統合プラットフォームコンフィギュレーションガイド、Cisco IOS Release 15.2(3) E（Catalyst 3560-CX および 2960 CX スイッチ）

初版：2015 年 03 月 11 日

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

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

目 次

はじめに lxxvii

表記法 lxxvii

関連資料 lxxix

マニュアルの入手方法およびテクニカル サポート lxxix

コマンドライン インターフェイスの使用 1

コマンドライン インターフェイスの使用に関する情報 1

コマンド モード 1

コマンドの省略形 5

コマンドの no 形式および default 形式 5

CLI のエラー メッセージ 6

コンフィギュレーション ロギング 6

ヘルプ システムの使用 7

CLI を使用して機能を設定する方法 8

コマンド履歴の設定 8

コマンド履歴バッファ サイズの変更 8

コマンドの呼び出し 8

コマンド履歴機能の無効化 9

編集機能の有効化および無効化 10

キー入力によるコマンドの編集 10

画面幅よりも長いコマンドラインの編集 12

show および more コマンド出力の検索およびフィルタリング 13

コンソール接続または Telnet 経由での CLI へのアクセス 14

インターフェイスおよびハードウェア 15

インターフェイス特性の設定 17

機能情報の確認 17

インターフェイス特性の設定に関する情報 17

インターフェイス タイプ 17
ポートベースの VLAN 18
スイッチ ポート 18
アクセス ポート 19
トランク ポート 19
スイッチ仮想インターフェイス 20
SVI 自動ステート除外 20
EtherChannel ポート グループ 21
Power over Ethernet（PoE）ポート 21
スイッチの USB ポートの使用 21
USB ミニタイプ B コンソール ポート 22
コンソール ポート変更ログ 22
USB タイプ A ポート 22
インターフェイスの接続 22
インターフェイス コンフィギュレーション モード 23
イーサネット インターフェイスのデフォルト設定 24
インターフェイス速度およびデュプレックス モード 25
速度とデュプレックス モードの設定時の注意事項 26
IEEE 802.3x フロー制御 26
インターフェイスの特性の設定方法 27
インターフェイスの設定 27
インターフェイスに関する記述の追加 28
インターフェイス範囲の設定 30
インターフェイス レンジ マクロの設定および使用方法 31
イーサネット インターフェイスの設定 33
インターフェイス速度およびデュプレックス パラメータの設定 33
IEEE 802.3x フロー制御の設定 35
SVI 自動ステート除外の設定 37
インターフェイスのシャットダウンおよび再起動 38
コンソール メディア タイプの設定 39
USB 無活動タイムアウトの設定 41
インターフェイス特性のモニタ 42

インターフェイス ステータスのモニタ 42
インターフェイスおよびカウンタのクリアとリセット 43
インターフェイス特性の設定例 44
インターフェイスの説明の追加：例 44
インターフェイス範囲の設定：例 44
インターフェイス レンジ マクロの設定および使用方法：例 45
インターフェイス速度およびデュプレックス モードの設定：例 45
コンソール メディア タイプの設定：例 46
USB 無活動タイムアウトの設定：例 46
Auto-MDIX の設定 47
Auto-MDIX の前提条件 47
Auto-MDIX の制約事項 47
Auto-MDIX の設定に関する情報 48
インターフェイスでの Auto-MDIX 48
Auto-MDIX の設定方法 49
インターフェイスでの Auto-MDIX の設定 49
Auto-MDIX の設定例 50
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定 51
機能情報の確認 51
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要 51
LLDP 51
LLDP でサポートされる TLV 52
LLDP および Cisco Medianet 52
LLDP-MED 52
LLDP-MED でサポートされる TLV 53
ワイヤード ロケーション サービス 54
デフォルトの LLDP 設定 55
LLDP に関する制約事項 56
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定方法 56
LLDP のイネーブル化 56
LLDP 特性の設定 58
LLDP-MED TLV の設定 60
Network-Policy TLV の設定 62

ロケーション TLV およびワイヤード ロケーション サービスの設定 65
スイッチ上でのワイヤード ロケーション サービスのイネーブル化 68
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定例 69
Network-Policy TLV の設定：例 69
LLDP、LLDP-MED、ワイヤード ロケーション サービスのモニタリングとメンテナンス 69
システム MTU の設定 73
機能情報の確認 73
MTU に関する情報 73
システム MTU のガイドライン 74
MTU の設定方法 74
システム MTU の設定 74
システム MTU の設定例 75
PoE の設定 77
機能情報の確認 77
PoE について 77
Power over Ethernet（PoE）ポート 77
サポート対象のプロトコルおよび標準 78
受電装置の検出および初期電力割り当て 78
電力管理モード 80
電力モニタリングおよび電力ポリシング 81
PoE ポートでの最大電力割り当て（カットオフ電力） 82
電力消費値 82
PoE の設定方法 83
PoE ポートの電力管理モードの設定 83
PoE ポートに接続された受電装置の電力バジェット 85
すべての PoE ポートのパワー バジェット 86
特定の PoE ポートのパワー バジェット 87
電力ポリシングの設定 89
電力ステータスのモニタ 91
PoE の設定例 92
パワー バジェット：例 92

EEE の設定 93
機能情報の確認 93
EEE について 93
EEE の概要 93
デフォルトの EEE 設定 94
EEE の制約事項 94
EEE の設定方法 94
EEE のイネーブル化またはディセーブル化 94
EEE のモニタリング 96
EEE の設定例 96
IPv6 97
MLD スヌーピングの設定 99
機能情報の確認 99
IPv6 MLD スヌーピングの設定に関する情報 99
MLD スヌーピングの概要 100
MLD メッセージ 101
MLD クエリー 101
マルチキャスト クライアント エージングの堅牢性 102
マルチキャスト ルータ検出 102
MLD レポート 102
MLD Done メッセージおよび即時脱退 103
TCN 処理 103
IPv6 MLD スヌーピングの設定方法 104
MLD スヌーピングのデフォルト設定 104
MLD スヌーピング設定時の注意事項 105
スイッチでの MLD スヌーピングのイネーブル化またはディセーブル化（CLI） 105
VLAN での MLD スヌーピングのイネーブル化またはディセーブル化（CLI） 106
スタティック マルチキャスト グループの設定（CLI） 107
マルチキャスト ルータ ポートの設定（CLI） 108
MLD 即時脱退の有効化（CLI） 109
MLD スヌーピング クエリーの設定（CLI） 110

MLD リスナー メッセージ抑制の無効化（CLI） 112
MLD スヌーピング情報の表示 113
MLD スヌーピングの設定例 114
スタティックなマルチキャスト グループの設定：例 114
マルチキャスト ルータ ポートの設定：例 114
MLD 即時脱退のイネーブル化：例 115
MLD スヌーピング クエリーの設定：例 115
IPv6 ユニキャスト ルーティングの設定 117
機能情報の確認 117
IPv6 ユニキャスト ルーティングの設定について 117
IPv6 の概要 117
IPv6 アドレス 118
サポート対象の IPv6 ユニキャスト ルーティング機能 118
128 ビット幅のユニキャスト アドレス 119
IPv6 の DNS 119
IPv6 ユニキャストのパス MTU ディスカバリ 119
ICMPv6 119
ネイバー探索 120
DRP 120
IPv6 のステートレス自動設定および重複アドレス検出 120
IPv6 アプリケーション 120
DHCP for IPv6 アドレスの割り当て 121
IPv6 のスタティック ルート 121
RIP for IPv6 121
OSPF for IPv6 121
OSPFv3 グレースフル リスタート 121
高速コンバージェンス：LSA および SPF スロットリング 122
IPsec を使用した認証サポート 122
IPv6 の HSRP の設定 122
EIGRP IPv6 123
SNMP と Syslog、IPv6 による 123
IPv6 による HTTP（S） 124
サポートされていない IPv6 ユニキャスト ルーティング機能 124

IPv6 機能の制限 125
IPv6 の設定 125
IPv6 のデフォルト設定 125
IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化（CLI） 125
IPv6 でのファースト ホップ セキュリティの設定 128
IPv6 でのファースト ホップ セキュリティの前提条件 128
IPv6 でのファースト ホップ セキュリティの制約事項 128
IPv6 でのファースト ホップ セキュリティに関する情報 128
IPv6 スヌーピング ポリシーの設定方法 131
IPv6スヌーピングポリシーのインターフェイスまたはVLANへのアタッチ方法 133
デバイスでのIPv6ネイバー探索マルチキャスト抑制ポリシーのアタッチ方法 134
インターフェイスでの IPv6 ネイバー探索マルチキャスト抑制ポリシーのアタッチ方法 135
レイヤ 2 EtherChannel インターフェイスへの IPv6 ネイバー探索マルチキャスト抑制ポリシーのアタッチ方法 136
IPv6 DHCP ガード ポリシーの設定方法 137
IPv6 ソース ガードの設定方法 139
デフォルト ルータ プリファレンスの設定（CLI） 140
IPv6 ICMP レート制限の設定（CLI） 142
IPv6 の CEF および dCEF の設定 143
IPv6 のスタティック ルーティングの設定（CLI） 143
RIP for IPv6 の設定（CLI） 145
OSPF for IPv6 の設定（CLI） 148
OSPFv3 高速コンバージェンスに対する LSA および SPF タイマーの調整 150
OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定 152
IPv6 の EIGRP の設定 153
IPv6 の HSRP の設定 153
HSRP バージョン 2 のイネーブル化 154
IPv6 の HSRP グループのイネーブル化 155
Multi-VRF CE の設定 157

Multi-VRF CE のデフォルト設定 157
VRF の設定 157
VRF 認識サービスの設定 159
ネイバー探索用 VRF 認識サービスの設定 160
ping 用 VRF 認識サービスの設定 160
HSRP 用 VRF 認識サービスの設定 160
traceroute 用 VRF 認識サービスの設定 161
FTP および TFTP 用 VRF 認識サービスの設定 162
VPN ルーティング セッションの設定 163
BGP PE/CE ルーティング セッションの設定 165
Multi-VRF CE の設定例 166
Multi-VRF CE ステータスの表示 170
IPv6 の表示 170
DHCP for IPv6 アドレス割り当ての設定 171
DHCPv6 アドレス割り当てのデフォルト設定 171
DHCPv6 アドレス割り当ての設定時の注意事項 171
DHCPv6 サーバ機能のイネーブル化（CLI） 171
DHCPv6 クライアント機能のイネーブル化（CLI） 174
IPv6 ユニキャスト ルーティングの設定例 175
IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化：例 175
デフォルト ルータ プリファレンスの設定：例 176
IPv6 の HSRP グループのイネーブル化：例 176
DHCPv6 サーバ機能のイネーブル化：例 177
DHCPv6 クライアント機能のイネーブル化：例 177
IPv6 ICMP レート制限の設定：例 178
IPv6 のスタティック ルーティングの設定：例 178
IPv6 の RIP の設定：例 178
IPv6 の表示：例 178
IPv6 マルチキャストの実装 181
機能情報の確認 181
IPv6 マルチキャスト ルーティングの実装に関する情報 181
IPv6 マルチキャストの概要 182

IPv6 マルチキャスト ルーティングの実装 182
MLD アクセス グループ 183
受信側の明示的トラッキング 183
IPv6 マルチキャスト ユーザ認証およびプロファイル サポート 183
IPv6 MLD プロキシ 184
Protocol Independent Multicast 184
PIM スパース モード 184
指定スイッチ 185
Rendezvous Point 186
PIMv6 エニーキャスト RP ソリューションの概要 187
IPv6 BSR：RP マッピングの設定 187
PIM 送信元固有マルチキャスト 188
IPv6 用の SSM マッピング 188
PIM 共有ツリーおよびソース ツリー（最短パス ツリー） 189
Reverse Path Forwarding 189
ルーティング可能アドレスの hello オプション 190
双方向 PIM 191
スタティック mroute 191
MRIB 191
MFIB 192
IPv6 マルチキャスト VRF Lite 192
IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング 192
IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 193
IPv6 マルチキャストでの NSF と SSO のサポート 194
IPv6 マルチキャストの帯域幅ベースの CAC 194
IPv6 マルチキャストの実装 194
IPv6 マルチキャスト ルーティングのイネーブル化 194
MLD プロトコルのカスタマイズおよび確認 195
インターフェイスでの MLD のカスタマイズおよび確認 195
MLD グループ制限の実装 197
MLD グループ制限のグローバルな実装 197
MLD グループ制限のインターフェイス単位での実装 198

受信側の明示的トラッキングによってホストの動作を追跡するための設定 199
マルチキャスト ユーザ認証およびプロファイル サポートの設定 199
IPv6マルチキャストに対するAAAアクセス コントロールのイネーブル化 200
方式リストの指定およびマルチキャスト アカウンティングのイネーブル化 200
スイッチでの未認証マルチキャスト トラフィックの受信のディセーブル化 201
IPv6 での MLD プロキシのイネーブル化 202
MLD インターフェイスでの許可ステータスのリセット 203
MLD トラフィック カウンタのリセット 203
MLD インターフェイス カウンタのクリア 204
PIM の設定 204
PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示 204
PIM オプションの設定 206
双方向 PIM の設定および双方向 PIM 情報の表示 207
PIM トラフィック カウンタのリセット 208
PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット 209
BSR の設定 210
BSR の設定および BSR 情報の確認 211
BSR への PIM RP アドバタイズメントの送信 212
限定スコープ ゾーン内で BSR を使用できるようにするための設定 212
BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定 213
SSM マッピングの設定 214
スタティック mroute の設定 215
IPv6 マルチキャストでの MFIB の使用 217
IPv6 マルチキャストでの MFIB の動作の確認 217
MFIB トラフィック カウンタのリセット 218
レイヤ 2 219
IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定 221

機能情報の確認 221
トンネリング設定の前提条件 221
IEEE 802.1Q トンネリング 222
レイヤ 2 プロトコル トンネリング 223
EtherChannel のレイヤ 2 トンネリング 224
トンネリングについて 224
IEEE 802.1Q およびレイヤ 2 プロトコルの概要 224
IEEE 802.1Q トンネリング 225
IEEE 802.1Q トンネリング設定時の注意事項 228
ネイティブ VLAN 228
システム MTU 229
IEEE 802.1Q トンネリングのデフォルト設定 230
レイヤ 2 プロトコル トンネリングの概要 230
ポートでのレイヤ 2 プロトコル トンネリング 233
レイヤ 2 プロトコル トンネリングのデフォルト設定 234
トンネリングの設定方法 235
IEEE 802.1Q トンネリング ポートの設定 235
レイヤ 2 プロトコル トンネリングの設定 238
サービスプロバイダー エッジ スイッチの設定 241
カスタマー スイッチの設定 244
IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定例 247
例：IEEE 802.1Q トンネリング ポートの設定 247
例：レイヤ 2 プロトコル トンネリングの設定 248
例：サービスプロバイダー エッジ スイッチとカスタマー スイッチの設定 248
トンネリング ステータスのモニタリング 250
次の作業 251
スパニングツリー プロトコルの設定 253
機能情報の確認 253
STP の制約事項 253
スパニング ツリー プロトコルに関する情報 254
スパニングツリー プロトコル 254
スパニングツリー トポロジと BPDU 255

ブリッジ ID、デバイス プライオリティ、および拡張システム ID 256
ポート プライオリティとパス コスト 257
スパニングツリー インターフェイス ステート 258
ブロッキング ステート 259
リスニング ステート 260
ラーニング ステート 260
フォワーディング ステート 260
ディセーブル ステート 260
スイッチまたはポートがルート スイッチまたはルート ポートになる仕組み 261
スパニングツリーおよび冗長接続 262
スパニングツリー アドレスの管理 262
接続を維持するためのエージング タイムの短縮 262
スパニングツリー モードおよびプロトコル 263
サポートされるスパニングツリー インスタンス 264
スパニングツリーの相互運用性と下位互換性 264
STP および IEEE 802.1Q トランク 265
VLAN ブリッジ スパニングツリー 265
スパニングツリー機能のデフォルト設定 266
スパニングツリー機能の設定方法 267
スパニングツリー モードの変更 267
スパニング ツリーのディセーブル化 268
ルート スイッチの設定 269
セカンダリ ルート デバイスの設定 271
ポート プライオリティの設定 273
パス コストの設定 274
VLAN のデバイス プライオリティの設定 276
hello タイムの設定 277
VLAN の転送遅延時間の設定 278
VLAN の最大エージング タイムの設定 279
転送保留カウントの設定 280
スパニングツリー ステータスのモニタリング 281

複数のスパニング ツリー プロトコルの設定 283
機能情報の確認 283
MSTP の前提条件 283
MSTP の制約事項 284
MSTP について 285
MSTP の設定 285
MSTP 設定時の注意事項 286
ルート スイッチ 287
MST リージョン 288
IST、CIST、CST 288
MST リージョン内の動作 289
MST リージョン間の動作 290
IEEE 802.1s の用語 290
MST リージョンの図 291
ホップ カウント 292
境界ポート 293
IEEE 802.1s の実装 294
ポートの役割名の変更 294
レガシーおよび規格スイッチの相互運用 294
単一方向リンク障害の検出 295
IEEE 802.1D STP との相互運用性 296
RSTP 概要 296
ポートの役割およびアクティブ トポロジー 296
高速コンバージェンス 297
ポート ロールの同期 299
ブリッジ プロトコル データ ユニットの形式および処理 300
優位 BPDU 情報の処理 301
下位 BPDU 情報の処理 301
トポロジの変更 301
プロトコル移行プロセス 302
MSTP のデフォルト設定 303
MSTP 機能の設定方法 304

MST リージョン設定の指定と MSTP のイネーブル化 304
ルート スイッチの設定 307
セカンダリ ルート スイッチの設定 308
ポート プライオリティの設定 309
パス コストの設定 312
スイッチ プライオリティの設定 313
hello タイムの設定 315
転送遅延時間の設定 316
最大エージング タイムの設定 318
最大ホップ カウントの設定 319
高速移行を確実にするためのリンク タイプの指定 320
ネイバー タイプの設定 321
プロトコルの移行プロセスの再開 323
MST の設定およびステータスのモニタリング 324
MSTP の機能情報 325
オプションのスパニングツリー機能の設定 327
機能情報の確認 327
オプションのスパニング ツリー機能の制約事項 327
オプションのスパニングツリー機能について 328
PortFast 328
BPDU ガード 328
BPDU フィルタリング 329
UplinkFast 330
BackboneFast 332
EtherChannel ガード 335
ルート ガード 335
ループ ガード 336
オプションのスパニングツリー機能の設定方法 337
PortFast のイネーブル化 337
BPDU ガードのイネーブル化 338
BPDU フィルタリングのイネーブル化 340
冗長リンクで使用するための UplinkFast のイネーブル化 342
UplinkFast のディセーブル化 344

BackboneFast をイネーブル化 345
EtherChannel ガードのイネーブル化 346
ルート ガードのイネーブル化 347
ループ ガードのイネーブル化 349
スパニングツリー ステータスのモニタリング 350
双方向フォワーディング検出の設定 353
機能情報の確認 353
双方向フォワーディング検出の前提条件 353
双方向フォワーディング検出の制約事項 354
双方向フォワーディング検出について 354
BFD の動作 354
ネイバー関係 355
BFD の障害検出 356
BFD バージョンの相互運用性 356
BFD セッションの制限 356
非ブロードキャスト メディア インターフェイスに対する BFD サポート 357
ステートフル スイッチオーバーでのノンストップ フォワーディングの BFD サポート 357
ステートフル スイッチオーバーの BFD サポート 357
スタンバイ RP のステートフル BFD 357
スタティック ルーティングの BFD サポート 358
障害検出に BFD を使用することの利点 359
双方向フォワーディング検出の設定方法 359
インターフェイスでの BFD セッション パラメータの設定 359
ダイナミック ルーティング プロトコルに対する BFD サポートの設定 360
BGP に対する BFD サポートの設定 361
EIGRP に対する BFD サポートの設定 362
OSPF に対する BFD サポートの設定 364
すべてのインターフェイスの OSPF に対する BFD サポートの設定 365
1 つ以上のインターフェイスの OSPF に対する BFD サポートの設定 367
スタティック ルーティングに対する BFD サポートの設定 369
BFD エコー モードの設定 371

前提条件 371
制限事項 372
BFD 低速タイマーの設定 372
非対称性のない BFD エコー モードのディセーブル化 372
BFD のモニタリングとトラブルシューティング 373
双方向フォワーディング検出の設定例 374
例：エコーモードがデフォルトでイネーブルになったEIGRPネットワークでの BFD の設定 374
例：OSPF ネットワークでの BFD の設定 380
例：スタティック ルーティングに対する BFD サポートの設定 383
EtherChannel の設定 385
機能情報の確認 385
EtherChannel の制約事項 385
EtherChannel について 386
EtherChannel の概要 386
EtherChannel のモード 387
スイッチ上の EtherChannel 388
EtherChannel リンクのフェールオーバー 389
チャネル グループおよびポートチャネル インターフェイス 389
ポート集約プロトコル 391
PAgP モード 391
サイレント モード 392
PAgP 学習方式およびプライオリティ 393
PAgP と仮想スイッチとの相互作用およびデュアルアクティブ検出 394
PAgP と他の機能との相互作用 395
Link Aggregation Control Protocol 395
LACP モード 395
LACP と他の機能との相互作用 396
EtherChannel の On モード 396
ロードバランシングおよび転送方式 397
MAC アドレス転送 397
IP アドレス転送 398

ロードバランシングの利点 398
EtherChannel のデフォルト設定 399
EtherChannel 設定時の注意事項 401
レイヤ 2 EtherChannel 設定時の注意事項 403
EtherChannel の設定方法 404
レイヤ 2 EtherChannel の設定 404
EtherChannel ロード バランシングの設定 407
PAgP 学習方式およびプライオリティの設定 408
LACP ホット スタンバイ ポートの設定 409
LACP システム プライオリティの設定 410
LACP ポート プライオリティの設定 411
EtherChannel、PAgP、および LACP ステータスのモニタ 413
EtherChannel の設定例 414
レイヤ 2 EtherChannel の設定：例 414
リンクステート トラッキングの設定 415
機能情報の確認 415
リンク ステート トラッキングの設定の制約事項 415
リンクステート トラッキングの概要 416
リンクステート トラッキングの設定方法 419
リンクステート トラッキングのモニタリング 421
リンクステート トラッキングの設定：例 421
Resilient Ethernet Protocol の設定 423
機能情報の確認 423
REP の概要 423
リンク完全性 426
高速コンバージェンス 427
VLAN ロード バランシング 427
スパニングツリー インタラクション 429
REP ポート 429
REP の設定方法 430
REP のデフォルト設定 430
REP 設定時の注意事項 430

REP 管理 VLAN の設定 432
REP インターフェイスの設定 433
VLAN ロード バランシングの手動によるプリエンプションの設定 437
REP の SNMP トラップ設定 437
REP のモニタリング 439
REP の設定例 439
REP 管理 VLAN の設定：例 439
REP インターフェイスの設定：例 440
Flex Link および MAC アドレス テーブル移動更新機能の設定 443
機能情報の確認 443
Flex Link および MAC アドレス テーブル移動更新設定の制約事項 443
Flex Link および MAC アドレス テーブル移動更新に関する情報 444
Flex Link 444
Flex Link の設定 445
VLAN Flex Link ロード バランシングおよびサポート 446
Flex Link フェールオーバーによるマルチキャスト高速コンバージェンス 446
その他の Flex Link ポートを mrouter ポートとして学習 447
IGMP レポートの生成 447
IGMP レポートのリーク 447
MAC アドレス テーブル移動更新 448
Flex Link の VLAN ロード バランシング設定時の注意事項 450
MAC アドレス テーブル移動更新設定時の注意事項 450
デフォルトの Flex Link および MAC アドレス テーブル移動更新の設定 450
Flex Link および MAC アドレス テーブル移動更新機能の設定方法 451
Flex Link の設定 451
Flex Link ペアのプリエンプション方式の設定 452
Flex Link の VLAN ロード バランシングの設定 454
MAC アドレス テーブル移動更新の設定 456
MACアドレステーブル移動更新メッセージの取得および処理用のスイッチ設定 457
Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタリング 458

