:                 512
  IGMP and Multicast groups:                      8192
  Overflow IGMP and Multicast groups:             512
  Directly connected routes:                      32768
  Indirect routes:                                8192
  Security Access Control Entries:                3072
  QoS Access Control Entries:                     2816
  Policy Based Routing ACEs:                      1024
  Netflow ACEs:                                   1024
  Input Microflow policer ACEs:                   256
  Output Microflow policer ACEs:                  256
  Flow SPAN ACEs:                                 256
  Tunnels:                                        256
  Control Plane Entries:                          512
  Input Netflow flows:                            8192
  Output Netflow flows:                           16384
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.


スイッチ#
```

次に、VLAN テンプレート情報を表示した出力例を示します。

```
スイッチ# show sdm prefer vlan

Showing SDM Template Info

This is the VLAN template for a typical Layer 2 network.
  Number of VLANs:                                4094
  Unicast MAC addresses:                          32768
  Overflow Unicast MAC addresses:                 512
  IGMP and Multicast groups:                      8192
  Overflow IGMP and Multicast groups:             512
  Directly connected routes:                      32768
  Indirect routes:                                8192
  Security Access Control Entries:                3072
  QoS Access Control Entries:                     3072
  Policy Based Routing ACEs:                      0
  Netflow ACEs:                                   1024
  Input Microflow policer ACEs:                   0
  Output Microflow policer ACEs:                  0
  Flow SPAN ACEs:                                 256
  Tunnels:                                        0
  Control Plane Entries:                          512
```

```
  Input Netflow flows:                              16384
  Output Netflow flows:                             8192
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

スイッチ#
```

Additional References for SDM Templates

Related Documents

Related Topic	Document Title
SDM command reference	*System Management Command Reference (Catalyst 3650 Switches)*
VLAN configuration guide	*VLAN Configuration Guide*（*Catalyst 3850 Switches*）

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
本リリースでサポートするすべての MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

SDM テンプレートの設定の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 95 章

システム メッセージ ログの設定

- 機能情報の確認，2197 ページ
- システム メッセージ ログの設定に関する情報，2197 ページ
- システム メッセージ ログの設定方法，2201 ページ
- システム メッセージ ログのモニタリングおよびメンテナンス，2211 ページ
- システム メッセージ ログの設定例，2211 ページ
- システム メッセージ ログに関する追加情報，2212 ページ
- システム メッセージ ログの機能履歴と情報，2213 ページ

機能情報の確認

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

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

システム メッセージ ログの設定に関する情報

システム メッセージ ロギング

スイッチはデフォルトで、システム メッセージおよび **debug** 特権 EXEC コマンドの出力をロギング プロセスに送信します。スタック メンバーはシステム メッセージをトリガーできます。シス

テム メッセージを生成するスタック メンバは、ホスト名を hostname-n の形式で付加し（n はスイッチ）、出力をアクティブ スイッチのロギング プロセスにリダイレクトします。アクティブ スイッチはスタック メンバですが、そのホスト名はシステム メッセージの末尾に追加されません。ロギング プロセスはログ メッセージを各宛先（設定に応じて、ログ バッファ、端末回線、UNIX Syslog サーバなど）に配信する処理を制御します。ロギング プロセスは、コンソールにもメッセージを送信します。

ロギング プロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。メッセージがアクティブなコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。ログ メッセージにタイム スタンプを設定したり、Syslog 送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。表示されるメッセージについては、このリリースに対応するシステム メッセージ ガイドを参照してください。

ロギングされたシステム メッセージにアクセスするには、スイッチのコマンドライン インターフェイス（CLI）を使用するか、または適切に設定された Syslog サーバにこれらのシステム メッセージを保存します。スイッチ ソフトウェアは、Syslog メッセージをスタンドアロン スイッチ上の内部バッファに保存します。スイッチ スタックの場合は、アクティブ スイッチ上に保存します。スタンドアロン スイッチまたはスタック マスターに障害が発生すると、ログをフラッシュ メモリに保存していなかった場合、ログは失われます。

システム メッセージをリモートで監視するには、Syslog サーバ上でログを表示するか、あるいは Telnet、コンソール ポート、またはイーサネット管理ポート経由でスイッチにアクセスします。スイッチ スタックでは、すべてのスタック メンバ コンソールにより、同じコンソール出力が用意されます。

（注） Syslog フォーマットは 4.3 Berkeley Standard Distribution（BSD）UNIX と互換性があります。

システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字とパーセント記号（%）、およびその前に配置されるオプションのシーケンス番号やタイム スタンプ情報（設定されている場合）で構成されています。スイッチに応じて、メッセージは次のいずれかの形式で表示されます。

- *seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)*
- *seq no:timestamp: %facility-severity-MNEMONIC:description*

パーセント記号の前にあるメッセージの部分は、次のグローバル コンフィギュレーション コマンドの設定によって異なります。

- **service sequence-numbers**
- **service timestamps log datetime**
- **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]

- **service timestamps log uptime**

表 *163* : システム ログ メッセージの要素

要素	説明
seq no:	**service sequence-numbers** グローバル コンフィギュレーション コマンドが設定されている場合だけ、ログ メッセージにシーケンス番号をスタンプします。
timestamp のフォーマット： *mm/dd hh:mm:ss* または *hh:mm:ss*（短時間） または *d h*（長時間）	メッセージまたはイベントの日時です。**service timestamps log** [**datetime** | **log**] グローバル コンフィギュレーション コマンドが設定されている場合だけ、この情報が表示されます。
facility	メッセージが参照する機能（SNMP、SYSなど）です。
severity	メッセージの重大度を示す 0 ～ 7 の 1 桁のコードです。
MNEMONIC	メッセージを一意に示すテキスト ストリングです。
description	レポートされているイベントの詳細を示すテキスト ストリングです。
hostname-n	スタック メンバーのホスト名およびスタック内のスイッチ番号。アクティブ スイッチはスタック メンバですが、そのホスト名はシステム メッセージの末尾に追加されません。

デフォルトのシステム メッセージ ロギングの設定

表 *164* : デフォルトのシステム メッセージ ロギングの設定

機能	デフォルト設定
コンソールへのシステム メッセージ ロギング	イネーブル

機能	デフォルト設定
コンソールの重大度	デバッグ
ログ ファイル設定	ファイル名の指定なし
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1 メッセージ
タイム スタンプ	ディセーブル
同期ロギング	ディセーブル
ロギング サーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
サーバ機能	local7
サーバの重大度	Informational

syslog メッセージの制限

snmp-server enable trap グローバル コンフィギュレーション コマンドを使用して、SNMP ネットワーク管理ステーション（NMS）に送信されるようにSyslogメッセージ トラップがイネーブルに設定されている場合は、スイッチの履歴テーブルに送信および格納されるメッセージの重大度を変更できます。また、履歴テーブルに格納されるメッセージの数を変更することもできます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。デフォルトでは、Syslog トラップが有効でない場合も、レベルが **warning** であるメッセージや数値的に下位レベルのメッセージの 1 つが履歴テーブルに格納されます。

履歴テーブルがいっぱいの場合（**logging history size** グローバル コンフィギュレーション コマンドで指定した最大メッセージエントリ数が格納されている場合）は、新しいメッセージエントリを格納できるように、最も古いエントリがテーブルから削除されます。

履歴テーブルは、level キーワードおよび重大度を示します。SNMP を使用している場合は、重大度の値が 1 だけ増えます。たとえば、*emergencies* は 0 ではなく 1 に、*critical* は 2 ではなく 3 になります。

システム メッセージ ログの設定方法

メッセージ表示宛先デバイスの設定

メッセージ ロギングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **logging buffered** [*size*]
3. **logging***host*
4. **logging file flash:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]
5. **end**
6. **terminalmonitor**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging buffered** [*size*] 例： `スイッチ(config)# logging buffered 8192`	スタンドアロン スイッチ上か、または、スイッチ スタックの場合はアクティブ スイッチ上で、ログ メッセージを内部バッファに保存します。指定できる範囲は 4096 ～ 2147483647 バイトです。デフォルトのバッファ サイズは 4096 バイトです。 スタンドアロン スイッチまたはアクティブ スイッチに障害が発生すると、ログ ファイルをフラッシュ メモリに保存していなかった場合、ログ ファイルは失われます。ステップ 4 を参照してください。 （注） バッファ サイズを大きすぎる値に設定しないでください。他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサ メモリを表示するには、**show memory** 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値であるため、バッファ サイズをこの値に設定しないでください。

	コマンドまたはアクション	目的
ステップ 3	**logging***host* 例： スイッチ(config)# **logging 125.1.1.100**	UNIX Syslog サーバ ホストにメッセージを保存します。 *host* には、syslog サーバとして使用するホストの名前または IP アドレスを指定します。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。
ステップ 4	**logging file flash:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*] 例： スイッチ(config)# **logging file flash:log_msg.txt 40960 4096 3**	スタンドアロン スイッチ上か、または、スイッチ スタックの場合はアクティブ スイッチ上で、フラッシュ メモリにあるファイルにログ メッセージを保存します。 • *filename*：ログ メッセージのファイル名を入力します。 • （任意）**max-file-size**：ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ～ 2147483647 です。デフォルトは 4096 バイトです。 • （任意）*min-file-size*：ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ～ 2147483647 です。デフォルトは 2048 バイトです。 • （任意）*severity-level-number* | *type*：ロギングの重大度またはロギング タイプを指定します。重大度に指定できる範囲は 0 ～ 7 です。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**terminalmonitor** 例： スイッチ# **terminal monitor**	現在のセッション間、非コンソール端末にメッセージを保存します。 端末パラメータ コンフィギュレーション コマンドはローカルに設定され、セッションの終了後は無効になります。デバッグ メッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。

ログ メッセージの同期化

特定のコンソール ポート回線または仮想端末回線に対して、非送信請求メッセージおよび **debug** 特権 EXEC コマンドの出力を送信請求デバイスの出力およびプロンプトと同期させることができます。重大度に応じて非同期に出力されるメッセージのタイプを特定できます。また、端末の非同期メッセージが削除されるまで保存しておくバッファの最大数を設定することもできます。

非送信請求メッセージおよび **debug** コマンド出力の同期ロギングがイネーブルの場合、送信請求デバイス出力がコンソールに表示または印刷された後に、非送信請求デバイスからの出力が表示または印刷されます。非送信請求メッセージおよび **debug** コマンドの出力は、ユーザ入力用プロンプトが返された後に、コンソールに表示されます。したがって、非送信請求メッセージおよび **debug** コマンドの出力は、送信請求デバイス出力およびプロンプトに割り込まれることはありません。非送信請求メッセージが表示された後に、コンソールはユーザ プロンプトを再表示します。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **line** [**console** | **vty**] *line-number* [*ending-line-number*]
3. **logging synchronous** [**level** [*severity-level* | **all**] | **limit***number-of-buffers*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console**	**vty**] *line-number* [*ending-line-number*] 例： スイッチ(config)# **line console**	メッセージの同期ロギングに設定する回線を指定します。 • **console**：スイッチ コンソール ポートまたはイーサネット管理ポートでの設定を指定します。 • **line vty***line-number*：どの vty 行の同期ロギングをイネーブルにするかを指定します。Telnet セッションを介して行われる設定には、vty 接続を使用します。回線番号に指定できる範囲は 0 ～ 15 です。 16 個の vty 回線の設定をすべて一度に変更するには、次のように入力します。 line vty 0 15 また、現在の接続に使用されている 1 つの vty 回線の設定を変更することもできます。たとえば、vty 回線 2 の設定を変更するには、次のように入力します。 line vty 2 このコマンドを入力すると、ライン コンフィギュレーション モードになります。

	コマンドまたはアクション	目的
ステップ 3	**logging synchronous** [**level** [*severity-level* | **all**] | **limit***number-of-buffers*] 例： `スイッチ(config)# logging synchronous level 3 limit 1000`	メッセージの同期ロギングをイネーブルにします。 • （任意）**level***severity-level*：メッセージの重大度を指定します。重大度がこの値以上であるメッセージは、非同期に出力されます。値が小さいほど重大度は大きく、値が大きいほど重大度は小さくなります。デフォルトは 2 です。 • （任意）**level all**：重大度に関係なく、すべてのメッセージが非同期に出力されます。 • （任意）**limit***number-of-buffers*：キューイングされる端末のバッファ数を指定します。これを超える新しいメッセージは廃棄されます。指定できる範囲は 0 ～ 2147483647 です。デフォルトは 20 です。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

メッセージ ロギングのディセーブル化

メッセージ ロギングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージ ロギングをイネーブルにする必要があります。メッセージ ロギングがイネーブルの場合、ログ メッセージはロギング プロセスに送信されます。ロギング プロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

ロギング プロセスをディセーブルにすると、メッセージがコンソールに書き込まれるまでプロセスは処理続行を待機する必要があるため、スイッチの処理速度が低下することがあります。ロギング プロセスがディセーブルの場合、メッセージは生成後すぐに（通常はコマンド出力に割り込む形で）コンソールに表示されます。

logging synchronous グローバル コンフィギュレーション コマンドも、コンソールへのメッセージ表示に影響します。このコマンドをイネーブルにすると、Return を押さなければメッセージが表示されません。

メッセージ ロギングをディセーブルにした後に再びイネーブルにするには、**logging on** グローバル コンフィギュレーション コマンドを使用します。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **no logging console**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no logging console** 例： `スイッチ(config)# no logging console`	メッセージ ロギングをディセーブルにします。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化

デフォルトでは、ログ メッセージにはタイム スタンプが適用されません。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを使用します。
   - **servicetimestampsloguptime**
   - **service timestamps log datetime**[**msec** | **localtime** | **show-timezone**]
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	次のいずれかのコマンドを使用します。 • **servicetimestampsloguptime** • **service timestamps log datetime**[**msec** | **localtime** | **show-timezone**] 例： スイッチ(config)# **service timestamps log uptime** または スイッチ(config)# **service timestamps log datetime**	ログのタイムスタンプをイネーブルにします。 • **log uptime**：ログ メッセージのタイムスタンプをイネーブルにして、システムの再起動以降の経過時間を表示します。 • **log datetime**：ログ メッセージのタイムスタンプをイネーブルにします。選択したオプションに応じて、ローカル タイム ゾーンを基準とした日付、時間（ミリ秒）、タイム ゾーン名をタイム スタンプとして表示できます。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

タイムスタンプが同じログ メッセージが複数ある場合、これらのメッセージを表示するには、シーケンス番号を使用してメッセージを表示できます。デフォルトでは、ログ メッセージにシーケンス番号は表示されません。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **service sequence-numbers**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service sequence-numbers** 例： スイッチ(config)# **service sequence-numbers**	シーケンス番号をイネーブルにします。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

メッセージ重大度の定義

メッセージの重大度を指定して、選択したデバイスに表示されるメッセージを制限します。このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **logging console***level*
3. **logging monitor***level*
4. **logging trap***level*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging console***level* 例： スイッチ(config)# **logging console 3**	コンソールに保存するメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 3	**logging monitor***level* 例： スイッチ(config)# **logging monitor 3**	端末回線に出力するメッセージを制限します。 デフォルトで、端末はデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 4	**logging trap***level* 例： スイッチ(config)# **logging trap 3**	Syslog サーバに保存するメッセージを制限します。 デフォルトで、Syslogサーバは通知メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

履歴テーブルおよび SNMP に送信される syslog メッセージの制限

このタスクでは、履歴テーブルおよび SNMP に送信される syslog メッセージを制限する方法について説明します。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **logging history***level*
3. **logging history size***number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging history***level* 例： スイッチ(config)# **logging history 3**	履歴ファイルに保存され、SNMP サーバに送信される syslog メッセージのデフォルト レベルを変更します。 デフォルトでは、**warnings**、**errors**、**critical**、**alerts**、および **emergencies** のメッセージが送信されます。
ステップ 3	**logging history size***number* 例： スイッチ(config)# **logging history size 200**	履歴テーブルに保存できる Syslog メッセージの数を指定します。 デフォルトでは 1 つのメッセージが格納されます。指定できる範囲は 0 ～ 500 です。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

UNIX Syslog デーモンへのメッセージのロギング

このタスクはオプションです。

（注） 最新バージョンのUNIX Syslogデーモンの中には、デフォルトでネットワークからのSyslogパケットを受け入れないものがあります。このようなシステムの場合に、Syslogメッセージのリモート ロギングをイネーブルにするには、Syslog コマンド ラインに追加または削除する必要があるオプションを、UNIX の **man syslogd** コマンドを使用して判別します。

はじめる前に

- root としてログインします。
- システム ログ メッセージを UNIX Syslog サーバに送信する前に、UNIX サーバ上で Syslog デーモンを設定する必要があります。

手順の概要

1. /etc/syslog.conf ファイルに次の行を追加します。
2. UNIX シェル プロンプトに次のコマンドを入力します。
3. Syslog デーモンに新しい設定を認識させます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	/etc/syslog.conf ファイルに次の行を追加します。 例： `local7.debug /usr/adm/logs/cisco.log`	• **local7**：ロギング機能を指定します。 • **debug**：syslog レベルを指定します。このファイルは、syslogデーモンに書き込み権限がある既存ファイルである必要があります。

ステップ 2	UNIX シェル プロンプトに次のコマンドを入力します。
	
	例：
	
	`$ touch /var/log/cisco.log`
	`$ chmod 666 /var/log/cisco.log`
		ログ ファイルを作成します。syslog デーモンは、このレベルまたはこのファイルのより高い重大度レベルでメッセージを送信します。

ステップ 3	Syslogデーモンに新しい設定を認識させます。 例： `$ kill -HUP `cat /etc/syslog.pid``	詳細については、ご使用の UNIX システムの **man syslog.conf** および **man syslogd** コマンドを参照してください。

システム メッセージ ログのモニタリングおよびメンテナンス

コンフィギュレーション アーカイブ ログのモニタリング

コマンド	目的
show archive log config {**all** | **number** [*end-number*] | **user***username* [**session***number*] *number* [*end-number*] | **statistics**} [**provisioning**]	コンフィギュレーション ログ全体、または指定されたパラメータのログを表示します。

システム メッセージ ログの設定例

例：システム メッセージのスタック構成

次の例に、アクティブ スイッチおよびスタック メンバの部分的なスイッチ システム メッセージを示します（ホスト名は *Switch-2*）。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/2, changed state to up (Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
(Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/1, changed
state to down 2 (Switch-2)
```

例：スイッチ システム メッセージ

次に、スイッチ上のスイッチ システム メッセージの一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
 to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

```
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

システム メッセージ ログに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference (Catalyst 3650 Switches)*
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S（Catalyst 3650 Switches）*
プラットフォームに依存しない設定情報	*IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S（Catalyst 3650 Switches）* *Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S（Catalyst 3650 Switches）*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

システム メッセージ ログの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 96 章

オンライン診断の設定

- 機能情報の確認，2215 ページ
- オンライン診断の設定に関する情報，2215 ページ
- オンライン診断の設定方法，2216 ページ
- オンライン診断のモニタリングおよびメンテナンス，2222 ページ
- オンライン診断テストの設定例，2223 ページ
- オンライン診断に関する追加情報，2225 ページ
- オンライン診断設定の機能履歴と情報，2226 ページ

機能情報の確認

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

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

オンライン診断の設定に関する情報

オンライン診断

オンライン診断では、スイッチが稼働中のネットワークに接続している間に、スイッチのハードウェア機能をテストし、確認できます。

オンライン診断には、異なるハードウェア コンポーネントをチェックするパケット交換テストが含まれ、データ パスおよび制御信号が確認されます。

オンライン診断では、次の領域の問題が検出されます。

- ハードウェア コンポーネント
- インターフェイス（イーサネット ポートなど）
- はんだ接合

オンライン診断は、オンデマンド診断、スケジュール診断、ヘルスモニタリング診断に分類できます。オンデマンド診断は、CLI から実行されます。スケジュールされた診断は、動作中のネットワークにスイッチが接続されているときに、ユーザが指定した間隔または指定した時刻に実行されます。ヘルスモニタリングは、バックグラウンドでユーザが指定した間隔で実行されます。デフォルトでは、30 秒ごとにヘルス モニタリング テストが実行されます。

オンライン診断を設定したあと、手動で診断テストを開始したり、テスト結果を表示したりできます。また、スイッチまたはスイッチ スタックに設定されているテストの種類、およびすでに実行された診断テスト名を確認できます。

オンライン診断の設定方法

オンライン診断テストの開始

スイッチで実行する診断テストを設定しスイッチ、**diagnostic start** 特権 EXEC コマンドを使用して診断テストを開始します。

テストを開始したら、テスト プロセスの停止はできません。

手動でオンライン診断テストを開始するには、次の特権 EXEC コマンドを使用します。

手順の概要

1. **diagnostic start switch***number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**diagnostic start switch***number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**} 例：	診断テストを開始します。 **switch***number* キーワードは、スタック構成スイッチのみでサポートされます。指定できる範囲は 1 ～ 4 です。 次のいずれかのオプションを使用してテストを指定できます。 • *name*：テストの名前を入力します。

	コマンドまたはアクション	目的
	`スイッチ# diagnostic start switch 2 test basic`	• *test-id*：テストの ID 番号を入力します。 • *test-id-range*：カンマとハイフンで区切ってテスト ID の範囲を整数で入力します。 • **all**：すべてのテストを開始します。 • **basic**：基本テスト スイートを開始します。 • **complete**：完全なテスト スイートを開始します。 • **minimal**：最小限のブートアップ テスト スイートを開始します。 • **non-disruptive**：ノンディスラプティブ テスト スイートを開始します。 • **per-port**：ポート単位のテスト スイートを開始します。

オンライン診断の設定

診断モニタリングをイネーブルにする前に、障害しきい値およびテストの間隔を設定する必要があります。

オンライン診断のスケジューリング

特定のスイッチについて指定した時間、または日、週、月単位でオンライン診断をスケジューリングできます。スケジューリングを削除するには、コマンドの **no** 形式を入力します。

手順の概要

1. **configureterminal**
2. **diagnostic schedule switch***number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**} {**daily** | **on***mm dd yyyy hh:mm* | **port***inter-port-numberport-number-list* | **weekly***day-of-week hh:mm*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**diagnostic schedule switch***number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**} {**daily** | **on***mm dd yyyy hh:mm* | **port***inter-port-numberport-number-list* | **weekly***day-of-week hh:mm*} 例： スイッチ(config)# **diagnostic schedule switch 3 test 1-5 on July 3 2013 23:10**	特定日時のオンデマンド診断テストをスケジュールします。 **switch***number* キーワードは、スタック構成スイッチだけでサポートされます。指定できる範囲は 1 ～ 4 です。 スケジュールするテストを指定する場合は、次のオプションを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべてのテスト ID です。 • **basic**：基本的なオンデマンドの診断テストを開始します。 • **complete**：完全なテスト スイートを開始します。 • **minimal**：最小限のブートアップ テスト スイートを開始します。 • **non-disruptive**：ノンディスラプティブ テスト スイートを開始します。 • **per-port**：ポート単位のテスト スイートを開始します。 テストは次のようにスケジュールできます。 • 毎日：**daily***hh:mm* パラメータを使用します。 • 特定日時：**on***mm dd yyyy hh:mm* パラメータを使用します。 • 毎週：**weekly***day-of-week hh:mm* パラメータを使用します。

ヘルス モニタリング診断の設定

スイッチが稼働中のネットワークに接続されている間に、スイッチに対しヘルス モニタリング診断テストを設定できます。ヘルスモニタリングテストの実行間隔を設定したり、テスト失敗時のスイッチのsyslogメッセージ生成をイネーブルにしたり、特定のテストをイネーブルにできます。テストをディセーブルにするには、コマンドの **no** 形式を入力します。

デフォルトでは、ヘルスモニタリングはディセーブルですが、スイッチはテストの失敗時にSyslogメッセージを生成します。

ヘルス モニタリング診断テストを設定し、イネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **diagnostic monitor interval switch***number***test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day*
4. **diagnostic monitor syslog**
5. **diagnostic monitor threshold switch***number***test** {*name* | *test-id* | *test-id-range* | **all**} **failure count***count*
6. **diagnostic monitor switch***number***test** {*name* | *test-id* | *test-id-range* | **all**}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**diagnostic monitor interval switch***number***test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day*	指定のテストに対し、ヘルス モニタリングの実行間隔を設定します。 **switch***number* キーワードは、スタック構成スイッチだけでサポートされます。範囲は 1 ～ 9 です。

	コマンドまたはアクション	目的
	例： スイッチ(config)# **diagnostic monitor interval switch 2 test 1 12:30:00 750 5**	テストを指定する場合は、次のいずれかのパラメータを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべての診断テスト。 間隔を指定する場合は、次のパラメータを設定します。 • *hh:mm:ss*：モニタリング間隔（時間、分、秒）。指定できる範囲は *hh* が 0 ~ 24、*mm* および *ss* が 0 ~ 60 です。 • *milliseconds*：モニタリング間隔（ミリ秒（ms））。指定できる範囲は 0 ～ 999 です。 • *day*：モニタリング間隔（日数）。指定できる範囲は 0 ～ 20 です。
ステップ 4	**diagnostic monitor syslog** 例： スイッチ(config)# **diagnostic monitor syslog**	（任意）ヘルス モニタリング テストの失敗時にスイッチが Syslog メッセージを生成するように設定します。
ステップ 5	**diagnostic monitor threshold switch***number***test** {*name* | *test-id* | *test-id-range* | **all**} **failure count***count* 例： スイッチ(config)# **diagnostic monitor threshold switch 2 test 1 failure count 20**	（任意）ヘルスモニタリングテストの失敗しきい値を設定します。 **switch***number* キーワードは、スタック構成スイッチだけでサポートされます。指定できる範囲は 1 ～ 9 です。 テストを指定する場合は、次のいずれかのパラメータを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべての診断テスト。

	コマンドまたはアクション	目的
		失敗しきい値 *count* に指定できる範囲は 0 ～ 99 です。
ステップ 6	**diagnostic monitor switch***number***test** {*name* | *test-id* | *test-id-range* | **all**} 例： スイッチ(config)# **diagnostic monitor switch 2 test 1**	指定のヘルス モニタリング テストをイネーブルにします。 **switch***number* キーワードは、スタック構成スイッチだけでサポートされます。指定できる範囲は 1 ～ 9 です。 テストを指定する場合は、次のいずれかのパラメータを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべての診断テスト。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

間隔をデフォルトの値またはゼロに変更するには、**no diagnostic monitor interval test***test-id* | *test-id-range* } グローバル コンフィギュレーション コマンドを使用します。ヘルスモニタリング テストに失敗した場合、**no diagnostic monitor syslog** コマンドを使用して、Syslog メッセージの生

成をディセーブルに設定します。失敗しきい値を削除するには、**diagnostic monitor threshold test***test-id* | *test-id-range* }**failure count** コマンドを使用します。

オンライン診断のモニタリングおよびメンテナンス

オンライン診断テストとテスト結果の表示

スイッチまたはスイッチ スタックに設定されているオンライン診断テストを表示し、この表に示す **show** 特権 EXEC コマンドを使用してテスト結果を確認することができます。

表 *165*：診断テストの設定および結果用のコマンド

コマンド	目的
show diagnostic content switch [*number* | **all**]	スイッチに対して設定されたオンライン診断を表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic status	現在実行中の診断テストを表示します。
show diagnostic result switch [*number* | **all**] [**detail** | **test** {*name* | *test-id* | *test-id-range* | **all**} [**detail**]]	オンライン診断テストの結果を表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic switch [*number* | **all**] [**detail**]	オンライン診断テストの結果を表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic schedule switch [*number* | **all**]	オンライン診断テストのスケジュールを表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic post	POST 結果を表示します（この出力は、**show post** コマンドの出力と同じです）。

オンライン診断テストの設定例

例：診断テストの開始

次に、テスト名を指定して診断テストを開始する例を示します。

```
スイッチ# diagnostic start switch 2 test TestInlinePwrCtlr
```

次に、すべての基本診断テストを開始する例を示します。

```
スイッチ# diagnostic start switch 1 test all
```

例：ヘルス モニタリング テストの設定

次に、ヘルス モニタリング テストを設定する例を示します。

```
スイッチ(config)# diagnostic monitor threshold switch 1 test 1 failure count 50
スイッチ(config)# diagnostic monitor interval switch 1 test TestPortAsicStackPortLoopback
```

例：診断テストのスケジューリング

次に、特定のスイッチに対して、特定の日時に診断テストを実行するようにスケジューリングする例を示します。

```
スイッチ(config)# diagnostic schedule test DiagThermalTest on June 3 2013  22:25
```

次の例では、指定されたスイッチで毎週特定の時間に診断テストを実行するようにスケジューリングする方法を示します。

```
スイッチ(config)# diagnostic schedule switch 1 test 1,2,4-6 weekly saturday 10:30
```

例：オンライン診断の表示

次に、オンデマンド診断設定を表示する例を示します。

```
スイッチ# show diagnostic ondemand settings

Test iterations = 1
Action on test failure = continue
```

次に、障害の診断イベントを表示する例を示します。

```
スイッチ# show diagnostic events event-type error
```

```
Diagnostic events (storage for 500 events, 0 events recorded)
Number of events matching above criteria = 0

No diagnostic log entry exists.
```

次に、診断テストの説明を表示する例を示します。

```
スイッチ# show diagnostic description switch 1 test all

DiagGoldPktTest :
        The GOLD packet Loopback test verifies the MAC level loopback
        functionality. In this test, a GOLD packet, for which doppler
        provides the support in hardware, is sent. The packet loops back
        at MAC level and is matched against the stored packet. It is a non
        -disruptive test.

DiagThermalTest :
        This test verifies the temperature reading from the sensor is below the yellow
        temperature threshold. It is a non-disruptive test and can be run as a health
monitoring test.

DiagFanTest :
        This test verifies all fan modules have been inserted and working properly on the
board
        It is a non-disruptive test and can be run as a health monitoring test.

DiagPhyLoopbackTest :
        The PHY Loopback test verifies the PHY level loopback
        functionality. In this test, a packet is sent which loops back
        at PHY level and is matched against the stored packet. It is a
        disruptive test and cannot be run as a health monitoring test.

DiagScratchRegisterTest :
        The Scratch Register test monitors the health of application-specific
        integrated circuits (ASICs) by writing values into registers and reading
        back the values from these registers. It is a non-disruptive test and can
        be run as a health monitoring test.

DiagPoETest :
        This test checks the PoE controller functionality. This is a disruptive test
        and should not be performed during normal switch operation.

DiagStackCableTest :
        This test verifies the stack ring loopback functionality
        in the stacking environment. It is a disruptive test and
        cannot be run as a health monitoring test.

DiagMemoryTest :
        This test runs the exhaustive ASIC memory test during normal switch operation
        NG3K utilizes mbist for this test. Memory test is very disruptive
        in nature and requires switch reboot after the test.

スイッチ#
```

次に、ブートアップ レベルを表示する例を示します。

```
スイッチ# show diagnostic bootup level

Current bootup diagnostic level: minimal

スイッチ#
```

オンライン診断に関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference (Catalyst 3650 Switches)*
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S（Catalyst 3850 Switches）*
プラットフォームに依存しない設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S（Catalyst 3850 Switches）*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

オンライン診断設定の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 97 章

コンフィギュレーション ファイルの管理

- コンフィギュレーション ファイルの管理の前提条件，2227 ページ
- コンフィギュレーション ファイルの管理の制約事項，2227 ページ
- コンフィギュレーション ファイルの管理について，2228 ページ
- コンフィギュレーション ファイル情報の管理方法，2235 ページ
- その他の参考資料，2271 ページ

コンフィギュレーション ファイルの管理の前提条件

- ユーザには、少なくとも Cisco IOS 環境とコマンドライン インターフェイスに関する基本的な知識が必要です。
- システムでは、少なくとも最小限の設定が実行されていることが必要です。基本設定ファイルは、**setup** コマンドを使用して作成できます。

コンフィギュレーション ファイルの管理の制約事項

- このドキュメントで説明されている Cisco IOS コマンドの多くが使用可能であり機能するのは、スイッチの特定のコンフィギュレーション モードでのみです。
- Cisco IOS コンフィギュレーション コマンドのいくつかは、特定のスイッチ プラットフォームでのみ使用可能であり、コマンド構文はプラットフォームによって異なる可能性があります。

コンフィギュレーション ファイルの管理について

コンフィギュレーション ファイルのタイプ

コンフィギュレーション ファイルには、Cisco スイッチの機能をカスタマイズするための Cisco IOS ソフトウェア コマンドが含まれています。コマンドは、システムを起動したとき（startup-config ファイルから）、またはコンフィギュレーション モードで CLI にコマンドを入力したときに、Cisco IOS ソフトウェアによって解析（変換および実行）されます。

スタートアップ コンフィギュレーション ファイル（startup-config）は、ソフトウェアを設定するためにシステムの起動時に使用されます。実行コンフィギュレーションファイル（running-config）には、ソフトウェアの現在の設定が含まれています。2 つのコンフィギュレーション ファイルは別々の設定にできます。たとえば、コンフィギュレーションを永続的ではなく短期間で変更する場合があります。このような場合、**configure terminal** EXEC コマンドを使用して実行コンフィギュレーションを変更しますが、**copy running-config startup-config** EXEC コマンドを使用して設定を保存することはありません。

実行コンフィギュレーションを変更するには、コンフィギュレーション ファイルの変更（CLI）の説明に従って、**configure terminal** コマンドを使用します。Cisco IOS コンフィギュレーション モードの使用時には、通常コマンドはすぐに実行され、入力直後またはコンフィギュレーション モードを終了した時点で実行コンフィギュレーション ファイルに保存されます。

スタートアップ コンフィギュレーション ファイルを変更するには、**copy running-config startup-config** EXEC コマンドを使用してスタートアップ コンフィギュレーションに実行コンフィギュレーション ファイルを保存するか、ファイル サーバからスタートアップ コンフィギュレーションにコンフィギュレーション ファイルをコピーします（詳細については、TFTP サーバからスイッチへのコンフィギュレーション ファイルのコピー（CLI）を参照してください）。

コンフィギュレーション モードとコンフィギュレーション ソースの選択

スイッチ上でコンフィギュレーション モードを開始するには、特権 EXEC プロンプトで **configure** コマンドを入力します。Cisco IOS ソフトウェアは次のプロンプトで応答し、端末、メモリ、またはネットワーク サーバ（ネットワーク）上に格納されたファイルのいずれかを、コンフィギュレーション コマンドのソースとして指定するように要求されます。

```
Configuring from terminal, memory, or network [terminal]?
```

端末からの設定では、コマンドラインにコンフィギュレーション コマンドを入力できます（次の項を参照してください）。詳細については、スタートアップコンフィギュレーションファイルでのコンフィギュレーション コマンドの再実行（CLI）の項を参照してください。

ネットワークからの設定では、ネットワーク経由でコンフィギュレーション コマンドをロードして実行できます。詳細については、TFTP サーバからスイッチへのコンフィギュレーション ファイルのコピー（CLI）の項を参照してください。

CLI を使用したコンフィギュレーション ファイルの変更

Cisco IOS ソフトウェアは、1 行につき 1 つのコンフィギュレーション コマンドを受け入れます。コンフィギュレーションコマンドは、必要なだけ入力できます。コンフィギュレーションファイルには、入力したコマンドを説明するコメントを追加できます。コメントの先頭には、感嘆符（!）を付けます。コメントは NVRAM にもコンフィギュレーション ファイルのアクティブ コピーにも格納されないため、**show running-config** または **more system:running-config** EXEC コマンドでアクティブな設定のリストを表示しても、コメントは表示されません。**show startup-config** または **more nvram:startup-config** EXEC モード コマンドでスタートアップ コンフィギュレーションのリストを表示しても、コメントは表示されません。コメントは、コンフィギュレーション ファイルがスイッチにロードされたときにコンフィギュレーション ファイルから削除されます。ただし、File Transfer Protocol（FTP）、Remote Copy Protocol（RCP）、または Trivial File Transfer Protocol（TFTP）サーバ上に格納されているコンフィギュレーションファイルのコメントのリストは表示できます。CLI を使用してソフトウェアは設定するときは、ユーザの入力に従ってソフトウェアによりコマンドが実行されます。

コンフィギュレーション ファイルの場所

コンフィギュレーション ファイルは、次の場所に格納されます。

- 実行コンフィギュレーションは RAM に格納されます。
- クラス A フラッシュ ファイル システム プラットフォーム以外のすべてのプラットフォーム上では、スタートアップ コンフィギュレーションは不揮発性 RAM（NVRAM）に格納されます。
- クラス A フラッシュ ファイル システム プラットフォーム上では、スタートアップ コンフィギュレーションは CONFIG_FILE 環境変数で指定された場所に格納されます（詳細については、セクションクラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定（CLI）を参照してください）。CONFIG_FILE 変数は、デフォルトでは NVRAM になりますが、次のファイル システムのファイルも指定できます。
  - **nvram:**（NVRAM）
  - **bootflash:**（内部フラッシュ メモリ）
  - **usbflash0:**（フラッシュ ファイル システム）

ネットワーク サーバからスイッチへのコンフィギュレーション ファイルのコピー

TFTP、rcp、または FTP サーバからスイッチの実行コンフィギュレーションまたはスタートアップコンフィギュレーションへコンフィギュレーションファイルをコピーできます。この機能は、次のいずれかの理由により実行する場合があります。

- バックアップ コンフィギュレーション ファイルを復元するため。

- 別のスイッチにコンフィギュレーション ファイルを使用するため。たとえば、別のスイッチをネットワークに追加して、そのコンフィギュレーションを元のスイッチと同様にする場合です。新しいスイッチにファイルをコピーすることにより、ファイル全体を再作成するのではなく、該当部分を変更できます。
- 同一のコンフィギュレーション コマンドをネットワーク内のすべてのスイッチにロードして、すべてのスイッチのコンフィギュレーションを同様にするため。

コマンドラインにコマンドを入力した場合と同様に、**copy**{**ftp:** | **rcp:** | **tftp:system:running-config**} EXEC コマンドはスイッチにコンフィギュレーション ファイルをロードします。コマンドを追加する前に、スイッチにより既存の実行コンフィギュレーションが消去されることはありません。コピーされたコンフィギュレーション ファイル内のコマンドによって既存のコンフィギュレーション ファイル内のコマンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定のコマンドの IP アドレスが、既存のコンフィギュレーションに格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内の一部のコマンドには、置き換えられたり無効になったりしないものもあります。このようなコマンドがある場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーションファイルが組み合わされた（コピーされたコンフィギュレーションファイルが優先する）コンフィギュレーション ファイルが作成されます。

コンフィギュレーション ファイルをサーバ上に格納されているファイルの正確なコピーとして復元するには、そのコンフィギュレーションファイルをスタートアップ コンフィギュレーションに直接コピーし（**copy ftp:**| **rcp:**| **tftp:**} **nvram:startup-config** コマンドを使用）、スイッチをリロードする必要があります。

サーバからスイッチへコンフィギュレーション ファイルをコピーするには、次の項で説明する作業を実行します。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および rcp のトランスポート メカニズムは、TFTP よりも高速でデータ配信の信頼性も優れています。これらの改善は、FTP および rcp のトランスポート メカニズムがコネクション型の TCP/IP スタック上に構築されており、これを使用しているために可能になりました。

スイッチから TFTP サーバへのコンフィギュレーション ファイルのコピー

一部の TFTP 実装では、TFTP サーバ上にダミー ファイルを作成し、読み取り、書き込み、および実行を許可してから、ダミー ファイルを上書きする形でファイルをコピーする必要があります。詳細については、ご使用の TFTP のマニュアルを参照してください。

スイッチから RCP サーバへのコンフィギュレーション ファイルのコピー

スイッチから RCP サーバへコンフィギュレーション ファイルをコピーできます。

ネットワークを UNIX コミュニティでリソースとして使用する最初の試みの 1 つは、リモート シェル（RSH）およびリモート コピー（rcp）機能が含まれた、リモート シェル プロトコルの設計および実装につながりました。rsh および rcp により、ユーザはリモートでコマンドを実行し、ネットワーク上のリモート ホストまたはサーバにあるファイル システムからまたはファイル シ

ステムへファイルをコピーすることが可能になります。シスコの rsh および rcp 実装は、標準実装と相互運用できます。

rcp の **copy** コマンドは、リモート システム上の rsh サーバ（またはデーモン）に依存します。rcp を使用してファイルをコピーするために、TFTP のようにファイル配布用のサーバを作成する必要はありません。必要なのは、リモート シェル（rsh）をサポートするサーバへのアクセスだけです（ほとんどの UNIX システムは rsh をサポートしています）。ファイルをある場所から別の場所へコピーするため、コピー元ファイルに対する読み取り権限と、コピー先ファイルに対する書き込み権限が必要です。コピー先ファイルが存在しない場合は、rcp により作成されます。

シスコの rcp 実装は UNIX の rcp 実装（ネットワーク上のシステム間でファイルをコピー）の関数をエミュレートしたものですが、シスコのコマンド構文は UNIX の rcp コマンド構文とは異なります。シスコの rcp サポートは、rcp をトランスポート メカニズムとして使用する一連の **copy** コマンドを提供しています。これらの rcp **copy** コマンドは、シスコの TFTP **copy** コマンドに類似していますが、高速で信頼性の高いデータ配信を実現する代替方法を備えているという点が異なります。これらの改善は、rcp のトランスポート メカニズムがコネクション型の TCP/IP スタック上に構築されており、これを使用しているために可能になりました。rcp コマンドを使用して、スイッチからネットワークサーバ、またはその逆へシステム イメージおよびコンフィギュレーション ファイルをコピーできます。

また、rcp サポートをイネーブルにし、リモート システムのユーザがスイッチから、またはその逆へファイルをコピーできるようにすることも可能です。

リモート ユーザによるスイッチとのファイルのコピーができるように Cisco IOS ソフトウェアを設定するには、**ip rcmd rcp-enable** グローバル コンフィギュレーション コマンドを使用します。

機能制限

RCP プロトコルでは、クライアントは RCP 要求ごとにリモート ユーザ名をサーバに送信する必要があります。RCP を使用してスイッチからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアによって、次の順番で最初に発見された有効なユーザ名が送信されます。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip rcmd remote-username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 現在の TTY（端末）プロセスに関連付けられているリモート ユーザ名。たとえば、ユーザが Telnet を介してスイッチに接続されており、**username** コマンドを介して認証された場合は、Telnet ユーザ名がリモート ユーザ名としてスイッチ ソフトウェアによって送信されます。
4. スイッチの管理ホスト名。

RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモートユーザ名のアカウントを定義する必要があります。このサーバがディレクトリ構造をとっている場合、コンフィギュレーションファイルまたはイメージは、サーバ上のリモートユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホームディレクトリにある場合は、そのユーザの名前をリモートユーザ名として指定できます。

ip rcmd remote-username コマンドを使用して、すべてのコピーに対してユーザ名を指定します。（rcmd は、スーパーユーザ レベルで使用される UNIX ルーチンで、予約されたポート番号に基づいた認証スキームを使用してリモートマシン上でコマンドを実行します。rcmd は「Remote Command（リモート コマンド）」の略です）。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

サーバに書き込む場合、スイッチ上のユーザからの RCP 書き込み要求を受け入れるよう、RCP サーバを適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の .rhosts ファイルにエントリを追加する必要があります。たとえば、スイッチに次の設定行が含まれているとします。

```
hostname スイッチ1
ip rcmd remote-username User0
```

スイッチの IP アドレスが スイッチ1.example.com に変換される場合、RCP サーバ上の User0 の .rhosts ファイルには、次の行が含まれることになります。

```
スイッチ1.example.com スイッチ1
```

RCP ユーザ名に関する要件

RCP プロトコルでは、クライアントは RCP 要求ごとにリモート ユーザ名をサーバに送信する必要があります。RCP を使用してスイッチからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアによって、次の順番で最初に発見された有効なユーザ名が送信されます。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip rcmd remote-username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 現在の TTY（端末）プロセスに関連付けられているリモート ユーザ名。たとえば、ユーザが Telnet を介してスイッチに接続されており、**username** コマンドを介して認証された場合は、Telnet ユーザ名がリモート ユーザ名としてスイッチ ソフトウェアによって送信されます。
4. スイッチの管理ホスト名。

RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。このサーバがディレクトリ構造をとっている場合、コンフィギュレーション ファイルまたはイメージは、サーバ上のリモート ユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

詳細については、ご使用の RCP サーバのマニュアルを参照してください。

スイッチから FTP サーバへのコンフィギュレーション ファイルのコピー

スイッチから FTP サーバへコンフィギュレーション ファイルをコピーできます。

FTP ユーザ名およびパスワードの概要

FTPプロトコルでは、FTP要求ごとにリモートユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してスイッチからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは、次の順番で最初に発見した有効なユーザ名を送信します。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip ftp username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. Anonymous

スイッチは次の順番で最初に発見した有効なパスワードを送信します。

1. **copy** コマンドで指定されたパスワード（パスワードが指定されている場合）。
2. **ip ftp password** コマンドで設定されたパスワード（コマンドが設定されている場合）。
3. スイッチは、*username* @スイッチ*name.domain* というパスワードを生成します。変数 *username* は現在のセッションと関連付けられたユーザ名、スイッチ*name* は設定済みホスト名、*domain* はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合、スイッチ上のユーザからのFTP書き込み要求を受け入れるよう、FTPサーバを適切に設定する必要があります。

このサーバがディレクトリ構造をとっている場合、コンフィギュレーション ファイルまたはイメージは、サーバ上のユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システムイメージがサーバ上のユーザのホームディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

詳細については、ご使用の FTP サーバのマニュアルを参照してください。

ip ftp username および **ip ftp password** グローバル コンフィギュレーション コマンドを使用して、すべてのコピーに対してユーザ名とパスワードを指定します。当該のコピー操作だけに対してユーザ名を指定する場合は、**copy** EXEC コマンドにユーザ名を含めます。

スイッチから別のスイッチへの設定ファイルのコピー

あるスイッチから別のスイッチに設定をコピーすることができます。これは2ステップ プロセスです。スイッチからTFTPサーバに設定をコピーし、次にTFTPから別のスイッチに設定をコピーします。

スイッチから現在の設定をコピーするには、**copy startup-config tftp:** コマンドを実行し、続く指示に従います。コンフィギュレーションが TFTP サーバにコピーされます。

次に、別のスイッチへログインし、**copy tftp: startup-config** コマンドを実行して、続く指示に従います。これで、設定は別のスイッチにコピーされます。

設定をコピーした後、その設定を保存するには、**write memory** コマンドを使用し、その後スイッチをリロードするか、または **copy startup-config running-config** コマンドを実行します。

詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 16.1 (Catalyst 3850 Switches)*』を参照してください。

NVRAM より大きいコンフィギュレーション ファイル

NVRAM より大きいコンフィギュレーション ファイルを維持管理するには、以降の項の情報を知っておく必要があります。

コンフィギュレーション ファイルの圧縮

service compress-config グローバル コンフィギュレーション コマンドは、コンフィギュレーション ファイルを圧縮して NVRAM に格納することを指定します。コンフィギュレーション ファイルが圧縮されると、スイッチは正常に機能します。システムの起動時に、システムはコンフィギュレーションファイルが圧縮されていることを認識し、圧縮されたコンフィギュレーションファイルを展開して、正常に処理を進めます。**more nvram:startup-config** EXEC コマンドにより、コンフィギュレーションが展開されてから表示されます。

コンフィギュレーション ファイルを圧縮する前に、適切なハードウェアのインストレーションおよびメンテナンス マニュアルを参照してください。ご利用のシステムの ROM がファイル圧縮をサポートしていることを確認します。サポートしていない場合、ファイル圧縮をサポートしている新しい ROM をインストールできます。

コンフィギュレーションのサイズは、NVRAM のサイズの 3 倍を超えてはいけません。NVRAM のサイズが 128 KB の場合、展開できる最大のコンフィギュレーション ファイルのサイズは 384 KB です。

service compress-config グローバル コンフィギュレーション コマンドは、Cisco IOS ソフトウェア リリース 10.0 以降のブート ROM を使用している場合に限り実行できます。新しい ROM をインストールするのは 1 回限りの操作で、ROM に Cisco IOS Release 10.0 がない場合だけ必要です。ブート ROM が圧縮コンフィギュレーションを認識しない場合は、次のメッセージが表示されます。

```
Boot ROMs do not support NVRAM compression Config NOT written to NVRAM
```

コンフィギュレーションのクラス A フラッシュ ファイル システム上のフラッシュ メモリへの格納

クラス A フラッシュ ファイル システムのスイッチ上では、内部フラッシュ メモリのファイルまたは PCMCIA スロットのフラッシュ メモリのファイルに CONFIG_FILE 環境変数を設定することにより、スタートアップ コンフィギュレーションをフラッシュ メモリに格納できます。

詳細については、クラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定（CLI）を参照してください。

大きいコンフィギュレーションを編集または変更する場合は、注意する必要があります。フラッシュ メモリ領域は **copy system:running-config nvram:startup-config** EXEC コマンドが発行されるたびに使用されます。フラッシュ メモリのファイル管理（空き領域の最適化などの）は自動的には行われないため、利用可能なフラッシュ メモリに十分注意を払う必要があります。**squeeze** コ

マンドを使用して、使用済み領域を再要求します。20 MB 以上の大容量フラッシュ カードを使用することを推奨します。

ネットワークからのコンフィギュレーション コマンドのロード

コンフィギュレーションが大きい場合は、FTP、RCP、TFTP のいずれかのサーバに格納しておき、システムの起動時にダウンロードすることもできます。ネットワーク サーバを大きいコンフィギュレーションの保存に使用するためのコマンドの詳細については、セクションスイッチから TFTP サーバへのコンフィギュレーション ファイルのコピー（CLI）およびコンフィギュレーション ファイルをダウンロードするスイッチの設定を参照してください。

コンフィギュレーション ファイルをダウンロードするスイッチの設定

システムの起動時に 1 つまたは 2 つのコンフィギュレーション ファイルをロードするようにスイッチを設定できます。コンフィギュレーション ファイルは、コマンドラインにコマンドを入力した場合と同様に、メモリにロードされ読み込まれます。そのため、スイッチのコンフィギュレーションは、元のスタートアップ コンフィギュレーションと 1 つまたは 2 つのダウンロードされたコンフィギュレーション ファイルが混在したものになります。

ネットワークとホストのコンフィギュレーション ファイル

歴史的な理由から、スイッチが最初にダウンロードするファイルは、ネットワーク コンフィギュレーション ファイルと呼ばれます。スイッチが 2 番目にダウンロードするファイルは、ホスト コンフィギュレーション ファイルと呼ばれます。2 つのコンフィギュレーション ファイルは、ネットワーク上のすべてのスイッチが同一コマンドの多くを使用する場合に使用できます。ネットワーク コンフィギュレーションファイルには、すべてのスイッチを設定するために使用される標準コマンドが含まれます。ホスト コンフィギュレーション ファイルには、特定の 1 つのホストに固有のコマンドが含まれます。2 つのコンフィギュレーション ファイルをロードする場合、ホスト コンフィギュレーション ファイルを、もう 1 つのファイルより優先させる必要があります。ネットワーク コンフィギュレーションファイルとホスト コンフィギュレーションファイルの両方とも、TFTP、RCP、FTP のいずれかを介して到達可能なネットワーク サーバ上にあり、読み取り可能である必要があります。

コンフィギュレーション ファイル情報の管理方法

コンフィギュレーション ファイル情報の表示（CLI）

コンフィギュレーション ファイルに関する情報を表示するには、このセクションの手順を実行します。

手順の概要

1. **enable**
2. **showboot**
3. **more***file-url*
4. **showrunning-config**
5. **showstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showboot** 例： `スイッチ# show boot`	BOOT 環境変数の内容（設定されている場合）、CONFIG_FILE 環境変数によって指定されているコンフィギュレーション ファイルの名前、および BOOTLDR 環境変数の内容を示します。
ステップ 3	**more***file-url* 例： `スイッチ# more 10.1.1.1`	指定されたファイルの内容を表示します。
ステップ 4	**showrunning-config** 例： `スイッチ# show running-config`	実行コンフィギュレーション ファイルの内容を表示します（**more system:running-config**コマンドのコマンド エイリアス）。
ステップ 5	**showstartup-config** 例： `スイッチ# show startup-config`	スタートアップ コンフィギュレーション ファイルの内容を表示します。（**more nvram:startup-config** コマンドのコマンドエイリアス）。 クラス A フラッシュ ファイル システム プラットフォーム以外のすべてのプラットフォーム上では、通常、デフォルトの startup-config ファイルは NVRAM に格納されます。 クラス A フラッシュ ファイル システム プラットフォーム上では、CONFIG_FILE 環境変数はデフォルトの startup-config ファイルを指定します。 CONFIG_FILE 変数のデフォルトは NVRAM になります。

コンフィギュレーション ファイルの変更（CLI）

Cisco IOS ソフトウェアは、1 行につき 1 つのコンフィギュレーション コマンドを受け入れます。コンフィギュレーションコマンドは、必要なだけ入力できます。コンフィギュレーションファイルには、入力したコマンドを説明するコメントを追加できます。コメントの先頭には、感嘆符（!）を付けます。コメントは NVRAM にもコンフィギュレーション ファイルのアクティブ コピーにも格納されないため、**showrunning-config** または **moresystem:running-config** EXEC コマンドでアクティブな設定のリストを表示しても、コメントは表示されません。また、**show startup-config** または **morenvram:startup-config** EXEC モード コマンドでスタートアップ コンフィギュレーションのリストを表示しても、コメントは表示されません。コメントは、コンフィギュレーション ファイルがスイッチにロードされたときにコンフィギュレーション ファイルから削除されます。ただし、ファイル転送プロトコル（FTP）、リモート コピー プロトコル（RCP）、または Trivial File Transfer Protocol（TFTP）サーバ上に格納されているコンフィギュレーション ファイルのコメントのリストは表示できます。CLI を使用してソフトウェアは設定するときは、ユーザの入力に従ってソフトウェアによりコマンドが実行されます。CLI を使用してソフトウェアを設定するには、特権 EXEC モードを開始して次のコマンドを使用します。

手順の概要

1. **enable**
2. **configureterminal**
3. **configurationcommand**
4. 次のいずれかを実行します。
   - **end**
   - **^Z**
5. **copysystem:running-configvram:startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**configurationcommand** 例： スイッチ(config)# configuration command	必要なコンフィギュレーション コマンドを入力します。Cisco IOS マニュアルセットに、テクノロジー別に編成されたコンフィギュレーション コマンドが説明されています。
ステップ 4	次のいずれかを実行します。 • **end** • **^Z** 例： スイッチ(config)# end	コンフィギュレーションセッションを終了し、EXEC モードに戻ります。 （注） Ctrl キーと Z キーを同時に押すと、画面に ^Z と表示されます。
ステップ 5	**copysystem:running-confignvram:startup-config** 例： スイッチ# copy system:running-config nvram:startup-config	実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルとして保存します。 **copy running-config startup-config** コマンド エイリアスも使用できますが、このコマンドは精度が高くないため、注意する必要があります。ほとんどのプラットフォーム上では、このコマンドによりコンフィギュレーションは NVRAM に保存されます。クラス A フラッシュ ファイル システムのプラットフォーム上では、この手順によりコンフィギュレーションは CONFIG_FILE 環境変数によって指定された場所に保存されます（デフォルトの CONFIG_FILE 変数では、ファイルの保存先は NVRAM に指定されています）。

例

次の例では、スイッチのスイッチプロンプト名が設定されています。感嘆符（!）で示されたコメント行では、いずれのコマンドも実行されません。**hostname** コマンドは、スイッチから new_name へスイッチ名を変更するために使用されます。Ctrl-Z（^Z）キーを押すか、**end** コマンドを入力すると、コンフィギュレーション モードが終了します。**copysystem:running-confignvram:startup-config** コマンドにより、現在のコンフィギュレーションがスタートアップ コンフィギュレーションに保存されます。

```
スイッチ# configure terminal
スイッチ(config)# !The following command provides the switch host name.
スイッチ(config)# hostname new_name
new_name(config)# end
new_name# copy system:running-config nvram:startup-config
```

スタートアップ コンフィギュレーションが NVRAM にある場合は、現在の設定情報がコンフィギュレーション コマンドとしてテキスト形式で格納され、デフォルト以外の設定だけが記録されます。破損データから保護するために、メモリはチェックサム算出されます。

（注） 一部の特定のコマンドは、NVRAMに保存されない場合があります。これらのコマンドは、マシンをリブートしたときに再入力する必要があります。これらのコマンドは、マニュアルに記載されています。リブート後にすばやくスイッチを再設定できるように、これらの設定のリストを保管しておくことを推奨します。

スイッチから TFTP サーバへのコンフィギュレーション ファイルのコピー（CLI）

TFTP ネットワーク サーバ上の設定をコピーするには、以下の手順を実行します。

手順の概要

1. **enable**
2. **copysystem:running-configtftp:**[[[*//location*]*/directory*]*/filename*]
3. **copynvram:startup-configtftp:**[[[*//location*]*/directory*]*/filename*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copysystem:running-configtftp:**[[[*//location*]*/directory*]*/filename*] 例： `スイッチ# copy system:running-config tftp: //server1/topdir/file10`	TFTP サーバへ実行コンフィギュレーション ファイルをコピーします。
ステップ 3	**copynvram:startup-configtftp:**[[[*//location*]*/directory*]*/filename*] 例： `スイッチ# copy nvram:startup-config tftp: //server1/1stdir/file10`	TFTP サーバへスタートアップ コンフィギュレーション ファイルをコピーします。

例

次に、スイッチからTFTPサーバへコンフィギュレーションファイルをコピーする例を示します。

```
スイッチ# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] Y
Writing tokyo-confg!!! [OK]
```

次の作業

copy コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

スイッチから RCP サーバへのコンフィギュレーション ファイルのコピー(CLI)

スイッチからRCPサーバへスタートアップ コンフィギュレーション ファイルまたは実行コンフィギュレーション ファイルをコピーするには、特権EXECモードを開始して次のコマンドを使用します。

手順の概要

1. **enable**
2. **configureterminal**
3. **iprcmdremote-username***username*
4. **end**
5. 次のいずれかを実行します。
   - **copysystem:running-configrcp:**[[[//[*username@*]*location*]/*directory*]/*filename*]
   - **copynvram:startup-configrcp:**[[[//[*username@*]*location*]/*directory*]/*filename*]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**iprcmdremote-username***username* 例： `スイッチ(config)# ip rcmd remote-username NetAdmin1`	（任意）デフォルトのリモートユーザ名を変更します。
ステップ 4	**end** 例： `スイッチ(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。
ステップ 5	次のいずれかを実行します。 • **copysystem:running-configrcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] • **copynvram:startup-configrcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] 例： `スイッチ# copy system:running-config rcp: //NetAdmin1@example.com/dir-files/file1`	• スイッチの実行コンフィギュレーション ファイルが RCP サーバ上に格納されるように指定します。 または • スイッチのスタートアップ コンフィギュレーション ファイルが RCP サーバ上に格納されるように指定します。

例

RCP サーバへの実行コンフィギュレーション ファイルの格納

次に、rtr2-confg という名前の実行コンフィギュレーション ファイルを IP アドレス 172.16.101.101 のリモート ホスト上の netadmin1 ディレクトリにコピーする例を示します。

```
スイッチ# copy system:running-config rcp://netadmin1@172.16.101.101/runfile2-confg
Write file runfile2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
スイッチ#
```

RCP サーバへのスタートアップ コンフィギュレーション ファイルの格納

次に、RCP を使用してファイルをコピーすることによって、サーバ上にスタートアップ コンフィギュレーション ファイルを格納する例を示します。

```
スイッチ# configure terminal

スイッチ(config)# ip rcmd remote-username netadmin2

スイッチ(config)# end
```

```
スイッチ# copy nvram:startup-config rcp:

Remote host[]? 172.16.101.101

Name of configuration file to write [start-confg]?
Write file start-confg on host 172.16.101.101?[confirm]
![OK]
```

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

スイッチから FTP サーバへのコンフィギュレーション ファイルのコピー(CLI)

スイッチからFTPサーバへスタートアップコンフィギュレーションファイルまたは実行コンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipftpusername***username*
4. **ipftppassword***password*
5. **end**
6. 次のいずれかを実行します。
   - **copysystem:running-configftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] or
   - **copynvram:startup-configftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ipftpusername***username* 例： `スイッチ(config)# ip ftp username NetAdmin1`	（任意）デフォルトのリモート ユーザ名を指定します。
ステップ 4	**ipftppassword***password* 例： `スイッチ(config)# ip ftp password adminpassword`	（任意）デフォルトのパスワードを指定します。
ステップ 5	**end** 例： `スイッチ(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 6	次のいずれかを実行します。 • **copysystem:running-configftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] or • **copynvram:startup-configftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] 例： `スイッチ# copy system:running-config ftp:`	FTP サーバの指定された場所へ実行コンフィギュレーションまたはスタートアップ コンフィギュレーション ファイルをコピーします。

例

FTP サーバへの実行コンフィギュレーション ファイルの格納

次に、runfile-confg という名前の実行コンフィギュレーション ファイルを IP アドレス 172.16.101.101 のリモート ホスト上の netadmin1 ディレクトリにコピーする例を示します。

```
スイッチ# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/runfile-confg
Write file runfile-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
スイッチ#
```

FTP サーバへのスタートアップ コンフィギュレーション ファイルの格納

次に、FTP を使用してファイルをコピーすることによって、サーバ上にスタートアップ コンフィギュレーション ファイルを格納する例を示します。

```
スイッチ# configure terminal

スイッチ(config)# ip ftp username netadmin2

スイッチ(config)# ip ftp password mypass

スイッチ(config)# end

スイッチ# copy nvram:startup-config ftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [start-confg]?
Write file start-confg on host 172.16.101.101?[confirm]
![OK]
```

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

TFTP サーバからスイッチへのコンフィギュレーション ファイルのコピー（CLI）

TFTP サーバからスイッチへコンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順の概要

1. **enable**
2. **copytftp:**[[[*//location*]/*directory*]/*filename*] **system:running-config**
3. **copytftp:**[[[*//location*]/*directory*]/*filename*] **nvram:startup-config**
4. **copytftp:**[[[*//location*]/*directory*]/*filename*]**flash-[n]:/directory/startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ2	**copytftp:**[[[*//location*]/*directory*]/*filename*] **system:running-config** 例： `スイッチ# copy tftp://server1/dir10/datasource system:running-config`	TFTPサーバから実行コンフィギュレーションへコンフィギュレーションファイルをコピーします。
ステップ3	**copytftp:**[[[*//location*]/*directory*]/*filename*] **nvram:startup-config** 例： `スイッチ# copy tftp://server1/dir10/datasource nvram:startup-config`	TFTP サーバからスタートアップコンフィギュレーションへコンフィギュレーションファイルをコピーします。
ステップ4	**copytftp:**[[[*//location*]/*directory*]/*filename*]**flash-[n]:/directory/startup-config** 例： `スイッチ# copy tftp://server1/dir10/datasource flash:startup-config`	TFTP サーバからスタートアップコンフィギュレーションへコンフィギュレーションファイルをコピーします。

例

次に、IP アドレス 172.16.2.155 にある、tokyo-confgという名前のファイルからソフトウェアを設定する例を示します。

```
スイッチ# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] Y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

rcp サーバからスイッチへのコンフィギュレーション ファイルのコピー（CLI）

rcp サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **iprcmdremote-username***username*
4. **end**
5. 次のいずれかを実行します。
   - **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]**system:running-config**
   - **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]**nvram:startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	（任意）端末からコンフィギュレーション モードを開始します。この手順は、デフォルトのリモート ユーザ名を上書きする場合にだけ必要です（ステップ 3 を参照）。
ステップ 3	**iprcmdremote-username***username* 例： `スイッチ(config)# ip rcmd remote-username NetAdmin1`	（任意）リモート ユーザ名を指定します。
ステップ 4	**end** 例： `スイッチ(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 を参照）。
ステップ 5	次のいずれかを実行します。 • **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]**system:running-config**	rcp サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします。

	コマンドまたはアクション	目的
	• **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]**nvram:startup-config** 例： スイッチ# copy rcp://[user1@example.com/dir10/fileone] nvram:startup-config	

例

RCP の *Running-Config* のコピー

次に、host1-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからコピーし、スイッチでコマンドをロードし実行する例を示します。

```
スイッチ# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
スイッチ#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

RCP の *Startup-Config* のコピー

次に、リモート ユーザ名 netadmin1 を指定する例を示します。次に host2-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからスタートアップ コンフィギュレーションへコピーします。

```
スイッチ# configure terminal
スイッチ(config)# ip rcmd remote-username netadmin1
スイッチ(config)# end
スイッチ# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
スイッチ#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from 172.16.101.101
```

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

FTP サーバからスイッチへのコンフィギュレーション ファイルのコピー（CLI）

FTP サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipftpusername***username*
4. **ipftppassword***password*
5. **end**
6. 次のいずれかを実行します。
   - **copyftp:** [[[//[*username*[**:***password*]**@**]*location*] */directory*]*/filename*]**system:running-config**
   - **copyftp:** [[[//[*username*[**:***password*]**@**]*location*]*/directory*]*/filename*]**nvram:startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	（任意）グローバル コンフィギュレーション モードを開始できます。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 3 および 4 を参照）。
ステップ 3	**ipftpusername***username* 例： `スイッチ(config)# ip ftp username NetAdmin1`	（任意）デフォルトのリモート ユーザ名を指定します。
ステップ 4	**ipftppassword***password* 例： `スイッチ(config)# ip ftp password adminpassword`	（任意）デフォルトのパスワードを指定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `スイッチ(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 3 および 4 を参照）。
ステップ 6	次のいずれかを実行します。 • **copyftp:** [[[//[*username*[**:***password*]**@**]*location*] */directory*]/*filename*]**system:running-config** • **copyftp:** [[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*]**nvram:startup-config** 例： `スイッチ# copy ftp:nvram:startup-config`	FTP を使用して、ネットワーク サーバから実行メモリまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします。

例

FTP の *Running-Config* のコピー

次に、host1-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからコピーし、スイッチでコマンドをロードし実行する例を示します。

```
スイッチ# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
スイッチ#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

FTP の *Startup-Config* のコピー

次に、リモート ユーザ名 netadmin1 を指定する例を示します。次に host2-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからスタートアップ コンフィギュレーションへコピーします。

```
スイッチ# configure terminal
スイッチ(config)# ip ftp username netadmin1
スイッチ(config)# ip ftp password mypass
スイッチ(config)# end
スイッチ# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[host1-confg]? host2-confg
```

```
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
スイッチ#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from 172.16.101.101
```

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

NVRAM より大きいコンフィギュレーション ファイルの保守

NVRAM のサイズを超えるコンフィギュレーション ファイルを保守するには、以降のセクションで説明するタスクを実行します。

コンフィギュレーション ファイルの圧縮（CLI）

コンフィギュレーション ファイルを圧縮するには、このセクションの手順を実行してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **servicecompress-config**
4. **end**
5. 次のいずれかを実行します。
   - 新しいコンフィギュレーションをコピーするには、FTP、RCP、TFTP を使用します。
   - **configureterminal**
6. **copysystem:running-confignvram:startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**servicecompress-config** 例： スイッチ(config)# service compress-config	コンフィギュレーション ファイルを圧縮することを指定します。
ステップ 4	**end** 例： スイッチ(config)# end	グローバル コンフィギュレーション モードを終了します。
ステップ 5	次のいずれかを実行します。 • 新しいコンフィギュレーションをコピーするには、FTP、RCP、TFTP を使用します。 • **configureterminal** 例： スイッチ# configure terminal	新しいコンフィギュレーションを入力します。 • NVRAM のサイズの 3 倍以上のコンフィギュレーションをロードしようとすると、次のエラー メッセージが表示されます。 「[buffer overflow - *file-size* /*buffer-size* bytes]。」
ステップ 6	**copysystem:running-confignvram:startup-config** 例： スイッチ(config)# copy system:running-config nvram:startup-config	実行コンフィギュレーションの変更が終わったら、新しいコンフィギュレーションを保存します。

例

次に、129 KB のコンフィギュレーション ファイルを 11 KB に圧縮する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# service compress-config
スイッチ(config)# end
スイッチ# copy tftp://172.16.2.15/tokyo-confg system:running-config
```

```
Configure using tokyo-confg from 172.16.2.155? [confirm] y

Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
スイッチ# copy system:running-config nvram:startup-config

Building configuration...
Compressing configuration from 129648 bytes to 11077 bytes
[OK]
```

コンフィギュレーションのクラス A フラッシュ ファイル システム上のフラッシュ メモリへの格納（CLI）

スタートアップ コンフィギュレーションをフラッシュ メモリに格納するには、このセクションの手順を実行してください。

手順の概要

1. **enable**
2. **copynvram:startup-config***flash-filesystem:filename*
3. **configureterminal**
4. **bootconfigflash-filesystem:***filename*
5. **end**
6. 次のいずれかを実行します。
   - 新しいコンフィギュレーションをコピーするには、FTP、RCP、TFTP を使用します。NVRAM サイズの 3 倍を超える大きさのコンフィギュレーションをロードしようとすると、次のエラー メッセージが表示されます。「[buffer overflow - *file-size* /*buffer-size* bytes]」
   - **configureterminal**
7. **copysystem:running-confignvram:startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copynvram:startup-config***flash-filesystem:filename* 例： `スイッチ# copy nvram:startup-config usbflash0:switch-config`	新しい場所に現在のスタートアップ コンフィギュレーションをコピーして、コンフィギュレーション ファイルを作成します。

	コマンドまたはアクション	目的
ステップ 3	**configureterminal** 例： スイッチ# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**bootconfigflash-filesystem:***filename* 例： スイッチ(config)# boot config usbflash0:switch-config	CONFIG_FILE 環境変数を設定することにより、フラッシュ メモリにスタートアップ コンフィギュレーション ファイルを格納することを指定します。
ステップ 5	**end** 例： スイッチ(config)# end	グローバル コンフィギュレーション モードを終了します。
ステップ 6	次のいずれかを実行します。 • 新しいコンフィギュレーションをコピーするには、FTP、RCP、TFTP を使用します。NVRAM サイズの 3 倍を超える大きさのコンフィギュレーションをロードしようとすると、次のエラー メッセージが表示されます。「[buffer overflow - *file-size* /*buffer-size* bytes]」 • **configureterminal** 例： スイッチ# configure terminal	新しいコンフィギュレーションを入力します。
ステップ 7	**copysystem:running-confignvram:startup-config** 例： スイッチ(config)# copy system:running-config nvram:startup-config	実行コンフィギュレーションの変更が終わったら、新しいコンフィギュレーションを保存します。

例

以下に、usbflash0: に格納したコンフィギュレーションの例を示します。