Flex Link の設定例 459
Flex Link の設定：例 459
Flex Link における VLAN ロード バランシングの設定：例 460
MAC アドレス テーブル移動更新の設定：例 461
Flex Link フェールオーバーによるマルチキャスト高速コンバージェンスの設定: 例 462
単方向リンク検出の設定 465
機能情報の確認 465
UDLD 設定の制約事項 465
UDLD について 466
動作モード 466
通常モード 466
Aggressive Mode 467
単一方向の検出方法 467
ネイバー データベース メンテナンス 468
イベントドリブン検出およびエコー 468
UDLD リセット オプション 468
UDLD のデフォルト設定 469
UDLD の設定方法 469
UDLD のグローバルなイネーブル化 469
インターフェイスでの UDLD のイネーブル化 471
UDLD のモニタおよびメンテナンス 472
High Availability（高可用性） 473
HSRP および VRRP の設定 475
HSRP の設定 475
機能情報の確認 475
HSRP の設定に関する情報 476
HSRP の概要 476
HSRP のバージョン 478
MHSRP 478
SSO HSRP 479
HSRP の設定方法 480
HSRP のデフォルト設定 480

HSRP HSRP 設定時の注意事項 480
HSRP のイネーブル化 481
HSRP のプライオリティの設定 483
MHSRP の設定 486
ルータ A の設定 487
ルータ B の設定 491
HSRP 認証およびタイマーの設定 495
ICMP リダイレクト メッセージの HSRP サポートのイネーブル化 496
HSRP グループおよびクラスタリングの設定 497
HSRP のトラブルシューティング 497
HSRP の確認 497
HSRP コンフィギュレーションの確認 497
HSRP の設定例 498
HSRP のイネーブル化：例 498
HSRP のプライオリティの設定：例 498
MHSRP の設定：例 499
HSRP 認証およびタイマーの設定：例 499
HSRP グループおよびクラスタリングの設定：例 500
VRRP の概要 500
VRRP の設定 500
VRRP の制約事項 500
サービス レベル契約の設定 501
機能情報の確認 501
SLA の制約事項 501
SLA について 502
Cisco IOS IP サービス レベル契約（SLA） 502
Cisco IOS IP SLA でのネットワーク パフォーマンスの測定 503
IP SLA レスポンダおよび IP SLA 制御プロトコル 504
IP SLA の応答時間の計算 505
IP SLA 動作のスケジューリング 506
IP SLA 動作のしきい値のモニタリング 506
UDP Jitter 507

IP SLA 動作の設定方法 508
デフォルト設定 508
設定時の注意事項 508
IP SLA レスポンダの設定 509
IP SLA ネットワーク パフォーマンス測定の実装 511
UDP ジッター動作を使用した IP サービス レベルの分析 515
ICMP エコー動作を使用した IP サービス レベルの分析 519
IP SLA 動作のモニタリング 522
IP SLA 動作のモニタリングの例 523
拡張オブジェクト トラッキングの設定 525
機能情報の確認 525
拡張オブジェクト トラッキングに関する情報 525
拡張オブジェクト トラッキングの概要 525
インターフェイス ラインプロトコルまたは IP ルーティング ステートのトラッキング 526
追跡リスト 527
他の特性のトラッキング 527
IP SLA オブジェクト トラッキング 527
スタティック ルート オブジェクト トラッキング 528
拡張オブジェクト トラッキングの設定方法 528
インターフェイスでのライン ステート プロトコルまたは IP ルーティング ステートのトラッキングの設定 528
追跡リストの設定 530
重みしきい値による追跡リストの設定 530
パーセントしきい値による追跡リストの設定 532
HSRP オブジェクト トラッキングの設定 534
IP SLA オブジェクト トラッキングの設定 538
スタティック ルート オブジェクト トラッキングの設定 540
スタティック ルーティング用のプライマリ インターフェイスの設定 540
DHCP のプライマリ インターフェイスの設定 541
IP SLA モニタリング エージェントの設定 542
ルーティング ポリシーおよびデフォルト ルートの設定 545

拡張オブジェクト トラッキングのモニタリング 547
Network Management 549
Cisco IOS Configuration Engine の設定 551
機能情報の確認 551
Configuration Engine を設定するための前提条件 551
Configuration Engine の設定に関する制約事項 552
Configuration Engine の設定について 552
Cisco Configuration Engine ソフトウェア 552
コンフィギュレーション サービス 553
イベント サービス 554
名前空間マッパー 554
Cisco Networking Service ID およびデバイスのホスト名 554
ConfigID 555
DeviceID 555
ホスト名および DeviceID 555
ホスト名、DeviceID、および ConfigID 556
Cisco IOS CNS エージェント 556
初期設定 556
差分（部分的）設定 557
コンフィギュレーションの同期 558
自動 CNS 設定 558
Configuration Engine の設定方法 559
CNS イベント エージェントのイネーブル化 559
Cisco IOS CNS エージェントのイネーブル化 561
Cisco IOS CNS エージェントの初期設定のイネーブル化 563
DeviceID の更新 569
Cisco IOS CNS エージェントの部分的設定のイネーブル化 571
CNS 設定のモニタリング 573
Cisco Discovery Protocol の設定 575
機能情報の確認 575
CDP に関する情報 575
CDP の概要 575
CDP のデフォルト設定 576

CDP の設定方法 577
CDP 特性の設定 577
CDP のディセーブル化 579
CDP のイネーブル化 580
インターフェイス上での CDP のディセーブル化 582
インターフェイス上での CDP のイネーブル化 583
CDP のモニタおよびメンテナンス 585
簡易ネットワーク管理プロトコルの設定 587
機能情報の確認 587
SNMP の前提条件 587
SNMP の制約事項 590
SNMP に関する情報 591
SNMP の概要 591
SNMP マネージャ機能 591
SNMP エージェント機能 592
SNMP コミュニティ ストリング 592
SNMP MIB 変数アクセス 593
SNMP 通知 593
SNMP ifIndex MIB オブジェクト値 594
SNMP のデフォルト設定 594
SNMP 設定時の注意事項 595
SNMP の設定方法 596
SNMP エージェントのディセーブル化 596
コミュニティ ストリングの設定 598
SNMP グループおよびユーザの設定 601
SNMP 通知の設定 606
エージェント コンタクトおよびロケーションの設定 613
SNMP を通して使用する TFTP サーバの制限 614
SNMP ステータスのモニタリング 616
SNMP の例 617
SPAN および RSPAN の設定 619
機能情報の確認 619

SPAN および RSPAN の前提条件 619
SPAN および RSPAN の制約事項 620
SPAN および RSPAN について 623
SPAN および RSPAN 623
ローカル SPAN 623
リモート SPAN 625
SPAN と RSPAN の概念および用語 626
SPAN セッション 626
モニタ対象トラフィック 627
送信元ポート 629
送信元 VLAN 629
VLAN フィルタリング 630
宛先ポート 630
RSPAN VLAN 631
SPAN および RSPAN と他の機能の相互作用 632
フローベースの SPAN 633
SPAN および RSPAN のデフォルト設定 635
設定時の注意事項 635
SPAN 設定時の注意事項 635
RSPAN 設定時の注意事項 635
FSPAN および FRSPAN 設定時の注意事項 636
SPAN および RSPAN の設定方法 637
ローカル SPAN セッションの作成 637
ローカル SPAN セッションの作成および着信トラフィックの設定 640
フィルタリングする VLAN の指定 642
RSPAN VLAN としての VLAN の設定 645
RSPAN 送信元セッションの作成 647
フィルタリングする VLAN の指定 649
RSPAN 宛先セッションの作成 652
RSPAN 宛先セッションの作成および着信トラフィックの設定 654
FSPAN セッションの設定 657
FRSPAN セッションの設定 660

SPAN および RSPAN 動作のモニタリング 664
SPAN および RSPAN の設定例 664
例：ローカル SPAN の設定 664
例：RSPAN VLAN の作成 665
RMON の設定 667
機能情報の確認 667
RMON について 667
RMON の概要 667
RMON の設定方法 669
RMON のデフォルト設定 669
RMON アラームおよびイベントの設定 669
インターフェイス上でのグループ履歴統計情報の収集 672
インターフェイス上でのイーサネット グループ統計情報の収集 673
RMON ステータスのモニタリング 675
Embedded Event Manager の設定 677
Embedded Event Manager について 677
Embedded Event Manager の概要 677
Embedded Event Manager のアクション 678
Embedded Event Manager ポリシー 679
Embedded Event Manager の環境変数 679
Embedded Event Manager 3.2 680
Embedded Event Manager の設定方法 680
Embedded Event Manager アプレットの登録と定義 680
Embedded Event Manager TCL スクリプトの登録と定義 682
Embedded Event Manager のモニタリング 683
Embedded Event Manager 情報の表示 683
Embedded Event Manager の設定例 684
例：SNMP 通知の生成 684
例：EEM イベントへの応答 684
例：EEM 環境変数の表示 684
NetFlow Lite の設定 685
機能情報の確認 685

NetFlow Lite の前提条件 685
NetFlow Lite の制約事項 686
NetFlow Lite について 687
NetFlow Lite の概要 687
Flexible NetFlow のコンポーネント 688
フロー レコード 688
NetFlow の事前定義済みのレコード 689
ユーザ定義レコード 689
NetFlow Liteの match パラメータ 689
NetFlow Lite の collect パラメータ 691
フロー エクスポータ 692
フロー モニタ 694
フロー サンプラー 696
デフォルト設定 697
NetFlow Lite の設定方法 697
フロー レコードの作成 697
フロー エクスポータの作成 700
フロー モニタの作成 703
サンプラーの作成 705
インターフェイスへのフローの適用 707
VLAN 上でのブリッジ型 NetFlow の設定 708
レイヤ 2 NetFlow の設定 709
Flexible NetFlow のモニタリング 711
NetFlow Lite の設定例 712
例：フローの設定 712
Web Cache Communication Protocol を使用したキャッシュ サービスの設定 715
機能情報の確認 715
WCCP の前提条件 715
WCCP に関する制約事項 716
WCCP に関する情報 717
WCCP の概要 717
WCCP メッセージ交換 718

WCCP ネゴシエーション 718
MD5 セキュリティ 719
パケットのリダイレクトおよびサービス グループ 719
WCCP の設定方法 721
WCCP のデフォルト設定 721
キャッシュ サービスのイネーブル化 721
QoS 729
QoS の設定 731
機能情報の確認 731
QoS の前提条件 731
QoS ACL の注意事項 732
ポリシングの注意事項 732
一般的な QoS の注意事項 733
QoS の制約事項 733
QoS の概要 734
QoS の実装 734
レイヤ 2 フレームのプライオリティ ビット 735
レイヤ 3 パケットのプライオリティ ビット 736
分類を使用したエンドツーエンドの QoS ソリューション 736
QoS 基本モデル 736
入力ポートでのアクション 737
出力ポートでのアクション 737
分類の概要 738
Non-IP のトラフィック分類 738
IP のトラフィック分類 739
分類フローチャート 741
アクセス コントロール リスト 741
クラス マップおよびポリシー マップに基づく分類 742
ポリシングおよびマーキングの概要 743
物理ポートのポリシング 744
マッピング テーブルの概要 746
キューイングおよびスケジューリングの概要 747
WTD 747

SRR のシェーピングおよび共有 748
入力キューでのキューイングおよびスケジューリング 749
設定可能な入力キュー タイプ 750
WTD しきい値 751
バッファおよび帯域幅の割り当て 751
プライオリティ キューイング 751
出力キューでのキューイングおよびスケジューリング 752
出力緊急キュー 753
出力キューのバッファ割り当て 753
バッファおよびメモリの割り当て 754
キューおよび WTD しきい値 754
シェーピング モードまたは共有モード 755
パケットの変更 756
標準 QoS のデフォルト設定 756
入力キューのデフォルト設定 757
出力キューのデフォルト設定 758
マッピング テーブルのデフォルト設定 761
DSCP マップ 762
デフォルトの CoS/DSCP マップ 762
デフォルトの IP Precedence/DSCP マップ 763
デフォルトの DSCP/CoS マップ 763
QoS の設定方法 764
QoS のグローバルなイネーブル化 764
ポートの信頼状態による分類の設定 765
QoS ドメイン内のポートの信頼状態の設定 766
インターフェイスの CoS 値の設定 768
ポート セキュリティを確保するための信頼境界の設定 770
DSCP トランスペアレント モードのイネーブル化 773
DSCP 透過モード 774
別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定 775
QoS ポリシーの設定 777
ACL を使用したトラフィックの分類 778

IPv4 トラフィック用の IP 標準 ACL の作成 778
IPv4 トラフィック用の IP 拡張 ACL の作成 779
IPv6 トラフィック用の IPv6 ACL の作成 781
非 IP トラフィック用のレイヤ 2 MAC ACL の作成 784
クラス マップによるトラフィックの分類 786
クラスマップの使用と IPv6 トラフィックのフィルタリングによるトラフィックの分類 789
ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング 791
集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング 796
DSCP マップの設定 799
CoS/DSCP マップの設定 799
IP precedence/DSCP マップの設定 801
ポリシング済み DSCP マップの設定 802
DSCP/CoS マップの設定 804
DSCP/DSCP 変換マップの設定 805
入力キューの特性の設定 807
入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定 808
入力キュー間のバッファ スペースの割り当て 810
入力キュー間の帯域幅の割り当て 812
入力プライオリティ キューの設定 813
出力キューの特性の設定 815
設定時の注意事項 816
出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定 816
出力キューおよびしきい値 ID への DSCP または CoS 値のマッピング 820
出力キューでの SRR シェーピング重みの設定 822
出力キューでの SRR 共有重みの設定 824
出力緊急キューの設定 826
出力インターフェイスの帯域幅の制限 828

標準 QoS のモニタリング 830
QoS の設定例 831
例：DSCP 信頼状態へのポートの設定および DSCP/DSCP 変換マップの変更 831
例：ACL によるトラフィックの分類 831
例：クラス マップによるトラフィックの分類 832
例：ポリシー マップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング 834
例：階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング 835
例：集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング 837
例：DSCP マップの設定 838
例：入力キューの特性の設定 840
例：出力キューの特性の設定 840
次の作業 842
auto-QoS の設定 843
機能情報の確認 843
自動 QoS の前提条件 843
自動 QoS の設定に関する情報 844
自動 QoS の概要 844
自動 QoS 短縮機能の概要 844
生成された自動 QoS 設定 845
VOIP デバイスの詳細 845
ビデオ、信頼、および分類用の拡張自動 QoS 847
自動 QoS 設定の移行 847
自動 QoS 設定時の注意事項 848
自動 QoS VoIP に関する考慮事項 848
拡張された自動 QoS に関する考慮事項 849
実行コンフィギュレーションでの自動 QoS の影響 849
実行コンフィギュレーションに対する自動 QoS 短縮機能の影響 849
自動 QoS の設定方法 850

auto-QoS の設定 850
自動 QoS のイネーブル化 850
自動 QoS 短縮機能のイネーブル化 852
自動 QoS に関するトラブルシューティング 854
自動 QoS のモニタリング 854
自動 QoS の設定例 855
例：グローバルな自動 QoS 設定 855
例：VoIP デバイス用に生成される自動 QoS 設定 858
例：VoIP デバイス用に生成される自動 QoS 設定 861
例：拡張されたビデオ、信頼、および分類デバイス用に自動 QoS で生成される設定 862
auto qos global compact 864
自動 QoS の関連情報 865
ルーティング 867
IP ユニキャスト ルーティングの設定 869
機能情報の確認 870
IP ユニキャスト ルーティングの設定に関する情報 870
IP ルーティングに関する情報 870
ルーティング タイプ 871
IP ルーティングの設定方法 871
IP アドレッシングの設定方法 872
IP アドレス指定のデフォルト設定 873
ネットワーク インターフェイスへの IP アドレスの割り当て 874
サブネット ゼロの使用 876
クラスレス ルーティング 877
クラスレス ルーティングのディセーブル化 879
アドレス解決方法の設定 880
アドレス解決 880
スタティック ARP キャッシュの定義 881
ARP のカプセル化の設定 883
プロキシ ARP のイネーブル化 884
IP ルーティングがディセーブルの場合のルーティング支援機能 885

プロキシ ARP 885
プロキシ ARP 885
デフォルト ゲートウェイ 886
ICMP Router Discovery Protocol 887
ICMP Router Discovery Protocol（IRDP） 887
ブロードキャスト パケットの処理方法の設定 889
ブロードキャスト パケットの処理 889
ダイレクトブロードキャストから物理ブロードキャストへの変換のイネーブル化 890
UDP ブロードキャスト パケットおよびプロトコル 892
UDP ブロードキャスト パケットおよびプロトコルの転送 892
IP ブロードキャスト アドレスの確立 894
IP ブロードキャストのフラッディング 895
IP ブロードキャストのフラッディング 896
IP アドレスのモニタリングおよびメンテナンス 898
IP ユニキャスト ルーティングの設定方法 899
IP ユニキャスト ルーティングのイネーブル化 899
IP ユニキャスト ルーティングのイネーブル化の例 900
RIP 情報 900
RIP の設定方法 901
RIP のデフォルト設定 901
基本的な RIP パラメータの設定 902
RIP 認証の設定 905
サマリー アドレスおよびスプリット ホライズン 906
サマリー アドレスおよびスプリット ホライズンの設定 906
スプリット ホライズンの設定 908
サマリー アドレスおよびスプリット ホライズンの設定例 909
OSPF に関する情報 910
OSPF の設定方法 911
OSPF のデフォルト設定 911
ルーテッド アクセスの OSPF 912
OSPF NSF 913
OSPF NSF 認識 913

OSPF NSF 対応 913
基本的な OSPF パラメータの設定 914
例：基本的な OSPF パラメータの設定 915
OSPF インターフェイスの設定 916
OSPF エリア パラメータ 918
OSPF エリア パラメータの設定 919
その他の OSPF パラメータ 920
その他の OSPF パラメータの設定 922
LSA グループ ペーシング 924
LSA グループ ペーシングの変更 924
ループバック インターフェイス 925
ループバック インターフェイスの設定 926
OSPF のモニタリング 926
EIGRP に関する情報 927
EIGRP の機能 928
EIGRP コンポーネント 928
EIGRP の設定方法 929
EIGRP のデフォルト設定 930
EIGRP NSF 931
EIGRP NSF 認識 931
EIGRP NSF 対応 932
基本的な EIGRP パラメータの設定 932
EIGRP インターフェイスの設定 934
EIGRP ルート認証の設定 936
EIGRP スタブ ルーティング 938
EIGRP のモニタリングおよびメンテナンス 939
BGP に関する情報 940
BGP ネットワーク トポロジ 940
BGP の設定方法 941
BGP のデフォルト設定 941
NSF 認識 945
BGP ルーティングに関する情報 945

BGP ルーティングのイネーブル化 946
例：ルータでの BGP の設定 948
ルーティング ポリシーの変更 949
ルーティング ポリシー変更の管理 950
BGP 判断属性 951
BGP 判断属性の設定 953
ルート マップ 955
ルート マップによる BGP フィルタリングの設定 955
BGP フィルタリング 956
ネイバーによる BGP フィルタリングの設定 957
アクセス リストおよびネイバーによる BGP フィルタリングの設定 958
BGP フィルタリングのプレフィックス リスト 959
BGP フィルタリング用のプレフィックス リストの設定 960
BGP コミュニティ フィルタリング 961
BGP コミュニティ フィルタリングの設定 962
BGP ネイバーおよびピア グループ 964
BGP ネイバーおよびピア グループの設定 964
集約ルート 967
ルーティング テーブルでの集約アドレスの設定 967
ルーティング ドメイン コンフェデレーション 969
ルーティング ドメイン連合の設定 969
BGP ルート リフレクタ 970
BGP ルート リフレクタの設定 971
ルート ダンプニング 972
ルート ダンプニングの設定 973
BGP の追加情報 974
BGP のモニタリングおよびメンテナンス 974
ISO CLNS ルーティングに関する情報 976
コネクションレス型ルーティング 976
ISO CLNS ルーティングの設定方法 977
IS-IS ダイナミック ルーティング 977
IS-IS のデフォルト設定 978

NSF 認識 979
IS-IS ルーティングのイネーブル化 979
例：IS-IS ルーティングの設定 981
IS-IS グローバル パラメータ 982
IS-IS グローバル パラメータの設定 983
IS-IS インターフェイス パラメータ 987
IS-IS インターフェイス パラメータの設定 988
ISO IGRP と IS-IS のモニタリングおよびメンテナンス 990
Multi-VRF CE に関する情報 993
Multi-VRF CE の概要 993
ネットワーク トポロジ 994
パケット転送処理 995
ネットワーク コンポーネント 995
VRF 認識サービス 995
Multi-VRF CE の設定方法 996
Multi-VRF CE のデフォルト設定 996
Multi-VRF CE の設定時の注意事項 997
VRF の設定 1000
VRF 認識サービスの設定 1001
ARP 用 VRF 認識サービスの設定 1002
ping 用 VRF 認識サービスの設定 1002
SNMP 用 VRF 認識サービスの設定 1002
HSRP 用 VRF 認識サービスの設定 1004
uRPF 用 VRF 認識サービスの設定 1005
VRF 認識 RADIUS の設定 1006
syslog 用 VRF 認識サービスの設定 1006
traceroute 用 VRF 認識サービスの設定 1007
FTP および TFTP 用 VRF 認識サービスの設定 1008
マルチキャスト VRF の設定 1009
VPN ルーティング セッションの設定 1011
BGP PE/CE ルーティング セッションの設定 1013
Multi-VRF CE の設定例 1014

Multi-VRF CE のモニタリング 1018
ユニキャスト リバース パス転送の設定 1018
プロトコル独立機能 1019
分散型シスコ エクスプレス フォワーディング 1019
シスコ エクスプレス フォワーディングに関する情報 1019
シスコ エクスプレス フォワーディングの設定方法 1020
等コスト ルーティング パスの個数 1022
等コスト ルーティング パスに関する情報 1022
等コスト ルーティング パスの設定方法 1023
スタティック ユニキャスト ルート 1023
スタティック ユニキャスト ルートに関する情報 1023
スタティック ユニキャスト ルートの設定 1024
デフォルトのルートおよびネットワーク 1026
デフォルトのルートおよびネットワークに関する情報 1026
デフォルトのルートおよびネットワークの設定方法 1027
ルーティング情報を再配信するためのルート マップ 1027
ルート マップの概要 1027
ルート マップの設定方法 1028
ルート配信の制御方法 1032
Policy-Based Routing：ポリシーベース ルーティング 1034
ポリシーベース ルーティングの概要 1034
PBR の設定方法 1036
ルーティング情報のフィルタリング 1039
受動インターフェイスの設定 1039
ルーティング アップデートのアドバタイズおよび処理の制御 1040
ルーティング情報の送信元のフィルタリング 1042
認証キーの管理 1043
前提条件 1043
認証キーの設定方法 1043
IP ネットワークのモニタリングおよびメンテナンス 1045
フォールバック ブリッジングの設定 1047
機能情報の確認 1047

フォールバック ブリッジングの制約事項 1047
フォールバック ブリッジングに関する情報 1048
フォールバック ブリッジングの概要 1048
例：フォールバック ブリッジング ネットワーク 1049
フォールバック ブリッジングの設定方法 1050
ブリッジ グループの作成 1050
スパニングツリー パラメータの調整 1052
VLAN ブリッジ スパニング ツリーのプライオリティの変更 1052
インターフェイスのプライオリティの変更 1054
パス コストの割り当て 1055
BPDU 間隔の調整 1057
hello BPDU 間のインターバルの調整 1057
転送遅延時間の変更 1059
最大アイドル時間の変更 1060
インターフェイスでのスパニング ツリーのディセーブル化 1061
フォールバック ブリッジングのモニタリングおよびメンテナンス 1063
フォールバック ブリッジングのデフォルト設定 1063
マルチキャスト ルーティング 1065
IP マルチキャスト ルーティング テクノロジーの概要 1067
機能情報の確認 1067
IP マルチキャスト テクノロジーに関する情報 1067
情報配信における IP マルチキャストの役割 1067
IP マルチキャスト ルーティング プロトコル 1068
マルチキャスト グループ伝送方式 1068
IP マルチキャスト境界 1070
IP マルチキャスト グループ アドレッシング 1071
IP クラス D アドレス 1071
IP マルチキャスト アドレスのスコーピング 1071
レイヤ 2 マルチキャスト アドレス 1073
IP マルチキャスト配信モード 1074
Source Specific Multicast 1074
IGMP の設定 1075

機能情報の確認 1075
IGMP の前提条件 1075
IGMP 設定の制約事項 1076
IGMP に関する情報 1076
Internet Group Management Protocol の役割 1076
IGMP マルチキャスト アドレス 1077
IGMP のバージョン 1077
IGMPv1 1078
IGMPv2 1078
IGMP バージョン 3 1078
IGMPv3 ホスト シグナリング 1078
IGMP のバージョンの違い 1079
IGMP の加入および脱退処理 1081
IGMP の加入処理 1081
IGMP の脱退処理 1082
IGMP のデフォルト設定 1083
IGMP の設定方法 1083
グループのメンバとしてのスイッチの設定 1083
IP マルチキャスト グループへのアクセスの制御 1085
IGMP バージョンの変更 1088
IGMP ホストクエリー メッセージ インターバルの変更 1089
IGMPv2 の IGMP クエリー タイムアウトの変更 1091
IGMPv2 の最大クエリー応答時間の変更 1093
静的に接続されたメンバとしてのスイッチの設定 1094
IGMP のモニタリング 1096
IGMP の設定例 1097
例：マルチキャスト グループのメンバとしてのスイッチの設定 1097
例：IP マルチキャスト グループへのアクセスの制御 1097
CGMP の設定 1099
機能情報の確認 1099
CGMP の設定の前提条件 1099
CGMP の制約事項 1100
CGMP に関する情報 1100

CGMP サーバ サポートのイネーブル化 1100
CGMP のモニタリング 1102
PIM の設定 1105
機能情報の確認 1105
PIM の前提条件 1105
PIM に関する制約事項 1106
PIMv1 および PIMv2 の相互運用性 1106
PIM スタブ ルーティングの設定に関する制約事項 1107
Auto-RP および BSR の設定に関する制約事項 1107
PIM に関する情報 1109
Protocol Independent Multicast 1109
PIM デンス モード（PIM-DM） 1109
PIM スパース モード（PIM-SM） 1110
スパース-デンス モード 1111
PIM のバージョン 1112
PIM スタブ ルーティング 1113
IGMP ヘルパー 1114
ランデブー ポイント 1114
Auto-RP 1115
Auto-RP のスパース - デンス モード 1116
ブートストラップ ルータ 1117
PIM ドメイン境界 1117
マルチキャスト転送 1117
マルチキャスト配信のソース ツリー 1118
マルチキャスト配信の共有ツリー 1119
ソース ツリーの利点 1120
共有ツリーの利点 1120
PIM 共有ツリーおよびソース ツリー 1120
リバース パス フォワーディング 1122
RPF チェック 1123
PIM ルーティングのデフォルト設定 1124
PIM の設定方法 1125
PIM スタブ ルーティングのイネーブル化 1125

ランデブー ポイントの設定 1126
マルチキャスト グループへの RP の手動割り当て 1127
新規インターネットワークでの Auto-RP の設定 1130
既存のスパース モード クラウドへの Auto-RP の追加 1134
単一スタティック RP でのスパース モードの設定 1138
問題のある RP への Join メッセージの送信禁止 1141
着信 RP アナウンスメント メッセージのフィルタリング 1142
PIMv2 BSR の設定 1144
PIM ドメイン境界の定義 1144
IP マルチキャスト境界の定義 1146
候補 BSR の設定 1148
候補 RP の設定 1150
PIM 最短パス ツリーの使用の延期 1152
PIM ルータクエリー メッセージ間隔の変更 1154
PIM の動作の確認 1156
PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト動作の確認 1156
ファースト ホップ ルータでの IP マルチキャストの確認 1156
SPT 上のルータでの IP マルチキャストの確認 1157
ラスト ホップ ルータでの IP マルチキャスト動作の確認 1159
PIM 対応ルータを使用した IP マルチキャストの到達可能性のテスト 1163
マルチキャスト ping に応答するルータの設定 1163
マルチキャスト ping に応答するように設定されたルータへの ping 1164
PIM のモニタリングとトラブルシューティング 1165
PIM 情報のモニタリング 1165
RP マッピングおよび BSR 情報のモニタリング 1165
PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング 1166
PIM の設定例 1167
例：PIM スタブ ルーティングのイネーブル化 1167
例：PIM スタブ ルーティングの確認 1167
例：マルチキャスト グループへの RP の手動割り当て 1168
例：Auto-RP の設定 1168

例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義 1168
例：着信 RP アナウンスメント メッセージのフィルタリング 1169
例：問題のある RP への Join メッセージの送信禁止 1169
例：候補 BSR の設定 1169
例：候補 RP の設定 1170
HSRP 認識 PIM の設定 1171
HSRP 認識 PIM 1171
機能情報の確認 1171
HSRP 認識 PIM の制約事項 1171
HSRP 認識 PIM に関する情報 1172
HSRP 1172
HSRP 認識 PIM 1173
HSRP 認識 PIM の設定方法 1174
インターフェイスでの HSRP グループの設定 1174
PIM 冗長性の設定 1176
HSRP 認識 PIM の設定例 1177
例：インターフェイスでの HSRP グループの設定 1177
例：PIM 冗長性の設定 1177
VRRP 認識 PIM の設定 1179
VRRP 認識 PIM 1179
機能情報の確認 1179
VRRP 認識 PIM の制約事項 1179
VRRP 認識 PIM に関する情報 1180
VRRP 認識 PIM の概要 1180
VRRP 認識 PIM の設定方法 1181
VRRP 認識 PIM の設定 1181
VRRP 認識 PIM の設定例 1183
例：VRRP 認識 PIM 1183
基本的な IP マルチキャスト ルーティングの設定 1185
機能情報の確認 1185
基本的な IP マルチキャスト ルーティングの前提条件 1185
基本的な IP マルチキャスト ルーティングの制約事項 1186

基本的な IP マルチキャスト ルーティングに関する情報 1186
IP マルチキャスト ルーティングのデフォルト設定 1187
sdr リスナー サポート 1187
基本的な IP マルチキャスト ルーティングの設定方法 1188
基本的な IP マルチキャスト ルーティングの設定 1188
オプションの IP マルチキャスト ルーティングの設定 1190
IP マルチキャスト境界の定義 1190
マルチキャスト VRF の設定 1192
SAP リスナーを使用したマルチキャスト マルチメディア セッションのアドバタイジング 1195
基本的な IP マルチキャスト ルーティングのモニタリングおよびメンテナンス 1196
キャッシュ、テーブル、およびデータベースのクリア 1196
システムおよびネットワーク統計情報の表示 1197
SSM の設定 1199
機能情報の確認 1199
SSM の設定の前提条件 1199
SSM 設定の制約事項 1200
SSM および SSM マッピングに関する情報 1201
SSM コンポーネント 1201
Internet Standard Multicast と SSM の違い 1202
SSM の動作 1203
IGMPv3 ホスト シグナリング 1203
の利点 1204
SSM マッピングの概要 1205
スタティック SSM マッピング 1206
DNS ベースの SSM マッピング 1206
SSM マッピングの利点 1208
SSM および SSM マッピングの設定方法 1209
SSM の設定 1209
SSM マッピングの設定 1211
スタティック SSM マッピングの設定 1211
DNS ベースの SSM マッピングの設定 1213

SSM マッピングを使用したスタティック トラフィック転送の設定 1215
SSM マッピングの設定と動作の確認 1217
SSM および SSM マッピングのモニタリング 1219
SSM のモニタリング 1219
SSM マッピングのモニタリング 1219
SSM および SSM マッピングの設定例 1220
IGMPv3 を使用した SSM の例 1220
SSM フィルタリングの例 1220
SSM マッピングの例 1221
DNS サーバの設定例 1224
IGMP スヌーピングおよびマルチキャスト VLAN レジストレーションの設定 1227
機能情報の確認 1227
IGMP スヌーピングおよび MVR の設定の前提条件 1227
IGMP スヌーピングの前提条件 1227
MVR の前提条件 1228
IGMP スヌーピングおよび MVR の設定の制約事項 1228
IGMP スヌーピングの制約事項 1228
MVR の制約事項 1229
IGMP スヌーピングおよび MVR に関する情報 1230
IGMP スヌーピング 1230
IGMP のバージョン 1231
マルチキャスト グループへの加入 1232
マルチキャスト グループからの脱退 1234
即時脱退 1234
IGMP 設定可能 Leave タイマー 1235
IGMP レポート抑制 1235
IGMP スヌーピングのデフォルト設定 1235
マルチキャスト VLAN レジストレーション 1236
MVR と IGMP 1236
動作モード 1237
マルチキャスト TV アプリケーションでの MVR 1237
MVR のデフォルト設定 1239

IGMP フィルタリングおよびスロットリング 1240
IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定 1241
IGMP スヌーピングおよび MVR の設定方法 1241
スイッチでの IGMP スヌーピングのイネーブル化またはディセーブル化 1241
VLAN インターフェイスでの IGMP スヌーピングのイネーブル化またはディセーブル化 1243
スヌーピング方法の設定 1244
マルチキャスト ルータ ポートの設定 1246
グループに加入するホストの静的な設定 1248
IGMP 即時脱退のイネーブル化 1249
IGMP 脱退タイマーの設定 1251
TCN 関連コマンドの設定 1253
TCN イベント後のマルチキャスト フラッディング時間の制御 1253
フラッディング モードからの回復 1254
TCN イベント中のマルチキャスト フラッディングのディセーブル化 1255
IGMP スヌーピング クエリアの設定 1257
IGMP レポート抑制のディセーブル化 1260
MVR グローバル パラメータの設定 1261
MVR インターフェイスの設定 1264
IGMP プロファイルの設定 1267
IGMP プロファイルの適用 1269
IGMP グループの最大数の設定 1271
IGMP スロットリング アクションの設定 1272
IGMP スヌーピングおよび MVR のモニタリング 1275
IGMP スヌーピング情報のモニタリング 1275
MVR のモニタリング 1276
IGMP フィルタリングおよび IGMP スロットリングの設定のモニタリング 1277
IGMP スヌーピングおよび MVR の設定例 1278
例：CGMP パケットを使用した IGMP スヌーピングの設定 1278
例：マルチキャスト ルータへの静的な接続のイネーブル化 1278
例：グループに加入するホストの静的な設定 1278
例：IGMP 即時脱退のイネーブル化 1279

例：IGMP スヌーピング クエリアの送信元アドレスの設定 1279
例：IGMP スヌーピング クエリアの最大応答時間の設定 1279
例：IGMP スヌーピング クエリア タイムアウトの設定 1279
例：IGMP スヌーピング クエリア機能の設定 1280
例：IGMP プロファイルの設定 1280
例：IGMP プロファイルの適用 1280
例：IGMP グループの最大数の設定 1280
例：MVR グローバル パラメータの設定 1280
例：MVR インターフェイスの設定 1281
MSDP の設定 1283
機能情報の確認 1283
MSDP の前提条件 1283
Multicast Source Discovery Protocol に関する情報 1284
1284
MSDP の利点 1286
デフォルト MSDP ピア 1287
MSDP メッシュ グループ 1288
MSDP メッシュ グループの利点 1289
SA 発信フィルタ 1289
MSDP での発信フィルタ リストの使用 1290
MSDP での着信フィルタ リストの使用 1291
MSDP の TTL しきい値 1292
MSDP メッセージ タイプ 1292
SA メッセージ 1292
SA 要求メッセージ 1292
SA 応答メッセージ 1293
キープアライブ メッセージ 1293
MSDP のデフォルト設定 1293
MSDP の設定方法 1293
デフォルトの MSDP ピアの設定 1293
SA ステートのキャッシング 1295
MSDP ピアからの送信元情報の要求 1297

スイッチから発信される送信元情報の制御 1298
送信元の再配信 1298
SA 要求メッセージのフィルタリング 1301
スイッチで転送される送信元情報の制御 1302
フィルタの使用法 1303
SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限 1305
スイッチで受信される送信元情報の制御 1306
MSDP メッシュ グループの設定 1308
MSDP ピアのシャットダウン 1310
境界 PIM デンス モード領域の MSDP への包含 1311
RP アドレス以外の発信元アドレスの設定 1313
MSDP のモニタリングおよびメンテナンス 1315
MSDP のモニタリング 1315
MSDP 接続統計情報および SA キャッシュ エントリの消去 1317
MSDP の設定例 1318
デフォルト MSDP ピアの設定：例 1318
SA ステートのキャッシング：例 1319
MSDP ピアからの送信元情報の要求：例 1319
スイッチから発信される送信元情報の制御：例 1319
スイッチから転送される送信元情報の制御：例 1319
スイッチで受信される送信元情報の制御：例 1320
例：MSDP メッシュ グループの設定 1320
MSDP ピアからの送信元情報の要求：例 1320
セキュリティ 1321
セキュリティ機能の概要 1323
セキュリティ機能の概要 1323
不正アクセスの防止 1327
機能情報の確認 1327
不正アクセスの防止 1327
パスワードおよび権限レベルによるスイッチ アクセスの制御 1329
機能情報の確認 1329

パスワードおよび権限によるスイッチ アクセスの制御の制約事項 1329
パスワードおよび権限レベルに関する情報 1330
デフォルトのパスワードおよび権限レベル設定 1330
追加のパスワード セキュリティ 1330
パスワードの回復 1331
端末回線の Telnet 設定 1331
ユーザ名とパスワードのペア 1332
権限レベル 1332
パスワードおよび権限レベルでスイッチ アクセスを制御する方法 1333
スタティック イネーブル パスワードの設定または変更 1333
暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 1334
パスワード回復のディセーブル化 1337
端末回線に対する Telnet パスワードの設定 1338
ユーザ名とパスワードのペアの設定 1340
コマンドの特権レベルの設定 1342
回線のデフォルト特権レベルの変更 1344
権限レベルへのログインおよび終了 1346
スイッチ アクセスのモニタリング 1346
パスワードおよび権限レベルの設定例 1347
例：スタティック イネーブル パスワードの設定または変更 1347
例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 1347
例：端末回線に対する Telnet パスワードの設定 1347
例：コマンドの権限レベルの設定 1347
TACACS+ の設定 1349
機能情報の確認 1349
Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件 1349
TACACS+ の概要 1351
TACACS+ およびスイッチ アクセス 1351
TACACS+ の概要 1351
TACACS+ の動作 1353

方式リスト 1354
TACACS+ 設定オプション 1354
TACACS+ ログイン認証 1354
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可 1355
TACACS+ アカウンティング 1355
TACACS+ のデフォルト設定 1355
TACACS+ を設定する方法 1356
TACACS+ サーバ ホストの指定および認証キーの設定 1356
TACACS+ ログイン認証の設定 1358
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定 1361
TACACS+ アカウンティングの起動 1363
AAA サーバが到達不能な場合のルータとのセッションの確立 1364
TACACS+ のモニタリング 1365
RADIUS の設定 1367
機能情報の確認 1367
RADIUS によるSwitch アクセスの制御の前提条件 1367
RADIUS によるSwitch アクセスの制御の制約事項 1368
RADIUS に関する情報 1369
RADIUS およびスイッチ アクセス 1369
RADIUS の概要 1369
RADIUS の動作 1370
RADIUS 許可の変更 1371
Change-of-Authorization 要求 1372
RFC 5176 規定 1372
CoA 要求応答コード 1373
セッションの識別 1373
CoA ACK 応答コード 1374
CoA NAK 応答コード 1374
CoA 要求コマンド 1374
セッション再認証 1375
セッションの終了 1375

CoA 接続解除要求 1376
CoA 要求：ホスト ポートのディセーブル化 1376
CoA 要求：バウンス ポート 1376
RADIUS のデフォルト設定 1377
RADIUS サーバ ホスト 1377
RADIUS ログイン認証 1378
AAA サーバ グループ 1378
AAA 許可 1379
RADIUS アカウンティング 1379
ベンダー固有の RADIUS 属性 1379
ベンダー独自仕様の RADIUS サーバ通信 1380
RADIUS の設定方法 1380
RADIUS サーバ ホストの識別 1380
RADIUS ログイン認証の設定 1383
AAA サーバ グループの定義 1386
ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定 1389
RADIUS アカウンティングの起動 1391
すべての RADIUS サーバの設定 1393
ベンダー固有の RADIUS 属性を使用するスイッチ設定 1394
ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定 1396
スイッチ上での CoA の設定 1398
CoA 機能のモニタリング 1401
RADIUS によるスイッチ アクセスの制御の設定例 1401
例：RADIUS サーバ ホストの識別 1401
例：2 台の異なる RADIUS グループ サーバの使用 1402
例：ベンダー固有の RADIUS 属性を使用するスイッチ設定 1402
例：ベンダー独自仕様の RADIUS サーバとの通信に関するスイッチ設定 1403
Kerberos の設定 1405
機能情報の確認 1405
Kerberos によるスイッチ アクセスの制御の前提条件 1405
Kerberos に関する情報 1406

Kerberos とスイッチ アクセス 1406
Kerberos の概要 1406
Kerberos の動作 1409
境界スイッチに対する認証の取得 1410
KDC からの TGT の取得 1410
ネットワーク サービスに対する認証の取得 1410
Kerberos を設定する方法 1411
Kerberos 設定のモニタリング 1411
ローカル認証および許可の設定 1413
機能情報の確認 1413
ローカル認証および許可の設定方法 1413
スイッチのローカル認証および許可の設定 1413
ローカル認証および許可のモニタリング 1416
セキュア シェル（SSH）の設定 1417
機能情報の確認 1417
セキュア シェル（SSH）およびセキュア コピープロトコル（SCP）用にスイッチを設定するための前提条件 1417
SSH 用にSwitchを設定するための制約事項 1418
SSH に関する情報 1418
SSH およびスイッチ アクセス 1419
SSH サーバ、統合クライアント、およびサポートされているバージョン 1419
SSH 設定時の注意事項 1419
セキュア コピー プロトコルの概要 1420
Secure Copy Protocol（SCP） 1421
SSH の設定方法 1421
SSH を実行するためのSwitchの設定 1421
SSH サーバの設定 1423
SSH の設定およびステータスのモニタリング 1425
Secure Socket Layer HTTP の設定 1427
機能情報の確認 1427
Secure Sockets Layer（SSL）HTTP に関する情報 1427
セキュア HTTP サーバおよびクライアントの概要 1427

認証局のトラストポイント 1428
CipherSuite 1429
SSL のデフォルト設定 1430
SSL の設定時の注意事項 1430
セキュア HTTP サーバおよびクライアントの設定方法 1430
CA のトラストポイントの設定 1430
セキュア HTTP サーバの設定 1433
セキュア HTTP クライアントの設定 1436
セキュア HTTP サーバおよびクライアントのステータスのモニタリング 1437
IPv4 ACL の設定 1439
機能情報の確認 1439
ACL によるネットワーク セキュリティの設定の前提条件 1439
ACL によるネットワーク セキュリティの設定の制約事項 1440
ACL によるネットワーク セキュリティに関する情報 1441
ACL の概要 1441
アクセス コントロール エントリ 1442
ACL でサポートされるタイプ 1442
サポートされる ACL 1442
ACL 優先順位 1443
ポート ACL 1443
ルータ ACL 1445
VLAN マップ 1445
ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック 1446
例：ACEおよびフラグメント化されたトラフィックとフラグメント化されていないトラフィック 1446
標準 IPv4 ACL および拡張 IPv4 ACL 1447
IPv4 ACL スイッチでサポートされていない機能 1448
アクセス リスト番号 1448
番号付き標準 IPv4 ACL 1449
番号付き拡張 IPv4 ACL 1449
名前付き IPv4 ACL 1450

ACL ロギング 1451
ハードウェアおよびソフトウェアによる IP ACL の処理 1451
VLAN マップの設定時の注意事項 1452
VLAN マップとルータ ACL 1453
VLAN マップとルータ ACL の設定時の注意事項 1453
VACL ロギング 1454
ACL の時間範囲 1454
IPv4 ACL のインターフェイスに関する注意事項 1455
ACL の設定方法 1456
IPv4 ACL の設定 1456
番号付き標準 ACL の作成 1456
番号付き拡張 ACL の作成 1458
名前付き標準 ACL の作成 1462
名前付き拡張 ACL の作成 1464
ACL の時間範囲の設定 1465
端末回線への IPv4 ACL の適用 1467
インターフェイスへの IPv4 ACL の適用 1469
名前付き MAC 拡張 ACL の作成 1470
レイヤ 2 インターフェイスへの MAC ACL の適用 1472
VLAN マップの設定 1474
VLAN マップの作成 1477
VLAN への VLAN マップの適用 1478
IPv4 ACL のモニタリング 1479
ACL の設定例 1481
例：ACL での時間範囲を使用 1481
例：ACL へのコメントの挿入 1482
IPv4 ACL の設定例 1482
小規模ネットワークが構築されたオフィス用の ACL 1482
例：小規模ネットワークが構築されたオフィスの ACL 1483
例：番号付き ACL 1484
例：拡張 ACL 1484
例：名前付き ACL 1485

例：IP ACL に適用される時間範囲 1486
例：コメント付き IP ACL エントリ 1486
例：ACL ロギング 1487
ACL および VLAN マップの設定例 1488
例：パケットを拒否する ACL および VLAN マップの作成 1488
例：パケットを許可する ACL および VLAN マップの作成 1488
例：IP パケットのドロップおよび MAC パケットの転送のデフォルト アクション 1488
例：MAC パケットのドロップおよび IP パケットの転送のデフォルト アクション 1489
例：すべてのパケットをドロップするデフォルト アクション 1490
ネットワークでの VLAN マップの使用方法の設定例 1490
例：ワイヤリング クローゼットの設定 1490
例：別の VLAN にあるサーバへのアクセスの制限 1492
例：別の VLAN にあるサーバへのアクセスの拒否 1492
VLAN に適用されるルータ ACL と VLAN マップの設定例 1493
例：ACL およびスイッチド パケット 1493
例：ACL およびブリッジド パケット 1493
例：ACL およびルーテッド パケット 1494
例：ACL およびマルチキャスト パケット 1495
IPv6 ACL の設定 1497
機能情報の確認 1497
IPv6 ACL の概要 1497
他の機能およびスイッチとの相互作用 1498
IPv6 ACL の制限 1498
IPv6 ACL のデフォルト設定 1499
IPv6 ACL の設定 1500
インターフェイスへの IPv6 ACL の付加 1504
IPv6 ACL のモニタリング 1506
DHCP の設定 1507
機能情報の確認 1507
DHCP に関する情報 1507

DHCP サーバ 1507
DHCP リレー エージェント 1508
DHCP スヌーピング 1508
Option 82 データ挿入 1510
Cisco IOS DHCP サーバ データベース 1513
DHCP スヌーピング バインディング データベース 1513
DHCP 機能の設定方法 1515
DHCP スヌーピングのデフォルト設定 1515
DHCP スヌーピング設定時の注意事項 1516
DHCP サーバの設定 1516
DHCP リレー エージェントの設定 1516
パケット転送アドレスの指定 1518
DHCP スヌーピングおよび Option 82 を設定するための前提条件 1520
DHCP スヌーピングおよび Option 82 のイネーブル化 1522
Cisco IOS DHCP サーバ データベースのイネーブル化 1525
DHCP スヌーピング情報のモニタリング 1525
DHCP サーバ ポートベースのアドレス割り当ての設定 1526
DHCP サーバ ポートベースのアドレス割り当ての設定の概要 1526
ポートベースのアドレス テーブルのデフォルト設定 1527
ポートベースのアドレス割り当て設定時の注意事項 1527
DHCP スヌーピング バインディング データベース エージェントのイネーブル化 1527
DHCP サーバ ポートベースのアドレス割り当てのイネーブル化 1530
DHCP サーバ ポートベースのアドレス割り当てのモニタリング 1531
IP ソース ガードの設定 1533
機能情報の確認 1533
IP ソース ガードの概要 1534
IP ソース ガード 1534
スタティック ホスト用 IP ソース ガード 1534
IP ソース ガードの設定時の注意事項 1535
IP ソース ガードの設定方法 1537
IP ソース ガードのイネーブル化 1537

レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定 1538
IP ソース ガードのモニタリング 1540
ダイナミック ARP インスペクションの設定 1543
機能情報の確認 1543
ダイナミック ARP インスペクションの制約事項 1544
ダイナミック ARP インスペクションの概要 1545
インターフェイスの信頼状態とネットワーク セキュリティ 1547
ARP パケットのレート制限 1549
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ 1549
廃棄パケットのロギング 1549
ダイナミック ARP インスペクションのデフォルト設定 1550
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ 1550
非 DHCP 環境での ARP ACL の設定 1551
DHCP 環境でのダイナミック ARP インスペクションの設定 1554
着信 ARP パケットのレート制限 1556
ダイナミック ARP インスペクション検証チェックの実行 1559
DAI のモニタリング 1561
DAI の設定の確認 1562
IEEE 802.1x ポートベースの認証の設定 1563
機能情報の確認 1563
802.1x ポートベース認証について 1563
ポートベース認証プロセス 1564
ポートベース認証の開始およびメッセージ交換 1566
ポートベース認証の認証マネージャ 1568
ポートベースの認証方法 1568
ユーザ単位 ACL および Filter-Id 1569
ポートベース認証マネージャ CLI コマンド 1570
許可ステートおよび無許可ステートのポート 1572
802.1X のホスト モード 1573
802.1x 複数認証モード 1573
ユーザごとのマルチ認証 VLAN 割り当て 1574
ユーザごとのマルチ認証 VLAN 割り当ての制限 1576

MAC 移動 1576
MAC 置換 1577
802.1x アカウンティング 1577
802.1x アカウンティング属性値ペア 1578
802.1x 準備状態チェック 1579
スイッチと RADIUS サーバ間の通信 1580
VLAN 割り当てを使用した 802.1x 認証 1580
ユーザ単位 ACL を使用した 802.1x 認証 1582
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証 1583
Cisco Secure ACS およびリダイレクト URL の属性と値のペア 1585
Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア 1585
VLAN ID ベース MAC 認証 1586
ゲスト VLAN を使用した 802.1x 認証 1586
制限付き VLAN による 802.1x 認証 1587
アクセス不能認証バイパスを使用した 802.1x 認証 1588
複数認証ポートのアクセス不能認証バイパスのサポート 1589
アクセス不能認証バイパスの認証結果 1589
アクセス不能認証バイパス機能の相互作用 1589
802.1x クリティカル音声 VLAN 1590
802.1x ユーザ ディストリビューション 1591
802.1x ユーザ ディストリビューションの設定時の注意事項 1591
音声 VLAN ポートを使用した IEEE 802.1x 認証 1592
ポート セキュリティを使用した IEEE 802.1x 認証 1593
WoL 機能を使用した IEEE 802.1x 認証 1593
MAC 認証バイパスを使用した IEEE 802.1x 認証 1593
Network Admission Control レイヤ 2 IEEE 802.1x 検証 1595
柔軟な認証の順序設定 1595
Open1x 認証 1596
マルチドメイン認証 1596
Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ 1598
音声認識 802.1x セキュリティ 1600

コモン セッション ID 1600
802.1x ポートベース認証の設定方法 1601
802.1x 認証のデフォルト設定 1601
802.1x 認証設定時の注意事項 1602
802.1X 認証 1602
VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス 1603
MAC 認証バイパス 1604
ポートあたりのデバイスの最大数 1605
802.1x 準備状態チェックの設定 1605
音声認識 802.1x セキュリティの設定 1607
802.1x 違反モードの設定 1609
802.1X 認証の設定 1611
802.1x ポートベース認証の設定 1612
スイッチと RADIUS サーバ間の通信の設定 1615
ホスト モードの設定 1617
定期的な再認証の設定 1618
待機時間の変更 1619
スイッチからクライアントへの再送信時間の変更 1621
スイッチからクライアントへのフレーム再送信回数の設定 1622
再認証回数の設定 1623
MAC 移動のイネーブル化 1625
MAC 置換のイネーブル化 1626
IEEE 802.1x アカウンティングの設定 1628
ゲスト VLAN の設定 1630
制限付き VLAN の設定 1631
制限付き VLAN の認証試行回数の設定 1633
クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定 1634
アクセス不能認証バイパスの設定例 1638
WoL を使用した 802.1x 認証の設定 1638
MAC 認証バイパスの設定 1640
MAC 認証バイパスのユーザ名とパスワードの形式作成 1641

802.1x ユーザ ディストリビューションの設定 1643
VLAN グループの設定例 1644
NAC レイヤ 2 802.1x 検証の設定 1644
NEAT を使用したオーセンティケータ スイッチの設定 1646
NEAT を使用したサプリカント スイッチの設定 1648
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定 1651
ダウンロード可能な ACL の設定 1652
ダウンロード ポリシーの設定 1653
VLAN ID ベース MAC 認証の設定 1656
柔軟な認証順序の設定 1657
Open1x の設定 1658
ポート上での 802.1x 認証のディセーブル化 1661
802.1x 認証設定のデフォルト値へのリセット 1662
802.1x の統計情報およびステータスのモニタリング 1663
Web ベース認証の設定 1665
機能情報の確認 1665
Web ベース認証について 1665
デバイスのロール 1666
ホストの検出 1667
セッションの作成 1667
認証プロセス 1667
ローカル Web 認証バナー 1668
Web 認証カスタマイズ可能な Web ページ 1671
ガイドライン 1671
認証プロキシ Web ページの注意事項 1673
成功ログインに対するリダイレクト URL の注意事項 1674
その他の機能と Web ベース認証の相互作用 1674
ポート セキュリティ 1674
LAN ポート IP 1675
ゲートウェイ IP 1675
ACL 1675

コンテキストベース アクセス コントロール 1675

EtherChannel 1675

Web ベース認証の設定方法 1676

デフォルトの Web ベース認証の設定 1676

Web ベース認証の設定に関する注意事項と制約事項 1676

認証ルールとインターフェイスの設定 1678

AAA 認証の設定 1680

スイッチ/RADIUS サーバ間通信の設定 1682

HTTP サーバの設定 1684

認証プロキシ Web ページのカスタマイズ 1685

成功ログインに対するリダイレクション URL の指定 1687

Web ベース認証パラメータの設定 1688

Web 認証ローカル バナーの設定 1689

Web ベース認証キャッシュ エントリの削除 1690

Web ベース認証ステータスのモニタリング 1691

ポート単位のトラフィック制御の設定 1693

ポートベースのトラフィック制御の概要 1694

機能情報の確認 1694

ストーム制御に関する情報 1694

ストーム制御 1694

トラフィック アクティビティの測定方法 1695

トラフィック パターン 1696

ストーム制御の設定方法 1697

ストーム制御およびしきい値レベルの設定 1697

スモール フレーム到着レートの設定 1700

保護ポートに関する情報 1702

保護ポート 1702

保護ポートのデフォルト設定 1703

保護ポートのガイドライン 1703

保護ポートの設定方法 1703

保護ポートの設定 1703

保護ポートのモニタリング 1705

次の作業 1705
ポート ブロッキングに関する情報 1705
ポート ブロッキング 1705
ポート ブロッキングの設定方法 1706
インターフェイスでのフラッディング トラフィックのブロッキング 1706
ポート ブロッキングのモニタリング 1708
ポート セキュリティの前提条件 1708
ポート セキュリティの制約事項 1708
ポート セキュリティの概要 1708
ポート セキュリティ 1708
セキュア MAC アドレスのタイプ 1709
スティッキ セキュア MAC アドレス 1709
セキュリティ違反 1710
ポート セキュリティ エージング 1711
デフォルトのポート セキュリティ設定 1711
ポート セキュリティの設定時の注意事項 1712
ポートベースのトラフィック制御の概要 1714
ポート セキュリティの設定方法 1714
ポート セキュリティのイネーブル化および設定 1714
ポート セキュリティ エージングのイネーブル化および設定 1720
機能情報の確認 1722
ストーム制御に関する情報 1722
ストーム制御 1722
トラフィック アクティビティの測定方法 1722
トラフィック パターン 1723
ストーム制御の設定方法 1724
ストーム制御およびしきい値レベルの設定 1724
スモール フレーム到着レートの設定 1727
保護ポートに関する情報 1730
保護ポート 1730
保護ポートのデフォルト設定 1730
保護ポートのガイドライン 1730

保護ポートの設定方法 1730
保護ポートの設定 1730
保護ポートのモニタリング 1732
次の作業 1732
ポート ブロッキングに関する情報 1733
ポート ブロッキング 1733
ポート ブロッキングの設定方法 1733
インターフェイスでのフラッディング トラフィックのブロッキング 1733
ポート ブロッキングのモニタリング 1735
ポート セキュリティの設定例 1735
プロトコル ストーム プロテクションに関する情報 1736
プロトコル ストーム プロテクション 1736
デフォルトのプロトコル ストーム プロテクションの設定 1737
プロトコル ストーム プロテクションの設定方法 1737
プロトコル ストーム プロテクションのイネーブル化 1737
プロトコル ストーム プロテクションのモニタリング 1738
IPv6 ファースト ホップ セキュリティの設定 1739
機能情報の確認 1739
IPv6 でのファースト ホップ セキュリティの前提条件 1740
IPv6 でのファースト ホップ セキュリティの制約事項 1740
IPv6 でのファースト ホップ セキュリティに関する情報 1740
IPv6 スヌーピング ポリシーの設定方法 1743
IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法 1744
IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1746
IPv6 バインディング テーブルの内容を設定する方法 1747
IPv6 ネイバー探索インスペクション ポリシーの設定方法 1749
IPv6 ネイバー探索インスペクション ポリシーをインターフェイスにアタッチする方法 1751
IPv6 ネイバー探索インスペクション ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1752
IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法 1753

IPv6ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法 1756
IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1757
IPv6 DHCP ガード ポリシーの設定方法 1759
IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法 1761
IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1763
IPv6 ソース ガードの設定方法 1764
IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法 1765
IPv6 ソース ガードの設定方法 1766
IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法 1768
IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1769
IPv6 プレフィックス ガードの設定方法 1770
IPv6 プレフィックス ガード ポリシーをインターフェイスにアタッチする方法 1771
IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 1772
FIPS の設定 1775
FIPS および共通基準に関する情報 1775
システム管理 1777
システムの管理 1779
スイッチの管理に関する情報 1779
システム日時管理に関する情報 1779
システム クロック 1779
Real Time Clock（リアルタイム クロック） 1780
ネットワーク タイム プロトコル 1780
NTP ストラタム 1782
NTP アソシエーション 1782
NTP セキュリティ 1782

NTP の実装 1782
NTP バージョン 4 1783
システム名およびシステム プロンプト 1784
デフォルトのシステム名とプロンプトの設定 1784
DNS 1784
DNS のデフォルト設定値 1785
ログイン バナー 1785
バナーのデフォルト設定 1785
MAC Address Table 1785
MAC アドレス テーブルの作成 1786
MAC アドレスおよび VLAN 1786
MAC アドレス テーブルのデフォルト設定 1786
ARP テーブルの管理 1787
スイッチを管理する方法 1787
手動による日付と時刻の設定 1787
システム クロックの設定 1787
タイム ゾーンの設定 1788
夏時間の設定 1790
1792
システム名の設定 1793
DNS の設定 1795
Message-of-the-Day ログイン バナーの設定 1797
ログイン バナーの設定 1798
MAC アドレス テーブルの管理 1800
アドレス エージング タイムの変更 1800
MAC アドレス変更通知トラップの設定 1801
MAC アドレス移動通知トラップの設定 1804
MAC しきい値通知トラップの設定 1807
スタティック アドレス エントリの追加および削除 1809
ユニキャスト MAC アドレス フィルタリングの設定 1810
スイッチのモニタリングおよび保守の管理 1812
スイッチ管理の設定例 1813
例：システム クロックの設定 1813

例：サマー タイムの設定 1813
例：MOTD バナーの設定 1814
例：ログイン バナーの設定 1814
例：MAC アドレス変更通知トラップの設定 1814
例：MAC しきい値通知トラップの設定 1815
例：MAC アドレス テーブルへのスタティック アドレスの追加 1815
例：ユニキャスト MAC アドレス フィルタリングの設定 1815
スイッチのセットアップ設定の実行 1817
スイッチセットアップ設定の実行に関する情報 1817
ブート プロセス 1817
スイッチ情報の割り当て 1818
デフォルトのスイッチ情報 1819
DHCP ベースの自動設定の概要 1819
DHCP クライアント要求プロセス 1820
DHCP ベースの自動設定およびイメージ アップデート 1821
DHCP ベースの自動設定の制約事項 1821
DHCP 自動設定 1822
DHCP 自動イメージ アップデート 1822
DHCP サーバ設定時の注意事項 1823
DNS サーバの目的 1823
コンフィギュレーション ファイルの入手方法 1824
環境変数の制御方法 1825
一般的な環境変数 1825
TFTP の環境変数 1828
ソフトウェア イメージのリロードのスケジューリング 1829
スイッチ設定コンフィギュレーションの実行方法 1829
DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定 1830
DHCP 自動イメージアップデート（コンフィギュレーション ファイルおよびイメージ）の設定 1832
DHCP サーバからファイルをダウンロードするクライアントの設定 1836
複数の SVI への IP 情報の手動割り当て 1837
NVRAM バッファ サイズの設定 1839

スイッチのスタートアップ コンフィギュレーションの変更 1841
システム コンフィギュレーションを読み書きするためのファイル名の指定 1841
スイッチの手動による起動 1842
ソフトウェア イメージのリロードのスケジュール設定 1843
スイッチのセットアップ設定のモニタリング 1845
例：スイッチ実行コンフィギュレーションの確認 1845
例：ソフトウェア インストールの表示 1845
スイッチ のセットアップを実行する場合の設定例 1846
例：DHCP サーバとしてのスイッチの設定 1846
例：DHCP 自動イメージ アップデートの設定 1846
例：DHCP サーバから設定をダウンロードするためのスイッチの設定 1846
例：NVRAM バッファ サイズの設定 1847
スイッチのクラスタリング 1849
機能情報の確認 1849
RTU ライセンスの設定に関する制約事項 1849
RTU ライセンスの設定に関する情報 1850
Right-To-Use ライセンス 1850
Right-To-Use イメージ ベースのライセンス 1851
Right-To-Use ライセンスの状態 1851
モビリティ コントローラ モード 1852
Right-To-Use Adder AP-Count 再ホスト ライセンス 1852
RTU ライセンスの設定方法 1852
イメージ ベース ライセンスのアクティブ化 1852
ap-count ライセンスのアクティブ化 1854
アップグレード ライセンスまたはキャパシティ Adder ライセンスの取得 1854
ライセンスの再ホスト 1855
RTU ライセンスのモニタリングおよびメンテナンス 1856
RTU ライセンスの設定例 1857
例：RTU イメージ ベースのライセンスのアクティブ化 1857
例：RTU ライセンス情報の表示 1857
例：RTU ライセンスの詳細の表示 1857

例：RTU ライセンスの不一致の表示 1857
例：RTU ライセンス使用状況の表示 1858
スイッチのクラスタリング 1859
スイッチ クラスタの概要 1859
クラスタ コマンド スイッチの特性 1861
スタンバイ クラスタ コマンド スイッチの特性 1861
候補スイッチおよびクラスタ メンバ スイッチの特性 1862
スイッチ クラスタのプランニング 1862
クラスタ候補およびメンバの自動検出 1863
CDP ホップによる検出 1863
CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出 1864
異なる VLAN からの検出 1865
異なる管理 VLAN からの検出 1865
ルーテッド ポートからの検出 1866
新しく設置したスイッチの検出 1867
HSRP およびスタンバイ クラスタ コマンド スイッチ 1868
仮想 IP アドレス 1869
クラスタ スタンバイ グループに関する他の考慮事項 1869
クラスタ設定の自動回復 1871
IP Addresses 1871
ホスト名 1872
パスワード 1872
SNMP コミュニティ ストリング 1873
TACACS+ および RADIUS 1873
LRE プロファイル 1873
CLI を使用したスイッチ クラスタの管理 1873
Catalyst 1900 および Catalyst 2820 の CLI に関する考慮事項 1874
SNMP を使用したスイッチ クラスタの管理 1874
SDM テンプレートの設定 1877
機能情報の確認 1877
SDM テンプレートの設定に関する情報 1877
SDM テンプレートの制約事項 1877

SDM テンプレート 1878
Catalyst 2960-CX のデフォルト テンプレート 1878
Catalyst 3560-CX のデフォルト テンプレート 1879
SDM テンプレートの設定方法 1880
SDM テンプレートの設定 1880
SDM テンプレートの設定例 1881
例：SDM テンプレートの表示 1881
例：SDM テンプレートの設定 1882
システム メッセージ ログの設定 1883
システム メッセージ ログの設定に関する情報 1883
システム メッセージ ロギング 1883
システム ログ メッセージのフォーマット 1884
デフォルトのシステム メッセージ ロギングの設定 1885
syslog メッセージの制限 1886
システム メッセージ ログの設定方法 1886
メッセージ表示宛先デバイスの設定 1886
ログ メッセージの同期化 1888
メッセージ ロギングのディセーブル化 1890
ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化 1891
ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化 1892
メッセージ重大度の定義 1893
履歴テーブルおよび SNMP に送信される syslog メッセージの制限 1894
UNIX Syslog デーモンへのメッセージのロギング 1895
システム メッセージ ログのモニタリングおよびメンテナンス 1896
コンフィギュレーション アーカイブ ログのモニタリング 1896
システム メッセージ ログの設定例 1897
例：スイッチ システム メッセージ 1897
例：サービス タイムスタンプ ログの表示 1897
オンライン診断の設定 1899
オンライン診断の設定に関する情報 1899
オンライン診断 1899
オンライン診断の設定方法 1900

オンライン診断テストの開始 1900

オンライン診断の設定 1900

オンライン診断のスケジューリング 1901

ヘルス モニタリング診断の設定 1902

オンライン診断のモニタリングおよびメンテナンス 1905

オンライン診断テストとテスト結果の表示 1905

オンライン診断テストの設定例 1906

オンライン診断テストの開始 1906

例：ヘルス モニタリング テストの設定 1907

例：診断テストのスケジューリング 1907

オンライン診断の表示：例 1907

ソフトウェア設定のトラブルシューティング 1911

ソフトウェア設定のトラブルシューティングに関する情報 1911

スイッチのソフトウェア障害 1911

スイッチのパスワードを紛失したか忘れた場合 1912

Power over Ethernet（PoE）ポート 1912

電力消失によるポートの障害 1912

PoE ポート ステータスのモニタリング 1913

不正リンク アップによるポート障害 1913

ping 1913

レイヤ 2 Traceroute 1914

レイヤ 2 の traceroute のガイドライン 1914

IP Traceroute 1915

Time Domain Reflector ガイドライン 1916

debug コマンド 1917

スイッチのオンボード障害ロギング 1917

CPU 使用率が高い場合に起こりうる症状 1918

ソフトウェア設定のトラブルシューティング方法 1919

ソフトウェア障害からの回復 1919

パスワードを忘れた場合の回復 1921

パスワード回復がイネーブルになっている場合の手順 1922

パスワード回復がディセーブルになっている場合の手順 1924

コマンド スイッチで障害が発生した場合の回復 1926

故障したコマンド スイッチをクラスタ メンバーと交換する場合 1927
故障したコマンド スイッチを他のスイッチと交換する場合 1929
自動ネゴシエーションの不一致の防止 1930
SFP モジュールのセキュリティと識別に関するトラブルシューティング 1931
SFP モジュール ステータスのモニタリング 1931
ping の実行 1931
温度のモニタリング 1932
物理パスのモニタリング 1932
IP traceroute の実行 1933
TDR の実行および結果の表示 1933
デバッグおよびエラー メッセージ出力のリダイレクト 1933
show platform forward コマンドの使用 1934
OBFL の設定 1934
ソフトウェア設定のトラブルシューティングの確認 1935
OBFL 情報の表示 1935
例：高い CPU 使用率に関する問題と原因の確認 1937
ソフトウェア設定のトラブルシューティングのシナリオ 1938
Power over Ethernet（PoE）に関するトラブルシューティングのシナリオ 1938
ソフトウェアのトラブルシューティングの設定例 1942
例：IP ホストの ping 1942
例：IP ホストに対する traceroute の実行 1943
例：すべてのシステム診断をイネーブルにする 1944
VLAN 1945
VTP の設定 1947
機能情報の確認 1947
VTP の前提条件 1947
VTP の制約事項 1948
VTP の概要 1948
VTP 1948
VTP ドメイン 1949
VTP モード 1950
VTP アドバタイズ 1951
VTP バージョン 2 1952

VTP バージョン 3 1953
VTP プルーニング 1954
VTP 設定時の注意事項 1955
VTP の設定要件 1955
VTP の設定 1955
VTP 設定のためのドメイン名 1955
VTP ドメインのパスワード 1956
VTP バージョン 1956
VTP のデフォルト設定 1958
VTP の設定方法 1958
VTP モードの設定 1958
VTP バージョン 3 のパスワードの設定 1961
VTP バージョン 3 のプライマリ サーバの設定 1962
VTP バージョンのイネーブル化 1963
VTP プルーニングのイネーブル化 1965
ポート単位の VTP の設定 1966
VTP ドメインへの VTP クライアント スイッチの追加 1968
VTP のモニタ 1971
VTP の設定例 1971
例：スイッチをプライマリ サーバとして設定する 1971
例：VTP サーバとしてのスイッチの設定 1972
例：インターフェイスでの VTP のイネーブル化 1972
例：VTP パスワードの作成 1972
次の作業 1973
VLAN の設定 1975
機能情報の確認 1975
VLAN の前提条件 1975
VLAN の制約事項 1976
VLAN について 1976
論理ネットワーク 1976
サポートされる VLAN 1977
VLAN ポート メンバーシップ モード 1977

VLAN コンフィギュレーション ファイル 1979
標準範囲 VLAN 設定時の注意事項 1979
拡張範囲 VLAN 設定時の注意事項 1981
VLAN のデフォルト設定 1982
イーサネット VLAN のデフォルト設定 1982
VLAN のデフォルト設定 1983
VLAN の設定方法 1983
標準範囲 VLAN の設定方法 1983
イーサネット VLAN の作成または変更 1984
VLAN の削除 1986
VLAN へのスタティック アクセス ポートの割り当て 1988
拡張範囲 VLAN の設定方法 1990
拡張範囲 VLAN の作成 1990
VLAN のモニタリング 1992
設定例 1994
例：VLAN 名の作成 1994
例：アクセス ポートとしてのポートの設定 1995
例：拡張範囲 VLAN の作成 1995
次の作業 1995
VLAN トランクの設定 1997
機能情報の確認 1997
VLAN トランクの前提条件 1997
VLAN トランクについて 1998
トランキングの概要 1998
トランキング モード 1998
レイヤ 2 インターフェイス モード 1999
トランクでの許可 VLAN 2000
トランク ポートでの負荷分散 2001
STP プライオリティによるネットワーク負荷分散 2001
STP パス コストによるネットワーク負荷分散 2001
機能の相互作用 2001
レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定 2002

VLAN トランクの設定方法 2003
トランク ポートとしてのイーサネット インターフェイスの設定 2003
トランク ポートの設定 2003
トランクでの許可 VLAN の定義 2005
プルーニング適格リストの変更 2007
タグなしトラフィック用ネイティブ VLAN の設定 2009
トランク ポートの負荷分散の設定 2011
STP ポート プライオリティによる負荷分散の設定 2011
STP パス コストによる負荷分散の設定 2016
VLAN トランキングの設定例 2019
例：トランク ポートの設定 2019
例：ポートからの VLAN の削除 2019
次の作業 2019
VMPS の設定 2021
機能情報の確認 2021
VMPS の前提条件 2021
VMPS の制約事項 2022
VMPS について 2022
ダイナミック VLAN 割り当て 2022
ダイナミックアクセス ポート VLAN メンバーシップ 2023
デフォルトの VMPS クライアント設定 2024
VMPS の設定方法 2025
VMPS の IP アドレスの入力 2025
VMPS クライアント上のダイナミックアクセス ポートの設定 2026
VLAN メンバーシップの再確認 2028
再確認インターバルの変更 2029
再試行回数の変更 2031
ダイナミックアクセス ポート VLAN メンバーシップのトラブルシューティング 2032
VMPS のモニタリング 2032
VMPS の設定例 2033
例：VMPS の設定 2033

次の作業 2034
音声 VLAN の設定 2037
機能情報の確認 2037
音声 VLAN の前提条件 2037
音声 VLAN の制約事項 2038
音声 VLAN に関する情報 2038
音声 VLAN 2038
Cisco IP Phone の音声トラフィック 2038
Cisco IP Phone のデータ トラフィック 2039
音声 VLAN 設定時の注意事項 2039
音声 VLAN のデフォルト設定 2041
音声 VLAN の設定方法 2041
Cisco IP Phone の音声トラフィックの設定 2041
着信データ フレームのプライオリティ設定 2044
音声 VLAN のモニタリング 2046
設定例 2046
例：Cisco IP Phone の音声トラフィックの設定 2046
例：着信データ フレームのプライオリティの設定 2046
次の作業 2047
プライベート VLAN の設定 2049
機能情報の確認 2049
プライベート VLAN の前提条件 2049
プライベート VLAN の制約事項 2050
プライベート VLAN について 2051
プライベート VLAN ドメイン 2051
セカンダリ VLAN 2052
プライベート VLAN ポート 2052
ネットワーク内のプライベート VLAN 2054
プライベート VLAN での IP アドレッシング方式 2054
複数のスイッチにまたがるプライベート VLAN 2055
プライベート VLAN の他機能との相互作用 2055

プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック 2055
プライベート VLAN と SVI 2056
プライベート VLAN 設定時の注意事項 2057
セカンダリ VLAN およびプライマリ VLAN の設定 2057
プライベート VLAN ポートの設定 2059
プライベート VLAN の設定タスク 2060
プライベート VLAN の設定方法 2060
プライベート VLAN 内の VLAN の設定および対応付け 2060
プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 2064
プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 2066
セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング 2068
プライベート VLAN のモニタ 2071
プライベート VLAN の設定例 2071
例：ホスト ポートとしてのインターフェイスの設定 2071
例：インターフェイスをプライベート VLAN 無差別ポートとして設定する 2072
例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする 2072
例：プライベート VLAN のモニタリング 2073
次の作業 2073
その他の参考資料 2073
重要な通知 2077
免責事項 2077
ステートメント 361：電源障害が発生した場合に VoIP および緊急コール サービスは機能しない 2078
ステートメント 1071：警告の定義 2078

はじめに

このマニュアルでは、スイッチに関するNetFlow Liteの設定情報および例について説明します。

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

表記法

このマニュアルでは、次の表記法を使用しています。

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

表記法	説明
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。 stringの前後には引用符を使用しません。 引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

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

ヒント 「問題解決に役立つ情報」です。

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

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

警告 安全上の重要事項

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

SAVE THESE INSTRUCTIONS

関連資料

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

- 次の URL にある Cisco Catalyst 3560-CX および 2960-CXスイッチのマニュアル：http://www.cisco.com/c/en/us/support/switches/catalyst-3560-cx-series-switches/tsd-products-support-series-home.htmlおよび http://www.cisco.com/c/en/us/support/switches/catalyst-2960-cx-series-switches/tsd-products-support-series-home.html
- 次の URL にある Cisco Validated Design（CVD）のマニュアル：

  http://www.cisco.com/go/designzone

マニュアルの入手方法およびテクニカル サポート

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

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

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

第 1 章

コマンドライン インターフェイスの使用

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

コマンドライン インターフェイスの使用に関する情報

コマンド モード

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

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

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

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

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

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

表 *1*：コマンド モードの概要

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

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

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

コマンドの省略形

スイッチでコマンドが一意に認識される長さまでコマンドを入力します。

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

```
Switch# show conf
```

コマンドの no 形式および default 形式

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

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

CLI のエラー メッセージ

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

表 2 : *CLI* の代表的なエラー メッセージ

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

コンフィギュレーション ロギング

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

（注） CLI または HTTP の変更のみがログとして記録されます。

ヘルプ システムの使用

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**help** 例： `Switch# help`	コマンド モードのヘルプ システムの簡単な説明を表示します。

ステップ 2	*abbreviated-command-entry***?**
	
	例：
	`Switch# di?`
	`dir disable disconnect`
		特定のストリングで始まるコマンドのリストを表示します。

ステップ 3	*abbreviated-command-entry* <Tab>
	
	例：
	`Switch# sh conf<tab>`
	`Switch# show configuration`
		特定のコマンド名を補完します。

ステップ 4	**?** 例： `Switch> ?`	特定のコマンド モードで使用可能なすべてのコマンドをリストします。
ステップ 5	*command***?** 例： `Switch> show ?`	コマンドに関連するキーワードを一覧表示します。

	コマンドまたはアクション	目的

ステップ 6	*command keyword*?
	
	例：
	`Switch(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`
		キーワードに関連する引数を一覧表示します。

CLI を使用して機能を設定する方法

コマンド履歴の設定

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

コマンド履歴バッファ サイズの変更

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

手順の概要

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

手順の詳細

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

コマンドの呼び出し

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

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

手順の概要

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

手順の詳細

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

コマンド履歴機能の無効化

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

手順の概要

1. **terminal no history**

手順の詳細

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

編集機能の有効化および無効化

拡張編集モードは自動的に有効にされますが、無効にしたり、再び有効にしたりできます。

手順の概要

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

手順の詳細

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

キー入力によるコマンドの編集

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

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

表 *3*：編集コマンド

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

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

画面幅よりも長いコマンドラインの編集

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

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

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

次に、画面上で 1 行を超える長いコマンドラインを折り返す例を示します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**access-list**
	
	例：
	`Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		1 行分を超えるグローバル コンフィギュレーション コマンド入力を表示します。
		最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。 ドル記号（$）は、その行が左へスクロールされたことを表します。 カーソルが行末に達するたびに、その行は再び10文字分だけ左へシフトされます。

ステップ 2	**Ctrl+A** 例： `Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	完全な構文をチェックします。 行末に表示されるドル記号（$）は、その行が右へスクロールされたことを表します。
ステップ 3	**Return** キー	コマンドを実行します。 ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。 画面の幅が異なる場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。 ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンドエントリを呼び出して変更できます。

show および more コマンド出力の検索およびフィルタリング

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

コンソール接続または Telnet 経由での CLI へのアクセス

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

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

次のいずれかの方法で、スイッチとの接続を確立できます。

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

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

第 I 部

インターフェイスおよびハードウェア

- インターフェイス特性の設定，17 ページ
- Auto-MDIX の設定，47 ページ
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定，51 ページ
- システム MTU の設定，73 ページ
- PoE の設定，77 ページ
- EEE の設定，93 ページ

第 2 章

インターフェイス特性の設定

- 機能情報の確認，17 ページ
- インターフェイス特性の設定に関する情報，17 ページ
- インターフェイスの特性の設定方法，27 ページ
- インターフェイス特性のモニタ，42 ページ
- インターフェイス特性の設定例，44 ページ

機能情報の確認

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

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

インターフェイス特性の設定に関する情報

インターフェイス タイプ

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

ポートベースの VLAN

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

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

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

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

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

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

スイッチ ポート

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

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

アクセス ポート

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

2 種類のアクセス ポートがサポートされています。

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

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

トランク ポート

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

スイッチは IEEE 802.1Q トランク ポートだけをサポートします。 IEEE 802.1Q トランク ポートは、タグ付きとタグなしの両方のトラフィックを同時にサポートします。 IEEE 802.1Q トランク ポートは、デフォルトのポート VLAN ID（PVID）に割り当てられ、すべてのタグなしトラフィックはポートのデフォルト PVID 上を流れます。 NULL VLAN ID を備えたすべてのタグなしおよびタグ付きトラフィックは、ポートのデフォルト PVID に所属するものと見なされます。 発信ポートのデフォルト PVID と等しい VLAN ID を持つパケットは、タグなしで送信されます。 残りのトラフィックはすべて、VLAN タグ付きで送信されます。

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

した場合、ポートはその VLAN のメンバーにはならず、その VLAN のトラフィックはそのポート間で転送されません。

スイッチ仮想インターフェイス

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

（注） インターフェイス VLAN 1 は削除できません。

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

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

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

SVI 自動ステート除外

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

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

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

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

するとVLANもダウンするよう自動ステート除外機能をポートに設定できます。 ポートがイネーブルである場合、**autostate exclude** は、ポート上でイネーブルであるすべての VLAN に適用されます。

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

EtherChannel ポート グループ

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

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

（注） Cisco Catalyst 2960-CX および 3560-CX は最大で 6 個のイーサチャネル ポート グループをサポートします。

Power over Ethernet（PoE）ポート

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

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

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

スイッチの USB ポートの使用

スイッチには、USB ミニ タイプ B コンソール ポートと 2 つの USB タイプ A ポートの 3 つの USB ポートが前面パネルにあります。

USB ミニタイプ B コンソール ポート

スイッチには、次のコンソール ポートがあります。

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

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

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

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

コンソール ポート変更ログ

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

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

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

USB タイプ A ポート

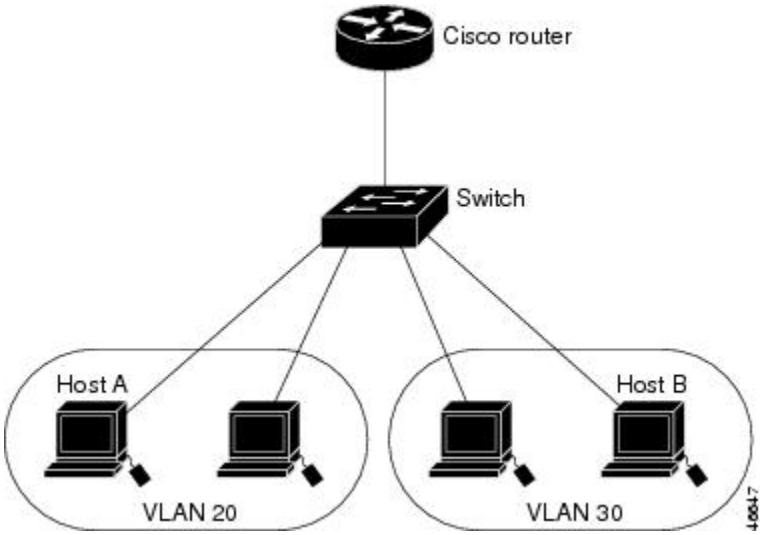
USB タイプ A ポートは、外部 USB フラッシュ デバイス（サム ドライブまたは USB キーとも呼ばれる）へのアクセスを提供します。 スイッチで Cisco 64 MB、256 MB、512 MB、1 GB、4 GB、および 8 GB のフラッシュ ドライブがサポートされます。 標準 Cisco IOS コマンドライン インターフェイス（CLI）コマンドを使用して、フラッシュ デバイスの読み取り、書き込み、および、コピー元やコピー先として使用できます。 スイッチを USB フラッシュ ドライブから起動するようにも設定できます。

インターフェイスの接続

単一 VLAN 内のデバイスは、スイッチを通じて直接通信できます。 異なる VLAN に属すポート間では、ルーティングデバイスを介さなければデータを交換できません。

次の設定例では、VLAN 20 のホスト A が VLAN 30 のホスト B にデータを送信する場合は、データはホスト A からスイッチを経由してルータへ送られた後、再びスイッチに戻ってからホスト B へ送信される必要があります。

図 *1*：スイッチと *VLAN* との接続



標準のレイヤ 2 スイッチを使用すると、異なる VLAN のポートは、ルータを通じて情報を交換する必要があります。

（注） Catalyst 3560-CX スイッチおよび 2960-CX スイッチは、スタッキングをサポートしません。 このドキュメント全体を通じて、すべてのスタッキングへの参照を無視します。

インターフェイス コンフィギュレーション モード

スイッチは、次のインターフェイス タイプをサポートします。

- 物理ポート：スイッチ ポートおよびルーテッド ポート
- VLAN：スイッチ仮想インターフェイス
- ポート チャネル：EtherChannel インターフェイス

インターフェイス範囲も設定できます。

物理インターフェイス（ポート）を設定するには、インターフェイス タイプ、モジュール番号、およびスイッチポート番号を指定して、インターフェイスコンフィギュレーションモードを開始します。

- タイプ：10/100/1000 Mbps イーサネット ポートの場合はギガビット イーサネット（gigabitethernet または gi）、または Small Form-Factor Pluggable（SFP）モジュール ギガビット イーサネット インターフェイス（gigabitethernet または gi）。

- モジュール番号：スイッチのモジュールまたはスロット番号（常に 0）。
- ポート番号：スイッチ上のインターフェイス番号。 10/100/1000 ポート番号は常に 1 から始まり、スイッチに向かって左のポートから順番に付けられています。たとえば、gigabitethernet1/0/1 または gigabitethernet1/0/8 のようになります。 10/100/1000 ポートと SFP モジュール ポートのあるスイッチの場合、SFP モジュール ポートの番号は 10/100/1000 ポートの後に連続して付けられます。

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

イーサネット インターフェイスのデフォルト設定

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

表 *4*：レイヤ *2* イーサネット インターフェイスのデフォルト設定

機能	デフォルト設定
動作モード	レイヤ 2 またはスイッチング モード（**switchport** コマンド）
VLAN 許容範囲	VLAN 1 ～ 4094
デフォルト VLAN（アクセス ポート用）	VLAN 1
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1
802.1p プライオリティ タグ付きトラフィック	VLAN 0 のタグが付いたパケットをすべてドロップします。
VLAN トランキング	Switchport mode dynamic auto（DTP をサポート）
ポート イネーブル ステート	すべてのポートがイネーブル
ポート記述	未定義
速度	自動ネゴシエーション（10 ギガビットインターフェイス上では未サポート）
デュプレックス モード	自動ネゴシエーション（10 ギガビットインターフェイス上では未サポート）

機能	デフォルト設定
フロー制御	フロー制御は **receive: off** に設定されます。 送信パケットでは常にオフです。
EtherChannel（PAgP）	すべてのイーサネット ポートでディセーブル。
ポートブロッキング（不明マルチキャストおよび不明ユニキャスト トラフィック）	ディセーブル（ブロッキングされない）。
ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御	ディセーブル
保護ポート	ディセーブル
ポート セキュリティ	ディセーブル
PortFast	ディセーブル
Auto-MDIX	イネーブル （注） 受電デバイスがクロス ケーブルでスイッチに接続されている場合、スイッチは、IEEE 802.3af に完全には準拠していない、Cisco IP Phone やアクセス ポイントなどの準規格の受電をサポートしていない場合があります。 これは、スイッチ ポート上で Automatic Medium-Dependent Interface Crossover（Auto-MIDX）がイネーブルかどうかは関係ありません。
Power over Ethernet（PoE）	イネーブル（auto）
キープアライブ メッセージ	SFP モジュールでディセーブル。他のすべてのポートでイネーブル。

インターフェイス速度およびデュプレックス モード

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

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

速度とデュプレックス モードの設定時の注意事項

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

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

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

IEEE 802.3x フロー制御

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

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

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

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

デバイスのフロー制御設定には、次のルールが適用されます。

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

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

インターフェイスの特性の設定方法

インターフェイスの設定

次の一般的な手順は、すべてのインターフェイス設定プロセスに当てはまります。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	インターフェイス
	
	例：
	
	`Switch(config)# interface gigabitethernet1/0/1`
	`Switch(config-if)#`
		インターフェイス タイプ、スイッチおよびコネクタの数を識別します。
		
		（注） インターフェイス タイプとインターフェイス番号の間にスペースを入れる必要はありません。 たとえば、前出の行の場合は、**gigabitethernet 1/0/1**、**gigabitethernet1/0/1**、**gi 1/0/1**、または **gi1/0/1** のいずれかを指定できます。

ステップ 4	各 **interface** コマンドの後ろに、インターフェイスに必要なインターフェイス コンフィギュレーション コマンドを続けて入力します。	インターフェイス上で実行するプロトコルとアプリケーションを定義します。 別のインターフェイス コマンドまたは **end** を入力して特権EXECモードに戻ると、コマンドが収集されてインターフェイスに適用されます。
ステップ 5	**interface range** or **interface range macro**	（任意）インターフェイスの範囲を設定します。 （注） ある範囲内で設定したインターフェイスは、同じタイプである必要があります。また、同じ機能オプションを指定して設定しなければなりません。
ステップ 6	**show interfaces**	スイッチ上のまたはスイッチに対して設定されたすべてのインターフェイスのリストを表示します。 デバイスがサポートする各インターフェイスまたは指定したインターフェイスのレポートが出力されます。

インターフェイスに関する記述の追加

手順の概要

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

手順の詳細

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

インターフェイス範囲の設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface range** {*port-range* | **macro***macro_name*} 例： `Switch(config)# interface range macro`	設定するインターフェイス範囲（VLAN または物理ポート）を指定し、インターフェイス コンフィギュレーション モードを開始します。 • **interface range** コマンドを使用すると、最大 5 つのポート範囲または定義済みマクロを 1 つ設定できます。 • **macro** 変数については、インターフェイス レンジ マクロの設定および使用方法, （31 ページ）を参照してください。 • カンマで区切った *port-range* では、各エントリに対応するインターフェイス タイプを入力し、カンマの前後にスペースを含めます。

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

インターフェイス レンジ マクロの設定および使用方法

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

手順の概要

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

手順の詳細

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

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

イーサネット インターフェイスの設定

インターフェイス速度およびデュプレックス パラメータの設定

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/3`	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**speed** {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**} 例： `Switch(config-if)# speed 10`	このコマンドは、10 ギガビットイーサネットインターフェイスでは使用できません。 インターフェイスに対する適切な速度パラメータを入力します。 • インターフェイスの特定の速度を設定するには、**10**、**100**、または **1000** を入力します。 **1000** キーワードを使用できるのは、10/100/1000 Mbps ポートに対してだけです。 • インターフェイスに接続されたデバイスと自動ネゴシエーションが行えるようにするには、**auto** を入力します。 **auto**キーワードと一緒に **10**、**100**、または **1000** キーワードを使用した場合、ポートは指定の速度でのみ自動ネゴシエートします。 • **nonegotiate** キーワードを使用できるのは、SFP モジュールポートに対してだけです。 SFP モジュール ポートは 1000 Mbps だけで動作しますが、自動ネゴシエーションをサポートしていないデバイスに接続されている場合は、ネゴシエートしないように設定できます。
ステップ 5	**duplex** {**auto** | **full** | **half**} 例： `Switch(config-if)# duplex half`	このコマンドは、10 ギガビットイーサネットインターフェイスでは使用できません。 インターフェイスのデュプレックス パラメータを入力します。 半二重モードをイネーブルにします（10 または 100Mbps のみで動作するインターフェイスの場合）。 1000 Mbps で動作するインターフェイスには半二重モードを設定できません。

	コマンドまたはアクション	目的
		デュプレックス設定を行うことができるのは、速度が **auto** に設定されている場合です。
ステップ **6**	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ **7**	**show interfaces***interface-id* 例： `Switch# show interfaces gigabitethernet1/0/3`	インターフェイス速度およびデュプレックス モードの設定を表示します。
ステップ **8**	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ **9**	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IEEE 802.3x フロー制御の設定

手順の概要

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

手順の詳細

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

SVI 自動ステート除外の設定

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	レイヤ 2 インターフェイス（物理ポートまたはポートチャネル）を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport autostate exclude** 例： `Switch(config-if)# switchport autostate exclude`	SVI ライン ステート（アップまたはダウン）のステータスを定義する際、アクセスまたはトランク ポートを除外します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running config interface***interface-id*	（任意）実行コンフィギュレーションを表示します。 設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスのシャットダウンおよび再起動

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

手順の概要

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

手順の詳細

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

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

コンソール メディア タイプの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lineconsole 0** 例： `Switch(config)# line console 0`	コンソールを設定し、ライン コンフィギュレーション モードを開始します。
ステップ 4	**media-typerj45** 例： `Switch(config-line)# media-type rj45`	コンソール メディア タイプがRJ-45ポート以外に設定されないようにします。 このコマンドを入力せず、両方のタイプが接続された場合は、デフォルトでUSBポートが使用されます。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config`	（任意）コンフィギュレーションファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

USB 無活動タイムアウトの設定

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

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**usb-inactivity-timeout** *timeout-minutes* 例： `Switch(config-line)#` **`usb-inactivity-timeout 30`**	コンソールポートの無活動タイムアウトを指定します。指定できる範囲は 1 ～ 240 分です。 デフォルトでは、タイムアウトが設定されていません。
ステップ 5	**copy running-config startup-config** 例： `Switch#` **`copy running-config startup-config`**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイス特性のモニタ

インターフェイス ステータスのモニタ

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

表 *5*：インターフェイス用の ***show*** コマンド

コマンド	目的
show interfaces*interface-id* **status** [**err-disabled**]	インターフェイスのステータスまたはerrdisableステートにあるインターフェイスのリストを表示します。
show interfaces [*interface-id*] **switchport**	スイッチング（非ルーティング）ポートの管理上および動作上のステータスを表示します。 このコマンドを使用すると、ポートがルーティングまたはスイッチングのどちらのモードにあるかが判別できます。
show interfaces [*interface-id*] **description**	1つのインターフェイスまたはすべてのインターフェイスに関する記述とインターフェイスのステータスを表示します。

コマンド	目的
show ip interface [*interface-id*]	IP ルーティング用に設定されたすべてのインターフェイスまたは特定のインターフェイスについて、使用できるかどうかを表示します。
show interface [*interface-id*] **stats**	インターフェイスのパスごとに入出力パケットを表示します。
show interfaces*interface-id*	（任意）インターフェイスの速度およびデュプレックスを表示します。
show interfaces transceiver dom-supported-list	（任意）接続 SFP モジュールの Digital Optical Monitoring（DOM）ステータスを表示します。
show interfaces transceiver properties	（任意）インターフェイスの温度、電圧、電流量を表示します。
show interfaces [*interface-id*] [{**transceiver properties** | **detail**}] *module number*]	SFP モジュールに関する物理および動作ステータスを表示します。
show running-config interface [*interface-id*]	インターフェイスに対応する RAM 上の実行コンフィギュレーションを表示します。
show version	ハードウェア設定、ソフトウェアバージョン、コンフィギュレーションファイルの名前と送信元、およびブートイメージを表示します。
show controllers ethernet-controller*interface-id***phy**	インターフェイスの Auto-MDIX 動作ステートを表示します。

インターフェイスおよびカウンタのクリアとリセット

表 ***6*** : インターフェイス用の ***clear*** コマンド

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

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

インターフェイス特性の設定例

インターフェイスの説明の追加：例

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

インターフェイス範囲の設定：例

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

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 4
Switch(config-if-range)# speed 100
```

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

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

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

インターフェイス レンジ マクロの設定および使用方法：例

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

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

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

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

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

```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

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

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

インターフェイス速度およびデュプレックス モードの設定：例

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

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

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

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

コンソール メディア タイプの設定：例

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

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# media-type rj45
```

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

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# no media-type rj45
```

USB 無活動タイムアウトの設定：例

次に、無活動タイムアウトを 30 分に設定する例を示します。

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# usb-inactivity-timeout 30
```

設定をディセーブルにするには、次のコマンドを使用します。

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# no usb-inactivity-timeout
```

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

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

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

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

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

第 3 章

Auto-MDIX の設定

- Auto-MDIX の前提条件，47 ページ
- Auto-MDIX の制約事項，47 ページ
- Auto-MDIX の設定に関する情報，48 ページ
- Auto-MDIX の設定方法，49 ページ
- Auto-MDIX の設定例，50 ページ

Auto-MDIX の前提条件

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

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

Auto-MDIX の制約事項

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

Auto-MDIX の設定に関する情報

インターフェイスでの Auto-MDIX

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

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

表 *7*：リンク状態と *Auto-MDIX* の設定

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

Auto-MDIX の設定方法

インターフェイスでの Auto-MDIX の設定

手順の概要

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

手順の詳細

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

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

Auto-MDIX の設定例

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

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

第 4 章

LLDP、LLDP-MED、およびワイヤードロケーション サービスの設定

- 機能情報の確認，51 ページ
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要，51 ページ
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定方法，56 ページ
- LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定例，69 ページ
- LLDP、LLDP-MED、ワイヤード ロケーション サービスのモニタリングとメンテナンス，69 ページ

機能情報の確認

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

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

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要

LLDP

Cisco Discovery Protocol（CDP）は、すべてのシスコ製デバイス（ルータ、ブリッジ、アクセス サーバ、スイッチ、およびコントローラ）のレイヤ 2（データ リンク層）上で動作するデバイス

検出プロトコルです。 ネットワーク管理アプリケーションはCDPを使用することにより、ネットワーク接続されている他のシスコ デバイスを自動的に検出し、識別できます。

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

LLDP でサポートされる TLV

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

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

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

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

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

LLDP および Cisco Medianet

LLDP またはCDPのロケーション情報をポート単位で設定すると、リモートデバイスからスイッチに Cisco Medianet のロケーション情報を送信できます。 詳細については、 http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.html を参照してください。