```
スイッチ# copy nvram:startup-config usbflash0:switch-config
```

```
スイッチ# configure terminal
スイッチ(config)# boot config usbflash0:switch-config
スイッチ(config)# end
スイッチ# copy system:running-config nvram:startup-config
```

ネットワークからのコンフィギュレーション コマンドのロード（CLI）

ネットワーク サーバを使用して、大きなコンフィギュレーションを保存するには、このセクションの手順を実行します。

手順の概要

1. **enable**
2. **copysystem:running-config** {**ftp:** | **rcp:** | **tftp:**}
3. **configureterminal**
4. **bootnetwork**{**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*]}
5. **serviceconfig**
6. **end**
7. **copysystem:running-confignvram:startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copysystem:running-config** {**ftp:**	**rcp:**	**tftp:**} 例： `スイッチ# copy system:running-config ftp:`	実行コンフィギュレーションをFTP、RCP、TFTPのいずれかのサーバに保存します。
ステップ 3	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**bootnetwork**{**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*]} 例： `スイッチ(config)# boot network ftp://user1:guessme@example.com/dir10/file1`	起動時にスタートアップ コンフィギュレーション ファイルをネットワーク サーバからロードすることを指定します。
ステップ 5	**serviceconfig** 例： `スイッチ(config)# service config`	システムの起動時にコンフィギュレーション ファイルをダウンロードするようにスイッチをイネーブルにします。
ステップ 6	**end** 例： `スイッチ(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 7	**copysystem:running-confignvram:startup-config** 例： `スイッチ# copy system:running-config nvram:startup-config`	設定を保存します。

フラッシュ メモリからスタートアップまたは実行コンフィギュレーションへのコンフィギュレーション ファイルのコピー（CLI）

フラッシュ メモリから現在の NVRAM にあるスタートアップ コンフィギュレーションまたは実行コンフィギュレーションへコンフィギュレーション ファイルを直接コピーするには、ステップ 2 のいずれかのコマンドを入力します。

手順の概要

1. **enable**
2. 次のいずれかを実行します。
   - **copy***filesystem*: [*partition-number***:**][*filename*] **nvram:startup-config**
   - **copy***filesystem*: [*partition-number***:**][*filename*] **system:running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかを実行します。 • **copy***filesystem*: [*partition-number***:**][*filename*] **nvram:startup-config** • **copy***filesystem*: [*partition-number***:**][*filename*] **system:running-config** 例： スイッチ# copy usbflash0:4:ios-upgrade-1 nvram:startup-config	• NVRAM にコンフィギュレーション ファイルを直接ロードする、または • 現在の実行コンフィギュレーションにコンフィギュレーション ファイルをコピーします。

例

次に、usbflash0 にあるフラッシュ メモリ PC カードのパーティション 4 からスイッチのスタートアップ コンフィギュレーションへ ios-upgrade-1 という名前のファイルをコピーする例を示します。

```
スイッチ# copy usbflash0:4:ios-upgrade-1 nvram:startup-config
Copy 'ios-upgrade-1' from flash device as 'startup-config' ? [yes/no] yes
[OK]
```

フラッシュ メモリ ファイル システム間でのコンフィギュレーション ファイルのコピー（CLI）

複数のフラッシュ メモリ ファイル システムを備えたプラットフォーム上では、内部フラッシュ メモリなどのフラッシュ メモリ ファイル システムから他のフラッシュ メモリ ファイル システムへファイルをコピーできます。異なるフラッシュ メモリ ファイル システムへファイルをコピーすると、使用中のコンフィギュレーションのバックアップ コピーを作成し、他のスイッチにコンフィギュレーションを複製できます。フラッシュ メモリ ファイル システム間でコンフィギュレーション ファイルをコピーするには、EXEC モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **show***source-filesystem*:
3. **copy***source-filesystem*: [*partition-number***:**][*filename*] *dest-filesystem***:**[*partition-number***:**][*filename*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードを有効化します。 • パスワードを入力します（要求された場合）。
ステップ 2	**show***source-filesystem*: 例： `スイッチ# show flash:`	フラッシュ メモリのレイアウトと内容を表示して、ファイル名を確認します。
ステップ 3	**copy***source-filesystem*: [*partition-number***:**][*filename*] *dest-filesystem***:**[*partition-number***:**][*filename*] 例： `スイッチ# copy flash: usbflash0:`	フラッシュ メモリ デバイス間でコンフィギュレーション ファイルをコピーします。 • コピー元デバイスとコピー先デバイスは同じにはできません。例えば、**copy usbflash0: usbflash0:** コマンドは無効です。

例

次に、内部フラッシュ メモリのパーティション 1 からスイッチ上の usbflash0 のパーティション 1 へ running-config という名前のファイルをコピーする例を示します。この例では、コピー元のパーティションが指定されていないため、スイッチからパーティション番号を要求されます。

```
スイッチ# copy flash: usbflash0:

System flash
Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1         4096K   3070K     1025K     4096K      Read/Write     Direct
  2        16384K   1671K    14712K     8192K      Read/Write     Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]
System flash directory, partition 1:
File  Length   Name/status
  1   3142748  dirt/network/mars-test/c3600-j-mz.latest
  2   850      running-config
[3143728 bytes used, 1050576 available, 4194304 total]
usbflash0 flash directory:
```

```
File  Length   Name/status
  1   1711088  dirt/gate/c3600-i-mz
  2   850      running-config
[1712068 bytes used, 2482236 available, 4194304 total]
Source file name? running-config

Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)...  OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'running-config' from flash: device
  as 'running-config' into usbflash0: device WITH erase? [yes/no] yes

Erasing device... eeee
```

	コマンドまたはアクション	目的
		要です（ステップ 3 および 4 を参照）。
ステップ 3	**ipftpusername***username* 例： `スイッチ(config)# ip ftp username Admin01`	（任意）リモート ユーザ名を指定します。
ステップ 4	**ipftppassword***password* 例： `スイッチ(config)# ip ftp password adminpassword`	（任意）リモート パスワードを指定します。
ステップ 5	**end** 例： `スイッチ(config)# end`	（任意）コンフィギュレーション モードを終了します。このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 3 および 4 を参照）。
ステップ 6	**copyftp:**[[*//location*]*/directory*]*/bundle_name***flash:** 例： `スイッチ>copy ftp:/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash:`	FTP を使用してネットワーク サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーします。

次の作業

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

RCP サーバからフラッシュ メモリ デバイスへのコンフィギュレーション ファイルのコピー（CLI）

RCP サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **iprcmdremote-username***username*
4. **end**
5. **copyrcp:**[[[//[*username*@]*location*]/*directory*] /*bundle_name*]**flash:**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードを有効化します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	（任意）グローバル コンフィギュレーション モードを開始します。この手順は、デフォルトのリモートユーザ名またはパスワードを上書きする場合にのみ必要です（ステップ 3 を参照）。
ステップ 3	**iprcmdremote-username***username* 例： `スイッチ(config)# ip rcmd remote-username Admin01`	（任意）リモート ユーザ名を指定します。
ステップ 4	**end** 例： `スイッチ(config)# end`	（任意）コンフィギュレーション モードを終了します。この手順は、デフォルトのリモートユーザ名またはパスワードを上書きする場合にのみ必要です（ステップ 3 を参照）。
ステップ 5	**copyrcp:**[[[//[*username*@]*location*]/*directory*] /*bundle_name*]**flash:** 例： `スイッチ# copy rcp://netadmin@172.16.101.101/bundle1 flash:`	RCP を使用してネットワーク サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーします。追加情報または確認を要求するスイッチからのプロンプトに対し応答します。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** コマンドの現在の設定によって異なります。

TFTP サーバからフラッシュ メモリ デバイスへのコンフィギュレーション ファイルのコピー（CLI）

TFTP サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーするには、以下の手順を実行します。

手順の概要

1. **enable**
2. **copytftp:**[[[//*location*]/*directory*]/bundle_name**flash:**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードを有効化します。 • パスワードを入力します（要求された場合）。

ステップ 2	**copytftp:**[[[//*location*]/*directory*]/bundle_name**flash:**
	
	例：
	
	`スイッチ#`
	`copy`
	`tftp:/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin`
	` flash:`
		TFTP サーバからフラッシュ メモリ デバイスへファイルをコピーします。追加情報または確認を要求するスイッチからのプロンプトに対し応答します。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** コマンドの現在の設定によって異なります。

例

次に、TFTP サーバから usbflash0 に挿入されているフラッシュ メモリ カードへ、switch-config という名前のコンフィギュレーション ファイルをコピーする例を示します。コピーされたファイルの名前は new-config に変更されます。

```
スイッチ#
copy tftp:switch-config usbflash0:new-config
```

スタートアップ コンフィギュレーション ファイルでのコンフィギュレーション コマンドの再実行（CLI）

スタートアップコンフィギュレーションファイルのコマンドを再実行するには、このセクションの手順を実行します。

手順の概要

1. **enable**
2. **configurememory**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configurememory** 例： `スイッチ# configure memory`	スタートアップ コンフィギュレーション ファイルでコンフィギュレーション コマンドを再実行します。

スタートアップ コンフィギュレーションのクリア（CLI）

スタートアップ コンフィギュレーションから設定情報を消去できます。スイッチをスタートアップ コンフィギュレーションなしで再起動した場合は、スイッチを最初から設定できるように、スイッチは、Setup コマンド ファシリティに移行します。スタートアップ コンフィギュレーションの内容をクリアするには、次の手順を実行します。

手順の概要

1. **enable**
2. **erasenvram**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**erasenvram** 例： `スイッチ# erase nvram`	スタートアップ コンフィギュレーションの内容をクリアします。 （注） クラス A フラッシュ ファイル システムのプラットフォーム以外のすべてのプラットフォームでは、このコマンドにより NVRAM が消去されます。スタートアップ コンフィギュレーション ファイルは、いったん削除すると復元できません。クラス A フラッシュ ファイル システムのプラットフォーム上では、**erasestartup-config** EXEC コマンドを使用すると、スイッチが CONFIG_FILE 環境変数により指定されたコンフィギュレーションを消去または削除します。この変数が NVRAM を指定している場合は、スイッチにより NVRAM が消去されます。CONFIG_FILE 環境変数がフラッシュ メモリ デバイスとコンフィギュレーション ファイル名を指定している場合は、スイッチによりコンフィギュレーション ファイルが削除されます。つまり、そのコンフィギュレーション ファイルは、スイッチにより消去されるのではなく、「削除済み」としてマークされます。この機能では、削除されたファイルを回復できます。

指定されたコンフィギュレーション ファイルの削除（CLI）

特定のフラッシュ デバイスの指定された設定を削除するには、このセクションの手順を実行します。

手順の概要

1. **enable**
2. **delete***flash-filesystem*:*filename*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**delete***flash-filesystem***:***filename* 例： `スイッチ# delete usbflash0:myconfig`	特定のフラッシュ デバイス上の指定されたコンフィギュレーション ファイルを削除します。 （注） クラス A および B フラッシュ ファイル システムでは、フラッシュ メモリ内の特定のファイルを削除すると、そのファイルは削除済みとしてシステムによりマークされます。これにより、**undelete** EXEC コマンドを使用して、削除したファイルを後で回復できるようになります。消去されたファイルは回復できません。コンフィギュレーション ファイルを完全に消去するには、**squeeze** EXEC コマンドを使用します。クラス C フラッシュ ファイル システムでは、削除されたファイルは回復できません。CONFIG_FILE 環境変数で指定されたコンフィギュレーション ファイルを消去または削除しようとした場合、システムにより削除の確認を求めるプロンプトが表示されます。

クラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定（CLI）

クラス A フラッシュ ファイル システムでは、CONFIG_FILE 環境変数で指定されたスタートアップ コンフィギュレーション ファイルをロードするように Cisco IOS ソフトウェアを設定できます。CONFIG_FILE 変数のデフォルトは NVRAM になります。CONFIG_FILE 環境変数を変更するには、このセクションの手順を実行してください。

手順の概要

1. **enable**
2. **copy**[*flash-url*| *ftp-url* | *rcp-url*| *tftp-url* | **system:running-config** | **nvram:startup-config**] *dest-flash-url*
3. **configureterminal**
4. **bootconfig***dest-flash-url*
5. **end**
6. **copysystem:running-confignvram:startup-config**
7. **showboot**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copy**[*flash-url*| *ftp-url* | *rcp-url*| *tftp-url* | **system:running-config** | **nvram:startup-config**] *dest-flash-url* 例： `スイッチ# copy system:running-config nvram:startup-config`	フラッシュ ファイル システムにコンフィギュレーション ファイルをコピーします。再起動時には、ここからスイッチにファイルがロードされます。
ステップ 3	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**bootconfig***dest-flash-url* 例： `スイッチ(config)# boot config 172.16.1.1`	CONFIG_FILE 環境変数を設定します。この手順により、実行時の CONFIG_FILE 環境変数が変更されます。
ステップ 5	**end** 例： `スイッチ(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**copysystem:running-confignvram:startup-config** 例： `スイッチ# copy system:running-config nvram:startup-config`	スタートアップ コンフィギュレーションにステップ 3 で実行されたコンフィギュレーションを保存します。
ステップ 7	**showboot** 例： `スイッチ# show boot`	（任意）CONFIG_FILE 環境変数の内容を確認できます。

例

次の例は、実行コンフィギュレーション ファイルをスイッチにコピーします。その後、システムが再起動されるとこのコンフィギュレーションがスタートアップ コンフィギュレーションとして使用されます。

```
スイッチ# copy system:running-config usbflash0:config2
スイッチ# configure terminal
スイッチ(config)# boot config usbflash0:config2
スイッチ(config)# end
スイッチ# copy system:running-config nvram:startup-config
[ok]
スイッチ# show boot
BOOT variable = usbflash0:rsp-boot-m
CONFIG_FILE variable = nvram:
Current CONFIG_FILE variable = usbflash0:config2
Configuration register is 0x010F
```

次の作業

スタートアップ コンフィギュレーション ファイルの場所を指定すると、**nvram:startup-config** コマンドは、スタートアップコンフィギュレーションファイルの新しい場所のエイリアスとなります。**more nvram:startup-config** EXEC コマンドにより、スタートアップ コンフィギュレーションが、その場所に関係なく表示されます。**erase nvram:startup-config** EXEC コマンドにより、NVRAM の内容が消去され、CONFIG_FILE 環境変数で指定されたファイルが削除されます。

copy system:running-config nvram:startup-config コマンドを使用して設定を保存した場合、スイッチにより、コンフィギュレーション ファイルの完全バージョンは CONFIG_FILE 環境変数で指定した場所に保存され、抽出バージョンは NVRAM に保存されます。抽出バージョンとは、アクセス リスト情報を含まないバージョンです。NVRAM に完全バージョンのコンフィギュレーションファイルが含まれている場合、スイッチは、完全バージョンを抽出バージョンで上書きすることを確認するプロンプトを表示します。NVRAM に抽出コンフィギュレーションが含まれている場合、スイッチは確認のプロンプトを表示しないで NVRAM にある既存の抽出バージョンのコンフィギュレーション ファイルを上書きする処理を続行します。

（注） フラッシュ デバイスにあるファイルを CONFIG_FILE 環境変数として指定した場合、**copy system:running-config nvram:startup-config** コマンドでコンフィギュレーション ファイルを保存するたびに、古いコンフィギュレーション ファイルは「deleted」とマークされ、新しいコンフィギュレーションファイルがそのデバイスに保存されます。それでも古いコンフィギュレーション ファイルがメモリを使用するため、最終的にフラッシュ メモリは一杯になります。**squeeze** EXEC コマンドを使用して、古いコンフィギュレーション ファイルを完全に削除してから、領域を再要求してください。

コンフィギュレーション ファイルをダウンロードするスイッチの設定

ネットワーク コンフィギュレーションおよびホスト コンフィギュレーション ファイル名の順序付きリストを指定できます。Cisco IOS XE ソフトウェアは、適切なネットワークまたはホスト コンフィギュレーション ファイルをロードするまで、このリストをスキャンします。

システムの起動時にコンフィギュレーション ファイルをダウンロードするようにスイッチを設定するには、次の項で説明する作業を少なくとも 1 つ実行します。

- ネットワーク コンフィギュレーション ファイルをダウンロードするスイッチの設定（CLI）
- ホスト コンフィギュレーション ファイルをダウンロードするスイッチの設定（CLI）

起動中にコンフィギュレーション ファイルをロードできなかった場合、要求されたファイルがホストから提供されるまで、スイッチは10分ごと（デフォルト設定）に再試行します。試行が失敗するごとに、スイッチにより以下のメッセージがコンソール端末に表示されます。

```
Booting host-confg... [timed out]
```

スタートアップコンフィギュレーションファイルになんらかの問題がある場合、またはコンフィギュレーション レジスタが NVRAM を無視するように設定されている場合は、スイッチは Setup コマンド ファシリティに移行します。

ネットワーク コンフィギュレーション ファイルをダウンロードするスイッチの設定（CLI）

起動時にサーバからネットワーク コンフィギュレーション ファイルをダウンロードするように Cisco IOS ソフトウェアを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **bootnetwork**{**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*]}
4. **serviceconfig**
5. **end**
6. **copysystem:running-configvram:startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bootnetwork**{**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*]} 例： `スイッチ(config)# boot network tftp:hostfile1`	起動時にダウンロードするネットワーク コンフィギュレーション ファイルおよび使用されるプロトコル（TFTP、RCP、または FTP）を指定します。 • ネットワーク コンフィギュレーション ファイル名を指定しない場合、Cisco IOS ソフトウェアはデフォルトのファイル名の network-confg を使用します。アドレスを省略した場合、スイッチはブロードキャスト アドレスを使用します。 • 複数のネットワーク コンフィギュレーション ファイルを指定できます。ソフトウェアは、ネットワーク コンフィギュレーション ファイルをロードできるまで、入力された順に試行します。この手順は、異なる設定情報を持つ、ネットワーク サーバ上にロードされるファイルを複数保持する場合に役立ちます。
ステップ 4	**serviceconfig** 例： `スイッチ(config)# service config`	再起動時にネットワーク ファイルを自動的にロードするようにシステムをイネーブルにします。
ステップ 5	**end** 例： `スイッチ(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**copysystem:running-confignvram:startup-config** 例： `スイッチ# copy system:running-config nvram:startup-config`	実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに保存します。

ホスト コンフィギュレーション ファイルをダウンロードするスイッチの設定（CLI）

起動時にサーバからホスト コンフィギュレーション ファイルをダウンロードするようにCisco IOS ソフトウェアを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **boothost**{**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*] }
4. **serviceconfig**
5. **end**
6. **copysystem:running-confignvram:startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**boothost**{**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*] } 例： `スイッチ(config)# boot host tftp:hostfile1`	起動時にダウンロードするホスト コンフィギュレーション ファイルおよび使用されるプロトコル（FTP、RCP、または TFTP）を指定します。 • ホスト コンフィギュレーション ファイルの名前を指定しない場合、スイッチは、それ自身の名前を使用してホスト コンフィギュレーション ファイル名を形成します。このとき、その名前はすべて小文字に変換され、すべてのドメイン情報は削除され、「-config」が追加されます。ホスト名の情報を利用できない場合は、ソフトウェアはデフォルトのホスト コンフィギュレーション ファイル名の スイッチ-confg を使用します。アドレスを省略した場合、スイッチはブロードキャスト アドレスを使用します。

	コマンドまたはアクション	目的
		• 複数のホストコンフィギュレーションファイルを指定できます。Cisco IOS ソフトウェアは、ホスト コンフィギュレーション ファイルをロードできるまで、入力された順に試行します。この手順は、異なる設定情報を持つ、ネットワーク サーバ上にロードされるファイルを複数保持する場合に役立ちます。
ステップ 4	**serviceconfig** 例： `スイッチ(config)# service config`	再起動時にホスト ファイルを自動的にロードするようにシステムをイネーブルにします。
ステップ 5	**end** 例： `スイッチ(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**copysystem:running-confignvram:startup-config** 例： `スイッチ# copy system:running-config nvram:startup-config`	実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに保存します。

例

次に、hostfile1 という名前のホスト コンフィギュレーション ファイルおよび networkfile1 という名前のネットワーク コンフィギュレーションファイルをダウンロードするようにスイッチを設定する例を示します。スイッチは TFTP およびブロードキャスト アドレスを使用してファイルを取得します。

```
スイッチ# configure terminal
スイッチ(config)# boot host tftp:hostfile1
スイッチ(config)# boot network tftp:networkfile1
スイッチ(config)# service config
スイッチ(config)# end
スイッチ# copy system:running-config nvram:startup-config
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS コンフィギュレーション コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

エラー メッセージ デコーダ

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

標準

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
• 新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 98 章

コンフィギュレーションの置換とロールバック

- コンフィギュレーションの置換とロールバックの前提条件，2273 ページ
- コンフィギュレーションの置換とロールバックの制約事項，2274 ページ
- コンフィギュレーションの置換とロールバックについて，2274 ページ
- コンフィギュレーションの置換とロールバックの使用方法，2277 ページ
- コンフィギュレーションの置換とロールバックの設定例，2284 ページ
- その他の参考資料，2286 ページ

コンフィギュレーションの置換とロールバックの前提条件

コンフィギュレーションの置換とロールバックの機能に対する入力となるコンフィギュレーション ファイルの形式は、標準の Cisco ソフトウェア コンフィギュレーション ファイルの、次に示すインデント規則に準拠している必要があります。

- 新しい行のすべてのコマンドは、コマンドがコンフィギュレーション サブモードにない限り、インデントなしで開始します。
- レベル 1 コンフィギュレーション サブモード内のコマンドは、スペース 1 個分インデントします。
- レベル 2 コンフィギュレーション サブモード内のコマンドは、スペース 2 個分インデントします。
- 以下、続くサブモード内のコマンドは、同じようにインデントします。

これらのインデント規則には、ソフトウェアが **show running-config** や **copy running-config***destination-url* などのコマンドのコンフィギュレーション ファイルを作成する方法が記述されています。シスコデバイスで生成されるコンフィギュレーションファイルは、いずれもこうした規則に従います。

2 つのコンフィギュレーション ファイル（現在の実行コンフィギュレーションと、保存された置換用コンフィギュレーション）を合わせたサイズより大きな空きメモリが必要です。

コンフィギュレーションの置換とロールバックの制約事項

デバイスに、2 つのコンフィギュレーション ファイル（現在の実行コンフィギュレーションと、保存された置換用コンフィギュレーション）を合わせたサイズより大きな空きメモリがない場合、コンフィギュレーション置換操作は実行されません。

ネットワーク デバイスの物理コンポーネント（物理インターフェイスなど）に関連する特定の Cisco コンフィギュレーション コマンドは、実行コンフィギュレーションについて追加または削除することはできません。たとえば、コンフィギュレーション置換操作を行っても、そのインターフェイスがデバイス上に物理的に存在する場合、現在の実行コンフィギュレーションから **interface ethernet 0** コマンド行を削除することはできません。同様に、**interface ethernet 1** コマンド行は、そのようなインターフェイスがデバイス上に物理的に存在しない場合、実行コンフィギュレーションに追加することはできません。コンフィギュレーション置換操作でこのタイプの変更を試行すると、その特定のコマンド行が失敗したことを示すエラー メッセージが表示されます。

非常にまれなケースですが、ルータをリロードしないと特定の Cisco コンフィギュレーション コマンドを実行コンフィギュレーションから削除できないことがあります。コンフィギュレーション置換操作でこのタイプのコマンドの削除を試行すると、その特定のコマンド行が失敗したことを示すエラー メッセージが表示されます。

コンフィギュレーションの置換とロールバックについて

コンフィギュレーション アーカイブ

Cisco IOS コンフィギュレーション アーカイブは、**configure replace** コマンドを使用するコンフィギュレーションのロールバック機能を強化するために、Cisco IOS コンフィギュレーション ファイルのアーカイブの保存、編成、管理を行うことを目的とした機能です。この機能の導入前にも、実行コンフィギュレーションのコピーを **copy running-config** *destination-url* コマンドを使用して保存し、ローカルやリモートに置換ファイルを保管できました。ただし、この方法ではファイルの自動管理を行うことはできませんでした。一方、コンフィギュレーションの置換とロールバック機能では、実行コンフィギュレーション ファイルを自動的に Cisco IOS コンフィギュレーション アーカイブに保存できます。アーカイブされたファイルはコンフィギュレーションのチェックポイントとして参照することができ、**configure replace** コマンドを使用して以前のコンフィギュレーション状態に戻すために利用できます。

archive config コマンドを使用すると、Cisco IOS コンフィギュレーションをコンフィギュレーション アーカイブに保存できます。その場合、標準のディレクトリとファイル名のプレフィクスが使用され、バージョン番号（およびオプションでタイムスタンプ）が自動的に付加されます。バージョン番号は連続したファイルを保存するごとに、1 つずつ大きくなります。この機能により、保存した Cisco IOS コンフィギュレーション ファイルを一貫して識別できます。アーカイブに保存する実行コンフィギュレーションの数は指定することができます。アーカイブ内のファイル数

が上限値に達すると、次に最新のファイルが保存されるときに、最も古いファイルが自動的に消去されます。**show archive** コマンドを使用すると、Cisco IOS コンフィギュレーション アーカイブに保存されているすべてのコンフィギュレーション ファイルに関する情報が表示されます。

コンフィギュレーション ファイルを保存する Cisco IOS コンフィギュレーション アーカイブは、**configure replace** コマンドで使用することによって、FTP、HTTP、RCP、TFTP のファイル システム上に配置できます。

コンフィギュレーションの置換

configure replace 特権 EXEC コマンドにより、現在の実行コンフィギュレーションを、保存しておいた Cisco IOS コンフィギュレーション ファイルで置換することができます。この機能は、コンフィギュレーションを保存しておいた状態へ戻すために使用することができ、そのコンフィギュレーション状態が保存された後にどのような変更が加えられても、効果的にロールバックさせることができます。

configure replace コマンドを使用するときは、現在の実行コンフィギュレーションと置換するための、保存された Cisco IOS コンフィギュレーション ファイルを指定する必要があります。置換ファイルは、Cisco IOS デバイスによって作成された完全なコンフィギュレーション（**copy running-config** *destination-url* コマンドによって作成されたものなど）であることが必要です。置換ファイルを外部的に作成する場合は、Cisco IOS デバイスが作成するファイル形式に完全に準拠していなければなりません。**configure replace** コマンドを入力すると、現在の実行コンフィギュレーションが指定された置換コンフィギュレーションと比較され、一連の diff が生成されます。2 つのファイルの比較に使用されるアルゴリズムは、**show archive config differences** コマンドで使用されるものと同じです。置換コンフィギュレーションの状態になるよう、diff の結果が Cisco IOS パーサーによって適用されます。diff のみが適用されるため、現在の実行コンフィギュレーション上にすでに存在していた設定コマンドを再適用することにより生じる、潜在的なサービスの中断を避けられます。このアルゴリズムでは、順序に依存するコマンド（アクセス リストなど）へのコンフィギュレーション変更を、複数のパス プロセスを通して効果的に実行します。通常の環境では、コンフィギュレーション置換操作の完了に必要なパスは 3 つまでであり、ループ動作を防ぐためのパスは最大 5 つまでに制限されます。

copy *source-url* **running-config** 特権 EXEC コマンドは、保存された Cisco IOS コンフィギュレーション ファイルを実行コンフィギュレーションへコピーするためによく使用されます。**copy** *source-url* **running-config** コマンドを **configure replace** *target-url* 特権 EXEC コマンドの代わりに使用する場合、主な相違点として次の点に注意が必要です。

- **copy** *source-url* **running-config** コマンドはマージ動作であり、ソース ファイルと現在の実行コンフィギュレーションの両方のコマンドがすべて保持されます。このコマンドでは、現在の実行コンフィギュレーションにのみ含まれ、ソース ファイルには存在しないコマンドが削除されることはありません。これに対し、**configure replace** *target-url* コマンドでは、置換ファイルに存在しないコマンドは現在の実行コンフィギュレーションから削除され、現在の実行コンフィギュレーションに追加が必要なコマンドが追加されます。
- **copy** *source-url* **running-config** コマンドでは、現在の実行コンフィギュレーションにすでに存在しているかどうかにかかわらず、ソース ファイル中のすべてのコマンドが適用されます。このアルゴリズムは効率的でない上、場合によってはサービスの停止が発生します。これに

対し、**configure replace** *target-url* コマンドでは適用が必要なコマンドのみを適用し、現在の実行コンフィギュレーションに存在しているコマンドは再適用されません。

- **copy** *source-url* **running-config** コマンドでは部分的なコンフィギュレーション ファイルもコピー元として使用できますが、**configure replace** *target-url* コマンドの置換ファイルとして使用できるのは、完全な Cisco IOS コンフィギュレーション ファイルのみです。

コンフィギュレーション置換操作にロック機能が導入されました。**configure replace** コマンドが使用されると、コンフィギュレーション置換中、デフォルトで実行コンフィギュレーション ファイルがロックされます。このロック メカニズムによって、置換動作の実行中に他のユーザが実行コンフィギュレーションを変更しようとしたために、置換動作の不正終了が発生することを防止できます。**no lock** キーワードを **configure replace** コマンドの実行時に使用すると、実行コンフィギュレーションのロックをディセーブルにできます。

実行コンフィギュレーションのロックは、コンフィギュレーションの置換動作終了時に自動的にクリアされます。**show configuration lock** コマンドを使用すると、現在実行コンフィギュレーションに適用されているロックをすべて表示できます。

設定のロール バック

ロールバックの概念は、データベースの操作ではトランザクション プロセス モデルに由来します。データベース トランザクションでは、あるデータベースのテーブルに一連の変更を加えることがあります。その後、変更を実行する（変更を恒久的に適用する）か、変更をロールバックする（変更を破棄してテーブルを以前の状態に戻す）かを選択することになります。ここでロールバックが意味するのは、変更のログを含んだジャーナル ファイルが破棄され、何の変更も加えられないということです。ロールバック操作の結果として、加えた変更が適用される前の状態に戻ります。

configure replace コマンドを使用することで、以前のコンフィギュレーション状態へ戻ることが可能になり、コンフィギュレーション状態の保存後に加えた変更を効率的にロールバックさせることができます。Cisco IOS コンフィギュレーション ロールバックは、適用された一連の変更をもとにロールバック動作を行うのではなく、保存された Cisco コンフィギュレーション ファイルに基づいた特定のコンフィギュレーション状態へ戻るというコンセプトを採用しています。このコンセプトは、チェックポイント（データベースの保存されたバージョン）に特定の状態を保存しておくという、データベースの考え方に類似しています。

コンフィギュレーションのロールバック機能が必要な場合、コンフィギュレーションの変更に先立って Cisco IOS 実行コンフィギュレーションを保存する必要があります。そして、コンフィギュレーションへの変更を入力した後に、保存しておいたコンフィギュレーション ファイルを変更のロールバックに使用できます（**configure replace** *target-url* コマンドを使用）。保存された Cisco IOS コンフィギュレーション ファイルならどれでも置換コンフィギュレーションとして指定できるため、一部のロールバック モデルのように、ロールバックの数が制限されることもありません。

コンフィギュレーション ロールバック変更確認

コンフィギュレーション ロールバック変更確認機能により、コンフィギュレーション変更の実行に際して確認を要求するようオプションで設定できます。この確認が受信できない場合、コンフィギュレーションは変更が適用される前の状態に戻されます。このメカニズムは、ネットワーク デバイスとユーザまたは管理アプリケーションとの接続において、コンフィギュレーション変更に起因する切断を防止するものです。

コンフィギュレーションの置換およびロールバックの利点

- コンフィギュレーションの変更を効率的にロールバックさせて、以前のコンフィギュレーション状態へ戻ることが可能。
- スイッチをリロードしたり、CLI で実行コンフィギュレーション ファイルに加えた変更を手動で元に戻したりすることなく、現在の実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルと置換できるため、システムのダウンタイムが減少。
- 保存しておいたどの Cisco IOS コンフィギュレーション状態に戻すことも可能。
- 追加や削除が必要なコマンドだけが影響を受ける場合、スイッチに完全なコンフィギュレーション ファイルを適用することができるため、コンフィギュレーションの変更が簡素化。
- **configurereplace** コマンドを **copy***source-url***running-config** コマンドの代用として使用する場合、現在の実行コンフィギュレーションに存在しているコマンドを再度適用することがないため、効率が向上し、かつサービス停止のリスクを回避。

コンフィギュレーションの置換とロールバックの使用方法

コンフィギュレーション アーカイブの作成（CLI）

configure replace コマンドを使用するために、前提条件となる設定はありません。**configurereplace** コマンドと Cisco IOS コンフィギュレーション アーカイブおよび **archiveconfig** コマンドとの併用は任意ですが、コンフィギュレーション ロールバックの使用にあたっては大きな利点があります。**archive config** コマンドを使用する前に、コンフィギュレーション アーカイブを設定しておく必要があります。コンフィギュレーション アーカイブの特性を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **archive**
4. **path***url*
5. **maximum***number*
6. **time-period***minutes*
7. **end**
8. **archiveconfig**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードを有効化します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**archive** 例： `スイッチ(config)# archive`	アーカイブ コンフィギュレーション モードを開始します。
ステップ 4	**path***url* 例： `スイッチ(config-archive)# path flash:myconfiguration`	Cisco IOS コンフィギュレーション アーカイブの場所と、ファイル名のプレフィックスを指定します。 （注） パスのところでファイルの代わりにディレクトリを指定する場合、ディレクトリ名は path flash:/directory/ のように後ろにスラッシュを付ける必要があります。このスラッシュはファイル名の後ろでは必要ありません。ディレクトリを指定する場合にだけ使います。
ステップ 5	**maximum***number* 例： `スイッチ(config-archive)# maximum 14`	（任意）Cisco IOS コンフィギュレーション アーカイブに保存される実行コンフィギュレーションのアーカイブ ファイル数の上限値を設定します。 • *number* 引数は、Cisco IOS コンフィギュレーション アーカイブに保存される実行コンフィギュレーションのアーカイブ ファイル数

	コマンドまたはアクション	目的
		の上限値を示します。有効な値は 1 ～ 14 で、デフォルトは 10 です。 （注） このコマンドを使用する前に、**path** コマンドを設定して Cisco IOS コンフィギュレーション アーカイブの位置とファイル名プレフィックスを指定しておく必要があります。
ステップ 6	**time-period***minutes* 例： `スイッチ(config-archive)# time-period 1440`	（任意）Cisco IOS コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する間隔を設定します。 • Cisco IOS コンフィギュレーション アーカイブに現在の実行コンフィギュレーションのアーカイブ ファイルをどれほどの頻度で自動保存するかを、minutes 引数により分単位で指定します。 （注） このコマンドを使用する前に、**path** コマンドを設定して Cisco IOS コンフィギュレーション アーカイブの位置とファイル名プレフィックスを指定しておく必要があります。
ステップ 7	**end** 例： `スイッチ(config-archive)# end`	特権 EXEC モードに戻ります。
ステップ 8	**archiveconfig** 例： `スイッチ# archive config`	現在の実行コンフィギュレーション ファイルをコンフィギュレーション アーカイブに保存します。 （注） このコマンドを使用する前に、**path** コマンドを設定する必要があります。

コンフィギュレーションの置換またはロールバックの実行（CLI）

保存された Cisco IOS コンフィギュレーション ファイルで現在の実行コンフィギュレーション ファイルを置換するには、次の作業を実行します。

（注） この手順の前に、コンフィギュレーション アーカイブを作成しておく必要があります。詳細については、コンフィギュレーション アーカイブの作成（CLI）を参照してください。次に、現在の実行コンフィギュレーションで問題が生じた場合に、アーカイブしておいたコンフィギュレーションに戻す手順の詳細を示します。

手順の概要

1. **enable**
2. **configurereplace***target-url* [**nolock**] [**list**] [**force**] [**ignore case**] [**revert trigger** [**error**][**timer***minutes*] | **time***minutes*]]
3. **configurerevert**{**now**|**timer**{*minutes*| **idle***minutes*} }
4. **configureconfirm**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configurereplace***target-url* [**nolock**] [**list**] [**force**] [**ignore case**] [**revert trigger** [**error**][**timer***minutes*]	**time***minutes*]] 例： `スイッチ# configure replace flash: startup-config time 120`	保存しておいた Cisco IOS コンフィギュレーション ファイルで現在の実行コンフィギュレーション ファイルを置換します。 • *target - url* 引数は、**archiveconfig** コマンドで作成されたコンフィギュレーションファイルなど、現在の実行コンフィギュレーションと置換する、保存された Cisco IOS コンフィギュレーション ファイルの URL です（Cisco IOS ファイル システムでアクセス可能なもの）。 • **list** キーワードは、コンフィギュレーション置換動作のパスごとに、Cisco IOS ソフトウェア パーサーによって適用されるコマンド ラインのリストを表示します。実行されたパスの総数も表示されます。 • **force** キーワードは、現在の実行コンフィギュレーションから指定した Cisco IOS コンフィギュレーション ファイルへの置換を、確認プロンプトを出さずに実行します。 • **time***minutes* キーワードおよび引数は、現在の実行コンフィギュレーション ファイルの置換確認のために **configureconfirm** コマンドを入力する制限時間（分単位）を指定します。**configureconfirm** コマンドが指定の制限時間内に入力されない場合、コンフィギュレーション置換操作は自動的に戻されます（つまり、現在の実行コンフィギュレーション ファイルが **configurereplace** コマンド入力以前のコンフィギュレーション状態へと回復されます）。 • **nolock** キーワードは、コンフィギュレーション置換操作中に他のユーザが実行コンフィギュレーションを変更しないように実行コンフィギュレーション ファイルをロックする機能をオフにします。

	コマンドまたはアクション	目的
		• **reverttrigger** キーワードは、元のコンフィギュレーションへ戻すトリガーを次の内容から設定します。 • **error**：エラー時に元のコンフィギュレーションに戻します。 • **timer***minutes*：指定した時間が過ぎると元のコンフィギュレーションに戻します。 • **ignore case** キーワードで、コンフィギュレーションに確認コマンドの大文字と小文字の区別を無視させることができます。
ステップ 3	**configurerevert**{**now**|**timer**{*minutes*|**idle***minutes*} } 例： `スイッチ# configure revert now`	（任意）時間指定ロールバックをキャンセルしてロールバックを即時トリガーする、または時間指定ロールバックのパラメータをリセットするには、特権 EXEC モードで **configurerevert** コマンドを使用します。 • **now**：ロールバックをただちにトリガーします。 • **timer**：コンフィギュレーションを元に戻すタイマーをリセットします。 • 元に戻す時間を分単位で新たに指定するには、*minutes* 引数を **timer** キーワードとともに使用します。 • 保存されたコンフィギュレーションに戻すまでに、操作が行われないアイドル時間を最大どれほど長く許容できるかを設定するには、分単位の時間とともに **idle** キーワードを使用します。
ステップ 4	**configureconfirm** 例： `スイッチ# configure confirm`	（任意）保存しておいた Cisco IOS コンフィギュレーション ファイルの現在の実行コンフィギュレーション ファイルへの置換を確認します。 （注） このコマンドは、**time***seconds* キーワードと **configurereplace** コマンドの引数が指定されているときのみ使用します。
ステップ 5	**exit** 例： `スイッチ# exit`	ユーザ EXEC モードに戻ります。

機能のモニタリングおよびトラブルシューティング（CLI）

コンフィギュレーションの置換とロールバック機能をモニタおよびトラブルシューティングするには、この手順を実行します。

手順の概要

1. **enable**
2. **showarchive**
3. **debugarchiveversioning**
4. **debugarchiveconfigtimestamp**
5. **exit**

手順の詳細

ステップ 1 **enable**

このコマンドを使用して、特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

例：

```
スイッチ> enable
スイッチ#
```

ステップ 2 **showarchive**

Cisco IOS コンフィギュレーション アーカイブに保存されているファイルに関する情報を表示するには、次のコマンドを使用します。

例：

```
スイッチ# show archive
There are currently 1 archive configurations saved.
The next archive file will be named flash:myconfiguration-2
 Archive #  Name
   0
   1       flash:myconfiguration-1 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10
   11
   12
   13
   14
```

次に、実行コンフィギュレーションのアーカイブ ファイルをいくつか保存した状態で **showarchive** コマンドを使用した場合の出力例を示します。この例では、保存されるアーカイブファイルの最大数が3に設定されています。

例：

```
スイッチ# show archive
There are currently 3 archive configurations saved.
```

```
The next archive file will be named flash:myconfiguration-8
 Archive #  Name
   0
   1       :Deleted
   2       :Deleted
   3       :Deleted
   4       :Deleted
   5       flash:myconfiguration-5
   6       flash:myconfiguration-6
   7       flash:myconfiguration-7 <- Most Recent
   8
   9
   10
   11
   12
   13
   14
```

ステップ 3 **debugarchiveversioning**

このコマンドを使用して、Cisco IOS コンフィギュレーション アーカイブのアクティビティのデバッグを有効にして、コンフィギュレーションの置換とロールバックをモニタおよびトラブルシューティングします。

例：

```
スイッチ# debug archive versioning
Jan  9 06:46:28.419:backup_running_config
Jan  9 06:46:28.419:Current = 7
Jan  9 06:46:28.443:Writing backup file flash:myconfiguration-7
Jan  9 06:46:29.547: backup worked
```

ステップ 4 **debugarchiveconfigtimestamp**

このコマンドを使用して、コンフィギュレーション置換操作の各必須段階の処理時間、および操作中のコンフィギュレーション ファイルのサイズのデバッグをイネーブルにします。

例：

```
スイッチ# debug archive config timestamp
スイッチ# configure replace flash:myconfiguration force
Timing Debug Statistics for IOS Config Replace operation:
       Time to read file usbflash0:sample_2.cfg = 0 msec (0 sec)
       Number of lines read:55
       Size of file        :1054
Starting Pass 1
       Time to read file system:running-config = 0 msec (0 sec)
       Number of lines read:93
       Size of file        :2539
       Time taken for positive rollback pass = 320 msec (0 sec)
       Time taken for negative rollback pass = 0 msec (0 sec)
       Time taken for negative incremental diffs pass = 59 msec (0 sec)
       Time taken by PI to apply changes = 0 msec (0 sec)
       Time taken for Pass 1 = 380 msec (0 sec)
Starting Pass 2
       Time to read file system:running-config = 0 msec (0 sec)
       Number of lines read:55
       Size of file        :1054
       Time taken for positive rollback pass = 0 msec (0 sec)
       Time taken for negative rollback pass = 0 msec (0 sec)
       Time taken for Pass 2 = 0 msec (0 sec)
```

```
Total number of passes:1
Rollback Done
```

ステップ 5 **exit**

このコマンドを使用して、ユーザ EXEC モードに戻ります。

例：

```
スイッチ# exit
スイッチ>
```

コンフィギュレーションの置換とロールバックの設定例

コンフィギュレーション アーカイブの作成

次の例は、Cisco IOS コンフィギュレーション アーカイブの初期設定を実行する方法を示しています。この例では、flash:myconfiguration がコンフィギュレーション アーカイブの保存位置およびファイル名のプレフィックスとして設定され、保存するアーカイブ ファイルが最大 10 個に設定されます。

```
configure terminal
!
archive
 path flash:myconfiguration
 maximum 10
end
```

現在の実行コンフィギュレーションを保存された Cisco IOS コンフィギュレーション ファイルで置換する

次の例では、flash:myconfiguration という名前で保存された Cisco IOS コンフィギュレーション ファイルで現在の実行コンフィギュレーションを置換する方法を示します。**configure replace** コマンドでは、確認プロンプトでインタラクティブに操作を進めます。

```
スイッチ# configure replace flash:myconfiguration
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
```

次の例では、コンフィギュレーション置換操作中に適用されるコマンド ラインを表示するために、**list** キーワードを指定しています。

```
スイッチ# configure replace flash:myconfiguration list
```

```
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
!Pass 1
!List of Commands:
no snmp-server community public ro
snmp-server community mystring ro

end
Total number of passes: 1
Rollback Done
```

スタートアップ コンフィギュレーション ファイルへの復帰

次の例に、**configure replace** コマンドを使用して Cisco IOS スタートアップ コンフィギュレーション ファイルへ復帰する方法を示します。この例は、オプションの **force** キーワードを使用して、インタラクティブ ユーザ プロンプトをオーバーライドする方法を示しています:

```
スイッチ# configure replace flash:startup-config force
Total number of passes: 1
Rollback Done
```

configure confirm コマンドを使用したコンフィギュレーション置換操作の実行

次に、**configure replace** コマンドを **time***minutes* キーワードおよび引数と共に使用する例を示します。現在実行中のコンフィギュレーション ファイルの置換を実行するには、指定の制限時間内に **configure confirm** コマンドを入力する必要があります。**configure confirm** コマンドが指定の制限時間内に入力されない場合、コンフィギュレーション置換操作は自動的に戻されます（つまり、現在実行中のコンフィギュレーション ファイルが **configure replace** コマンド入力以前のコンフィギュレーション状態へと回復されます）。

```
スイッチ# configure replace flash:startup-config time 120
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
スイッチ# configure confirm
```

次に、**configure revert** コマンドを **timer** キーワードとともに使用する例を示します。時間指定ロールバックをキャンセルしてロールバックを即時トリガーする、または時間指定ロールバックのパラメータをリセットするには、**configure revert** コマンドを入力する必要があります。

```
スイッチ# configure revert timer 100
```

コンフィギュレーション ロールバック操作の実行

次の例は、現在実行中のコンフィギュレーションへの変更を行い、その変更をロールバックする方法を示しています。コンフィギュレーション ロールバック操作の一部として、ファイルに変更を加える前に現在の実行コンフィギュレーションを保存する必要があります。この例では、現在

実行中のコンフィギュレーションの保存に **archive config** コマンドが使用されています。**configure replace** コマンドで生成された出力は、ロールバック操作を完了するために 1 つのパスのみが実行されたことを示します。

（注） **archive config** コマンドを使用する前に、**path** コマンドで Cisco IOS コンフィギュレーション アーカイブのファイルの位置とファイル名のプレフィックスを指定する必要があります。

次のように、設定アーカイブの現在実行中のコンフィギュレーションを保存します。

```
archive config
```

それから、次の例に示すようにコンフィギュレーションの変更を入力します。

```
configure terminal
!
user netops2 password rain
user netops3 password snow
exit
```

実行コンフィギュレーション ファイルに変更を加えた後、それらの変更をロールバックさせて、変更前のコンフィギュレーションに戻したくなったとします。**show archive** コマンドは、交換ファイルとして使用される設定のバージョンを確認するために使用されます。次の例に示すように、**configure replace** コマンドは交換コンフィギュレーション ファイルへ戻すために使用されます。

```
スイッチ# show archive
There are currently 1 archive configurations saved.
The next archive file will be named flash:myconfiguration-2
 Archive #  Name
   0
   1       flash:myconfiguration-1 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10
スイッチ# configure replace flash:myconfiguration-1
Total number of passes: 1
Rollback Done
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
設定ロック	『*Exclusive Configuration Change Access and Access Session Locking*』

関連項目	マニュアル タイトル
コンフィギュレーション ファイルを管理するためのコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
コンフィギュレーション ファイルの管理についての情報	*Managing Configuration Files*

エラー メッセージ デコーダ

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

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

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

第 99 章

フラッシュ ファイル システムの操作

- フラッシュ ファイル システムについて，2289 ページ
- 使用可能なファイル システムの表示，2290 ページ
- デフォルト ファイル システムの設定，2292 ページ
- ファイル システムのファイルに関する情報の表示，2293 ページ
- ディレクトリの変更および作業ディレクトリの表示（CLI），2293 ページ
- ディレクトリの作成（CLI），2295 ページ
- ファイルのコピー，2296 ページ
- ファイルの作成、表示および抽出（CLI），2298 ページ
- その他の参考資料，2300 ページ

フラッシュ ファイル システムについて

フラッシュ ファイル システムは、ファイルを格納できる単一のフラッシュ デバイスです。ソフトウェアバンドルおよびコンフィギュレーションファイルの管理に役立つ複数のコマンドも備えています。スイッチのデフォルトのフラッシュ ファイル システムは flash: です。

アクティブなスイッチまたは任意のスタック メンバから参照できる flash: は、ローカル フラッシュデバイスを指します。これは、ファイルシステムが参照されているのと同じスイッチに接続されているデバイスです。スイッチ スタックでは、さまざまなスタック メンバからの各フラッシュ デバイスを、アクティブなスイッチから参照できます。これらのフラッシュ ファイル システムの名前には、対応するスイッチ メンバ番号が含まれています。たとえば、アクティブなスイッチから参照できる flash-3: は、スタック メンバ 3 にある flash: と同じファイル システムを指します。スイッチ スタックにあるフラッシュ ファイル システムを含むすべてのファイル システムのリストを表示するには、**show file systems** 特権 EXEC コマンドを使用します。

スイッチ スタックでは、一度に 1 人のユーザのみが、ソフトウェア のバンドルおよび設定ファイルを管理できます。

使用可能なファイル システムの表示

スイッチ で使用可能なファイル システムを表示するには、**show file systems** 特権 EXEC コマンドを使用します（次のスタンドアロン スイッチ の例を参照）。

```
スイッチ# show file systems
File Systems:
     Size(b)     Free(b)      Type    Flags   Prefixes
*   15998976     5135872     flash     rw     flash:
           -           -    opaque     rw     bs:
           -           -    opaque     rw     vb:
      524288      520138     nvram     rw     nvram:
           -           -   network     rw     tftp:
           -           -    opaque     rw     null:
           -           -    opaque     rw     system:
           -           -    opaque     ro     xmodem:
           -           -    opaque     ro     ymodem:
```

次の例では、スイッチ スタックを示します。この例では、アクティブな スイッチ がスタック メンバ 1 です。スタック メンバ 2 のファイル システムはフラッシュ 2 として表示されます。スタック メンバ 3 のファイル システムはフラッシュ 3 として表示されます。メンバ数 9 のスタックの場合、スタック メンバ 9 のファイルは、フラッシュ 9 として同様にそれぞれ表示されます。また、この例では、次のように、crashinfo ディレクトリと、アクティブな スイッチ に接続された USB フラッシュ ドライブも示します。

```
スイッチ# show file systems
File Systems:
      Size(b)       Free(b)      Type   Flags   Prefixes
     145898496      5479424      disk     rw    crashinfo:crashinfo-1:
     248512512     85983232      disk     rw    crashinfo-2:stby-crashinfo:
     146014208     17301504      disk     rw    crashinfo-3:
     146014208            0      disk     rw    crashinfo-4:
     146014208      1572864      disk     rw    crashinfo-5:
     248512512     30932992      disk     rw    crashinfo-6:
     146014208      6291456      disk     rw    crashinfo-7:
     146276352     15728640      disk     rw    crashinfo-8:
     146276352     73400320      disk     rw    crashinfo-9:
*    741621760    481730560      disk     rw    flash:flash-1:
    1622147072   1360527360      disk     rw    flash-2:stby-flash:
     729546752    469762048      disk     rw    flash-3:
     729546752    469762048      disk     rw    flash-4:
     729546752    469762048      disk     rw    flash-5:
    1622147072   1340604416      disk     rw    flash-6:
     729546752    469762048      disk     rw    flash-7:
    1749549056   1487929344      disk     rw    flash-8:
    1749549056   1487929344      disk     rw    flash-9:
             0            0      disk     rw    unix:
             -            -      disk     rw    usbflash0:usbflash0-1:
             -            -      disk     rw    usbflash0-2: stby-usbflash0:
             -            -      disk     rw    usbflash0-3:
             -            -      disk     rw    usbflash0-4:
             -            -      disk     rw    usbflash0-5:
             -            -      disk     rw    usbflash0-6:
             -            -      disk     rw    usbflash0-7:
             -            -      disk     rw    usbflash0-8:
             -            -      disk     rw    usbflash0-9:
             0            0      disk     ro    webui:
             -            -    opaque     rw    system:
             -            -    opaque     rw    tmpsys:
       2097152      2055643     nvram     rw    stby-nvram:
             -            -     nvram     rw    stby-rcsf:
             -            -    opaque     rw    null:
             -            -    opaque     ro    tar:
```

```
        -           -   network     rw    tftp:
  2097152     2055643     nvram     rw    nvram:
        -           -    opaque     wo    syslog:
        -           -   network     rw    rcp:
        -           -   network     rw    http:
        -           -   network     rw    ftp:
        -           -   network     rw    scp:
        -           -   network     rw    https:
        -           -    opaque     ro    cns:
        -           -    opaque     rw    revrcsf:
```

表 ***166*** : ***show file systems*** のフィールドの説明

フィールド	値
Size(b)	ファイル システムのメモリ サイズ（バイト単位）です。
Free(b)	ファイルシステムの空きメモリ サイズ（バイト単位）です。
Type	ファイル システムのタイプです。 **disk**：ファイル システムは、フラッシュ メモリ デバイス、USB フラッシュ、crashinfo ファイル用です。 **network**：ファイル システムは、FTP サーバや HTTP サーバなどのネットワーク デバイス用です。 **nvram**：ファイルシステムはNVRAM（不揮発性RAM）デバイス用です。 **opaque**：ファイルシステムは、ローカルに生成されたpseudoファイルシステム（systemなど）、またはダウンロードインターフェイス（brimux など）です。 **unknown**：ファイル システムのタイプは不明です。
Flags	ファイル システムの権限です。 **ro**：読み取り専用です。 **rw**：読み取りおよび書き込みです。 **wo**：書き込み専用です。

フィールド	値
Prefixes	ファイル システムのエイリアスです。 **crashinfo**：crashinfo ファイルです。 **flash**：フラッシュ ファイル システムです。 **ftp**：FTP サーバです。 **http**：HTTP サーバです。 **https**：セキュア HTTP サーバです。 **nvram**：NVRAM です。 **null**：コピーのヌル宛先です。リモート ファイルをヌルへコピーして、サイズを判別できます。 **rcp**：Remote Copy Protocol（RCP）サーバです。 **scp**：Session Control Protocol（SCP）サーバです。 **system**：実行コンフィギュレーションを含むシステム メモリが格納されています。 **tftp**：TFTP ネットワーク サーバです。 **usbflash0**：USB フラッシュ メモリです。 **xmodem**：XMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。 **ymodem:** ：YMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。

デフォルト ファイル システムの設定

デフォルトのファイルシステムとして使用されるファイルシステムまたはディレクトリを指定するには、**cd** *filesystem:* 特権 EXEC コマンドを使用します。デフォルト ファイル システムを設定すると、関連するコマンドを実行するときに *filesystem:* 引数を省略できます。たとえば、オプションの filesystem: 引数を持つすべての特権 EXEC コマンドでは、**cd** コマンドで指定されたファイル システムが使用されます。

デフォルトでは、デフォルト ファイル システムは *flash:* です。

cd コマンドで指定された現在のデフォルトのファイル システムを表示するには、**pwd** 特権 EXEC コマンドを使用します。

ファイル システムのファイルに関する情報の表示

ファイル システムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイル システムに同じ名前のコンフィギュレーション ファイルが格納されていないことを確認できます。同様に、フラッシュ コンフィギュレーション ファイルを別の場所にコピーする前に、ファイル名を確認して、その名前を別のコマンドで使用できます。ファイル システムのファイルに関する情報を表示するには、次の表に記載する特権 EXEC コマンドのいずれかを使用します。

表 *167*：ファイルに関する情報を表示するためのコマンド

コマンド	説明
dir [/all] [*filesystem:filename***]**	ファイル システムのファイル リストを表示します。
show file systems	ファイル システムのファイルごとの詳細を表示します。
show file information*file-url*	特定のファイルに関する情報を表示します。
show file descriptors	開いているファイルの記述子のリストを表示します。ファイル記述子は開いているファイルの内部表現です。このコマンドを使用して、別のユーザによってファイルが開かれているかどうかを調べることができます。

たとえば、ファイル システムのすべてのファイルのリストを表示するには、次のように **dir** 特権 EXEC コマンドを使用します。

```
スイッチ# dir flash:
Directory of flash:/
7386  -rwx     2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
7378  drwx        4096 Jan 23 2013 09:35:11 +00:00 mnt
7385  -rw-   221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
7389  -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
712413184 bytes total (445063168 bytes free)
スイッチ#
```

ディレクトリの変更および作業ディレクトリの表示（CLI）

ディレクトリを変更し、作業ディレクトリを表示するには、次の手順を実行します。

手順の概要

1. **enable**
2. **dir***filesystem:*
3. **cd***directory_name*
4. **pwd**
5. **cd**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**dir***filesystem:* 例： `スイッチ# dir flash:`	指定されたファイル システムのディレクトリを表示します。 *filesystem:* には、システム ボードのフラッシュ デバイスの flash: を使用します。 スタックのスイッチメンバのフラッシュ パーティションにアクセスするには、flash-*n* を使用します。*n* は、スタック メンバ番号を表します。例えば、flash-4。
ステップ 3	**cd***directory_name* 例： `スイッチ# cd new_configs`	指定されたディレクトリへ移動します。 コマンド例では、*new_configs* という名前のディレクトリに移動する方法を示します。
ステップ 4	**pwd** 例： `スイッチ# pwd`	作業ディレクトリを表示します。
ステップ 5	**cd** 例： `スイッチ# cd`	デフォルト ディレクトリに移動します。

ディレクトリの作成（CLI）

特権 EXEC モードを開始して、ディレクトリを作成するには次の手順を実行します。

手順の概要

1. **dir***filesystem:*
2. **mkdir***directory_name*
3. **dir***filesystem:*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dir***filesystem:* 例： `スイッチ# dir flash:`	指定されたファイル システムのディレクトリを表示します。 *filesystem:* には、システム ボードのフラッシュ デバイスの flash: を使用します。
ステップ 2	**mkdir***directory_name* 例： `スイッチ# mkdir new_configs`	新しいディレクトリを作成します。スラッシュ (/) 間に指定できるディレクトリ名は最大 45 文字で、大文字と小文字の区別があります。ディレクトリ名には制御文字、スペース、スラッシュ、引用符、セミコロン、またはコロンは使用できません。
ステップ 3	**dir***filesystem:* 例： `スイッチ# dir flash:`	入力を確認します。

ディレクトリの削除

ディレクトリを、その内部のすべてのファイルおよびサブディレクトリとともに削除するには、**delete /force /recursive** *filesystem:/file-url* 特権 EXEC コマンドを使用します。

名前で指定されたディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。

filesystem でシステム ボードのフラッシュ デバイスを指定する場合は、**flash:** を使用します。*file-url* には、削除するディレクトリの名前を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

注意 ディレクトリが削除された場合、その内容は回復できません。

ファイルのコピー

送信元から宛先にファイルをコピーするには、**copy** *source-url destination-url* 特権 EXEC コマンドを使用します。送信元および宛先の URL には、**running-config** および **startup-config** キーワード ショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドを実行すると、現在の実行コンフィギュレーション ファイルがフラッシュ メモリの NVRAM セクションに保存され、システム初期化中のコンフィギュレーションとして使用されます。

XMODEM または YMODEM プロトコルを使用するネットワーク マシンのファイルに対する送信元として特殊なファイル システム（**xmodem:**、**ymodem:**）を指定し、そこからコピーすることもできます。

ネットワーク ファイル システムの URL には、ftp: 、rcp: 、tftp などがあり、構文は次のとおりです。

- FTP：ftp:[[//username [:password]@location]/directory]/filename
- RCP：rcp:[[//username@location]/directory]/filename
- TFTP：tftp:[[//location]/directory]/filename

ローカルにある書き込み可能なファイル システムには flash: などがあります。

送信元および宛先の組み合わせによっては、無効な場合があります。特に、次に示す組み合わせの場合は、コピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- デバイスから同じ名前のデバイスへ（たとえば、**copy flash: flash:** コマンドは無効）

スタック内のスイッチから同じスタックの別のスイッチにファイルをコピーする

スタック内のあるスイッチから同じスタック内の別のスイッチにファイルをコピーするには、**flash-X:** 表記を使用します。**X** はスイッチ番号です。

スタック内のすべてのスイッチを表示するには、9 メンバー スイッチ スタックの例のように、特権 EXEC モードで **show switch** コマンドを使用します。

```
スイッチ# show switch
Switch/Stack Mac Address : 0006.f6b9.b580 - Local Mac Address Mac persistency wait time:
Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Active   0006.f6b9.b580     15     P3B     Ready
 2       Standby  0006.f6ba.0c80     14     P3B     Ready
 3       Member   0006.f6ba.3300     7      P3B     Ready
```

```
 4       Member   0006.f6b9.df80     6      P3B     Ready
 5       Member   0006.f6ba.3880     13     P1A     Ready
 6       Member   1ce6.c7b6.ef00     4      PP      Ready
 7       Member   2037.06ce.2580     3      P2A     Ready
 8       Member   2037.0653.7e00     2      P5A     Ready
 9       Member   2037.0653.9280     1      P5B     Ready
```

特定のスイッチのコピー可能なすべてのファイル システムを表示するには、次に示す 5 メンバー スタックの例のように、**copy** コマンドを使用します。

```
スイッチ# copy flash: ?
  crashinfo-1:     Copy to crashinfo-1: file system
  crashinfo-2:     Copy to crashinfo-2: file system
  crashinfo-3:     Copy to crashinfo-3: file system
  crashinfo-4:     Copy to crashinfo-4: file system
  crashinfo-5:     Copy to crashinfo-5: file system
  crashinfo:       Copy to crashinfo: file system
  flash-1:         Copy to flash-1: file system
  flash-2:         Copy to flash-2: file system
  flash-3:         Copy to flash-3: file system
  flash-4:         Copy to flash-4: file system
  flash-5:         Copy to flash-5: file system
  flash:           Copy to flash: file system
  ftp:             Copy to ftp: file system
  http:            Copy to http: file system
  https:           Copy to https: file system
  null:            Copy to null: file system
  nvram:           Copy to nvram: file system
  rcp:             Copy to rcp: file system
  revrcsf:         Copy to revrcsf: file system
  running-config   Update (merge with) current system configuration
  scp:             Copy to scp: file system
  startup-config   Copy to startup configuration
  stby-crashinfo:  Copy to stby-crashinfo: file system
  stby-flash:      Copy to stby-flash: file system
  stby-nvram:      Copy to stby-nvram: file system
  stby-rcsf:       Copy to stby-rcsf: file system
  stby-usbflash0:  Copy to stby-usbflash0: file system
  syslog:          Copy to syslog: file system
  system:          Copy to system: file system
  tftp:            Copy to tftp: file system
  tmpsys:          Copy to tmpsys: file system
  usbflash0-1:     Copy to usbflash0-1: file system
  usbflash0-2:     Copy to usbflash0-2: file system
  usbflash0-3:     Copy to usbflash0-3: file system
  usbflash0-4:     Copy to usbflash0-4: file system
  usbflash0-5:     Copy to usbflash0-5: file system
  usbflash0:       Copy to usbflash0: file system

スイッチ#
```

次の例では、スイッチ 2 のフラッシュ パーティションに保存されているコンフィギュレーション ファイルをスイッチ 4 のフラッシュ パーティションにコピーする方法を示しています。スイッチ 2 とスイッチ 4 が同じスタック内にあるとします。

```
スイッチ# copy flash-2:config.txt flash-4:config.txt
```

ファイルの削除

フラッシュ メモリ デバイスのファイルが不要になった場合は、そのファイルを永久に削除できます。指定されたフラッシュ デバイスからファイルまたはディレクトリを削除するには、**delete** [**/force**] [**/recursive**] [*filesystem:*]*/file-url* 特権 EXEC コマンドを使用します。

ディレクトリを、その内部のすべてのサブディレクトリやファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**/force** キーワードおよび **/recursive** キーワードを使用して、**archive download-sw** コマンドを使用してインストールされ、不要になった古いソフトウェアイメージを削除します。

filesystem: オプションを省略すると、スイッチは **cd** コマンドで指定したデフォルトのデバイスを使用します。*file-url* には、削除するファイルのパス（ディレクトリ）および名前を指定します。

ファイルを削除しようとすると、削除の確認を求めるプロンプトが表示されます。

注意 ファイルが削除された場合、その内容は回復できません。

ここでは、デフォルトのフラッシュ メモリ デバイスからファイル *myconfig* を削除する例を示します。

```
スイッチ# delete myconfig
```

ファイルの作成、表示および抽出（CLI）

ファイルを作成してそこにファイルを書き込んだり、ファイル内のファイルをリスト表示したり、ファイルからファイルを抽出したりできます（次の項を参照）。

ファイルの作成、内容の表示、およびファイルの抽出を行うには、特権 EXEC コマンドで次の手順を実行します。

手順の概要

1. **archive tar /create***destination-url***flash:***/file-url*
2. **archive tar /table***source-url*
3. **archive tar /xtract***source-url* **flash:***/file-url* [*dir/file...*]
4. **more** [**/ascii** | **/binary** | **/ebcdic**] */file-url*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**archive tar /create***destination-url***flash:***/file-url* 例： `スイッチ# archive tar /create tftp:172.20.10.30/saved. flash:/new-configs`	ファイルを作成し、そこにファイルを追加します。 destination-url には、ローカルまたはネットワーク ファイル システムの宛先 URL のエイリアス、および作成するファイルの名前を指定します。 • ローカル フラッシュ ファイル システム構文 **flash:** • FTP 構文

	コマンドまたはアクション	目的
		ftp:[[//*username*[:*password*]@*location*]/*directory*]/*-filename*. • RCP 構文 **rcp**:[[//*username@location*]/*directory*]/*-filename*. • TFTP 構文 **tftp**:[[//*location*]/*directory*]/*-filename*. **flash:/file-url**/*file-url* には、ローカル フラッシュ ファイル システム上の、新しいファイルが作成される場所を指定します。送信元ディレクトリ内に格納されている任意のファイルまたはディレクトリの一覧を指定して、新しいファイルに追加することもできます。何も指定しないと、このレベルにおけるすべてのファイルおよびディレクトリが、新規に作成されたファイルに書き込まれます。
ステップ 2	**archive tar /table***source-url* 例： `スイッチ# archive tar /table flash: /new_configs`	ファイルの内容を表示します。 *source-url* には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。*-filename.* は、表示するファイルです。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システム構文 **flash:** • FTP 構文 **ftp**:[[//*username*[:*password*]@*location*]/*directory*]/*-filename*. • RCP 構文 **rcp**:[[//*username@location*]/*directory*]/*-filename*. • TFTP 構文 **tftp**:[[//*location*]/*directory*]/*-filename*. ファイルのあとにファイルまたはディレクトリのリストを指定して、ファイルの表示を制限することもできます。指定したファイルだけが表示されます。何も指定しないと、すべてのファイルおよびディレクトリが表示されます。
ステップ 3	**archive tar /xtract***source-url* **flash:**/*file-url* [*dir/file...*] 例： `スイッチ# archive tar /xtract tftp:/172.20.10.30/saved. flash:/new-configs`	ファイルをフラッシュ ファイル システム上のディレクトリに抽出します。 *source-url* には、ローカル ファイル システムの送信元 URL のエイリアスを指定します。*-filename.* は、ファイルの抽出元のファイルです。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システム構文 **flash:**

	コマンドまたはアクション	目的
		• FTP 構文 **ftp**:[[//*username*[:*password*]@*location*]/*directory*]/*-filename*. • RCP 構文 **rcp**:[[//*username@location*]/*directory*]/*-filename*. • TFTP 構文 **tftp**:[[//*location*]/*directory*]/*-filename*. **flash:/file-url[dir/file...]**/*file-url*[*dir/file...*] には、ファイルの抽出元にするローカルフラッシュ ファイル システム上の場所を指定します。抽出対象のファイル内のファイルまたはディレクトリのリストを指定するには、*dir/file...* オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。
ステップ 4	**more** [**/ascii** | **/binary** | **/ebcdic**] */file-url* 例： `スイッチ# more flash:/new-configs`	リモート ファイル システム上のファイルを含めて、読み取り可能なファイルの内容を表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
flash: ファイル システムの管理コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

エラー メッセージ デコーダ

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

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

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

第 100 章

Cisco IOS XE ソフトウェア バンドルの使用

- ソフトウェアのバンドルとパッケージについて，2303 ページ
- スイッチでのバンドルおよびパッケージ ファイルの場所，2303 ページ
- Cisco IOS XE ソフトウェアのアップグレード，2304 ページ
- その他の参考資料，2313 ページ

ソフトウェアのバンドルとパッケージについて

Cisco IOS XE ソフトウェア バンドルには一連の Cisco IOS XE パッケージ（.pkg）ファイルが含まれています。スイッチにパッケージファイルをインストールできます。また、IOS XE バンドルからスイッチを起動することもできます。

Cisco IOS XE バンドル（.bin ファイル）の内容に関する情報を表示するには、特権 EXEC モードで **show software package** コマンドを使用します。IOS XE パッケージ（.pkg ファイル）に関する情報を表示する場合も、このコマンドを使用します。

スイッチでのバンドルおよびパッケージ ファイルの場所

スイッチがインストール モードで実行されると、Cisco IOS XE パッケージ（.pkg）ファイルとプロビジョニング ファイル（packages.conf）は、システム ボードのフラッシュ メモリ（flash:）に保存されます。スイッチがバンドル モードで実行されると、ブートした Cisco IOS XE ソフトウェア バンドル（.bin）ファイルは、システム ボードのフラッシュ メモリ（flash:）または USB フラッシュ メモリ（usbflash0:）に保存されます。

現在スイッチ上で実行中のプロビジョニング ソフトウェアに関する情報を表示するには、**show version** 特権 EXEC コマンドを使用します。ディスプレイでは、以下から始まる行をチェックします。

```
System bundle file is....
```

スイッチがインストール モードで実行されると、この行には、ブートした Cisco IOS XE プロビジョニング ファイルの名前と場所（通常 flash:packages.conf）が表示されます。

スイッチがバンドル モードで実行されると、この行にはブートした Cisco IOS XE バンドル ファイルの名前と場所が表示されます。

スイッチで実行中の Cisco IOS XE パッケージ ファイルに関する情報を表示するには、**show version running** 特権 EXEC コマンドを使用します。

スイッチがインストール モードで実行されると、このコマンドではブートしたプロビジョニング ファイルに含まれる一連のパッケージ ファイルに関する情報を表示します。

スイッチがバンドル モードで実行されると、このコマンドではブートした Cisco IOS XE ソフトウェア バンドルに含まれる一連のパッケージ ファイルに関する情報を表示します。

（注） Usbflash0: の場合、デフォルトのフォーマットは FAT16 ですが、FAT32 フォーマットもサポートされます。

```
スイッチ# format usbflash0: ?
  FAT16   FAT16  filesystem type
  FAT32   FAT32  filesystem type
```

Cisco IOS XE ソフトウェアのアップグレード

Cisco IOS XE ソフトウェアをアップグレードするために使用する方法は、スイッチが動作しているのがインストール モードかバンドル モードかによって異なります。

Cisco IOS XE ソフトウェアのアップグレード：インストール モード

スイッチがインストール モードで実行されているときに Cisco IOS XE ソフトウェアをアップグレードするには、**software install** 特権 EXEC コマンドを使用して、新しいソフトウェア バンドル ファイルからパッケージをインストールします。ソフトウェア バンドルは、ローカルのストレージ メディアからインストールすることも、TFTP または FTP を使用してネットワーク経由でインストールすることもできます。

software install コマンドは指定された送信元バンドル ファイルからパッケージ ファイルを展開し、ローカルの flash: ストレージ デバイスにコピーします。送信元バンドルが tftp: または ftp: URL として指定されている場合、バンドル ファイルが最初にスイッチのメモリ（RAM）にダウンロードされます。バンドル ファイルはローカルのストレージ メディアにはコピーされません。

パッケージ ファイルが展開され flash: にコピーされたら、実行されているプロビジョニング ファイル（flash:packages.conf）が新規インストール パッケージを反映するよう更新され、スイッチではリロードのプロンプトが表示されます。

（注） **software install** コマンドは、スイッチがバンドル モードで動作している場合はサポートされません。**software expand** 特権 EXEC コマンドを使用して、スイッチをバンドル モードからインストール モードに変換します。

Cisco IOS XE ソフトウェア インストール モードのアップグレードの例

この例では、**software install file** コマンドを使用して TFTP サーバにある Cisco IOS XE バンドルからパッケージを展開およびコピーし、新しいイメージにアップグレードする方法を示しています。

```
スイッチ#
software install file
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
Preparing install operation ...
[1]: Downloading file
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 to active switch 1
[1]: Finished downloading file
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 to active switch 1
[1]: Starting install operation
[1]: Expanding bundle cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
[1]: Copying package files
[1]: Package files copied
[1]: Finished expanding bundle
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
[1]: Verifying and copying expanded package files to flash:
[1]: Verified and copied expanded package files to flash:
[1]: Starting compatibility checks
[1]: Finished compatibility checks
[1]: Starting application pre-installation processing
[1]: Finished application pre-installation processing
[1]: Old files list:
Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[1]: New files list:
Added cat3k_caa-base.SPA.03.02.00.SE.pkg
Added cat3k_caa-drivers.SPA.03.02.00.SE.pkg
Added cat3k_caa-infra.SPA.03.02.00SE.pkg
Added cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
Added cat3k_caa-platform.SPA.03.02.00.SE.pkg
Added cat3k_caa-wcm.SPA.03.02.00.SE.pkg
[1]: Creating pending provisioning file
[1]: Finished installing software. New software will load on reboot.
[1]: Setting rollback timer to 45 minutes
[1]: Do you want to proceed with reload? [yes/no]:
```

Cisco IOS XE ソフトウェアのアップグレード：バンドル モード

スイッチがバンドル モードで動作しているときに Cisco IOS XE ソフトウェアをアップグレードするには、次の手順を実行します。

1. バンドル ファイルをローカルのストレージ メディアにダウンロードします。
2. **boot system** グローバル コンフィギュレーション コマンドを、バンドル ファイルを指すよう設定します。
3. スイッチをリロードします。

Cisco IOS XE ソフトウェア バンドル モードのアップグレード例

この例では、バンドル モードで実行中のスイッチの Cisco IOS XE ソフトウェアをアップグレードする手順を示します。これはバンドル ファイルをフラッシュにコピーするために **copy** コマンドを使用する方法を示します。バンドル ファイルを指示するようにブートシステム変数を設定し、実行コンフィギュレーションのコピーを保存し、最後に、スイッチをリロードします。

```
スイッチ#
copy
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 flash:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Accessing
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...Loading
/tftpboot/cstohs/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
from 172.19.211.47 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK - 220766688 bytes]
220766688 bytes copied in 124.330 secs (1775651 bytes/sec)

スイッチ#
スイッチ#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
スイッチ(config)# boot system switch all
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
スイッチ(config)# end
スイッチ#

*Nov 19 14:02:42.441: %SYS-5-CONFIG_I: Configured from console by console

スイッチ#
スイッチ# write memory
Building configuration...
Compressed configuration from 4941 bytes to 2236 bytes[OK]

スイッチ# reload
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]
```

バンドル実行モードからインストール実行モードに変換

バンドル モードからインストール モードにスイッチの実行モードを切り替えるには、**software expand running** 特権 EXEC コマンドを使用します。このコマンドは、起動された IOS XE ソフトウェア バンドルからのパッケージを展開し、指定されている宛先にそれらおよびプロビジョニング ファイルをコピーします。

スイッチをバンドル モードからインストール モードに変換するために **software expand running** コマンドを使用する場合、**to** 宛先を **flash:** に指定します。コマンドを実行した後、展開されたプロビジョニング ファイル（flash:packages.conf）を指定するために **boot system** コマンドを設定し、その後インストール モードで起動するようにスイッチをリロードします。

（注） スイッチがインストール モードで動作しているときは、**software expand running** コマンドはサポートされません。

バンドル実行モードからインストール実行モード変換例

この例では、**software expand running to** コマンドを使用して、スイッチ スタック内のアクティブなスイッチをバンドル実行モードからインストール実行モードに変換します。

```
スイッチ# dir flash:
Directory of flash:/
 7386 -rwx     2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
 7378 drwx        4096 Jan 23 2013 09:35:11 +00:00 mnt
 7385 -rw-   221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 7389 -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
712413184 bytes total (445063168 bytes free)

スイッチ#
スイッチ# software expand running to flash:
Preparing expand operation ...
[2]: Expanding the running bundle
[2]: Copying package files
[2]: Package files copied
[2]: Finished expanding the running bundle
スイッチ#
スイッチ# dir flash:
Directory of flash:/
 7386 -rwx     2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
 7378 drwx        4096 Jan 23 2013 09:35:11 +00:00 mnt
 7385 -rw-   221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 7391 -rw-    74410468 Jan 23 2013 14:16:57 +00:00 cat3k_caa-base.SPA.03.02.00SE.pkg
 7392 -rw-     2773680 Jan 23 2013 14:16:57 +00:00 cat3k_caa-drivers.SPA.03.02.00.SE.pkg
 7393 -rw-    32478044 Jan 23 2013 14:16:57 +00:00 cat3k_caa-infra.SPA.03.02.00SE.pkg
 7394 -rw-   30393116 Jan 23 2013 14:16:57 +00:00 cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg

 7389 -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
 7395 -rw-    18313952 Jan 23 2013 14:16:57 +00:00 cat3k_caa-platform.SPA.03.02.00.SE.pkg
 7396 -rw-    63402700 Jan 23 2013 14:16:57 +00:00 cat3k_caa-wcm.SPA.10.0.100.0.pkg
 7388 -rw-        1218 Jan 23 2013 14:17:43 +00:00 packages.conf
712413184 bytes total (223019008 bytes free)

スイッチ#
スイッチ# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
スイッチ(config)# boot system switch all flash:packages.conf
スイッチ(config)# end
スイッチ#

*Jan 23 14:28:47.722: %SYS-5-CONFIG_I: Configured from console by console

スイッチ# write memory
Building configuration...
Compressed configuration from 4851 bytes to 2187 bytes[OK]

スイッチ#
スイッチ# reload
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]
```

1 台のスタック メンバから他のスタック メンバへの IOS XE パッケージおよびバンドル ファイルのコピー

スイッチ スタックがインストール モードで実行されている場合、**software install source switch** 特権 EXEC コマンドを使用して、別の（互換性のある）ソフトウェア パッケージを実行中の、他の 1 台以上のスタック メンバへ、既存のスタック メンバから実行中のソフトウェア パッケージをインストールします。

1 つのスタック メンバから別のスタック メンバに IOS XE パッケージおよびバンドル ファイルをコピーする例

この例では、それぞれのスイッチが、異なる（しかし互換性のある）ソフトウェアパッケージを実行する 2 メンバー スタックを示しています。**software install source switch** コマンドは、スタンバイ スイッチ（スイッチ1）で実行中のパッケージを、アクティブなスイッチ（スイッチ2）にインストールする場合に使用します。

```
スイッチ# show version running
Package: Base, version: 03.02.00SE, status: active
File: cat3k_caa-base.SPA.03.02.00SE.pkg, on: Switch1
Built: Wed Jan 09 21:59:52 PST 2013, by: gereddy

Package: Drivers, version: 03.02.00.SE, status: active
File: cat3k_caa-drivers.SPA.03.02.00.SE.pkg, on: Switch1
Built: Wed Jan 09 22:03:41 PST 2013, by: gereddy

Package: Infra, version: 03.02.00SE, status: active
File: cat3k_caa-infra.SPA.03.02.00SE.pkg, on: Switch1
Built: Wed Jan 09 22:00:56 PST 2013, by: gereddy

Package: IOS, version: 150-1.EX, status: active
File: cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg, on: Switch1
Built: Wed Jan 09 22:02:23 PST 2013, by: gereddy

Package: Platform, version: 03.02.00.SE, status: active
File: cat3k_caa-platform.SPA.03.02.00.SE.pkg, on: Switch1
Built: Wed Jan 09 22:01:46 PST 2013, by: gereddy

Package: WCM, version: 10.0.100.0, status: active
File: cat3k_caa-wcm.SPA.10.0.100.0.pkg, on: Switch1
Built: Wed Jan 09 22:03:05 PST 2013, by: gereddy

スイッチ#
スイッチ# software install source switch 1
Preparing install operation ...
[2]: Copying software from source switch 1 to switch 2
[2]: Finished copying software to switch 2
[2]: Starting install operation
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: New files list:
Added cat3k_caa-base.SPA.03.02.00.SE.pkg
Added cat3k_caa-drivers.SPA.03.02.00.SE.pkg
```

```
Added cat3k_caa-infra.SPA.03.02.00.SE.pkg
Added cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
Added cat3k_caa-platform.SPA.03.02.00.SE.pkg
Added cat3k_caa-wcm.SPA.10.0.100.0.pkg
[2]: Creating pending provisioning file
[2]: Finished installing software. New software will load on reboot.
[2]: Committing provisioning file
[2]: Do you want to proceed with reload? [yes/no]:
```

バンドル モードで動作するスイッチ スタックの場合、1 つのスタック メンバーーから別のスタック メンバーへバンドル ファイルをコピーするには、次の手順を実行します。

1. 実行中のバンドルを、スタック中のスイッチから別のスイッチへコピーするには、**copy** 特権 EXEC コマンドを使用します。
2. バンドル ファイルを指示するように **boot system** グローバル コンフィギュレーション コマンドを設定します。
3. スイッチをリロードします。

次の例では、それぞれのスイッチが、異なる（しかし互換性のある）ソフトウェア パッケージを実行する 2 メンバー スタックを示しています。

```
スイッチ# copy flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 flash-1:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Copy in progress...
...
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)
スイッチ#
スイッチ# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

スイッチ(config)# boot system switch 1
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
スイッチ(config)# end
スイッチ#
```

互換性のないソフトウェアを実行しているスイッチのアップグレード

インストールモードで実行されているスイッチを、スイッチスタック（これもインストールモードで実行されている）との互換性がないソフトウェア パッケージでアップグレードするには、**software auto-upgrade** 特権 EXEC コマンドを使用して、既存のスタック メンバから、互換性のないソフトウェアを実行しているスタック メンバへ、ソフトウェア パッケージをインストールします。自動アップグレードのインストールが完了したら、互換性のないスイッチが自動的にリロードされ、、完全に機能するメンバとしてスタックに参加します。

（注） グローバル **software auto-upgrade enable** コマンドを設定すると、互換性のないソフトウェアがインストール モードで動作しているスイッチがインストール モードで動作しているスタックに参加するときに、自動アップグレード機能が自動的に開始します。詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』を参照してください。

互換性のないソフトウェアを実行するスイッチのアップグレード例

次に、2 つのメンバスイッチスタックの例を示します。スイッチ 2 はアクティブなスイッチで、スイッチ 1 は互換性のないソフトウェアを実行しています。

```
スイッチ# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
------------------------------------------------------------
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready
スイッチ#
スイッチ# software auto-upgrade
% Auto upgrade has been initiated for the following incompatible switches: 1

INFO level system messages will be generated to provide status information during
the auto upgrade process

スイッチ#
*Oct 19 06:59:14.521: %INSTALLER-6-AUTO_UPGRADE_SW_INITIATED: 2 installer: Auto upgrade
initiated for switch 1
*Oct 19 06:59:14.522: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Searching stack for software
 to upgrade switch 1
*Oct 19 06:59:14.523: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Found donor switch 2 to
auto upgrade switch 1
*Oct 19 06:59:14.523: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Upgrading switch 1 with
software from switch 2
*Oct 19 07:00:47.829: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Finished installing software
 on switch 1
*Oct 19 07:00:47.829: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Reloading switch 1 to
complete the auto upgrade
```

スイッチスタック（バンドル モードで実行中）と互換性のないソフトウェア バンドルを使用して、バンドルモードで実行中のスイッチをアップグレードするには、次の手順を実行します。

1. 実行中のバンドルをスタック内のあるスイッチから別へコピーするには、**copy** 特権 EXEC コマンドを使用します。
2. **boot system** グローバル コンフィギュレーション コマンドを設定して、バンドル ファイルを指します。
3. スイッチをリロードします。

次に、バンドル モードで実行する 2 つのメンバスイッチスタックの例を示します。スイッチ 2 はアクティブなスイッチで、スイッチ 1 は互換性のないバンドルを実行しています。

```
スイッチ# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
------------------------------------------------------------
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready
スイッチ#
スイッチ# copy flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 flash-1:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Copy in progress...
...
```

```
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)

スイッチ#
スイッチ# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
スイッチ(config)# boot system switch 1
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
スイッチ(config)# end
スイッチ#
*Nov 19 16:08:14.857: %SYS-5-CONFIG_I: Configured from console by console
スイッチ# reload slot 1
Stack is in Half ring setup; Reloading a switch might cause stack split
Proceed with reload? [confirm]
```

互換性のない実行モードで実行中のスイッチのアップグレード

バンドルモードで動作しているスイッチが、インストールモードでスタック動作に接続しようとする場合は、**software auto-upgrade** 特権 EXEC コマンドを、互換性のないスイッチの実行パッケージをインストールし、スイッチをインストール モードへ移行するために使用します。自動アップグレード実行変換が完了した後、互換性のないスイッチが自動的にリロードし、インストール モードのスタックに参加を試みます。

（注） グローバル **software auto-upgrade enable** コマンドを設定すると、自動アップグレード機能が、スイッチとインストール モードで動作している互換性がないソフトウェアが、インストール モードで動作するスタックに追加されたときに自動的に開始されます。詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』を参照してください。

互換性のない実行モードで実行中のスイッチのアップグレード例

この例では、インストール モードで実行中の 2 メンバー スイッチ スタックを示しています。スイッチ 2 はアクティブ スイッチであり、スイッチ 1 はバンドル モードで実行中です。

```
スイッチ# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
------------------------------------------------------------
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready

スイッチ#
スイッチ# software auto-upgrade
% Auto upgrade has been initiated for the following incompatible switches: 1

INFO level system messages will be generated to provide status information during the auto
 upgrade process

スイッチ#
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW_INITIATED: 2 installer: Auto upgrade
initiated for switch 1
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Converting switch 1 to
installed mode by
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: installing its running
```

```
software
*Oct 19 07:18:50.488: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Setting the boot var on
switch 1
*Oct 19 07:18:51.553: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Finished installing the
running software on switch 1
*Oct 19 07:18:51.553: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Reloading switch 1 to boot
 in installed mode
```

（注） 互換性のない スイッチをインストール モードに変換するために **software auto-upgrade** コマンドを使用すると、コマンドは、互換性がない スイッチ の実行バンドルからパッケージをインストールします。互換性のないスイッチがインストール モードでブートおよびリロードされた後に、スイッチのインストールされたパッケージがスタックと互換性がないことが確認された場合、**software auto-upgrade** コマンドを再度使用します。詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』を参照してください。

インストールモードで実行中でバンドルモードで動作しているスタックに加わっているスイッチを変換するには、次のステップを実行します。

1. 実行中のバンドルを、スタック中のスイッチから別のスイッチへコピーするには、**copy** 特権 EXEC コマンドを使用します。
2. バンドル ファイルを指示するように **boot system** グローバル コンフィギュレーション コマンドを設定します。
3. スイッチをリロードします。

リロードの後、互換性のないスイッチはバンドル モードでブートし、完全に機能するメンバーとしてスタックに加わります。

この例では、バンドル モードで実行中の 2 メンバー スイッチ スタックを示しています。スイッチ 2 はアクティブ スイッチであり、スイッチ 1 はインストール モードで実行中です。

```
スイッチ#
スイッチ# copy flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 flash-1:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Copy in progress...
....
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)
スイッチ#
スイッチ# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
スイッチ(config)# boot system switch 1
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
スイッチ(config)# end
スイッチ#
*Nov 19 16:08:14.857: %SYS-5-CONFIG_I: Configured from console by console
スイッチ# reload slot 1
Stack is in Half ring setup; Reloading a switch might cause stack split
Proceed with reload? [confirm]
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ソフトウェアバンドルとパッケージを管理するコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

エラー メッセージ デコーダ

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

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

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

第 101 章

条件付きデバッグおよび放射線トレース

- 機能情報の確認，2315 ページ
- 条件付きデバッグの概要，2316 ページ
- ラジオアクティブ トレースの概要，2316 ページ
- 条件付きデバッグおよび放射線トレース，2316 ページ
- トレースファイルの場所，2317 ページ
- 条件付きデバッグの設定，2317 ページ
- トレース ファイルの推奨ワークフロー，2320 ページ
- ボックス外へのトレース ファイルのコピー，2320 ページ
- 条件付きデバッグ設定の例，2321 ページ
- 条件付きデバッグのモニタリング，2322 ページ

機能情報の確認

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

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

条件付きデバッグの概要

条件付きデバッグ機能によって、定義した条件に基づき、特定の機能のデバッグおよびロギングを選択して有効にすることができます。この機能は、多くの機能がサポートされているシステムで有用です。

（注） Cisco IOS 16.1 では、コントロール プレーンのトレースのみがサポートされています。

条件付きデバッグは、多数の機能が導入されて稼働する大規模なネットワークでも、非常に詳細な方法でデバッグが可能です。これにより、システム内の細かなインスタンスに対しても、詳細なデバッグを実行できます。これは、何千ものセッションのうちの特定のセッションのみをデバッグするような場合に、非常に有用です。条件は複数指定することもできます。

条件とは、機能またはアイデンティティをいいます。アイデンティティは、インターフェイス、IP アドレス、MAC アドレスなどです。

（注） Cisco IOS リリース 16.1 でサポートされる条件は MAC アドレスのみです。これ以外の機能のサポートは、今後のリリースで導入されます。

これは、処理する機能オブジェクトを区別せずに出力を生成することで多くのシステム リソースを消費してシステム パフォーマンスに影響する、一般的なデバッグ コマンドとは対照的です。

ラジオアクティブ トレースの概要

ラジオアクティブ トレースにより、冗長性のレベルを高めた状態で、システムの全体にわたって目的とする動作を連鎖的に実行できます。複数のスレッド、プロセス、および関数呼び出しにわたって、デバッグ情報を条件に基づいて（DEBUG レベルまで、または指定のデバッグ レベルまで）出力する方法を提供します。

（注） Cisco IOS リリース 16.1 では、デフォルトのレベルは **DEBUG** です。ユーザは別のレベルに変更することはできません。これ以外のレベルのサポートは、今後のリリースで導入されます。

条件付きデバッグおよび放射線トレース

放射線トレースを条件付きデバッグと組み合わせると、条件に関連したすべての実行コンテキストをデバッグする単一のデバッグ CLI を使用することができます。その場合、フロー制御機能の一部である対象内のさまざまなプロセスを気にすることなく、これらのプロセスに個別にデバッグを発行する必要はありません。

トレースファイルの場所

デフォルトでは、トレースファイルログは各プロセスで生成され、**/tmp/rp/trace** または **/tmp/fp/trace** ディレクトリに保存されます。この一時ディレクトリで、トレース ログがファイルに書き込まれます。各ファイルは 1 MB サイズです。このディレクトリでは、特定のプロセスのこうしたファイルを、最大 25 件保持できます。**/tmp** ディレクトリのトレースファイルがその 1 MB 制限またはブート時に設定されたサイズに達した場合、ローテーションから外れ、**tracelogs** ディレクトリの **/crashinfo** パーティションの下にあるアーカイブの場所に移動します。

/tmp ディレクトリが 1 つのプロセスで保持するトレースファイルは 1 つのみです。ファイルがそのファイルサイズの制限に達したら、ローテーションから外れ、**/crashinfo/tracelogs** に移動します。アーカイブ ディレクトリに蓄積されるファイルは最大 25 ファイルであり、その後は最も古いものから順に、**/tmp** から新たにローテーションされたファイルに置換されます。

トレースファイルは crashinfo ディレクトリに、次の形式で配置されます。

1. Process-name_Process-ID_running-counter.timestamp.gz
   例：IOSRP_R0-0.bin_0.14239.20151101234827.gz
2. Process-name_pmanlog_Process-ID_running-counter.timestamp.bin.gz
   例：wcm_pmanlog_R0-0.30360_0.20151028233007.bin.gz

条件付きデバッグの設定

条件付デバッグを設定するには、以下の手順に従います。

-

手順の概要

1. **enable**
2. **debug platform condition mac** {*mac-address*}
3. **debug platform condition start**
4. **show platform condition** OR **show debug**
5. **debug platform condition stop**
6. **request platform software trace archive** [**last** {*number*} **days**] [**target** {*crashinfo:* | *flashinfo:*}]
7. **request platform software trace filter-binary** {*wire* | *wireless*} [**context** {*mac-address*} | **level** | **module**]
8. **show platform software trace** [**filter-binary** | **level** | **message**]
9. **clear platform condition all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**debug platform condition mac** {*mac-address*} 例： スイッチ# **debug platform condition mac bc16.6509.3314**	指定された MAC アドレスの条件付きデバッグを設定します。
ステップ 3	**debug platform condition start** 例： スイッチ# **debug platform condition start**	条件付きデバッグを開始します（上記のいずれかの条件に一致すると放射線トレースを開始します）。
ステップ 4	**show platform condition** OR **show debug** 例： スイッチ# **show platform condition** スイッチ# **show debug**	現在設定されている条件を表示します。
ステップ 5	**debug platform condition stop** 例： スイッチ# **debug platform condition stop**	条件付きデバッグを停止します（放射線トレースを停止します）。
ステップ 6	**request platform software trace archive** [**last** {*number*} **days**] [**target** {*crashinfo:* | *flashinfo:*}] 例： スイッチ# **request platform software trace archive last 2 days**	（任意）システムのマージされたトレースファイルの履歴ログを表示します。日数またはロケーションの組み合わせのフィルタ。
ステップ 7	**request platform software trace filter-binary** {*wire* | *wireless*} [**context** {*mac-address*} | **level** | **module**] 例： スイッチ# **request platform software trace filter-binary wireless context bc16.6509.3314**	（任意）指定された MAC アドレスのコンテキストと情報（ネットワークまたはワイヤレス）を照合するには、モジュールをフィルタリングします。これらのログはオフラインで確認できます。 （注） Cisco IOS リリース 16.1 では、使用可能なすべてのキーワードのうち、サポートされている唯一のキーワードは、ワイヤレスです。これは、プロセス（ios、wcm、fman_rp、fman_fp）からファイルを収集します。

	コマンドまたはアクション	目的
ステップ 8	**show platform software trace** [**filter-binary** | **level** | **message**] 例： スイッチ# **show platform software trace message**	（任意）最新のトレースファイルからマージされたログを表示します。アプリケーションの状態、トレース モジュール名およびトレース レベルをさまざまな組み合わせでフィルタリングします。 • **filter-binary**：照合するモジュールをフィルタリングします。例えば、ワイヤレス。 • **level**：トレース レベルを示します。 • **message**：トレース メッセージのリングの内容を表示します。 （注） ボックスでは： • Linux シェルだけでなく、IOS のコンソールからも使用できます。 • マージされたログを含むファイルをボックスで生成します。 • ステージング エリアからのみマージされたログを表示します。
ステップ 9	**clear platform condition all** 例： スイッチ# **clear platform condition all**	すべての条件をクリアします。

次の作業

（注） **request platform software trace filter-binary** および **show platform software trace filter-binary** コマンドは、似たように動作します。唯一の違いは次のとおりです。

- **request platform software trace filter-binary**：履歴ログからのデータを送信します。
- **show platform software trace filter-binary**：フラッシュの一時ディレクトリからデータを送信します。

（注） **request platform software trace filter-binary wireless** {*mac-address*} コマンドは、3 つのフラッシュ ファイルを生成します。

- *collated_log_<.date..>*
- *mac_log <..date..>*
- *mac_database .. file*

その中でも、*mac_log <..date..>* は、デバッグする MAC 用のメッセージを伝えるため、最も重要なファイルです。**show platform software trace filter-binary** コマンドも同じフラッシュ ファイルを生成し、また、画面に mac_log を出力します。

トレース ファイルの推奨ワークフロー

トレース ファイルの推奨ワークフローの概要は次のとおりです。

1. 特定の期間、例えば 1 日、トレースログをリクエストします。
   使用するコマンドは、次のとおりです。

   スイッチ#リクエストプラットフォームソフトウェアトレースアーカイブ過去 1 日間
2. システムは、/flash: ロケーション内のトレースログの tar ball（.gz ファイル）を生成します。
3. ボックス外にファイルをコピーします。ファイルをコピーすることによって、オフラインでトレースログが使用できます。ファイルのコピーについての詳細は、次のセクションを参照してください。
4. /flash: location からトレースログファイル（.gz）ファイルを削除します。これはボックスに他の操作のための十分な空き領域があることを確保します。

ボックス外へのトレース ファイルのコピー

トレース ファイルの例を以下に示します。

```
スイッチ# dir crashinfo:/tracelogs
Directory of crashinfo:/tracelogs/

50664 -rwx 760 Sep 22 2015 11:12:21 +00:00 plogd_F0-0.bin_0.gz
50603 -rwx 991 Sep 22 2015 11:12:08 +00:00 fed_pmanlog_F0-0.bin_0.9558.20150922111208.gz
50610 -rw- 11 Nov 2 2015 00:15:59 +00:00 timestamp
50611 -rwx 1443 Sep 22 2015 11:11:31 +00:00
auto_upgrade_client_sh_pmanlog_R0-.bin_0.3817.20150922111130.gz
50669 -rwx 589 Sep 30 2015 03:59:04 +00:00 cfgwr-8021_R0-0.bin_0.gz
50612 -rwx 1136 Sep 22 2015 11:11:46 +00:00 reflector_803_R0-0.bin_0.1312.20150922111116.gz
50794 -rwx 4239 Nov 2 2015 00:04:32 +00:00 IOSRP_R0-0.bin_0.14239.20151101234827.gz
50615 -rwx 131072 Nov 2 2015 00:19:59 +00:00 linux_iosd_image_pmanlog_R0-0.bin_0
--More--
```

トレース ファイルは、次に示すさまざまなオプションのいずれかを使用して、コピーできます。

```
スイッチ# copy crashinfo:/tracelogs ?
```

```
  crashinfo: Copy to crashinfo: file system
  flash: Copy to flash: file system
  ftp: Copy to ftp: file system
  http: Copy to http: file system
  https: Copy to https: file system
  null: Copy to null: file system
  nvram: Copy to nvram: file system
  rcp: Copy to rcp: file system
  running-config Update (merge with) current system configuration
  scp: Copy to scp: file system
  startup-config Copy to startup configuration
  syslog: Copy to syslog: file system
  system: Copy to system: file system
  tftp: Copy to tftp: file system
  tmpsys: Copy to tmpsys: file system
```

TFTP サーバにコピーするための一般的な構文は次のとおりです。

```
スイッチ# copy source: tftp:
スイッチ# copy crashinfo:/tracelogs/IOSRP_R0-0.bin_0.14239.20151101234827.gz tftp:
Address or name of remote host []? 2.2.2.2
Destination filename [IOSRP_R0-0.bin_0.14239.20151101234827.gz]?
```

（注） tracelogおよび他の目的に使用可能な空き容量があることを確認するために、生成されたレポート/アーカイブ ファイルをクリアすることが重要です。

条件付きデバッグ設定の例

次に、*show platform condition* コマンドの出力例を示します。

```
スイッチ# show platform condition
Conditional Debug Global State: Stop
Conditions Direction
------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
----------------------|----------------------|--------------------------------
スイッチ#
```

次に、*show debug* コマンドの出力例を示します。

```
スイッチ# show debug
IOSXE Conditional Debug Configs:
Conditional Debug Global State: Start
Conditions Direction
------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
----------------------|----------------------|--------------------------------
Packet Infra debugs:
Ip Address Port
------------------------------------------------------|----------
スイッチ#
```

次に、*debug platform condition stop* コマンドの例を示します。

```
スイッチ# debug platform condition stop
Conditional Debug Global State: Stop
```

条件付きデバッグのモニタリング

以下の表に、条件付きデバッグのモニタに使用できる各種コマンドを示します。

コマンド	目的
show platform condition	現在設定されている条件を表示します。
show debug	現在設定されているデバッグ条件を表示します。
show platform software trace filter-binary	最新のトレースファイルからマージされたログを表示します。
request platform software trace filter-binary	システムにマージされたトレースファイルの履歴ログを表示します。

第 102 章

ソフトウェア設定のトラブルシューティング

この章では、スイッチが稼働する Cisco IOS ソフトウェアに関連する問題を特定し、解決する方法について説明します。問題の性質に応じて、コマンドラインインターフェイス（CLI）、デバイス マネージャ、または Network Assistant を使用して、問題を特定し解決できます。

LED の説明など、トラブルシューティングの詳細については、ハードウェア インストレーション ガイドを参照してください。

- 機能情報の確認，2323 ページ
- ソフトウェア設定のトラブルシューティングに関する情報，2324 ページ
- ソフトウェア設定のトラブルシューティング方法，2333 ページ
- ソフトウェア設定のトラブルシューティングの確認，2347 ページ
- ソフトウェア設定のトラブルシューティングのシナリオ，2350 ページ
- ソフトウェアのトラブルシューティングの設定例，2354 ページ
- ソフトウェア設定のトラブルシューティングに関する追加情報，2357 ページ
- ソフトウェア設定のトラブルシューティングの機能履歴と情報，2358 ページ

機能情報の確認

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

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

ソフトウェア設定のトラブルシューティングに関する情報

スイッチのソフトウェア障害

スイッチ ソフトウェアがアップグレード中に破損する原因として、誤ったファイルがスイッチにダウンロードされた場合やイメージ ファイルが削除された場合があります。いずれの場合にも、スイッチは電源投入時自己診断テスト（POST）に失敗し、接続できなくなります。

関連トピック

ソフトウェア障害からの回復，（2333 ページ）

スイッチのパスワードを紛失したか忘れた場合

スイッチのデフォルト設定では、スイッチに物理的にアクセスしているエンドエンド ユーザは、スイッチの電源投入中に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復できます。ここで紹介する回復手順を実行するには、スイッチに物理的にアクセスする必要があります。

（注） これらのスイッチでは、システム管理者は、デフォルト設定に戻すことに同意した場合に限り、エンド ユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできます。パスワード回復がディセーブルになっている場合に、エンド ユーザがパスワードをリセットしようとすると、ステータス メッセージで回復プロセスの間はデフォルトの設定に戻すように指示されます。

関連トピック

パスワードを忘れた場合の回復，（2335 ページ）

Power over Ethernet（PoE）ポート

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

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

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

受電デバイスを検出すると、スイッチは受電デバイスの電力要件を判断し、受電デバイスへの電力供給を許可または拒否します。また、スイッチは消費電力をモニタリングおよびポリシングすることで、装置の電力の消費をリアルタイムに検知できます。

詳細については、『*Interface and Hardware Component Configuration Guide*（*Catalyst 3650 Switches*）』の「Configuring Failover」の章を参照してください。

関連トピック

Power over Ethernet（PoE）に関するトラブルシューティングのシナリオ, （2350 ページ）

電力消失によるポートの障害

PoE スイッチ ポートに接続され、AC 電源から電力が供給されている受電デバイス（Cisco IP Phone 7910 など）に AC 電源から電力が供給されない場合、そのデバイスは errdisable ステートになることがあります。error-disabled ステートから回復するには、**shutdown** インターフェイス コンフィギュレーション コマンドを入力してから、**no shutdown** インターフェイス コマンドを入力します。スイッチで自動回復を設定し、error-disabled ステートから回復することもできます。

スイッチの場合、**errdisable recovery cause loopback** および **errdisable recovery interval***seconds* グローバル コンフィギュレーション コマンドは、指定した期間が経過したあと自動的にインターフェイスを error-disabled ステートから復帰させます。

不正リンク アップによるポート障害

シスコ受電デバイスをポートに接続し、**power inline never** インターフェイス コンフィギュレーション コマンドを使用してポートを設定した場合は、不正リンク アップが発生し、ポートが error-disabled ステートになることがあります。ポートを error-disabled ステートから回復するには、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

power inline never コマンドで設定したポートにシスコ受電デバイスを接続しないでください。

ping

スイッチは IP の ping をサポートしており、これを使ってリモート ホストへの接続をテストできます。ping はアドレスにエコー要求パケットを送信し、応答を待ちます。ping は次のいずれかの応答を返します。

- 正常な応答：正常な応答（*hostname* が存在する）は、ネットワーク トラフィックにもよりますが、1 ～ 10 秒以内で発生します。
- 宛先の応答なし：ホストが応答しない場合、*no-answer* メッセージが返されます。
- 不明なホスト：ホストが存在しない場合、*unknown host* メッセージが返されます。

- 宛先到達不能：デフォルト ゲートウェイが指定されたネットワークに到達できない場合、*destination-unreachable* メッセージが返されます。
- ネットワークまたはホストへの到達不能：ルートテーブルにホストまたはネットワークのエントリがない場合、*network or host unreachable* メッセージが返されます。

関連トピック

ping の実行, （2343 ページ）

例：IP ホストの ping, （2354 ページ）

レイヤ 2 Traceroute

レイヤ 2 traceroute 機能により、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを識別できます。レイヤ 2 traceroute は、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。transroute は、パス内にあるスイッチの MAC アドレス テーブルを使用してパスを識別します。スイッチがパス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 trace クエリーを送信し続け、タイムアウトにします。

スイッチは、送信元デバイスから宛先デバイスへのパスのみを識別できます。パケットが通過する、送信元ホストから送信元デバイスまで、または宛先デバイスから宛先ホストまでのパスは識別できません。

レイヤ 2 の traceroute のガイドライン

- ネットワーク内のすべてのデバイスで、Cisco Discovery Protocol（CDP）をイネーブルにする必要があります。レイヤ 2 traceroute が適切に動作するために、CDP をディセーブルにしないでください。

  物理パス内のデバイスが CDP に対して透過的な場合、スイッチはこれらのデバイスを通過するパスを識別できません。

- **ping** 特権 EXEC コマンドを使用して接続をテストできれば、このスイッチは別のスイッチから到達可能といえます。物理パス内のすべてのスイッチは、他のスイッチから相互に到達可能でなければなりません。
- パス内で識別可能な最大ホップ数は 10 です。
- 送信元デバイスと宛先デバイスの間の物理パス内にないスイッチで、**traceroute mac** または **traceroute mac ip** の特権 EXEC コマンドを実行できます。パス内のすべてのスイッチは、このスイッチから到達可能でなければなりません。
- **traceroute mac** コマンドの出力結果としてレイヤ 2 パスが表示されるのは、指定の送信元および宛先 MAC アドレスが、同一の VLAN に属している場合だけです。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。
- マルチキャストの送信元または宛先 MAC アドレスを指定すると、パスは識別されず、エラーメッセージが表示されます。

- 送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。VLAN を指定しないと、パスは識別されず、エラー メッセージが表示されます。
- 指定した送信元および宛先の IP アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力にレイヤ 2 パスが表示されます。IP アドレスを指定した場合、スイッチは Address Resolution Protocol（ARP）を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を関連付けます。
  - 指定の IP アドレスに ARP のエントリが存在している場合、スイッチは関連する MAC アドレスを使用して、物理パスを識別します。
  - ARP のエントリが存在しない場合、スイッチは ARP クエリを送信し、IP アドレスの解決を試みます。IP アドレスが解決されない場合は、パスは識別されず、エラー メッセージが表示されます。
- 複数のデバイスがハブを介して 1 つのポートに接続されている場合（たとえば複数の CDP ネイバーがポートで検出された場合）、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされません。

IP Traceroute

IP traceroute を使用すると、ネットワーク上でパケットが通過するパスをホップバイホップで識別できます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク層（レイヤ 3）デバイスが表示されます。

スイッチは、**traceroute** 特権 EXEC コマンドの送信元または宛先として指定できます。また、スイッチは **traceroute** コマンドの出力でホップとして表示される場合があります。スイッチを traceroute の宛先とすると、スイッチは、traceroute の出力で最終の宛先として表示されます。中間スイッチが同じ VLAN 内でポート間のパケットのブリッジングだけを行う場合、traceroute の出力に中間スイッチは表示されません。ただし、中間スイッチが、特定のパケットをルーティングするマルチレイヤ スイッチの場合、中間スイッチは traceroute の出力にホップとして表示されます。

traceroute 特権 EXEC コマンドは、IP ヘッダーの存続可能時間（TTL）フィールドを使用して、ルータおよびサーバで特定のリターン メッセージが生成されるようにします。traceroute の実行は、ユーザ データグラム プロトコル（UDP）データグラムを、TTL フィールドが 1 に設定されている宛先ホストへ送信することから始まります。ルータで TTL 値が 1 または 0 であることを検出すると、データグラムをドロップし、インターネット制御メッセージ プロトコル（ICMP）time-to-live-exceeded メッセージを送信元に送信します。traceroute は、ICMP time-to-live-exceeded メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判別します。

ネクスト ホップを識別するために、traceroute は TTL 値が 2 の UDP パケットを送信します。1 番めのルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番めのルータは、TTL 値が 1 であることを確認すると、このデータグラムを廃棄し、

time-to-live-exceeded メッセージを送信元へ返します。このように、データグラムが宛先ホストに到達するまで（または TTL の最大値に達するまで）TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを学習するために、traceroute は、データグラムの UDP 宛先ポート番号を、宛先ホストが使用する可能性のない大きな値に設定します。ホストが、ローカルで使用されない宛先ポート番号を持つ自分自身宛てのデータグラムを受信すると、送信元に ICMP ポート到達不能エラーを送信します。ポート到達不能エラーを除くすべてのエラーは中間ホップから送信されるため、ポート到達不能エラーを受信するということは、このメッセージが宛先ポートから送信されたことを意味します。

関連トピック

IP traceroute の実行，（2344 ページ）

例：IP ホストに対する traceroute の実行，（2355 ページ）

Time Domain Reflector ガイドライン

Time Domain Reflector（TDR）機能を使用すると、ケーブル配線の問題を診断して解決できます。TDR 稼働時、ローカルデバイスはケーブルを介して信号を送信して、最初に送信した信号と反射された信号を比べます。

TDR は 10/100/1000 の銅線イーサネット ポート上でだけサポートされます。10 ギガビット イーサネット ポートまたは SFP モジュール ポートではサポートされません。

TDR は次のケーブル障害を検出します。

- ツイストペア ケーブルの導線のオープン、損傷、切断：導線がリモート デバイスからの導線に接続されていない状態。
- ツイストペア ケーブルの導線のショート：導線が互いに接触している状態、またはリモート デバイスからの導線に接触している状態。たとえば、ツイスト ペア ケーブルの一方の導線が、もう一方の導線にはんだ付けされている場合、ツイストペア ケーブルのショートが発生します。

ツイストペアの導線の一方がオープンになっている場合、TDR はオープンになっている導線の長さを検出できます。

次の状況で TDR を使用して、ケーブル障害を診断および解決してください。

- スイッチの交換
- 配線クローゼットの設定
- リンクが確立できない、または適切に動作していない場合における、2 つのデバイス間の接続のトラブルシューティング

TDR の実行時、次の場合にスイッチは正確な情報をレポートします。

- ギガビット リンク用のケーブルが単線コア ケーブル
- オープンエンド ケーブルが未終端

TDR の実行時、次の場合にスイッチは正確な情報をレポートしません。

- ギガビット リンク用のケーブルがツイストペア ケーブルまたは連続接続された単線コア ケーブル
- リンクが 10 Mb または 100 Mb
- より線ケーブル
- リンク パートナーが Cisco IP Phone
- リンク パートナーが IEEE 802.3 に準拠していない

debug コマンド

注意 デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

debug コマンドはすべて特権 EXEC モードで実行します。ほとんどの **debug** コマンドは引数を取りません。

関連トピック

デバッグおよびエラー メッセージ出力のリダイレクト，（2345 ページ）

例：すべてのシステム診断をイネーブルにする，（2356 ページ）

システム レポート

crashinfo ファイルには、シスコのテクニカル サポート担当者が Cisco IOS イメージの障害（クラッシュ）が原因で起きた問題をデバッグするときに使用する情報が保存されています。明瞭度と整合性の高い重要なクラッシュ情報を迅速かつ確実に収集することが必要です。さらに、この情報の収集とバンドルが、特定のクラッシュの発生に対し関連付けか特定ができるような方法で行われることが必要です。

これをサポートするため、プロセスのクラッシュ時には、次の情報がローカルにスイッチから収集されます。

1. 完全なプロセス core
2. トレースログ
3. IOS の syslog（非アクティブなクラッシュの場合には保証されません）
4. システム プロセス情報

5 ブートアップ ログ

6 リロード ログ

7 特定のタイプの /proc 情報

加えて、IOS がクラッシュした場合、crashinfo ファイルが生成されます。

この情報は個別のファイルに格納されてから、アーカイブされて1つのバンドルに圧縮されます。これは、そのクラッシュのスナップショットを 1 つの場所で取得できる利便性を持たせ、分析のためにボックス外に移動できるようにします。このレポートは、スイッチがROMmon/ブートローダにダウンする前に生成されます。

完全な core およびトレースログ以外はテキスト ファイルです。

crashinfo ファイル

デフォルトでは、生成されたシステム レポート ファイルは /crashinfo ディレクトリに格納されます。スペースがなくてcrashinfoファイルのパーティションに格納できない場合、/flashディレクトリに保存されます。

ファイルは、通常の「dir crashinfo:」コマンドを使用して表示できます。次にcrashinfoディレクトリの出力例を示します。

```
Switch#dir crashinfo:
Directory of crashinfo:/
46553 drwx 1024 Jun 29 2015 14:52:09 +00:00 ap_crash
12 -rw- 0 Jan 1 1970 00:00:11 +00:00 koops.dat
11 -rw- 0 Mar 22 2013 07:50:30 +00:00 deleted_crash_files
13 -rwx 594269 Mar 22 2013 07:50:30 +00:00 crashinfo_platform_mgr_20130322-075017-UTC
14 -rw- 44 Sep 9 2015 09:28:47 +00:00 last_crashinfo
15 -rw- 355 Sep 9 2015 09:29:31 +00:00 last_systemreport_log
16 -rw- 105753 Mar 22 2013 07:50:47 +00:00 system-report_1_20130322-075017-UTC.gz
17 -rw- 39 Sep 9 2015 09:29:31 +00:00 last_systemreport
18 -rwx 585996 Mar 22 2013 08:01:58 +00:00 crashinfo_platform_mgr_20130322-080144-UTC
19 -rw- 105065 Mar 22 2013 08:02:15 +00:00 system-report_1_20130322-080144-UTC.gz
20 -rwx 3426209 Sep 9 2015 06:49:12 +00:00 crashinfo_iosd_20150909-064754-UTC
21 -rwx 9540376 Sep 9 2015 06:49:13 +00:00 fullcore_iosd_20150909-064754-UTC
22 -rw- 469476 Sep 9 2015 06:49:56 +00:00 system-report_1_20150909-064754-UTC.gz
23 -rwx 3425350 Sep 9 2015 09:28:47 +00:00 crashinfo_iosd_20150909-092728-UTC
24 -rwx 9535535 Sep 9 2015 09:28:47 +00:00 fullcore_iosd_20150909-092728-UTC
25 -rw- 459709 Sep 9 2015 09:29:28 +00:00 system-report_1_20150909-092728-UTC.gz
26 -rw- 0 Sep 22 2015 11:11:33 +00:00 tracelogs.J8C

50601 drwx 10240 Oct 28 2015 22:42:50 +00:00 tracelogs

248354816 bytes total (204800000 bytes free)
```

システム レポートは、次の形式で crashinfo ディレクトリに配置されます。

```
system-report_[switch number]_[date]-[timestamp]-UTC.gz
```

スイッチがクラッシュしたら、システム レポート ファイルをチェックする必要があります。 最後に生成されたシステム レポート ファイルは、crashinfo ディレクトリの下に last_systemreport というファイル名で保存されます。問題のトラブルシューティングを行う際、システム レポートおよび crashinfo ファイルが TAC の役に立ちます。

生成されたシステム レポートは、TFTP や HTTP などいくつかのオプションを使用して、さらにコピーできます。

```
Switch#copy crashinfo: ?
crashinfo:     Copy to crashinfo: file system
flash:         Copy to flash: file system
ftp:           Copy to ftp: file system
```

```
http:          Copy to http: file system
https:         Copy to https: file system
null:          Copy to null: file system
nvram:         Copy to nvram: file system
rcp:           Copy to rcp: file system
running-config Update (merge with) current system configuration
scp:           Copy to scp: file system
startup-config Copy to startup configuration
syslog:        Copy to syslog: file system
system:        Copy to system: file system
tftp:          Copy to tftp: file system
tmpsys:        Copy to tmpsys: file system
```

TFTP サーバにコピーするための一般的な構文は次のとおりです。

```
Switch#copy crashinfo: tftp:
Source filename [system-report_1_20150909-092728-UTC.gz]?
Address or name of remote host []? 1.1.1.1
Destination filename [system-report_1_20150909-092728-UTC.gz]?
```

スタックの全メンバからのトレースログは、trace archive コマンドを発行することで取得できます。このコマンドには、時間帯オプションがあります。コマンド構文は次のとおりです。

```
Switch#request platform software trace archive ?
last     Archive trace files of last x days
target   Location and name for the archive file
```

crashinfo: または flash: ディレクトリに格納されている過去 3650 日以内のトレースログが取得できます。

```
Switch# request platform software trace archive last ?
<1-3650> Number of days (1-3650)
Switch#request platform software trace archive last 3650 days target ?
crashinfo: Archive file name and location
flash:     Archive file name and location
```

（注） 一度コピーされたら、システム レポートやトレースのアーカイブを flash ディレクトリまたは crashinfo ディレクトリからクリアし、トレースログやその他の目的に使用できる領域を確保することが重要です。

スイッチのオンボード障害ロギング

オンボード障害ロギング（OBFL）機能を使用すれば、スイッチに関する情報を収集できます。この情報には稼働時間、温度、電圧などの情報が含まれており、シスコのテクニカル サポート担当者がスイッチの問題をトラブルシューティングする際に役立ちます。OBFL はイネーブルにしておき、フラッシュ メモリに保存されたデータは消さないようにすることを推奨します。

OBFL は、デフォルトでイネーブルになっています。スイッチおよび Small Form-Factor Pluggable（SFP）モジュールに関する情報が収集されます。スイッチは、次の情報をフラッシュ メモリに保存します。

- CLI コマンド：スタンドアロン スイッチまたはスイッチ スタック メンバに入力された OBFL CLI コマンドの記録
- 環境データ：スタンドアロン スイッチまたはスタック メンバおよび接続されているすべての FRU デバイスの一意のデバイス ID（UDI）情報、製品 ID（PID）、バージョン ID（VID）、およびシリアル番号

- メッセージ：スタンドアロン スイッチまたはスタック メンバにより生成されたハードウェア関連のシステム メッセージの記録
- イーサネット経由の電源供給（PoE）：スタンドアロン スイッチまたはスイッチ スタック メンバの PoE ポートの消費電力の記録
- 温度：スタンドアロン スイッチまたはスタック メンバの温度
- 稼働時間：スタンドアロン スイッチまたはスタック メンバが起動されたときの時刻、スイッチが再起動された理由、およびスイッチが最後に再起動されて以来の稼働時間
- 電圧：スタンドアロン スイッチまたはスタック メンバのシステム電圧

システム時計は、手動で時刻を設定するか、またはネットワーク タイム プロトコル（NTP）を使用するように設定します。

スイッチの稼働中には、**show logging onboard** 特権 EXEC コマンドを使用することにより、OBFL データを取得できます。スイッチに障害が発生した場合のデータの取得方法については、お客様担当のシスコ テクニカル サポート担当者にお問い合わせください。

OBFL がイネーブルになっているスイッチが再起動された場合、新しいデータの記録が開始するまでに 10 分間の遅延があります。

関連トピック

OBFL の設定，（2346 ページ）

OBFL 情報の表示，（2347 ページ）

ファン障害

デフォルトでは、この機能はディセーブルです。現場交換可能ユニット（FRU）または電源装置の複数のファンが故障した場合、スイッチはシャットダウンせず、次のようなエラー メッセージが表示されます。

```
Multiple fan(FRU/PS) failure detected. System may get overheated. Change fan quickly.
```

スイッチが過熱状態となり、シャットダウンすることもあります。

ファン障害機能をイネーブルにするには、**system env fan-fail-action shut** 特権 EXEC コマンドを入力します。スイッチ内の複数のファンに障害が発生した場合、スイッチは自動的にシャットダウンし、次のようなエラー メッセージが表示されます。

```
Faulty (FRU/PS) fans detected, shutting down system!
```

最初のファンの停止後、スイッチが 2 つめのファンの障害を検知すると、スイッチは 20 秒待機してからシャットダウンします。

スイッチを再起動するには、電源をオフにしてから再度オンにする必要があります。

CPU 使用率が高い場合に起こりうる症状

CPU 使用率が高すぎることで次の症状が発生する可能性がありますが、他の原因で発生する場合もあります。

- スパニングツリー トポロジの変更
- 通信が切断されたために EtherChannel リンクがダウンした
- 管理要求（ICMP ping、SNMP のタイムアウト、低速な Telnet または SSH セッション）に応答できない
- UDLD フラッピング
- SLA の応答が許容可能なしきい値を超えたことによる IP SLA の失敗
- スイッチが要求を転送しない、または要求に応答しない場合の DHCP または IEEE 802.1x の処理の失敗

（注）

ソフトウェア設定のトラブルシューティング方法

ソフトウェア障害からの回復

はじめる前に

ここで紹介する回復手順を実行するには、スイッチを直接操作する必要があります。

ここで紹介する手順では、破損したイメージファイルまたは不適切なイメージファイルの回復に boot loader コマンドおよび TFTP を使用します。

ステップ 1 PC 上で、Cisco.com からソフトウェア イメージ ファイル（*image.bin*）をダウンロードします。

ステップ 2 TFTP サーバにソフトウェア イメージをロードします。

ステップ 3 PC をスイッチのイーサネット管理ポートに接続します。

ステップ 4 スイッチの電源コードを取り外します。

ステップ 5 [Mode] ボタンを押しながら、電源コードを再度スイッチに接続します。

ステップ 6 ブートローダ（ROMMON）プロンプトで、TFTP サーバに ping を実行できることを確認します。

a) **switch: set IP_ADDR***ip_addresssubnet_mask* コマンドを実行して、IP アドレス を設定します。

例：

```
switch: set IP_ADDR 192.0.2.123/255.255.255.0
```

b) **switch: set DEFAULT_ROUTER***ip_address* コマンドを実行して、デフォルト ルータの IP アドレスを設定します。

例：
```
switch: set DEFAULT_ROUTER 192.0.2.1
```

c) **switch: ping***ip_address_of_TFTP_server* コマンドを実行して、TFTP サーバに ping を実行できることを確認します。

例：
```
switch: ping 192.0.2.15
ping 192.0.2.1 with 32 bytes of data...
Host 192.0.2.1 is alive.
switch:
```

ステップ 7 回復パーティション（sda9:）に回復イメージが存在することを確認します。
この回復イメージは、emergency-install 機能を使用して回復を実施する場合に必要となります。

例：

```
switch: dir sda9:
Directory of sda9:/

    2  drwx  1024       .
    2  drwx  1024       ..
   11  -rw-  18923068   c3850-recovery.bin

36939776 bytes available (20830208 bytes used)
switch:
```

ステップ 8 ブートローダ（ROMMON）プロンプトで、emergency-install 機能を開始します。この機能を使用すると、スイッチでソフトウェア イメージを容易に回復できます。
警告：emergency-install コマンドを実行すると、ブート フラッシュ全体が消去されます。

例：
```
Switch#
emergency-install
tftp://192.0.2.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin

The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin)...
Reading full image into memory.....................done
Nova Bundle Image
-------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000, 0x90000000].
@@@
```

```
### Launching Linux Kernel (flags = 0x5)


Initiating Emergency Installation of bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin


Downloading bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Validating bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Installing bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Verifying bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Package cat3k_caa-base..pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.03.02.00.SE.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM +++@@@@####...++@@++@@++@@++@
```

関連トピック

スイッチのソフトウェア障害, （2324 ページ）

パスワードを忘れた場合の回復

スイッチのデフォルト設定では、スイッチを直接操作するエンドユーザが、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復できます。ここで紹介する回復手順を実行するには、スイッチを直接操作してください。

（注） これらのスイッチでは、システム管理者はデフォルト設定に戻す場合に限りエンドユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできます。パスワード回復がディセーブルになっている場合に、エンドユーザがパスワードをリセットしようとすると、回復プロセスの間、ステータス メッセージにその旨が表示されます。

手順の概要

1. 端末または PC をスイッチに接続します。
2. エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。
3. スタンドアロン スイッチまたはスイッチ スタック全体の電源を切断します。
4. 電源コードまたはアクティブ スイッチを再度接続します。15 秒以内に [**Mode**] ボタンを押します。このときシステム LED はグリーンに点滅しています。すべてのシステム LED が点灯した状態になるまで、[**Mode**] ボタンを押し続けます。その後、[**Mode**] ボタンを放します。
5. パスワードの回復後、スイッチまたはアクティブ スイッチをリロードします。
6. スタック内の残りのスイッチに電源を投入します。

手順の詳細

ステップ 1 端末または PC をスイッチに接続します。

- 端末または端末エミュレーション ソフトウェアが稼働している PC をスイッチのコンソール ポートに接続します。スイッチ スタックのパスワードを回復する場合は、アクティブ スイッチのコンソール ポートに接続するか、または
- PC をイーサネット管理ポートに接続します。スイッチ スタックのパスワードを回復する場合は、スタック メンバのイーサネット管理ポートに接続します。

ステップ 2 エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 3 スタンドアロン スイッチまたはスイッチ スタック全体の電源を切断します。

ステップ 4 電源コードまたはアクティブ スイッチを再度接続します。15 秒以内に [**Mode**] ボタンを押します。このときシステム LED はグリーンに点滅しています。すべてのシステム LED が点灯した状態になるまで、[**Mode**] ボタンを押し続けます。その後、[**Mode**] ボタンを放します。

-

```
Switch:
Xmodem file system is available.
Base ethernet MAC Address: 20:37:06:4d:e9:80
Verifying bootloader digital signature.


The system has been interrupted prior to loading the operating
system software, console will be reset to 9600 baud rate.
```

「パスワード回復がイネーブルになっている場合の手順」セクションに記載されている手順を実行します。

ステップ 5 パスワードの回復後、スイッチまたはアクティブ スイッチをリロードします。

スイッチの場合

```
Switch> reload
Proceed with reload? [confirm] y
```

アクティブ スイッチの場合

```
Switch> reload slot <stack-active-member-number>
Proceed with reload? [confirm] y
```

ステップ 6 スタック内の残りのスイッチに電源を投入します。

関連トピック

スイッチのパスワードを紛失したか忘れた場合，（2324 ページ）

パスワード回復がイネーブルになっている場合の手順

パスワード回復動作がイネーブルになっている場合は、次のメッセージが表示されます。

ステップ 1 フラッシュ ファイル システムを初期化します。

```
スイッチ: flash_init
```

ステップ 2 次のコマンドを使用して、スタートアップ コンフィギュレーションを無視します。

```
スイッチ: SWITCH_IGNORE_STARTUP_CFG=1
```

ステップ 3 *packages.conf* ファイルでスイッチをフラッシュからブートします。

```
スイッチ: boot flash:packages.conf
```

ステップ 4 **No** と応答して初期設定ダイアログを終了します。

```
Would you like to enter the initial configuration dialog? [yes/no]: No
```

ステップ 5 スイッチ プロンプトで、特権 EXEC モードを開始します。

```
スイッチ> enable
Switch#
```

ステップ 6 スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。

```
スイッチ# copy startup-config running-config Destination filename [running-config]?
```

確認を求めるプロンプトに、Return を押して応答します。これで、コンフィギュレーション ファイルがリロードされ、パスワードを変更できます。

ステップ 7 グローバル コンフィギュレーション モードを開始して、**イネーブル** パスワードを変更します。

```
スイッチ# configure terminal
スイッチ(config)#
```

ステップ 8 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
スイッチ# copy running-config startup-config
```

ステップ 9 手動ブート モードがイネーブルになっていることを確認します。

```
スイッチ# show boot

 BOOT variable = flash:packages.conf;
 Manual Boot = yes
 Enable Break = yes
```

ステップ 10 スイッチをリロードします。

```
スイッチ# reload
```

ステップ 11 （ステップ 2 と 3 で変更した）ブートローダ パラメータを元の値に戻します。

```
スイッチ: switch: SWITCH_IGNORE_STARTUP_CFG=0
```

ステップ 12 フラッシュからのスイッチ *packages.conf* を起動します。

```
スイッチ: boot flash:packages.conf
```

ステップ 13 スイッチ のブート後に、スイッチ で手動ブートをディセーブルにします。

```
スイッチ(config)# no boot manual
```

パスワード回復がディセーブルになっている場合の手順

パスワード回復メカニズムがディセーブルの場合、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

注意 スイッチをデフォルト設定に戻すと、既存の設定がすべて失われます。システム管理者に問い合わせて、バックアップ スイッチと VLAN（仮想 LAN）コンフィギュレーション ファイルがあるかどうかを確認してください。

- **n**（no）を入力すると、Mode ボタンを押さなかった場合と同様に、通常のブート プロセスが継続されます。ブートローダ プロンプトにはアクセスできません。したがって、新しいパスワードを入力できません。次のメッセージが表示されます。

  ```
  Press Enter to continue........
  ```

- **y**（yes）を入力すると、フラッシュ メモリ内のコンフィギュレーション ファイルおよび VLAN データベース ファイルが削除されます。デフォルト設定がロードされるときに、パスワードをリセットできます。

ステップ 1 パスワード回復手順の継続を選択すると、既存の設定が失われます。

```
Would you like to reset the system back to the default configuration (y/n)? Y
```

ステップ 2 フラッシュ メモリの内容を表示します。

スイッチ: **dir flash:**

スイッチのファイル システムが表示されます。

```
Directory of flash:/
.
.
.i'
15494  drwx        4096   Jan 1 2000 00:20:20 +00:00  kirch
15508  -rw-   258065648   Sep 4 2013 14:19:03 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
162196684
```

ステップ 3 システムを起動します。
```
スイッチ: boot
```

セットアッププログラムを起動するように求められます。パスワード回復手順を継続するには、プロンプトに **N** を入力します。

```
Continue with the configuration dialog? [yes/no]: N
```

ステップ 4 スイッチ プロンプトで、特権 EXEC モードを開始します。
```
スイッチ> enable
```

ステップ 5 グローバル コンフィギュレーション モードを開始します。
```
スイッチ# configure terminal
```

ステップ 6 パスワードを変更します。
```
スイッチ(config)# enable secret password
```

シークレット パスワードは 1 ～ 25 文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 7 特権 EXEC モードに戻ります。
```
スイッチ(config)# exit
スイッチ#
```

（注） ステップ 9 に進む前に、接続されているすべてのスタック メンバの電源を入れ、それらが完全に初期化されるまで待ちます。

ステップ 8 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
スイッチ# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。

ステップ 9 ここでスイッチを再設定する必要があります。システム管理者によって、バックアップ スイッチと VLAN コンフィギュレーション ファイルが使用可能に設定されている場合は、これらを使用します。

スイッチ スタック問題の回避

スイッチ スタックの問題を防止するには、次の作業を実行する必要があります。

- スイッチ スタックにスイッチを追加したり、そこから取り外したりする場合には、必ずスイッチの電源を切ってください。スイッチ スタックでの電源関連のあらゆる考慮事項については、ハードウェア インストレーション ガイドの「Switch Installation（スイッチのインストール）」の章を参照してください。

- スタック モード LED が点灯するまで、スタック メンバの **Mode** ボタンを押します。スイッチの最後の 2 つのポート LED がグリーンになります。スイッチ モデルに応じて、最後の 2 つのポートは 10/100/1000 ポートまたは Small Form-Factor Pluggable モジュールになります。最後の 2 つのポート LED の片方または両方がグリーンになっていない場合は、スタックが全帯域幅で稼働していません。
- スイッチ スタックを管理する場合は、1 つの CLI セッションだけを使用することを推奨します。アクティブ スイッチに複数の CLI セッションを使用する場合は注意が必要です。1 つのセッションで入力したコマンドは、別のセッションには表示されません。そのため、コマンドを入力したセッションを識別できなくなることがあります。
- スタック内での位置に従ってスタック メンバ番号を手動で割り当てると、リモートから行うスイッチ スタックのトラブルシューティングが容易になります。ただし、後からスイッチを追加したり、取り外したり、場所を入れ替えたりする際に、スイッチに手動で番号を割り当てたことを覚えておく必要があります。スタック メンバー番号を手動で割り当てるには、**switch***current-stack-member-number***renumber***new-stack-member-number* グローバル コンフィギュレーション コマンドを使用します。

スタック メンバをまったく同じモデルで置き換えると、新しいスイッチは、置き換えられたスイッチとまったく同じ設定で稼働します。この場合、新しいスイッチは置き換えられたスイッチと同じメンバ番号を使用するものと想定されます。

電源が入った状態のスタック メンバを取り外すと、スイッチ スタックが、それぞれ同じ設定を持つ 2 つ以上のスイッチ スタックに分割（パーティション化）されます。スイッチ スタックを分離されたままにしておきたい場合は、新しく作成されたスイッチ スタックの IP アドレス（複数の場合あり）を変更してください。パーティション化されたスイッチ スタックを元に戻すには、次の手順を実行します。

1. 新しく作成されたスイッチ スタックの電源を切ります。
2. 新しいスイッチ スタックを、StackWise Plus ポートを介して元のスイッチ スタックに再度接続します。
3. スイッチの電源を入れます。

スイッチ スタックおよびそのメンバのモニタリングに使用できるコマンドについては、「*Displaying Switch Stack Information*」の項を参照してください。

自動ネゴシエーションの不一致の防止

IEEE 802.3ab 自動ネゴシエーション プロトコルは速度（10 Mbps、100 Mbps、および SFP モジュール ポート以外の 1000 Mbps）およびデュプレックス（半二重または全二重）に関するスイッチの設定を管理します。このプロトコルは設定を適切に調整しないことがあり、その場合はパフォーマンスが低下します。不一致は次の条件で発生します。

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動で設定された速度またはデュプレックスのパラメータと異なっている場合。

- ポートを自動ネゴシエーションに設定したが、接続先ポートは自動ネゴシエーションを使用しない全二重に設定されている場合。

スイッチのパフォーマンスを最大限に引き出してリンクを確保するには、次のいずれかの注意事項に従って、デュプレックスおよび速度の設定を変更してください。

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 接続の両側でポートの速度とデュプレックスのパラメータを手動で設定します。

（注） 接続先装置が自動ネゴシエーションを実行しない場合は、2 つのポートのデュプレックス設定を一致させます。速度パラメータは、接続先のポートが自動ネゴシエーションを実行しない場合でも自動調整が可能です。

SFP モジュールのセキュリティと識別に関するトラブルシューティング

シスコの Small Form-Factor Pluggable（SFP）モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリティ コード、および巡回冗長検査（CRC）が格納されたシリアル EEPROM（電気的に消去可能でプログラミング可能な ROM）を備えています。スイッチに SFP モジュールを装着すると、スイッチ ソフトウェアは、EEPROM を読み取ってシリアル番号、ベンダー名、およびベンダー ID を確認し、セキュリティ コードおよび CRC を再計算します。シリアル番号、ベンダー名、ベンダー ID、セキュリティ コード、または CRC が無効な場合、ソフトウェアは、セキュリティ エラー メッセージを生成し、インターフェイスを errdisable ステートにします。

（注） セキュリティ エラー メッセージは、GBIC_SECURITY 機能を参照します。スイッチは、SFP モジュールをサポートしていますが、GBIC（ギガビット インターフェイス コンバータ）モジュールはサポートしていません。エラーメッセージテキストは、GBIC インターフェイスおよびモジュールを参照しますが、セキュリティ メッセージは、実際は SFP モジュールおよびモジュール インターフェイスを参照します。

他社の SFP モジュールを使用している場合、スイッチから SFP モジュールを取り外し、シスコのモジュールに交換します。シスコの SFP モジュールを装着したら、**errdisable recovery cause gbic-invalid** グローバル コンフィギュレーション コマンドを使用してポート ステータスを確認し、error-disabled ステートから回復する時間間隔を入力します。この時間間隔が経過すると、スイッチは error-disabled ステートからインターフェイスを復帰させ、操作を再試行します。**errdisable recovery** コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

モジュールがシスコ製 SFP モジュールとして識別されたにもかかわらず、システムがベンダー データ情報を読み取ってその情報が正確かどうかを確認できないと、SFP モジュール エラー メッ

セージが生成されます。この場合、SFP モジュールを取り外して再び装着してください。それでも障害が発生する場合は、SFP モジュールが不良品である可能性があります。

SFP モジュール ステータスのモニタリング

show interfaces transceiver 特権 EXEC コマンドを使用すると、SFP モジュールの物理または動作ステータスを確認できます。このコマンドは、温度や特定のインターフェイス上の SFP モジュールの現状などの動作ステータスと、アラーム ステータスを表示します。また、このコマンドを使用して SFP モジュールの速度およびデュプレックス設定も確認できます。詳細については、このリリースのコマンド リファレンスに記載された **show interfaces transceiver** コマンドの説明を参照してください。

ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティック ルートを定義するか、またはこれらのサブネット間でルーティングされるように IP ルーティングを設定する必要があります。

IP ルーティングは、デフォルトではすべてのスイッチでディセーブルになります。

（注） **ping** コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

このコマンドは、スイッチからネットワーク上の他のデバイスに ping を実行する目的で使用します。

コマンド	目的
ping ip*host* | *address* `スイッチ# ping 172.20.52.3`	IP またはホスト名やネットワーク アドレスを指定してリモート ホストに ping を実行します。

関連トピック

ping, （2325 ページ）
例：IP ホストの ping, （2354 ページ）

温度のモニタリング

スイッチは温度条件をモニタし、温度情報を使用してファンを制御します。

温度の値、状態、しきい値を表示するには、**show env temperature status** 特権 EXEC コマンドを使用します。温度の値は、スイッチ内の温度であり、外部の温度ではありません。**system env temperature threshold yellow** *value* グローバル コンフィギュレーション コマンドを使用してイエローのしきい値レベル（摂氏）だけを設定し、イエローのしきい値およびレッドのしきい値の差

を設定できます。グリーンまたはレッドのしきい値は設定できません。詳細については、このリリースのコマンド リファレンスを参照してください。

物理パスのモニタリング

次のいずれかの特権 EXEC コマンドを使用して、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスをモニタできます。

表 *168*：物理パスのモニタリング

コマンド	目的
tracetroute mac [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]	指定の送信元 MAC アドレスから、指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示します。
tracetroute mac ip {*source-ip-address* | *source-hostname*}{*destination-ip-address* | *destination-hostname*} [**detail**]	指定の送信元IPアドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示します。

IP traceroute の実行

（注） **traceroute** 特権 EXEC コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

コマンド	目的
traceroute ip*host* `スイッチ# traceroute ip 192.51.100.1`	ネットワーク上でパケットが通過するパスを追跡します。

関連トピック

IP Traceroute, （2327 ページ）
例：IP ホストに対する traceroute の実行, （2355 ページ）

TDR の実行および結果の表示

TDR を実行する場合、**test cable-diagnostics tdr interface***interface-id* 特権 EXEC コマンドを入力します。

TDR の結果を表示するには、**show cable-diagnostics tdr interface***interface-id* 特権 EXEC コマンドを入力します。

デバッグおよびエラー メッセージ出力のリダイレクト

ネットワーク サーバはデフォルトで、**debug** コマンドおよびシステム エラー メッセージの出力をコンソールに送信します。このデフォルトの設定を使用する場合は、コンソール ポートまたはイーサネット管理ポートに接続する代わりに、仮想端末接続によってデバッグ出力をモニタできます。

指定できる宛先として、コンソール、仮想端末、内部バッファ、および syslog サーバを実行している UNIX ホストがあります。Syslog フォーマットは、4.3 BSD UNIX およびそのバリエーションと互換性があります。

（注） デバッグの出力先がシステムのオーバーヘッドに影響を与えることがないように注意してください。メッセージをコンソールに記録すると、非常に高いオーバーヘッドが発生します。仮想端末にメッセージを記録すると、発生するオーバーヘッドは低くなります。Syslog サーバでメッセージ ロギングを行うと、オーバーヘッドはさらに小さくなり、内部バッファであれば最小限ですみます。

システム メッセージのロギングに関する詳細については、「システム メッセージ ロギングの設定」を参照してください。

関連トピック

debug コマンド, （2329 ページ）

show platform forward コマンドの使用

show platform forward 特権 EXEC コマンドの出力からは、インターフェイスに入るパケットがシステムを介して送信された場合、転送結果に関して、有意義な情報がいくつか得られます。パケットに関して入力されたパラメータに応じて、参照テーブル結果、転送宛先の計算に使用されるポート マップ、ビットマップ、および出力側の情報が表示されます。

このコマンドで出力される情報のほとんどは、主に、スイッチの用途別集積回路（ASIC）に関する詳細情報を使用するテクニカル サポート担当者に役立つものです。ただし、パケット転送情報はトラブルシューティングにも役立ちます。

show debug コマンドの使用方法

show debug コマンドは、特権 EXEC モードで入力します。このコマンドは、スイッチで使用可能なすべてのデバッグ オプションを表示します。

すべての条件付きデバッグ オプションを表示するには、コマンド **show debug condition** を実行します。コマンドは、条件 ID *<1-1000>*または *all* 条件を選択することで一覧表示できます。

デバッグを無効にするには、**no debug all** コマンドを使用します。

注意 デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 16.1 (Catalyst 3850 Switches)*』を参照してください。

OBFL の設定

注意 OBFL はディセーブルにせず、フラッシュ メモリに保存されたデータは削除しないことを推奨します。

- OBFL をイネーブルにするには、**hw-switch switch** [*switch-number*] **logging onboard** [**message level***level*] グローバル コンフィギュレーション コマンドを使用します。スイッチの場合、*switch-number* に指定できる範囲は 1 ～ 9 です。スイッチが生成してフラッシュ メモリに保存するハードウェア関連のメッセージの重大度を指定するには、**message level***level* パラメータを使用します。
- OBFL データをローカル ネットワークまたは指定したファイル システムにコピーするには、**copy onboard switch***switch-number***url***url-destination* 特権 EXEC コマンドを使用します。
- OBFL をディセーブルにするには、**no hw-switch switch** [*switch-number*] **logging onboard** [**message level**] グローバル コンフィギュレーション コマンドを使用します。
- フラッシュ メモリ内の稼働時間と CLI コマンド情報以外のすべての OBFL データをクリアするには、**clear onboard switch***switch-number* 特権 EXEC コマンドを使用します。
- スイッチ スタックでは、**hw-switch switch** [*switch-number*] **logging onboard** [**message level***level*] グローバル コンフィギュレーション コマンドを使用することにより、スタンドアロン スイッチまたはすべてのスタック メンバの OBFL をイネーブルにできます。
- アクティブ スイッチのメンバ スイッチの OBFL をイネーブルまたはディセーブルにできます。

ここで説明した各コマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

関連トピック

スイッチのオンボード障害ロギング, （2331 ページ）

OBFL 情報の表示, （2347 ページ）

ソフトウェア設定のトラブルシューティングの確認

OBFL 情報の表示

表 *169* : *OBFL* 情報を表示するためのコマンド

コマンド	目的
show onboard switch *switch-number* **clilog** `スイッチ# show onboard switch 1 clilog`	スタンドアロン スイッチまたは指定されたスタック メンバで入力されたOBFL CLI コマンドを表示します。
show onboard switch *switch-number* **environment** `スイッチ# show onboard switch 1 environment`	スタンドアロン スイッチまたは指定されたスタック メンバおよび接続されているすべての FRU デバイスの UDI 情報、PID、VID、およびシリアル番号を表示します。
show onboard switch *switch-number* **message** `スイッチ# show onboard switch 1 message`	スタンドアロン スイッチまたは指定されたスタック メンバによって生成されたハードウェア関連のメッセージを表示します。
show onboard switch *switch-number* **counter** `スイッチ# show onboard switch 1 counter`	スタンドアロン スイッチまたは指定したスタック メンバのカウンタ情報を表示します。
show onboard switch *switch-number* **temperature** `スイッチ# show onboard switch 1 temperature`	スタンドアロン スイッチまたは指定されたスイッチ スタック メンバの温度を表示します。
show onboard switch *switch-number* **uptime** `スイッチ# show onboard switch 1 uptime`	スタンドアロン スイッチまたは指定されたスタック メンバが起動した時刻、スタンドアロン スイッチまたは指定されたスタック メンバが再起動された理由、およびスタンドアロン スイッチまたは指定されたスタック メンバが最後に再起動されて以来の稼働時間を表示します。

コマンド	目的
show onboard switch *switch-number* **voltage** スイッチ# show onboard switch 1 voltage	スタンドアロン スイッチまたは指定されたスタック メンバのシステム電圧を表示します。
show onboard switch *switch-number* **status** スイッチ# show onboard switch 1 status	スタンドアロン スイッチまたは指定されたスタック メンバの状態を表示します。

関連トピック

スイッチのオンボード障害ロギング，（2331 ページ）
OBFL の設定，（2346 ページ）

例：高い CPU 使用率に関する問題と原因の確認

CPU 使用率が高いことが問題となっているかどうか判別するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の 1 行目にある下線が付いた部分に注目してください。