LLDP-MED

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

LLDP-MED でサポートされる TLV

LLDP-MED では、次の TLV がサポートされます。

- LLDP-MED 機能 TLV

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

- ネットワーク ポリシー TLV

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

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

- 電源管理 TLV

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

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

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

- インベントリ管理 TLV

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

- ロケーション TLV

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

- 都市ロケーション情報

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

- ELIN ロケーション情報

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

ワイヤード ロケーション サービス

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

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

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

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

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

- スイッチによる関連付け検出後の時間（秒）

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

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

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

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

デフォルトの LLDP 設定

表 *8*：デフォルトの *LLDP* 設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	ディセーブル（すべての TLV との送受信）
LLDP インターフェイス ステート	ディセーブル
LLDP 受信	ディセーブル

機能	デフォルト設定
LLDP 転送	ディセーブル
LLDP med-tlv-select	ディセーブル（すべての LLDP-MED TLV への送信）。LLDP がグローバルにイネーブルにされると、LLDP-MED-TLV もイネーブルになります。

LLDP に関する制約事項

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

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

LLDP のイネーブル化

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lldp run** 例： `Switch (config)# lldp run`	スイッチで LLDP をグローバルにイネーブルにします。
ステップ 4	**interface***interface-id* 例： `Switch (config)# interface gigabitethernet2/0/1`	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**lldp transmit** 例： `Switch(config-if)# lldp transmit`	LLDP パケットを送信するようにインターフェイスをイネーブルにします。
ステップ 6	**lldp receive** 例： `Switch(config-if)# lldp receive`	LLDP パケットを受信するようにインターフェイスをイネーブルにします。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show lldp** 例： `Switch# show lldp`	設定を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

LLDP 特性の設定

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch>` **`enable`**	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch#` **`configure terminal`**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lldp holdtime***seconds* 例： `Switch(config)#` **`lldp holdtime 120`**	（任意）デバイスから送信された情報を受信側デバイスが廃棄するまで保持する必要がある期間を指定します。 指定できる範囲は 0 ～ 65535 秒です。デフォルトは 120 秒です。
ステップ 4	**lldp reinit***delay* 例： `Switch(config)#` **`lldp reinit 2`**	（任意）任意のインターフェイス上で LLDP の初期化の遅延時間（秒）を指定します。 指定できる範囲は 2 ～ 5 秒です。デフォルトは 2 秒です。
ステップ 5	**lldp timer***rate* 例： `Switch(config)#` **`lldp timer 30`**	（任意）インターフェイス上で LLDP の更新の遅延時間（秒）を指定します。 指定できる範囲は 5 ～ 65534 秒です。デフォルトは 30 秒です。
ステップ 6	**lldp tlv-select** 例： `Switch(config)#` **`tlv-select`**	（任意）送受信する LLDP TLV を指定します。
ステップ 7	**interface***interface-id* 例： `Switch (config)#` **`interface gigabitethernet2/0/1`**	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**lldp med-tlv-select** 例： `Switch (config-if)# lldp med-tlv-select inventory management`	（任意）送受信する LLDP-MED TLV を指定します。
ステップ 9	**end** 例： `Switch (config-if)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show lldp** 例： `Switch# show lldp`	設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

LLDP-MED TLV の設定

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

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

表 *9*：***LLDP-MED TLV***

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

LLDP-MED TLV	説明
power-management	LLDP-MED 電源管理 TLV

インターフェイスで TLV をイネーブルにするには、次の手順に従います。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch (config)# interface gigabitethernet2/0/1`	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lldp med-tlv-select** 例： `Switch(config-if)# lldp med-tlv-select inventory management`	イネーブルにする TLV を指定します。

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

Network-Policy TLV の設定

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**network-policy profile***profile number* 例： `Switch(config)# network-policy profile 1`	ネットワーク ポリシープロファイル番号を指定し、ネットワーク ポリシー コンフィギュレーション モードを開始します。 指定できる範囲は 1 ～ 4294967295 です。
ステップ 4	{**voice** | **voice-signaling**} **vlan** [*vlan-id* {**cos***cvalue* | **dscp***dvalue*}] | [[**dot1p** {**cos***cvalue* | **dscp***dvalue*}] | **none** | **untagged**] 例： `Switch(config-network-policy)# voice vlan 100 cos 4`	ポリシー属性の設定： • **voice**：音声アプリケーション タイプを指定します。 • **voice-signaling**：音声シグナリング アプリケーション タイプを指定します。 • **vlan**：音声トラフィックのネイティブ VLAN を指定します。 • *vlan-id*：（任意）音声トラフィックの VLAN を指定します。 指定できる範囲は 1 ～ 4094 です。 • **cos***cvalue*：（任意）設定された VLAN のレイヤ 2 プライオリティ サービス クラス（CoS）を指定します。 指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。 • **dscp***dvalue*：（任意）設定された VLAN の Differentiated Services Code Point（DSCP）値を指定します。 指定できる範囲は 0 ～ 63 です。デフォルト値は 46 です。 • **dot1p**：（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話機を設定します。 • **none**：（任意）音声 VLAN に関して IP Phone に指示しません。 IP Phone のキーパッドから入力された設定を使用します。 • **untagged**：（任意）タグなしの音声トラフィックを送信するように IP Phone を設定します。 これが IP Phone のデフォルト設定になります。 • **untagged**：（任意）タグなしの音声トラフィックを送信するように IP Phone を設定します。 これが IP Phone のデフォルト設定になります。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Switch(config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface***interface-id* 例： `Switch (config)# interface gigabitethernet2/0/1`	ネットワーク ポリシープロファイルを設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 7	**network-policy***profile number* 例： `Switch(config-if)# network-policy 1`	ネットワーク ポリシー プロファイル番号を指定します。
ステップ 8	**lldp med-tlv-select network-policy** 例： `Switch(config-if)# lldp med-tlv-select network-policy`	ネットワーク ポリシー TLV を指定します。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show network-policy profile** 例： `Switch# show network-policy profile`	設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ロケーション TLV およびワイヤード ロケーション サービスの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**location** {**admin-tag** *string* | **civic-location identifier** {*id* | **host**} | **elin-location** *string* **identifier** *id* | **custom-location identifier** {*id* | **host**} | **geo-location identifier** {*id* | **host**}}	エンドポイントにロケーション情報を指定します。 • **admin-tag**：管理タグまたはサイト情報を指定します。

	コマンドまたはアクション	目的

	例：
	`Switch(config)# location civic-location identifier 1`
	`Switch(config-civic)# number 3550`
	`Switch(config-civic)# primary-road-name "Cisco Way"`
	`Switch(config-civic)# city "San Jose"`
	`Switch(config-civic)# state CA`
	`Switch(config-civic)# building 19`
	`Switch(config-civic)# room C6`
	`Switch(config-civic)# county "Santa Clara"`
	`Switch(config-civic)# country US`
		• **civic-location**：都市ロケーション情報を指定します。
		• **elin-location**：緊急ロケーション情報（ELIN）を指定します。
		• **custom-location**：カスタム ロケーション情報を指定します。
		• **geo-location**：地理空間のロケーション情報を指定します。
		• **identifier** *id*：都市、ELIN、カスタム、または地理ロケーションの ID を指定します。
		• **host**：ホストの都市、カスタム、または地理ロケーションを指定します。
		• *string*：サイト情報またはロケーション情報を英数字形式で指定します。

ステップ 3	**exit** 例： `Switch(config-civic)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**interface** *interface-id* 例： `Switch (config)# interface gigabitethernet2/0/1`	ロケーション情報を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**location** {**additional-location-information** *word* | **civic-location-id** {*id* | **host**} | **elin-location-id** *id* | **custom-location-id** {*id* | **host**} | **geo-location-id** {*id* | **host**} } 例： `Switch(config-if)# location elin-location-id 1`	インターフェイスのロケーション情報を入力します。 • **additional-location-information**：ロケーションまたは場所に関する追加情報を指定します。 • **civic-location-id**：インターフェイスのグローバル都市ロケーション情報を指定します。 • **elin-location-id**：インターフェイスの緊急ロケーション情報を指定します。 • **custom-location-id**：インターフェイスのカスタム ロケーション情報を指定します。 • **geo-location-id**：インターフェイスの地理空間のロケーション情報を指定します。

	コマンドまたはアクション	目的
		• **host**：ホストのロケーションの ID を指定します。 • *word*：追加のロケーション情報を指定する語またはフレーズを指定します。 • *id*：都市、ELIN、カスタム、または地理ロケーションの ID を指定します。 指定できる ID 範囲は 1 ～ 4095 です。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

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

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

スイッチ上でのワイヤード ロケーション サービスのイネーブル化

はじめる前に

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

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 5	**show network-policy profile** 例： `Switch# show network-policy profile`	設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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

Network-Policy TLV の設定：例

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

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

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

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

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

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

コマンド	説明
clear lldp counters	トラフィック カウンタを0にリセットします。
clear lldp table	LLDP ネイバー情報テーブルを削除します。
clear nmsp statistics	NMSP 統計カウンタをクリアします。
show lldp	送信頻度、送信するパケットのホールドタイム、LLDP初期化の遅延時間のような、インターフェイス上のグローバル情報を表示します。
show lldp entry *entry-name*	特定のネイバーに関する情報を表示します。 アスタリスク（*）を入力すると、すべてのネイバーの表示、またはネイバーの名前の入力が可能です。
show lldp interface [*interface-id*]	LLDP がイネーブルに設定されているインターフェイスに関する情報を表示します。 表示対象を特定のインターフェイスに限定できます。
show lldp neighbors [*interface-id*] [**detail**]	デバイスタイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、ポート ID など、ネイバーに関する情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show lldp traffic	送受信パケットの数、廃棄したパケットの数、認識できない TLV の数など、LLDP カウンタを表示します。
show location admin-tag *string*	指定した管理タグまたはサイトのロケーション情報を表示します。
show location civic-location identifier *id*	特定のグローバル都市ロケーションのロケーション情報を表示します。
show location elin-location identifier *id*	緊急ロケーションのロケーション情報を表示します。
show network-policy profile	設定されたネットワークポリシープロファイルを表示します。

コマンド	説明
show nmsp	NMSP 情報を表示します。

第 5 章

システム MTU の設定

- 機能情報の確認，73 ページ
- MTU に関する情報，73 ページ
- MTU の設定方法，74 ページ
- システム MTU の設定例，75 ページ

機能情報の確認

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

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

MTU に関する情報

すべてのインターフェイスで送受信されるフレームのデフォルト最大伝送単位（MTU）サイズは、1500 バイトです。 10 または 100 Mbps で動作するすべてのインターフェイスで MTU サイズを増やすには、**system mtu** グローバル コンフィギュレーション コマンドを使用します。 また、**system mtu jumbo** グローバル コンフィギュレーション コマンドを使用すると、すべてのギガビット イーサネット インターフェイス上でジャンボ フレームをサポートするように MTU サイズを増やすことができます。

（注） スイッチは CPU でジャンボ フレームをサポートします。

システム MTU のガイドライン

システム MTU 値を設定する場合、次の注意事項に留意してください。

- すべてのインターフェイスで送受信されるフレームのデフォルト最大伝送単位（MTU）サイズは、1500 バイトです。 10 または 100 Mbps で動作するすべてのインターフェイスで MTU サイズを増やすには、**system mtu** グローバル コンフィギュレーション コマンドを使用します。 また、**system mtu jumbo** グローバル コンフィギュレーション コマンドを使用すると、すべてのギガビット イーサネット インターフェイス上でジャンボ フレームをサポートするように MTU サイズを増やすことができます。
- **system mtu** コマンドはギガビット イーサネット ポートには影響せず、**system mtu jumbo** コマンドは 10/100 ポートには影響しません。 **system mtu jumbo** コマンドを設定していない場合、**system mtu** コマンドの設定はすべてのギガビット イーサネット インターフェイスに適用されます。

MTU の設定方法

システム MTU の設定

10/100 インターフェイスまたはギガビット イーサネット インターフェイスすべての MTU サイズを変更するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **system mtu***bytes*
3. **system mtujumbo***bytes*
4. **end**
5. **copyrunning-config startup-config**
6. **reload**
7. **show system mtu**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**system mtu***bytes* 例： `Switch(config)# system mtu 2500`	指定できる範囲は、1500 ～ 1998 バイトです。デフォルトは 1500 バイトです。
ステップ 3	**system mtujumbo***bytes* 例： `Switch(config)# system mtu jumbo 7500`	指定できる範囲は、1500 ～ 9198 バイトです。デフォルトは 1500 バイトです。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copyrunning-config startup-config** 例： `Switch# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。
ステップ 6	**reload** 例： `Switch# reload`	オペレーティング システムをリロードします。
ステップ 7	**show system mtu** 例： `Switch# show system mtu`	設定を確認します。

システム MTU の設定例

次に、ギガビット イーサネット ポートの最大パケット サイズを 7500 バイトに設定する例を示します。

```
Switch(config)# system mtu 1900
Switch(config)# system mtu jumbo 7500
Switch(config)# exit
```

特定のインターフェイス タイプで許容範囲外の値を入力した場合、その値は受け入れられません。 次に、ギガビット イーサネット インターフェイスを範囲外の値に設定しようとした場合に表示される応答の例を示します。

```
Switch(config)# system mtu jumbo 25000
                                 ^
% Invalid input detected at '^' marker.
```

次の例では、**show system mtu** コマンドの出力を示します。

```
Switch# show system mtu
Global Ethernet MTU is 1500 bytes.
```

第 6 章

PoE の設定

- 機能情報の確認，77 ページ
- PoE について，77 ページ
- PoE の設定方法，83 ページ
- 電力ステータスのモニタ，91 ページ
- PoE の設定例，92 ページ

機能情報の確認

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

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

PoE について

Power over Ethernet（PoE）ポート

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

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

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

サポート対象のプロトコルおよび標準

スイッチは PoE のサポートで次のプロトコルと規格を使用します。

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

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

  シスコのインテリジェントな電力管理の機能には、電力消費に関して CDP との下位互換性があるため、スイッチは、受信する CDP メッセージに従って応答します。 CDP はサードパーティの受電デバイスをサポートしません。このため、スイッチは IEEE 分類を使用して装置の消費電力を判断します。
- IEEE 802.3a：この規格の主な機能は、受電装置の検出、電力の管理、切断の検出です。オプションとして受電装置の電力分類があります。 詳細については、この規格を参照してください。

関連トピック

Cisco Universal Power Over Ethernet

受電装置の検出および初期電力割り当て

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

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

- 初期電力割り当ては、受電装置が要求する最大電力量です。 スイッチは、受電装置を検出および電力供給する場合、この電力を最初に割り当てます。 スイッチが受電装置から CDP メッセージを受信し、受電装置が CDP 電力ネゴシエーション メッセージを通じてスイッチと電力レベルをネゴシエートしたときに、初期電力割り当てが調整される場合があります。

- スイッチは検出したIEEE装置を消費電力クラス内で分類します。 スイッチは、電力バジェットに使用可能な電力量に基づいて、ポートに通電できるかどうかを決定します。 表 10：IEEE 電力分類, （79 ページ） に、各種レベルの一覧を示します。

表 *10*：*IEEE* 電力分類

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

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

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

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

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

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

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

電力管理モード

スイッチでは、次の PoE モードがサポートされます。

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

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

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

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

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

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

- **static**：スイッチは、受電装置が接続されていなくてもポートに電力をあらかじめ割り当て、そのポートで電力が使用できるようにします。 スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電装置からの CDP メッセージによって調節されることはありません。 これは、電力があらかじめ割り当てられていることから、最

大ワット数以下の電力を使用するすべての受電装置が固定ポートに接続されている場合に電力が保証されるためです。 ポートはもう先着順方式ではなくなります。

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

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

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

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

電力モニタリングおよび電力ポリシング

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

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

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

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

1. スイッチは、個々のポートでリアルタイム消費電力をモニタリングします。
2. スイッチは、ピーク時の電力消費を含め、電力消費を記録します。 スイッチは CISCO-POWER-ETHERNET-EXT-MIB を介して情報を報告します。
3. 電力ポリシングがイネーブルの場合、スイッチはリアルタイムの消費電力を装置に割り当てられた最大電力と比較して、消費電力をポリシングします。 最大消費電力は、PoE ポートでカットオフ電力とも呼ばれます。

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

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

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

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

PoE ポートでの最大電力割り当て（カットオフ電力）

パワー ポリシングがイネーブルである場合、スイッチは次の順序で PoE ポートのカットオフ電力として、これらの値の 1 つを特定します。

1 スイッチがポートに対して予定しているユーザ定義電力レベルを設定している場合は、**power inline consumption default** *wattage* グローバル コンフィギュレーション コマンドまたはインターフェイス コンフィギュレーション コマンドを使用して手動で行う。

2 ポートで許可されている電力を制限するユーザ定義電力レベルを設定している場合は、**power inline auto max** *max-wattage* または **power inline static max** *max-wattage* インターフェイス コンフィギュレーション コマンドを使用して手動で行う。

3 スイッチにおいて受電装置の電力消費が設定されている場合は、CDP 電力ネゴシエーションまたは IEEE 分類と LLDP 電力ネゴシエーションを使用して自動的に行われる。

power inline consumption default *wattage* または **power inline** [**auto** | **static max**] *max-wattage* コマンドを入力することにより、カットオフ電力値を手動で設定するには、前述のリストの 1 番目または 2 番目の方法を使用します。

カットオフ電力量の値を手動で設定しない場合、スイッチは、CDP 電力ネゴシエーションまたはデバイスの IEEE 分類と LLDP 電力ネゴシエーションを使用して自動的に値を決定します。 CDP または LLDP がイネーブルでない場合は、デフォルト値の 30 W が適用されます。 ただし、CDP または LLDP がない場合は、15400 ～ 30000 mW の値が CDP 要求または LLDP 要求だけに基づいて割り当てられるため、装置で 15.4 W を超える電力の消費がスイッチから許可されません。 受電デバイスが CDP または LLDP のネゴシエーションなしに 15.4 W を超える電力を消費する場合、装置は 最大電流（*Imax*）の制限に違反し、最大値を超える電流が供給されるという *Icut* 障害が発生する可能性があります。 再び電源を入れるまで、ポートは障害状態のままになります。 ポートで継続的に 15.4 W を超える電力が給電される場合、このサイクルが繰り返されます。

（注） PoE+ ポートに接続されている受電デバイスが再起動し、電力 TLV で CDP パケットまたは LLDP パケットが送信される場合、スイッチは最初のパケットの電力ネゴシエーションプロトコルをロックし、その他のプロトコルからの電力要求に応答しません。 たとえば、スイッチが CDP にロックされている場合、LLDP 要求を送信する装置に電力を供給しません。 スイッチが CDP にロックされた後で CDP がディセーブルになった場合、スイッチは LLDP 電源要求に応答せず、アクセサリの電源がオンにならなくなります。 この場合、受電デバイスを再起動する必要があります。

電力消費値

ポートの初期電力割り当ておよび最大電力割り当てを設定することができます。 ただし、これらの値は、スイッチが PoE ポートの電力をオンまたはオフにするときを指定するために設定する値

です。 最大電力割り当ては、受電装置の実際の電力消費と同じではありません。 スイッチによって電力ポリシングに使用される実際のカットオフ電力値は、設定済みの電力値と同等ではありません。

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

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

スイッチは内部電源装置および Cisco Redundant Power System 2300（RPS 2300）をサポートしており、受電装置が利用できる総電力量は電源装置の設定によって異なります。

PoE の設定方法

PoE ポートの電力管理モードの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**power inline** {**auto** [**max***max-wattage*] | **never** | **static** [**max***max-wattage*]} 例： `Switch(config-if)# power inline auto`	ポートの PoE モードを設定します。 キーワードの意味は次のとおりです。 • **auto**：受電デバイスの検出をイネーブルにします。 十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。 これがデフォルト設定です。 • **max***max-wattage*：ポートで許可されている電力を制限します。 値を指定しない場合は、最大電力が供給されます。 • **max***max-wattage*：ポートで許可されている電力を制限します。 範囲は 4000 ~ 30000 mW です。 値が指定されていない場合は、最大値が許可されます。 • **never**：装置検出とポートへの電力供給をディセーブルにします。

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

PoE ポートに接続された受電装置の電力バジェット

シスコの受電デバイスが PoE ポートに接続されている場合、スイッチは Cisco Discovery Protocol（CDP）を使用して、受電デバイスの *CDP* 固有の電力消費を判断し、また、スイッチはこれに合せて電力バジェットを調整します。 この機能は、IEEE サードパーティの受電デバイスには適用されません。 この装置の場合、スイッチが電力要求を許可したときに、スイッチが受電装置の IEEE 分類に応じて電力バジェットを調整します。 受電デバイスがクラス 0（クラス ステータス不明）またはクラス 3 の場合、スイッチは CDP 固有の電力所要量に関係なく、受電デバイスに 15,400 mW を計上します。 受電デバイスが CDP 固有の消費よりも高いクラスを報告してきたり、または電力分類（デフォルトはクラス 0）をサポートしていない場合、スイッチは IEEE クラス情報を使用してグローバル電力バジェットを追跡するため、電力供給できるデバイスが少なくなります。

power inline consumption*wattage* インターフェイス コンフィギュレーション コマンドまたは **power inline consumption default***wattage* グローバル コンフィギュレーション コマンドを使用すれば、IEEE 分類で指定されたデフォルトの電力要件を上書きできます。 IEEE 分類で指定された電力と実際に装置が必要とする電力の差は、追加の装置が使用するためグローバル電力バジェットに入れられます。 したがって、スイッチの電力バジェットを拡張してもっと効率的に使用できます。

注意 スイッチの電力バジェットは慎重に計画し、電力モニタリング機能をイネーブルにし、電源装置に対してオーバーサブスクライブにならないようにする必要があります。

（注） 手動で電力バジェットを設定する場合、スイッチと受電デバイスの間のケーブルでの電力消失を考慮する必要があります。

すべての PoE ポートのパワー バジェット

手順の概要

1. **enable**
2. **configure terminal**
3. **no cdp run**
4. **power inline consumption default***wattage*
5. **end**
6. **show power inline consumption default**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no cdp run** 例： `Switch(config)# no cdp run`	（任意）CDP をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**power inline consumption default***wattage* 例： `Switch(config)# power inline consumption default 5000`	各 PoE ポートに接続された受電装置の消費電力を設定します。 各受電装置に指定できる範囲は 4000 ～ 30000 mW（PoE+）です。 デフォルト値は 30000 mW です。 （注）
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show power inline consumption default** 例： `Switch# show power inline consumption default`	消費電力のステータスを表示します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

特定の PoE ポートのパワー バジェット

手順の概要

1. **enable**
2. **configure terminal**
3. **no cdp run**
4. **interface***interface-id*
5. **power inline consumption***wattage*
6. **end**
7. **show power inline consumption**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no cdp run** 例： `Switch(config)# no cdp run`	（任意）CDP をディセーブルにします。
ステップ 4	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**power inline consumption***wattage* 例： `Switch(config-if)# power inline consumption 5000`	スイッチの PoE ポートに接続された受電装置の消費電力を設定します。 各受電装置に指定できる範囲は 4000 ～ 30000 mW（PoE+）です。 デフォルトは 30000 mW（PoE+）です。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show power inline consumption** 例： `Switch# show power inline consumption`	電力消費データを表示します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

電力ポリシングの設定

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

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**power inline police** [**action**{**log** | **errdisable**}] 例： `Switch(config-if)# power inline police`	ポートでリアルタイム消費電力が最大電力割り当てを超えるときに、次のいずれかのアクションを実行するようにスイッチを設定します。 • **power inline police**：PoE ポートをシャット ダウンし、ポートへの電力供給をオフにし、PoE ポートを error-disabled ステートに移行します。 （注） **errdisable detect cause inline-power** グローバル コンフィギュレーション コマンドを使用すると、PoE error-disabled の原因についてエラー検出をイネーブルにできます。 **errdisable recovery cause inline-powerinterval***interval* グローバル コンフィギュレーション コマンドを使用すると、PoE error-disabled ステートから回復するためのタイマーをイネーブルにすることもできます。 • **power inline police action errdisable**：リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、ポートへの電力をオフにします。 • **power inline police action log**：ポートに電力を供給しながら syslog メッセージを生成します。 **action log** キーワードを入力しない場合、デフォルトのアクションによってポートがシャットダウンされ、errdisable ステートになります。
ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	次のいずれかを使用します。 • **errdisable detect cause inline-power** • **errdisable recovery cause inline-power** • **errdisable recovery interval***interval*	（任意）PoE errdisable ステートからのエラー回復をイネーブルにし、PoE 回復メカニズム変数を設定します。 デフォルトでは、回復間隔は 300 秒です。 **interval***interval* では、err-disabled ステートから回復する時間を秒単位で指定します。 指定できる範囲は 30 ～ 86400 です。