```
スイッチ# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

この例は、正常なCPU使用率を示しています。この出力によると、最後の5秒間の使用率が8%/0%となっていますが、この意味は次のとおりです。

- Cisco IOS の処理時間と割り込みの処理にかかった時間を合わせた CPU の合計の使用率は全体の 8%
- 割り込みの処理にかかった時間は全体の 0%

表 *170* : *CPU* 使用率に関する問題のトラブルシューティング

問題のタイプ	Cause	修正措置
割り込みのパーセント値が合計の CPU 使用率の値とほぼ同程度に高い	CPU がネットワークから受信するパケット数が多すぎる。	ネットワーク パケットのソースを判別する。データの流れを遮断するか、スイッチの設定を変更します。「Analyzing Network Traffic（ネットワークトラフィックの解析）」の項を参照してください。
割り込みの所要時間は最小限であったにもかかわらず CPU の合計使用率が 50% を超える	CPU 時間を過度に消費する Cisco IOS 処理が 1 つ以上存在する。これは通常、処理をアクティブ化するイベントによって始動されます。	異常なイベントを特定して根本的な原因を解消する。「Debugging Active Processes（アクティブなプロセスのデバッグ）」のセクションを参照してください。

ソフトウェア設定のトラブルシューティングのシナリオ

Power over Ethernet（PoE）に関するトラブルシューティングのシナリオ

表 *171*：*Power over Ethernet* に関するトラブルシューティングのシナリオ

症状または問題	考えられる原因と解決法
PoE がないポートは 1 つに限りません。 1 つのスイッチ ポートに限り問題が発生する。このポートでは PoE 装置と PoE 非対応の装置のいずれも動作しないが、他のポートでは動作します。	この受電デバイスが他の PoE ポートで動作するかを確認する。 **show run**、または **show interface status** ユーザ EXEC コマンドを使用して、ポートがシャットダウンしていないか、または error-disabled になっていないかを確認します。 （注） ほとんどのスイッチはポートがシャットダウンしているときはポートの電力供給をオフにします。これは、IEEE 仕様でこれがオプションに指定されている場合も同様です。 受電デバイスからスイッチ ポートまでのイーサネット ケーブルの動作が正常であることを確認します。具体的には、既知の正常な PoE 非対応のイーサネット装置とイーサネット ケーブルを接続して、受電デバイスがリンクを確立し他のホストとトラフィックを交換することを確認します。 スイッチのフロント パネルから受電デバイスまでのケーブル長の合計が 100 メートル以下であることを確認します。 スイッチ ポートからイーサネット ケーブルを外します。短いイーサネット ケーブルを使用して、既知の正常なイーサネット装置を、スイッチのフロント パネルの（パッチ パネルではない）このポートに直接接続します。これによってイーサネット リンクが確立され他のホストとトラフィックを交換できることを確認します。あるいは、ポートの VLAN SVI で ping を実行してください。次に、受電デバイスをこのポートに接続し、電源がオンになることを確認します。 パッチ コードをスイッチ ポートに接続しても受電デバイスの電源がオンにならない場合、接続する受電デバイスの合計数とスイッチの電力バジェット（使用可能な PoE）とを比較してください。**show inline power** コマンドを使用して、利用可能な電源の量を確認します。

症状または問題	考えられる原因と解決法
すべてのポートまたは 1 つのポートグループでPoEが機能しない。 すべてのスイッチポートで問題が発生する。電力が供給されていないイーサネット装置がどのポートでもイーサネットリンクを確立できず、PoE 装置の電源がオンになりません。	

症状または問題	考えられる原因と解決法
	電力に関するアラームが継続的に発生する、断続的に発生する、または再発する場合は、可能であれば電源モジュールを交換します（現場交換可能ユニットです）。そうでない場合はスイッチを交換してください。 連続する複数のポートで問題があるものの、すべてのポートで問題が発生するわけではない場合、電源の故障ではないと考えられ、スイッチのPoEレギュレータに関連した異常の可能性があります。 PoEの状況やステータスの変更について過去に報告されているアラームまたはシステムメッセージを確認するには、**show log** 特権 EXEC コマンドを使用します。 アラームがない場合は、**show interface status** コマンドを使用して、ポートがシャットダウンしていないかerrdisableになっていないかを確認します。ポートが error-disabled の場合、**shut** および **no shut** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。 特権 EXEC コマンドの **show env power** および **show power inline** を使用して、PoE のステータスおよび電力バジェット（使用可能な PoE）を調べます。 実行コンフィギュレーションを調べて **power inline never** がこのポートに設定されていないことを確認します。 受電していないイーサネット装置をスイッチ ポートに直接接続します。接続には短いパッチ コードだけを使用します。既存の配線ケーブルは使用しないでください。**shut** および **no shut** インターフェイス コンフィギュレーション コマンドを入力し、イーサネット リンクが確立されていることを確認します。正しく接続している場合、短いパッチ コードを使用して受電デバイスをこのポートに接続し、電源がオンになることを確認します。装置の電源がオンになったら、すべての中間パッチ パネルが正しく接続されているか確認してください。 1 本を除くすべてのイーサネット ケーブルをスイッチ ポートから抜きます。短いパッチ コードを使用して、1 つの PoE ポートにだけ受電デバイスを接続します。スイッチ ポートからの受電に比較して、受電デバイスが多くの電力を必要としないことを確認してください。 **show power inline** 特権 EXEC コマンドを使用して、ポートがシャットダウンしていない場合に、受電デバイスに電力が供給されることを確認します。あるいは、受電デバイスを観察して電源がオンになることを確認してください。

症状または問題	考えられる原因と解決法
	1 台の受電デバイスだけがスイッチに接続しているときに電力が供給される場合、残りのポートで **shut** および **no shut** インターフェイス コンフィギュレーション コマンドを入力してから、イーサネット ケーブルをスイッチの PoE ポートに 1 本ずつ再び接続してください。show interface status および **show power inline** 特権 EXEC コマンドを使用して、インライン電源の統計情報およびポートの状態をモニタします。 すべてのポートで、まだPoEが機能しない場合は、電源装置のPoEセクションでヒューズを開くことができる場合があります。この場合、アラームが生成されるのが一般的です。過去にシステム メッセージでアラームが報告されていないか、ログをもう一度チェックしてください。
Cisco IP Phone が切断またはリセットされる。 正常に動作した後で、Cisco phone またはワイヤレス アクセス ポイントが断続的にリロードしたり、PoE から切断されたりします。	スイッチから受電デバイスまでのすべての電気系統を確認してください。信頼性の低い接続は、電力供給の中断や受電デバイスの機能が不安定になる原因となり、受電デバイスの断続的な切断やリロードなどが発生します。 スイッチ ポートから受電デバイスまでのケーブル長が 100 メートル以下であることを確認してください。 スイッチが配置されている場所で電気環境にどのような変化があるか、切断時に、受電デバイスに何が起きるかについて注意してください。 切断と同時にエラー メッセージが表示されたか注意します。**show log** 特権 EXEC コマンドを使用してエラー メッセージを確認します。 リロードの発生直前に IP Phone から Call Manager へのアクセスが失われていないか確認してください（PoE の障害ではなくネットワークに問題が発生している場合があります）。 受電デバイスをPoE非対応の装置に交換し、装置が正しく動作することを確認します。PoE非対応の装置にリンク障害または高いエラー率がある場合、スイッチ ポートと受電デバイスを接続する信頼性の低いケーブル接続が問題の可能性があります。

症状または問題	考えられる原因と解決法
シスコ以外の受電デバイスがシスコ PoE スイッチで動作しない。 シスコ PoE スイッチに接続するシスコ以外の受電デバイスに電源が供給されないか、電源投入後すぐに電源が切れます。PoE 非対応装置は正常に動作します。	**show power inline** コマンドを使用して、受電デバイスの接続前後に、スイッチの電力バジェット（使用可能な PoE）が使い果たされていないか確認してください。受電デバイスを接続する前に、このタイプの装置に十分な電力が使用可能であることを確認します。 **show interface status** コマンドを使用して、接続されている受電デバイスをスイッチが検出することを確認します。 **show log** コマンドを使用して、ポートの過電流状態を報告したシステム メッセージがないか確認します。症状を正確に特定してください。最初に電力が受電デバイスに供給され、その後、切断される状態ですか。その場合は、問題は最初のサージ電流（突入電流）が原因で、ポートの電流上限しきい値が超過した可能性があります。

関連トピック

Power over Ethernet（PoE）ポート，（2324 ページ）

ソフトウェアのトラブルシューティングの設定例

例：IP ホストの ping

次に、IP ホストに ping を実行する例を示します。

```
スイッチ# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
スイッチ#
```

表 *172*：*Ping* の出力表示文字

文字	説明
!	感嘆符 1 個につき 1 回の応答を受信したことを示します。
.	ピリオド 1 個につき応答待ちの間にネットワーク サーバのタイムアウトが 1 回発生したことを示します。

文字	説明
U	宛先到達不能エラー PDU を受信したことを示します。
C	輻輳に遭遇したパケットを受信したことを示します。
I	ユーザによりテストが中断されたことを示します。
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

ping セッションを終了するには、エスケープ シーケンス（デフォルトでは Ctrl+^ X）を入力してください。Ctrl キー、Shift キー、および 6 キーを同時に押してから放し、その後 X キーを押します。

関連トピック

ping, （2325 ページ）
ping の実行, （2343 ページ）

例：IP ホストに対する traceroute の実行

次に、IP ホストに **traceroute** を実行する例を示します。

```
スイッチ# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

  1 192.0.2.1 0 msec 0 msec 4 msec
  2 192.0.2.203 12 msec 8 msec 0 msec
  3 192.0.2.100 4 msec 0 msec 0 msec
  4 192.0.2.10 0 msec 4 msec 0 msec
```

ディスプレイには、送信される 3 つのプローブごとに、ホップ カウント、ルータの IP アドレス、およびラウンドトリップ タイム（ミリ秒単位）が表示されます。

表 *173*：*traceroute* の出力表示文字

文字	説明
*	プローブがタイムアウトになりました。

文字	説明
?	パケット タイプが不明です。
A	管理上、到達不能です。通常、この出力は、アクセスリストがトラフィックをブロックしていることを表しています。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	発信元。
U	ポートが到達不能です。

実行中の追跡を終了するには、エスケープ シーケンス（デフォルトでは Ctrl+^ X）を入力してください。Ctrl キー、Shift キー、および 6 キーを同時に押してから放し、その後 X キーを押します。

関連トピック

IP Traceroute, （2327 ページ）
IP traceroute の実行, （2344 ページ）

例：すべてのシステム診断をイネーブルにする

注意 デバッグ出力は他のネットワーク トラフィックより優先され、**debug all** 特権 EXEC コマンドは他の **debug** コマンドより出力が大量になるので、スイッチのパフォーマンスが極度に低下したり、場合によっては使用不能になったりすることがあります。状況にかかわらず、特定性の高い **debug** コマンドを使用するのが原則です。

このコマンドは、すべてのシステム診断をディセーブルにします。

```
スイッチ# debug all
```

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。いずれかの **debug** コマンドが誤ってイネーブルのままにならないようにするには、**no debug all** コマンドを使用すると便利です。

関連トピック

debug コマンド, （2329 ページ）

ソフトウェア設定のトラブルシューティングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference (Catalyst 3650 Switches)*
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S（Catalyst 3650 Switches）*
Platform_independent の設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S（Catalyst 3650 Switches）*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

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

シスコのテクニカル サポート

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

ソフトウェア設定のトラブルシューティングの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

関連トピック

機能情報の確認，（49 ページ）

第 XV 部

VideoStream

- VideoStream の設定，2361 ページ

第 103 章

VideoStream の設定

- 機能情報の確認，2361 ページ
- VideoStream の前提条件，2361 ページ
- VideoStream の設定に関する制限，2362 ページ
- VideoStream について，2362 ページ
- VideoStream の設定方法，2362 ページ
- メディア ストリームの監視，2368 ページ

機能情報の確認

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

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

VideoStream の前提条件

マルチキャスト機能が有効であることを確認します。コントローラ上の IP マルチキャストは multicast-multicast モードで設定することをお勧めします。

クライアント マシン上の IP アドレスを確認します。マシンには、それぞれの VLAN の IP アドレスが必要です。

アクセス ポイントがコントローラに join していることを確認します。

VideoStream の設定に関する制限

この MC2UC 機能を作動させるには、IGMP スヌーピングがオンになっている必要があります。

VideoStream について

IEEE 802.11 ワイヤレス マルチキャスト配信メカニズムには、パケットの消失や破損を認識するための、信頼できる方法がありません。マルチキャスト フレーム パケットは、ワイヤレス クライアントの最適なデータ レートに関係なく、所定のレートで送信されます。結果として、無線配信中にマルチキャストパケットが消失しても再送されないため、IPマルチキャストストリームが表示できなくなることがあります。また、パケットが高速で渡された場合、パケットは輻輳状態になります。

VideoStream 機能では、マルチキャスト フレームをユニキャスト ストリームにワイヤレスで変換することで、IP マルチキャスト ストリームのワイヤレス配信を信頼できるものにします。VideoStream クライアントは、それぞれビデオ IP マルチキャスト ストリームの受信を認識します。

VideoStream の設定方法

メディア ストリームのマルチキャストダイレクトのグローバル設定

手順の概要

1. **configure terminal**
2. **wireless multicast**
3. **IP igmp snooping**
4. **IP igmp snooping querier**
5. **wireless media-stream multicast-direct**
6. **wireless media-stream message**
7. **wireless media-stream group**<*name*><*startIp*><*endIp*>
8. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**wireless multicast**	ワイヤレス転送のマルチキャストをイネーブルにします。
ステップ 3	**IP igmp snooping**	VLAN ごとに IGMP スヌーピングをイネーブルにします。グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。
ステップ 4	**IP igmp snooping querier**	クエリーを生成するマルチキャストルータが VLAN 内に存在しない場合に、インターフェイスのスヌーピング クエリアを設定します。
ステップ 5	**wireless media-stream multicast-direct** 例： `Switch(config)#wireless media-stream multicast-direct`	コントローラのグローバルなマルチキャストダイレクト機能を設定します。

ステップ 6	**wireless media-stream message**
	
	例：
	`Switch(config)#wireless media-stream message ?`
	`  Email  Configure Session Announcement Email`
	`  Notes  Configure Session Announcement notes`
	`  URL  Configure Session Announcement URL`
	`  phone  Configure Session Announcement Phone number`
	`  <cr>`
		電話、URL、電子メール、メモなど、さまざまなメッセージ設定パラメータを設定します。つまり、メディア ストリームが（帯域幅制約が原因で）拒否される場合、メッセージをユーザに送信できます。これらのパラメータは、IT サポートの電子メールアドレス、メモ（ストリームが拒否された理由を説明する画面メッセージ）、ユーザがリダイレクトされる URL、拒否されたストリームについてユーザが問い合わせをする電話番号など、送信するメッセージを設定します。

ステップ 7	**wireless media-stream group** *<name><startIp><endIp>*
	
	例：
	`Switch(config)#wireless media-stream group grp1 231.1.1.1 239.1.1.3`
	`Switch(config-media-stream)#?`
	
	`  avg-packet-size  Configures average packet size`
	`  default  Set a command to its defaults`
	`  exit  Exit sub-mode`
	`  max-bandwidth  Configures maximum Expected Stream Bandwidth in Kbps`
	`  no  Negate a command or set its defaults`
	`  policy  Configure media stream admission policy`
	`  qos  Configure  Over the AIR QoS class, <'video'> ONLY`
	
	`  <cr>`
		予想されるマルチキャスト宛先アドレス、ストリームの帯域幅の使用量およびストリームの優先順位のパラメータなど、各メディア ストリームとそのパラメータを設定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 帯域のメディア ストリームの設定

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz media-stream multicast-direct**
3. **ap dot11 24ghz | 5ghz media-stream video-redirect**
4. **ap dot11 24ghz | 5ghz media-stream multicast-direct admission-besteffort**
5. **ap dot11 24ghz | 5ghz media-stream multicast-direct client-maximum [<value >]**
6. **ap dot11 24ghz | 5ghz media-stream multicast-direct radio-maximum 20**
7. **ap dot11 24ghz | 5ghz cac multimedia max-bandwidth [<bandwidth>]**
8. **ap dot11 24ghz | 5ghz cac media-stream multicast-direct min_client_rate [<dot11_rate>]**
9. **ap dot11 5ghz cac media-stream**
10. **ap dot11 5ghz cac multimedia**
11. **ap dot11 5ghz cac video**
12. **ap dot11 5ghz cac voice**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz media-stream multicast-direct** 例： スイッチ(config)#**ap dot11 24ghz media-stream multicast-direct**	メディア ストリーム（mc2uc）で 802.11 帯域が使用できる場合に設定します

	コマンドまたはアクション	目的
ステップ 3	**ap dot11 24ghz | 5ghz media-stream video-redirect** 例： スイッチ(config)#**ap dot11 24ghz media-stream video-redirect**	ユニキャスト ビデオ トラフィックをベスト エフォート キューにリダイレクトするように設定します。
ステップ 4	**ap dot11 24ghz | 5ghz media-stream multicast-direct admission-besteffort** 例： スイッチ(config)#**ap dot11 24ghz media-stream multicast-direct admission-besteffort**	帯域幅のアベイラビリティの制約によりメディア ストリームを優先できない場合でも、メディア ストリームがベスト エフォート キューを介して送信されるように設定します。帯域幅のアベイラビリティの制約によりメディア ストリームを優先できない場合、noをコマンドに追加して、ストリームをドロップします。
ステップ 5	**ap dot11 24ghz | 5ghz media-stream multicast-direct client-maximum [<value >]** 例： スイッチ(config)#**ap dot11 24ghz media-stream multicast-direct client-max 15**	個々のクライアントごとに許可されたメディア ストリームの最大数を設定します。最大値は 15 で、デフォルトは 0 です。値 0 は、無制限のストリームを意味します。
ステップ 6	**ap dot11 24ghz | 5ghz media-stream multicast-direct radio-maximum 20**	無線ストリームの最大数を設定します。有効な範囲は 1 ～ 20 です。デフォルトは 0 です。値 0 は、無制限のストリームを意味します。
ステップ 7	**ap dot11 24ghz | 5ghz cac multimedia max-bandwidth [<bandwidth>]** 例： スイッチ(config)#**ap dot11 24ghz cac multimedia max-bandwidth 60**	最大メディア（音声およびビデオ）帯域幅を % 単位で設定します。範囲は 5 % ～ 85 % です。
ステップ 8	**ap dot11 24ghz | 5ghz cac media-stream multicast-direct min_client_rate [<dot11_rate>]** 例： スイッチ(config)#**ap dot11 24ghz cac media-stream multicast-direct min_client_rate**	クライアントがユニキャストとしてメディア ストリームを送信するために必要な最小 PHY レートを設定します。これよりも低いレートで通信するクライアントは、メディア ストリームをユニキャスト フローとして受信しません。通常、この PHY レートは、マルチキャスト フレームが送信されるレートと同じかそれ以上です。
ステップ 9	**ap dot11 5ghz cac media-stream**	メディア ストリーム アクセス カテゴリの CAC パラメータを設定します。
ステップ 10	**ap dot11 5ghz cac multimedia**	音声およびビデオに使用されるメディア アクセス カテゴリの CAC パラメータを設定します。
ステップ 11	**ap dot11 5ghz cac video**	音声シグナリングに使用されるビデオ アクセス カテゴリの CAC パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 12	**ap dot11 5ghz cac voice**	音声アクセス カテゴリの CAC パラメータを設定します。
ステップ 13	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ビデオ ストリーミング用の WLAN 設定

手順の概要

1. **configure terminal**
2. **wlan** *wlan_name*
3. **shutdown**
4. **media-stream multicast-direct**
5. **no shutdown**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan_name* 例： Switch(config)#**wlan wlan50**	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**shutdown** 例： Switch(config-wlan)#**shutdown**	パラメータを設定するために、WLAN をディセーブルにします。
ステップ 4	**media-stream multicast-direct** 例： Switch(config)#**media-stream multicast-direct**	メディア ストリームのマルチキャスト ダイレクト機能を WLAN で設定します。

	コマンドまたはアクション	目的
ステップ 5	**no shutdown** 例： `Switch(config-wlan)#no shutdown`	WLAN をイネーブルにします。
ステップ 6	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

メディア ストリームの削除

はじめる前に

メディア ストリームをイネーブルにしてから、削除を設定する必要があります。

手順の概要

1. **configure terminal**
2. **no wireless media-stream group media_stream_name**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no wireless media-stream group media_stream_name** 例： `スイッチ(config)#no wireless media-stream grp1`	コマンドで指定する名前を持つメディア ストリームを削除します。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

メディア ストリームの監視

表 *174* : メディア ストリームの監視用のコマンド

コマンド	説明
show wireless media-stream client detail *group name*	特定のグループのメディア ストリーム クライアントの詳細を表示します。
show wireless media-stream client summary	すべてのクライアントのメディア ストリーム情報を表示します。
show wireless media-stream group detail *group name*	特定のグループのメディア ストリーム設定の詳細を表示します。
show wireless media-stream group summary	すべてのグループのメディア ストリーム設定の詳細を表示します。
show wireless media-stream message details	セッション通知メッセージの詳細を表示します。
show wireless multicast	マルチキャストダイレクト設定の状態を表示します。
show ap dot11 24ghz | 5ghz media-stream rrc	802.11 メディアのリソース予約コントロールの設定を表示します。

第 XVI 部

VLAN

- VTP の設定，2371 ページ
- VLAN の設定，2401 ページ
- VLAN グループの設定，2425 ページ
- VLAN トランクの設定，2433 ページ
- 音声 VLAN の設定，2459 ページ
- プライベート VLAN の設定，2471 ページ

第 104 章

VTP の設定

- 機能情報の確認，2371 ページ
- VTP の前提条件，2372 ページ
- VTP の制約事項，2372 ページ
- VTP の概要，2373 ページ
- VTP の設定方法，2383 ページ
- VTP のモニタ，2396 ページ
- VTP の設定例，2397 ページ
- 次の作業，2397 ページ
- その他の参考資料，2397 ページ
- VTP の機能履歴と情報，2399 ページ

機能情報の確認

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

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

VTP の前提条件

VLAN を作成する前に、ネットワークで VLAN Trunking Protocol（VTP）を使用するかどうかを決定する必要があります。VTP を使用すると、1 つまたは複数のスイッチ上で中央集約的に設定変更を行い、その変更を自動的にネットワーク上の他のスイッチに伝達できます。VTP を使用しない場合、VLAN 情報を他のスイッチに送信することはできません。

VTP は、1 つのスイッチで行われた更新が VTP を介してドメイン内の他のスイッチに送信される環境で動作するように設計されています。VLAN データベースに対する複数の更新が同一ドメイン内のスイッチ上で同時に発生する環境の場合、VTP は適切に機能せず、VLAN データベースの不整合が生じます。

スイッチは合計 4094 の VLAN をサポートします。ただし、設定済み機能の個数によって、スイッチ ハードウェアの使用状況は左右されます。VTP が新しい VLAN をスイッチに通知し、スイッチが使用可能な最大限のハードウェア リソースをすでに使用している場合、コントローラはハードウェア リソース不足を伝えるメッセージを送信して、VLAN をシャットダウンします。**show vlan** ユーザ EXEC コマンドの出力に、サスペンド ステートの VLAN が示されます。

トランク ポートは VTP アドバタイズを送受信するので、スイッチまたはスイッチ スタック上で少なくとも 1 つのトランクポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。

関連トピック

VTP アドバタイズ, （2375 ページ）

VTP ドメインへの VTP クライアント スイッチの追加（CLI）, （2393 ページ）

VTP Domain, （2373 ページ）

VTP モード, （2374 ページ）

VTP の制約事項

次に、VTP に関する制約事項を示します。

- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

注意 VTP クライアント スイッチを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。

VTP の概要

VTP

VTP は、レイヤ 2 のメッセージプロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。VTP により、VLAN 名の重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。

VTP 機能はスタック全体でサポートされており、スタック内のすべてのスイッチが、アクティブスイッチから継承した同一の VLAN および VTP コンフィギュレーションを保持します。スイッチが VTP メッセージを通じて新しい VLAN について学習したり、ユーザが新しい VLAN を設定したりすると、新しい VLAN 情報がスタック内のすべてのスイッチに伝達されます。

スイッチがスタックに参加するか、またはスタックの結合が発生すると、新しいスイッチはアクティブ スイッチから VTP 情報を取得します。

VTP Domain

VTP ドメイン（別名 VLAN 管理ドメイン）は、1 つのスイッチ、または同じ VTP ドメイン名を共有して同一管理下にある相互接続された複数のスイッチまたはスイッチスタックで構成されます。スイッチは、1 つの VTP ドメインにだけ所属できます。そのドメインに対してグローバル VLAN の設定を変更します。

デフォルトの設定では、トランク リンク（複数 VLAN のトラフィックを伝送するリンク）を介してドメインについてのアドバタイズを受信しない限り、またはユーザがドメイン名を設定しない限り、スイッチは VTP 非管理ドメイン ステートです。管理ドメイン名を指定するか学習するまでは、VTP サーバ上で VLAN を作成または変更できません。また、VLAN 情報はネットワークを介して伝播されません。

スイッチが、トランク リンクを介して VTP アドバタイズを受信した場合、管理ドメイン名および VTP 設定のリビジョン番号を継承します。その後スイッチは、別のドメイン名または古いコンフィギュレーション リビジョン番号が指定されたアドバタイズについては、すべて無視します。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのスイッチに伝播されます。VTP アドバタイズは、IEEE 802.1Q を含め、すべての IEEE トランク接続に送信されます。VTP は、複数の LAN タイプにわたり、固有の名前と内部インデックスの対応によって VLAN を動的にマッピングします。このマッピングにより、ネットワーク管理者がデバイスを管理するための作業負担が大幅に軽減されます。

VTP トランスペアレント モードでスイッチを設定した場合、VLAN の作成および変更は可能ですが、その変更はドメイン内の他のスイッチには送信されません。また、変更が作用するのは、個々のスイッチに限られます。ただし、スイッチがこのモードのときに設定を変更すると、変更内容がスイッチの実行コンフィギュレーションに保存されます。この変更はスイッチのスタートアップ コンフィギュレーション ファイルに保存することもできます。

関連トピック

VTP ドメインへの VTP クライアント スイッチの追加（CLI），（2393 ページ）

VTP の前提条件，（2372 ページ）

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング，（2494 ページ）

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする，（2498 ページ）

VTP モード

表 *175*：*VTP* モード

VTP Mode	説明
VTP サーバ	VTP サーバモードでは、VLAN の作成、変更、削除ができます。また、VTP ドメイン全体に対して他のコンフィギュレーション パラメータ（VTP バージョンなど）を指定できます。VTP サーバは、同一 VTP ドメイン内の他のスイッチに自身の VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズに基づいて、自身の VLAN 設定を他のスイッチと同期させます。 VTP サーバがデフォルトのモードです。 VTP サーバ モードでは、VLAN 設定は NVRAM に保存されます。スイッチがコンフィギュレーションを NVRAM に書き込んでいる間に障害を検出すると、VTP モードはサーバ モードからクライアント モードに自動的に移行します。この場合、NVRAM が正常に動作するまで、スイッチを VTP サーバ モードに戻すことはできません。
VTP クライアント	VTP クライアントは VTP サーバと同様に機能し、そのトランクで VTP アップデートを送受信しますが、VTP クライアント上で VLAN の作成、変更、削除を行うことはできません。VLAN は、ドメインに含まれる、他のサーバ モードのスイッチで設定します。 VTP バージョン 1 および 2 の VTP クライアント モードでは、VLAN 設定は NVRAM に保存されません。VTP バージョン 3 では、VLAN 設定はクライアント モードで NVRAM に保存されます。

VTP Mode	説明
VTP トランスペアレント	VTP トランスペアレント スイッチは、VTP に参加しません。VTP トランスペアレントスイッチは自身のVLAN設定をアドバタイズせず、受信したアドバタイズに基づいて自身のVLAN設定を同期させることもありません。ただし、VTPバージョン2またはバージョン3では、トランスペアレント スイッチは、トランク インターフェイスを介して他のスイッチから受信したVTPアドバタイズを転送します。VTP トランスペアレント モードでは、スイッチ上の VLAN を作成、変更、削除できます。 スイッチが VTP トランスペアレント モードの場合、VTP および VLAN の設定はNVRAMに保存されますが、他のスイッチにはアドバタイズされません。このモードでは、VTP モードおよびドメイン名はスイッチの実行コンフィギュレーションに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。 スイッチ スタックでは、実行コンフィギュレーションと保存されているコンフィギュレーションは、スタック内のすべてのスイッチについて同じです。
VTP オフ	VTP オフ モードでのスイッチの機能は、トランクを介して VTP アドバタイズを転送しないことを除くと VTP トランスペアレント スイッチとしての機能と同じです。

関連トピック

VTP の前提条件, （2372 ページ）
VTP モードの設定（CLI）, （2383 ページ）

VTP アドバタイズ

VTP ドメイン内の各スイッチは、専用のマルチキャスト アドレスに対して、それぞれのトランク ポートからグローバル コンフィギュレーション アドバタイズを定期的に送信します。ネイバー スイッチは、このようなアドバタイズを受信し、必要に応じて各自の VTP および VLAN 設定をアップデートします。

VTP アドバタイズにより、次のグローバル ドメイン情報が配信されます。

- VTP ドメイン名
- VTP 設定のリビジョン番号
- アップデート ID およびアップデート タイムスタンプ
- 各 VLAN の最大伝送単位（MTU）サイズを含む MD5 ダイジェスト VLAN コンフィギュレーション
- フレーム形式

VTP アドバタイズではさらに、設定されている各 VLAN について、次の VLAN 情報が配信されます。

- VLAN ID（IEEE 802.1Q を含む）
- VLAN 名
- VLAN タイプ
- VLAN ステート
- VLAN タイプ固有のその他の VLAN 設定情報

VTP バージョン 3 では、VTP アドバタイズにはプライマリ サーバ ID、インスタンス番号、および開始インデックスも含まれます。

関連トピック

VTP の前提条件, （2372 ページ）

VTP バージョン 2

ネットワークで VTP を使用する場合、VTP のどのバージョンを使用するかを決定する必要があります。デフォルトでは、バージョン 1 の VTP が動作します。

VTP バージョン 1 でサポートされず、バージョン 2 でサポートされる機能は、次のとおりです。

- トークンリング サポート：VTP バージョン 2 は、トークンリング ブリッジ リレー機能（TrBRF）およびトークンリング コンセントレータ リレー機能（TrCRF）VLAN をサポートします。
- 認識不能な Type-Length-Value（TLV）のサポート：VTP サーバまたは VTP クライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。認識されなかった TLV は、スイッチが VTP サーバ モードで動作している場合、NVRAM に保存されます。
- バージョン依存型トランスペアレント モード：VTP バージョン 1 の場合、VTP トランスペアレント スイッチが VTP メッセージ中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限りメッセージを転送します。VTP バージョン 2 がサポートするドメインは 1 つだけですが、VTP バージョン 2 トランスペアレント スイッチは、ドメイン名が一致した場合のみメッセージを転送します。
- 整合性検査：VTP バージョン 2 では、CLI または SNMP を介して新しい情報が入力された場合に限り、VLAN 整合性検査（VLAN 名、値など）を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

関連トピック

VTP バージョンのイネーブル化（CLI）, （2388 ページ）

VTP バージョン 3

VTP バージョン 1 または 2 でサポートされず、バージョン 3 でサポートされる機能は、次のとおりです。

- 拡張認証：認証を **hidden** または **secret** として設定できます。設定を **hidden** にしている場合、パスワード文字列からの秘密キーは VLAN のデータベース ファイルに保存されますが、設定においてプレーンテキストで表示されることはありません。代わりに、パスワードに関連付けられているキーが 16 進表記で実行コンフィギュレーションに保存されます。ドメインにテイクオーバー コマンドを入力するときは、パスワードを再入力する必要があります。キーワード **secret** を入力する場合、パスワードに秘密キーを直接設定できます。
- 拡張範囲 VLAN （VLAN 1006 ～ 4094）データベース伝播のサポート：VTP バージョン 1 および 2 では VLAN 1 ～ 1005 だけが伝播されます。

  （注） VTP プルーニングは引き続き VLAN 1 ～ 1005 にだけ適用され、VLAN 1002 ～ 1005 は予約されたままで変更できません。

- ドメイン内のデータベースのサポート：VTP 情報の伝播に加え、バージョン 3 では、Multiple Spanning Tree（MST）プロトコル データベース情報も伝播できます。VTP プロトコルの個別インスタンスが VTP を使用する各アプリケーションで実行されます。
- VTP プライマリ サーバと VTP セカンダリ サーバ：VTP プライマリ サーバは、データベース情報を更新し、システム内のすべてのデバイスに適用されるアップデートを送信します。VTP セカンダリ サーバで実行できるのは、プライマリ サーバから NVRAM に受け取ったアップデート済み VTP コンフィギュレーションのバックアップだけです。

  デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。**vtp primary** 特権 EXEC コマンドを入力してプライマリ サーバを指定することができます。プライマリ サーバのステータスは、管理者がドメインでテイクオーバー メッセージを発行する場合、データベースのアップデート用に必要となるだけです。プライマリ サーバなしで実用 VTP ドメインを持つことができます。プライマリ サーバのステータスは、スイッチにパスワードが設定されている場合でも、装置がリロードしたり、ドメインのパラメータが変更したりすると失われます。
- VTP をトランク単位（ポート単位）でオンまたオフにするオプション：ポート単位で VTP をイネーブルまたはディセーブルにするには、**[no] vtp** インターフェイス コンフィギュレーション コマンドを入力します。トランク ポート上で VTP をディセーブルにすると、そのポートのすべての VTP インスタンスがディセーブルになります。VTP の設定を、MST データベースには *off* にする一方で、同じポートの VLAN データベースには *on* にすることはできません。

  グローバルに VTP モードをオフに設定すると、システムのすべてのトランク ポートにこの設定が適用されます。ただし、VTP インスタンス ベースでこのモードのオンまたはオフを指定することはできます。たとえば、VLAN データベースには、スイッチを VTP サーバとして設定する一方で、MST データベースには VTP を *off* に設定することができます。

関連トピック

VTP バージョンのイネーブル化（CLI），（2388 ページ）

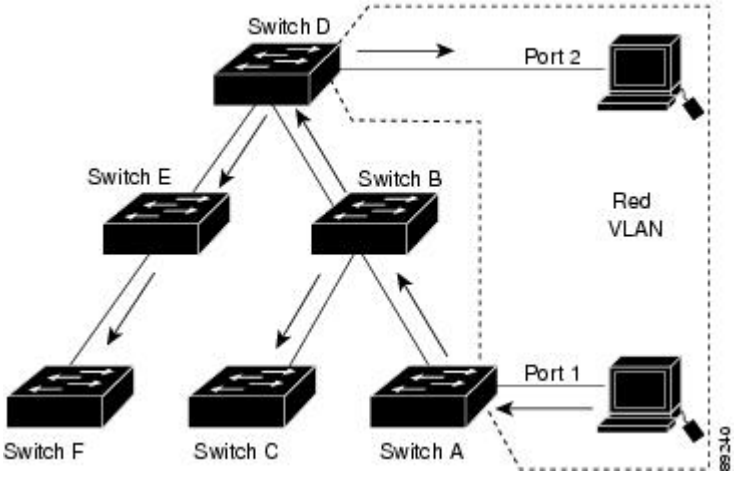
VTP プルーニング

VTP プルーニングを使用すると、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されるので、使用可能なネットワーク帯域幅が増えます。VTP プルーニングを使用しない場合、スイッチは受信側のスイッチで廃棄される可能性があっても、VTP ドメイン内のすべてのトランク リンクに、ブロードキャスト、マルチキャスト、および不明のユニキャスト トラフィックをフラッディングします。VTP プルーニングはデフォルトでディセーブルです。

VTP プルーニングは、プルーニング適格リストに指定された VLAN トランク ポートへの不要なフラッディング トラフィックを阻止します。プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトでは、スイッチのトランク ポート上で VLAN 2 ～ 1001 がプルーニング適格です。プルーニング不適格として設定した VLAN については、引き続きフラッディングが行われます。VTP プルーニングはすべてのバージョンの VTP でサポートされます。

VTP プルーニングは、スイッチド ネットワークではディセーブルです。スイッチ A のポート 1 およびスイッチ D のポート 2 は、Red という VLAN に割り当てられています。スイッチ A に接続されたホストからブロードキャストが送信された場合、スイッチ A は、このブロードキャストをフラッディングします。Red VLAN にポートを持たないスイッチ C、E、F も含めて、ネットワーク内のすべてのスイッチがこのブロードキャストを受信します。

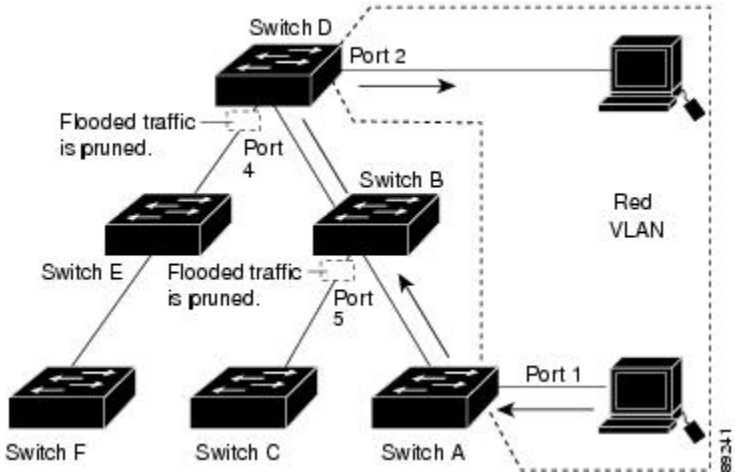
図 *96*：*VTP* プルーニングを使用しない場合のフラッディング トラフィック



VTP プルーニングは、スイッチド ネットワークではイネーブルです。スイッチ A からのブロードキャスト トラフィックは、スイッチ C、E、F には転送されません。図に示されているリンク ポー

ト（スイッチ B のポート 5、およびスイッチ D のポート 4）で、Red VLAN のトラフィックがプルーニングされるからです。

図 *97* : *VTP* プルーニングによるフラッディング トラフィックの最適化



VTP バージョン 1 および 2 では、VTP サーバでプルーニングをイネーブルにすると、その VTP ドメイン全体でプルーニングがイネーブルになります。VTP バージョン 3 では、ドメイン内の各スイッチ上で手動によってプルーニングをイネーブルにする必要があります。VLAN をプルーニング適格または不適格として設定する場合、影響を受けるのは、そのトランク上の VLAN のプルーニングだけです（VTP ドメイン内のすべてのスイッチに影響するわけではありません）。

VTP プルーニングは、イネーブルにしてから数秒後に有効になります。VTP プルーニング不適格の VLAN からのトラフィックは、プルーニングの対象になりません。VLAN 1 および VLAN 1002 ～ 1005 は常にプルーニング不適格です。これらの VLAN からのトラフィックはプルーニングできません。拡張範囲 VLAN（1005 を超える VLAN ID）もプルーニング不適格です。

関連トピック

VTP プルーニングのイネーブル化（CLI），（2390 ページ）

VTP とスイッチ スタック

VTP 設定は、スイッチ スタックのすべてのメンバで同一です。スイッチ スタックが VTP サーバ、クライアント、またはトランスペアレント モードになっている場合、スタック内のすべてのスイッチの VTP 設定が同一になります。

- スタックに参加したスイッチは、VTP および VLAN のプロパティをアクティブなスイッチから継承します。
- すべての VTP アップデートが、スタック全体で保持されます。
- スタック内のスイッチの VTP モードが変更されると、そのスタック内のその他のスイッチも VTP モードを変更し、スイッチの VLAN データベースの一貫性が保たれます。

VTP バージョン 3 は、スタンドアロン スイッチでもスタックでも同じように機能しますが、スイッチ スタックが VTP データベースのプライマリ サーバである場合だけは例外です。この場合は、アクティブなスイッチの MAC アドレスがプライマリ サーバ ID として使用されます。アクティブなスイッチがリロードされるか電源オフになると、新たにアクティブなスイッチが選択されます。

- 固定 MAC アドレス機能を設定しない場合、新たにアクティブなスイッチが選択されると、現在のスタック MAC アドレスを使用してテイクオーバー メッセージを送信します。

（注） デフォルトでは、永続的 MAC アドレスがオンになっています。

VTP 設定時の注意事項

VTP の設定要件

VTP を設定する場合は、スイッチがドメイン内の他のスイッチと VTP アドバタイズを送受信できるように、トランク ポートを設定する必要があります。

VTP の設定

VTP 情報は VTP VLAN データベースに保存されます。VTP モードがトランスペアレントである場合、VTP ドメイン名およびモードはスイッチの実行コンフィギュレーション ファイルにも保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。スイッチをリセットした場合にも、VTP モードをトランスペアレントとして保存するには、このコマンドを使用する必要があります。

スイッチのスタートアップ コンフィギュレーション ファイルに VTP 情報を保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

関連トピック

ポート単位の VTP の設定（CLI），（2391 ページ）

VTP バージョン 3 のプライマリ サーバの設定（CLI），（2387 ページ）

VTP 設定のためのドメイン名

VTP を初めて設定するときは、必ずドメイン名を割り当てる必要があります。また、VTP ドメイン内のすべてのスイッチを、同じドメイン名で設定しなければなりません。VTP トランスペアレントモードのスイッチは、他のスイッチと VTP メッセージを交換しません。これらのコントローラについては VTP ドメイン名を設定する必要はありません。

（注） NVRAM および DRAM の記憶域が十分にある場合は、VTP ドメイン内のすべてのスイッチを VTP サーバ モードにする必要があります。

注意 すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメインを設定しないでください。ドメインを設定すると、そのドメインの VLAN 設定を変更できなくなります。VTP ドメイン内の少なくとも 1 台のスイッチを VTP サーバ モードに設定してください。

関連トピック

VTP ドメインへの VTP クライアント スイッチの追加（CLI），（2393 ページ）

VTP ドメインのパスワード

VTP ドメインのパスワードは設定できますが、必須ではありません。ドメイン パスワードを設定する場合は、すべてのドメイン スイッチで同じパスワードを共有し、管理ドメイン内のスイッチごとにパスワードを設定する必要があります。パスワードのないスイッチ、またはパスワードが不正なコントローラは、VTP アドバタイズを拒否します。

ドメインに VTP パスワードを設定する場合、VTP 設定なしで起動したスイッチは、正しいパスワードを使用して設定しない限り、VTP アドバタイズを受信しません。設定後、スイッチは同じパスワードおよびドメイン名を使用した次の VTP アドバタイズを受信します。

VTP 機能を持つ既存のネットワークに新しいスイッチを追加した場合、その新しいスイッチに適切なパスワードを設定して初めて、そのコントローラはドメイン名を学習します。

注意 VTP ドメイン パスワードを設定したにもかかわらず、ドメイン内の各スイッチに管理ドメイン パスワードを割り当てなかった場合には、管理ドメインが正常に動作しません。

関連トピック

VTP バージョン 3 のパスワードの設定（CLI），（2385 ページ）

例：スイッチをプライマリ サーバとして設定する，（2397 ページ）

VTP Version

実装する VTP バージョンを決定する場合は、次の注意事項に従ってください。

- VTP ドメイン内のすべてのスイッチは同じドメイン名を使用する必要がありますが、すべてが同じ VTP バージョンを実行する必要はありません。
- VTP バージョン 2 対応のスイッチ上で VTP バージョン 2 がディセーブルに設定されている場合、VTP バージョン 2 対応スイッチは、VTP バージョン 1 を実行しているスイッチと同じ VTP ドメインで動作できます（デフォルトでは VTP バージョン 2 はディセーブルになっています）。
- VTP バージョン 1 を実行しているものの、VTP バージョン 2 に対応可能なスイッチが VTP バージョン 3 アドバタイズを受信すると、このコントローラは VTP バージョン 2 に自動的に移行します。
- VTP バージョン 3 を実行しているスイッチが VTP バージョン 1 を実行しているスイッチに接続すると、VTP バージョン 1 のスイッチは VTP バージョン 2 に移行し、VTP バージョン 3 のスイッチは、スケールダウンしたバージョンの VTP パケットを送信するため、VTP バージョン 2 スイッチは自身のデータベースをアップデートできます。
- VTP バージョン 3 を実行するスイッチは、拡張 VLAN を持つ場合はバージョン 1 または 2 に移行できません。
- 同一 VTP ドメイン内のすべてのスイッチがバージョン 2 に対応可能な場合を除いて、スイッチ上で VTP バージョン 2 をイネーブルにしないでください。1 つのスイッチでバージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応スイッチでバージョン 2 がイネーブルになります。バージョン 1 専用のスイッチがドメインに含まれている場合、そのコントローラはバージョン 2 対応スイッチとの間で VTP 情報を交換できません。
- VTP バージョン 1 および 2 スイッチは、VTP バージョン 3 アドバタイズメントを転送できないため、ネットワークのエッジに配置することをお勧めします。
- 使用環境に TrBRF および TrCRF トークンリング ネットワークが含まれている場合に、トークンリング VLAN スイッチング機能を正しく動作させるには、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net を実行する場合は、VTP バージョン 2 をディセーブルにします。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN（VLAN 1006 ～ 4094）の設定情報を伝播しません。これらの VLAN は各装置で手動によって設定する必要があります。VTP バージョン 3 は拡張範囲 VLAN と、拡張範囲 VLAN データベースの伝播をサポートします。
- VTP バージョン 3 装置のトランク ポートが VTP バージョン 2 装置からのメッセージを受信した場合、この装置は、VLAN データベースをスケールダウンし、その特定のトランク上で VTP バージョン 2 フォーマットを使用して送信します。VTP バージョン 3 装置は、最初にそのトランク ポートで VTP バージョン 2 パケットを受信しない限り、VTP バージョン 2 フォーマットのパケットを送信しません。
- VTP バージョン 3 装置が、あるトランク ポートで VTP バージョン 2 装置を検出した場合、両方のネイバーが同一トランク上で共存できるように、VTP バージョン 2 パケットだけでなく VTP バージョン 3 パケットの送信も継続します。
- VTP バージョン 3 装置は、VTP バージョン 2 またはバージョン 1 の装置からの設定情報は受け入れません。

- 2 つの VTP バージョン 3 リージョンは、VTP バージョン 1 リージョンまたはバージョン 2 リージョンでは、トランスペアレント モードでだけ通信できます。
- VTP バージョン 1 にだけ対応する装置は、VTP バージョン 3 装置との相互運用はできません。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN（VLAN 1006 ～ 4094）の設定情報を伝播しません。これらの VLAN を各装置上に手動で設定する必要があります。

関連トピック

VTP バージョンのイネーブル化（CLI），（2388 ページ）

VTP の設定方法

VTP モードの設定（CLI）

次のいずれかに VTP モードを設定できます。

- VTP サーバ モード：VTP サーバ モードでは、VLAN の設定を変更し、ネットワーク全体に伝播させることができます。
- VTP クライアント モード：VTP クライアント モードでは、VLAN の設定を変更できません。クライアント スイッチは、VTP ドメイン内の VTP サーバから VTP アップデート情報を受信し、それに基づいて設定を変更します。
- VTP トランスペアレント モード：VTP トランスペアレント モードでは、スイッチで VTP がディセーブルになります。スイッチは VTP アップデートを送信せず、他のスイッチから受信した VTP アップデートにも反応しません。ただし、VTP バージョン 2 を実行する VTP トランスペアレント モードのスイッチは、対応するトランク リンクで、受信した VTP アドバタイズを転送します。
- VTP オフ モード：VTP オフ モードは、VTP アドバタイズが転送されない以外は、VTP トランスペアレント モードと同じです。

設定したドメイン名は、削除できません。別のドメインにスイッチを再び割り当てるしかありません。

手順の概要

1. **enable**
2. **configureterminal**
3. **vtp domain***domain-name*
4. **vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}
5. **vtp password***password*
6. **end**
7. **show vtp status**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp domain***domain-name* 例： スイッチ(config)# **vtp domain eng_group**	VTP 管理ドメイン名を設定します。1 ～ 32 文字の名前を使用できます。同一管理下にある VTP サーバ モードまたはクライアント モードのスイッチは、すべて同じドメイン名に設定する必要があります。 サーバ モード以外にはこのコマンドは任意です。VTP サーバ モードではドメイン名が必要です。スイッチが VTP ドメインにトランク接続されている場合、スイッチはドメイン内の VTP サーバからドメイン名を取得します。 他の VTP パラメータを設定する前に、VTP ドメインを設定する必要があります。 （注）
ステップ 4	**vtp mode** {**client**	**server**	**transparent**	**off**} {**vlan**	**mst**	**unknown**}	VTP モード（クライアント、サーバ、トランスペアレント、またはオフ）のスイッチの設定。 • **vlan**：何も設定されていない場合は VLAN データベースがデフォルトです。

	コマンドまたはアクション	目的
	例： スイッチ(config)# **vtp mode server**	• **mst**：マルチ スパニング ツリー（MST）データベース。 • **unknown**：データベース タイプは不明。
ステップ 5	**vtp password***password* 例： スイッチ(config)# **vtp password mypassword**	（任意）VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ～ 64 文字です。VTP パスワードを設定したにもかかわらず、ドメイン内の各スイッチに同じパスワードを割り当てなかった場合には、VTP ドメインが正常に動作しません。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show vtp status** 例： スイッチ# **show vtp status**	表示された *[VTP Operating Mode]* および *[VTP Domain Name]* フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）スタートアップ コンフィギュレーション ファイルに設定を保存します。 スイッチの実行コンフィギュレーションに保存され、スタートアップ コンフィギュレーション ファイルにコピーできるのは、VTP モードおよびドメイン名だけです。

関連トピック

VTP モード, （2374 ページ）

VTP バージョン 3 のパスワードの設定（CLI）

スイッチで VTP バージョン 3 のパスワードを設定できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vtp password***password* [**hidden** | **secret**]
4. **end**
5. **show vtp password**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp password***password* [**hidden**	**secret**] 例： スイッチ(config)# **vtp password mypassword hidden**	（任意）VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ～ 64 文字です。 • （任意）**hidden**：パスワード文字列から生成される秘密キーが、nvram:vlan.dat ファイルに保存されます。VTP プライマリ サーバを設定してテイクオーバーを設定しようとすると、パスワードの再入力を要求されます。 • （任意）**secret**：パスワードを直接設定します。シークレット パスワードには 16 進数文字を 32 個含める必要があります。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show vtp password** 例： スイッチ# **show vtp password**	入力を確認します。次のような出力が表示されます。 VTP password: 89914640C8D90868B6A0D8103847A733
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VTP ドメインのパスワード，（2381 ページ）
例：スイッチをプライマリ サーバとして設定する，（2397 ページ）

VTP バージョン 3 のプライマリ サーバの設定（CLI）

VTP サーバを VTP プライマリ サーバとして設定すると、テイクオーバー操作が開始されます。

手順の概要

1. **vtp primary** [**vlan** | **mst**] [**force**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vtp primary** [**vlan**	**mst**] [**force**] 例： スイッチ# **vtp primary vlan force**	スイッチの動作ステートをセカンダリ サーバ（デフォルト）からプライマリ サーバに変更し、その設定をドメインにアドバタイズします。スイッチのパスワードが **hidden** に設定されている場合は、パスワードの再入力を要求されます。 • （任意）**vlan**：テイクオーバー機能として VLAN データベースを選択します。これはデフォルトです。 • （任意）**mst**：テイクオーバー機能としてマルチ スパニング ツリー（MST）データベースを選択します。 • （任意）**force**：競合するサーバの設定が上書きされます。**force** を入力しない場合、テイクオーバーの実行前に確認を求められます。

	コマンドまたはアクション	目的

関連トピック

VTP の設定, （2380 ページ）

VTP バージョンのイネーブル化（CLI）

デフォルトで VTP バージョン 2 およびバージョン 3 はディセーブルになっています。

- 1 つのスイッチ上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内の VTP バージョン 2 に対応可能なすべてのスイッチでバージョン 2 がイネーブルになります。VTP バージョン 3 をイネーブルにするには、各スイッチ上で手動によって設定する必要があります。
- VTP バージョン 1 および 2 では、このバージョンを設定できるのは、VTP サーバ モードまたはトランスペアレント モードのスイッチだけです。スイッチが VTP バージョン 3 を実行し、かつスイッチがクライアント モードの場合、既存の拡張 VLAN がなく、パスワードが非表示に設定されていないときであれば、バージョン 2 に変更できます。

  注意 同一 VTP ドメイン内のスイッチ上で、VTP バージョン 1 と VTP バージョン 2 は相互運用できません。VTP ドメイン内のすべてのスイッチが VTP バージョン 2 をサポートしている場合を除き、VTP バージョン 2 をイネーブルにはしないでください。

- TrCRF および TrBRF トークンリング環境では、トークンリング VLAN スイッチング機能を正しく動作させるために、VTP バージョン 2 または VTP バージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net メディアの場合は、VTP バージョン 2 をディセーブルにします。
- **注意** VTP バージョン 3 では、プライマリ サーバとセカンダリ サーバの両方がドメイン内の 1 つのインスタンスに存在できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **VTP バージョン {1 | 2 | 3}**
4. **end**
5. **show vtp status**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**VTP バージョン {1	2	3}** 例： `スイッチ(config)# vtp version 2`	スイッチで VTP バージョンをイネーブルにします。デフォルトは VTP バージョン 1 です。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例： `スイッチ# show vtp status`	設定された VTP バージョンがイネーブルであることを確認します。
ステップ 6	**copy running-config startup-config** 例： `スイッチ# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

関連トピック

VTP Version, （2381 ページ）
VTP バージョン 2, （2376 ページ）
VTP バージョン 3, （2377 ページ）

VTP プルーニングのイネーブル化（CLI）

はじめる前に

VTP プルーニングは VTP トランスペアレント モードでは機能しないように設計されています。ネットワーク内に VTP トランスペアレント モードのスイッチが 1 台または複数存在する場合は、次のいずれかの操作を実行する必要があります。

- ネットワーク全体の VTP プルーニングをオフにします。
- VTP トランスペアレント スイッチのアップストリーム側にあるスイッチのトランク上で、すべての VLAN をプルーニング不適格にすることによって、VTP プルーニングをオフにします。

インターフェイスに VTP プルーニングを設定するには、**switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します。VTPプルーニングは、インターフェイスがトランキングを実行している場合に作用します。VLAN プルーニングの適格性は、VTP ドメインでVTPプルーニングがイネーブルであるかどうか、特定のVLANが存在するかどうか、およびインターフェイスが現在トランキングを実行しているかどうかにかかわらず、設定できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vtp pruning**
4. **end**
5. **show vtp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp pruning** 例： `スイッチ(config)# vtp pruning`	VTP 管理ドメインでプルーニングをイネーブルにします。 プルーニングは、デフォルトではディセーブルに設定されています。VTP サーバ モードの 1 台のスイッチ上に限ってプルーニングをイネーブルにする必要があります。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例： `スイッチ# show vtp status`	表示された [VTP Pruning Mode] フィールドの設定を確認します。

関連トピック

VTP プルーニング，（2378 ページ）

ポート単位の VTP の設定（CLI）

VTP バージョン 3 では、ポート単位で VTP をイネーブルまたはディセーブルにできます。VTP は、トランク モードのポート上でだけイネーブルにできます。VTP トラフィックの着信または発信はブロックされ、転送されません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **vtp**
5. **end**
6. **show running-config interface***interface-id*
7. **show vtp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**vtp** 例： スイッチ(config)# **vtp**	指定したポートの VTP をイネーブルにします。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config interface***interface-id* 例： スイッチ# **show running-config interface gigabitethernet1/0/1**	ポートの変更を確認します。
ステップ 7	**show vtp status** 例： スイッチ# **show vtp status**	設定を確認します。

関連トピック

VTP の設定, （2380 ページ）

VTP ドメインへの VTP クライアント スイッチの追加（CLI）

VTP ドメインに追加する前にスイッチ上で VTP コンフィギュレーション リビジョン番号を確認およびリセットするには、次の手順に従います。

はじめる前に

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。VTP バージョン 1 および 2 では、VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP バージョン 3 では、VLAN 情報が消去されることはありません。

スイッチ上で VTP をディセーブルにし、VTP ドメイン内の他のスイッチに影響を与えることなく VLAN 情報を変更するには、**vtp mode transparent** グローバル コンフィギュレーション コマンドを使用します。

手順の概要

1. **enable**
2. **show vtp status**
3. **configureterminal**
4. **vtp domain***domain-name*
5. **end**
6. **show vtp status**
7. **configure terminal**
8. **vtp domain***domain-name*
9. **end**
10. **show vtp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**show vtp status** 例： スイッチ# **show vtp status**	VTP コンフィギュレーション リビジョン番号をチェックします。 番号が 0 の場合は、スイッチを VTP ドメインに追加します。 番号が 0 より大きい場合は、次の手順に従います。 • ドメイン名を書き留めます。 • コンフィギュレーション リビジョン番号を書き留めます。 • 次のステップに進んで、スイッチのコンフィギュレーション リビジョン番号をリセットします。
ステップ 3	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**vtp domain***domain-name* 例： スイッチ(config)# **vtp domain domain123**	ドメイン名を、ステップ 1 で表示された元の名前から新しい名前に変更します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。スイッチの VLAN 情報が更新され、コンフィギュレーション リビジョン番号が 0 にリセットされます。
ステップ 6	**show vtp status** 例： スイッチ# **show vtp status**	コンフィギュレーション リビジョン番号が 0 にリセットされていることを確認します。
ステップ 7	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 8	**vtp domain***domain-name* 例： スイッチ(config)# **vtp domain domain012**	スイッチの元のドメイン名を開始します。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。スイッチの VLAN 情報が更新されます。
ステップ 10	**show vtp status** 例： スイッチ# **show vtp status**	（任意）ドメイン名がステップ 1 のものと同じであり、コンフィギュレーション リビジョン番号が 0 であることを確認します。

関連トピック

VTP Domain, （2373 ページ）

VTP の前提条件, （2372 ページ）

VTP 設定のためのドメイン名, （2381 ページ）

VTP のモニタ

ここでは、VTP の設定を表示およびモニタリングするために使用するコマンドについて説明します。

VTP の設定情報（ドメイン名、現在の VTP バージョン、VLAN 数）を表示することによって、VTP をモニタします。スイッチで送受信されたアドバタイズに関する統計情報を表示することもできます。

表 *176* : *VTP* モニタ コマンド

コマンド	目的
show vtp counters	送受信された VTP メッセージに関するカウンタを表示します。
show vtp devices [**conflict**]	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。プライマリ サーバと競合する VTP バージョン 3 の装置が表示されます。**show vtp devices** コマンドは、スイッチがトランスペアレント モードまたはオフ モードのときは情報を表示しません。
show vtp interface [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。
show vtp password	VTP パスワードを表示します。表示されるパスワードの形式は、**hidden** キーワードが入力されているか、または、暗号化がスイッチでイネーブル化されているかどうかによって異なります。
show vtp status	VTP スイッチ設定情報を表示します。