	コマンドまたはアクション	目的

	例：
	`Switch(config)# errdisable detect cause inline-power`
	
	`Switch(config)# errdisable recovery cause inline-power`
	
	`Switch(config)# errdisable recovery interval 100`	

ステップ 7	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。

ステップ 8	次のいずれかを使用します。
	• **show power inline police**
	• **show errdisable recovery**
	
	例：
	`Switch# show power inline police`
	
	`Switch# show errdisable recovery`
		電力モニタリング ステータスを表示し、エラー回復設定を確認します。

ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

電力ステータスのモニタ

表 *11*：電力ステータスの *show* コマンド

コマンド	目的
show env power switch	（任意）指定したスイッチの内部電源装置のステータスを表示します。
show power inline[*interface-id*	スイッチ、インターフェイス、の PoE ステータスを表示します。

コマンド	目的
show power inline police	電力ポリシングのデータを表示します。

PoE の設定例

パワー バジェット：例

次のいずれかのコマンドを入力すると、

- [**no**] **power inline consumption default** *wattage* グローバル コンフィギュレーション コマンド
- [**no**] **power inline consumption** *wattage*

  インターフェイス コンフィギュレーション コマンド

次の注意メッセージが表示されます。

```
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline  consumption/allocation'
command may cause damage to the
switch and void your warranty. Take precaution not to oversubscribe the power supply. It
is recommended to enable power
policing if the switch supports it. Refer to documentation.
```

第 7 章

EEE の設定

- 機能情報の確認，93 ページ
- EEE について，93 ページ
- EEE の制約事項，94 ページ
- EEE の設定方法，94 ページ
- EEE のモニタリング，96 ページ
- EEE の設定例，96 ページ

機能情報の確認

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

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

EEE について

EEE の概要

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

低電力アイドル（LPI）モードをサポートするデバイスで EEE をイネーブルにできます。 このようなデバイスは、低い使用率のときに LPI モードを開始して、電力を節約できます。 LPI モード

では、リンクの両端にあるシステムは、特定のサービスをシャット ダウンして、電力を節約できます。 EEE は上位層プロトコルおよびアプリケーションに対して透過的であるように、LPI モードに移行したり、LPI モードから移行する必要があるプロトコルを提供します。

デフォルトの EEE 設定

EEE はデフォルトでディセーブルになっています。

EEE はデフォルトでイネーブルになっています。

EEE の制約事項

EEE には、次の制約事項があります。

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

EEE の設定方法

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

EEE のイネーブル化またはディセーブル化

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**power efficient-ethernet auto** 例： `Switch(config-if)# power efficient-ethernet auto`	特定のインターフェイスで EEE をイネーブルにします。 EEE がイネーブルの場合、デバイスはリンクパートナーにEEEをアドバタイズし、自動ネゴシエートします。
ステップ 4	**no power efficient-ethernet auto** 例： `Switch(config-if)# no power efficient-ethernet auto`	指定したインターフェイス上で EEE をディセーブルにします。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

EEE のモニタリング

表 *12* : *EEE* 設定を表示するコマンド

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

EEE の設定例

次に、インターフェイスで EEE をイネーブルにする例を示します。

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

次に、インターフェイスで EEE をディセーブルにする例を示します。

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

第 II 部

IPv6

- MLD スヌーピングの設定，99 ページ
- IPv6 ユニキャスト ルーティングの設定，117 ページ
- IPv6 マルチキャストの実装，181 ページ

第 8 章

MLD スヌーピングの設定

このモジュールには、MLD スヌーピングの設定の詳細が含まれています。

- 機能情報の確認，99 ページ
- IPv6 MLD スヌーピングの設定に関する情報，99 ページ
- IPv6 MLD スヌーピングの設定方法，104 ページ
- MLD スヌーピング情報の表示，113 ページ
- MLD スヌーピングの設定例，114 ページ

機能情報の確認

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

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

IPv6 MLD スヌーピングの設定に関する情報

スイッチ上で Multicast Listener Discovery（MLD）スヌーピングを使用して、スイッチド ネットワーク内のクライアントおよびルータに IP Version 6（IPv6）マルチキャスト データを効率的に配信することができます。 特に明記しない限り、スイッチという用語は、スタンドアロン スイッチを指します。

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

MLD スヌーピングの概要

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

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

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

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

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

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

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

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

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

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

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

MLD クエリー

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

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

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

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

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

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ（IGMP Leave メッセージと同等）を送信できます。 スイッチが MLDv1 Done メッセージを受信した際に、即時脱退

がイネーブルでなければ、スイッチはメッセージを受信したポートにMASQを送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

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

マルチキャスト ルータ検出

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

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。
- 複数のルータが同じレイヤ2インターフェイス上にある場合、MLD スヌーピングではポート上の単一のマルチキャスト ルータ（直前にルータ制御パケットを送信したルータ）を追跡します。
- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの 5 分に基づきます。ポート上で制御パケットが 5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合のみです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出された後は、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

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

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナー メッセージ抑制）は自動的にイネーブルになります。 レポート抑制により、スイッチはグループで受信された最初の

MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。 MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

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

MLD Done メッセージおよび即時脱退

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

VLAN で即時脱退がイネーブルでない場合に（1 つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。 ユーザは、既存アドレスのポート メンバーシップが削除される時期を MASQ 数の観点から制御できます。 アドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

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

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

TCN 処理

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

IPv6 MLD スヌーピングの設定方法

MLD スヌーピングのデフォルト設定

表 *13* : ***MLD*** スヌーピングのデフォルト設定

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

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。
- IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。 スイッチで両方の機能を同時にイネーブルにできます。

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

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

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

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config** 例： `Switch(config)# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 5	**reload** 例： `Switch(config)# reload`	OS（オペレーティング システム）をリロードします。

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

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

手順の詳細

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

	コマンドまたはアクション	目的
	vlan 1	（注） VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。
ステップ 4	**end** 例： `Switch(config)# ipv6 mld snooping vlan 1`	特権 EXEC モードに戻ります。

スタティック マルチキャスト グループの設定（CLI）

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

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

手順の詳細

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

	コマンドまたはアクション	目的
		• *interface-id* は、メンバ ポートです。 物理インターフェイスまたはポート チャネル（1 ～ 48）に設定できます。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ステップ 4	次のいずれかを使用します。
	• **show ipv6 mld snooping address**
	• **show ipv6 mld snooping address vlan***vlan-id*
	
	例：
	`Switch# show ipv6 mld snooping address`
	または
	`Switch# show ipv6 mld snooping vlan 1`
		スタティック メンバ ポートおよび IPv6 アドレスを確認します。

マルチキャスト ルータ ポートの設定（CLI）

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

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ipv6 mld snooping vlan***vlan-id***mrouter interface***interface-id* 例： `Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet 0/2`	マルチキャスト ルータの VLAN ID を指定して、マルチキャスト ルータにインターフェイスを指定します。 • 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。 指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping mrouter** [**vlan***vlan-id*] 例： `Switch# show ipv6 mld snooping mrouter vlan 1`	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。

MLD 即時脱退の有効化（CLI）

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping vlan***vlan-id* 例： `Switch# show ipv6 mld snooping vlan 1`	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。

MLD スヌーピング クエリーの設定（CLI）

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**ipv6 mld snooping last-listener-query-count***count* 例： `Switch(config)# ipv6 mld snooping last-listener-query-count 7`	（任意）MLD クライアントがエージング アウトされる前にスイッチが送信する MASQ 数を設定します。 指定できる範囲は 1 ～ 7 です。デフォルトは 2 です。 クエリーは 1 秒後に送信されます。
ステップ 5	**ipv6 mld snooping vlan***vlan-id***last-listener-query-count***count* 例： `Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-count 7`	（任意）VLAN 単位で last-listener クエリー カウントを設定します。 この値はグローバルに設定された値を上書きします。 指定できる範囲は 1 ～ 7 です。デフォルトは 0 です。 0 に設定すると、グローバルなカウント値が使用されます。 クエリーは 1秒後に送信されます。
ステップ 6	**ipv6 mld snooping last-listener-query-interval***interval* 例： `Switch(config)# ipv6 mld snooping last-listener-query-interval 2000`	（任意）スイッチが MASQ を送信したあと、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。 指定できる範囲は、100 ～ 32,768 ミリ秒です。 デフォルト値は 1000（1 秒）です。
ステップ 7	**ipv6 mld snooping vlan***vlan-id***last-listener-query-interval***interval* 例： `Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 2000`	（任意）VLAN 単位で last-listener クエリー インターバルを設定します。 この値はグローバルに設定された値を上書きします。 指定できる範囲は、0 ～ 32,768 ミリ秒です。 デフォルトは 0 です。 0 に設定すると、グローバルな最後のリスナー クエリー インターバルが使用されます。
ステップ 8	**ipv6 mld snooping tcn query solicit** 例： `Switch(config)# ipv6 mld snooping tcn query solicit`	（任意）トポロジ変更通知（TCN）をイネーブルにします。 これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラフィックすべてをフラッディングしてから、マルチキャストデータをマルチキャストデータの受信を要求するポートに対してのみ送信します。 デフォルトでは、TCN はディセーブルに設定されています。
ステップ 9	**ipv6 mld snooping tcn flood query count***count* 例： `Switch(config)# ipv6 mld snooping tcn flood query count 5`	（任意）TCN がイネーブルの場合、送信される TCN クエリー数を指定します。 指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 10	**end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**show ipv6 mld snooping querier** [**vlan***vlan-id*] 例： `Switch(config)# show ipv6 mld snooping querier vlan 1`	（任意）スイッチまたは VLAN の MLD スヌーピング クエリア情報を確認します。

MLD リスナー メッセージ抑制の無効化（CLI）

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

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

手順の詳細

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

MLD スヌーピング情報の表示

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

表 *14* : ***MLD*** スヌーピング情報表示用のコマンド

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

コマンド	目的
show ipv6 mld snooping address [**vlan***vlan-id*] [**count** | **dynamic** | **user**]	すべての IPv6 マルチキャスト アドレス情報あるいはスイッチまたは VLAN の特定の IPv6 マルチキャスト アドレス情報を表示します。 • **count** を入力して、スイッチまたは VLAN のグループ数を表示します。 • **dynamic** を入力して、スイッチまたは VLAN の MLD スヌーピング学習済みグループ情報を表示します。 • **user** を入力して、スイッチまたは VLAN の MLD スヌーピング ユーザ設定グループ情報を表示します。
show ipv6 mld snooping address vlan*vlan-id* [*ipv6-multicast-address*]	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。

MLD スヌーピングの設定例

スタティックなマルチキャスト グループの設定：例

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

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet

          1/0/1
Switch(config)# end
```

マルチキャスト ルータ ポートの設定：例

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

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet

          0/2
Switch(config)# exit
```