VTP の設定例

例：スイッチをプライマリ サーバとして設定する

次に、パスワードが非表示またはシークレットに設定されている場合に、VLAN データベースのプライマリ サーバ（デフォルト）としてスイッチを設定する方法の例を示します。

```
スイッチ# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- --------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

関連トピック

VTP バージョン 3 のパスワードの設定（CLI），（2385 ページ）

VTP ドメインのパスワード，（2381 ページ）

次の作業

VTP を設定したら、次の項目を設定できます。

- VLANs
- VLAN グループ
- VLAN トランキング
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN Command Reference (Catalyst 3650 Switches)* *Layer 2/3 Command Reference (Catalyst 3650 Switches)*

関連項目	マニュアル タイトル
追加の設定コマンドおよび手順。	*LAN Switching Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)* *Layer 2/3 Configuration Guide (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

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

シスコのテクニカル サポート

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

VTP の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 105 章

VLAN の設定

- 機能情報の確認，2401 ページ
- VLAN の前提条件，2401 ページ
- VLAN の制約事項，2402 ページ
- VLAN について，2402 ページ
- VLAN の設定方法，2409 ページ
- VLAN のモニタリング，2419 ページ
- 次の作業，2422 ページ
- その他の参考資料，2422 ページ
- VLAN の機能履歴と情報，2424 ページ

機能情報の確認

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

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

VLAN の前提条件

VLAN 設定時の前提条件と考慮事項を次に示します。

- VLAN を作成する前に、VLAN トランキング プロトコル（VTP）を使用してネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。
- スイッチで多数の VLAN を設定し、ルーティングをイネーブルにしない予定の場合は、Switch Database Management（SDM）機能を VLAN テンプレートに設定します。これにより、最大数のユニキャスト MAC アドレスをサポートするようにシステム リソースが設定されます。
- LAN ベース フィーチャ セットが稼働しているスイッチでは、SVI のスタティック ルーティングだけがサポートされます。
- VLAN グループに VLAN を追加できるようにするため、VLAN がスイッチに存在している必要があります。

VLAN の制約事項

次に、VLAN の制約事項を示します。

- スイッチは、最大 128 のスパニングツリー インスタンスを持つ Per-VLAN Spanning-Tree Plus（PVST+）または Rapid PVST+ をサポートします。VLAN ごとに 1 つずつスパニングツリー インスタンスを使用できます。
- スイッチは、イーサネット ポート経由の VLAN トラフィックの送信方式として、IEEE 802.1Q トランキングをサポートします。
- インターフェイス VLAN ルータの MAC アドレスの設定はサポートされていません。インターフェイス VLAN にはデフォルトですでに MAC アドレスが割り当てられています。
- プライベート VLAN はスイッチではサポートされません。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

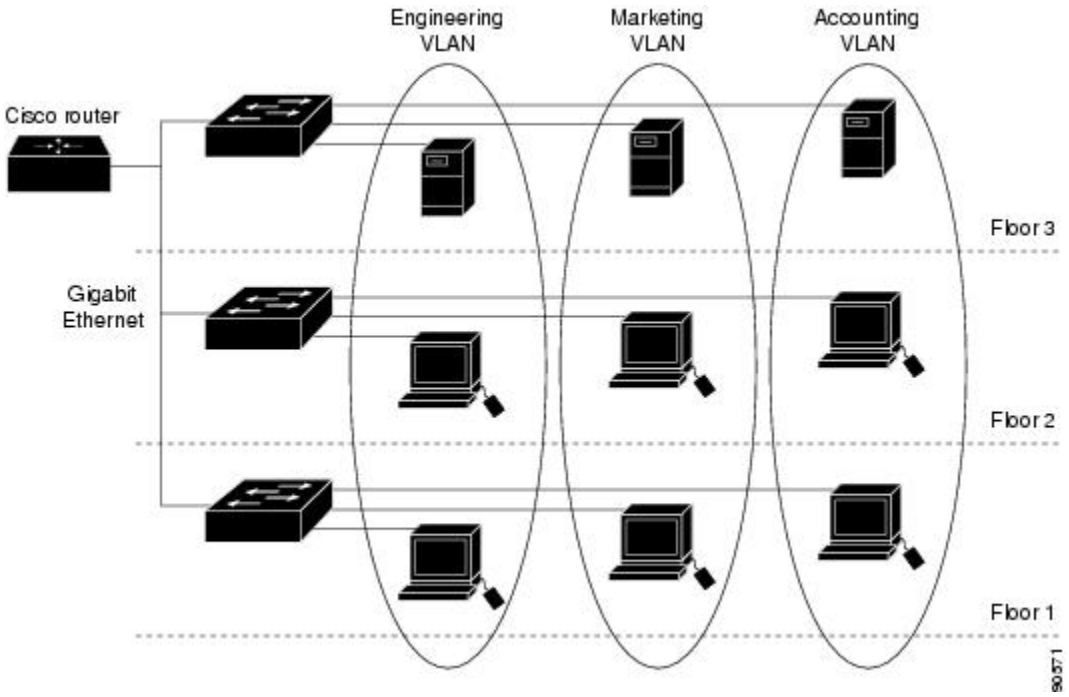
VLAN について

論理ネットワーク

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。どのようなスイッチ ポートでも VLAN に属することができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN 内のエンド ステーションだけに転送またはフラッディングされます。各 VLAN は 1 つの論理ネットワークと見なされ、VLAN に属さないステーション宛のパケットは、ルータまたはフォールバック ブリッジングをサポートするスイッチを経由して伝送しなければなりません。スイッチ スタックでは、ポートを使用して VLAN をスタック全体に形成できます。VLAN はそれぞれが独立した論理ネットワークと見なさ

れるので、VLAN ごとに独自のブリッジ管理情報ベース（MIB）情報があり、スパニングツリーの独自の実装をサポートできます。

図 *98*：論理的に定義されたネットワークとしての *VLAN*



VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットに含まれるエンドステーションはすべて同じVLANに属します。スイッチ上のインターフェイスのVLANメンバーシップは、インターフェイスごとに手動で割り当てます。この方法でスイッチ インターフェイスを VLAN に割り当てた場合、これをインターフェイス ベース（またはスタティック）VLAN メンバーシップと呼びます。

VLAN 間のトラフィックは、ルーティングする必要があります。

スイッチは、スイッチ仮想インターフェイス（SVI）を使用して、VLAN間でトラフィックをルーティングできます。VLAN 間でトラフィックをルーティングするには、SVI を明示的に設定して IP アドレスを割り当てる必要があります。

サポートされる VLAN

スイッチは、VTP クライアント、サーバ、およびトランスペアレントの各モードで VLAN をサポートしています。VLAN は、1 ～ 4094 の番号で識別します。VLAN 1 はデフォルト VLAN で、システム初期化中に作成されます。VLAN ID 1002 ～ 1005 は、トークンリングおよびファイバ分散データ インターフェイス（FDDI）VLAN 専用です。1002 ～ 1005 を除くすべての VLAN がユーザ設定のために使用できます。

VTP バージョン 1、バージョン 2、およびバージョン 3 の 3 つの VTP バージョンがあります。すべての VTP バージョンが標準および拡張範囲 VLAN の両方をサポートしますが、VTP バージョ

ン 3 のみが スイッチ 伝播拡張範囲 VLAN 設定情報を実行します。拡張範囲 VLAN が VTP バージョン 1 および 2 で作成された場合、設定情報は伝播されません。スイッチ上のローカル VTP データベース エントリも更新されませんが、拡張範囲 VLAN 設定情報が作成され、実行設定ファイルに保存されます。

最大 4094 の VLAN をスイッチに設定できます。

関連トピック

イーサネット VLAN の作成または変更（CLI），（2410 ページ）

VLAN の削除（CLI），（2412 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI），（2414 ページ）
VLAN のモニタリング，（2419 ページ）

拡張範囲 VLAN の作成（CLI），（2417 ページ）

内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN のモニタリング，（2419 ページ）

イーサネット VLAN の作成または変更（CLI），（2410 ページ）

VLAN の削除（CLI），（2412 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI），（2414 ページ）
VLAN のモニタリング，（2419 ページ）

拡張範囲 VLAN の作成（CLI），（2417 ページ）

内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN のモニタリング，（2419 ページ）

イーサネット VLAN の作成または変更（CLI），（2410 ページ）

VLAN の削除（CLI），（2412 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI），（2414 ページ）
VLAN のモニタリング，（2419 ページ）

拡張範囲 VLAN の作成（CLI），（2417 ページ）

内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN のモニタリング，（2419 ページ）

イーサネット VLAN の作成または変更（CLI），（2410 ページ）

VLAN の削除（CLI），（2412 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI），（2414 ページ）
VLAN のモニタリング，（2419 ページ）

拡張範囲 VLAN の作成（CLI），（2417 ページ）

内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN のモニタリング，（2419 ページ）

VLAN ポート メンバーシップ モード

VLAN に所属するポートは、メンバーシップ モードを割り当てることで設定します。メンバーシップ モードは、各ポートが伝送できるトラフィックの種類、および所属できる VLAN の数を指定します。

ポートが VLAN に所属すると、スイッチは VLAN 単位で、ポートに対応するアドレスを学習して管理します。

表 *177*：ポートのメンバーシップ モードとその特性

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1 つの VLAN だけに所属します。	VTP は必須ではありません。VTP にグローバルに情報を伝播させないようにする場合は、VTP モードをトランスペアレント モードに設定します。VTP に加入するには、別のスイッチまたはスイッチ スタックのトランク ポートに接続されているスイッチまたはスイッチ スタック上に少なくとも 1 つのトランク ポートが必要です。
トランク（IEEE 802.1Q） • IEEE 802.1Q：業界標準のトランキング カプセル化方式です。	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべての VLAN のメンバです。ただし、メンバーシップは許可 VLAN リストを設定して制限できます。また、プルーニング適格リストを変更して、リストに指定したトランク ポート上の VLAN へのフラッディング トラフィックを阻止することもできます。	VTP を推奨しますが、必須ではありません。VTP は、ネットワーク全体にわたって VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。VTP はトランク リンクを通じて他のスイッチと VLAN コンフィギュレーション メッセージを交換します。
音声 VLAN	音声 VLAN ポートは、Cisco IP Phone に接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データ トラフィックに別の VLAN を使用するように設定されたアクセス ポートです。	VTP は不要です。VTP は音声 VLAN に対して無効です。

関連トピック

VLAN へのスタティック アクセス ポートの割り当て（CLI），（2414 ページ）
VLAN のモニタリング，（2419 ページ）
VLAN へのスタティック アクセス ポートの割り当て（CLI），（2414 ページ）

VLAN コンフィギュレーション ファイル

VLAN ID 1 ～ 1005 の設定は vlan.dat（VLAN データベース）ファイルに書き込まれます。この設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。vlan.dat ファイルはフラッシュ メモリに格納されます。VTP モードがトランスペアレント モードの場合、それらの設定もスイッチの実行コンフィギュレーション ファイルに保存されます。

スイッチ スタックでは、スタック全体が同一の vlan.dat ファイルと実行コンフィギュレーションを使用します。一部のスイッチでは、vlan.dat ファイルがアクティブ スイッチのフラッシュ メモリに保存されます。

さらに、インターフェイス コンフィギュレーション モードを使用して、ポートのメンバーシップ モードの定義、VLAN に対するポートの追加および削除を行います。これらのコマンドの実行結果は、実行コンフィギュレーション ファイルに書き込まれます。このファイルを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

VLAN および VTP 情報（拡張範囲 VLAN 設定情報を含む）をスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントで、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。
- VTP バージョン 1 および 2 では、VTP モードがサーバである場合、VLAN ID 1 ～ 1005 のドメイン名と VLAN 設定で VLAN データベース情報が使用されます。VTP バージョン 3 は、VLAN 1006 ～ 4094 もサポートします。

標準範囲 VLAN 設定時の注意事項

標準範囲 VLAN は、ID が 1 ～ 1005 の VLAN です。

ネットワーク内で標準範囲 VLAN を作成または変更する場合には、次の注意事項に従ってください。

- 標準範囲 VLAN は、1 ～ 1001 の番号で識別します。VLAN 番号 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 専用です。
- VLAN 1 ～ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードがトランスペアレントモードの場合、VTP と VLAN の設定もスイッチの実行コンフィギュレーション ファイルに保存されます。
- スイッチが VTP サーバ モードまたは VTP トランスペアレント モードにある場合は、VLAN データベース内の VLAN 2 ～ 1001 について設定を追加、変更、または削除できます（VLAN ID 1 および 1002 ～ 1005 は自動作成され、削除できません）。
- VTP トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースに保存されず、伝播されません。VTP バージョン 3 では、VTP サーバ モードでの拡張範囲 VLAN（VLAN 1006～4094）データベース伝播をサポートします。
- VLAN を作成する前に、スイッチを VTP サーバ モードまたは VTP トランスペアレント モードにする必要があります。スイッチが VTP サーバである場合には、VTP ドメインを定義する必要があります。VTP ドメインを定義しないと、VTP は機能しません。
- スイッチは、トークンリングまたは FDDI メディアをサポートしません。スイッチは FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを転送するのではなく、VTP を介して VLAN 設定を伝播します。
- スイッチは 128 のスパニングツリー インスタンスをサポートします。スイッチのアクティブな VLAN 数が、サポートされているスパニングツリー インスタンス数よりも多い場合、スパニングツリーは 128 の VLAN でイネーブルにできます。残りの VLAN で、スパニングツリーはディセーブルになります。スイッチ上の使用可能なスパニングツリー インスタンスをすべて使い切ってしまった後に、VTP ドメインの中にさらに別の VLAN を追加すると、そのスイッチ上にスパニングツリーが稼働しない VLAN が生成されます。そのスイッチのトランク ポート上でデフォルトの許可リスト（すべての VLAN を許可するリスト）が設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチでスパニングツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパニングツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。

  スイッチ上の VLAN の数がサポートされているスパニングツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s Multiple STP（MSTP）を設定して、複数の VLAN を単一のスパニングツリー インスタンスにマッピングすることを推奨します。
- スタック内のスイッチが新しい VLAN を学習するか、または既存の VLA を削除または変更すると（ネットワーク ポートを介した VTP を通じてか、または CLI を通じて）、その VLAN 情報はすべてのスタック メンバに伝達されます。
- スイッチがスタックに参加した場合またはスタックの結合が発生した場合は、新しいスイッチ上の VTP 情報（vlan.dat ファイル）とアクティブなスイッチの一貫性が維持されます。

関連トピック

イーサネット VLAN の作成または変更（CLI），（2410 ページ）

VLAN の削除（CLI），（2412 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI），（2414 ページ）
VLAN のモニタリング，（2419 ページ）

イーサネット VLAN の作成または変更（CLI），（2410 ページ）

VLAN の削除（CLI），（2412 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI），（2414 ページ）
VLAN のモニタリング，（2419 ページ）

イーサネット VLAN の作成または変更（CLI），（2410 ページ）

VLAN の削除（CLI），（2412 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI），（2414 ページ）
VLAN のモニタリング，（2419 ページ）

イーサネット VLAN の作成または変更（CLI），（2410 ページ）

VLAN の削除（CLI），（2412 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI），（2414 ページ）
VLAN のモニタリング，（2419 ページ）

イーサネット VLAN の作成または変更（CLI），（2410 ページ）

VLAN のモニタリング，（2419 ページ）

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN は、ID が 1006 ～ 4094 の VLAN です。

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- 拡張範囲の VLAN ID は、スイッチが VTP バージョン 3 を実行していない場合は VLAN データベースに保存されず、VTP で認識されません。
- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。
- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで、VTP モードをトランスペアレントに設定できます。VTP トランスペアレント モードでスイッチが始動するように、この設定をスタートアップ コンフィギュレーションに保存する必要があります。このようにしないと、スイッチをリセットした場合に、拡張範囲VLAN設定が失われます。VTP バージョン 3 で拡張範囲 VLAN を作成する場合は、VTP バージョン 1 または 2 に変更できません。
- スイッチスタックでは、スタック全体が同一の実行コンフィギュレーションと保存されているコンフィギュレーションを使用しており、拡張範囲VLAN情報はスタック全体で共有されます。

関連トピック

拡張範囲 VLAN の作成（CLI），（2417 ページ）

内部 VLAN ID を指定した拡張範囲 VLAN の作成

VLAN のモニタリング，（2419 ページ）

拡張範囲 VLAN の作成（CLI），（2417 ページ）

内部 VLAN ID を指定した拡張範囲 VLAN の作成

VLAN のモニタリング，（2419 ページ）

拡張範囲 VLAN の作成（CLI），（2417 ページ）

内部 VLAN ID を指定した拡張範囲 VLAN の作成

VLAN のモニタリング，（2419 ページ）

拡張範囲 VLAN の作成（CLI），（2417 ページ）

内部 VLAN ID を指定した拡張範囲 VLAN の作成

VLAN のモニタリング，（2419 ページ）

拡張範囲 VLAN の作成（CLI），（2417 ページ）

VLAN のモニタリング，（2419 ページ）

VLAN の設定方法

標準範囲 VLAN の設定方法

VLANデータベースに新しい標準範囲VLANを作成したり、VLANデータベース内の既存のVLANを変更したりする場合、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ
  - イーサネット
  - Fiber Distributed Data Interface [FDDI]
  - FDDI ネットワーク エンティティ タイトル [NET]
  - TrBRF または TrCRF
  - Token Ring
  - トークンリング Net
- VLAN ステート（アクティブまたは中断）
- VLAN の最大伝送単位（MTU）

- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN のスパニングツリー プロトコル（STP）タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号

vlan.datファイルを手動で削除しようとすると、VLANデータベースに不整合が生じる可能性があります。VLAN 設定を変更する場合は、この項の手順に従ってください。

イーサネット VLAN の作成または変更（CLI）

はじめる前に

VTP バージョン 1 および 2 でスイッチが VTP トランスペアレント モードの場合は、1006 を超える VLAN ID を割り当てることができますが、それらを VLAN データベースに追加できません。

スイッチは、イーサネット インターフェイスだけをサポートしています。FDDI およびトークンリング VLAN は、ローカルではサポートされないので、FDDI およびトークンリング メディア固有の特性は、他のスイッチに対する VTP グローバル アドバタイズにのみ設定します。

このスイッチはトークンリング接続をサポートしていませんが、トークンリング接続を行っているリモート デバイスを、サポート対象スイッチのうちの 1 台から管理できます。VTP バージョン 2 が稼働しているスイッチは、次のトークンリング VLAN に関する情報をアドバタイズします。

- トークンリング TrBRF VLAN
- トークンリング TrCRF VLAN

手順の概要

1. **configureterminal**
2. **vlan***vlan-id*
3. **name***vlan-name*
4. **media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** }
5. **remote-span**
6. **end**
7. **show vlan** {**name***vlan-name* | **id***vlan-id*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan***vlan-id* 例： スイッチ(config)# **vlan 20**	VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。 （注） このコマンドで指定できる VLAN ID 範囲は 1 ～ 4094 です。
ステップ 3	**name***vlan-name* 例： スイッチ(config-vlan)# **name test20**	（任意）VLAN の名前を入力します。VLAN 名を指定しなかった場合には、デフォルトとして、VLAN という語の後ろに先行ゼロを含めた *vlan-id* 値が付加されます。たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。
ステップ 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } 例： スイッチ(config-vlan)# **media ethernet**	VLAN のメディア タイプを設定します。コマンド オプションは次のとおりです。 • **ethernet**：VLAN のメディア タイプをイーサネットに設定します。 • **fd-net**：VLAN のメディア タイプを FDDI-net に設定します。 • **fddi**：VLAN のメディア タイプを FDDI に設定します。 • **tokenring**：VLAN メディア タイプをトークン リングに設定します。 • **trn-net**：VLAN メディア タイプをトークン リング ネットに設定します。
ステップ 5	**remote-span** 例： スイッチ(config-vlan)# **remote-span**	（任意）リモート スイッチド ポート アナライザ（SPAN）セッションに対する RSPAN VLAN として、VLAN を設定します。リモート SPAN の詳細については、『*Catalyst 3650 Network Management Configuration Guide*』を参照してください。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show vlan** {**name***vlan-name* | **id***vlan-id*} 例： スイッチ# **show vlan name test20** **id 20**	入力を確認します。

関連トピック

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

VLAN の削除（CLI）

VTP サーバ モードのスイッチから VLAN を削除すると、VTP ドメイン内のすべてのスイッチの VLAN データベースから、その VLAN が削除されます。VTP トランスペアレント モードのスイッチから VLAN を削除した場合、その特定のスイッチスイッチまたはスイッチスタック上に限り VLAN が削除されます。

イーサネット VLAN 1 および FDDI、またはトークンリング VLAN 1002 ～ 1005 の、メディア タイプ別のデフォルト VLAN は削除できません。

注意 VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。これらのポートは、新しいVLANに割り当てられるまで、元のVLANに（非アクティブで）対応付けられたままです。

手順の概要

1. **enable**
2. **configureterminal**
3. **no vlan***vlan-id*
4. **end**
5. **show vlan brief**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no vlan***vlan-id* 例： スイッチ(config)# **no vlan 4**	VLAN ID を入力して、VLAN を削除します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show vlan brief** 例： スイッチ# **show vlan brief**	VLAN が削除されたことを確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

VLAN のモニタリング, （2419 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI）

VTP をディセーブルにすることによって（VTP トランスペアレント モード）、VTP に VLAN 設定情報をグローバルに伝播させずに、スタティック アクセス ポートを VLAN に割り当てることができます。

クラスタ メンバ スイッチ上のポートを VLAN に割り当てる場合、最初に **rcommand** 特権 EXEC コマンドを使用して、クラスタ メンバ スイッチにログインします。

存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **switchport mode access**
5. **switchport access vlan***vlan-id*
6. **end**
7. **show running-config interface***interface-id*
8. **show interfaces***interface-id***switchport**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	VLANに追加するインターフェイスを入力します。
ステップ 4	**switchport mode access** 例： スイッチ(config-if)# **switchport mode access**	ポート（レイヤ 2 アクセス ポート）の VLAN メンバーシップ モードを定義します。
ステップ 5	**switchport access vlan***vlan-id* 例： スイッチ(config-if)# **switchport access vlan 2**	VLANにポートを割り当てます。指定できるVLAN ID の範囲は 1 ～ 4094 です。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config interface***interface-id* 例： スイッチ# **show running-config interface gigabitethernet2/0/1**	インターフェイスの VLAN メンバーシップ モードを確認します。
ステップ 8	**show interfaces***interface-id***switchport** 例： スイッチ# **show interfaces gigabitethernet2/0/1 switchport**	表示された *Administrative Mode* および *Access Mode VLAN* フィールドの設定を確認します。
ステップ 9	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング, （2419 ページ）

サポートされる VLAN, （2403 ページ）

標準範囲 VLAN 設定時の注意事項, （2406 ページ）

VLAN のモニタリング，（2419 ページ）
VLAN ポート メンバーシップ モード，（2405 ページ）
VLAN のモニタリング，（2419 ページ）
VLAN ポート メンバーシップ モード，（2405 ページ）

拡張範囲 VLAN の設定方法

サービス プロバイダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応できます。拡張範囲 VLAN ID は、VLAN ID を許可するどの **switchport** コマンドでも許可されます。

VTP バージョン 1 または 2 での拡張範囲 VLAN の設定は VLAN データベースに格納されません。ただし、VTP モードがトランスペアレントであるため、スイッチの実行コンフィギュレーション ファイルに格納されます。また、設定をスタートアップ コンフィギュレーション ファイルに保存できます。VTP バージョン 3 で作成された拡張範囲 VLAN は、VLAN データベースに保存されます。

拡張範囲 VLAN については MTU サイズおよびリモート SPAN 設定ステートしか変更できません。残りのすべての特性はデフォルト状態のままでなければなりません。

拡張範囲 VLAN の作成（CLI）

手順の概要

1. **enable**
2. **configureterminal**
3. **vlan***vlan-id*
4. **remote-span**
5. **exit**
6. **end**
7. **show vlan id***vlan-id*
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan***vlan-id* 例： スイッチ(config)# **vlan 2000** スイッチ(config-vlan)#	拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 1006 ～ 4094 です。
ステップ 4	**remote-span** 例： スイッチ(config-vlan)# **remote-span**	（任意）RSPAN VLAN として VLAN を設定します。
ステップ 5	**exit** 例： スイッチ(config-vlan)# **exit** スイッチ(config)#	コンフィギュレーション モードに戻ります。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show vlan id***vlan-id* 例： スイッチ# **show vlan id 2000**	VLAN が作成されたことを確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

サポートされる VLAN, （2403 ページ）
拡張範囲 VLAN 設定時の注意事項, （2408 ページ）
VLAN のモニタリング, （2419 ページ）
サポートされる VLAN, （2403 ページ）
拡張範囲 VLAN 設定時の注意事項, （2408 ページ）
VLAN のモニタリング, （2419 ページ）
サポートされる VLAN, （2403 ページ）
拡張範囲 VLAN 設定時の注意事項, （2408 ページ）
VLAN のモニタリング, （2419 ページ）
サポートされる VLAN, （2403 ページ）
拡張範囲 VLAN 設定時の注意事項, （2408 ページ）
VLAN のモニタリング, （2419 ページ）
拡張範囲 VLAN 設定時の注意事項, （2408 ページ）
VLAN のモニタリング, （2419 ページ）

VLAN の設定方法（GUI）

VLAN のモニタリング

表 *178*：特権 *EXEC* 表示コマンド

コマンド	目的
show interfaces [**vlan***vlan-id*]	スイッチ上に設定されたすべてのインターフェイスまたは特定の VLAN の特性を表示します。

コマンド	目的
show vlan [**access-map** *name* | **brief** | **dot1q** { **tag native** } | **filter** [**access-map** | **vlan**] | **group** [**group-name** *name*] | **id***vlan-id* | **ifindex** | **mtu** | **name** *name* | **remote-span** | **summary**]	スイッチ上のすべての VLAN または特定の VLAN のパラメータを表示します。次のコマンド オプションが使用可能です。 • **access-map**：VLAN アクセスマップを表示します。 • **brief**：VTP VLAN のステータス概要を表示します。 • **dot1q**：dot1q パラメータを表示します。 • **filter**：VLAN フィルタ情報を表示します。 • **group**：VLAN グループをグループ名と使用可能な接続済みの VLAN と一緒に表示します。 • **id**：識別番号別に VTP VLAN ステータスを表示します。 • **ifindex**：SNMP ifIndex を表示します。 • **mtu**：VLAN MTU 情報を表示します。 • **name**：指定された名前の VTP VLAN 情報を表示します。 • **remote-span**：リモート SPAN VLAN を表示します。 • **summary**：VLAN 情報の要約を表示します。

関連トピック

サポートされる VLAN, （2403 ページ）
標準範囲 VLAN 設定時の注意事項, （2406 ページ）
イーサネット VLAN の作成または変更（CLI）, （2410 ページ）
VLAN の削除（CLI）, （2412 ページ）
VLAN へのスタティック アクセス ポートの割り当て（CLI）, （2414 ページ）
サポートされる VLAN, （2403 ページ）
拡張範囲 VLAN 設定時の注意事項, （2408 ページ）
拡張範囲 VLAN の作成（CLI）, （2417 ページ）
内部 VLAN ID を指定した拡張範囲 VLAN の作成

サポートされる VLAN, （2403 ページ）
標準範囲 VLAN 設定時の注意事項, （2406 ページ）
イーサネット VLAN の作成または変更（CLI）, （2410 ページ）
VLAN の削除（CLI）, （2412 ページ）
VLAN へのスタティック アクセス ポートの割り当て（CLI）, （2414 ページ）
サポートされる VLAN, （2403 ページ）
拡張範囲 VLAN 設定時の注意事項, （2408 ページ）
拡張範囲 VLAN の作成（CLI）, （2417 ページ）
内部 VLAN ID を指定した拡張範囲 VLAN の作成
サポートされる VLAN, （2403 ページ）
標準範囲 VLAN 設定時の注意事項, （2406 ページ）
イーサネット VLAN の作成または変更（CLI）, （2410 ページ）
VLAN の削除（CLI）, （2412 ページ）
VLAN へのスタティック アクセス ポートの割り当て（CLI）, （2414 ページ）
サポートされる VLAN, （2403 ページ）
拡張範囲 VLAN 設定時の注意事項, （2408 ページ）
拡張範囲 VLAN の作成（CLI）, （2417 ページ）
内部 VLAN ID を指定した拡張範囲 VLAN の作成
サポートされる VLAN, （2403 ページ）
標準範囲 VLAN 設定時の注意事項, （2406 ページ）
イーサネット VLAN の作成または変更（CLI）, （2410 ページ）
VLAN の削除（CLI）, （2412 ページ）
VLAN へのスタティック アクセス ポートの割り当て（CLI）, （2414 ページ）
サポートされる VLAN, （2403 ページ）
拡張範囲 VLAN 設定時の注意事項, （2408 ページ）
拡張範囲 VLAN の作成（CLI）, （2417 ページ）
内部 VLAN ID を指定した拡張範囲 VLAN の作成
イーサネット VLAN の作成または変更（CLI）, （2410 ページ）
標準範囲 VLAN 設定時の注意事項, （2406 ページ）
VLAN の削除（CLI）, （2412 ページ）
VLAN へのスタティック アクセス ポートの割り当て（CLI）, （2414 ページ）
VLAN ポート メンバーシップ モード, （2405 ページ）
拡張範囲 VLAN の作成（CLI）, （2417 ページ）
拡張範囲 VLAN 設定時の注意事項, （2408 ページ）

次の作業

VLAN を設定したら、次の項目を設定できます。

- VLAN グループ
- VLAN トランキング プロトコル（VTP）
- VLAN トランク
- VLAN メンバーシップ ポリシー サーバ（VMPS）
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN Command Reference (Catalyst 3650 Switches)* *Layer 2/3 Command Reference (Catalyst 3650 Switches)*
VLAN アクセス マップ	*Security Configuration Guide (Catalyst 3650 Switches)* *Security Command Reference (Catalyst 3650 Switches)*
VLAN およびモビリティ エージェント	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
Cisco Flexible NetFlow	*Cisco Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)* *Flexible Netflow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
IGMP スヌーピング	*IP Multicast Routing Command Reference (Catalyst 3650 Switches)* *IP Multicast Routing Configuration Guide (Catalyst 3650 Switches)*
IPv6	*IPv6 Configuration Guide (Catalyst 3650 Switches)* *IPv6 Command Reference (Catalyst 3650 Switches)*

関連項目	マニュアル タイトル
SPAN	*Network Management Command Reference (Catalyst 3650 Switches)* *Network Management Configuration Guide (Catalyst 3650 Switches)*
プラットフォームに依存しない設定情報	*Identity Based Networking Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

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

シスコのテクニカル サポート

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

VLAN の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	VLAN（GUI）サポート。

第 106 章

VLAN グループの設定

- 機能情報の確認，2425 ページ
- VLAN グループの前提条件，2425 ページ
- VLAN グループの制約事項，2426 ページ
- VLAN グループについて，2426 ページ
- VLAN グループの設定方法，2427 ページ
- 次の作業，2430 ページ
- その他の参考資料，2430 ページ
- VLAN グループの機能履歴と情報，2432 ページ

機能情報の確認

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

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

VLAN グループの前提条件

- VLAN グループに VLAN を追加できるようにするため、VLAN がスイッチに存在している必要があります。

- VLAN グループが適切に機能するためには、DHCP スヌーピングを全体的にイネーブルにする他に、DHCP スヌーピングがすべての VLAN でイネーブルになっていることを確認する必要があります。

VLAN グループの制約事項

1 つの VLAN グループにマッピングされる VLAN の数は、Cisco IOS Software Release による制限を受けません。ただし、VLAN グループの VLAN の数が推奨値である 32 を超えた場合、予期されないモビリティの動作が発生し、VLAN グループ内の一部の VLAN で L2 マルチキャストが中断します。したがって、VLAN グループ内で適切な数の VLAN を設定する責任は管理者にあります。すでに 32 個の VLAN が含まれている WLAN にマップされている VLAN グループに VLAN を追加すると、警告が生成されます。ただし、32 を超える VLAN が含まれている WLAN に新しい VLAN グループがマッピングされると、エラーが生成されます。

VLAN グループが予期通り動作するためには、グループでマッピングされた VLAN がスイッチに存在している必要があります。スタティック IP クライアント動作はサポートされません。

VLAN グループについて

クライアントがワイヤレス ネットワーク（WLAN）に接続するたびに、WLANに関連付けられている VLANにクライアントが配置されます。講堂、競技場、会議場などといった大規模な会場では、大量のワイヤレス クラインアントが使用されており、単一の WLAN だけで多数のクライアントに対応することは困難な場合があります。

VLANグループ機能は、複数のVLANに対応可能な単一WLANを使用します。クライアントは、設定されている VLAN の 1 つに割り当てることができます。この機能は、VLAN グループを使用して WLAN を 1 つまたは複数の VLAN にマップします。ワイヤレス クライアントが WLAN に関連付けられると、ワイヤレスクライアントのMACアドレスに基づいてアルゴリズムにより VLAN が生成されます。VLAN がクライアントに割り当てられ、クライアントが割り当てられた VLAN からIPアドレスを取得します。またこの機能は、現行のAPグループアーキテクチャおよびAAAオーバーライドアーキテクチャを拡張します。これらのアーキテクチャではAPグループとAAAオーバーライドが、WLAN がマップされている 1 つの VLAN または VLAN グループをオーバーライドできます。

Cisco IOS XE Release 3.7.0E で導入された動作の変更：クライアントが WLAN に関連付けられ、WLAN が VLAN グループに適用されると、クライアントの MAC アドレスと VLAN グループの VLAN の数に基づき、ハッシュ アルゴリズムを使用してインデックスが算出されます。このインデックスに基づいて、VLAN がクライアントに割り当てられます。インデックスが「ダーティ」である場合、別のインデックスがラウンドロビン方式で生成され、新たに生成されたインデックスに基づいて VLAN がクライアントに割り当てられます。

クライアントが DHCP を使用して IP アドレスを受信できない場合、VLAN が 30 分間にわたり「ダーティ」としてマークされます。30分経過しても、VLANグループのVLANから「ダーティ」フラグがクリアされないことがあります。これは、グローバル タイマーが期限切れになるまでに 5 分の遅延があるために、各インターフェイスのタイムスタンプを調べて 30 分よりも大きいかどうかを確認する必要があるため、予期される動作です。

関連トピック

VLAN グループの作成（CLI），（2427 ページ）

VLAN グループの設定方法

VLAN グループの作成（CLI）

手順の概要

1. **configure terminal**
2. **vlan group** *WORD* **vlan-list** *vlan-ID*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan group** *WORD* **vlan-list** *vlan-ID* 例： `スイッチ(config)#vlan group vlangrp1 vlan-list 91-95`	所定のグループ名（vlangrp1）でVLAN グループを作成し、コマンドに一覧表示されているすべての VLAN を追加します。VLAN リストの範囲は 1 ～ 4096 で、1 つのグループの VLAN の数として推奨される数は 32 です。
ステップ 3	**end** 例： `スイッチ(config)#end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。また、**CTRL-Z** を押して、グローバル コンフィギュレーション モードを終了します。

関連トピック

VLAN グループについて，（2426 ページ）

VLAN グループの削除（CLI）

手順の概要

1. **configure terminal**
2. **vlan group** *WORD* **vlan-list** *vlan-ID*
3. **no vlan group** *WORD* **vlan-list** *vlan-ID*
4. **end**

手順の詳細

ステップ 1 **configure terminal**

例：
```
スイッチ# configure terminal
```
グローバル コマンド モードを開始します。

ステップ 2 **vlan group** *WORD* **vlan-list** *vlan-ID*

例：
```
スイッチ(config)#vlan group vlangrp1 vlan-list 91-95
```
所定のグループ名（vlangrp1）でVLANグループを作成し、コマンドに一覧表示されているすべてのVLANを追加します。VLAN リストの範囲は 1 ～ 4096 で、1 つのグループの VLAN の数として推奨される数は 32 です。

ステップ 3 **no vlan group** *WORD* **vlan-list** *vlan-ID*

例：
```
スイッチ(config)#no vlan group vlangrp1 vlan-list 91-95
```
所定のグループ名（vlangrp1）の VLAN グループが削除されます。

ステップ 4 **end**

例：
```
スイッチ(config)#end
```
グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。また、**CTRL-Z** を押して、グローバル コンフィギュレーション モードを終了します。

WLAN への VLAN グループの追加（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *WORD number*
3. **client vlan** *WORD*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コマンド モードを開始します。
ステップ 2	**wlan** *WORD number* 例： スイッチ(config)#**wlan wlanname 512**	WLAN が ID を使用して VLAN グループをマッピングできるようにします。WLAN ID 値の範囲は 1 ～ 512 です。
ステップ 3	**client vlan** *WORD* 例： スイッチ(config-wlan)#client vlan vlangrp1	VLAN ID、VLAN グループ、または VLAN 名を入力して、VLAN グループを WLAN にマッピングします。
ステップ 4	**end** 例： スイッチ(config-wlan)#end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。また、**CTRL-Z** を押して、グローバル コンフィギュレーション モードを終了します。

VLAN グループの VLAN の表示（CLI）

コマンド	説明
show vlan group	VLAN グループの名前と使用可能な VLAN のリストを表示します。
show vlan group group-name **<group_name>**	指定された VLAN グループの詳細を表示します。

コマンド	説明
`show wireless vlan group <group_name>`	指定されたワイヤレスVLANグループの詳細を表示します。

次の作業

VLANグループを設定したら、次の項目を設定できます。

- VLANs
- VLANトランキング プロトコル（VTP）
- VLANトランク
- 音声VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN Command Reference (Catalyst 3650 Switches)* *Layer 2/3 Command Reference (Catalyst 3650 Switches)*
VLANアクセス マップ	*Security Configuration Guide (Catalyst 3650 Switches)* *Security Command Reference (Catalyst 3650 Switches)*
VLANおよびモビリティ エージェント	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
Cisco Flexible NetFlow	*Cisco Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)* *Flexible Netflow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
IGMP スヌーピング	*IP Multicast Routing Command Reference (Catalyst 3650 Switches)* *IP Multicast Routing Configuration Guide (Catalyst 3650 Switches)*

関連項目	マニュアル タイトル
IPv6	*IPv6 Configuration Guide (Catalyst 3650 Switches)* *IPv6 Command Reference (Catalyst 3650 Switches)*
SPAN	*Network Management Command Reference (Catalyst 3650 Switches)* *Network Management Configuration Guide (Catalyst 3650 Switches)*
プラットフォームに依存しない設定情報	*Identity Based Networking Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

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

シスコのテクニカル サポート

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

VLAN グループの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	VLAN（GUI）サポート。

第 107 章

VLAN トランクの設定

- 機能情報の確認，2433 ページ
- VLAN トランクの前提条件，2433 ページ
- VLAN トランクの制約事項，2434 ページ
- VLAN トランクについて，2435 ページ
- VLAN トランクの設定方法，2439 ページ
- 次の作業，2456 ページ
- その他の参考資料，2456 ページ
- VLAN トランクの機能履歴と情報，2458 ページ

機能情報の確認

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

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

VLAN トランクの前提条件

IEEE 802.1Q トランクは、ネットワークのトランキング方式について次の制約があります。

- IEEE 802.1Q トランクを使用して接続している Cisco スイッチのネットワークでは、スイッチはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持しま

す。他社製のデバイスは、すべての VLAN でスパニングツリー インスタンスを 1 つサポートする場合があります。

IEEE 802.1Q トランクを使用して Cisco スイッチを他社製のデバイスに接続する場合、Cisco スイッチは、トランクの VLAN のスパニングツリー インスタンスを、他社製の IEEE 802.1Q スイッチのスパニングツリー インスタンスと結合します。ただし、各 VLAN のスパニングツリー情報は、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離された Cisco スイッチによって維持されます。Cisco スイッチと分離された他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

- IEEE 802.1Qトランクに対応するネイティブVLANが、トランク リンクの両側で一致していなければなりません。トランクの片側のネイティブ VLAN と反対側のネイティブ VLAN が異なっていると、スパニングツリー ループが発生する可能性があります。
- ネットワーク上のすべてのネイティブVLANについてスパニングツリーをディセーブルにせずに、IEEE 802.1Q トランクのネイティブ VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリーループが発生することがあります。IEEE 802.1Qトランクのネイティブ VLAN 上でスパニングツリーをイネーブルのままにしておくか、またはネットワーク上のすべてのVLANでスパニングツリーをディセーブルにすることを推奨します。また、ネットワークにループがないことを確認してから、スパニングツリーをディセーブルにしてください。

VLAN トランクの制約事項

次に、VLAN トランクに関する制約事項を示します。

- トランク ポートをセキュア ポートにすることはできません。
- トランク ポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内のすべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次に示すパラメータのいずれかの設定を変更すると、スイッチは、入力された設定をグループ内のすべてのポートに伝播します。
  - 許可 VLAN リスト。
  - 各 VLAN の STP ポート プライオリティ。
  - STP PortFast の設定値。
  - トランク ステータス：

    ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- Per VLAN Spanning Tree（PVST）モードでは最大 24 までのトランク ポート、マルチ スパニング ツリー（MST）モードでは最大 40 までのトランク ポートを設定することを推奨します。

- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。
- ダイナミック トランキング プロトコル（DTP）はトンネル ポートではサポートされていません。
- スイッチはレイヤ 3 トランクをサポートしません。したがって、サブインターフェイスを設定する、またはレイヤ 3 インターフェイスで **encapsulation** キーワードを使用することはできません。ただし、スイッチは、同等の機能を備えたレイヤ 2 トランクおよびレイヤ 3 VLAN インターフェイスをサポートします。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

VLAN トランクについて

トランキングの概要

トランクとは、1 つまたは複数のイーサネット スイッチ インターフェイスと他のネットワーキング デバイス（ルータ、スイッチなど）の間のポイントツーポイント リンクです。イーサネット トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張できます。

すべてのイーサネット インターフェイス上で、次のトランキング カプセル化方式を使用できます。

- IEEE 802.1Q：業界標準のトランキング カプセル化方式です。

トランキング モード

イーサネット トランク インターフェイスは、さまざまなトランキング モードをサポートします。インターフェイスをトランキングまたは非トランキングとして設定したり、ネイバー インターフェイスとトランキングのネゴシエーションを行ったりするように設定できます。トランキングを自動ネゴシエーションするには、インターフェイスが同じ VTP ドメインに存在する必要があります。

トランク ネゴシエーションは、ポイントツーポイント プロトコル（PPP）であるダイナミック トランキング プロトコル（DTP）によって管理されます。ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。

関連トピック

トランク ポートの設定（CLI），（2439 ページ）
レイヤ 2 インターフェイス モード，（2436 ページ）

レイヤ 2 インターフェイス モード

表 *179*：レイヤ *2* インターフェイス モード

モード	機能
switchport mode access	インターフェイス（アクセス ポート）を永続的な非トランキング モードにして、リンクの非トランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスかどうかに関係なく、非トランク インターフェイスになります。
switchport mode dynamic auto	インターフェイスがリンクをトランク リンクに変換できるようにします。インターフェイスは、ネイバー インターフェイスが **trunk** または **desirable** モードに設定されている場合、トランク インターフェイスになります。すべてのイーサネット インターフェイスのデフォルトのスイッチポート モードは、**dynamic auto** です。
switchport mode dynamic desirable	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、ネイバー インターフェイスが **trunk**、**desirable**、または **auto** モードに設定されている場合、トランク インターフェイスになります。
switchport mode trunk	インターフェイスを永続的なトランキング モードにして、ネイバー リンクのトランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスでない場合でも、トランク インターフェイスになります。

モード	機能
switchport nonegotiate	インターフェイスが DTP フレームを生成しないようにします。このコマンドは、インターフェイス スイッチポート モードが **access** または **trunk** の場合だけ使用できます。トランク リンクを確立するには、手動でネイバーインターフェイスをトランク インターフェイスとして設定する必要があります。

関連トピック

トランク ポートの設定（CLI），（2439 ページ）
トランキング モード，（2435 ページ）

トランクでの許可 VLAN

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランクですべての VLAN ID（1 ～ 4094）が許可されます。ただし、許可リストから VLAN を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。

スパニングツリー ループまたはストームのリスクを減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにできます。トランク ポートから VLAN 1 を削除した場合、インターフェイスは引き続き VLAN 1 内で Cisco Discovery Protocol（CDP）、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、DTP、および VTP などの管理トラフィックを送受信します。

VLAN 1 をディセーブルにしたトランク ポートが非トランク ポートになると、そのポートはアクセス VLAN に追加されます。アクセス VLAN が 1 に設定されると、**switchport trunk allowed** の設定には関係なく、ポートは VLAN 1 に追加されます。ポート上でディセーブルになっている任意の VLAN について同様のことが当てはまります。

トランク ポートは、VLAN がイネーブルになっており、VTP が VLAN を認識し、なおかつポートの許可リストにその VLAN が登録されている場合に、VLAN のメンバになることができます。VTP が新しくイネーブルにされた VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバになります。VTP が新しい VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されていない場合には、トランク ポートはその VLAN のメンバにはなりません。

関連トピック

トランクでの許可 VLAN の定義（CLI），（2442 ページ）

トランク ポートでの負荷分散

負荷分散により、スイッチに接続しているパラレル トランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、スイッチ間で 1 つのパラレル リンク以外のすべてのリンクをブロックします。負荷分散を行うと、トラフィックの所属する VLAN に基づいて、リンク間でトラフィックが分散されます。

トランク ポートで負荷分散を設定するには、STP ポート プライオリティまたは STP パス コストを使用します。STP ポート プライオリティを使用して負荷分散を設定する場合には、両方の負荷分散リンクを同じスイッチに接続する必要があります。STP パス コストを使用して負荷分散を設定する場合には、それぞれの負荷分散リンクを同一のスイッチに接続することも、2 台の異なるスイッチに接続することもできます。

STP プライオリティによるネットワーク負荷分散

同一のスイッチ上の 2 つのポートがループを形成すると、スイッチは STP ポート プライオリティを使用して、どのポートをイネーブルとし、どのポートをブロッキング ステートとするかを判断します。パラレル トランク ポートにプライオリティを設定することにより、そのポートに、特定の VLAN のすべてのトラフィックを伝送させることができます。VLAN に対するプライオリティの高い（値の小さい）トランク ポートがその VLAN のトラフィックを転送します。同じ VLAN に対してプライオリティの低い（値の大きい）トランク ポートは、その VLAN に対してブロッキング ステートのままです。1 つのトランク ポートが特定の VLAN に関するすべてのトラフィックを送受信することになります。

関連トピック

STP ポート プライオリティによる負荷分散の設定（CLI），（2448 ページ）

STP パス コストによるネットワーク負荷分散

トランクにそれぞれ異なるパス コストを設定し、各パス コストをそれぞれ異なる VLAN 群に対応付け、各 VLAN でポートをブロックすることによって、VLAN トラフィックを分散するパラレル トランクを設定できます。VLAN はトラフィックを分離し、リンクが失われた場合に備えて冗長性を維持します。

関連トピック

STP パス コストによる負荷分散の設定（CLI），（2453 ページ）

機能の相互作用

トランキングは他の機能と次のように相互作用します。

- トランク ポートをセキュア ポートにすることはできません。
- トランク ポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内のすべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き

継ぎます。次に示すパラメータのいずれかの設定を変更すると、スイッチは、入力された設定をグループ内のすべてのポートに伝播します。

- 許可 VLAN リスト。
- 各 VLAN の STP ポート プライオリティ。
- STP PortFast の設定値。
- トランク ステータス：

  ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。

- Per VLAN Spanning Tree（PVST）モードでは最大 24 までのトランク ポート、マルチ スパニング ツリー（MST）モードでは最大 40 までのトランク ポートを設定することを推奨します。
- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。

VLAN トランクの設定方法

トランクの誤設定を避けるために、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように（つまり DTP をオフにするように）設定してください。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

トランク ポートとしてのイーサネット インターフェイスの設定

トランク ポートの設定（CLI）

トランク ポートは VTP アドバタイズを送受信するので、VTP を使用する場合は、スイッチ上で少なくとも 1 つのトランク ポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。

はじめる前に

デフォルトでは、インターフェイスはレイヤ 2 モードです。レイヤ 2 インターフェイスのデフォルト モードは、**switchport mode dynamic auto** です。隣接インターフェイスがトランキングをサポートし、トランキングを許可するように設定されている場合、リンクはレイヤ2トランクです。また、インターフェイスがレイヤ 3 モードの場合は、**switchport** インターフェイス コンフィギュレーション コマンドを入力するとレイヤ 2 トランクになります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}
5. **switchport access vlan***vlan-id*
6. **switchport trunk native vlan***vlan-id*
7. **end**
8. **show interfaces***interface-id***switchport**
9. **show interfaces***interface-id***trunk**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	トランクに設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**} 例： `スイッチ(config-if)# switchport mode dynamic desirable`	インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートであり、トランキング モードを設定する場合に限り必要となります）。 • **dynamic auto**：ネイバー インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。これはデフォルトです。 • **dynamic desirable**：ネイバー インターフェイスが trunk、desirable、または auto モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 • **trunk**：ネイバー インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リンクに変換するようにネゴシエートします。
ステップ 5	**switchport access vlan***vlan-id* 例： `スイッチ(config-if)# switchport access vlan 200`	（任意）インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。
ステップ 6	**switchport trunk native vlan***vlan-id* 例： `スイッチ(config-if)# switchport trunk native vlan 200`	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
ステップ 7	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces***interface-id***switchport** 例： `スイッチ# show interfaces gigabitethernet1/0/2 switchport`	インターフェイスのスイッチ ポート設定を表示します。[Administrative Mode] および [Administrative Trunking Encapsulation] フィールドに表示されます。

	コマンドまたはアクション	目的
ステップ 9	**show interfaces***interface-id***trunk** 例： スイッチ# **show interfaces gigabitethernet1/0/2 trunk**	インターフェイスのトランクの設定を表示します。
ステップ 10	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

トランキング モード, （2435 ページ）
レイヤ 2 インターフェイス モード, （2436 ページ）

トランクでの許可 VLAN の定義（CLI）

VLAN 1 は、すべての Cisco スイッチのすべてのトランク ポートのデフォルト VLAN です。以前は、すべてのトランク リンクで VLAN 1 を必ずイネーブルにする必要がありました。VLAN 1 の最小化機能を使用して、個々の VLAN トランク リンクで VLAN 1 をディセーブルに設定できます。これにより、ユーザ トラフィック（スパニングツリー アドバタイズなど）は VLAN 1 で送受信されなくなります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode trunk**
5. **switchport trunk allowed vlan** { *word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list*
6. **end**
7. **show interfaces***interface-id***switchport**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk** 例： スイッチ(config-if)# **switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 5	**switchport trunk allowed vlan** {*word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list* 例： スイッチ(config-if)# **switchport trunk allowed vlan remove 2**	（任意）トランク上で許容されるVLANのリストを設定します。 *vlan-list* パラメータは、1 ～ 4094 の単一の VLAN 番号、または2つのVLAN番号（小さい方が先、ハイフンで区切る）で指定されたVLAN範囲です。カンマで区切ったVLANパラメータの間、またはハイフンで指定した範囲の間には、スペースを入れないでください。 デフォルトでは、すべての VLAN が許可されます。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show interfaces***interface-id***switchport** 例： スイッチ# **show interfaces gigabitethernet1/0/1 switchport**	表示された [Trunking VLANs Enabled] フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

トランクでの許可 VLAN, （2437 ページ）

プルーニング適格リストの変更（CLI）

プルーニング適格リストは、トランク ポートだけに適用されます。トランク ポートごとに独自の適格リストがあります。この手順を有効にするには、VTP プルーニングがイネーブルに設定されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**}*vlan-list* [,*vlan* [,*vlan* [,,,]]
5. **end**
6. **show interfaces***interface-id***switchport**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet2/0/1**	VLAN プルーニングを適用するトランク ポートを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**}*vlan-list* [,*vlan* [,*vlan* [,,,]]	トランクからのプルーニングを許可する VLAN のリストを設定します。 **add**、**except**、**none**、および **remove** キーワードの使用方法については、このリリースに対応するコマンド リファレンスを参照してください。 連続していない VLAN ID は、カンマ（スペースなし）で区切ります。ID の範囲はハイフンで指定します。有効な ID 範囲は 2 ～ 1001 です。拡張範囲 VLAN（VLAN ID 1006 ～ 4094）はプルーニングできません。 プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。 デフォルトでは、プルーニングが許可される VLAN のリストには、VLAN 2 ～ 1001 が含まれます。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show interfaces***interface-id***switchport** 例： スイッチ# **show interfaces gigabitethernet2/0/1 switchport**	表示された [Pruning VLANs Enabled] フィールドの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

タグなしトラフィック用ネイティブ VLAN の設定（CLI）

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、スイッチ はタグなしトラフィックを、ポートに設定されたネイティブ VLAN に転送します。ネイティブ VLAN は、デフォルトでは VLAN 1 です。

ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

パケットの VLAN ID が出力ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport trunk native vlan***vlan-id*
5. **end**
6. **show interfaces***interface-id***switchport**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	IEEE 802.1Q トランクとして設定するインターフェイスを定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport trunk native vlan***vlan-id* 例： スイッチ(config-if)# **switchport trunk native vlan 12**	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。 *vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces***interface-id***switchport** 例： スイッチ# **show interfaces gigabitethernet1/0/2 switchport**	[Trunking Native Mode VLAN] フィールドの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

トランク ポートの負荷分散の設定

STP ポート プライオリティによる負荷分散の設定（CLI）

スイッチがスイッチ スタックのメンバである場合、**spanning-tree** [**vlan** *vlan-id*] **port-priority***priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree** [**vlan** *vlan-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させるインターフェイスには、低いコスト値を割り当て、最後に選択させるインターフェイスには高いコスト値を割り当てます。

次の手順では、STP ポート プライオリティを使用した負荷分散を指定してネットワークを設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vtp domain***domain-name*
4. **vtp mode server**
5. **end**
6. **show vtp status**
7. **show vlan**
8. **configure terminal**
9. **interface***interface-id*
10. **switchport mode trunk**
11. **end**
12. **show interfaces***interface-id***switchport**
13. スイッチ A で、スイッチ またはスイッチ スタック の 2 番目のポートに対して前述の手順を繰り返します。
14. スイッチ B で前述の手順を繰り返し、スイッチ A で設定したトランク ポートに接続するトランク ポートを設定します。
15. **show vlan**
16. **configure terminal**
17. **interface***interface-id*
18. **spanning-tree vlan***vlan-range***port-priority***priority-value*
19. **exit**
20. **interface***interface-id*
21. **spanning-tree vlan***vlan-range***port-priority***priority-value*
22. **end**
23. **show running-config**
24. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp domain***domain-name* 例： スイッチ(config)# **vtp domain workdomain**	VTP 管理ドメインを設定します。 1 ～ 32 文字のドメイン名を使用できます。
ステップ 4	**vtp mode server** 例： スイッチ(config)# **vtp mode server**	スイッチ A を VTP サーバとして設定します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show vtp status** 例： スイッチ# **show vtp status**	スイッチ A およびスイッチ B の両方で、VTP 設定を確認します。 表示された *VTP Operating Mode* および *VTP Domain Name* フィールドをチェックします。
ステップ 7	**show vlan** 例： スイッチ# **show vlan**	スイッチ A のデータベースに VLAN が存在していることを確認します。
ステップ 8	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 9	**interface***interface-id* 例： スイッチ(config)# **interface**	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	gigabitethernet1/0/1	
ステップ 10	**switchport mode trunk** 例： スイッチ(config-if)# **switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 11	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 12	**show interfaces***interface-id***switchport** 例： スイッチ# **show interfaces gigabitethernet1/0/1 switchport**	VLAN の設定を確認します。
ステップ 13	スイッチ A で、スイッチ またはスイッチ スタック の 2 番目のポートに対して前述の手順を繰り返します。	
ステップ 14	スイッチ B で前述の手順を繰り返し、スイッチ A で設定したトランク ポートに接続するトランク ポートを設定します。	
ステップ 15	**show vlan** 例： スイッチ# **show vlan**	トランク リンクがアクティブになると、VTP がスイッチ B に VTP および VLAN 情報を渡します。このコマンドは、スイッチ B が VLAN 設定を学習したことを確認します。
ステップ 16	**configure terminal** 例： スイッチ# **configure terminal**	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 17	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 18	**spanning-tree vlan***vlan-range***port-priority***priority-value* 例： スイッチ(config-if)# **spanning-tree vlan 8-10 port-priority 16**	指定されたVLAN範囲にポートプライオリティを割り当てます。0 ～ 240 のポート プライオリティ値を入力します。ポート プライオリティ値は 16 ずつ増分します。
ステップ 19	**exit** 例： スイッチ(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 20	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 21	**spanning-tree vlan***vlan-range***port-priority***priority-value* 例： スイッチ(config-if)# **spanning-tree vlan 3-6 port-priority 16**	指定されたVLAN範囲にポートプライオリティを割り当てます。0 ～ 240 のポート プライオリティ値を入力します。ポート プライオリティ値は 16 ずつ増分します。
ステップ 22	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 23	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。
ステップ 24	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

STP プライオリティによるネットワーク負荷分散, （2438 ページ）

STP パス コストによる負荷分散の設定（CLI）

次の手順では、STP パス コストを使用した負荷分散を指定してネットワークを設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **switchport mode trunk**
5. **exit**
6. スイッチ A またはスイッチ A スタック内の別のインターフェイスでステップ 2 ～ 4 を繰り返します。
7. **end**
8. **show running-config**
9. **show vlan**
10. **configure terminal**
11. **interface***interface-id*
12. **spanning-tree vlan***vlan-range***cost***cost-value*
13. **end**
14. スイッチ A に設定したもう一方のトランク インターフェイスでステップ 9 ～ 13 を繰り返し、VLAN 8、9、および 10 のスパニングツリー パス コストを 30 に設定します。
15. **exit**
16. **show running-config**
17. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： スイッチ# **configure terminal**	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk** 例： スイッチ(config-if)# **switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 5	**exit** 例： スイッチ(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	スイッチ A またはスイッチ A スタック内の別のインターフェイスでステップ 2 ～ 4 を繰り返します。	
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。画面で、インターフェイスがトランク ポートとして設定されていることを確認してください。
ステップ 9	**show vlan** 例： スイッチ# **show vlan**	トランク リンクがアクティブになると、スイッチ A がもう一方のスイッチから VTP 情報を受信します。このコマンドは、スイッチ A が VLAN コンフィギュレーションを学習したことを確認します。

	コマンドまたはアクション	目的
ステップ 10	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 11	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	STP コストを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**spanning-tree vlan***vlan-range***cost***cost-value* 例： スイッチ(config-if)# **spanning-tree vlan 2-4 cost 30**	VLAN 2 ～ 4 のスパニングツリー パス コストを 30 に設定します。
ステップ 13	**end** 例： スイッチ(config-if)# **end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	スイッチ A に設定したもう一方のトランク インターフェイスでステップ 9 ～ 13 を繰り返し、VLAN 8、9、および 10 のスパニングツリー パス コストを 30 に設定します。	
ステップ 15	**exit** 例： スイッチ(config)# **exit**	特権 EXEC モードに戻ります。
ステップ 16	**show running-config** 例： スイッチ# **show running-config**	入力を確認します。両方のトランク インターフェイスに対してパス コストが正しく設定されていることを表示で確認します。
ステップ 17	**copy running-config startup-config** 例： スイッチ# **copy running-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

関連トピック

STP パス コストによるネットワーク負荷分散, （2438 ページ）

次の作業

VLAN トランクを設定したら、次の項目を設定できます。

- VLANs
- VLAN グループ
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN Command Reference (Catalyst 3650 Switches)* *Layer 2/3 Command Reference (Catalyst 3650 Switches)*
スパニング ツリー プロトコル（STP）	*Network Management Command Reference (Catalyst 3650 Switches)* *Network Management Configuration Guide (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

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

シスコのテクニカル サポート

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

VLAN トランクの機能履歴と情報

リリース	変更内容

第 108 章

音声 VLAN の設定

- 機能情報の確認，2459 ページ
- 音声 VLAN の前提条件，2459 ページ
- 音声 VLAN の制約事項，2460 ページ
- 音声 VLAN に関する情報，2460 ページ
- 音声 VLAN の設定方法，2463 ページ
- 音声 VLAN のモニタリング，2467 ページ
- 次の作業，2467 ページ
- その他の参考資料，2468 ページ
- 音声 VLAN の機能履歴と情報，2469 ページ

機能情報の確認

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

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

音声 VLAN の前提条件

音声 VLAN の前提条件は、次のとおりです。

- 音声 VLAN 設定はスイッチのアクセス ポートだけでサポートされており、トランク ポートではサポートされていません。

（注） トランク ポートは、標準 VLAN と同様に、任意の数の音声 VLAN を伝送できます。トランク ポートでは、音声 VLAN の設定がサポートされません。

- 音声 VLAN を有効にする前に、 **trust device cisco-phone** インターフェイス設定コマンドを入力し、スイッチ上の QoS をイネーブルにします。Auto QoS 機能を使用すると、これらは自動的に設定されます。
- IP Phone にコンフィギュレーションを送信するために、Cisco IP Phone に接続するスイッチ ポート上で CDP をイネーブルにする必要があります（デフォルト設定では、CDP がすべてのスイッチ インターフェイスでグローバルにイネーブルになっています）。

音声 VLAN の制約事項

音声 VLAN には、スタティック セキュア MAC アドレスを設定できません。

音声 VLAN に関する情報

音声 VLAN

音声 VLAN 機能を使用すると、アクセス ポートで IP Phone からの IP 音声トラフィックを伝送できます。スイッチを Cisco 7960 IP Phone に接続すると、IP Phone はレイヤ 3 IP 値およびレイヤ 2 サービス クラス（CoS）値を使用して、音声トラフィックを送信します。どちらの値もデフォルトでは 5 に設定されます。データ送信が均質性に欠ける場合、IP Phone の音質が低下することがあります。そのため、このスイッチは IEEE 802.1p CoS に基づく Quality of Service（QoS）をサポートしています。QoS は、分類およびスケジューリングを使用して、スイッチからのネットワークトラフィックを予測可能な方法で送信します。

Cisco7960 IP Phone は設定可能なデバイスであり、IEEE 802.1p プライオリティに基づいてトラフィックを転送するように設定できます。Cisco IP Phone によって割り当てられたトラフィック プライオリティを信頼したり、オーバーライドしたりするようにスイッチを設定できます。

Cisco IP Phone の音声トラフィック

Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。Cisco Discovery Protocol（CDP）パケットを送信するよう、スイッチ上のアクセス ポートを設定できます。CDP パケットは、接続する IP Phone に対して、次のいずれかの方法で音声トラフィックをスイッチに送信するよう指示します。

- レイヤ 2 CoS プライオリティ値のタグ付き音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値のタグ付きアクセス VLAN による送信
- タグなし（レイヤ 2 CoS プライオリティ値なし）のアクセス VLAN による送信

（注） いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（音声トラフィックはデフォルトで 5、音声制御トラフィックは 3）を伝送します。

関連トピック

Cisco IP Phone の音声トラフィックの設定（CLI），（2463 ページ）
音声 VLAN のモニタリング，（2467 ページ）

Cisco IP Phone のデータ トラフィック

スイッチは、Cisco IP Phone のアクセス ポートに接続されたデバイスから送られる、タグ付きデータ トラフィック（IEEE 802.1Q または IEEE 802.1p フレーム タイプのトラフィック）を処理することもできます。CDP パケットを送信するよう、スイッチ上のレイヤ 2 アクセス ポートを設定できます。CDP パケットは、接続する IP Phone に対して、次のいずれかのモードで IP Phone アクセス ポートを設定するよう指示します。

- trusted（信頼性がある）モードでは、Cisco IP Phone のアクセス ポート経由で受信したすべてのトラフィックがそのまま IP Phone を通過します。
- untrusted（信頼性がない）モードでは、Cisco IP Phone のアクセス ポート経由で受信した IEEE 802.1Q および IEEE 802.1p フレームのすべてのトラフィックに、設定されたレイヤ 2 CoS 値を与えます。デフォルトのレイヤ 2 CoS 値は 0 です。信頼できないモードがデフォルト設定です。

（注） Cisco IP Phone に接続されたデバイスからのタグなしトラフィックは、IP Phone のアクセス ポートの信頼状態に関係なく、そのまま IP Phone を通過します。

関連トピック

着信データ フレームのプライオリティ設定（CLI），（2465 ページ）
音声 VLAN のモニタリング，（2467 ページ）

音声 VLAN 設定時の注意事項

- Cisco7960 IP Phone は、PC やその他のデバイスとの接続もサポートしているので、スイッチを Cisco IP Phone に接続するポートは、さまざまな種類のトラフィックを伝送できます。ポー

トを設定することによって、Cisco IP Phone による音声トラフィックおよびデータ トラフィックの伝送方法を決定できます。

- IP Phone で音声 VLAN 通信が適切に行われるには、スイッチ上に音声 VLAN が存在し、アクティブになっている必要があります。VLAN が存在しているかどうかを確認するには、**show vlan** 特権 EXEC コマンドを使用します（リストで表示されます）。VLAN がリストされていない場合は、音声 VLAN を作成します。
- Power Over Ethernet（PoE）スイッチは、シスコ先行標準の受電デバイスまたは IEEE 802.3af 準拠の受電デバイスが AC 電源から電力を供給されてない場合に、それらの受電デバイスに自動的に電力を供給できます。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。
- Cisco IP Phone とその IP Phone に接続されたデバイスが同じ VLAN 上にある場合、両方とも同じ IP サブネットに属していなければなりません。次の条件が満たされている場合は、同じ VLAN 上にあります。
  - 両方とも IEEE 802.1p またはタグなしフレームを使用する。
  - Cisco IP Phone が IEEE 802.1p フレームを使用し、デバイスがタグなしフレームを使用する。
  - Cisco IP Phone がタグなしフレームを使用し、デバイスが IEEE 802.1p フレームを使用する。
  - Cisco IP Phone が IEEE 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである。
- Cisco IP Phone と IP Phone に接続されたデバイスは、同一 VLAN、同一サブネット上にあっても、使用するフレーム タイプが異なる場合は通信できません。トラフィックは同一サブネット上でルーティングされないからです（ルーティングによってフレーム タイプの相違が排除されます）。
- 音声 VLAN ポートには次のポート タイプがあります。
  - ダイナミック アクセス ポート。
  - IEEE 802.1x 認証ポート。

  （注） 音声 VLAN が設定され Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x をイネーブルにした場合、その IP Phone からスイッチへの接続が最大 30 秒間失われます。
  - 保護ポート。
  - SPAN または RSPAN セッションの送信元ポートまたは宛先ポート。
  - セキュア ポート。

（注） 音声 VLAN も設定しているインターフェイス上でポート セキュリティをイネーブルにする場合、ポートで許容されるセキュア アドレスの最大数を、アクセス VLAN におけるセキュア アドレスの最大数に 2 を足した数に設定する必要があります。ポートを Cisco IP Phone に接続している場合、IP Phone に最大で 2 つの MAC アドレスが必要になります。IP Phone のアドレスは、音声 VLAN で学習され、アクセス VLAN でも学習される場合があります。PC を IP Phone に接続する場合、追加の MAC アドレスが必要になります。

音声 VLAN の設定方法

Cisco IP Phone の音声トラフィックの設定（CLI）

Cisco IP Phone に CDP パケットを送信して IP Phone による音声トラフィックの送信方法を設定するように、IP Phone に接続するポートを設定できます。IP Phone は指定された音声 VLAN に、レイヤ 2 CoS 値を使用して、IEEE 802.1Q フレームの音声トラフィックを伝送できます。IEEE 802.1p のプライオリティ タグを使用すると、音声トラフィックにさらに高いプライオリティを与え、すべての音声トラフィックをネイティブ（アクセス）VLAN 経由で転送できます。Cisco IP Phone はタグなしの音声トラフィックを送信する、または独自の設定を使用してアクセス VLAN で音声トラフィックを送信することもできます。いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（デフォルトは 5）を伝送します。

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. **trust device cisco-phone**
4. **switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}
5. **end**
6. 次のいずれかを使用します。
   - **show interfaces***interface-id***switchport**
   - **show running-config interface***interface-id*
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**trust device cisco-phone** 例： スイッチ(config-if)# **trust-device cisco-phone**	Cisco IP Phone の着信トラフィック パケットを信頼するようにインターフェイスを設定します。
ステップ 4	**switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**} 例： スイッチ(config-if)# **switchport voice vlan dot1p**	音声 VLAN を設定します。 • *vlan-id*：すべての音声トラフィックが特定の VLAN を経由して転送されるように IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。指定できる VLAN ID の範囲は 1 ～ 4094 です。 • **dot1p**：VLAN ID 0（ネイティブ VLAN）のタグが付けられた音声およびデータ IEEE 802.1p プライオリティ フレームを受け入れるよう、スイッチを設定します。デフォルトでは、スイッチは VLAN 0 のタグが付いたすべての音声およびデータ トラフィックをドロップします。802.1p に対応するよう設定されると、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用してトラフィックを転送します。 • **none**：IP Phone で独自の設定を使ってタグなし音声トラフィックを送信できるようにします。 • **untagged**：タグなし音声トラフィックを送信するように IP Phone を設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

ステップ 6	次のいずれかを使用します。
	• **show interfaces***interface-id***switchport**
	• **show running-config interface***interface-id*
	
	例：
	`スイッチ# show interfaces gigabitethernet1/0/1 switchport`
	または
	`スイッチ# show running-config interface gigabitethernet1/0/1`
		音声 VLAN の設定、または QoS および音声 VLAN の設定を確認します。

ステップ 7	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

Cisco IP Phone の音声トラフィック，（2460 ページ）
音声 VLAN のモニタリング，（2467 ページ）

着信データ フレームのプライオリティ設定（CLI）

PC またはその他のデータ デバイスを Cisco IP Phone ポートに接続できます。タグ付きデータ トラフィック（IEEE 802.1Q または IEEE 802.1p フレーム）を処理するために、CDP パケットを送信するようスイッチを設定できます。CDP パケットは Cisco IP Phone に対して、IP Phone 上のアクセス ポートに接続されたデバイスからのデータ パケット送信方法を指示します。PC は、CoS 値が割り当てられたパケットを生成できます。接続デバイスから IP Phone のポートに届いたフレームのプライオリティを変更しない（信頼する）または変更する（信頼しない）ように、IP Phone を設定できます。

Cisco IP Phone で非音声ポートから受信するデータ トラフィックのプライオリティを設定するには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport priority extend** {**cos***value* | **trust**}
5. **end**
6. **show interfaces***interface-id***switchport**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/1**	Cisco IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport priority extend** {**cos***value*	**trust**} 例： スイッチ(config-if)# **switchport priority extend trust**	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプライオリティを次のように設定します。 • **cos***value*：PC または接続しているデバイスから受信したプライオリティを、指定の CoS 値にオーバーライドするよう、IP Phone を設定します。値は 0 ～ 7 です。7 が最高のプライオリティです。デフォルトのプライオリティは **cos** 0 です。 • **trust**：PC または接続しているデバイスから受信したプライオリティを信頼するよう IP Phone アクセス ポートを設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces***interface-id***switchport** 例： スイッチ# **show interfaces gigabitethernet1/0/1 switchport**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

Cisco IP Phone のデータ トラフィック，（2461 ページ）
音声 VLAN のモニタリング，（2467 ページ）

音声 VLAN のモニタリング

インターフェイスの音声 VLAN 設定を表示するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを使用します。

関連トピック

Cisco IP Phone の音声トラフィックの設定（CLI），（2463 ページ）
Cisco IP Phone の音声トラフィック，（2460 ページ）
着信データ フレームのプライオリティ設定（CLI），（2465 ページ）
Cisco IP Phone のデータ トラフィック，（2461 ページ）

次の作業

音声 VLAN を設定した後は、次の設定を行うことができます。

- VLANs

- VLAN グループ
- VLAN トランキング
- VTP

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN Command Reference (Catalyst 3650 Switches)* *Layer 2/3 Command Reference (Catalyst 3650 Switches)*
追加の設定コマンドおよび手順。	*LAN Switching Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)* *Layer 2/3 Configuration Guide (Catalyst 3650 Switches)*
プラットフォームに依存しない設定情報	*Identity Based Networking Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

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

シスコのテクニカル サポート

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

音声 VLAN の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

第 109 章

プライベート VLAN の設定

- 機能情報の確認，2471 ページ
- プライベート VLAN の前提条件，2471 ページ
- プライベート VLAN の制約事項，2472 ページ
- プライベート VLAN について，2473 ページ
- プライベート VLAN の設定方法，2484 ページ
- プライベート VLAN のモニタ，2496 ページ
- プライベート VLAN の設定例，2496 ページ
- 次の作業，2499 ページ
- その他の参考資料，2499 ページ

機能情報の確認

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

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

プライベート VLAN の前提条件

プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は、VTP 3 のサーバ モードでもサポートされます。

プライベート VLAN をスイッチに設定するときに、ユニキャスト ルートとレイヤ 2 エントリとの間のシステム リソースのバランスを取るために、常にデフォルトの Switch Database Management（SDM）テンプレートを使用してください。別の SDM テンプレートが設定されている場合、デフォルト テンプレートを設定するのに **sdm prefer default** グローバル コンフィギュレーション コマンドを使用します。

プライベート VLAN の制約事項

プライベート VLAN はLAN Base イメージを実行しているスイッチではサポートされません。

（注） 一部の状況では、エラー メッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

- プライベート VLAN が設定されているスイッチでは、フォールバック ブリッジングを設定しないでください。
- リモート SPAN（RSPAN）をプライベート VLAN のプライマリまたはセカンダリ VLAN として設定しないでください。
- 次のような機能が設定されているインターフェイスにプライベート VLAN ポートを設定しないでください。
  - ダイナミック アクセス ポート VLAN メンバーシップ
  - ダイナミック トランキング プロトコル（DTP）
  - IPv6 Security Group（SG）
  - ポート集約プロトコル（PAgP）
  - リンク集約制御プロトコル（LACP）
  - マルチキャスト VLAN レジストレーション（MVR）
  - 音声 VLAN
  - Web Cache Communication Protocol（WCCP）
- IEEE 802.1x ポートベース認証をプライベート VLAN ポートに設定できますが、802.1x とポート セキュリティ、音声 VLAN、またはポート単位のユーザ ACL は、プライベート VLAN ポートに設定できません。
- プライベート VLAN ホストまたは無差別ポートは SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートに設定した場合、ポートは非アクティブになります。
- プライマリ VLAN の無差別ポートでスタティック MAC アドレスを設定する場合は、すべての関連セカンダリ VLAN に同じスタティック アドレスを追加する必要はありません。同様に、セカンダリ VLAN のホスト ポートでスタティック MAC アドレスを設定する場合は、関

連プライマリ VLAN に同じスタティック MAC アドレスを追加する必要はありません。さらに、スタティック MAC アドレスをプライベート VLAN ポートから削除する際に、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要はありません。

（注） プライベート VLAN のセカンダリ VLAN で学習したダイナミック MAC アドレスは、関連プライマリ VLAN で複製されます。プライマリ VLAN からトラフィックが入力される場合でも、すべての MAC エントリはセカンダリ VLAN で学習されます。MAC アドレスがプライマリ VLAN で動的に学習される場合は、関連セカンダリ VLAN では複製されません。

- レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。

プライベート VLAN について

プライベート VLAN ドメイン

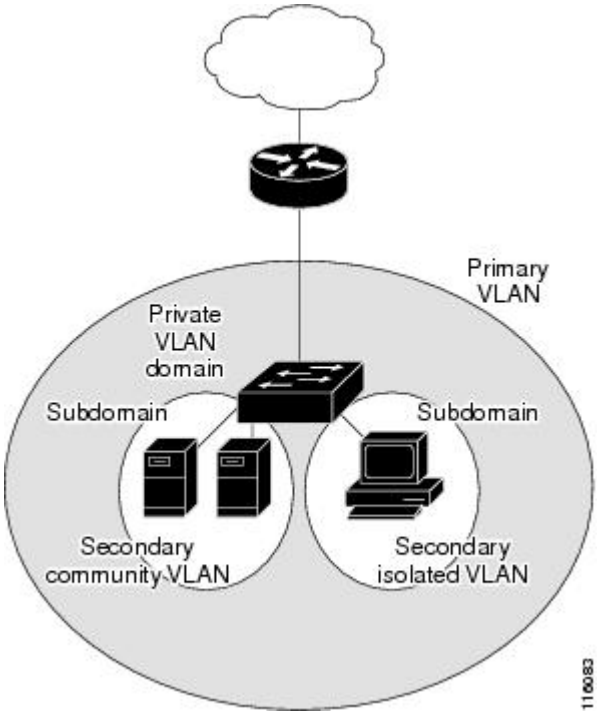
PVLAN 機能を使用すると、サービス プロバイダーが VLAN を使用したときに直面する 2 つの問題に対処できます。

- IP Base イメージまたは IP Services イメージを実行している場合、最大で 4094 個のアクティブ VLAN がスイッチでサポートされます。サービス プロバイダーが 1 カスタマーあたり 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数はこれに制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てますが、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。

プライベート VLAN を使用することでスケーラビリティの問題に対処でき、サービス プロバイダーにとっては IP アドレス管理上の利得がもたらされ、カスタマーに対してはレイヤ 2 セキュリティを提供できます。プライベート VLAN では、通常の VLAN ドメインをサブドメインに分割します。サブドメインは、プライマリ VLAN とセカンダリ VLAN のペアで表されます。プライベート VLAN には複数の VLAN ペアを設定可能で、各サブドメインにつき 1 ペアになります。プライ

ベート VLAN 内のすべての VLAN ペアは同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、各サブドメインの区別に使用されます。

図 *99*：プライベート *VLAN* ドメイン



Secondary VLANs

セカンダリ VLAN には、次の 2 種類があります。

- 独立 VLAN：独立 VLAN 内のポートは、レイヤ 2 レベルでは相互に通信できません。
- コミュニティ VLAN：コミュニティ VLAN 内のポートは互いに通信できますが、レイヤ 2 レベルにある他のコミュニティ内のポートとは通信できません。

関連トピック

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング，（2494 ページ）

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする，（2498 ページ）

プライベート VLAN ポート

プライベート VLAN では、同じプライベート VLAN 内のポート間をレイヤ 2 で分離します。プライベート VLAN ポートは、次のいずれかの種類に属するアクセス ポートです。

- 無差別：無差別ポートは、プライベート VLAN に属し、プライマリ VLAN と関連しているセカンダリ VLAN に属するコミュニティ ポートや独立ホスト ポートなどの、すべてのインターフェイスと通信できます。
- 独立：独立ポートは、独立セカンダリ VLAN に属しているホスト ポートです。これは、無差別ポートを除く、同じプライベート VLAN 内の他のポートからレイヤ 2 で完全に分離されています。プライベート VLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。
- コミュニティ：コミュニティ ポートは、1 つのコミュニティ セカンダリ VLAN に属しているホストポートです。コミュニティ ポートは、同一コミュニティ VLAN のその他のポート、および無差別ポートと通信します。これらのインターフェイスは、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN 内の独立ポートとレイヤ 2 で分離されます。

（注） トランク ポートは、通常の VLAN からのトラフィックを伝送し、またプライマリ、独立、およびコミュニティ VLAN からのトラフィックも伝送します。

プライマリおよびセカンダリ VLAN には次のような特性があります。

- プライマリ VLAN：プライベート VLAN には、プライマリ VLAN を 1 つだけ設定できます。プライベート VLAN 内のすべてのポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、無差別ポートからの単一方向トラフィックのダウンストリームを、（独立およびコミュニティ）ホスト ポートおよび他の無差別ポートへ伝送します。
- 独立 VLAN：プライベート VLAN の独立 VLAN は 1 つだけです。独立 VLAN はセカンダリ VLAN であり、ホストから無差別ポートおよびゲートウェイに向かう単一方向トラフィック アップストリームを搬送します。
- コミュニティ VLAN：コミュニティ VLAN は、アップストリーム トラフィックをコミュニティ ポートから無差別ポート ゲートウェイおよび同じコミュニティ内の他のホスト ポートに伝送するセカンダリ VLAN です。複数のコミュニティ VLAN を 1 つのプライベート VLAN に設定できます。

無差別ポートは、1 つのプライマリ VLAN、1 つの独立 VLAN、複数のコミュニティ VLAN だけで動作できます。レイヤ 3 ゲートウェイは通常、無差別ポートを介してスイッチに接続されます。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションから監視したりバックアップしたりするのに、無差別ポートを使用できます。

関連トピック

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定，（2489 ページ）
プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定，（2491 ページ）
例：ホスト ポートとしてのインターフェイスの設定，（2497 ページ）

例：インターフェイスをプライベート VLAN 無差別ポートとして設定する，（2498 ページ）

ネットワーク内のプライベート VLAN

スイッチング環境では、個々のエンドステーションに、または共通グループのエンドステーションに、個別のプライベートVLANや、関連するIPサブネットを割り当てることができます。エンド ステーションはデフォルト ゲートウェイとの通信を行うだけで、プライベート VLAN の外部と通信することができます。

プライベート VLAN を使用し、次の方法でエンド ステーションへのアクセスを制御できます。

- エンド ステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ 2 の通信をしないようにします。たとえば、エンド ステーションがサーバの場合、この設定によりサーバ間のレイヤ 2 通信ができなくなります。
- デフォルト ゲートウェイおよび選択したエンド ステーション（バックアップ サーバなど）に接続されているインターフェイスを無差別ポートとして設定し、すべてのエンド ステーションがデフォルト ゲートウェイにアクセスできるようにします。

複数のデバイスにわたるようにプライベート VLAN を拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他のデバイスにトランキングします。使用するプライベート VLAN 設定のセキュリティを確保して、プライベート VLAN として設定された VLAN が他の目的に使用されないようにするには、プライベート VLAN ポートがないデバイスを含めて、すべての中間デバイスでプライベート VLAN を設定します。

プライベート VLAN での IP アドレッシング方式

各カスタマーに個別のVLANを割り当てると、次のようにIPアドレッシング方式が非効率的になります。

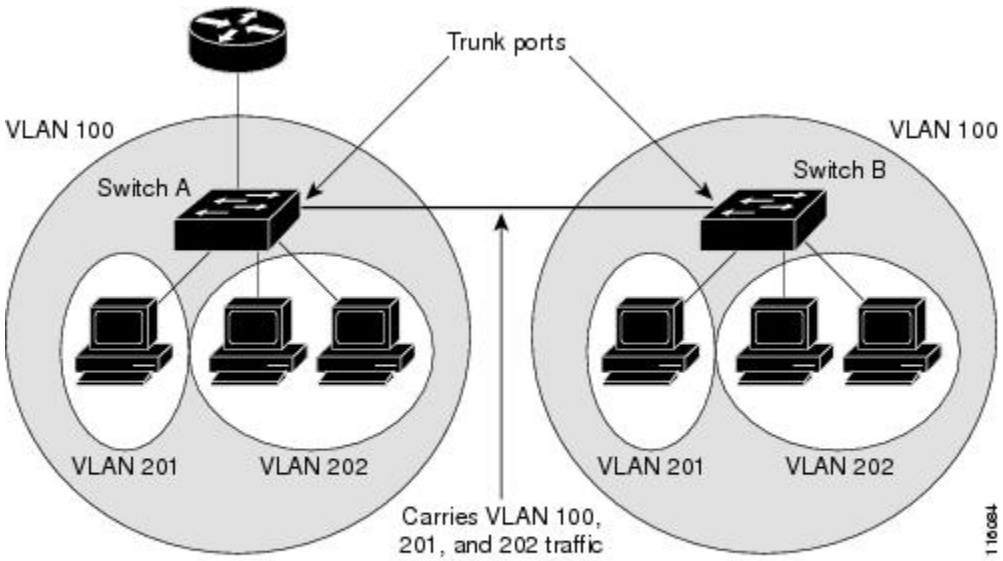
- カスタマー VLAN にアドレスのブロックを割り当てると、未使用 IP アドレスが発生することがあります。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベートVLANのすべてのメンバーが、プライマリ VLANに割り当てられている共通アドレス空間を共有するためです。ホストはセカンダリ VLANに接続され、プライマリ VLANに割り当てられているアドレスのブロックから IP アドレスが DHCP サーバによってホストに割り当てられますが、同一プライマリ VLAN内のセカンダリ VLANには割り当てられません。さまざまなセカンダリ VLAN のカスタマー デバイスには後続 IP アドレスが割り当てられます。新しいデバイスを追加すると、サブネットアドレスの巨大プールから次に使用できるアドレスが、DHCPサーバによって割り当てられます。

複数のスイッチにまたがるプライベート VLAN

通常の VLAN と同様に、プライベート VLAN を複数のスイッチにまたがるように設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN を隣接スイッチに伝送します。トランク ポートはプライベート VLAN を他の VLAN として扱います。複数のスイッチにまたがるプライベート VLAN の機能の特徴として、スイッチ A にある独立ポートからのトラフィックはスイッチ B に到達しません。

図 *100*：複数のスイッチにまたがるプライベート *VLAN*



VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community VLAN

プライベート VLAN は VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は VTP 3 のサーバ モードでもサポートされます。VTP 3 を使用して設定したサーバ クライアントがある場合、サーバに設定されているプライベート VLAN をクライアント上に反映させる必要があります。

プライベート VLAN の他機能との相互作用

プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック

通常の VLAN では、同じ VLAN にあるデバイスはレイヤ 2 レベルで互いに通信しますが、別の VLAN にあるインターフェイスに接続されたデバイスとはレイヤ 3 レベルで通信する必要があります。プライベート VLAN の場合、無差別ポートはプライマリ VLAN のメンバーであり、ホスト ポートはセカンダリ VLAN に属します。セカンダリ VLAN はプライマリ VLAN に対応付けられているため、これらの VLAN のメンバーはレイヤ 2 レベルで互いに通信できます。

通常の VLAN の場合、ブロードキャストはその VLAN のすべてのポートに転送されます。プライベート VLAN のブロードキャストの転送は、次のようにブロードキャストを送信するポートによって決まります。

- 独立ポートは、無差別ポートまたはトランク ポートだけにブロードキャストを送信します。
- コミュニティ ポートは、すべての無差別ポート、トランク ポート、同一コミュニティ VLAN のポートにブロードキャストを送信します。
- 無差別ポートは、プライベート VLAN のすべてのポート（その他の無差別ポート、トランク ポート、独立ポート、コミュニティ ポート）にブロードキャストを送信します。

マルチキャスト トラフィックのルーティングとブリッジングは、プライベート VLAN 境界を横断して行われ、単一コミュニティ VLAN 内でも行われます。マルチキャスト トラフィックは、同一独立 VLAN のポート間、または別々のセカンダリ VLAN のポート間で転送されません。

プライベート VLAN のマルチキャスト転送は次の状況をサポートします。

- 送信側が VLAN 外に存在する可能性があり、受信側が VLAN ドメイン内に存在している可能性がある。
- 送信側が VLAN 内に存在する可能性があり、受信側が VLAN ドメイン外に存在している可能性がある。
- 送信側と受信側が同一のコミュニティ VLAN に存在している可能性がある。

プライベート VLAN と SVI

レイヤ 3 スイッチスイッチでは、スイッチ仮想インターフェイス（SVI）が VLAN のレイヤ 3 インターフェイスを表します。レイヤ3デバイスは、セカンダリ VLAN ではなく、プライマリ VLAN だけを介してプライベート VLAN と通信します。レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。レイヤ 3 VLAN インターフェイスをセカンダリ VLAN 用に設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI はアクティブになりません。

- SVI がアクティブである VLAN をセカンダリ VLAN として設定する場合、SVI をディセーブルにしないと、この設定は許可されません。
- セカンダリ VLAN として設定されている VLAN に SVI を作成しようとしてセカンダリ VLAN がすでにレイヤ 3 にマッピングされている場合、SVI は作成されず、エラーが返されます。SVI がレイヤ 3 にマッピングされていない場合、SVI は作成されますが、自動的にシャットダウンされます。

プライマリ VLAN をセカンダリ VLAN と関連付けてマッピングすると、プライマリ VLAN の設定がセカンダリ VLAN の SVI に伝播されます。たとえば、プライマリ VLAN の SVI に IP サブネットを割り当てると、このサブネットは、プライベート VLAN 全体の IP サブネット アドレスになります。

プライベート VLAN とスイッチ スタック

プライベート VLAN はスイッチ スタック内で動作することができ、プライベート VLAN ポートはさまざまなスタック メンバーに存在することができます。ただし、スタックを次のように変更すると、プライベート VLAN の動作に影響が及ぶ可能性があります。

- スタックにプライベート VLAN 無差別ポートが 1 つだけ含まれ、このポートを含めたスタック メンバーがスタックから削除された場合、プライベート VLAN のホスト ポートとプライベート VLAN 外との接続が不能になります。
- スタック内にプライベート VLAN 無差別ポートが 1 つだけあるスタック マスターに障害が発生した場合、またはスタックを残し、新しいスタック マスターが選択された場合、古いスタック マスターに無差別ポートがあるプライベート VLAN のホスト ポートとプライベート VLAN 外との接続が不能になります。
- 2 つのスタックが統合された場合、権利を獲得したスタックのプライベート VLAN は影響を受けませんが、スイッチを再起動したときに、権利を獲得しなかったスイッチのプライベート VLAN 設定が失われます。

ダイナミック MAC アドレスを備えたプライベート VLAN

セカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN で複製されますが、その逆はありません。これにより、ハードウェアの L2 CAM スペースを節約できます。プライマリ VLAN は常に、両方向で正引きを実行するのに使用されます。

ダイナミック MAC アドレスは、プライベート VLAN のプライマリ VLAN で学習されると、必要に応じて、セカンダリ VLAN で複製されます。たとえば、MAC アドレスがセカンダリ VLAN で動的に受信されると、プライマリ VLAN の一部として学習されます。隔離 VLAN の場合、同じ MAC のブロックされたエントリは MAC アドレス テーブルのセカンダリ VLAN に追加されます。このため、セカンダリ ドメインのホスト ポートで学習された MAC は、ブロックされたタイプのエントリとしてインストールされます。プライマリ VLAN からトラフィックが入力される場合でも、すべての MAC エントリはセカンダリ VLAN で学習されます。

MAC アドレスがプライマリ VLAN で動的に学習される場合、関連セカンダリ VLAN では複製されません。

スタティック MAC アドレスのプライベート VLAN

ユーザは、従来型のようにプライベート VLAN のホストにスタティック MAC アドレス CLI を複製する必要はありません。

例：

- 従来のモデルでは、ユーザはスタティック MAC アドレスを設定すると、関連 VLAN 内にも同じスタティック MAC アドレスを追加する必要がありました。たとえば、MAC アドレス A が VLAN 101 のポート 1/0/1 でユーザ設定され、VLAN 101 ではセカンダリ VLAN で、VLAN 100 がプライマリ VLAN である場合は、ユーザは設定する必要があります。

```
mac-address static A vlan 101 interface G1/0/1
mac-address static A vlan 100 interface G1/0/1
```

- このスイッチでは、ユーザは関連 VLAN に MAC アドレスを複製する必要はありません。上記の例のみで、ユーザは設定する必要があります。

```
mac-address static A vlan 101 interface G1/0/1
```

プライベート VLAN と VACL/QOS との相互作用

プライベート VLAN は、このスイッチの場合、他のプラットフォームの「単方向」と比べ、双方向です。

レイヤ 2 の正引き後には、適切な出力 VLAN マッピングが行われ、すべての出力 VLAN ベースの機能による処理が出力 VLAN のコンテキストで実行されます。

レイヤ 2 のフレームがプライベート VLAN 内で転送されると、入力側と出力側とで VLAN マップが適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。同様に、フレームが外部ポートからプライベート VLAN にルーティングされると、プライベート VLAN は出力側に適用されます。これは、ブリッジされたトラフィックとルーティングされたトラフィックの両方に適用されます。

ブリッジング：

- セカンダリ VLAN からプライマリ VLAN へのアップストリーム トラフィックの場合、セカンダリ VLAN の MAP は入力側に適用され、プライマリ VLAN の MAP は出力側に適用されます。
- プライマリ VLAN からセカンダリ VLAN へのダウンストリーム トラフィックの場合は、プライマリ VLAN の MAP は入力方向で適用され、セカンダリ VLAN の MAP は出力方向で適用されます。

ルーティング

プライベート VLAN ドメインが 2 つ（PV1（sec1、prim1）および PV2（sec2、prim2））ある場合を想定します。PV1 から PV2 にルーティングされるフレームについては次のようになります。

- sec1 の MAP および prim1 の L3 ACL は、入力ポートに適用されます。
- sec2 の MAP および prim2 の L3 ACL は、出力ポートに適用されます。

分離されたホスト ポートから無差別ポートへのアップストリームまたはダウンストリームに従うパケットの場合、分離された VLAN の VACL は入力方向に適用され、プライマリ VLAN の VACL は出力方向に適用されます。これにより、ユーザは同じプライマリ VLAN ドメインの別のセカンダリ VLAN に異なる VACL を設定することができます。

（注） このスイッチでのプライベート VLAN は常に双方向であるため、双方向のコミュニティ VLAN は不要です。

プライベート VLAN および HA サポート

PVLANは、高可用性（HA）機能とシームレスに連携します。スイッチオーバーの前に、マスターにあるプライベート VLAN は、スイッチオーバー後と同じである必要があります（新しいマスターは IOS 側および、FED 側両方で以前のマスターと同様の PVLAN 設定が必要です）。

プライベート VLAN 設定時の注意事項

プライベート VLAN のデフォルト設定

プライベート VLAN は設定されていません。

セカンダリ VLAN およびプライマリ VLAN の設定

プライベート VLAN の設定時は、次の注意事項に従ってください。

- プライベート VLAN は VTP 1、2、および 3 のトランスペアレント モードでサポートされます。スイッチで VTP バージョン 1 または 2 が稼働している場合は、VTP をトランスペアレント モードに設定する必要があります。プライベート VLAN を設定した後で、VTP モードをクライアントまたはサーバに変更できません。VTP バージョン 3 は、すべてのモードでプライベート VLAN をサポートします。
- VTP バージョン 1 または 2 でプライベート VLAN を設定した後、**copy running-config startup config** 特権 EXEC コマンドを使用して、VTP トランスペアレント モード設定とプライベート VLAN 設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存します。保存しないと、スイッチをリセットした場合、デフォルトの VTP サーバ モードになり、プライベート VLAN をサポートしなくなります。VTP バージョン 3 ではプライベート VLAN をサポートします。
- VTP バージョン 1 および 2 では、プライベート VLAN 設定の伝播は行われません。プライベートVLANポートが必要なデバイスでVTPバージョン3が実行されていない場合は、VTP3はプライベート VLAN を伝播するため、そのデバイス上でプライベート VLAN を設定する必要があります。
- VLAN 1 または VLAN 1002 ～ 1005 をプライマリ VLAN またはセカンダリ VLAN として設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）はプライベート VLAN に属することができます。
- プライマリ VLAN には、1 つの独立 VLAN および複数のコミュニティ VLAN を関連付けることができます。独立 VLAN またはコミュニティ VLAN には、1 つのプライマリ VLAN だけを関連付けることができます。
- プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行可能なスパニングツリー プロトコル（STP）インスタンスは 1 つだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。

- TFTP サーバから PVLAN 設定をコピーし、それを実行中の設定に適用しても、PVLAN の関連付けは形成されません。プライマリ VLAN がすべてのセカンダリ VLAN に確実に関連付けられていることを確認する必要があります。

  また、**copy flash:config_file running-config** の代わりに **configure replace flash:config_file force** も使用できます。

- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、DHCP スヌーピングはセカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定しても、プライマリ VLAN をすでに設定している場合、DHCP 設定は有効になりません。

- プライベート VLAN ポートで IP ソース ガードをイネーブルにする場合は、プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。

- プライベート VLAN でトラフィックを伝送しないデバイスのトランクから、プライベート VLAN をプルーニングすることを推奨します。

- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の Quality of Service（QoS）設定を適用できます

- sticky ARP には、次の考慮事項があります。

  - sticky ARP エントリとは、SVI およびレイヤ 3 インターフェイス上で学習されるエントリです。これらのエントリは、期限切れになることはありません。

  - **ip sticky-arp** グローバル コンフィギュレーション コマンドは、プライベート VLAN に属する SVI でだけサポートされます。

  - **ip sticky-arp** インターフェイス コンフィギュレーション コマンドは、以下でのみサポートされます。

    - レイヤ 3 インターフェイス

    - 標準 VLAN に属する SVI

    - プライベート VLAN に属する SVI

    ip sticky-arp グローバル コンフィギュレーション コマンドおよび **ip sticky-arp インターフェイス** コンフィギュレーション コマンドの使用の詳細については、このリリースのコマンド リファレンスを参照してください。

- プライマリ VLAN およびセカンダリ VLAN で VLAN マップを設定できますただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。

- PVLAN は双方向です。これらは、入力側と出力側の両方に適用されます。

  レイヤ 2 のフレームがプライベート VLAN 内で転送されると、入力側と出力側で VLAN マップが適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。同様に、フレームが外部ポートからプライベート VLAN にルーティングされると、プライベート VLAN は出力側に適用されます。

ブリッジング

- セカンダリ VLAN からプライマリ VLAN へのアップストリーム トラフィックの場合、セカンダリ VLAN の MAP は入力側に適用され、プライマリ VLAN の MAP は出力側に適用されます。
- プライマリ VLAN からセカンダリ VLAN へのダウンストリーム トラフィックの場合は、プライマリ VLAN の MAP は入力方向で適用され、セカンダリ VLAN のMAP は出力方向で適用されます。

ルーティング

プライベート VLAN ドメインが 2 つ（PV1（sec1、prim1）および PV2（sec2、prim2））ある場合を想定します。PV1 から PV2 にルーティングされるフレームについては次のようになります。

- sec1 の MAP および prim1 の L3 ACL は入力ポートに適用されます。
- sec1 の MAP および prim2 の L3 ACL は出力ポートに適用されます。
- 分離されたホスト ポートから無差別ポートへのアップストリームまたはダウンストリームに従うパケットの場合、分離された VLAN の VACL は入力方向に適用され、プライマリ VLAN の VACL は出力方向に適用されます。これにより、ユーザは同じプライマリ VLAN ドメインの別のセカンダリ VLAN に異なる VACL を設定することができます。

プライベート VLAN の特定 IP トラフィックをフィルタリングするには、プライマリ VLAN およびセカンダリ VLAN の両方に VLAN マップを適用する必要があります。

- プライマリ VLAN SVI にだけルータ ACL を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。
- プライベート VLAN がレイヤ 2 でホストを分離していても、ホストはレイヤ 3 で互いに通信できます。
- プライベート VLAN では、次のスイッチド ポート アナライザ（SPAN）機能がサポートされます。
  - プライベート VLAN を SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN ベースの SPAN（VSPAN）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別に監視することができます。

プライベート VLAN ポートの設定

プライベート VLAN ポートの設定時は、次の注意事項に従ってください。

- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てるには、プライベート VLAN コンフィギュレーション コマンドだけを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定する VLAN に割り当てられているレイ

ヤ 2 アクセス ポートは、この VLAN がプライベート VLAN の設定に含まれている場合、非アクティブです。レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。

- PAgP または LACP EtherChannel に属するポートを、プライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN の設定に含まれている間は、そのポートの EtherChannel 設定はいずれも非アクティブです。
- 設定ミスによる STP ループの発生を防ぎ、STP コンバージェンスを高速化するには、独立ホスト ポートおよびコミュニティ ホスト ポート上で PortFast および BPDU ガードをイネーブルにしますイネーブルの場合、STP はすべての PortFast が設定されたレイヤ 2 LAN ポートに BPDU ガード機能を適用します。PortFast および BPDU ガードを無差別ポートでイネーブルにしないでください。
- プライベート VLAN の設定で使用される VLAN を削除すると、この VLAN に関連付けられたプライベート VLAN ポートが非アクティブになります。
- ネットワーク デバイスをトランク接続し、プライマリ VLAN およびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートはさまざまなネットワーク デバイス上で使用できます。

プライベート VLAN の設定方法

プライベート VLAN の設定

プライベート VLAN を設定するには、次の手順を実行します。

（注） プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は、VTP 3 のサーバ モードでもサポートされます。

手順の概要

1. VTP モードを **トランスペアレント** に設定します。
2. プライマリおよびセカンダリ VLAN を作成してこれらを対応付けします。
3. インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバーシップを割り当てます。
4. インターフェイスを無差別ポートとして設定し、無差別ポートをプライマリおよびセカンダリ VLAN のペアにマッピングします。
5. VLAN 間ルーティングを使用している場合、プライマリ SVI を設定し、セカンダリ VLAN をプライマリ SVI にマッピングします。
6. プライマリ VLAN 設定を確認します。

手順の詳細

ステップ 1 VTP モードを **トランスペアレント** に設定します。

（注） 注：VTP3 の場合、サーバまたはトランスペアレント モードのいずれにもモードを設定できます。

ステップ 2 プライマリおよびセカンダリ VLAN を作成してこれらを対応付けします。

See the プライベート VLAN 内の VLAN の設定および対応付け，（2485 ページ）

（注） VLAN がまだ作成されていない場合、プライベート VLAN 設定プロセスでこれを作成します。

ステップ 3 インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバーシップを割り当てます。

See the プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定，（2489 ページ）

ステップ 4 インターフェイスを無差別ポートとして設定し、無差別ポートをプライマリおよびセカンダリ VLAN のペアにマッピングします。

See the プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定，（2491 ページ）

ステップ 5 VLAN 間ルーティングを使用している場合、プライマリ SVI を設定し、セカンダリ VLAN をプライマリ SVI にマッピングします。

See the セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング，（2494 ページ）

ステップ 6 プライマリ VLAN 設定を確認します。

プライベート VLAN 内の VLAN の設定および対応付け

private-vlan コマンドは VLAN コンフィギュレーション モードを終了するまで機能しません。

プライベート VLAN 内で VLAN を設定し、関連付けるには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vtp mode transparent**
4. **vlan***vlan-id*
5. **private-vlan primary**
6. **exit**
7. **vlan***vlan-id*
8. **private-vlan isolated**
9. **exit**
10. **vlan***vlan-id*
11. **private-vlan community**
12. **exit**
13. **vlan***vlan-id*
14. **private-vlan community**
15. **exit**
16. **vlan***vlan-id*
17. **private-vlan association** [**add** | **remove**] *secondary_vlan_list*
18. **end**
19. **show vlan private-vlan** [**type**] または **show interfaces status**
20. **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp mode transparent** 例： `スイッチ(config)# vtp mode`	VTP モードをトランスペアレントに設定します（VTP をディセーブルにします）。 （注） VTP3 の場合、サーバまたはトランスペアレントモードのいずれにもモードを設定できます。

	コマンドまたはアクション	目的
	transport	
ステップ 4	**vlan***vlan-id* 例： スイッチ(config)# **vlan 20**	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 5	**private-vlan primary** 例： スイッチ(config-vlan)# **private-vlan primary**	VLAN をプライマリ VLAN として指定します。
ステップ 6	**exit** 例： スイッチ(config-vlan)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**vlan***vlan-id* 例： スイッチ(config)# **vlan 501**	（任意）VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 8	**private-vlan isolated** 例： スイッチ(config-vlan)# **private-vlan isolated**	VLAN を独立 VLAN として指定します。
ステップ 9	**exit** 例： スイッチ(config-vlan)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**vlan***vlan-id* 例： スイッチ(config)# **vlan 502**	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。

	コマンドまたはアクション	目的
ステップ 11	**private-vlan community** 例： スイッチ(config-vlan)# **private-vlan community**	VLAN をコミュニティ VLAN として指定します。
ステップ 12	**exit** 例： スイッチ(config-vlan)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**vlan***vlan-id* 例： スイッチ(config)# **vlan 503**	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 14	**private-vlan community** 例： スイッチ(config-vlan)# **private-vlan community**	VLAN をコミュニティ VLAN として指定します。
ステップ 15	**exit** 例： スイッチ(config-vlan)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**vlan***vlan-id* 例： スイッチ(config)# **vlan 20**	ステップ 4 で指定したプライマリ VLAN に関して VLAN コンフィギュレーション モードを開始します。
ステップ 17	**private-vlan association** [**add** | **remove**] *secondary_vlan_list* 例： スイッチ(config-vlan)# **private-vlan association 501-503**	セカンダリ VLAN をプライマリ VLAN に関連付けます。単一のプライベート VLAN ID でも、またはハイフンで連結したプライベート VLAN ID でもかまいません。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。

	コマンドまたはアクション	目的
		• *secondary_vlan_list* パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。 • *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN を関連付けます。 • セカンダリ VLAN とプライマリ VLAN 間の関連付けをクリアするには、*secondary_vlan_list* に **remove** キーワードを使用します。 • このコマンドは、VLAN コンフィギュレーションモードを終了するまで機能しません。
ステップ 18	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 19	**show vlan private-vlan** [**type**] または **show interfaces status** 例： `スイッチ# show vlan private-vlan`	設定を確認します。
ステップ 20	**copy running-config startup config** 例： `スイッチ# copy running-config startup-config`	スイッチ スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN ホスト ポートとして設定し、これをプライマリおよびセカンダリ VLAN に関連付けるには、次の手順を実行します。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode private-vlan host**
5. **switchport private-vlan host-association***primary_vlan_id secondary_vlan_id*
6. **end**
7. **show interfaces** [*interface-id*] **switchport**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/22**	設定するレイヤ 2 インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode private-vlan host** 例： スイッチ(config-if)# **switchport mode private-vlan host**	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 5	**switchport private-vlan host-association***primary_vlan_id secondary_vlan_id* 例： スイッチ(config-if)# **switchport private-vlan**	レイヤ 2 ポートをプライベート VLAN と関連付けます。 （注） これは、レイヤ 2 インターフェイスに PVLAN を関連付けるために必要な手順です。

	コマンドまたはアクション	目的
	`host-association 20 501`	
ステップ 6	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `スイッチ# show interfaces gigabitethernet1/0/22 switchport`	設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

プライベート VLAN ポート，（2474 ページ）
例：ホスト ポートとしてのインターフェイスの設定，（2497 ページ）
例：インターフェイスをプライベート VLAN 無差別ポートとして設定する，（2498 ページ）

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN 無差別ポートとして設定し、これをプライマリおよびセカンダリ VLAN にマッピングするには、次の手順を実行します。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode private-vlan promiscuous**
5. **switchport private-vlan mapping***primary_vlan_id* {**add** | **remove**} *secondary_vlan_list*
6. **end**
7. **show interfaces** [*interface-id*] **switchport**
8. **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： スイッチ(config)# **interface gigabitethernet1/0/2**	設定するレイヤ2インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode private-vlan promiscuous** 例： スイッチ(config-if)# **switchport mode private-vlan promiscuous**	レイヤ 2 ポートをプライベート VLAN 無差別ポートとして設定します。
ステップ 5	**switchport private-vlan mapping***primary_vlan_id* {**add**	**remove**} *secondary_vlan_list*	プライベート VLAN 無差別ポートをプライマリ VLAN、および選択したセカンダリ VLAN にマッピングします。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含める

	コマンドまたはアクション	目的
	例： スイッチ(config-if)# **switchport private-vlan mapping 20 add 501-503**	ことができます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。 • セカンダリ VLAN とプライマリ VLAN をプライベート VLAN 無差別ポートにマッピングするには、*secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用します。 • セカンダリ VLAN とプライベート VLAN 無差別ポートのマッピングを解除するには、**remove** キーワードを指定した *secondary_vlan_list* を使用します。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： スイッチ# **show interfaces gigabitethernet1/0/2 switchport**	設定を確認します。
ステップ 8	**copy running-config startup config** 例： スイッチ# **copy running-config startup-config**	スイッチ スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

関連トピック

プライベート VLAN ポート，（2474 ページ）
例：ホスト ポートとしてのインターフェイスの設定，（2497 ページ）
例：インターフェイスをプライベート VLAN 無差別ポートとして設定する，（2498 ページ）

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング

プライベート VLAN が VLAN 間ルーティングに使用される場合、SVI をプライマリ VLAN に設定してセカンダリ VLAN を SVI にマッピングできます。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

セカンダリ VLAN をプライマリ VLAN の SVI にマッピングしてプライベート VLAN トラフィックのレイヤ 3 スイッチングを可能にするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface vlan***primary_vlan_id*
4. **private-vlan mapping** [**add** | **remove**] *secondary_vlan_list*
5. **end**
6. **show interface private-vlan mapping**
7. **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface vlan***primary_vlan_id* 例： `スイッチ(config)# interface vlan 20`	プライマリ VLAN でインターフェイス コンフィギュレーション モードを開始して、VLAN を SVI として設定します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。

	コマンドまたはアクション	目的
ステップ 4	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list* 例： `スイッチ(config-if)# private-vlan mapping 501-503`	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。 （注） **private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされているプライベート VLAN トラフィックにだけ影響を与えます。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。 • *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN をプライマリ VLAN にマッピングします。 • **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN のマッピングを解除します。
ステップ 5	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interface private-vlan mapping** 例： `スイッチ# show interfaces private-vlan mapping`	設定を確認します。
ステップ 7	**copy running-config startup config** 例： `スイッチ# copy running-config startup-config`	スイッチ スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

関連トピック

VTP Domain, （2373 ページ）

Secondary VLANs, （2474 ページ）

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする, （2498 ページ）

プライベート VLAN のモニタ

次の表に、プライベート VLAN をモニタするために使用するコマンドを記載します。

表 *180*：プライベート *VLAN* モニタリング コマンド

コマンド	目的
show interfaces status	所属する VLAN を含む、インターフェイスのステータスを表示します。
show vlan private-vlan [**type**]	スイッチまたはスイッチ スタックのプライベート VLAN 情報を表示します。
show interface switchport	インターフェイス上のプライベート VLAN 設定を表示します。
show interface private-vlan mapping	VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。
show platform vlan pvlan	FED 側の PVLAN 情報を表示します。
show platform vlan pvlan hardware	FED 側の PVLAN で保持されているすべてのハードウェア リソースを表示します。

プライベート VLAN の設定例

例：プライベート VLAN 内の VLAN の設定および関連付け

次に、VLAN 20 をプライマリ VLAN、VLAN 501 を独立 VLAN、VLAN 502 および 503 をコミュニティ VLAN として設定し、これらをプライベート VLAN 内で関連付けして、設定を確認する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# vlan 20
スイッチ(config-vlan)# private-vlan primary
スイッチ(config-vlan)# exit
スイッチ(config)# vlan 501
スイッチ(config-vlan)# private-vlan isolated
スイッチ(config-vlan)# exit
```

```
スイッチ(config)# vlan 502
スイッチ(config-vlan)# private-vlan community
スイッチ(config-vlan)# exit
スイッチ(config)# vlan 503
スイッチ(config-vlan)# private-vlan community
スイッチ(config-vlan)# exit
スイッチ(config)# vlan 20
スイッチ(config-vlan)# private-vlan association 501-503
スイッチ(config-vlan)# end
スイッチ# show vlan private-vlan
Primary   Secondary      Type
--------- -------------- -----------------
20        501            isolated
20        502            community
20        503            community
```

例：ホスト ポートとしてのインターフェイスの設定

次に、インターフェイスをプライベート VLAN ホスト ポートとして設定し、それをプライベート VLAN ペアに関連付けて、その設定を確認する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# interface gigabitethernet1/0/22
スイッチ(config-if)# switchport mode private-vlan host
スイッチ(config-if)# switchport private-vlan host-association 20 501
スイッチ(config-if)# end
スイッチ# show interfaces gigabitethernet1/0/22 switchport
Name: Gi1/0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 501
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 501

<output truncated>
```

関連トピック

プライベート VLAN ポート，（2474 ページ）

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定，（2489 ページ）

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定，（2491 ページ）

例：インターフェイスをプライベート VLAN 無差別ポートとして設定する

次の例では、インターフェイスをプライベート VLAN 無差別ポートとして設定し、それをプライベート VLAN にマッピングする方法を示します。インターフェイスは、プライマリ VLAN 20 のメンバで、セカンダリ VLAN 501 ～ 503 がマッピングされます。

```
スイッチ# configure terminal
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# switchport mode private-vlan promiscous
スイッチ(config-if)# switchport private-vlan mapping 20 add 501-503
スイッチ(config-if)# end
```

show vlan private-vlan または **show interface status** 特権 EXEC コマンドを使用してプライマリおよびセカンダリ VLAN とスイッチ上のプライベート VLAN ポートを表示します。

関連トピック

プライベート VLAN ポート, （2474 ページ）

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定, （2489 ページ）

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定, （2491 ページ）

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする

次に、VLAN 501 および 502 のインターフェイスをプライマリ VLAN 10 にマッピングする例を示します。これにより、プライベート VLAN 501 および 502 からのセカンダリ VLAN 入力トラフィックのルーティングが可能になります。

```
スイッチ# configure terminal
スイッチ(config)# interface vlan 20
スイッチ(config-if)# private-vlan mapping 501-503
スイッチ(config-if)# end
スイッチ# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan20    501            isolated
vlan20    502            community
vlan20    503            community
```

関連トピック

VTP Domain, （2373 ページ）

Secondary VLANs, （2474 ページ）

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング, （2494 ページ）

例：プライベート VLAN のモニタリング

次に、**show vlan private-vlan** コマンドの出力例を示します。

```
スイッチ# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated          Gi1/0/22, Gi1/0/2
20      502       community         Gi1/0/2
20      503       community         Gi1/0/2
```

次の作業

次の設定を行えます。

- VTP
- VLANs
- VLAN トランキング
- VLAN メンバーシップ ポリシー サーバ（VMPS）
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CLI コマンド	LAN Switching Command Reference, Cisco IOS Release

標準および RFC

標準/RFC	タイトル
RFC 1573	
RFC 1757	
RFC 2021	

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB • BRIDGE-MIB（RFC1493） • CISCO-BRIDGE-EXT-MIB • CISCO-CDP-MIB • CISCO-PAGP-MIB • CISCO-PRIVATE-VLAN-MIB • CISCO-LAG-MIB • CISCO-L2L3-INTERFACE-CONFIG-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • IEEE8023-LAG-MIB • IF-MIB（RFC 1573） • RMON-MIB（RFC 1757） • RMON2-MIB（RFC 2021）	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

第 XVII 部

WLAN

- WLAN の設定，2505 ページ
- DHCP for WLANs の設定，2525 ページ
- WLAN セキュリティの設定，2537 ページ
- WLAN ごとのクライアント カウントの設定，2547 ページ
- 802.11w の設定，2555 ページ
- Wi-Fi Direct クライアント ポリシーの設定，2565 ページ
- 802.11r BSS の高速移行の設定，2571 ページ
- 経由ローミングの設定，2587 ページ
- アクセス ポイント グループの設定，2595 ページ

第 110 章

WLAN の設定

- 機能情報の確認，2505 ページ
- WLAN の前提条件，2505 ページ
- WLAN の制約事項，2506 ページ
- WLAN について，2507 ページ
- WLAN の設定方法，2512 ページ
- WLAN プロパティの監視（CLI），2522 ページ
- 次の作業，2522 ページ
- その他の参考資料，2522 ページ
- WLANs の機能情報，2524 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

WLAN の前提条件

- 最大 16 個の WLAN を各アクセス ポイント グループにアソシエートし、各グループに個々のアクセス ポイントを割り当てることができます。各アクセス ポイントは、有効化されて

いる WLAN のうち、そのアクセス ポイント グループに属する WLAN だけをアドバタイズします。アクセス ポイント グループで無効化されている WLAN または別のグループに属する WLAN はアドバタイズしません。

- スイッチが VLAN トラフィックを正常にルーティングできるように、WLAN と管理インターフェイスにはそれぞれ別の VLAN を割り当てることをお勧めします。

関連トピック

WLAN の作成（CLI），（2512 ページ）
WLAN の作成（GUI）
汎用 WLAN プロパティの設定（CLI），（2516 ページ）
WLAN の削除（CLI），（2513 ページ）
高度な WLAN プロパティの設定（CLI），（2519 ページ）
バンドの選択，（2508 ページ）
オフチャネル スキャンの延期
DTIM 周期
Session Timeout
Cisco Client Extensions，（2510 ページ）
ピアツーピア ブロッキング，（2510 ページ）
診断チャネル
WLAN ごとのクライアント カウント
WLAN のイネーブル化（CLI），（2514 ページ）
WLAN のディセーブル（CLI），（2515 ページ）

WLAN の制約事項

- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- 最大 1000 台のクライアントを設定できます。
- WLAN 名と SSID は 32 文字以内にする必要があります。スペースは WLAN プロファイル名と SSID では許可されません。WLAN 名はキーワードにすることができません。たとえば、**wlan s** というコマンドを入力して、「s」という名前で WLAN を作成すると、「s」はシャットダウン用のキーワードとして使用されているため、すべての WLAN がシャットダウンします。
- WLAN から VLAN0 へのマッピング、VLAN 1002～1006 のマッピングはできません。
- 固定 IPv4 アドレスのデュアル スタック クライアントはサポートされません。
- 同じ SSID を持つ WLAN を作成するときには、各 WLAN に対して一意のプロファイル名を作成する必要があります。

- 同じ SSID を持つ複数の WLAN を同じ AP 無線に割り当てる場合は、クライアントがその中から安全に選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。
- WLAN がローカル スイッチングの場合、AVC が有効化されているローカル スイッチング WLAN にクライアントをアソシエイトします。AVC の統計 90 秒後を確認した時、クライアントからトラフィックを送信します。Cisco WLC はトップ アプリケーション下では表示されますが、クライアントには表示されません。タイマーの問題があるため、CiscoWLC の最初のスロットはクライアントの統計が表示されないことがあります。以前に 1 秒のみのクライアントの統計が、AP および WLC のタイマーが 89 秒でオフになっている時に見られました。現在統計の削除は 180 秒後であるため、91 秒から 179 秒までのクライアントの統計情報が表示されます。これは、各クライアントあたり 2 つのコピーの統計がメモリの制約で 5500 に保持することができないために起こります。

注意 一部のクライアントが複数のセキュリティ ポリシーで同じ SSID を検出すると WLAN に正しく接続できない場合があります。この機能を使用する際は、十分注意してください。

関連トピック

WLAN の作成（CLI），（2512 ページ）
WLAN の作成（GUI）
汎用 WLAN プロパティの設定（CLI），（2516 ページ）
WLAN の削除（CLI），（2513 ページ）
高度な WLAN プロパティの設定（CLI），（2519 ページ）
バンドの選択，（2508 ページ）
オフチャネル スキャンの延期
DTIM 周期
Session Timeout
Cisco Client Extensions，（2510 ページ）
ピアツーピア ブロッキング，（2510 ページ）
診断チャネル
WLAN ごとのクライアント カウント
WLAN のイネーブル化（CLI），（2514 ページ）
WLAN のディセーブル（CLI），（2515 ページ）

WLAN について

この機能により、Lightweight アクセス ポイント全体に対して、最大 64 の WLAN を制御できます。各 WLAN には識別子である WLAN ID、プロファイル名、および WLAN SSID があります。すべてのスイッチは接続している各アクセス ポイントに対して最大 16 の WLAN を公開します

が、管理しやすくするため、サポートされる最大数の WLAN を作成し、これらの WLAN を異なるアクセスポイントに選択的に公開する（アクセス ポイント グループを使用）ことができます。

異なる SSID または同じ SSID で WLAN を設定できます。SSID は、スイッチがアクセスする必要がある特定の無線ネットワークを識別します。

バンドの選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、混雑の少ない 5 GHz アクセス ポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセス ポイントからの同一チャネル干渉も発生します。802.11b/g では、重複しないチャネルが 3 つしかないからです。このような原因による干渉を防ぎ、ネットワーク全体のパフォーマンスを向上させるには、スイッチで帯域選択を設定します。

帯域選択のしくみは、クライアントへのプローブ応答を規制するというものです。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。

関連トピック

高度な WLAN プロパティの設定（CLI），（2519 ページ）

WLAN の前提条件，（2505 ページ）

WLAN の制約事項，（2506 ページ）

オフチャネル スキャンの延期

特定の省電力モードのクライアントが展開される環境で、小容量クライアント（たとえば、省電力モードを使用し定期的にテレメトリ情報を送信する医療用デバイス）からの重要情報の欠落を防ぐために、場合によっては、無線リソース管理（RRM）の正常なオフチャネル スキャンを延期する必要があります。この機能は、Quality of Service（QoS）と RRM スキャン延期機能との相互作用の方法を向上させます。

クライアントの Wi-Fi マルチメディア（WMM）UP マーキングを使用して、UP がマークされたパケットを受信した場合に、設定可能な期間中オフチャネル スキャンを延期するアクセスポイントを設定することができます。

[Off-Channel Scanning Defer] は、ノイズや干渉など代替チャネル選択に関する情報を収集する RRM を使用するときに重要となります。また、[Off-Channel Scanning Defer] は、不正検出を行います。[Off-Channel Scanning Defer] を提供する必要があるデバイスは、可能な限り、同じ WLAN を使用する必要があります。このようなデバイスが多くある場合（この機能を使用して Off-Channel Defer スキャンが完全に無効化されている可能性があります）、モニタ アクセス ポイントや、この WLAN が割り当てられていない同じ位置にあるその他のアクセスポイントなど、代わりにローカル AP で [Off-Channel Scanning Defer] を実装する必要があります。

QoS ポリシー（Bronze、Silver、Gold、Platinum）を WLAN に割り当てることで、クライアントからアップリンクでどのように受信されたかに関係なく、パケットがアクセス ポイントからのダウ

ンリンク接続でどのようにマーキングされるかを制御できます。UP=1,2 は最低の優先順位で、UP=0,3 はその次に高い優先順位です。各 QoS ポリシーのマーキング結果は次のとおりです。

- ブロンズは、すべてのダウンリンク トラフィックを UP= 1 にマーキングします。
- シルバーは、すべてのダウンリンク トラフィックを UP=0 にマーキングします。
- ゴールドは、すべてのダウンリンク トラフィックを UP= 4 にマーキングします。
- プラチナは、すべてのダウンリンク トラフィックを UP= 6 にマーキングします。

DTIM Period

802.11 ネットワークでは、Lightweight アクセス ポイントは、Delivery Traffic Indication Map (DTIM) と一致するビーコンを定期的に送信します。アクセス ポイントでビーコンがブロードキャストされると、DTIM period で設定した値に基づいて、バッファされたブロードキャスト フレームおよびマルチキャスト フレームが送信されます。この機能により、ブロードキャストデータやマルチキャスト データが予想されると、適切なタイミングで省電力クライアントを再起動できます。

通常、DTIM の値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）または 2（ビーコン 1 回おきに送信）のいずれかに設定されます。たとえば、802.11 ネットワークのビーコン間隔が 100 ミリ秒で DTIM 値が 1 に設定されている場合、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 10 回送信します。ビーコン期間が 100ms で DTIM 値が 2 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 5 回送信します。これらの設定はいずれも、ブロードキャストフレームおよびマルチキャストフレームの頻度を想定する、Voice over IP（VoIP）を含むアプリケーションに適しています。

ただし、DTIM 値は、802.11 のすべてのクライアントで省電力モードがイネーブルである場合、255 まで設定できます（255 回のビーコンごとにブロードキャスト フレームおよびマルチキャスト フレームを送信します）。クライアントは DTIM 期間に達したときのみリッスンする必要があるため、ブロードキャストとマルチキャストをリッスンする頻度を少なく設定することで、結果的にバッテリー寿命を長くできます。たとえば、ビーコン期間が 100 ms、DTIM 値を 100 に設定すると、アクセスポイントは、バッファされたブロードキャストフレームおよびマルチキャストフレームを 10 秒ごとに 1 回送信します。このレートにより省電力クライアントで、ブロードキャストとマルチキャストをリッスンし、ウェイク アップするまでのスリープ状態が長くなり、バッテリ寿命を長くできます。

（注） ビーコン期間は、スイッチでミリ秒単位で指定され、ソフトウェアによって、802.11 の時間単位（TU）（1 TU = 1.024 ミリ秒）に、内部的に変換されます。Cisco の 802.11n アクセス ポイントでは、この値は直近の 17 TU の倍数に丸められます。たとえば、100 ミリ秒に設定されたビーコン間隔は 104 ミリ秒の実際のビーコン間隔の結果です。

多くのアプリケーションでは、ブロードキャストメッセージとマルチキャストメッセージとの間隔を長くすると、プロトコルとアプリケーションのパフォーマンスが低下します。このようなクライアントをサポートする 802.11 ネットワークでは、低い DTIM 値を推奨します。

セッション タイムアウト

WLAN にセッション タイムアウトを設定できます。セッション タイムアウトとは、クライアント セッションが再認証を要求することなくアクティブである最大時間を指します。

Cisco Client Extensions

Cisco Client Extensions（CCX）ソフトウェアは、サードパーティ製クライアント デバイスの製造業者およびベンダーに対してライセンスされます。これらのクライアント上の CCX コードにより、サードパーティ製クライアントデバイスは、シスコ製のアクセスポイントと無線で通信できるようになり、セキュリティの強化、パフォーマンスの向上、高速ローミング、電源管理などの、他のクライアント デバイスがサポートしていないシスコの機能もサポートできるようになります。

- ソフトウェアは、CCX バージョン 1 ～ 5 をサポートします。これによって、スイッチとそのアクセス ポイントは、CCX をサポートするサードパーティ製クライアント デバイスと無線で通信できます。CCX サポートは、スイッチ上の各 WLAN に対して自動的に有効になり、無効にすることはできません。ただし、Aironet Information Element（IE）を設定できます。
- Aironet IE のサポートが有効になっている場合、アクセス ポイントは、Aironet IE 0x85（アクセス ポイント名、ロード、アソシエートされたクライアントの数などを含む）をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセス ポイントが再アソシエーション要求内の Aironet IE 0x85 を受信する場合、スイッチは、Aironet IEs 0x85 および 0x95（スイッチの管理 IP アドレスおよびアクセス ポイントの IP アドレスを含む）を再アソシエーション応答に格納して送信します。

関連トピック

高度な WLAN プロパティの設定（CLI），（2519 ページ）

WLAN の前提条件，（2505 ページ）

WLAN の制約事項，（2506 ページ）

ピアツーピア ブロッキング

ピアツーピア ブロッキングが個別の WLAN に対して適用され、各クライアントが、アソシエート先の WLAN のピアツーピア ブロッキング設定を継承します。ピア ツー ピアにより、トラフィックをリダイレクトする方法を制御できます。たとえば、トラフィックがスイッチ内でローカルにブリッジされたり、スイッチによってドロップされたり、またはアップストリーム VLAN へ転送されるように選択することができます。

ローカル スイッチングの WLAN にアソシエートされたクライアントに対して、ピアツーピアブロッキングがサポートされます。

関連トピック

高度な WLAN プロパティの設定（CLI），（2519 ページ）

WLAN の前提条件, （2505 ページ）
WLAN の制約事項, （2506 ページ）

診断チャネル

クライアントのWLANによる通信で問題が生じる理由についてトラブルシューティングする診断チャネルを選択できます。クライアントで発生している問題を識別し、ネットワーク上でクライアントを動作させるための修正措置を講じるために、クライアントとアクセス ポイントをテストできます。診断チャネルを有効にするには、スイッチの GUI または CLI を使用します。また、診断テストを実行するには、スイッチの CLI を使用します。

（注） 診断チャネル機能は、管理インターフェイスを使用するアンカーされていない SSID に対してのみ有効にすることをお勧めします。CCX 診断機能は Cisco ADU カードを持つクライアントでのみテストされています。

WLAN ごとの RADIUS 送信元サポート

スイッチのダイナミック インターフェイスのいずれかを介してアクセス可能な VLAN 上に設定済みの RADIUS サーバが存在しない場合は、スイッチがその管理インターフェイスの IP アドレスから RADIUS トラフィックを送信します。RADIUS サーバがスイッチのダイナミック インターフェイスを介して到達可能な場合は、その特定の RADIUS サーバへの RADIUS 要求が対応するダイナミック インターフェイスを介してコントローラから取得されます。

デフォルトで、スイッチから取得された RADIUS パケットによって、そのパケットの 送信元 IP アドレス（トポロジに応じて管理またはダイナミック）に関係なく、NAS-IP-Address 属性が管理インターフェイスの IP アドレスの属性に設定されます。

WLAN 単位の RADIUS 送信元サポート（RADIUS サーバ上書きインターフェイス）が有効になっている場合は、NAS-IP-Address 属性がスイッチによって送信元のインターフェイスを反映するように上書きされます。また、それに応じて、RADIUS 属性が Identity に一致するように変更されます。この機能は、各 WLAN が別個のレイヤ 3 Identity を持つ可能性がある場合に、WLAN ごとの RADIUS トラフィックでスイッチを効果的に仮想化します。この機能は、ACS ネットワーク アクセス制限、およびネットワーク アクセス プロファイルと統合する展開に役立ちます。

WLAN をフィルタ処理するには、RFC 3580 で APMAC:SSID 形式に設定された callStationID を使用します。また、NAS-IP-Address 属性を使用することで、認証サーバ上のフィルタリングを WLAN ごとの送信元インターフェイス上にまで拡張できます。

アドレスの送信元として WLAN ごとの動的インターフェイスを用いる管理インターフェイスなどを使用するいくつかの WLAN および通常の RADIUS トラフィックの送信元と、WLAN ごとの RADIUS 送信元サポートを組み合わせることができます。

WLAN の設定方法

WLAN の作成（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name wlan-id* [*ssid*]
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name wlan-id* [*ssid*] 例： `スイッチ(config)# wlan mywlan 34 mywlan-ssid`	WLAN の名前と ID を指定します。 • *profile-name* に、プロファイル名を入力します。入力できる範囲は英数字で 1 ～ 32 文字です。 • *wlan-id*に、WLAN ID を入力します。範囲は 1 ～ 512 です。 • *ssid* では、この WLAN に対する Service Set Identifier (SSID) を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。 （注） WLAN はデフォルトでディセーブルにされています。
ステップ 3	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN の前提条件, （2505 ページ）
WLAN の制約事項, （2506 ページ）

WLAN の削除（CLI）

手順の概要

1. **configure terminal**
2. **nowlan***wlan name wlan id SSID*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**nowlan***wlan name wlan id SSID* 例： スイッチ(config)# **no wlan test2**	WLAN を削除します。引数は次のとおりです。 • *wlan-name*は WLAN プロファイル名です。 • *wlan-id*は、WLAN ID です。 • *ssid* は WLAN に設定された WLAN SSID 名前です。 （注） AP グループに属する WLAN を削除すると、WLAN は AP グループと AP の無線から削除されます。
ステップ 3	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN の前提条件, （2505 ページ）
WLAN の制約事項, （2506 ページ）

WLAN の検索（CLI）

手順の概要

1. **show wlan summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show wlan summary** 例： スイッチ# **show wlan summary**	デバイスに設定されているすべての WLAN のリストを表示します。出力内で WLAN を検索できます。

```
スイッチ# show wlan summary
Number of WLANs: 4

WLAN Profile Name                     SSID                                VLAN Status
-------------------------------------------------------------------------------------
1    test1                             test1-ssid                          137  UP
3    test2                             test2-ssid                          136  UP
2    test3                             test3-ssid                          1    UP
45   test4                             test4-ssid                          1    DOWN
```

WLAN を検索するときにワイルドカードを使用できます。例：。variable は、出力内の検索文字列です。

```
スイッチ# show wlan summary | include test-wlan-ssid
1    test-wlan                        test-wlan-ssid                       137   UP
```

WLAN のイネーブル化（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **no shutdown**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。

	コマンドまたはアクション	目的
ステップ 3	**no shutdown** 例： スイッチ(config-wlan)# **no shutdown**	WLAN をイネーブルにします。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN の前提条件, （2505 ページ）
WLAN の制約事項, （2506 ページ）

WLAN のディセーブル（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **end**
5. **show wlan summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： スイッチ(config-wlan)# **shutdown**	WLAN をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**show wlan summary** 例： スイッチ# **show wlan summary**	デバイスに設定されているすべての WLAN のリストを表示します。出力内で WLAN を検索できます。

関連トピック

WLAN の前提条件, （2505 ページ）
WLAN の制約事項, （2506 ページ）

汎用 WLAN プロパティの設定（CLI）

次のパラメータを設定できます。

- メディア ストリーム
- ブロードキャスト SSID
- コール スヌーピング
- 無線
- インターフェイス
- ステータス

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **broadcast-ssid**
5. **radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**}
6. **client vlan** *vlan-identifier*
7. **ip multicast vlan** *vlan-name*
8. **media-stream multicast-direct**
9. **call-snoop**
10. **no shutdown**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： スイッチ# **shutdown**	パラメータを設定する前に、WLAN をディセーブルにします。
ステップ 4	**broadcast-ssid** 例： スイッチ(config-wlan)# **broadcast-ssid**	この WLAN の SSID をブロードキャストします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 5	**radio** {**all**	**dot11a**	**dot11ag**	**dot11bg**	**dot11g**} 例： スイッチ# **radio all**	WLAN で無線をイネーブルにします。キーワードは次のとおりです。 • **all**：すべての無線帯域で WLAN を設定します。 • **dot1a**：802.11a の無線帯域でのみ WLAN を設定します。 • **dot11g**：802.11ag の無線帯域でのみ WLAN を設定します。

	コマンドまたはアクション	目的
		• **dot11bg**：802.11b/g の無線帯域でのみ WLAN を設定します（802.11g が無効の場合、802.11b のみ）。 • **dot11ag**：802.11g の無線帯域でのみワイヤレス LAN を設定します。
ステップ 6	**client vlan** *vlan-identifier* 例： `スイッチ# client vlan test-vlan`	WLAN のインターフェイス グループをイネーブルにします。*vlan-identifier*：VLAN ID を指定します。次に、VLAN 名、VLAN ID、または VLAN グループ名を指定できます。
ステップ 7	**ip multicast vlan** *vlan-name* 例： `スイッチ(config-wlan)# ip multicast vlan test`	WLAN のマルチキャストをイネーブルにします。キーワードは次のとおりです。 • **vlan**：VLAN ID を指定します。 • *vlan-name*：VLAN 名を指定します。
ステップ 8	**media-stream multicast-direct** 例： `スイッチ(config-wlan)# media-stream multicast-direct`	この WLAN でマルチキャスト VLAN をイネーブルにします。
ステップ 9	**call-snoop** 例： `スイッチ(config-wlan)# call-snoop`	コール スヌーピング サポートをイネーブルにします。
ステップ 10	**no shutdown** 例： `スイッチ(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 11	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN の前提条件, （2505 ページ）
WLAN の制約事項, （2506 ページ）

高度な WLAN プロパティの設定（CLI）

次の高度なパラメータを設定できます。

- AAA オーバーライド
- Coverage Hole Detection
- Session Timeout
- Cisco Client Extensions
- 診断チャネル
- インターフェイス オーバーライド ACL
- P2P ブロッキング
- Client Exclusion
- WLAN ごとの最大クライアント数
- オフ チャネル スキャンの延期

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **aaa-override**
4. **chd**
5. **session-timeout** *time-in-seconds*
6. **ccx aironet-iesupport**
7. **diag-channel**
8. **ip access-group** [web] *acl-name*
9. **peer-blocking** [**drop** | **forward-upstream**]
10. **exclusionlist** *time-in-seconds*
11. **client association limit** *max-number-of-clients*
12. **channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}}
13. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**aaa-override** 例： スイッチ(config-wlan)# **aaa-override**	AAA オーバーライドをイネーブルにします。
ステップ 4	**chd** 例： スイッチ(config-wlan)# **chd**	この WLAN のカバレッジホールの検出をイネーブルにします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 5	**session-timeout** *time-in-seconds* 例： スイッチ(config-wlan)# **session-timeout 450**	セッションタイムアウトを秒単位で設定します。範囲とデフォルト値は、セキュリティ設定によって異なります。WLAN セキュリティが dot1x に設定されている場合、範囲は 300～86400 秒で、デフォルト値は 1800 秒です。他のすべての WLAN セキュリティ設定では、有効範囲は 1～65535 秒であり、デフォルト値は 0 秒です。値 0 は、セッション タイムアウトなしを示します。
ステップ 6	**ccx aironet-iesupport** 例： スイッチ(config-wlan)# **ccx aironet-iesupport**	この WLAN の Aironet IE のサポートをイネーブルにします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 7	**diag-channel** 例： スイッチ(config-wlan)# **diag-channel**	WLAN でクライアントの通信の問題を修復するための診断チャネルのサポートをイネーブルにします。
ステップ 8	**ip access-group** [web] *acl-name* 例： スイッチ(config)# **ip access-group test-acl-name**	WLAN ACL グループを設定します。可変 *acl* 名前はユーザ定義する IPv4 ACL の名前を指定します。キーワード **web** は、IPv4 web ACL を指定します。
ステップ 9	**peer-blocking** [**drop** | **forward-upstream**] 例： スイッチ(config)# **peer-blocking drop**	ピアツーピア ブロッキング パラメータを設定します。キーワードは次のとおりです。 • **drop**：ドロップ アクションのピアツーピア ブロッキングをイネーブルにします。 • **forward-upstream**：アップストリーム転送処理のピアツーピア ブロッキングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	**exclusionlist** *time-in-seconds* 例： `スイッチ(config)# exclusionlist 10`	タイムアウトを秒単位で指定します。0 ～ 2147483647 の範囲の値を指定できます。タイムアウトなしでは、0 を入力します。ゼロ（0）タイムアウトは、クライアントが除外リストに追加されたことを示しています。
ステップ 11	**client association limit** *max-number-of-clients* 例： `スイッチ(config)# client association limit 200`	WLAN で設定できる最大クライアント数を設定します。
ステップ 12	**channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} 例： `スイッチ(config)# channel-scan defer-priority 6`	チャネル スキャンの延期プライオリティと延期時間を設定します。引数は次のとおりです。 • **defer-priority**：オフチャネル スキャンを延期できるパケットのプライオリティ マーキングを指定します。有効な範囲は 0 ～ 7 です。デフォルトは 3 です。 • **defer-time**：ミリ秒単位の遅延時間です。範囲は 0 ～ 6000 です。デフォルトは 100 です。
ステップ 13	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

バンドの選択，（2508 ページ）
オフチャネル スキャンの延期
DTIM 周期
Session Timeout
Cisco Client Extensions，（2510 ページ）
ピアツーピア ブロッキング，（2510 ページ）
診断チャネル
WLAN ごとのクライアント カウント
WLAN の前提条件，（2505 ページ）
WLAN の制約事項，（2506 ページ）
AAA Override について，（2538 ページ）
レイヤ 2 セキュリティの前提条件，（2537 ページ）

WLAN プロパティの監視（CLI）

コマンド	説明
show wlan id *wlan-id*	WLAN ID に基づいて WLAN プロパティを表示します。
show wlan name *wlan-name*	WLAN 名に基づいて WLAN プロパティを表示します。
show wlan all	設定されているすべての WLAN の WLAN プロパティを表示します。
show wlan summary	すべての WLAN の要約を表示します。サマリー詳細には、次の情報が含まれます。 • WLAN ID • プロファイル名 • SSID • VLAN • ステータス
show running-config wlan *wlan-name*	WLAN の名前に基づいて WLAN の実行コンフィギュレーションを表示します。
show running-config *wlan*	すべての WLAN の実行コンフィギュレーションを表示します。

次の作業

DHCP for WLANs の設定に進みます

その他の参考資料

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

関連項目	マニュアル タイトル
Mobility Anchor の設定	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
WebAuth の設定	*Security Configuration Guide (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

WLANs の機能情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能	リリース	変更内容
WLAN の機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 111 章

DHCP for WLANs の設定

- 機能情報の確認，2525 ページ
- DHCP for WLANs を設定するための前提条件，2525 ページ
- DHCP for WLANs の設定に関する制約事項，2527 ページ
- Dynamic Host Configuration Protocol について，2527 ページ
- DHCP for WLANs の設定方法，2532 ページ
- その他の参考資料，2535 ページ
- DHCP for WLANs の機能情報，2536 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

DHCP for WLANs を設定するための前提条件

- DHCP オプション 82 を使用するには、Cisco IOS ソフトウェアで DHCP を設定します。デフォルトでは、DHCP オプション 82 は、すべてのクライアントに対してイネーブルにされます。WLAN サブオプションを使用して無線クライアントの動作を制御できます。
- シスコのスマートサービス機能のプラットフォームでは、内部 DHCP サーバ機能をサポートしています。ただし、大規模なエンタープライズクラスのネットワークを構築する一般的な

導入ガイドラインとして、無線クライアントにダイナミック IP アドレスを提供するために、外部 DHCP サーバの使用をお勧めします。このような分散機能は、ネットワーク デバイスにかかる処理および設定の負荷を低減し、大規模環境で効率的に動作させることができます。

- DHCP スヌーピング設定：DHCP スヌーピング設定は、クライアントの参加機能をすばやくスイッチ上で設定するために必要なベストプラクティスです。DHCP スヌーピングは各クライアント VLAN 上で有効にする必要があります。WLAN でオーバーライドが適用される場合は、オーバライド VLAN も対象となります。

DHCP スヌーピング設定の例

1. グローバル DHCP スヌーピングの設定：

   1. スイッチ(config)#**ip dhcp snooping**

      スイッチ(config)#**ip dhcp snooping vlan 100**

   2. Bootp-broadcast コマンドを有効にします。これは、ブロードキャスト アドレスを使用して DHCP メッセージを送信するクライアントに必要で、ブロードキャスト ビットが DHCP メッセージに設定されます。

      スイッチ(config)#**ip dhcp snooping wireless bootp-broadcast enable**

   3. DHCP オプション情報を付加しないためには、次のコマンドを入力します。

      スイッチ(config)#**no ip dhcp snooping information option**

2. インターフェイス上で、次のように設定します。

   （注） IP DHCP snooping trust は、ポート チャネル インターフェイスのメンバ リンクおよびポート チャネル インターフェイスで必要です。

```
スイッチ(config)#interface range TenGigabitEthernet 1/0/1 - 2
スイッチ(config-if)#switchport mode trunk
スイッチ(config-if)#switchport trunk allowed vlan 100
スイッチ(config-if)#ip dhcp snooping trust
スイッチ(config)#interface port-channel 1
スイッチ(config-if)#switchport mode trunk
スイッチ(config-if)#switchport trunk allowed vlan 100
スイッチ(config-if)#ip dhcp snooping trust
```

（注） DHCP スヌーピングは、上記の設定と同様に、ゲスト アクセス用のゲスト アンカー スイッチで設定する必要があります。

関連トピック

WLAN 用の DHCP 設定（CLI），（2532 ページ）
Dynamic Host Configuration Protocol について，（2527 ページ）
内部 DHCP サーバ，（2528 ページ）
外部 DHCP サーバ，（2528 ページ）
DHCP 割り当て，（2529 ページ）
DHCP オプション 82 について，（2530 ページ）
DHCP スコープの設定，（2531 ページ）
DHCP スコープについて，（2531 ページ）

DHCP for WLANs の設定に関する制約事項

- WLAN で DHCP サーバをオーバーライドすると、DHCP サーバが到達可能であることを確認するために、基盤となる Cisco IOS 設定を行う必要があります。
- DHCP WLAN オーバーライドは DHCP サービスがスイッチ上で有効な場合にだけ動作します。

  次の方法で、DHCP サービスを設定できます。

  - スイッチで DHCP プールを設定します。
  - SVI で DHCP リレー エージェントを設定します。注: SVI の VLAN は DHCP のオーバーライドが設定された WLAN にマッピングする必要があります。

関連トピック

WLAN 用の DHCP 設定（CLI），（2532 ページ）
Dynamic Host Configuration Protocol について，（2527 ページ）
内部 DHCP サーバ，（2528 ページ）
外部 DHCP サーバ，（2528 ページ）
DHCP 割り当て，（2529 ページ）
DHCP オプション 82 について，（2530 ページ）
DHCP スコープの設定，（2531 ページ）
DHCP スコープについて，（2531 ページ）

Dynamic Host Configuration Protocol について

WLAN では、同じ Dynamic Host Configuration Protocol（DHCP）サーバまたは異なる DHCP サーバを使用するか、または DHCP サーバを使用しないように設定できます。DHCP サーバには、内部 DHCP サーバと外部 DHCP サーバの 2 つのタイプがあります。

関連トピック

WLAN 用の DHCP 設定（CLI），（2532 ページ）
DHCP for WLANs を設定するための前提条件，（2525 ページ）
DHCP for WLANs の設定に関する制約事項，（2527 ページ）

内部 DHCP サーバ

スイッチは、内部 DHCP サーバを持っています。このサーバは、一般的に、DHCP サーバを持たないブランチ オフィスで使用されます。無線ネットワークには、通常、スイッチと同じ IP サブネット上にある最大 10 台のアクセス ポイントが含まれます。内部サーバは、ワイヤレス クライアント、ダイレクトコネクト アクセス ポイント、およびアクセス ポイントからリレーされた DHCP 要求に対して DHCP アドレスを提供します。Lightweight アクセス ポイントのみサポートされています。内部 DHCP サーバを使用する場合は、スイッチの管理インターフェイスの IP アドレスを DHCP サーバの IP アドレスとして設定する必要があります。

内部サーバでは、DHCP オプション 43 はサポートされていません。したがって、アクセス ポイントは、ローカル サブネット ブロードキャスト、ドメイン ネーム システム（DNS）、またはプライミングなどの別の方法を使用してスイッチの管理インターフェイスの IP アドレスを見つける必要があります。

内部 DHCP サーバ プールは、そのスイッチの無線クライアントだけをサポートし、他のスイッチのクライアントはサポートしません。また、内部 DHCP サーバは、無線クライアントだけをサポートし、有線クライアントをサポートしません。

クライアントがスイッチの内部 DHCP サーバを使用する場合、IP アドレスは、再起動後には保持されません。その結果、複数のクライアントに同じ IP アドレスが割り当てられることがあります。IP アドレスの競合を解決するには、クライアントは既存の IP アドレスを解放し、新しいアドレスを要求する必要があります。有線ゲスト クライアントは常に、ローカルまたは外部スイッチに接続されたレイヤ 2 ネットワークにあります。

（注） DHCPv6 は内部 DHCP サーバではサポートされません。

関連トピック

WLAN 用の DHCP 設定（CLI），（2532 ページ）
DHCP for WLANs を設定するための前提条件，（2525 ページ）
DHCP for WLANs の設定に関する制約事項，（2527 ページ）

外部 DHCP サーバ

オペレーティング システムは、DHCP リレーをサポートする業界標準の外部 DHCP サーバを使用することにより、ネットワークに対しては DHCP リレーとして機能し、クライアントに対しては DHCP サーバとして機能するように設計されています。これは、各スイッチは、DHCP サーバに

対しては DHCP リレー エージェントとして機能し、無線クライアントに対しては仮想 IP アドレスでの DHCP サーバとして機能することを意味します。

スイッチは DHCP サーバから取得したクライアント IP アドレスをキャプチャするため、スイッチ内、スイッチ間、およびサブネット間でのクライアント ローミング時に、各クライアントに対して同じ IP アドレスが保持されます。

（注） 外部 DHCP サーバは DHCPv6 をサポートします。

関連トピック

WLAN 用の DHCP 設定（CLI）, （2532 ページ）

DHCP for WLANs を設定するための前提条件, （2525 ページ）

DHCP for WLANs の設定に関する制約事項, （2527 ページ）

DHCP 割り当て

DHCP はインターフェイスごとに、または WLAN ごとに設定できます。特定のインターフェイスに割り当てられたプライマリ DHCP サーバのアドレスを使用することをお勧めします。

個々のインターフェイスに DHCP サーバを割り当てることができます。プライマリおよびセカンダリ DHCP サーバの管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスの設定、DHCP サーバをイネーブルまたはディセーブルするためのサービス ポート インターフェイスの設定を行うことができます。WLAN で DHCP サーバを定義することもできます。この場合、サーバは、WLAN に割り当てられたインターフェイスの DHCP サーバアドレスを上書きします。

セキュリティに関する注意事項

高度なセキュリティが必要な場合は、すべてのクライアントが DHCP サーバから IP アドレスを取得するように設定してください。この要件を適用するために、DHCP アドレスですべての WLAN を設定できます。Assignment Required 設定で設定して、クライアントの固定 IP アドレスが禁止されるようにします。DHCP Addr.Assignment Required が選択されている場合、クライアントは DHCP を使って IP アドレスを取得する必要があります。固定 IP アドレスを持つクライアントはすべて、ネットワーク上で許可されなくなります。クライアントの DHCP プロキシとして動作するスイッチが、DHCP トラフィックを監視します。

（注） 無線による管理をサポートする WLAN では、管理（デバイスサービシング）クライアントが DHCP サーバから IP アドレスを取得できるようにする必要があります。

セキュリティが多少劣ってもかまわない場合は、DHCP Addr.Assignment Required を無効に設定して WLAN を作成できます。その後クライアントは、固定 IP アドレスを使用するか、指定された DHCP サーバの IP アドレスを取得するかを選択できます。

（注） DHCP アドレス有線ゲスト LAN に対する Assignment Required は、サポートされていません。

個別の WLAN は、[DHCP Address Assignment Required] を無効にして作成できます。これは、スイッチの DHCP プロキシがイネーブルの場合だけです。DHCP プロキシをディセーブルにする必要があるプライマリ/セカンダリ コンフィギュレーションの DHCP サーバを定義しないでください。このような WLAN では、すべての DHCP 要求がドロップするため、クライアントは固定 IP アドレスを使用しなければなりません。これらの WLAN は、無線接続による管理をサポートしていません。

関連トピック

WLAN 用の DHCP 設定（CLI），（2532 ページ）

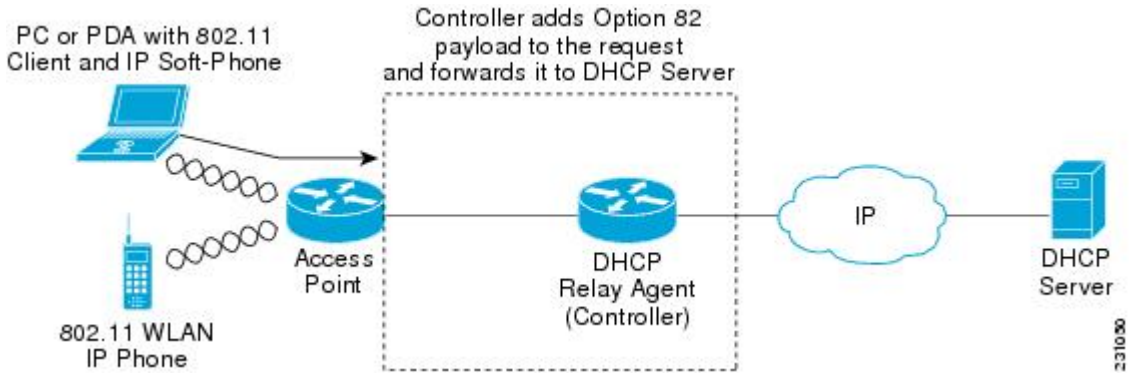
DHCP for WLANs を設定するための前提条件，（2525 ページ）

DHCP for WLANs の設定に関する制約事項，（2527 ページ）

DHCP オプション 82 について

DHCP オプション 82 では、DHCP を使用してネットワーク アドレスを割り当てる場合のセキュリティが強化されます。スイッチが DHCP リレー エージェントとして動作して、信頼できないソースからの DHCP クライアント要求を阻止できるようにします。DHCP サーバに転送するようにクライアントからの DHCP 要求にオプション 82 情報を追加するようにスイッチを設定できます。

図 *101*：*DHCP* オプション *82*



アクセス ポイントは、クライアントからのすべての DHCP 要求をスイッチに転送します。スイッチは、DHCP オプション 82 ペイロードを追加してから要求を DHCP サーバに転送します。このオプションの設定方法によって、ペイロードには MAC アドレス、または MAC アドレスとアクセス ポイントの SSID が含まれます。

（注） すでにリレー エージェント オプションが含まれている DHCP パケットは、スイッチでドロップされます。

DHCP オプション 82 が正しく動作するには、DHCP プロキシが有効でなければなりません。

関連トピック

WLAN 用の DHCP 設定（CLI）, （2532 ページ）
DHCP for WLANs を設定するための前提条件, （2525 ページ）
DHCP for WLANs の設定に関する制約事項, （2527 ページ）

DHCP スコープの設定

関連トピック

WLAN 用の DHCP 設定（CLI）, （2532 ページ）
DHCP for WLANs を設定するための前提条件, （2525 ページ）
DHCP for WLANs の設定に関する制約事項, （2527 ページ）

DHCP スコープについて

スイッチには組み込みの DHCP リレー エージェントがあります。ただし、別個の DHCP サーバを持たないネットワーク セグメントが必要な場合、スイッチに IP アドレスとサブネット マスクを無線クライアントに割り当てる組み込みの DHCP スコープを設定できます。一般に、1 つのスイッチには、それぞれある範囲の IP アドレスを指定する 1 つ以上の DHCP スコープを設定できます。

DHCP スコープは内部 DHCP が機能するために必要となります。スイッチで DHCP が定義されると、管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスのプライマリ DHCP サーバの IP アドレスをスイッチの管理インターフェイスにポイントすることができます。

関連トピック

WLAN 用の DHCP 設定（CLI）, （2532 ページ）
DHCP for WLANs を設定するための前提条件, （2525 ページ）
DHCP for WLANs の設定に関する制約事項, （2527 ページ）
DHCP スコープの設定（CLI）, （2534 ページ）

DHCP for WLANs の設定方法

WLAN 用の DHCP 設定（CLI）

WLAN で次の DHCP パラメータを設定するには、次の手順に従います。

- DHCP オプション 82 ペイロード
- DHCP（必須）
- DHCP オーバーライド

はじめる前に

- WLAN を設定するには admin 権限がなければなりません。
- DHCP のオーバーライドを設定するには、DHCP サーバの IP アドレスが必要です。

手順の概要

1. **configure terminal**
2. **shutdown**
3. **wlan** *profile-name*
4. **ip dhcp opt82** {**ascii** | **format** {*add-ssid* | *ap-ethmac*} | **rid**}
5. **ip dhcp required**
6. **ip dhcp server** *ip-address*
7. **no shutdown**
8. **end**
9. **show wlan** *wlan-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**shutdown** 例： スイッチ(config)# **shutdown**	WLAN をシャットダウンします。

	コマンドまたはアクション	目的
ステップ 3	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 4	**ip dhcp opt82** {**ascii** | **format** {*add-ssid* | *ap-ethmac*} | **rid**} 例： スイッチ(config)# **ip dhcp opt82 format add-ssid**	WLAN で DHCP82 ペイロードを指定します。キーワードおよび引数は、次のとおりです。 • **ascii**：DHCP オプション 82 の ASCII を設定します。これが設定されていない場合、オプション 82 の形式は ASCII 形式に設定されます。 • **format**：DHCP オプション 82 の形式を指定します。次のオプションを使用できます。 • *add-ssid*：AP 無線の MAC アドレスおよび SSID である RemoteID 形式を設定します。 • *ap-ethmac*：AP Ethernet MAC アドレスである RemoteID 形式を設定します。 （注） フォーマット オプションが設定されていない場合、AP 無線の MAC アドレスだけが使用されます。 • **rid**：DHCP オプション 82 に Cisco 2 バイト RID を追加します。
ステップ 5	**ip dhcp required** 例： スイッチ(config-wlan)# **ip dhcp required**	DHCP サーバから IP アドレスをクライアントが取得することを必須にします。スタティック クライアントは許可されません。
ステップ 6	**ip dhcp server** *ip-address* 例： スイッチ(config-wlan)# **ip dhcp server 200.1.1.2**	WLAN に割り当てられたインターフェイスの DHCP サーバ アドレスを上書きする WLAN 上の DHCP サーバを定義します。
ステップ 7	**no shutdown** 例： スイッチ(config-wlan)# **no shutdown**	WLAN を再起動します。
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

	コマンドまたはアクション	目的
ステップ 9	**show wlan** *wlan-name* 例： スイッチ(config-wlan)# **show wlan test-wlan**	DHCP の設定を確認します。

関連トピック

Dynamic Host Configuration Protocol について，（2527 ページ）
内部 DHCP サーバ，（2528 ページ）
外部 DHCP サーバ，（2528 ページ）
DHCP 割り当て，（2529 ページ）
DHCP オプション 82 について，（2530 ページ）
DHCP スコープの設定，（2531 ページ）
DHCP スコープについて，（2531 ページ）
DHCP for WLANs を設定するための前提条件，（2525 ページ）
DHCP for WLANs の設定に関する制約事項，（2527 ページ）

DHCP スコープの設定（CLI）

手順の概要

1. **configure terminal**
2. **ip dhcp pool** *pool-name*
3. **network** *network-name mask-address*
4. **dns-server** *hostname*
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ip dhcp pool** *pool-name* 例： スイッチ(config)#**ip dhcp pool test-pool**	DHCP プール アドレスを設定します。
ステップ 3	**network** *network-name mask-address* 例： スイッチ(dhcp-config)#**network 209.165.200.224 255.255.255.0**	ドット付き 10 進表記とマスク アドレスでネットワーク番号を指定します。
ステップ 4	**dns-server** *hostname* 例： スイッチ(dhcp-config)#**dns-server example.com**	DNS ネーム サーバを指定します。IP アドレスまたはホスト名を指定できます。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

DHCP スコープについて，（2531 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
システム管理	*System Management Configuration Guide*（*Catalyst 3650 Switches*）

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

DHCP for WLANs の機能情報

機能名	リリース	機能情報
WLAN の DHCP 機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 112 章

WLAN セキュリティの設定

- 機能情報の確認，2537 ページ
- レイヤ 2 セキュリティの前提条件，2537 ページ
- AAA Override について，2538 ページ
- WLAN セキュリティの設定方法，2539 ページ
- その他の参考資料，2544 ページ
- WLAN レイヤ 2 セキュリティに関する機能情報，2545 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

レイヤ 2 セキュリティの前提条件

同じ SSID を持つ WLAN は、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントが WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。使用可能なレイヤ 2 セキュリティ ポリシーは、次のとおりです。

- なし（オープン WLAN）
- Static WEP または 802.1X

（注） Static WEP と 802.1X は両方とも、ビーコン応答とプローブ応答で同じビットによってアドバタイズされるので、クライアントはこれらを区別できません。したがって、同じ SSID を持つ複数の WLAN では、Static WEP と 802.1X の両方を使用できません。

- WPA/WPA2

（注）
- 同じ SSID を持つ複数の WLAN で WPA と WPA2 を使用することはできませんが、同じ SSID を持つ 2 つの WLAN は、PSK を使用する WPA/TKIP と 802.1X を使用する Wi-Fi Protected Access（WPA）/Temporal Key Integrity Protocol（WPA）で設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES で設定することができます。
- TKIP サポートが設定された WLAN は RM3000AC モジュールで有効にされません。

関連トピック

静的 WEP と 802.1X レイヤ 2 セキュリティ パラメータの設定（CLI），（2539 ページ）
レイヤ 2 パラメータの設定（GUI）
静的 WEP レイヤ 2 セキュリティ パラメータの設定（CLI），（2540 ページ）
WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（CLI），（2541 ページ）
802.1X レイヤ 2 セキュリティ パラメータの設定（CLI），（2543 ページ）
高度な WLAN プロパティの設定（CLI），（2519 ページ）
AAA Override について，（2538 ページ）

AAA Override について

WLAN の AAA Override オプションを使用すると、WLAN で Identity ネットワーキングを設定できます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、Quality Of Service (QoS)、およびアクセス コントロール リスト (ACL) を適用することができます。

関連トピック

高度な WLAN プロパティの設定（CLI），（2519 ページ）
レイヤ 2 セキュリティの前提条件，（2537 ページ）

WLAN セキュリティの設定方法

静的 WEP と 802.1X レイヤ 2 セキュリティ パラメータの設定（CLI）

はじめる前に

管理者特権が必要です。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **security static-wep-key** {**authentication** {**open** | **sharedkey**} | **encryption** {**104** | **40**} [**ascii** | **hex**] {**0**|**8**}} *wep-key wep-key-index1-4*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**security static-wep-key** {**authentication** {**open**	**sharedkey**}	**encryption** {**104**	**40**} [**ascii**	**hex**] {**0**|**8**}} *wep-key wep-key-index1-4* 例： スイッチ(config-wlan)# **security static-wep-key encryption 40 hex 0 test 2**	WLAN の静的 WEP セキュリティを設定します。次のキーワードと引数があります。 • **authentication**：802.11 認証を設定します。 • **encryption**：静的 WEP キーとインデックスを設定します。 • **open**：オープン システム認証を設定します。 • **sharedkey**：共有キー認証を設定します。 • **104, 40**：WEP キーのサイズを指定します。 • **hex, ascii**：キーの入力形式を指定します。 • *wep-key-index*、*wep-key-index1-4* 指定するパスワードのタイプです。値が 0 である場合は、暗号化されないパスワードを指定することを示します。値が 8 である場合は、AES 暗号化を指定することを示します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： スイッチ(config)# **end**	特権EXECモードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件, （2537 ページ）

静的 WEP レイヤ 2 セキュリティ パラメータの設定（CLI）

はじめる前に

管理者特権が必要です。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **security static-wep-key** [**authentication** {**open** | **shared**} | **encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**security static-wep-key** [**authentication** {**open**	**shared**}	**encryption** {**104**	**40**} {**ascii**	**hex**} [**0**	**8**]] 例： スイッチ(config-wlan)# **security static-wep-key authentication open**	キーワードは次のとおりです。 • **static-wep-key**：静的 WEP キーの認証を設定します。 • **authentication**：ユーザが設定できる認証タイプを指定します。値は、open および shared です。

	コマンドまたはアクション	目的
		• **encryption**：ユーザが設定できる暗号化タイプを指定します。有効な値は 104 と 40 です。40 ビットキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。104 ビットキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。 • **ascii**：ASCII としてキー形式を指定します。 • **hex**：HEX としてキー形式を指定します。
ステップ 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件, （2537 ページ）

WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（CLI）

（注） デフォルト セキュリティ ポリシーは、WPA2 です。

はじめる前に

管理者特権が必要です。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **security wpa**
4. **security wpa wpa1**
5. **security wpa wpa1 ciphers** [**aes** | **tkip**]
6. **security wpa wpa2**
7. **security wpa wpa2 ciphers** [**aes** | **tkip**]
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**security wpa** 例： スイッチ(config-wlan)# **security wpa**	WPA をイネーブルにします。
ステップ 4	**security wpa wpa1** 例： スイッチ(config-wlan)# **security wpa wpa1**	WPA1 をイネーブルにします。
ステップ 5	**security wpa wpa1 ciphers** [**aes** | **tkip**] 例： スイッチ(config-wlan)# **security wpa wpa1 ciphers aes**	WPA1 暗号を指定します。次のいずれかの暗号化タイプを選択します。 • **aes**：WPA/AES のサポートを指示します。 • **tkip**：WPA/TKIP のサポートを指示します。
ステップ 6	**security wpa wpa2** 例： スイッチ(config-wlan)# **security wpa**	WPA 2 をイネーブルにします。
ステップ 7	**security wpa wpa2 ciphers** [**aes** | **tkip**] 例： スイッチ(config-wlan)# **security wpa wpa2 ciphers tkip**	WPA2 暗号化を設定します。次のいずれかの暗号化タイプを選択します。 • **aes**：WPA/AES のサポートを指示します。 • **tkip**：WPA/TKIP のサポートを指示します。
ステップ 8	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件, （2537 ページ）

802.1X レイヤ 2 セキュリティ パラメータの設定（CLI）

はじめる前に

管理者特権が必要です。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **security dot1x**
4. **security** [**authentication-list** *auth-list-name* | **encryption** {**0** | **104** | **40**}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**security dot1x** 例： スイッチ(config-wlan)# **security dot1x**	802.1X セキュリティを指定します。
ステップ 4	**security** [**authentication-list** *auth-list-name*	**encryption** {**0**	**104**	**40**} 例： スイッチ(config-wlan)# **security encryption 104**	次のキーワードと引数があります。 • **authentication-list**：IEEE 802.1X の認証リストを指定します。 • **encryption**：CKIP 暗号化キーの長さを指定します。有効な値は、0、40、および 104 です。ゼロ（0）では暗号化されません。これはデフォルトです。 （注） WLAN 内のすべてのキーは、同じサイズでなければなりません。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件, （2537 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
セキュリティ コンフィギュレーション ガイド	*Security Configuration Guide (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

WLAN レイヤ 2 セキュリティに関する機能情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
WLAN のセキュリティ機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 113 章

WLAN ごとのクライアント カウントの設定

- 機能情報の確認，2547 ページ
- WLAN ごとのクライアント カウントの設定に関する制約事項，2547 ページ
- WLAN ごとのクライアント カウントの設定について，2548 ページ
- WLAN ごとのクライアント カウントを設定する方法，2549 ページ
- クライアントの接続の監視（CLI），2551 ページ
- クライアント接続に関する追加情報，2552 ページ
- WLAN ごとのクライアント接続に関する機能情報，2553 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

WLAN ごとのクライアント カウントの設定に関する制約事項

- WLAN が接続クライアントの最大数の制限に達しているか、AP 無線および新しいクライアントが WLAN に参加しようとしている場合、クライアントは既存のクライアントが切断されるまで WLAN に接続できません。

- ローミング クライアントは新しいクライアントと見なされます。クライアントの接続数の最大制限に到達している WLAN に対して新しいクライアントは、既存のクライアントが切断されたときにのみ接続できます。

（注） サポートされているクライアント数の詳細については、スイッチの製品データ シートを参照してください。

関連トピック

WLAN ごとのクライアント カウントの設定（CLI），（2549 ページ）
WLAN ごとの各 AP のクライアント数の設定（CLI），（2550 ページ）
WLAN あたりの AP 無線ごとのクライアント数の設定（CLI），（2551 ページ）
WLAN ごとのクライアント カウントの設定について，（2548 ページ）

WLAN ごとのクライアント カウントの設定について

WLAN に接続できるクライアントの数に制限を設定できます。これは、スイッチに接続できるクライアントの数に制限があるシナリオで役立ちます。たとえば、スイッチが WLAN 上の最大 256 個のクライアントに対応でき、これらのクライアントが企業ユーザ（従業員）およびゲスト ユーザ間で共有される場合について考えます。特定の WLAN にアクセス可能なゲスト クライアントの数に制限を設定できます。WLAN ごとに設定できるクライアントの数は、使用しているプラットフォームによって異なります。

関連トピック

WLAN ごとのクライアント カウントの設定（CLI），（2549 ページ）
WLAN ごとの各 AP のクライアント数の設定（CLI），（2550 ページ）
WLAN あたりの AP 無線ごとのクライアント数の設定（CLI），（2551 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項，（2547 ページ）
クライアントの接続の監視（CLI），（2551 ページ）

WLAN ごとのクライアント カウントを設定する方法

WLAN ごとのクライアント カウントの設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client associationlimit***limit*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client associationlimit***limit* 例： スイッチ(config-wlan)# **client association limit 2000**	WLAN ごとのクライアント アソシエーションの最大数を設定します。有効な範囲は 0 ～ 2000.デフォルト値は 0 です（制限なし）。
ステップ 4	**end** 例： スイッチ(wlan-config)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN ごとのクライアント カウントの設定について，（2548 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項，（2547 ページ）
クライアントの接続の監視（CLI），（2551 ページ）

WLAN ごとの各 AP のクライアント数の設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client association limit ap** *ap-limit*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `スイッチ# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client association limit ap** *ap-limit* 例： `スイッチ(config-wlan)# client association limit ap 250`	WLAN ごとの AP あたりの最大クライアント数を設定します。範囲は 1 ～ 400 です。
ステップ 4	**end** 例： `スイッチ(wlan-config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN ごとのクライアント カウントの設定について，（2548 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項，（2547 ページ）
クライアントの接続の監視（CLI），（2551 ページ）

WLAN あたりの AP 無線ごとのクライアント数の設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client association limit radio** *max-client-connections*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client association limit radio** *max-client-connections* 例： スイッチ(config-wlan)# **client association limit radio 180**	WLAN あたりの AP 無線ごとのクライアント接続の最大数を設定します。a、b、および g 無線でこの範囲は 0～200 です。
ステップ 4	**end** 例： スイッチ(config-wlan)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN ごとのクライアント カウントの設定について，（2548 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項，（2547 ページ）
クライアントの接続の監視（CLI），（2551 ページ）

クライアントの接続の監視（CLI）

次のコマンドがスイッチクライアント接続の監視に使用できます。

コマンド	説明

show wlan name *wlan-name*	WLAN プロパティを表示します。次に例を示します。
	
	`. . . .`
	`Max Associated Clients per WLAN :0`
	`Max Associated Clients per AP per WLAN :0`
	`Max Associated Clients per AP Radio per WLAN :0`
	`. . .`
	`. . .`

show wlan id *wlan-id*	WLAN のプロパティを表示します。ここに一例を上げます:
	
	`. . . .`
	`Max Associated Clients per WLAN :0`
	`Max Associated Clients per AP per WLAN :0`
	`Max Associated Clients per AP Radio per WLAN :0`
	`. . .`
	`. . .`

関連トピック

WLAN ごとのクライアント カウントの設定（CLI），（2549 ページ）
WLAN ごとの各 AP のクライアント数の設定（CLI），（2550 ページ）
WLAN あたりの AP 無線ごとのクライアント数の設定（CLI），（2551 ページ）
WLAN ごとのクライアント カウントの設定について，（2548 ページ）

クライアント接続に関する追加情報

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

WLAN ごとのクライアント接続に関する機能情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
WLAN、AP、AP 無線ごとのクライアント接続	Cisco IOS XE 3.3SE	この機能が導入されました。

第 114 章

802.11w の設定

- 機能情報の確認，2555 ページ
- 802.11w の前提条件，2555 ページ
- 802.11w の制約事項，2556 ページ
- 802.11w に関する情報，2556 ページ
- 802.11w の設定方法，2557 ページ
- 802.11w のディセーブル（CLI），2559 ページ
- 802.11w の監視（CLI），2561 ページ
- 802.11w に関する追加情報，2562 ページ
- 802.11w の機能に関する情報，2563 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

802.11w の前提条件

- 任意および必須の 802.11w 機能を設定するには、WPA および AKM を設定する必要があります。

（注） Robust Secure Network（RNS）IE は AES 暗号化とともにイネーブルにする必要があります。

- 必須として 802.11w を設定するには、WPA AKM に加えて PMF AKM を有効にします。

関連トピック

802.11w の設定（CLI），（2557 ページ）

802.11w のディセーブル（CLI），（2559 ページ）

802.11w に関する情報，（2556 ページ）

802.11w の制約事項

- 802.11w は、オープン WLAN、 WEP 暗号化 WLAN、または TKIP 暗号化 WLAN に適用できません。
- 802.11w が設定された WLAN では、WPA2-PSK または WPA2-802.1x セキュリティを設定する必要があります。

関連トピック

802.11w の設定（CLI），（2557 ページ）

802.11w のディセーブル（CLI），（2559 ページ）

802.11w に関する情報，（2556 ページ）

802.11w に関する情報

Wi-Fiは、正規のデバイスまたは不法なデバイスのいずれであっても、あらゆるデバイスで傍受または参加が可能なブロードキャスト メディアです。認証/認証解除、アソシエーション/ディスアソシエーション、ビーコンおよびプローブなどの制御/管理フレームは、無線クライアントによって、AP を選択し、ネットワーク サービスのセッションを開始するために使用されます。

機密保持レベルを提供する暗号化可能なデータ トラフィックとは異なり、これらのフレームは、すべてのクライアントによって解釈されることが必要であり、したがってオープンまたは非暗号化形式で送信されます。これらのフレームは暗号化できませんが、攻撃から無線メディアを保護するために偽造を防止することが必要になります。 たとえば、攻撃者はクライアントと AP の間のセッションを切断するために、APから管理フレームをスプーフィングする可能性があります。

802.11w プロトコルは、管理フレーム保護（PMF）サービスによって保護された一連の強力な管理フレームにのみ適用されます。これらには、ディスアソシエーション、認証解除、ロバスト アクション フレームが含まれます。

したがって、ロバストアクションであり、保護されているものと見なされる管理フレームは次のとおりです。

- スペクトラム管理
- QoS
- ブロック ACK
- SA クエリ
- ベンダー固有保護

802.11w が無線メディアで実行されると、次のことが行われます。

- ディスアソシエーションフレームと認証解除フレームに対して、（MIC 情報要素を含めることにより）AP の暗号保護によるクライアント保護が追加されます。これによって、DoS 攻撃でのスプーフが防止されます。
- アソシエーションの復帰期間と SA クエリーの手順から構成されるセキュリティ アソシエーション（SA）ティアダウン保護メカニズムを追加することによって、インフラストラクチャの保護が追加され、スプーフィングされた要求によるすでに接続済みのクライアントの切断が防止されます。

関連トピック

802.11w の設定（CLI）, （2557 ページ）
802.11w のディセーブル（CLI）, （2559 ページ）
802.11w の前提条件, （2555 ページ）
802.11w の制約事項, （2556 ページ）
802.11w の監視（CLI）, （2561 ページ）

802.11w の設定方法

802.11w の設定（CLI）

はじめる前に

WPA および AKM を設定する必要があります。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **security pmf** {**association-check** *association-comeback-time-in-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-in-milliseconds*}
5. **no shutdown**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： スイッチ **shutdown**	PMF を設定する前に WLAN をシャットダウンします。
ステップ 4	**security pmf** {**association-check** *association-comeback-time-in-seconds*	**mandatory**	**optional**	**saquery** *saquery-time-in-milliseconds*} 例： スイッチ(config-wlan)# **security pmf saquery-retry-time 200**	次のオプションにより PMF パラメータを設定します。 • **association-comeback**：802.11w アソシエーション復帰期間を設定します。 範囲は、1 ～ 20 秒です。 • **mandatory**：クライアントが WLAN の 802.11w PMF 保護をネゴシエートすることを要求します。 • **optional**：WLAN の 802.11w PMF 保護を有効にします。 • **saquery**：SA クエリの応答を受け取るまでの時間（ミリ秒単位）。スイッチが応答を受け取らなかった場合、別の SQ クエリーが試行されます。 指定できる範囲は 100 ～ 500 ミリ秒です。値には 100 ミリ秒の倍数を指定する必要があります。

	コマンドまたはアクション	目的
ステップ 5	**no shutdown** 例： スイッチ **no shutdown**	変更内容を反映するために、WLAN サーバを再起動します。
ステップ 6	**end** 例： スイッチ(config-wlan)# **end**	特権EXECモードに戻ります。また、**Ctrl+Z**キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11w に関する情報，（2556 ページ）
802.11w の前提条件，（2555 ページ）
802.11w の制約事項，（2556 ページ）
802.11w の監視（CLI），（2561 ページ）

802.11w のディセーブル（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **no security pmf [association-comeback** *association-check-comback-interval-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-interval-milliseconds*]
5. **no shutdown**
6. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： スイッチ **shutdown**	PMF を設定する前に WLAN をシャットダウンします。
ステップ 4	**no security pmf [association-comeback** *association-check-comback-interval-seconds* **| mandatory | optional | saquery** *saquery-time-interval-milliseconds*] 例： スイッチ(config-wlan)# **no security pmf**	WLAN の PMF をディセーブルにします。次の属性を使用できます。 • **association-comeback**：802.11w のアソシエーションの復帰期間をディセーブルにします。 • **mandatory**：クライアントが WLAN の 802.11w PMF 保護をネゴシエートすることをディセーブルにします。 • **optional**：WLAN の 802.11w PMF 保護をディセーブルにします。 • **saquery**：アソシエーションを再試行する前に、すでにアソシエートされているクライアントへのアソシエーション応答で特定される時間間隔。アソシエーションの復帰期間中、この時間間隔により、クライアントが実際のクライアントであり、不正なクライアントではないかどうかが確認されます。クライアントがこの時間内に応答しない場合は、クライアント アソシエーションがスイッチから削除されます。 指定できる範囲は 100 ～ 500 ミリ秒です。値には 100 ミリ秒の倍数を指定する必要があります。
ステップ 5	**no shutdown** 例： スイッチ **no shutdown**	変更内容を反映するために、WLAN サーバを再起動します。
ステップ 6	**end** 例： スイッチ(config-wlan)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11w に関する情報, （2556 ページ）

802.11w の前提条件，（2555 ページ）
802.11w の制約事項，（2556 ページ）
802.11w の監視（CLI），（2561 ページ）

802.11w の監視（CLI）

802.11w の監視に使用できるコマンドは次のとおりです。

コマンド	説明
show wlan name *wlan-profile-name*	WLAN の WLAN パラメータを表示します。PMF パラメータが表示されます。次に例を示します。 . . . . Auth Key Management 802.1x : Disabled PSK : Enabled CCKM : Disabled FT dot1x : Disabled FT PSK : Disabled PMF dot1x : Disabled PMF PSK : Enabled FT Support : Disabled FT Reassociation Timeout : 20 FT Over-The-DS mode : Disabled PMF Support : Required PMF Association Comeback Timeout : 9 PMF SA Query Time : 200 . . . .

関連トピック

802.11w の設定（CLI），（2557 ページ）
802.11w のディセーブル（CLI），（2559 ページ）
802.11w に関する情報，（2556 ページ）

802.11w に関する追加情報

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
WLAN セキュリティ	このマニュアルの *WLAN* セキュリティの設定の章

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
802.11W	IEEE 802.11w 保護管理フレーム

MIB

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

シスコのテクニカル サポート

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

802.11w の機能に関する情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
802.11w	Cisco IOS XE 3.3SE	この機能が導入されました。

第 115 章

Wi-Fi Direct クライアント ポリシーの設定

- 機能情報の確認，2565 ページ
- Wi-Fi Direct クライアント ポリシーの制限，2565 ページ
- Wi-Fi Direct クライアント ポリシーについて，2566 ページ
- Wi-Fi Direct クライアント ポリシーの設定方法，2566 ページ
- Wi-Fi Direct クライアント ポリシーに関する追加リファレンス，2569 ページ
- Wi-Fi Direct クライアント ポリシーに関する機能情報，2570 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

Wi-Fi Direct クライアント ポリシーの制限

- Wi-Fi Direct クライアント ポリシーは、ローカル モードの AP が含まれる WLAN のみに適用できます。
- WLAN クライアントに適用されるポリシーが無効の場合、クライアントは「クライアント QoS ポリシー障害」という項目理由のため除外されます。

Wi-Fi Direct クライアント ポリシーについて

Wi-Fi Direct 対応のデバイスは迅速な相互接続が可能で、印刷、同期、データ共有などのタスクを効率的に実行できますWi-Fi Direct デバイスは、複数のピアツーピア（P2P）デバイスおよびインフラストラクチャ無線 LAN（WLAN）に同時にアソシエートしている場合があります。スイッチを使用して、Wi-Fi Direct クライアント ポリシーを WLAN 単位で設定できます。その際、Wi-Fi デバイスとインフラストラクチャ WLAN のアソシエーションを許可または禁止するか、WLAN に対して Wi-Fi Direct クライアント ポリシーをすべて無効にすることができます。

関連トピック

Wi-Fi Direct クライアント ポリシーの設定（CLI），（2566 ページ）
Wi-Fi Direct クライアント ポリシーのディセーブル（CLI），（2568 ページ）
Wi-Fi Direct クライアント ポリシーの監視（CLI），（2568 ページ）

Wi-Fi Direct クライアント ポリシーの設定方法

Wi-Fi Direct クライアント ポリシーの設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **wifidirect policy** {**permit** | **deny** }
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。

	コマンドまたはアクション	目的
ステップ 3	**wifidirect policy** {**permit** | **deny** } 例： スイッチ(config-wlan)# **wifidirect policy permit**	次のいずれかを使用して WLAN の Wi-Fi Direct クライアント ポリシーを設定します • **permit**：Wi-Fi Direct クライアントと WLAN のアソシエーションをイネーブルにします。 • **deny**：Wi-Fi Direct ポリシーが「拒否」に設定されている場合は、デバイス機能に基づいてスイッチが Wi-Fi Direct デバイスを許可または拒否します。Wi-Fi Direct デバイスは、スイッチへのアソシエーション要求でこれらの機能をにレポートします。これは、このデバイスの Wi-Fi 機能に基づいて行われます。次の作業を行います。 • 同時操作 • 相互接続 （注） コマンド **no wifidirect policy** は、クライアントの Wi-Fi Direct ステータスを無視します。さらに、アクセスポイントはビーコンおよびプローブをアドバタイズしません。実際には、このコマンドの **no** 形式では、WLAN の Wi-Fi Direct 機能はディセーブルになります。 Wi-Fiデバイスが同時操作または相互接続、あるいはその両方をサポートする場合は、クライアントの関連付けは拒否されます。クライアントは、デバイスが同時操作と相互接続をサポートしない場合に関連付けることができます。
ステップ 4	**end** 例： スイッチ(config-wlan)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

Wi-Fi Direct クライアント ポリシーについて，（2566 ページ）
Wi-Fi Direct クライアント ポリシーの監視（CLI），（2568 ページ）

Wi-Fi Direct クライアント ポリシーのディセーブル（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **no wifidirect policy**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**no wifidirect policy** 例： スイッチ(config)# **no wifidirect policy**	クライアントの Wi-Fi Direct ステータスを無視し、それによって Wi-Fi Direct クライアントのアソシエーションを許可します
ステップ 4	**end** 例： スイッチ(config-wlan)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

Wi-Fi Direct クライアント ポリシーについて，（2566 ページ）
Wi-Fi Direct クライアント ポリシーの監視（CLI），（2568 ページ）

Wi-Fi Direct クライアント ポリシーの監視（CLI）

次のコマンドが Wi-Fi Direct クライアント ポリシーを監視するために使用できます。

コマンド	説明
show wireless client wifidirect stats	関連付けられたクライアントの総数と、Wi-Fi Direct クライアント ポリシーを有効にした場合に拒否されたアソシエーション要求の数が表示されます。
show wlan summary	WLAN での Wi-Fi Direct の状態を表示します。
show wireless cli mac-address *mac-address*	クライアントの詳細情報を表示します。

関連トピック

Wi-Fi Direct クライアント ポリシーの設定（CLI），（2566 ページ）
Wi-Fi Direct クライアント ポリシーのディセーブル（CLI），（2568 ページ）
Wi-Fi Direct クライアント ポリシーについて，（2566 ページ）

Wi-Fi Direct クライアント ポリシーに関する追加リファレンス

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

Wi-Fi Direct クライアント ポリシーに関する機能情報

機能名	リリース	機能情報
Wi-Fi Direct の機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 116 章

802.11r BSS の高速移行の設定

- 機能情報の確認，2571 ページ
- 802.11r 高速移行の制約事項，2571 ページ
- 802.11r の高速移行について，2572 ページ
- 802.11r 高速移行を設定する方法，2576 ページ
- 802.11r 高速移行に関する追加情報，2584 ページ
- 802.11r 高速移行の機能に関する情報，2585 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

802.11r 高速移行の制約事項

- 802.11r クライアント アソシエーションは、スタンドアロン モードのアクセス ポイントではサポートされません。
- 802.11r 高速ローミングは、スタンドアロン モードのアクセス ポイントではサポートされません。
- ローカル認証 WLAN と中央認証 WLAN 間の 802.11r 高速ローミングはサポートされていません。

- FlexConnect モードの Aps では、802.11r 高速ローミングは APs が同じ FlexConnect グループの場合にのみ動作します。
- EAP LEAP 方式はサポートされません。
- TSpec は 802.11r 高速ローミングではサポートされません。したがって、RIC IE の処理はサポートされません。
- WAN リンク遅延がある場合、高速ローミングも遅延します。音声またはデータの最大遅延を確認する必要があります。スイッチは、Over-the-Air および Over-the-DS の両方式をローミングする間、802.11r 高速移行の認証要求を処理します。
- この機能は、オープンで WPA2 設定の WLAN でのみサポートされます。
- レガシー クライアントは、Robust Security Network Information Exchange（RSN IE）の解析を担当するサプリカントのドライバが古く、IE 内の追加 AKM を認識しない場合、802.11r が有効にされている WLAN にアソシエートできません。この制限のため、クライアントは、WLAN にアソシエーション要求を送信できません。ただし、これらのクライアントは、非 802.11r WLAN とアソシエートできます。802.11r 対応クライアントは、802.11r と 802.11i の両方の認証キー管理スイートが有効にされている WLAN の 802.11i クライアントとしてアソシエートできます。

  回避策は、レガシー クライアントのドライバを新しい 802.11r AKM で動作するようにするか、またはアップグレードすることです。そうすることで、レガシー クライアントは、802.11r 対応 WLAN と正常にアソシエートできます。

  もう 1 つの回避策は、同じ名前で異なるセキュリティ設定（FT および非 FT）の 2 つの SSID を持つことです。
- 高速移行のリソース要求プロトコルは、クライアントがこのプロトコルをサポートしていないため、サポートされません。また、リソース要求プロトコルはオプションのプロトコルです。
- DoS 攻撃を回避するため、各スイッチでは、異なる AP と最大 3 つの高速移行ハンドシェイクが可能です。

関連トピック

オープン WLAN での 802.11r 高速移行の設定（CLI），（2576 ページ）

802.11r 高速移行のディセーブル（CLI），（2581 ページ）

Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI），（2578 ページ）

PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI），（2579 ページ）

802.11r の高速移行について，（2572 ページ）

802.11r の高速移行について

高速ローミングの IEEE 標準である 802.11r は、クライアントがターゲット AP にローミングする前でも、新しい AP との最初のハンドシェイクが実行される、高速移行（FT）と呼ばれるローミ

ングの新しい概念が導入されています。初期ハンドシェイクによって、クライアントと AP が事前に Pairwise Transient Key（PTK）計算をできるようになります。これらの PTK キーは、クライアントが新しいターゲット AP の再アソシエーション要求または応答の交換をした後で、クライアントと AP に適用されます。

802.11r は、次の 2 通りのローミングを提供します。

- Over-the-Air
- Over-the-DS（分散システム）

FT キー階層は、クライアントが各 AP での再認証なしで、AP 間の高速 BSS 移行ができるように設計されています。WLAN設定には、FT（高速移行）と呼ばれる、新しい認証キー管理（AKM）タイプが含まれています。

リリース3Eから、WPAv2 WLANでもある802.11r WLANを作成できます。以前のリリースでは、802.11r の WLAN と通常のセキュリティ用にそれぞれ個別の WLAN を作成する必要がありました。802.11r WLAN が非 802.11r アソシエーションを受け入れることができるため、非 802.11r クライアントが802.11r WLAN対応WLANに接続できるようになりました。混合モードまたは802.11r接続をサポートしないクライアントは、非 802.11r WLAN に接続できます。FT PSK 以降を設定すると、PSKを混合モードでWLANを結合できるPSKだけ結合できるクライアントを定義します。

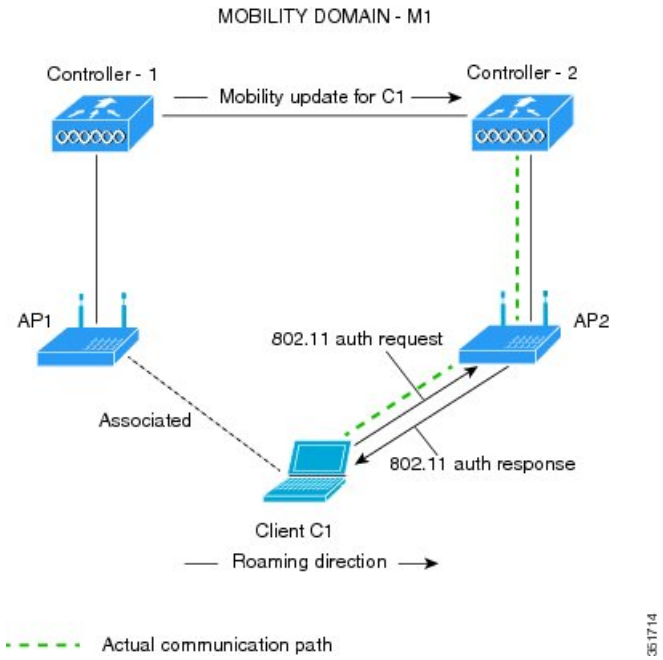
クライアントのローミング方法

FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の 2 つの方法のいずれかを使用して行われます。

- Over-the-Air：クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。
- Over-the-DS：クライアントは、現在の AP を介してターゲット AP と通信します。クライアントとターゲット AP との間の通信は、クライアントと現在の AP 間の FT アクション フレームで実行されてから、スイッチによって送信されます。

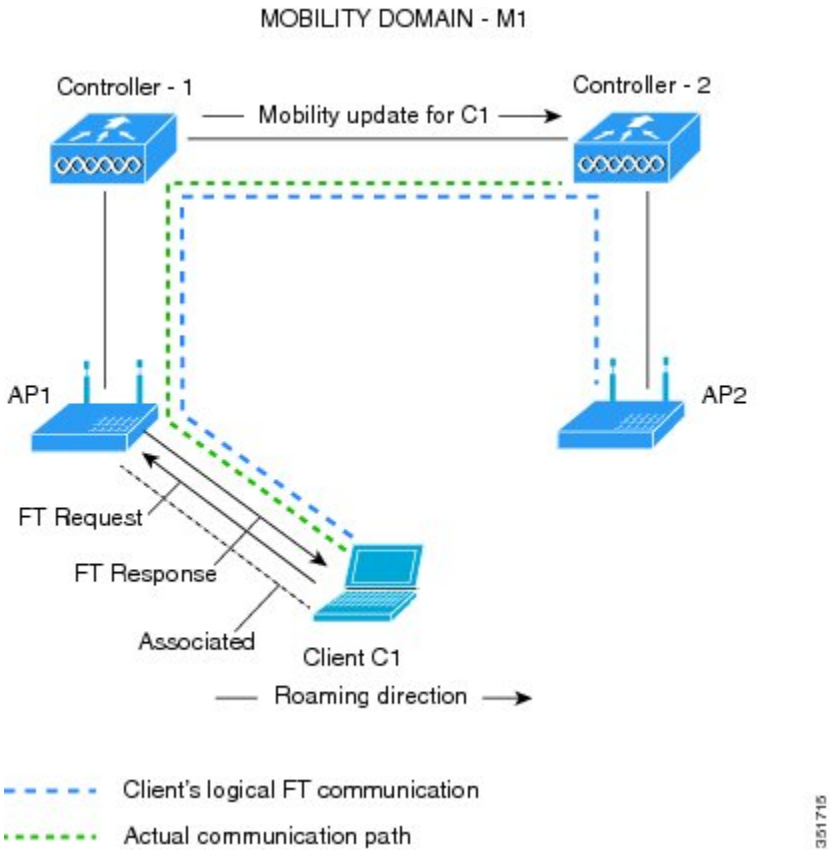
この図は、Over the Air クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

図 *102*：*Over the Air* クライアントのローミングの設定時にメッセージが交換されます



この図は、Over the DS クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

図 *103* : ***Over the DS*** クライアントのローミングの設定時にメッセージが交換されます



関連トピック

オープン WLAN での 802.11r 高速移行の設定（CLI），（2576 ページ）

802.11r 高速移行のディセーブル（CLI），（2581 ページ）

Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI），（2578 ページ）

PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI），（2579 ページ）

802.11r 高速移行の監視（CLI），（2582 ページ）

802.11r 高速移行の制約事項，（2571 ページ）

802.11r 高速移行を設定する方法

オープン WLAN での 802.11r 高速移行の設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client vlan** *vlan-id*
4. **no security wpa**
5. **no security wpa akm dot1x**
6. **no security wpa wpa2**
7. **no wpa wpa2 ciphers aes**
8. **security ft**
9. **no shutdown**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーションサブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-id* 例： スイッチ(config-wlan)# **client vlan 0120**	WLAN にクライアント VLAN を関連付けます。
ステップ 4	**no security wpa** 例： スイッチ(config-wlan)# **no security wpa**	WPA セキュリティをディセーブルにします。
ステップ 5	**no security wpa akm dot1x** 例： スイッチ(config-wlan)# **no security wpa akm dot1x**	dot1x に対して AKM セキュリティをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**no security wpa wpa2** 例： スイッチ(config-wlan)# **no security wpa wpa2**	WPA2 セキュリティを無効にします。
ステップ 7	**no wpa wpa2 ciphers aes** 例： スイッチ(config-wlan)# **no security wpa wpa2 ciphers aes**	AES の WPA2 暗号化をディセーブルにします。
ステップ 8	**security ft** 例： スイッチ(config-wlan)# **security ft**	802.11r 高速移行パラメータを指定します。
ステップ 9	**no shutdown** 例： スイッチ(config-wlan)# **shutdown**	WLAN を停止します。
ステップ 10	**end** 例： スイッチ(config-wlan)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11r の高速移行について，（2572 ページ）
802.11r 高速移行の監視（CLI），（2582 ページ）
802.11r 高速移行の制約事項，（2571 ページ）

Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client vlan** *vlan-name*
4. **local-auth** *local-auth-profile-eap*
5. **security dot1x authentication-list default**
6. **security ft**
7. **security wpa akm ft dot1x**
8. **no shutdown**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-name* 例： スイッチ(config-wlan)# **client vlan 0120**	この WLAN にクライアント VLAN を関連付けます。
ステップ 4	**local-auth** *local-auth-profile-eap* 例： スイッチ(config-wlan)# **local-auth**	local auth EAP プロファイルをイネーブルにします。
ステップ 5	**security dot1x authentication-list default** 例： スイッチ(config-wlan)# **security dot1x authentication-list default**	dot1x セキュリティ用のセキュリティ認証リストをイネーブルにします。この設定は、dot1x セキュリティ WLAN に似ています。
ステップ 6	**security ft** 例： スイッチ(config-wlan)# **security ft**	WLAN 上で 802.11r 高速移行をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**security wpa akm ft dot1x** 例： スイッチ(config-wlan)# **security wpa akm ft dot1x**	WLAN 上で 802.1x セキュリティをイネーブルにします。
ステップ 8	**no shutdown** 例： スイッチ(config-wlan)# **no shutdown**	WLAN をイネーブルにします。
ステップ 9	**end** 例： スイッチ(config-wlan)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11r の高速移行について，（2572 ページ）
802.11r 高速移行の監視（CLI），（2582 ページ）
802.11r 高速移行の制約事項，（2571 ページ）

PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client vlan** *vlan-name*
4. **no security wpa akm dot1x**
5. **security wpa akm ft psk**
6. **security wpa akm psk set-key** {**ascii** {**0** | **8**} | **hex** {**0** | **8**}}
7. **security ft**
8. **no shutdown**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： スイッチ# **wlan test4**	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-name* 例： スイッチ(config-wlan)# **client vlan 0120**	この WLAN にクライアント VLAN を関連付けます。
ステップ 4	**no security wpa akm dot1x** 例： スイッチ(config-wlan)# **no security wpa akm dot1x**	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**security wpa akm ft psk** 例： スイッチ(config-wlan)# **security wpa akm ft psk**	FT PSK サポートを設定します。
ステップ 6	**security wpa akm psk set-key {ascii {0 | 8} | hex {0 | 8}}** 例： スイッチ(config-wlan)# **security wpa akm psk set-key ascii 0 test**	PSK AKM の共有キーを設定します。
ステップ 7	**security ft** 例： スイッチ(config-wlan)# **security ft**	802.11r 高速移行を設定します。
ステップ 8	**no shutdown** 例： スイッチ(config-wlan)# **no shutdown**	WLAN をイネーブルにします。
ステップ 9	**end** 例： スイッチ(config-wlan)# **end**	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11r の高速移行について，（2572 ページ）

802.11r 高速移行の監視（CLI），（2582 ページ）

802.11r 高速移行の制約事項，（2571 ページ）

802.11r 高速移行のディセーブル（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `スイッチ# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*] 例： `スイッチ(config-wlan)# no security ft over-the-ds`	WLAN の 802.11r 高速移行をディセーブルにします。 （注） データ ソースに対して 802.11r 高速移行をディセーブルにすると、Over the Air の高速移行がイネーブルになります。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11r の高速移行について，（2572 ページ）

802.11r 高速移行の監視（CLI），（2582 ページ）

802.11r 高速移行の制約事項, （2571 ページ）

802.11r 高速移行の監視（GUI）

クライアントの認証キー管理の詳細情報を表示できます。

[Monitor] > [Client] を選択します。[Clients] ページが表示されます。クライアントの詳細を表示するには、該当するクライアントを選択します。[General] タブで、FT、PSK、802.1X、CCKM、802.1x＋CCKM など、クライアントの認証キー管理を確認できます。 AKM が 802.11r 混合モード用の場合、FT-802.1x、FT-802.1x-CCKM、または FT-PSK が表示されます。

802.11r 高速移行の監視（CLI）

次のコマンドを使用して、802.11r の高速移行を監視できます。

コマンド	説明
showwlanname*wlan-name*	WLANに設定されているパラメータの要約を表示します。

コマンド	説明

showwirelessclientmac-address*mac-address*	クライアントの 802.11r 認証キー管理の設定の概要を表示します。
	
	. . .
	. . .
	Client Capabilities
	  CF Pollable : Not implemented
	  CF Poll Request : Not implemented
	  Short Preamble : Not implemented
	  PBCC : Not implemented
	  Channel Agility : Not implemented
	  Listen Interval : 15
	  Fast BSS Transition : Implemented
	Fast BSS Transition Details :
	Client Statistics:
	  Number of Bytes Received : 9019
	  Number of Bytes Sent : 3765
	  Number of Packets Received : 130
	  Number of Packets Sent : 36
	  Number of EAP Id Request Msg Timeouts : 0
	  Number of EAP Request Msg Timeouts : 0
	  Number of EAP Key Msg Timeouts : 0
	  Number of Data Retries : 1
	  Number of RTS Retries : 0
	  Number of Duplicate Received Packets : 1
	  Number of Decrypt Failed Packets : 0
	  Number of Mic Failured Packets : 0
	  Number of Mic Missing Packets : 0
	  Number of Policy Errors : 0
	  Radio Signal Strength Indicator : -48 dBm
	  Signal to Noise Ratio : 40 dB
	. . .
	. . .
	
	クライアントの AKM が 802.11r 混合モードの場合、次の情報が出力に表示されます。
	
	. . .
	. . .
	Authentication Key Management : FT-PSK
	. . .
	. . .

関連トピック

オープン WLAN での 802.11r 高速移行の設定（CLI），（2576 ページ）

802.11r 高速移行のディセーブル（CLI），（2581 ページ）

Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI），（2578 ページ）

PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI），（2579 ページ）

802.11r の高速移行について，（2572 ページ）

802.11r 高速移行に関する追加情報

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
IEEE 802.11r。	802.11r 用の IEEE 規格

MIB

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

シスコのテクニカル サポート

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

802.11r 高速移行の機能に関する情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
802.11r の高速移行	Cisco IOS XE 3.3SE	この機能が導入されました。

第 117 章

経由ローミングの設定

- 機能情報の確認，2587 ページ
- 経由ローミングの制約事項，2587 ページ
- 経由ローミングについて，2588 ページ
- 経由ローミングの設定方法，2590 ページ
- 経由ローミングの監視，2591 ページ
- 経由ローミングの設定例，2592 ページ
- 経由ローミングに関する追加情報，2593 ページ
- 経由ローミング設定の機能履歴と情報，2594 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

経由ローミングの制約事項

- 経由ローミング機能は、複数のスイッチでサポートされます。

- この機能は、802.11n 対応の屋内アクセス ポイントでのみサポートされています。 シングル バンド構成の場合は、最大 6 つのネイバーがネイバー リストに表示されます。デュアル バンド構成の場合、最大 12 のネイバーが表示されます。
- スイッチ CLI をのみを使用して経由ローミングを設定できます。

関連トピック

経由ローミングについて，（2588 ページ）

経由ローミングの設定（CLI），（2590 ページ）

経由ローミングについて

802.11k 標準では、クライアントがサービス セットの移行の候補となる既知のネイバー アクセス ポイントに関する情報を含むネイバー レポートを要求することができます。802.11k ネイバー リストを使用すると、アクティブおよびパッシブ スキャンの必要性を軽減できます。

経由ローミング機能は、インテリジェントでクライアントによって最適化されたネイバー リストに基づいています。

Cisco Client Extension（CCX）ネイバー リストとは異なり、802.11k ネイバー リストは動的かつオンデマンドで生成されます。スイッチ上では維持されません。802.11k ネイバー リストは、クライアントのロケーションに基づくもので、Mobility Services Engine (MSE) を必要としません。同じスイッチ上であっても異なる AP の 2 クライアントが、周囲の AP の個々の関係に応じて提供される異なるネイバー リストを設定できます。

デフォルトでは、ネイバー リストには、クライアントがアソシエートされている同じ帯域のネイバーだけが含まれます。ただし、両方の帯域のネイバーを返すために、802.11k を可能にするスイッチが存在します。

クライアントは、ビーコン内の RRM（無線リソース管理）機能の情報要素（IE）をアドバタイズする AP に関連付けた後でのみ、ネイバー リストの要求を送信します。ネイバー リストには、隣接する無線の BSSID、チャネル、および処理の詳細についての情報が含まれます。

ネイバー リストの作成と最適化

802.11k ネイバー リスト要求をスイッチが受信すると、次の処理が実行されます。

1. スイッチは、クライアントが現在関連付けられている AP と同じ帯域で、ネイバー リストについて RRM ネイバー テーブルを検索バンドします。
2. スイッチは、帯域ごとにネイバー リストを 6 つに削減するために、AP 間の RSSI（Received Signal Strength Indication）、現在の AP の現在のロケーション、Cisco Prime インフラストラクチャからのネイバー AP のフロア情報、スイッチ上でのローミング履歴情報に従ってネイバーをチェックします。このリストは、同じフロアの AP に対して最適化されています。

非 802.11k クライアントの経由ローミング

非 802.11k クライアントのローミングを最適化することもできます。クライアントが 802.11k ネイバーリスト要求を送信する必要なく、各クライアントの予測ネイバーリストを生成できます。成功した各クライアント アソシエーション/再アソシエーションの後、WLAN でこれが有効である場合、ネイバー リストを生成し、モバイル ステーションのソフトウェア データ構造にリストを格納するために、同じネイバー リストの最適化を非 802.11k クライアントに適用する必要があります。クライアント プローブが異なるネイバーによって異なる RSSI 値により認識されるため、異なるロケーションのクライアントが異なるリストを持ちます。クライアントは、通常はアソシエーションまたは再アソシエーションの前にプローブするため、このリストは、更新されたほとんどのプローブ データによって構築され、クライアントがローミングする可能性が高い次の AP を予測します。

AP へのアソシエーション要求が保存された予測ネイバーリストのエントリに一致しない場合に、アソシエーションを拒否することによって、あまり望ましくないネイバーへのクライアントのローミングを抑止します。

アグレッシブ ロード バランシングに加えて、経由ローミング機能を毎 WLAN ごとおよびグローバルにオンにするスイッチがあります。次のオプションを使用できます。

- Denial count：クライアントでアソシエーションが拒否される最大回数です。
- Prediction threshold：経由ローミング機能をアクティブにするために、予測リスト内で必要なエントリの最小数です。

ロード バランシングおよび経由ローミングの両方で、クライアントがアソシエートする AP に影響を与えるように設計されているため、WLAN で両オプションを同時にイネーブルにすることはできません。

関連トピック

経由ローミングの設定（CLI），（2590 ページ）
経由ローミングの制約事項，（2587 ページ）
経由ローミングの監視，（2591 ページ）
経由ローミングの設定例，（2592 ページ）

経由ローミングの設定方法

経由ローミングの設定（CLI）

手順の概要

1. **configure terminal**
2. **wireless assisted-roaming floor-bias** *dBm*
3. **wlan** *wlan-id*
4. **assisted-roaming neighbor-list**
5. **assisted-roaming dual-list**
6. **assisted-roaming prediction**
7. **wireless assisted-roaming prediction-minimum** *count*
8. **wireless assisted-roaming denial-maximum** *count*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless assisted-roaming floor-bias** *dBm* 例： スイッチ(config)# **wireless assisted-roaming floor-bias 20**	ネイバー フロア ラベル バイアスを設定します。有効な範囲は –5 ～ 25 dBm で、デフォルト値は –15 dBm です。
ステップ 3	**wlan** *wlan-id* 例： スイッチ(config)# **wlan wlan1**	WLAN コンフィギュレーション サブモードを開始します。*wlan-name* は設定されている WLAN のプロファイル名です。
ステップ 4	**assisted-roaming neighbor-list** 例： スイッチ(wlan)# **assisted-roaming neighbor-list**	WLAN の 802.11k ネイバー リストを設定します。WLAN を作成すると、デフォルトでネイバー リストで経由ローミングがイネーブルになります。コマンドの **no** 形式では、経由ローミングのネイバー リストが無効になります。

	コマンドまたはアクション	目的
ステップ 5	**assisted-roaming dual-list** 例： スイッチ(wlan)# **assisted-roaming dual-list**	WLAN のデュアル バンド 802.11k デュアル リストを設定します。WLAN を作成すると、デフォルトでデュアル リストで経由ローミングがイネーブルになります。コマンドの **no** 形式では、経由ローミングのデュアル リストが無効になります。
ステップ 6	**assisted-roaming prediction** 例： スイッチ(wlan)# **assisted-roaming prediction**	WLAN の経由ローミング予測リスト機能を設定します。デフォルトでは、経由ローミング予測リストはディセーブルです。 （注） ロード バランシングが WLAN に対してすでにイネーブルである場合、警告メッセージが表示され、ロード バランシングが WLAN に対してディセーブルになります。
ステップ 7	**wireless assisted-roaming prediction-minimum** *count* 例： スイッチ# **wireless assisted-roaming prediction-minimum**	予測リスト機能が動作するために必要な予測 AP の最小数を設定します。デフォルト値は 3 です。 （注） クライアントに割り当てられた Forecast、AP が指定した数よりもこの値が小さい場合、経由ローミング機能はこのルールに適用されません。
ステップ 8	**wireless assisted-roaming denial-maximum** *count* 例： スイッチ# **wireless assisted-roaming denial-maximum 8**	AP に送信されたアソシエーション要求が予測の AP に一致しない場合に、クライアントでアソシエーションを拒否できる最大回数を設定します。有効な範囲は 1 ～ 10 で、デフォルト値は 5 です。
ステップ 9	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

経由ローミングについて，（2588 ページ）
経由ローミングの制約事項，（2587 ページ）
経由ローミングの監視，（2591 ページ）
経由ローミングの設定例，（2592 ページ）

経由ローミングの監視

WLAN に設定された経由ローミングを監視するために次のコマンドが使用できます。.

コマンド	説明
show wlan id *wlan-id*	WLAN の WLAN パラメータを表示します。

関連トピック

経由ローミングについて，（2588 ページ）
経由ローミングの設定（CLI），（2590 ページ）

経由ローミングの設定例

次に、ネイバー フロア ラベル バイアスを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wireless assisted-roaming floor-bias 10
スイッチ(config)# end
スイッチ# show wlan id 23
```

次に、特定の WLAN のネイバー リストをディセーブルにする例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wlan test1
スイッチ(config (wlan)# no assisted-roaming neighbor-list
スイッチ(config)(wlan)# end
スイッチ# show wlan id 23
```

次に、特定の WLAN の予測リストを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wlan test1
スイッチ(config)(wlan)# assisted-roaming prediction
スイッチ(config)(wlan)# end
スイッチ# show wlan id 23
```

次に、特定のWLANの経由ローミングの予測しきい値および最大の拒否数に基づいて予測リストを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# wireless assisted-roaming prediction-minimum 4
スイッチ(config)# wireless assisted-roaming denial-maximum 4
スイッチ(config)(wlan)# end
スイッチ# show wlan id 23
```

関連トピック

経由ローミングについて，（2588 ページ）
経由ローミングの設定（CLI），（2590 ページ）

経由ローミングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

標準および RFC

標準/RFC	タイトル
802.11k	—

MIB

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

シスコのテクニカル サポート

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

経由ローミング設定の機能履歴と情報

機能名	リリース	機能情報
経由ローミング	Cisco IOS XE 3.3SE	この機能が導入されました。

第 118 章

アクセス ポイント グループの設定

- 機能情報の確認，2595 ページ
- AP グループを設定するための前提条件，2595 ページ
- アクセス ポイント グループの設定に関する制約事項，2596 ページ
- アクセス ポイント グループについて，2596 ページ
- アクセス ポイント グループの設定方法，2597 ページ
- その他の参考資料，2600 ページ
- アクセス ポイント グループの機能履歴と情報，2601 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

AP グループを設定するための前提条件

次に、スイッチでアクセス ポイント グループを作成するための前提条件を示します。

- VLAN またはサブネットにサービスを提供するルータ上で、必要なアクセス コントロール リスト（ACL）を定義する必要があります。

- アクセス ポイント グループ VLAN では、マルチキャスト トラフィックがサポートされます。ただし、クライアントがあるアクセス ポイントから別のアクセス ポイントにローミングする場合、IGMP スヌーピングが有効になっていないと、クライアントによってマルチキャスト トラフィックの受信が停止されることがあります。

関連トピック

アクセス ポイント グループについて, （2596 ページ）
アクセス ポイント グループの設定に関する制約事項, （2596 ページ）

アクセス ポイント グループの設定に関する制約事項

- AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN インターフェイスと同じであるとします。WLAN インターフェイスが変更されると、AP グループ テーブル内の WLAN に対するインターフェイス マッピングも新しい WLAN インターフェイスに変わります。

  AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN に定義されたインターフェイスと異なるとします。WLAN インターフェイスが変更されても、AP グループ テーブル内の WLAN に対するインターフェイス マッピングは新しい WLAN インターフェイスに変わりません。

- スイッチ上の設定をクリアすると、アクセス ポイント グループのすべてが非表示となります。ただし、デフォルトのアクセス ポイント グループである「default-group」（自動的に作成される）は例外です。

- デフォルトのアクセス ポイント グループには、最大 16 の WLAN を関連付けることができます。デフォルトのアクセス ポイント グループの WLAN ID は、16 以下である必要があります。大規模なデフォルトのアクセス ポイント グループ内で ID が 16 以上の WLAN が作成されると、WLAN SSID はブロードキャストされません。デフォルトのアクセス ポイント グループのすべての WLAN ID で ID が 16 以下であることが必要です。16 を超える ID を含む WLAN は、カスタム アクセス ポイント グループに割り当てることができます。

- 同じ AP グループと同じ FlexConnect グループに属しているメッシュ ツリー（同じセクター）内のすべての フレックス + ブリッジ AP は WLAN-VLAN マッピングを正しく継承するように設定することをお勧めします。

関連トピック

アクセス ポイント グループについて, （2596 ページ）
AP グループを設定するための前提条件, （2595 ページ）

アクセス ポイント グループについて

スイッチ上に最大 512 の WLAN を作成した後では、さまざまなアクセス ポイントに WLAN を選択的に公開（アクセス ポイント グループを使用して）することで、ワイヤレス ネットワークを

より適切に管理できます。一般的な展開では、WLAN 上のすべてのユーザはスイッチ上の 1 つのインターフェイスにマップされます。したがって、WLAN に関連付けられているすべてのユーザは、同じサブネットまたは VLAN に存在します。しかし、複数のインターフェイス間で負荷を分散すること、またはアクセスポイントグループを作成して、個々の部門（たとえばマーケティング部門）などの特定の条件に基づくグループユーザへと負荷を分配することを選択できます。さらに、ネットワーク管理を簡素化するために、これらのアクセスポイントグループを別個の VLAN で設定できます。

関連トピック

アクセス ポイント グループの作成, （2597 ページ）
アクセス ポイント グループの表示, （2599 ページ）
AP グループへのアクセス ポイントの割り当て, （2598 ページ）
AP グループを設定するための前提条件, （2595 ページ）
アクセス ポイント グループの設定に関する制約事項, （2596 ページ）

アクセス ポイント グループの設定方法

アクセス ポイント グループの作成

はじめる前に

この操作を実行するには、管理者特権が必要です。

手順の概要

1. **configure terminal**
2. **ap group** *ap-group-name*
3. **wlan** *wlan-name*
4. （任意） **vlan** *vlan-name*
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ap group** *ap-group-name* 例： スイッチ(config)# **ap group my-ap-group**	アクセス ポイント グループを作成します。
ステップ 3	**wlan** *wlan-name* 例： スイッチ(config-apgroup)# **wlan wlan-name**	WLAN に AP グループを関連付けます。
ステップ 4	**vlan** *vlan-name* 例： スイッチ(config-apgroup)# **vlan test-vlan**	（任意） VLAN にアクセス ポイント グループを割り当てます。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

次に、AP グループを作成する例を示します。

```
スイッチ# configure terminal
スイッチ(config-apgroup)# ap group test-ap-group-16
スイッチ(config-wlan-apgroup)# wlan test-ap-group-16
スイッチ(config-wlan-apgroup)# vlan VLAN1300
```

関連トピック

アクセス ポイント グループについて，（2596 ページ）

AP グループへのアクセス ポイントの割り当て

はじめる前に

この操作を実行するには、管理者特権が必要です。

手順の概要

1. **ap name** *ap-name* **ap-group-name** *ap-group*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name* **ap-group-name** *ap-group* 例： スイッチ# **ap name 1240-101 ap-groupname apgroup_16**	アクセス ポイント グループにアクセス ポイントを割り当てます。次のキーワードと引数があります。 • **name**：このキーワードに続く引数が、スイッチと関連付けられた AP の名前となるように指定します。 • *ap-name*：AP グループに関連付けたい AP。 • **ap-group-name**：このキーワードに続く引数が、スイッチで設定された AP グループの名前となるように指定します。 • *ap-group*：スイッチで設定されたアクセス ポイント グループの名前。

関連トピック

アクセス ポイント グループについて，（2596 ページ）

アクセス ポイント グループの表示

はじめる前に

この操作を実行するには、管理者特権が必要です。

手順の概要

1. **show ap groups** [**extended**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ap groups** [**extended**] 例： スイッチ# **show ap groups**	スイッチで設定された AP グループを表示します。**extended** キーワードは、システムで詳細に定義されているすべての AP グループ情報を表示します。

関連トピック

アクセス ポイント グループについて，（2596 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
WLAN コマンド	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
Lightweightアクセス ポイント コンフィギュレーション	*Lightweight Access Point Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
Lightweight アクセス ポイント コマンド	*Lightweight Access Point Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

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

MIB

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

シスコのテクニカル サポート

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

アクセス ポイント グループの機能履歴と情報

次の表で、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
AP グループ数	Cisco IOS XE 3.3SE	この機能が導入されました。

索 引

数字

128 ビット 180
802.11h、説明 2067
802.11n 2067
  devices 2067
802.1x 1539

A

AAA サーバ グループの定義 1370
AAA でのローカル モード 1395
ABR 1153
ACE 1440
  IP 1440
  イーサネット 1440
ACL 919, 1440, 1441, 1446, 1447, 1448, 1450, 1451, 1452, 1453, 1454, 1456, 1463, 1464, 1466, 1467, 1473, 1478, 1479, 1480, 1491, 1492, 1493
  interface 1453
  IP 1446, 1448, 1453, 1463
    undefined 1453
    マッチング基準 1446
    暗黙のマスク 1448
    暗黙的な拒否 1463
  IPv4 1446, 1447, 1453, 1466, 1467
    インターフェイス 1453
    インターフェイスへの適用 1467
    サポートされていない機能 1447
    マッチング基準 1446
    作成 1446
    数値 1447
    端末回線、設定する 1466
  port 1440
  QoS 919
  VLAN マップ 1450, 1473
    設定 1473
    設定時の注意事項 1450
  VLAN マップを ACL ルータと共に使用 1451
ACL (続き)
  コンパイル 1480
  サポートされていない機能 1447
    IPv4 1447
  サポートされるタイプ 1440
  の例 1480
  ハードウェアでのサポート 1450
  へのコメント 1479
  マッチング 1453
  モニタリング 1478
  ルータ 1440
  ルータ ACL と VLAN マップの設定時の注意事項 1452
  レイヤ 4 情報 1452
  ロギング メッセージ 1450
  拡張 IPv4 1446, 1456
    マッチング基準 1446
    作成 1456
  時間範囲 1452
  定義 1446
  適用 919, 1464, 1467, 1491, 1492, 1493
    ルーテッド パケットの 1492
    QoS に適応 919
    インターフェイスへの 1467
    スイッチド パケットの 1491
    ブリッジド パケット上の 1492
    マルチキャスト パケット上の 1493
    時間範囲 1464
  標準 IPv4 1446, 1454
    マッチング基準 1446
    作成 1454
  優先順位 1441
ACS 306
All APs ページ 1064
alternate 386
  port 386
AnchorTime パラメータ 1054
AP Mode パラメータ 1064

ARP 1124, 1126, 1962, 2326
table 1962
アドレス解決 1962
カプセル化 1126
スタティック キャッシュの設定 1124
定義 1962
AS パス フィルタ、BGP 1187
auto モード 140
auto-copy 1893
auto-extract を使用したアップグレード 1893
Auto-MDIX 89
設定 89
説明 89
Auto-MDIX コマンドの設定例 90
Auto-MDIX、設定する 89
auto-upgrade 1893
auto-upgrade を使用した自動アップグレード 1893
automatic 1538

B

BackboneFast 471, 484
イネーブル化 484
説明 471
bandwidth percent 930
Berkeley r-tool の置換 1405
BGP 1184, 1185, 1186, 1187, 1188, 1189, 1190, 1191, 1195, 1206, 1211, 1213
マルチパス サポート 1186
CIDR 1189
イネーブル化 1195
コミュニティ フィルタリング 1206
デフォルト設定 1191
ネイバー、タイプ 1184
バージョン 4 1184
パスの選択 1186
プレフィックス フィルタリング 1188
リセット セッション 1185
ルーティング ドメイン コンフェデレーション 1213
ルート マップ 1187
ルート リフレクタ 1190
集約アドレス 1211
説明 1184
bindings 1515, 1538
IP ソース ガード 1538
アドレス、Cisco IOS DHCP サーバ 1515
boot network コマンド 2235
BPDU 387, 436, 465
RSTP 形式 436
フィルタリング 465
内容 387

C

CA トラストポイント 1424, 1427
設定 1427
定義 1424
Call Admission Control（コール アドミッション制御） 979
CCX 613, 2510
リンク テスト 613
説明 2510
CCX レイヤ 2 クライアント ローミング 2096
説明 2096
CDP 102, 138, 937, 2326
LLDP での定義 102
および信頼境界 937
電力ネゴシエーションの拡張機能 138
CDP に対する電力ネゴシエーションの拡張機能 138
CEF 197, 1263
distributed 1263
IPv6 197
CEFv6 197
Change Rules Priority パラメータ 1856
Channel Assignment Leader パラメータ 1054
Channel Assignment Method パラメータ 1053
Channel Scan Duration パラメータ 1043
CipherSuite 1425
Cisco 3300 シリーズ Mobility Services Engine（MSE）、wIPS での使用 1864
Cisco 7960 IP フォン 2460
Cisco Discovery Protocol（CDP） 697
Cisco Express Forwarding; シスコ エクスプレス フォワーディング 1262
「CEF」を参照 1262
Cisco IOS DHCP サーバ 1515
DHCP、Cisco IOS DHCP サーバを参照 1515
Cisco IOS IP SLA 750
Cisco IP Phone のデータ トラフィック 2461
Cisco IP Phone の音声トラフィック 2460
Cisco Networking Service 674
Cisco インテリジェント電力管理 138
Cisco ワークグループ ブリッジ 593
Cisco 以外のワークグループ ブリッジ 593
CIST リージョナル ルート 425, 426
「MSTP」を参照 425, 426

CIST ルート 426
「MSTP」を参照 426
class 949
classification 916, 917, 919
デバイス固有 917
レイヤ 2 916
レイヤ 3 916
CleanAir 22
コンポーネント 22
CleanAir のイネーブル化 27, 31
2.4 GHz 27
5 GHz 31
CleanAir のモニタリング 39, 41
CLI の使用 39
GUI の使用 41
CLNS 1219
ISO CLNS を参照 1219
clock 1954
システム クロックを参照 1954
CNS 674
CoA 要求コマンド 1342
CONFIG_FILE 環境変数 2264
指定 2264
Control and Provisioning of Wireless Access Points プロトコル（CAPWAP） 549
説明 549
controllers 549, 554
AP パススルー 554
ディスカバリ プロセス 549
copy rcp running-config コマンド 2245, 2248
copy rcp startup-config コマンド 2245, 2248
copy rcp コマンド 2258
copy running-config rcp コマンド 2240
copy running-config tftp コマンド 2239
copy startup-config rcp コマンド 2240, 2242
copy startup-config tftp コマンド 2239
copy startup-config コマンド 2252
copy tftp startup-config コマンド 2244
CoS 914, 2465
プライオリティのオーバーライド 2465
レイヤ 2 フレーム 914
CoS/DSCP マップ、QoS での 940
Country Code 605
説明 605
Coverage Exception Level per AP パラメータ 1057
Customer Edge デバイス 1237

D

DCA Channel Sensitivity パラメータ 1054
DCA Channels パラメータ 1054
debug コマンドを使用 2329
debugging 2329, 2345, 2356
エラー メッセージ出力のリダイレクト 2345
コマンドを使用 2329
すべてのシステム診断のイネーブル 2356
DHCP 183, 1509, 1519
DHCP for IPv6 183
「DHCPv6」を参照 183
イネーブル化 1509, 1519
サーバ 1509
リレー エージェント 1519
DHCP for IPv6 183
「DHCPv6」を参照 183
DHCP Option 82 1512, 1521
ヘルパー アドレス 1521
概要 1512
転送アドレス、指定 1521
DHCP オプション 43 582
DHCP オプション 60 582
DHCP オプション 82 1528, 2530
説明 2530
表示 1528
例 2530
DHCP サーバ 2528
internal 2528
DHCP サーバ ポート ベースのアドレス割り当て 1529, 1532
イネーブル化 1532
デフォルト設定 1529
DHCP スヌーピング 1510, 1511, 1512, 1538
Option 82 データ挿入 1512
信頼できないメッセージ 1510
信頼できるインターフェイス 1510
非信頼パケット形式エッジ スイッチの受信 1511
DHCP スヌーピング バインディング データベース 1515, 1516, 1524, 1530
イネーブル化 1530
バインディング ファイル 1516
形式 1516
場所 1516
バインディングの追加 1530
設定 1530
設定時の注意事項 1524
説明 1515

DHCPv6 183, 207, 208, 210
クライアント機能のイネーブル化 210
設定時の注意事項 207
DHCPv6 サーバ機能のイネーブル化 208
デフォルト設定 207
説明 183
DHCPv6 クライアント機能のイネーブル化：コマンド例 213
DHCPv6 サーバ機能のイネーブル化 208
DHCPv6 サーバ機能のイネーブル化：コマンド例 213
Differentiated Services（Diff-Serv）アーキテクチャ 913
DiffServ コード ポイント 915
disabled 394
state 394
distribute-list コマンド 1284
DNS 181, 1959, 1960, 1970
IPv6 181
セットアップ 1970
デフォルト設定 1960
概要 1959
Domain Name System; ドメイン ネーム システム 1959
「DNS」を参照 1959
DRP 182, 195
IPv6 182
説明 182
設定 195
DSCP 915
DSCP マップ 940
DSCP/CoS マップ、QoS での 941
DTIM 2509
DTLS データ暗号化。「データ暗号化」を参照 558
DUAL 有限状態マシン、EIGRP 1171

E

EDRRM 26
EIGRP 184, 1169, 1170, 1172, 1177, 1179, 1181
インターフェイス パラメータ、設定 1177
コンポーネント 1170
スタブ ルーティング 184, 1172
モニタリング 1181
定義 1169
認証 1179
EIGRP IPv6 コマンド 184
ELIN ロケーション 104
Enable Coverage Hole Detection パラメータ 1057
enable secret 1299
Enhanced Interior Gateway Routing Protocol（EIGRP）
IPv6 184
EIGRP IPv6 コマンド 184
erase startup-config コマンド 2262
erase コマンド 2263
EtherChannel 494, 497, 499, 501, 502, 503, 504, 505, 508, 510, 513, 516, 518, 520, 521, 523, 524, 526, 527, 1117, 1539
IEEE:802.3ad、説明 502
LACP 503, 504, 523, 524, 526, 527
システム プライオリティ 526
ポート プライオリティ 527
ホット スタンバイ ポート 523
モード 503
最小リンク 524
最大バンドル 523
他の機能との相互作用 504
PAgP 499, 501, 502, 521
モード 499
学習方式およびプライオリティについて 501
学習方式とプライオリティの設定 521
集約ポート ラーナー 521
集約ポート ラーナーについて 501
説明 499
他の機能との相互作用 502
スタック変更、の影響 508
チャネル グループ 497
番号 497
物理および論理インターフェイスのバインド 497
デフォルト設定 508
ポートチャネル インターフェイス 497
番号 497
レイヤ 3 インターフェイス 1117
ロード バランシング 505, 518
拡張ロードバランシング 520
自動作成の 499, 502
設定 513, 516
レイヤ 2 インターフェイス 513
レイヤ 3 516
設定時の注意事項 510
相互作用 510
STP を使用 510
転送方式 505, 518, 520
論理インターフェイス、説明 497
EtherChannel | 相互作用 510
VLAN を使用 510
EtherChannel ガード 473, 485
イネーブル化 485
説明 473

EtherChannel コマンドの設定例 530
EtherChannel フェールオーバー 497
EUI 181
Expiration Timeout for Rogue AP and Rogue Client Entries パラメータ 1843
Extended Universal Identifier 181
「EUI」を参照 181

F

Fa0 ポート 94
イーサネット管理ポートを参照 94
FAQ 43
Fast Uplink Transition Protocol 469
fastethernet0 ポート 94
イーサネット管理ポートを参照 94
file system 2290, 2292, 2293, 2296
デフォルトの設定 2292
ネットワーク ファイル システム名 2296
ファイル情報の表示 2293
ローカル ファイル システム名 2290
使用可能なファイル システムの表示 2290
flash 2289
ファイルシステム 2289
FTP サーバ 2269
コンフィギュレーション ファイルのダウンロード 2269

G

General（controller）ページ 1047
RF グループの設定 1047
Group Mode パラメータ 1067

H

hello タイム 411, 451
MSTP 451
STP 411
HTTP over SSL 1423
「HTTPS」を参照 1423
HTTP セキュア サーバ 1423
HTTPS 1423, 1424, 1429
自己署名証明書 1424
設定 1429
説明 1423

I

IBPG 1182
ICMP 182, 1438, 2327
IPv6 182
traceroute 2327
時間超過メッセージ 2327
到達不能メッセージ 1438
ICMP PING 2325, 2343
概要 2325
実行 2343
ICMP Router Discovery Protocol 1130
「IRDP」を参照 1130
ICMP Router Discovery Protocol（IRDP） 1115, 1130
設定 1130
定義 1115
ICMP エコー動作 767
IP SLAs 767
設定 767
ICMPv6 182
IEEE 502
802.3ad、説明 502
IEEE 802.1Q タギング 2446
IEEE 802.1s 421
「MSTP」を参照 421
IEEE 802.3ad 502
「EtherChannel」を参照 502
IEEE 電力分類レベル 138
IGMP 172, 175
スヌーピング 175
レポート抑制 175
ディセーブル化 175
脱退処理、イネーブル化 172
IGMP スヌーピング 166, 167, 168, 175
イネーブル化またはディセーブル化 168
デフォルト設定 166, 167
モニタリング 175
Inter-Switch Link; スイッチ間リンク 790
「ISL」を参照 790
interface 132, 150
interference 1039
Interference threshold パラメータ 1043
Interior Gateway Protocol 1152
「IGP」を参照 1152
Interval パラメータ 1054
Invoke Channel Update Now ボタン 1053
Invoke Power Update Now ボタン 1049
IP ACL 919, 1449
QoS 分類 919

IP ACL *(続き)*
ネームド **1449**
IP precedence **915**
IP precedence/DSCP マップ、QoS での **941**
IP SLA **752, 754, 756, 757, 770**
しきい値監視 **754**
モニタリング **770**
レスポンダ **752, 757**
イネーブル化 **757**
説明 **752**
設定時の注意事項 **756**
IP SLAs **750, 751, 753, 754, 755, 756, 763, 767**
ICMP エコー動作 **767**
SNMP のサポート **751**
UDP ジッター動作 **755, 763**
サポートされるメトリック **750**
ネットワーク パフォーマンスの測定 **751**
応答時間 **753**
設定 **756**
複数動作のスケジューリング **754**
利点 **751**
IP traceroute **2327, 2344**
概要 **2327**
実行 **2344**
IP アドレス **180, 1118, 1120, 1139, 1962**
128 ビット **180**
IP ルーティング **1118**
IPv6 **180**
クラス **1120**
モニタリング **1139**
検出する **1962**
IP アドレスおよびサブネット **2326**
IP ソース ガード **1538, 1539, 1540, 1542**
802.1x **1539**
DHCP スヌーピング **1538**
EtherChannel **1539**
TCAM エントリ **1539**
VRF **1539**
イネーブル化 **1540, 1542**
スタティック バインディング **1540, 1542**
追加 **1540, 1542**
スタティック ホスト **1542**
トランク インターフェイス **1539**
バインディング コンフィギュレーション **1538**
automatic **1538**
manual **1538**
バインディング テーブル **1538**
ポート セキュリティ **1539**
IP ソース ガード *(続き)*
ルーテッド ポート **1539**
設定時の注意事項 **1539**
説明 **1538**
IP ダイレクト ブロードキャスト **1133**
IP ブロードキャスト アドレス **1136**
IP ホスト ping コマンド例 **2354**
IP ホストに対する traceroute 実行コマンド例 **2355**
IP ユニキャスト ルーティング **181, 1109, 1110, 1112, 1114, 1115, 1116, 1117, 1118, 1120, 1122, 1129, 1133, 1136, 1140, 1261, 1266, 1269, 1270, 1282, 1285, 1286**
unicast Reverse Path Forwarding **1261**
プロトコル **1110**
ディスタンス ベクトル **1110**
broadcast **1116, 1136**
address **1136**
ストーム **1116**
パケット **1116**
フラッディング **1116**
directed ブロードキャスト **1133**
EtherChannel レイヤ 3 インターフェイス **1117**
ICMP Router Discovery Protocol（IRDP） **1115**
IP アドレッシング **1118, 1120**
classes **1120**
設定 **1118**
IPv6 **181**
MAC アドレスと IP アドレス **1114**
RIP を参照してください [IP ユニキャスト ルーティング **1110**
zzz] **1110**
SVI を使用 **1117**
VLAN 間 **1109**
アドミニストレーティブ ディスタンス **1285**
イネーブル化 **1140**
クラスレス ルーティング **1112**
サブネット ゼロ **1122**
サブネット マスク **1120**
スタティック ルーティング **1109**
スタティック ルートの設定 **1266**
ダイナミック ルーティング **1110**
デフォルト **1109, 1129, 1269**
ゲートウェイ **1129**
ネットワーク **1269**
ルーティング **1109**
ルート **1269**
プロキシ ARP **1114**
プロトコル **1110**
リンクステート **1110**

IP ユニキャスト ルーティング *(続き)*
ルーテッド ポート 1117
レイヤ 3 インターフェイス 1117
再配布 1270
受動インターフェイス 1282
設定手順 1118
認証キー 1286
IP ルーティング 1140
イネーブル化 1140
IP 電話 937
QoS によるポート セキュリティの保証 937
信頼される境界、QoS の 937
IPv4 ACL 1453, 1454, 1456, 1460, 1467
インターフェイス 1453
インターフェイスへの適用 1467
ネームド 1460
拡張、作成 1456
標準、作成 1454
IPv4 アドレスと IPv6 アドレスの割り当て 192
IPv4 および IPv6 プロトコル スタックの設定：コマンド例 212
IPv6 161, 180, 181, 182, 183, 184, 186, 187, 188, 197, 206, 903
CEFv6 197
Enhanced Interior Gateway Routing Protocol（EIGRP）
IPv6 184
EIGRP IPv6 コマンド 184
ICMP 182
OSPF 184
SDM テンプレート 161
アドレス 180
アドレスの割り当て 188
アドレス形式 180
アプリケーション 183
サポートされない機能 186
サポートされる機能 181
スイッチの制限 187
スタック マスターは、次に示す機能を実行します。 187
スタティック ルートの概要 183
ステートレス自動設定 182
デフォルト ルータ プリファレンス（DRP） 182
デフォルト設定 188
とスイッチ スタック 187
ネイバー探索 182
パス MTU 検出 181
フォワーディング 188
モニタリング 206
機能の制限 187
自動設定 182
IPv6 *(続き)*
定義 180
IPv6 ICMP レート制限の設定：コマンド例 214
IPv6 アドレスの割り当て 188
IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化：コマンド例 212
IPv6 によるSNMP と Syslog 185
IPv6 の RIP の設定：コマンド例 214
IPv6 のスタティック ルーティングの設定：コマンド例 214
IPv6 の場合 183, 184
IPv6 の表示：コマンド例 214
IPv6 ルーティング 187
IPv6 上の HTTP（S） 186
IS-IS 1220
エリア ルーティング 1220
システム ルーティング 1220
ISL 181
および IPv6 181
ISO CLNS 1219, 1220
OSI 標準 1219
ダイナミック ルーティング プロトコル 1220

K

KDC 1388, 1392
「Kerberos」も参照 1388
zzz] 1388
説明 1388
Kerberos 1388, 1391, 1392, 1393
KDC 1388
TGT 1388
クレデンシャル 1388
ご利用条件 1388
サーバ 1388
チケット 1388
レルム 1388
信頼済みサード パーティとしてのスイッチ 1388
設定 1393
設定例 1388
説明 1388
動作 1391
認証 1392
KDC 1392
ネットワーク サービス 1392
境界スイッチ 1392

L

LACP 495, 503, 504, 513, 523, 524, 526, 527
  システム プライオリティ 526
  ポート プライオリティ 527
  ホット スタンバイ ポート 523
  モード 503
  最小リンク 524
  最大バンドル 523
  他の機能との相互作用 504
LACP ホット スタンバイ ポートの設定：例 531
Layer 4（レイヤ 4） 916
lightweight モード、自律モードへの復帰 582
Lightweight モードに変換される Autonomous アクセス ポイント 582
Link Latency 612
LLDP 102, 105, 107, 108
  送信タイマーとホールドタイム、設定 108
  イネーブル化 107
  スイッチ スタックの考慮事項 102
  概要 102
  設定 105
    デフォルト設定 105
LLDP-MED 103, 111
  サポートされている TLV 103
  概要 103
  設定 111
    TLV 111
login 1324, 1367
LWAPP-enabled アクセス ポイント 583, 585
  クラッシュ情報のコントローラへの送信 583
  自律モードへの復帰 585

M

MAC アドレス 1114, 1897, 1961, 1962, 1975, 1984
  dynamic 1961
    ラーニング 1961
  IP アドレス アソシエーション 1114
  VLAN の関連付け 1961
  アドレス テーブルの構築 1961
  エージング時間 1975
  デフォルト設定 1962
  検出する 1962
  静的 1984
    特性 1984
MAC アドレスおよび VLAN 2326
MAC 拡張アクセス リスト 1439, 1471
  レイヤ 2 インターフェイスに適用 1439, 1471
MAC/PHY コンフィギュレーション ステータス TLV 102
manual 1538
maximum-paths コマンド 1265
member number 1899
merged 1883
Min Failed Client Count per AP パラメータ 1057
MLD クエリー 163
MLD スヌーピング 162
MLD スヌーピング クエリー コマンドの設定例 177
MLD スヌーピング クエリーの設定：コマンド例 177
MLD メッセージ 163
MLD レポート 165
MLD 即時脱退のイネーブル化：コマンド例 177
MLDv1 Done メッセージ 165
Modular QoS CLI 915
MQC 902
MSDP 1080
  概要 1080
MSDP コマンドの設定例 1105
MSDP ピアからの送信元情報の要求：コマンド例 1105
MST モード 2438
MSTP 397, 420, 422, 423, 424, 425, 426, 428, 429, 430, 432, 439, 440, 441, 443, 444, 446, 448, 449, 451, 452, 454, 455, 456, 457, 459, 463, 464, 465, 473, 474, 475, 477, 479, 485, 486, 488
  設定 440, 443, 444, 446, 448, 449, 451, 452, 454, 455, 456, 457
    ネイバー タイプ 457
  BPDU ガード 464, 477
    イネーブル化 477
    説明 464
  BPDU フィルタリング 465, 479
    イネーブル化 479
    説明 465
  CIST リージョナル ルート 425, 426
  CIST ルート 426
  CIST、説明 425
  CST 426
    領域間の動作 426
  EtherChannel ガード 473, 485
    イネーブル化 485
    説明 473
  IEEE 802.1D との相互運用性 432, 459
    移行プロセスの再開 459
    説明 432
  IEEE 802.1s 426, 430
    ポートの役割名の変更 430
    実装 430

MSTP *(続き)*
IEEE 802.1s *(続き)*
用語 426
IST 425
領域内の動作 425
MST 領域 424, 425, 428, 440
CIST 425
IST 424
サポートされるスパニングツリーインスタンス 424
ホップ カウント メカニズム 428
設定 440
説明 424
PortFast 463, 475
イネーブル化 475
説明 463
PortFast 対応ポートのシャットダウン 464
VLAN から MST インスタンスへのマッピング 441
インターフェイス ステート、ブロッキングからフォワーディングへ 463
サポートされるインスタンス 397
スタック変更、の影響 432
デフォルト設定 439
モードのイネーブル化 440
モード間の相互運用性と互換性 397, 420
ルート ガード 474, 486
イネーブル化 486
説明 474
ルート スイッチ選択の防止 474
ルート デバイス 423
拡張システム ID の影響 423
設定 423
予期しない動作 423
ループ ガード 475, 488
イネーブル化 488
説明 475
拡張システム ID 423, 444
セカンダリ ルート デバイスに対する効果 444
ルート デバイスに対する効果 423
予期しない動作 423
境界ポート 420, 429
設定時の注意事項 420
説明 429
設定 440, 443, 444, 446, 448, 449, 451, 452, 454, 455, 456, 457
hello タイム 451
MST 領域 440
セカンダリ ルート デバイス 444
デバイス プライオリティ 449
パス コスト 448
MSTP *(続き)*
設定 *(続き)*
ポート プライオリティ 446
ルート デバイス 443
高速コンバージェンスのリンク タイプ 456
最大エージング タイム 454
最大ホップ カウント 455
転送遅延時間 452
設定時の注意事項 422
MTU 125
system 125

N

Neighbor Packet Frequency パラメータ 1043
Network Assistant 1896
スイッチ スタックの管理 1896
Network Mobility Services Protocol（NMSP） 2179
クライアント、RFID タグ、および不正デバイスの通知間隔の変更 2179
NSAP、ISO IGRP アドレスとして 1220
NSF 認識 1221
IS-IS 1221
NTP 1954, 1957
time 1957
services 1957
アソシエーション 1957
定義 1957
概要 1954
NVRAM 2250
ファイル圧縮 2250

O

OBFL 2331, 2346, 2347
設定 2346
説明 2331
表示 2347
OSPF 184, 1154, 1155, 1156, 1158, 1168
LSA グループ ペーシング 1155
IPv6 の場合 184
エリア パラメータ、設定 1154
デフォルト設定 1155
メトリック 1155
ルート 1155
モニタリング 1168
ルータ ID 1156

OSPF *(続き)*
ルート集約 **1154**
仮想リンク **1154**
設定 **1158**

P

PaGP **495**
PAgP **499, 502, 513, 521**
「EtherChannel」を参照 **499**
モード **499**
学習方式とプライオリティの設定 **521**
集約ポート ラーナー **521**
説明 **499**
他の機能との相互作用 **502**
password **2381**
PBR **1277, 1281**
ローカル ポリシーベース ルーティング **1281**
高速スイッチングされたポリシーベース ルーティング **1281**
定義 **1277**
ping **2325, 2343, 2354**
概要 **2325**
実行 **2343**
文字出力の説明 **2354**
ping リンク テスト **612**
ping を使用 **2325**
PoE **54, 137, 138, 140, 141, 146**
auto モード **140**
CDP に対する電力ネゴシエーションの拡張機能 **138**
Cisco インテリジェント電力管理 **138**
IEEE 電力分類レベル **138**
サポートされているデバイス **54, 137**
サポートされる標準 **138**
サポートしているポート単位のワット数 **54, 137**
スタティック モード **140**
モニタリング **141**
受電装置の検出および初期電力割り当て **138**
消費電力のポリシング **141**
低電力モードで動作する高電力装置 **138**
電力ネゴシエーションを伴う CDP、説明 **138**
電力のモニタ **146**
電力管理モード **140**
電力消費のポリシング **146**
電力消費を伴う CDP、説明 **138**
PoE ポート **2324**
police **989**
port **387, 394**
priority **387**
root **394**
Power Neighbor Count パラメータ **1050**
Power Threshold パラメータ **1050**
priority **992, 2465**
CoS の無効化 **2465**
priority value **1901**
Protection Type パラメータ **1064**
PVST モード **2438**
PVST+ **396, 397, 398**
IEEE 802.1Q トランキングの相互運用性 **398**
サポートされるインスタンス **397**
説明 **396**

Q

QoS **915, 918, 919, 920, 921, 923, 930, 931, 937, 940, 941, 968, 972, 995, 2124**
classification **915, 918, 919, 920**
IP ACL、説明 **919**
MAC ACL、説明 **919**
クラス マップ、説明 **920**
定義 **918**
転送処理 **915**
IP 電話 **937**
検出と信頼済みの設定 **937**
インターフェイスに付加するポリシー **923**
キュー **930, 931, 995**
WTD、説明 **931**
ロケーション **930**
出力特性の設定 **995**
ポリサー **2124**
設定 **2124**
ポリシー マップ **921**
特性 **921**
物理ポートの非階層型 **921**
ポリシング **918, 919, 923**
トークンバケット アルゴリズム **923**
説明 **918, 919**
マーキング:説明 **918, 919**
マークされたアクション **2124**
マッピング テーブル **940, 941**
CoS/DSCP **940**
DSCP/CoS **941**
IP precedence/DSCP **941**
暗黙的な拒否 **920**

QoS *(続き)*
基本モデル 918, 919
出力ポート 919
入力ポート 918
出力キュー 919
説明 919
設定 968, 972, 995
ポリシー マップ、VLAN 972
出力キューの特性 995
物理ポートのポリシー マップ 968
QoS コンポーネント 900
QoS のクラス マップ 920
説明 920
QoS のポリシー マップ 921, 968, 972
SVI 972
設定 972
特性 921
物理ポートの非階層型 968
設定 968
QoS のマッピング テーブル 940, 941
設定 940, 941
CoS/DSCP 940
DSCP/CoS 941
IP precedence/DSCP 941
queue limit 998

R

RADIUS 1335, 1336, 1346, 1365, 1367, 1370, 1372, 1374, 1376, 1378, 1379
AAA サーバ グループの定義 1370
login 1367
キー 1365
サーバの指定 1365
デフォルト設定 1346
ネットワーク環境の提案 1335
ユーザによってアクセスされるサービスのトラッキング 1374
ユーザに対するサービスの制限 1372
概要 1335
設定 1365, 1367, 1372, 1374, 1376
アカウンティング 1374
許可 1372
通信、グローバル 1365, 1376
通信、サーバ単位 1365
認証 1367
複数の UDP ポート 1365
RADIUS *(続き)*
属性 1378, 1379
ベンダー固有 1378
ベンダー独自仕様 1379
動作 1336
RADIUS 許可の変更 1337
rcp（リモート コピー プロトコル） 2230
サーバ 2230
コンフィギュレーション ファイル 2230
references 1025
QoS 1025
Remote SPAN 794
RF グループ 1035, 1036, 1067
カスケード 1035
ステータスの監視 1067
GUI の使用 1067
ステータスの表示 1067
GUI の使用 1067
概要 1036
固定 1035
RF グループ モードの設定 1044
GUI の使用 1044
RF グループ リーダー 1034
説明 1034
RF グループ名 1036
説明 1036
RF-Network Name パラメータ 1047
RFC 1142, 1152, 1182, 1954
1058、RIP 1142
1163、BGP 1182
1267、BGP 1182
1305、NTP 1954
1587、NSSAs 1152
1771、BGP 1182
RFC 5176 規定 1339
RFID トラッキング 601
Right-To-Use 2041, 2042, 2043, 2044, 2046, 2047
AP-Count のアクティブ化 2047
イメージ ベースのライセンス 2043
スイッチ スタック 2044
ベース イメージのアクティブ化 2046
ライセンスの概要 2042
ライセンスの状態 2043
永久ライセンス 2042
制約事項 2041
評価ライセンス 2042
RIP 183, 1142, 1144, 1147, 1148
IPv6 の場合 183

RIP *(続き)*
サマリー アドレス 1148
スプリット ホライズン 1148
ホップ カウント 1142
設定 1144
説明 1142
認証 1147
RLDP「Rogue Location Discovery Protocol（RLDP）」を参照 1839
Rogue Detection パラメータ 1842
Rogue Location Discovery Protocol パラメータ 1843
Rogue Policies ページ 1842
role 386
port 386
root 386, 388
port 386
switch 386, 388
route-map コマンド 1280
rsh（リモート シェル） 2230
RSPAN 790, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 804, 814, 815, 818, 823
sessions 795, 814, 815, 818, 823
イネーブルにされた入力トラフィック 823
監視対象ポートの指定 814, 815
作成 814, 815
定義 795
特定の VLAN への送信元トラフィックの制限 818
VLAN ベース 798
およびスタックの変更 802
セッションの制限 790
デバイス スタック内 793
デフォルト設定 804
ポートのモニタリング 799
モニタ側ポート 798
宛先ポート 799
概要 792
受信トラフィック 796
設定時の注意事項 804
送信トラフィック 797
送信元ポート 798
他の機能との相互作用 801
特性 800
RSTP 432, 433, 434, 435, 436, 437, 456, 459
BPDU 436, 437
形式 436
処理 437
IEEE 802.1D との相互運用性 432, 437, 459
トポロジの変更 437
RSTP *(続き)*
IEEE 802.1D との相互運用性 *(続き)*
移行プロセスの再開 459
説明 432
アクティブなトポロジ 433
ポートのロール 432, 435
synchronized 435
説明 432
ルート ポート、定義済み 433
概要 432
高速コンバージェンス 434, 456
エッジ ポートと PortFast 434
クロススタック高速コンバージェンス 434
ポイントツーポイント リンク 434, 456
ルート ポート 434
説明 434
指定スイッチ、定義済み 433
指定ポート、定義済み 433

S

SA ステートのキャッシング：コマンド例 1105
SCP 1405
および SSH 1405
設定 1405
SDM 2190, 2192
テンプレート 2190, 2192
設定 2192
番号 2190
SDM テンプレート 161, 2190, 2192
のタイプ 2190
設定 2192
SDM テンプレート コマンドの設定例 2194
SDM テンプレートの選択 2191
SDM テンプレートの表示：コマンド例 2194
SDMテンプレートの設定：コマンド例 2194
Secure Copy Protocol
service compress-config コマンド 2250
services 674
ネットワーキング 674
Set to Factory Default ボタン 1043
SFP 2342, 2343
ステータス、表示 2343
ステータスのモニタリング 2343
セキュリティおよび識別 2342
SFP ステータス 2343
SFP セキュリティおよび識別 2342

show access-lists hw-summary コマンド 1450
show forward コマンド 2345
show platform forward コマンド 2345
SNMP 751, 1977, 1979, 1982
　および IP SLA 751
　トラップ 1977, 1979, 1982
　　MAC アドレス通知のイネーブル 1977, 1979, 1982
SPAN 790, 792, 795, 796, 797, 798, 799, 801, 802, 804, 806, 809, 811, 826
　sessions 795, 804, 806, 809, 811, 826
　　イネーブルにされた入力トラフィック 809
　　宛先（モニタリング）ポートの削除 804
　　監視対象ポートの指定 806, 826
　　作成 806, 826
　　定義 795
　　特定の VLAN への送信元トラフィックの制限 811
　VLAN ベース 798
　およびスタックの変更 802
　セッションの制限 790
　デフォルト設定 804
　ポートのモニタリング 799
　モニタ側ポート 798
　宛先ポート 799
　概要 792
　受信トラフィック 796
　設定時の注意事項 804
　送信トラフィック 797
　送信元ポート 798
　他の機能との相互作用 801
SPAN トラフィック 796
Spanning Tree 391
　状態 391
spanning-tree 387
　ポート プライオリティ 387
Spectrum Expert 37
　CLI を使用した設定 37
SSH 1403
　暗号化方式 1403
　ユーザ認証方式、サポートされる 1403
SSH サーバ 1407
SSID 2508
　説明 2508
SSID およびクライアント ポリシーの統計情報 2139
　GUI を使用した監視 2139
SSID ポリシー 910, 966
SSL 1426, 1427, 1429, 1432, 1434
　セキュア HTTP クライアントの設定 1432
　セキュア HTTP サーバの設定 1429
　モニタリング 1434
SSL *(続き)*
　設定時の注意事項 1427
STP 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 405, 407, 408, 410, 411, 412, 413, 414, 415, 420, 465, 466, 468, 471, 473, 481, 483, 484, 485
　BackboneFast 471, 484
　　イネーブル化 484
　　説明 471
　BPDU メッセージ交換 387
　EtherChannel ガード 473, 485
　　イネーブル化 485
　　説明 473
　IEEE 802.1D とブリッジ ID 389
　IEEE 802.1D とマルチキャスト アドレス 395
　IEEE 802.1Q トランクでの制限 398
　IEEE 802.1t と VLAN 識別子 390
　root 385, 388
　　switch 385, 388
　　選定 388
　　予期しない動作 385
　UplinkFast 465, 481, 483
　　イネーブル化 481
　　ディセーブル化 483
　　説明 465
　VLAN ブリッジ 399
　インターフェイス ステート 391, 392, 393, 394
　　disabled 394
　　フォワーディング 392, 393
　　ブロック 393
　　ラーニング 393
　　リスニング 393
　キープアライブ メッセージ 387
　クロススタック UplinkFast 468
　　説明 468
　サポートされるインスタンス 397
　サポートされるプロトコル 396
　サポートされるモード 396
　スタックのルート ポートの選択 388
　スタック変更、の影響 399
　ステータス、表示 415
　ステータスの表示 415
　ディセーブル化 402
　デフォルト設定 400
　モード間の相互運用性と互換性 397, 420
　ルート デバイス 389, 390, 403
　　拡張システム ID の影響 389, 403
　　設定 390
　ルート ポート、定義済み 388

STP *(続き)*
ルート ポート選択の高速化 **466**
概要 **386**
拡張システム ID **385, 389, 403, 405**
セカンダリ ルート デバイスに対する効果 **405**
ルート デバイスに対する効果 **403**
概要 **389**
予期しない動作 **385**
間接リンク障害の検出 **471**
指定ポート、定義済み **389**
指定定義 **389**
switch **389**
冗長接続 **395**
設定 **401, 403, 405, 407, 408, 410, 411, 412, 413, 414**
hello タイム **411**
スパニングツリー モード **401**
セカンダリ ルート デバイス **405**
デバイス プライオリティ **410**
パス コスト **408**
ポート プライオリティ **407**
ルート デバイス **403**
最大エージング タイム **413**
転送遅延時間 **412**
転送保留カウント **414**
STP パス コスト **2453**
STP ポート プライオリティ **2448**
STP を使用 **510**
SVI **1117, 1443**
および IP ユニキャスト ルーティング、 **1117**
およびルータ ACL **1443**
system **125**

T

TACACS+ **1317, 1319, 1321, 1322, 1324, 1327, 1328, 1331**
login **1324**
アカウンティング、定義 **1317**
キー **1322**
サーバの指定 **1322**
デフォルト設定 **1321**
ユーザによってアクセスされるサービスのトラッキング **1328**
ユーザに対するサービスの制限 **1327**
概要 **1317**
許可、定義 **1317**
設定 **1322, 1324, 1327, 1328**
アカウンティング **1328**
TACACS+ *(続き)*
設定 *(続き)*
ログイン認証 **1324**
許可 **1327**
認証キー **1322**
定義 **1317**
動作 **1319**
認証、定義 **1317**
表示 **1331**
tar ファイル **2298**
の内容の表示 **2298**
作成 **2298**
抽出しています **2298**
TCAM エントリ **1539**
tcp mss **612**
Telnet **1302**
パスワードの設定 **1302**
Terminal Access Controller Access Control System Plus **1317**
「TACACS+」を参照 **1317**
TFTP サーバ **2230, 2239, 2244, 2269**
コンフィギュレーション ファイル **2230, 2239, 2244, 2269**
からのコピー **2244**
ダウンロード **2269**
へのコピー **2230, 2239**
TGT **1388**
time **1954**
「NTP」および「システム クロック」を参照してください **1954**
time-range コマンド **1452**
TLV **102**
定義 **102**
traceroute **2327**
traceroute コマンド **2327**
「IP traceroute」も参照 **2327**
traceroute の使用 **2327**
traceroute、レイヤ 2 **2326**
ARP **2326**
CDP **2326**
IP アドレスおよびサブネット **2326**
MAC アドレスおよび VLAN **2326**
ブロードキャスト トラフィック **2326**
ポートへの複数のデバイスの設定 **2326**
マルチキャスト トラフィック **2326**
ユニキャスト トラフィック **2326**
使用上のガイドライン **2326**
説明 **2326**
Traffic Stream Metrics（TSM） **2150**
説明 **2150**

trust 937

U

U-APSD 2149
説明 2149
UDLD 535, 536, 537, 538, 539, 540, 541
aggressive 536, 537
normal 536
アグレッシブ モード 540
メッセージ タイム 540
イネーブル化 540, 541
インターフェイスごと 541
グローバル 540
エコー検出メカニズム 537, 538
ツイスト ペア リンク 537
ディセーブル化 541
インターフェイスごと 541
デフォルト設定 539
ネイバー データベース 537
ネイバー データベース メンテナンス 538
概要 536
光ファイバ リンク 537
制約事項 535
通常モード 536
UDP ジッタ、設定する 763
UDP ジッタ動作、IP SLA 755, 763
UplinkFast 465, 481, 483
イネーブル化 481
ディセーブル化 483
説明 465
User Datagram Protocol 1115, 1135
「UDP」を参照 1115, 1135

V

Validate Rogue Clients Against AAA パラメータ 1843
VCI 文字列 582
Virtual Private Network（バーチャル プライベート ネットワーク） 1236
VPN を参照 1236
VLAN 2402
定義 2402
VLAN ACL 1441
VLAN マップを参照 1441
VLAN ID、検出する 1962
VLAN のポリサーの割り当て 1021
VLAN のモニタリング コマンド 2419
VLAN フィルタリングと SPAN 799
VLAN ポート メンバーシップ モード 2405
VLAN マップ 1441, 1450, 1473, 1475, 1476, 1488, 1490
サーバに対するアクセス拒否の例 1490
パケットの拒否と許可 1473, 1475
一般的な使用方法 1488
作成 1475
設定 1473
設定時の注意事項 1450
定義 1441
適用 1476
VLAN マップ エントリ、順序 1451
VLAN 間ルーティング 1109
VLANs 396, 398, 399, 811, 818
RSPAN での送信元トラフィックの制限 818
SPAN での送信元トラフィックの制限 811
STP および IEEE 802.1Q トランク 398
VLAN ブリッジ STP 399
ダイナミック アドレスのエージング 396
Voice RSSI パラメータ 1057
voice-over-IP（VoIP）による通話ローミング 2095
VRF 1539
VRF 認識サービス 1245, 1246, 1248, 1249, 1250, 1251
RADIUS 1249
ARP 1246
ping 1246
SNMP 1246
syslog 1249
tftp 1251
traceroute 1250
uRPF 1248
設定 1245
VRF、マルチキャストの設定 1252
VTP 2373, 2380, 2381
version 2381
設定の要件 2380
VTP アドバタイズ 2375
VTP ドメイン（VTP domain） 2373, 2393
VTP の設定 2380
VTP バージョン 2388, 2403
VTP バージョン 2 2376
VTP バージョン 3 2377
VTP パスワード 2385
VTP プライマリ 2387
VTP プルーニング 2378, 2390
VTP モード 2374, 2383

W

Web ベース認証 1673, 1679
　カスタマイズ可能な Web ページ 1679
　説明 1673
Web ベース認証、他の機能との相互作用 1682
WLAN 2510
　セッション タイムアウト 2510
　　説明 2510
WLAN インターフェイス VLAN、設定 2516
WLAN コール スヌープ、設定 2516
WLAN ブロードキャスト ssid、設定 2516
WLAN メディア ストリーム マルチキャスト、設定 2516
WLAN 無線、設定 2516
WLAN、イネーブル、ディセーブル 2516
WTD 932
　デフォルト 932

Z

zzz] 1388

あ

アカウンティング 1317, 1328, 1374
　RADIUS 1374
　TACACS+ 1317, 1328
アカウンティング、定義 1317
アクセス グループ 1453
　レイヤ 3 1453
アクセス グループ、IPv4 ACL をインターフェイスに対して適用する 1467
アクセス コントロール エントリ 1440
　ACE を参照 1440
アクセス ポイント 548, 549, 591, 2096
　経由ローミング 2096
　join 情報の表示 549
　　GUI の使用 549
　サイズの大きなイメージのサポート 591
　プライミング 548
アクセス ポイントの 802.1X 認証 573
　説明 573
アクセス ポイントの MAC アドレス 583
　コントローラ GUI に表示された 583
アクセス ポイントのコア ダンプ、アップロード 583
　GUI の使用 583
アクセス ポイントの再試行回数 562
アクセス ポイントの再送信間隔 562
アクセス ポイントの認証 572
アクセス ポイント通信プロトコル 549
アクセス リスト 1446
　「ACL」を参照 1446
アクセス、テンプレートの 2190
アクセスの制限 1291, 1317, 1335
　RADIUS 1335
　TACACS+ 1317
　概要 1291
アクティブ リンク 94
アクティブ化、AP-Count 2047
アクティブ化、ベース 2046
アップグレード:ソフトウェア 2304, 2305, 2309, 2311
　インストール モード 2304
　バンドル モード 2305
　互換性のないソフトウェア 2309
　互換性のない実行モード 2311
アドホック ネットワーク パラメータの検出およびレポート 1843
アドミニストレーティブ ディスタンス 1155, 1285
　OSPF 1155
　定義 1285
アドレス 180, 395, 396, 1961, 1962, 1984
　dynamic 396, 1961
　　デフォルト エージング 396
　　ラーニング 1961
　　迅速なエージング 396
　　定義 1961
　IPv6 180
　MAC、検出する 1962
　multicast 395
　　STP アドレス管理 395
　静的 1984
　　追加と削除 1984
アドレスの割り当て 188
アドレス解決 1962
アドレス解決プロトコル 1114
　「ARP」を参照 1114
アドレス形式 180
アプリケーション 183

い

イーサネット VLAN 2410
イーサネット管理ポート 94, 95
　アクティブ リンク 94

イーサネット管理ポート *(続き)*
およびルーティング プロトコル 94
サポートされていない機能 95
サポートされる機能 95
デフォルト設定 94
ネットワーク管理用 94
ルーティング 94
説明 94
イーサネット管理ポート、内部 94, 95
およびルーティング プロトコル 94
サポートされていない機能 95
ルーティング 94
イーサネット管理ポートの設定 96
イーサネット管理ポートを参照 94
イーサネット経由の電源供給 621
イネーブル シークレット パスワード 1299
イネーブル パスワード 1299
イネーブル化 172, 1297, 1540, 1542, 2346
イネーブル化またはディセーブル化 168
イベント サービス 674
インターネット プロトコル バージョン 6 180
「IPv6」を参照 180
インターフェイス 89
Auto-MDIX、設定する 89
インベントリ管理 TLV 104
インライン電源 621

え

エージング時間 412, 452, 1975
MAC アドレス テーブル 1975
短縮 412, 452
MSTP 用 452
STP 用 412
エラー メッセージ出力のリダイレクト 2345
エリア ルーティング 1220
IS-IS 1220
エリア境界ルータ 1153
「ABRs」を参照 1153

お

オフライン設定 1890, 1902
割り当てられたスイッチ、定義済み 1890
割り当てられた設定、定義済み 1890
新しいメンバーのプロビジョニング 1902
および IPv6 181
および SSH 1405
およびルーティング プロトコル 94
オンボード障害ロギング 2331
オンライン診断 2215
概要 2215
説明 2215

か

カスタマー エッジ デバイスでの複数 VPN ルーティング/転送 1236
マルチ VRF CE を参照 1236
カスタマイズ可能な Web ページ、Web ベース認証 1679
カスタム ロケーション 104
カバレッジ ホールの検出 1057, 1058
コントローラごとの設定 1057, 1058
GUI の使用 1057, 1058
カバレッジ ホールの検出と修正 1040

き

キー 1322, 1365
キープアライブ メッセージ 387
キー発行局 1388
「KDC」を参照 1388
キュー バッファ 933, 934, 995
allocation 934

く

クライアント ポリシー 957
設定方法 957
クライアント機能のイネーブル化 210
クラスベースの無条件パケット マーキング 958
クラスレス ルーティング 1112
クレデンシャル 1388
グローバル コンフィギュレーション モード 2228
入力 2228
クロススタック EtherChannel 494, 496, 510, 513, 516
図 494
設定 513
レイヤ 2 インターフェイス上 513
説明 494

クロススタック UplinkFast、STP 468, 469, 470
Fast Uplink Transition Protocol 469
高速コンバージェンス イベント 470
説明 468
通常コンバージェンス イベント 470

こ

コマンド モード 2228
グローバル コンフィギュレーション 2228
コマンド、権限レベルを設定する 1307
コマンドの権限レベルの設定：コマンド例 1312
コマンドの設定 1307
コマンドを使用 2329
コメント 2229, 2237
コンフィギュレーション ファイルへの追加 2229, 2237
コンフィギュレーション アーカイブ 2277
作成 2277
コンフィギュレーション コマンド例 212
コンフィギュレーション ファイル 1301, 2228, 2229, 2230, 2234, 2235, 2239, 2240, 2242, 2244, 2250, 2254, 2255, 2256, 2258, 2264, 2267, 2269, 2296, 2406
CONFIG_FILE 環境変数 2264
network 2235
ネットワーク コンフィギュレーション ファイルの参照 2235
NVRAM より大きい 2234, 2250
コピー 2229, 2230, 2239, 2244, 2255, 2256, 2258
RCP サーバへ 2230
TFTP サーバから 2244
TFTP サーバへ 2230, 2239
ネットワーク サーバから 2229, 2258
フラッシュ メモリ デバイス間 2256
フラッシュ メモリから 2255
コピー時の無効な組み合わせ 2296
タイプ 2228
ダウンロード 2235, 2269
ホスト コンフィギュレーション ファイル 2269
ネットワークからのロード 2235, 2254
パスワード回復のディセーブル時の考慮事項 1301
フラッシュ メモリへの格納 2234
ホスト 2269
ホスト コンフィギュレーション ファイルを参照 2269
ロードの失敗 2267
圧縮 2250
コンフィギュレーション ファイル (続き)
実行 2240, 2242
実行コンフィギュレーションも参照 2240, 2242
場所 2229
表示 2235
情報 2235
変更 2228
ご利用条件 1388

さ

サーバ 1388
サーバの指定 1322, 1365
サービス プロバイダー ネットワーク、MSTP および RSTP 421
サービス プロバイダー ネットワーク内 1236
サブネット ゼロ 1122
サブネット マスク 1120
サブネットワーク アクセス プロトコル（SNAP） 697
サブネット間ローミング 2095
説明 2095
サポートされていない機能 95
サポートされているデバイス 54, 137
サポートされない機能 186
サポートされる機能 95, 181
サポートされる標準 138
サポートしているポート単位のワット数 54, 137

し

シェーピング 928, 1001
しきい値監視、IP SLA 754
システム MTU 125, 126, 1222
および IS-IS LSP 1222
システム クロック 1954, 1963, 1964, 1965
概要 1954
設定 1963, 1964, 1965
タイム ゾーン 1964
夏時間 1965
手動 1963
システム プライオリティ 526
システム プロンプト、デフォルト設定 1959
システム リソース、最適化する 2190
システム リソースを最適化する 2190
システム ルーティング 1220
IS-IS 1220

システム機能 TLV 102
システム記述 TLV 102
システム名 1959, 1969
　デフォルト設定 1959
　手動設定 1969
システム名 TLV 102

す

スイッチ アクセス 1311
　表示 1311
スイッチ スタック 2346, 2379
スイッチ スタックのライセンス 2044
スイッチ スタックの管理 1896
スイッチから転送される送信元情報の制御：コマンド例 1106
スイッチから発信される送信元情報の制御：コマンド例 1105
スイッチで受信される送信元情報の制御：コマンド例 1106
スイッチド パケット、ACL 1491
スイッチの制限 187
スタートアップ コンフィギュレーション 2229, 2235, 2241, 2244, 2247, 2249, 2254, 2262
　rcp サーバからのコピー 2247, 2249
　　（例） 2247, 2249
　RCP サーバへのコピー（例） 2241, 2244
　クリア 2262
　コンフィギュレーション コマンドの再実行 2262
　ネットワークからのロード 2235, 2254
　へのコンフィギュレーション ファイルのコピー 2229
スタック 387, 388, 397, 2308, 2310, 2311
　1 台のメンバから他のメンバへのバンドル ファイルのコピー 2308
　STP 387, 388
　　ブリッジ ID 387
　　ルート ポートの選択 388
　switch 388, 397
　アップグレード 2308
　アップグレード中、互換性のない実行モード 2311
　サポートされる MSTP インスタンス 397
　互換性のないソフトウェアのアップグレード 2310
スタック スイッチ 1889
　故障したメンバーの交換 1889
スタック マスター 187
　IPv6 187
スタック マスターは、次に示す機能を実行します。 187
スタック メンバ 187, 1889, 1899, 1901, 1902, 1903
　IPv6 187
　割り当てられたメンバーの削除 1903
　交換 1889
　新しいメンバーのプロビジョニング 1902
　設定 1899, 1901
　　member number 1899
　　priority value 1901
スタック、スイッチ 187, 1883, 1890, 1893, 1897, 1899, 1901, 1902, 1903, 1959, 1961, 2340
　auto-copy 1893
　auto-upgrade 1893
　IPv6 187
　MAC アドレス 1897
　MAC アドレスの考慮事項 1961
　merged 1883
　オフライン設定 1890, 1902, 1903
　　割り当てられたスイッチ、定義済み 1890
　　割り当てられたメンバーの削除 1903
　　割り当てられた設定、定義済み 1890
　　新しいメンバーのプロビジョニング 1902
　システム プロンプトの考慮事項 1959
　バージョン不一致（VM）モード 1893
　　auto-extract を使用したアップグレード 1893
　　auto-upgrade を使用した自動アップグレード 1893
　区分化 1883, 2340
　自動アドバイス 1893
　自動抽出 1893
　情報の割り当て 1899, 1901, 1902
　　member number 1899
　　priority value 1901
　　新しいメンバーのプロビジョニング 1902
スタック、スイッチバージョン不一致モード（VM） 1893
　自動アドバイスを使用した手動アップグレード 1893
スタックの変更 187
　への効果 187
　　IPv6 ルーティング 187
スタックの変更、影響 399, 432, 508, 510, 802, 1111, 1446, 1961, 2191
　ACL 設定 1446
　EtherChannel 508
　IP ルーティング 1111
　MAC アドレス テーブル 1961
　MSTP 432
　SDM テンプレートの選択 2191
　SPAN および RSPAN 802
　STP 399
　クロススタック EtherChannel 510
スタック変更、の影響 508

スタティック IP アドレス 583
説明 583
スタティック アドレス 1961
「アドレス」を参照 1961
スタティック イネーブル パスワードの設定または変更：コマンド例 1311
スタティック バインディング 1540, 1542
追加 1540, 1542
スタティック ホスト 1542
スタティック モード 140
スタティック ルーティング 1109
スタティック ルート 183, 1266
設定 1266
説明 183
スタティック ルートの概要 183
スタティックなマルチキャスト グループの設定：コマンド例 177
スタティック結合 170
スタブ ルーティング、EIGRP 184, 1172
ステータス、表示 2343
ステータスのモニタリング 2343
ステートレス自動設定 182
スヌーピング 175
スプリット ホライズン、RIP 1148
すべてのシステム診断のイネーブル 2356

せ

セカンダリ VLAN 2474
セカンダリ VLAN の設定 2481
セキュア HTTP クライアント 1432, 1434
設定 1432
表示 1434
セキュア HTTP クライアントの設定 1432
セキュア HTTP サーバ 1429, 1434
設定 1429
表示 1434
セキュア HTTP サーバの設定 1429
セキュア シェル 1403
セキュリティおよび識別 2342

そ

その他の参考資料 2397, 2422, 2430, 2456, 2468
VLAN トランク 2456
VLANs 2422, 2430
その他の参考資料 *(続き)*
VTP 2397
音声 VLAN 2468
ソフトウェア イメージ 2333
「ソフトウェアイメージのダウンロードとアップロード」も参照 2333
回復手順 2333

た

ダイナミック アドレス 396
「アドレス」を参照 396
ダイナミック ルーティング 1110
ダイナミックなしきい値および拡張 934
タイム ゾーン 1964
ダイレクトされたローミング要求 2097

ち

チケット 1388
チャネル グループ 497
番号 497
物理および論理インターフェイスのバインド 497

つ

ツイスト ペア、単方向リンクの検出 536

て

ディスタンスベクトル プロトコル 1110
ディセーブル化 175
ディレクトリ 2293, 2295
作業ディレクトリの表示 2293
作成 2295
削除 2295
変更 2293
テーブル マップ 975
テーブル マップのマーキング 1024
CoS 1024
デバイス 394
root 394
デバイス プライオリティ 410, 449
MSTP 449

デバイス プライオリティ *(続き)*
STP 410
デフォルト MSDP ピアの設定：コマンド例 1105
デフォルト ゲートウェイ 1129
デフォルト ネットワーク 1269
デフォルト ルータ プリファレンス 182
「DRP」を参照 182
デフォルト ルータ プリファレンス（DRP） 182
デフォルトルータ プリファレンスの設定：コマンド例 212
デフォルト ルーティング 1109
デフォルト ルート 1269
デフォルトグループ アクセス ポイント グループ 2596
デフォルトの Web ベース認証の設定 1684
802.1X 1684
デフォルトのイネーブル パスワード 572
デフォルトのワイヤレス QoS 設定 942
デフォルト設定 94, 105, 166, 167, 188, 207, 400, 439, 508, 539, 804, 1191, 1240, 1294, 1321, 1346, 1426, 1960, 1962
BGP 1191
DNS 1960
EtherChannel 508
IGMP スヌーピング 166, 167
IPv6 188
LLDP 105
MAC アドレス テーブル 1962
MSTP 439
RADIUS 1346
RSPAN 804
SPAN 804
SSL 1426
STP 400
TACACS+ 1321
UDLD 539
パスワードおよび権限レベル 1294
バナー 1960
マルチ VRF CE 1240
デュアルレート 3 カラー ポリシング 928
テンプレート 2190, 2192
設定 2192
番号 2190

と

トークン リング 2388
とスイッチ スタック 187
トポロジ変更通知処理 166
ドメイン ネーム サーバ（DNS）ディスカバリ 548
ドメイン、ISO IGRP ルーティング 1220
ドメイン名 1959, 2381
DNS 1959
トラストポイント、CA 1424
トラップ 1977, 1979, 1982
MAC アドレス通知設定 1977, 1979, 1982
イネーブル化 1977, 1979, 1982
トラフィック 1444, 1445
フラグメント化 1444, 1445
トラフィック シェーピング 929
トラフィックの調整 926
トラフィックの優先的処理 901
「QoS」を参照 901
トラブルシューティング 2325, 2327, 2329, 2342, 2345
debug コマンドを使用 2329
ping を使用 2325
SFP セキュリティおよび識別 2342
show forward コマンド 2345
traceroute の使用 2327
パケット転送の設定 2345
トラブルシューティング コマンド例 2354
トランキング 2435
トランキング モード 2435
トランク 2437, 2439, 2442
許可 VLAN 2437
設定 2439
トランク インターフェイス 1539
トランク ポート 2439

ね

ネイティブ VLAN 2446
ネイバー探索 182
ネイバー探索、IPv6 182
ネイバー探索および回復、EIGRP 1170
ネームスペース マッパー 674
ネットワーク コマンドの起動 2254
ネットワーク コンフィギュレーション ファイル 2235
ホスト コンフィギュレーション ファイルとの比較 2235
説明 2235
ネットワーク サービス 1392
ネットワーク パフォーマンス、IP SLA で測定する 751
ネットワーク ポリシー TLV 103
ネットワーク環境の提案 1335
ネットワーク管理用 94
ネットワーク負荷分散 2438
STP パス コスト 2438

ネットワーク負荷分散 *(続き)*
STP プライオリティ 2438

の

のタイプ 2190

は

バージョン不一致（VM）モード 1893
auto-extract を使用したアップグレード 1893
auto-upgrade を使用した自動アップグレード 1893
自動アドバイスを使用した手動アップグレード 1893
バインディング コンフィギュレーション 1538
automatic 1538
manual 1538
バインディング データベース 1515
アドレス、DHCP サーバ 1515
DHCP、Cisco IOS サーバ データベースを参照 1515
バインディング テーブル 1538
パケット転送の設定 2345
パス MTU 検出 181
パス コスト 387, 408, 448
MSTP 448
STP 408
パスワード 1291, 1294, 1297, 1299, 1301, 1302, 1304, 2324
デフォルト設定 1294
暗号化 1299
回復 2324
回復のディセーブル化 1301
概要 1291
設定 1297, 1299, 1302, 1304
enable secret 1299
Telnet 1302
イネーブル化 1297
ユーザ名 1304
パスワードおよび権限レベル 1294
パスワードおよび権限レベル コマンドの設定例 1311
パスワードの設定 1302
パスワード回復のディセーブル時の考慮事項 1301
バックアップ 386
port 386
バナー 1960, 1972, 1974
デフォルト設定 1960
設定 1972, 1974
login 1974
バナー *(続き)*
設定 *(続き)*
Message-of-The-Day ログイン 1972
ハブ 94
パラレル パス、ルーティング テーブル内 1265
バンドル ファイル 2303
アップロード 2303
ダウンロード 2303
内容の表示 2303

ひ

ピアツーピア ブロック 2510
説明 2510

ふ

ファイル 2296, 2297, 2298
tar 2298
作成 2298
抽出しています 2298
内容の表示 2298
コピー 2296
削除 2297
フィルタ、IP 1439
ACL、IP フィルタを参照 1439
IP 1439
zzz] 1439
フィルタリング 1469
非 IP トラフィック。 1469
フォールバック ブリッジング 387, 399
STP 387
キープアライブ メッセージ 387
VLAN ブリッジ STP 399
フォワーディング 188, 393, 1239
state 393
プライベート VLAN 2471, 2477, 2483, 2485, 2489, 2491, 2494
broadcast 2477
multicast 2477
unicast 2477
セカンダリ VLAN のマッピング 2494
ポート設定 2483
レイヤ 2 インターフェイスの設定 2489
設定 2485
複数のスイッチ 2477
無差別ポートの設定 2491

プライベート VLAN ドメイン 2473
プライベート VLAN のモニタ 2499
プライマリ VLAN の設定 2481
フラッシュ デバイス、 2290
　番号 2290
フラッシュ メモリ 2234, 2331
　コンフィギュレーション ファイルの格納 2234
フラッシュ メモリ デバイス 2256
　ファイル 2256
　　コピー 2256
ブリッジ プロトコル データ ユニット 387
ブリッジド パケット、ACL 1492
ブリッジ識別子（ブリッジID） 389
プルーニング適格リスト 2444
プレフィックス リスト、BGP 1188
ブロードキャスト ストーム 1116
ブロードキャスト トラフィック 2326
ブロードキャスト パケット 1116
　directed 1116
　フラッディング 1116
ブロードキャストのフラッディング 1116
プローブ要求、説明 599
プローブ要求フォワーディング 599
プロキシ ARP 1114, 1115
　ディセーブルにした IP ルーティング 1115
　定義 1114
ブロック 393
　state 393
プロトコル依存モジュール、EIGRP 1171
プロバイダー エッジ デバイス 1237
プロビジョニング、スイッチ スタックの新メンバの 1890

へ

への効果 187
　IPv6 ルーティング 187
ベンダー固有 1378
ベンダー独自仕様 1379

ほ

ポート 2474
　community 2474
　isolated 2474
　無差別 2474
ポート ACL 1440, 1442
　のタイプ 1442
　定義 1440
ポート VLAN ID TLV 102
ポート セキュリティ 1539
ポート プライオリティ 407, 446, 527
　MSTP 446
　STP 407
ポート ベース認証 1674, 1684, 1686, 1690, 1703
　switch 1674
　　プロキシとして 1674
　イネーブル化 1690
　　802.1X 認証 1690
　デバイスの役割 1674
　デフォルト設定 1684
　設定 1686, 1690
　　RADIUS サーバ 1686
　　スイッチ上の RADIUS サーバ パラメータ 1690
　設定時の注意事項 1684
　統計情報の表示 1703
ポートチャネル インターフェイス 497
　番号 497
ポートへの複数のデバイスの設定 2326
ポート記述 TLV 102
ポート集約プロトコル 499
　「EtherChannel」を参照 499
ホスト コンフィギュレーション ファイル 2235, 2247, 2249, 2269
　rcp サーバからスタートアップ コンフィギュレーションへのコピー（例） 2247, 2249
　サーバからのロード 2269
　ネットワーク コンフィギュレーション ファイルとの比較 2235
　説明 2235
ホット スタンバイ ポート 523
ポリシー 952, 964
　インターフェイスの付加 964
ポリシー マップ 952, 972, 2131
　設定 972
ポリシーベース ルーティング 1277
　「PBR」を参照 1277
ポリシング 918, 919, 922, 923, 927
　トークンバケット アルゴリズム 923
　説明 918, 919
　物理ポート 923

ま

マーキング 923, 924, 968
　テーブル マップ 924
　パケット ヘッダー 924
　ポリシー マップのアクション 968
　ルータ固有の情報 924
マッピング、VLAN の 2498
マルチ VRF CE 1236, 1238, 1239, 1240, 1241, 1258
　デフォルト設定 1240
　ネットワーク コンポーネント 1239
　パケット転送処理 1238
　設定時の注意事項 1241
　設定例 1258
　定義 1236
マルチキャスト VRF の設定 1252
マルチキャスト クライアント エージングの堅牢性 164
マルチキャスト グループ 170
　スタティック結合 170
マルチキャスト トラフィック 2326
マルチキャスト パケット 1493
　への ACL 1493
マルチキャスト ルータ ポートの設定：コマンド例 177
マルチキャスト ルータ検出 164

み

ミラーリング トラフィック、分析用の 792

め

メッセージ、ユーザに対するバナーを使用した 1960
メトリック、BGP 内 1187
メトリック変換、ルーティング プロトコル間 1276

も

モード 499, 503
モニタリング 141, 175, 206, 770, 792, 1004, 1139, 1168, 1181, 1263, 1434, 1478, 2343, 2396, 2467, 2496, 2582
　CEF 1263
　EIGRP 1181
　GUI の使用 2582
　IGMP 175
　　スヌーピング 175
モニタリング (続き)
　IP 1139
　　アドレス テーブル 1139
　IP SLA の動作 770
　IPv4 ACL コンフィギュレーション 1478
　IPv6 206
　OSPF 1168
　QoS 1004
　SFP ステータス 2343
　VTP 2396
　アクセス グループ 1478
　プライベート VLAN 2496
　プローブでの分析用のネットワーク トラフィック 792
　音声 VLAN 2467
モニタ間隔、GUI を使用した設定 1043
モビリティ グループ 1034
　RF グループとの違い 1034

ゆ

ユーザによってアクセスされるサービスのトラッキング 1328, 1374
ユーザに対するサービスの制限 1327, 1372
ユーザ認証方式、サポートされる 1403
ユーザ名 1304
ユーザ名ベース認証 1304
ユニキャスト MAC アドレス フィルタリング 1986
　設定 1986
ユニキャスト トラフィック 2326

ら

ライセンス AP-Count のアクティブ化 2047
ライセンス ベースのイメージのアクティブ化 2046

り

リスニング 393
　state 393
リセット、BGP 内 1185
リファレンス 430
リモート認証ダイヤルイン ユーザ サービス 1335
　「RADIUS」を参照 1335
リンク テスト 612
　パケットのタイプ 612

リンク ローカル ユニキャスト アドレス 181
リンクステート プロトコル 1110
リンクの失敗、単一方向の検出 431

る

ルータ ACL 1440, 1443
　のタイプ 1443
　定義 1440
ルータ ID、OSPF 1156
ルーティング 94, 1109, 1110, 1270
　dynamic 1110
　デフォルト 1109
　情報の再配信 1270
　静的 1109
ルーティング ドメイン連合、BGP 1213
ルーティングの設定 1254
ルーティング情報プロトコル 1110
　「RIP」を参照 1110
ルーテッド パケット、ACL 1492
ルーテッド ポート 1117, 1118, 1539
　IP アドレス 1118
　設定 1117
ルート ターゲット、VPN 1239
ルート デバイス 403, 443
　MSTP 443
　STP 403
ルート マップ 1187, 1278
　BGP 1187
　ポリシーベース ルーティング 1278
ルート リフレクタ、BGP 1190
ルート計算タイマー、OSPF 1155
ルート選択、BGP 1186

れ

レイヤ 2 917
レイヤ 2 EtherChannel の設定：例のコマンド 530
レイヤ 2 EtherChannel 設定時の注意事項 512
レイヤ 2 インターフェイス 513
レイヤ 2 インターフェイス モード 2436
レイヤ 2 インターフェイス上 513
レイヤ 2 の traceroute 2326
　ARP 2326
　CDP 2326
　IP アドレスおよびサブネット 2326
レイヤ 2 の traceroute (続き)
　MAC アドレスおよび VLAN 2326
　ブロードキャスト トラフィック 2326
　ポートへの複数のデバイスの設定 2326
　マルチキャスト トラフィック 2326
　ユニキャスト トラフィック 2326
　使用上のガイドライン 2326
　説明 2326
レイヤ 3 916
レイヤ 3 EtherChannel の設定：例のコマンド 531
レイヤ 3 EtherChannel 設定時の注意事項 513
レイヤ 3 インターフェイス 188, 192, 1117
　IPv4 アドレスと IPv6 アドレスの割り当て 192
　IPv6 アドレスの割り当て 188
　のタイプ 1117
レイヤ 3 インターフェイス コマンドの設定例 83
レイヤ 3 パケット、分類方式 915
レスポンダ、IP SLA 752, 757
　イネーブル化 757
　説明 752
レポート抑制 175
　ディセーブル化 175
レポート抑制、IGMP 175
　ディセーブル化 175
レルム 1388

ろ

ローカル SPAN 792
ロード バランシング 505, 518
ロードバランシングの利点 506
ローミングの最適化 1071
ローミングの最適化の設定 1072
　GUI の使用 1072
ローミング理由レポート 2097
ロギング メッセージ、ACL 1450
ログイン 1310
ログイン バナー 1960
ログイン認証 1324, 1367
　RADIUS 1367
　TACACS+ 1324
ロケーション TLV 104

わ

ワイヤード ロケーション サービス 104, 115
ロケーション TLV 104
設定 115
ワイヤード ロケーション サービス (続き)
説明 104
ワイヤレス アクセス 903
ワイヤレス侵入防御システム（wIPS） 1863
説明 1863