MLD 即時脱退のイネーブル化：例

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

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

MLD スヌーピング クエリーの設定：例

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

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit
```

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

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

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

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

第 9 章

IPv6 ユニキャスト ルーティングの設定

- 機能情報の確認，117 ページ
- IPv6 ユニキャスト ルーティングの設定について，117 ページ
- DHCP for IPv6 アドレス割り当ての設定，171 ページ
- IPv6 ユニキャスト ルーティングの設定例，175 ページ

機能情報の確認

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

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

IPv6 ユニキャスト ルーティングの設定について

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

IPv6 の概要

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

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

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 およびこの章のその他の機能については、

- 『*Cisco IOS IPv6 Configuration Library*』を参照してください。
- Cisco.com の [Search] フィールドを使用して、Cisco IOS ソフトウェア マニュアルを特定します。 たとえば、スタティック ルートについての情報が必要な場合は、[Search] フィールドで *Implementing Static Routes for IPv6* と入力すると、スタティック ルートについて調べられます。

IPv6 アドレス

スイッチがサポートするのは、IPv6ユニキャストアドレスのみです。 サイトローカルなユニキャスト アドレスおよびマルチキャスト アドレスはサポートされません。

IPv6 の 128 ビット アドレスは、コロンで区切られた一連の 8 つの 16 進フィールド（n:n:n:n:n:n:n:n. の形式）で表されます。 次に、IPv6 アドレスの例を示します。

2031:0000:130F:0000:0000:09C0:080F:130B

実装を容易にするために、各フィールドの先行ゼロは省略可能です。 上記アドレスは、先行ゼロを省略した次のアドレスと同じです。

2031:0:130F:0:0:9C0:80F:130B

2 つのコロン（::）を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この短縮形を使用できるのは、各アドレス内で 1 回のみです。

2031:0:130F::09C0:080F:130B

IPv6 アドレス形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Implementing Addressing and Basic Connectivity」の章では、次の項の内容が Catalyst 2960、2960-S、2960-C、2960-X、2960-CX、3560-CX スイッチに適用されます。

- IPv6 アドレス形式
- IPv6 アドレス タイプ：マルチキャスト
- IPv6 アドレスの出力表示
- 簡易 IPv6 パケット ヘッダー

サポート対象の IPv6 ユニキャスト ルーティング機能

ここでは、スイッチでサポートされている IPv6 プロトコル機能について説明します。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクに対してローカルなユニキャストアドレスをサポートします。 サイトに対してローカルなユニキャストアドレスはサポートされていません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能グローバル ユニキャスト プレフィックスの付いた IPv6 アドレスです。 このアドレス構造を使用すると、ルーティング プレフィックスを厳格に集約することができ、グローバル ルーティング テーブル内のルーティング テーブル エントリ数が制限されます。 これらのアドレスは、組織を経由して最終的にインターネット サービス プロバイダーに至る集約リンク上で使用されます。

  これらのアドレスはグローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID によって定義されます。 現在のグローバル ユニキャスト アドレス割り当てには、バイナリ値 001（2000::/3）で開始するアドレス範囲が使用されます。 プレフィックスが 2000::/3（001）～ E000::/3（111）のアドレスには、Extended Unique Identifier（EUI）64 フォーマットの 64 ビット インターフェイス ID を設定する必要があります。

- リンクに対してローカルなユニキャストアドレスをすべてのインターフェイスに自動的に設定するには、修飾EUIフォーマット内で、リンクに対してローカルなプレフィックスFE80::/10（1111 1110 10）およびインターフェイスIDを使用します。 ネイバー探索プロトコル（NDP）およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。 ローカル リンク上のノードは、リンクに対してローカルなアドレスを使用します。 通信する場合に、グローバルに一意なアドレスは不要です。 IPv6ルータは、リンクに対してローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章にある IPv6 ユニキャスト アドレスに関する項を参照してください。

IPv6 の *DNS*

IPv6 は、ドメイン ネーム システム（DNS）のレコード タイプを、DNS 名前/アドレスおよびアドレス/名前の検索プロセスでサポートします。 DNS AAAA リソース レコード タイプは IPv6 アドレスをサポートし、IPv4 の A アドレス レコードと同等です。 スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス *MTU* ディスカバリ

スイッチはシステム最大伝送単位（MTU）の IPv6 ノードへのアドバタイズおよびパス MTU ディスカバリをサポートします。 パス MTU ディスカバリを使用すると、ホストは指定されたデータパスを通るすべてのリンクのMTUサイズを動的に検出して、サイズに合せて調整できます。 IPv6 では、パスを通るリンクの MTU サイズが小さくてパケット サイズに対応できない場合、パケットの送信元がフラグメンテーションを処理します。

ICMPv6

IPv6のインターネット制御メッセージプロトコル（ICMP）は、ICMP宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。 IPv6 では、ネイバー探索プロトコルおよびパス MTU ディスカバリに ICMP パケットも使用されます。

ネイバー探索

スイッチは、IPv6 対応の NDP、ICMPv6 の最上部で稼働するプロトコル、および NDP をサポートしない IPv6 ステーション対応のスタティック ネイバー エントリをサポートします。 IPv6 ネイバー探索プロセスは ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 未満のルートに対して ICMPv6 リダイレクトをサポートしています。マスク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトがサポートされません。

ネイバー探索スロットリングにより、IPv6 パケットをルーティングするためにネクスト ホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。 IPv6 パケットのネクスト ホップがスイッチによってアクティブに解決しようとしている同じネイバーである場合は、そのようなパケットが追加されると、スイッチはそのパケットをドロップします。 このドロップにより、CPU に余分な負荷がかからないようになります。

DRP

スイッチは、ルータのアドバタイズメント メッセージの拡張機能である、IPv6 Default Router Prefernce（DRP）をサポートします。 DRP では、特にホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合に、ホストが適切なルータを選択する機能が向上しました。スイッチは、Route Information Option（RFC 4191）をサポートしません。

IPv6 ホストは、オフリンク宛先へのトラフィック用にルータを選択する、デフォルト ルータ リストを維持します。 次に、宛先用に選択されたルータは、宛先キャッシュに格納されます。 IPv6 NDP では、到達可能であるルータまたは到達可能性の高いルータが、到達可能性が不明または低いルータよりも優先されます。 NDP は、到達可能または到達可能の可能性があるルータとして、常に同じルータを選択するか、またはルータ リストから繰り返し使用できます。 DRP を使用することにより、IPv6 ホストが、両方ともが到達可能または到達可能の可能性がある 2 台のルータを差別化するように設定できます。

DRP for IPv6 の詳細情報については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチではステートレス自動設定が使用されているため、ホストやモバイル IP アドレスの管理のような、リンク、サブネット、およびサイト アドレス指定の変更を管理することができます。ホストはリンクに対してローカルな独自アドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をアドバタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- Ping、traceroute、および Telnet
- IPv6 トランスポートによるセキュア シェル（SSH）
- IPv6 トランスポートによる HTTP サーバ アクセス

- IPv4 トランスポートによる AAAA の DNS レゾルバ
- IPv6 アドレスの Cisco Discovery Protocol（CDP）サポート

これらのアプリケーションの管理に関する詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

DHCP for IPv6 アドレスの割り当て

DHCPv6 を使用すると、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。 このアドレス割り当て機能により、ホストが接続するネットワークに基づいて、適切なプレフィックス内での重複しないアドレス割り当てが管理されます。アドレスは、1 つまたは複数のプレフィックス プールから割り当てることができます。 デフォルトのドメインおよび DNS ネーム サーバ アドレスなど、その他のオプションは、クライアントに戻すことができます。アドレスプールは、特定のインターフェイス、複数のインターフェイス上で使用する場合に割り当てられます。または、サーバが自動的に適切なプールを検出できます。

これらの機能の詳細および設定方法については、『*Cisco IOS IPv6 Configuration Guide*』を参照してください。

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。 DHCPv6 クライアント、サーバ、またはリレーエージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーキング デバイス間のルートを明示的に定義します。 スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

RIP for IPv6

IPv6 の Routing Information Protocol（RIP）は、ルーティング メトリックとしてホップ カウントを使用するディスタンスベクトル プロトコルです。 IPv6 アドレスおよびプレフィックスのサポート、すべての RIP ルータを含むマルチキャスト グループ アドレス FF02::9 を RIP アップデート メッセージの宛先アドレスとして使用する機能などがあります。

IPv6 の RIP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

OSPF for IPv6

フィーチャ セットを実行しているスイッチは、IPv6 の Open Shortest Path First（OSPF）（IP のリンクステート プロトコル）をサポートします。 詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

OSPFv3 グレースフル リスタート

OSPFv3 機能により、OSPFv3 ルーティング プロトコル情報が復元されている間も、既知のルート上でノンストップのデータの転送が可能になります。 スイッチでは、グレースフル リスタートが

リスタート モード（グレースフル リスタート対応スイッチの場合）とヘルパー モード（グレースフル リスタート認識スイッチの場合）のいずれかで使用されます。

グレースフル リスタート機能を使用するには、スイッチがハイアベイラビリティ ステートフル スイッチオーバー（SSO）モードである必要があります（デュアルルートプロセッサ）。グレースフルリスタートに対応したスイッチでは、次の障害が発生したときにグレースフルリスタートが使用されます。

- スタンバイ ルート プロセッサへの切り替えが起こるルート プロセッサ障害
- 計画されたスタンバイ ルート プロセッサへのルート プロセッサの切り替え

グレースフルリスタート機能では、隣接スイッチがグレースフルリスタート認識である必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSFP for IPv6」の章を参照してください。

高速コンバージェンス：*LSA* および *SPF* スロットリング

OSPFv3 リンク ステート アドバタイズメント（LSA）および Shortest Path First（SPF）スロットリング機能は、ネットワークが不安定なときに、OSPFv3 でのリンク ステート アドバタイズメントの更新の速度を低下させる動的な方法ダイナミック方式を提供します。 またこの機能を使用すると、LSA のレート制限をミリ秒単位で指定することにより、OSPFv3 コンバージェンス時間の短縮が可能になります。

OSPFv3 では以前はレート制限 SPF 計算および LSA 生成にスタティック タイマーを使用しました。 これらのタイマーを設定することもできますが、値は秒単位で指定するため、OSPFv3 コンバージェンスに制限が課せられます。 LSA および SPF スロットリングは、すばやく応答できる高度な SPF および LSA レート制限方式を提供することにより、1 秒未満単位でのコンバージェンスを実現し、長引く不安定期間中にも安定性および保護を提供します。

IPsec を使用した認証サポート

OSPF for IPv6（OSPFv3）パケットが変更されずにスイッチに再送信されるようにするには、OSPFv3 パケットを認証する必要があります。 OSPFv3 は、IPsec セキュア ソケット API を使用して OSPFv3 パケットに認証を追加します。 この API は、IPv6 をサポートするように拡張されています。

OSPFv3 では、認証をイネーブルにするために IPsec を使用する必要があります。 OSPFv3 で使用するために必要な IPsec API は暗号イメージのみに含まれるため、認証を使用するには暗号イメージが必要です。

IPv6 の *HSRP* の設定

HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。 IPv6 ホストは、IPv6 ネイバー探索ルータのアドバタイズメントメッセージによって使用可能なルータを学習します。 これらのメッセージは定期的にマルチキャストされるか、ホストにより送信請求されます。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカル アドレスがあります。 HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカルアドレスに

送信されます。グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

（注） IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2（HSRPv2）をイネーブルにする必要があります。

EIGRP IPv6

IP サービス フィーチャ セットを実行中のスイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol（EIGRP）をサポートします。 IPv6 の EIGRP は稼働するインターフェイス上で設定されるため、グローバルな IPv6 アドレスは不要です。

（注） IP ベース フィーチャ セットを実行中のスイッチでは、IPv6 EIGRP スタブ ルーティングを含め、IPv6 EIGRP 機能はすべてサポートされません。

EIGRP IPv6 インスタンスでは、実行する前に暗示的または明示的なルータ ID が必要です。 暗示的なルータ ID はローカルの IPv4 アドレスを基にして作成されるため、すべての IPv4 ノードには常に使用可能なルータ ID があります。 ただし、EIGRP IPv6 は IPv6 ノードだけが含まれるネットワークで稼働するため、使用可能な IPv4 ルータ ID がない場合があります。

EIGRP for IPv6 の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

SNMP と *Syslog*、*IPv6* による

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。 IPv6 による Syslog は、このトランスポートのアドレス データ タイプをサポートします。

IPv6 による SNMP および Syslog は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および Syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

IPv6 に関連するサポートでは、SNMP は既存の IP トランスポート マッピングを変更して、IPv4 と IPv6 を同時にサポートします。 次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザ データグラム プロトコル（UDP）SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信

- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む、IPv6 による SNMP については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、IPv6 による Syslog については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 による *HTTP*（*S*）

HTTP クライアントは要求を IPv4 HTTP サーバと IPv6 HTTP サーバの両方に送信し、これらのサーバは IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。 IPv6 アドレスを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケット コールは、IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを選択します。 受信ソケットは、IPv4 ソケットまたは IPv6 ソケットのいずれかです。 リスニング ソケットは、接続を示す IPvv4 と IPv6 の両方の信号を待ち受け続けます。 IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされています。

基本 TCP/IP スタックは、デュアル スタック環境をサポートします。 HTTP には、TCP/IP スタック、およびネットワーク層相互作用を処理するためのソケットが必要です。

HTTP 接続を確立するには、基本ネットワーク接続（**ping**）がクライアントとサーバ ホストとの間に存在する必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

サポートされていない IPv6 ユニキャスト ルーティング機能

スイッチは、次の IPv6 機能をサポートしません。

- IPv6 ポリシーベース ルーティング
- IPv6 バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）テーブルのサポート
- サイトローカルなアドレス宛ての IPv6 パケット
- IPv4/IPv6 や IPv6/IPv4 などのトンネリング プロトコル
- IPv4/IPv6 または IPv6/IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ
- IPv6 ユニキャスト Reverse-Path Forwarding

IPv6 機能の制限

スイッチでは IPv6 はハードウェアに実装されるため、ハードウェア メモリ内の IPv6 圧縮アドレスによる制限がいくつか発生します。 これらのハードウェア制限により、機能の一部が失われて、制限されます。

機能の制限は次のとおりです。

- スイッチはハードウェアで SNAP カプセル化 IPv6 パケットを転送できません。 これらはソフトウェアで転送されます。
- スイッチはソースルート IPv6 パケットに関する QoS 分類をハードウェアで適用できません。

IPv6 の設定

IPv6 のデフォルト設定

表 *15* : *IPv6* のデフォルト設定

機能	デフォルト設定
SDM テンプレート	デフォルト
IPv6 アドレス	未設定

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化（CLI）

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチ上でグローバル転送する方法を説明します。

スイッチ上の IPv6 を設定する前に、次の注意事項に従ってください。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、16 ビット値を使用したコロン区切りの 16 進形式で指定したアドレスで *ipv6-address* 変数および *ipv6-prefix* 変数を入力する必要があります。 *prefix-length* 変数（スラッシュ（/）で始まる）は、プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバル IPv6 アドレスを設定する必要があります。 インターフェイス上で IPv6 アドレスを設定すると、リンクに対してローカルなアドレスの設定、およびそのインターフェイスに対する IPv6 のアクティブ化が自動的に行われます。 設定されたインターフェイスは、次に示す、該当リンクの必須マルチキャスト グループに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャスト アドレスの送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:ff00::/104（このアドレスはネイバー探索プロセスで使用される）
- すべてのノードを含む、ルータリンクに対してローカルなマルチキャスト グループ FF02::1
- すべてのルータを含む、リンクに対してローカルなマルチキャスト グループ FF02::2

IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

レイヤ 3 インターフェイスに IPv6 アドレスを割り当てて、IPv6 ルーティングをイネーブルにするは、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	スイッチのリロード後、グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 インターフェイスは物理インターフェイス、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できます。
ステップ 3	**noswitchport** 例： `Switch(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	次のいずれかを使用します。 • **ipv6 address***ipv6-prefix/prefix length***eui-64** • **ipv6 address***ipv6-address/prefix length* • **ipv6 address***ipv6-address***link-local** • **ipv6 enable**	• IPv6 アドレスの下位 64 ビットの拡張固有識別子（EUI）を使用して、グローバル IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。 これにより、インターフェイス上で IPv6 処理がイネーブルになります。 • インターフェイスの IPv6 アドレスを手動で設定します。 • インターフェイスで IPv6 がイネーブルな場合に自動設定されるリンクローカルなアドレスでなく、インター

	コマンドまたはアクション	目的

	例：
	`Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64`
	`Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64`
	`Switch(config-if)# ipv6 address 2001:0DB8:c18:1:: link-local`
	`Switch(config-if)# ipv6 enable`
		フェイス上の特定のリンクローカルなアドレスを使用するように指定します。 このコマンドにより、インターフェイス上で IPv6 処理がイネーブルになります。
		• インターフェイスに IPv6 リンクローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。 リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。

ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip routing** 例： `Switch(config)# ip routing`	スイッチ上で IP ルーティングをイネーブルにします。
ステップ 7	**ipv6unicast-routing** 例： `Switch(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データ パケットの転送をイネーブルにします。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ipv6 interface***interface-id* 例： `Switch# show ipv6 interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 10	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化：例, （175 ページ）

IPv6 でのファースト ホップ セキュリティの設定

IPv6 でのファースト ホップ セキュリティの前提条件

- IPv6 がイネーブルになった必要な SDM テンプレートが設定されていること。
- IPv6 ネイバー探索機能についての知識が必要です。

IPv6 でのファースト ホップ セキュリティの制約事項

- 次の制限は、FHS ポリシーを EtherChannel インターフェイスに適用する場合に該当します（ポート チャネル）。
  - FHS ポリシーがアタッチされた物理ポートは EtherChannel グループに参加することができません。
  - FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。

IPv6 でのファースト ホップ セキュリティに関する情報

IPv6 のファーストホップ セキュリティ（FHS IPv6）は、ポリシーを物理インターフェイス、または VLAN にアタッチできる一連の IPv6 セキュリティ機能です。 IPv6 ソフトウェア ポリシー データベース サービスは、これらのポリシーを保存しアクセスします。 ポリシーを設定または変更すると、ポリシー属性はソフトウェア ポリシーデータベースに保存または更新され、その後指定したとおりに適用されます。 次の IPv6 ポリシーが現在サポートされています。

- IPv6 スヌーピング ポリシー：IPv6 スヌーピング ポリシーは、IPv6 内の FHS で使用できるほとんどの機能をイネーブルにできるコンテナ ポリシーとして機能します。
- IPv6 FHS バインディング テーブルの内容：スイッチに接続された IPv6 ネイバーのデータベース テーブルはネイバー探索（ND）プロトコル スヌーピングなどの情報ソースから作成されます。 このデータベースまたはバインディング テーブルは、リンク層アドレス（LLA）、IPv4 または IPv6 アドレス、およびスプーフィングやリダイレクト攻撃を防止するためにネイバーのプレフィックス バインディングを検証するために、さまざまな IPv6 ガード機能（IPv6 ND インスペクションなど）によって使用されます。
- IPv6 ネイバー探索インスペクション：IPv6 ND インスペクションは、レイヤ 2 ネイバー テーブル内のステートレス自動設定アドレスのバインディングを学習し、保護します。 IPv6 ND 検査は、信頼できるバインディング テーブル データベースを構築するためにネイバー探索メッセージを分析します。準拠していない IPv6 ネイバー探索メッセージはドロップされます。 ND メッセージは、その IPv6 からメディア アクセス コントロール（MAC）へのマッピングが検証可能な場合に信頼できると見なされます。

この機能によって、DAD、アドレス解決、ルータ ディスカバリ、ネイバー キャッシュに対する攻撃などの、ND メカニズムに固有の脆弱性のいくつかが軽減されます。

- IPv6 ルータ アドバタイズメント ガード：IPv6 ルータ アドバタイズメント（RA）ガード機能を使用すると、ネットワーク管理者は、ネットワーク スイッチ プラットフォームに到着した不要または不正な RA ガード メッセージをブロックまたは拒否できます。 RA は、リンクで自身をアナウンスするためにルータによって使用されます。 RA ガード機能は、これらの RA を分析して、未承認のルータによって送信された偽の RA をフィルタリングして除外します。 ホスト モードでは、ポートではルータ アドバタイズメントとルータ リダイレクト メッセージはすべて許可されません。 RA ガード機能は、レイヤ 2 デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。 レイヤ 2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。 RA フレームの内容が検証されない場合は、RA はドロップされます。

- IPv6 DHCP ガード：IPv6 DHCP ガード機能は、承認されない DHCPv6 サーバおよびリレー エージェントからの返信およびアドバタイズメントメッセージをブロックします。 IPv6 DHCP ガードは、偽造されたメッセージがバインディング テーブルに入るのを防ぎ、DHCPv6 サーバまたは DHCP リレーからデータを受信することが明示的に設定されていないポートで受信された DHCPv6 サーバ メッセージをブロックできます。 この機能を使用するには、ポリシーを設定してインターフェイスまたは VLAN にアタッチします。 DHCP ガード パケットをデバッグするには、**debug ipv6 snooping dhcp-guard** 特権 EXEC コマンドを使用します。

- IPv6 ソース ガード：IPv4 ソース ガードと同様、IPv6 ソース ガードは送信元アドレス スプーフィングを防ぐために、送信元アドレスまたはプレフィックスを検証します。

  ソース ガードでは、送信元または宛先アドレスに基づいてトラフィックを許可または拒否するようにハードウェアをプログラムします。 ここでは、データ パケットのトラフィックのみを処理します。

  IPv6 ソース ガードとは、IPv6 バインディング テーブルを使用して PACL をインストールし、ホストが無効な IPv6 送信元アドレスを持つパケットを送信しないようにする機能です。

  ソース ガード パケットをデバッグするには、debug ipv6 snooping source-guard 特権 EXEC コマンドを使用します。

  （注） IPv6 PACL 機能は、入力方向だけでサポートされ、出力方向ではサポートされません。

  次の制約事項が適用されます。

  - FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。
  - IPv6 ソース ガードがスイッチ ポートでイネーブルになっている場合は、そのスイッチ ポートが属するインターフェイスで NDP または DHCP スヌーピングをイネーブルにする必要があります。 そうしないと、このポートからのすべてのデータ トラフィックがブロックされます。

- IPv6 ソース ガード ポリシーを VLAN に適用することはできません。 インターフェイス レベルのみでサポートされています。
- IPv6 ソース ガードとプレフィックス ガードは同時に使用できません。 ポリシーをインターフェイスに付加する際は、「アドレスを確認」するか「プレフィックスを確認」する必要はありますが、両方を確認する必要はありません。
- PVLAN と送信元/プレフィックス ガードは同時に適用できません。

IPv6 送信元ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Source Guard」の章を参照してください。

- IPv6 プレフィックス ガード：IPv6 プレフィックス ガードは、IPv6 送信元ガード機能内で動作し、デバイスがトポロジに不正なアドレスから発信されたトラフィックを拒否できるようにします。 IPv6 プレフィックス ガードは、IPv6 プレフィックスが DHCP プレフィックス委任を使用してデバイス（ホーム ゲートウェイなど）に委任される場合によく使用されています。 この機能は、リンクに割り当てられたアドレスの範囲を検出し、この範囲に入っていないアドレスを発信元とするトラフィックをブロックします。

  IPv6 プレフィックス ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Prefix Guard」の章を参照してください。

- IPv6宛先ガード：IPv6宛先ガード機能は、IPv6ネイバー探索で動作し、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決します。 アドレス グリーニング機能に依存して、リンク上でアクティブなすべての宛先をバインディング テーブルに挿入してから、バインディング テーブルで宛先が見つからなかったときに実行される解決をブロックします。

  （注） IPv6宛先 ガードはレイヤ 3 にのみ推奨されます。 レイヤ 2 については推奨しません。

  IPv6 宛先ガードに関する詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Destination Guard」の章を参照してください。

- IPv6 ネイバー検索マルチキャスト抑制：IPv6 ネイバー検索マルチキャスト抑制機能は、IPv6 のスヌーピング機能で、スイッチまたはワイヤレス コントローラで実行し、適切なリンク動作に必要な制御トラフィック量を削減するために使用されます。

- DHCPv6 リレー：Lightweight DHCPv6 リレー エージェント：Lightweight DHCPv6 リレー エージェント機能を使用するとリンクレイヤブリッジング（非ルーティング）機能を実行するアクセス ノードによってリレー エージェント情報が挿入されます。 Lightweight DHCPv6 リレー エージェント（LDRA）機能は、DSL アクセス マルチプレクサ（DSLAM）や IPv6 制御やルーティング機能をサポートしないイーサネット スイッチなどの既存のアクセス ノードに実装できます。 LDRA を使用して、DHCP バージョン 6（DHCPv6）メッセージ交換にリレー エージェント オプションを挿入して、主にクライアント側のインターフェイスを特定します。 LDRA 機能は、インターフェイスと VLAN でイネーブルにできます。

  DHCPv6 リレーの詳細については、『IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15.1SG』の「DHCPv6 Relay—Lightweight DHCPv6 Relay Agent」の項を参照してください。

IPv6 スヌーピング ポリシーの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. **IPv6 snooping policy***policy -name*
4. [**data-glean** |**default** | **device-role** [**node**|**switch**] |**limit**{**address-count***value*} | **no** | **protocol** [**all** | **nodhcp**| **ndp**] |**security-level** [**glean**|**guard**| **inspect**]| **tracking** [**disable**|**enable**]| **trusted-port** }
5. **exit**
6. **show ipv6 snooping policy***policy-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**IPv6 snooping policy***policy -name*	グローバル コンフィギュレーション モードでスヌーピング ポリシーを作成します。
ステップ 4	[**data-glean** |**default**	**device-role** [**node**|**switch**] |**limit**{**address-count***value*}	**no**	**protocol** [**all**	**nodhcp**| **ndp**] |**security-level** [**glean**|**guard**| **inspect**]| **tracking** [**disable**|**enable**]| **trusted-port** }	データ アドレス グリーニングをイネーブルにし、さまざまな条件に対してメッセージを検証し、メッセージのセキュリティ レベルを指定します。 • （任意）**data-glean**：データ アドレス グリーニングをイネーブルにします。 このオプションは、デフォルトで無効です。 • （任意）**default**：すべてのデフォルト オプションを設定します。 • （任意）**device-role** [**node**	**switch**]：ポートに接続されたデバイスのロールを認定します。 • （任意）**limit** {**address-count***value*}：ターゲットごとに許可されるアドレス数を制限します。 • （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。 • （任意）**protocol** [**all**	**dhcp**	**ndp**]：分析のために、スヌーピング機能にどのプロトコルをリダイレクトするかを指定します。 デフォルトは **all** です。 デフォルトを変更するには、**no protocol** コマンドを使用します。

	コマンドまたはアクション	目的
		• （任意）**security-level** [**glean** | **guard** | **inspect**]：この機能によって適用されるセキュリティのレベルを指定します。 ◦ **glean**：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。 ◦ **guard**：アドレスを収集し、メッセージを検査します。 さらに、RA および DHCP サーバ メッセージを拒否します。 これがデフォルトのオプションです。 ◦ **inspect**：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。 • （任意）**tracking** [**disable** | **enable**]：デフォルトのトラッキング動作を上書きし、トラッキング オプションを指定します。 • （任意）**trusted-port**：信頼できるポートを設定します。 これにより、該当するターゲットに対するガードがディセーブルになります。 信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。 また、テーブル内にエントリを作成しているときに衝突が発生した場合も、信頼できるポートが優先されます。
ステップ 5	**exit**	スヌーピング ポリシー コンフィギュレーション モードを終了します。
ステップ 6	**show ipv6 snooping policy***policy-name*	スヌーピング ポリシー設定を表示します。

IPv6 スヌーピング ポリシーのインターフェイスまたは *VLAN* へのアタッチ方法

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかの作業を実行します。
   - **interface***type number*
   - **switchport**
   - **ipv6snooping** [**attach-policy***policy_name*]
     または
   - **vlan configuration***vlan list*
   - **ipv6 snooping attach-policy***policy-name*
4. **show ipv6 snooping policy***policy-name*
5. **show ipv6 neighbors binding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかの作業を実行します。 • **interface***type number* • **switchport** • **ipv6snooping** [**attach-policy***policy_name*] または • **vlan configuration***vlan list* • **ipv6 snooping attach-policy***policy-name*	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。 （注） type は物理インターフェイスでも、イーサチャネルでもかまいません。 インターフェイスをレイヤ 2 ポートとして設定します。 スヌーピングポリシー（データ グリーニングがイネーブル）をインターフェイスに適用します。 ポートと、そのポートに適用されるポリシーを指定します。 （注） スヌーピング ポリシーで **data-glean** をイネーブルにした場合は、そのポリシーを VLAN ではなく、インターフェイスに適用する必要があります。

	コマンドまたはアクション	目的
ステップ 4	**show ipv6 snooping policy***policy-name*	スヌーピング ポリシー設定を表示します。
ステップ 5	**show ipv6 neighbors binding**	スヌーピングポリシーによって入力されたバインディングテーブル エントリを表示します。

デバイスでの *IPv6* ネイバー探索マルチキャスト抑制ポリシーのアタッチ方法

IPv6 ネイバー探索マルチキャスト抑制ポリシーをデバイスにアタッチするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd suppress policy***policy-name*
4. **mode dad-proxy**
5. **mode full-proxy**
6. **mode mc-proxy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd suppress policy***policy-name*	ネイバー探索抑制ポリシー名を定義して、ネイバー探索抑制ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**mode dad-proxy**	IPv6 DADプロキシモードでネイバー探索抑制をイネーブルにします。
ステップ 5	**mode full-proxy**	プロキシ マルチキャストおよびユニキャストのネイバー送信要求メッセージに対するネイバー探索抑制をイネーブルにします。
ステップ 6	**mode mc-proxy**	プロキシ マルチキャスト ネイバー送信要求メッセージに対するネイバー探索抑制をイネーブルにします。

インターフェイスでの IPv6 ネイバー探索マルチキャスト抑制ポリシーのアタッチ方法

IPv6 ネイバー探索マルチキャスト抑制ポリシーをインターフェイスにアタッチするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかの作業を実行します。
   - **interface***type number*
   - **ipv6ndinspection** [**attach-policy***policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]
     または
   - **vlan configuration***vlan-id*
   - **ipv6ndinspection** [**attach-policy***policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかの作業を実行します。 • **interface***type number* • **ipv6ndinspection** [**attach-policy***policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]] または • **vlan configuration***vlan-id* • **ipv6ndinspection** [**attach-policy***policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。 IPv6 ネイバー探索マルチキャスト ポリシーをインターフェイスまたは VLAN にアタッチします。

	コマンドまたはアクション	目的
ステップ 4	**exit**	インターフェイス コンフィギュレーション モードを終了します。

レイヤ 2 EtherChannel インターフェイスへの IPv6 ネイバー探索マルチキャスト抑制ポリシーのアタッチ方法

IPv6 ネイバー探索マルチキャスト抑制ポリシーを EtherChannel インターフェイスにアタッチするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかの作業を実行します。
   - **interface port-channel***port-channel-number*
   - **ipv6ndinspection** [**attach-policy***policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]
     または
   - **vlan configuration***vlan-id*
   - **ipv6ndinspection** [**attach-policy***policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかの作業を実行します。 • **interface port-channel***port-channel-number*	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
	• **ipv6ndinspection** [**attach-policy***policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]] または • **vlan configuration***vlan-id* • **ipv6ndinspection** [**attach-policy***policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]	IPv6 ネイバー探索マルチキャスト ポリシーをインターフェイスまたは VLAN にアタッチします。
ステップ 4	**exit**	インターフェイス コンフィギュレーション モードを終了します。

IPv6 DHCP ガード ポリシーの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp guardpolicy***policy-name*
4. [**default** | **device-role** [**client** | **server**] |**no** | **exit** | **trusted-port**]
5. **exit**
6. 次のいずれかの作業を実行します。
   - **interface***type number*
   - **ipv6 dhcp guard attach-policy***policy-name*

     または
   - **vlan configuration***vlan-id*
   - **ipv6 dhcp guard attach-policy***policy-name*
7. **show ipv6 dhcp guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp guardpolicy***policy-name*	DHCPv6 ガード ポリシー名を指定し、DHCPv6 ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	[**default** | **device-role** [**client** | **server**] |**no** | **exit** | **trusted-port**]	（任意）特定のロールのデバイスからのものではないポート上の DHCPv6 応答および DHCPv6 アドバタイズメントをフィルタします。 デフォルトは **client** です。 • **client**：デフォルト値。アタッチされたデバイスがクライアントであることを指定します。 サーバ メッセージにはこのポートでドロップされます。 • **server**：適用されたデバイスが DHCPv6 サーバであることを指定します。 このポートでは、サーバ メッセージが許可されます。 （任意）**trusted-port**：ポートを信頼モードに設定します。 このポートでは、これ以上のポリシングは実行されません。 （注） 信頼できるポートを設定した場合、device-role オプションは使用できません。
ステップ 5	**exit**	DHCP ガード ポリシー グローバル コンフィギュレーション モードを終了します。
ステップ 6	次のいずれかの作業を実行します。 • **interface***type number* • **ipv6 dhcp guard attach-policy***policy-name* または • **vlan configuration***vlan-id* • **ipv6 dhcp guard attach-policy***policy-name*	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。 DHCP ガードポリシーをインターフェイスまたはVLANに適用します。

	コマンドまたはアクション	目的
ステップ 7	**show ipv6 dhcp guard policy***policy_name*	DHCP ガード ポリシー設定を表示します。

DHCPv6 ガード設定の例

```
enable
configure terminal
ipv6 access-list acl1
 permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy pol1
 device-role server
 match server access-list acl1
 match reply prefix-list abc
 preference min 0
 preference max 255
 trusted-port
interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy pol1 vlan add 1
 vlan configuration 1
  ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

IPv6 ソース ガードの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 source-guard policy***policy_name*
4. [**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }]
5. **ipv6 source-guard**[**attach-policy***policy-name*]
6. **exit**
7. **show ipv6 source-guard policy***policy_name*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ipv6 source-guard policy***policy_name*	IPv6 ソース ガード ポリシー名を指定し、IPv6 ソース ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	[**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }]	IPv6 ソース ガード ポリシーを定義します。 • **deny global-autoconf**：自動設定されたグローバルアドレスからのデータ トラフィックを拒否します。 これは、リンク上のすべてのグローバルアドレスがDHCPによって割り当てられているときに、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。 • **permit link-local**：リンクローカル アドレスから送信されたすべてのデータ トラフィックを許可します。
ステップ 5	**ipv6 source-guard**[**attach-policy***policy-name*]	ポリシー名を指定します。 （任意）**attach-policy** *policy-name*：ポリシー名に基づいてフィルタリングします。
ステップ 6	**exit**	ソース ガード ポリシー コンフィギュレーション モードを終了します。
ステップ 7	**show ipv6 source-guard policy***policy_name*	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

デフォルト ルータ プリファレンスの設定（CLI）

ルータ アドバタイズメント（RA）メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドによって設定される DRP とともに送信されます。 DRP が設定されていない場合は、RA は中小規模のプリファレンスとともに送信されます。

リンク上の 2 つのルータが等価ではあっても、等コストではないルーティングを提供する可能性がある場合、およびポリシーでホストがいずれかのルータを選択するよう指示された場合は、DRP が有効です。

IPv6 の DRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

インターフェイス上のルータに DRP を設定するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始して、DRP を指定するレイヤ 3 インターフェイスを特定します。
ステップ 3	**ipv6 nd router-preference {high | medium | low}** 例： `Switch(config-if)# ipv6 nd router-preference medium`	スイッチ インターフェイス上のルータに DRP を指定します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**showipv6interface** 例： `Switch# show ipv6 interface`	設定を確認します。
ステップ 6	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

デフォルト ルータ プリファレンスの設定：例，（176 ページ）

IPv6 ICMP レート制限の設定（CLI）

ICMP レート制限はデフォルトでイネーブルです。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルト バケット サイズ（バケットに格納される最大トークン数）は 10 です。

ICMP レート制限パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 icmp error-interval***interval* [*bucketsize*] 例： `Switch(config)# ipv6 icmp error-interval 50 20`	IPv6 ICMP エラー メッセージの間隔とバケット サイズを設定します。 • *interval*：バケットに追加されるトークンの間隔（ミリ秒）。 指定できる範囲は 0 ～ 2147483647 ミリ秒です。 • *bucketsize*：（任意）バケットに格納される最大トークン数。 指定できる範囲は 1 ～ 200 です。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 interface** [*interface-id*] 例： `Switch# show ipv6 interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 5	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv6 ICMP レート制限の設定：例, （178 ページ）

IPv6 の CEF および dCEF の設定

シスコエクスプレスフォワーディング（CEF）は、ネットワークパフォーマンスを最適化するためのレイヤ 3 IP スイッチング テクノロジーです。 CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。 高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に振り分けることができます。 IPv4 CEF および dCEF はデフォルトでイネーブルです。 IPv6 CEF および dCEF はデフォルトでディセーブルですが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ルーティングが設定されていない場合は、IPv6 CEF および dCEF は自動的にディセーブルになります。 IPv6 CEF および dCEF は、設定中にディセーブルにできません。 IPv6 ステータスを確認するには、**show ipv6 cef** 特権 EXEC コマンドを入力します。

IPv6 ユニキャスト パケットをルーティングするには、最初に **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して、IPv6ユニキャストパケットの転送をグローバルに設定してから、**ipv6 address** インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイスに IPv6 アドレスおよび IPv6 処理を設定する必要があります。

CEF および dCEF の設定に関する詳細情報については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のスタティック ルーティングの設定（CLI）

スタティック IPv6 ルートを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、インターフェイスに IPv6 アドレスを設定して少なくとも 1 つのレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

スタティック IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ipv6 route***ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*] 例： `Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130`	スタティック IPv6 ルートを設定します。 • *ipv6-prefix*：スタティック ルートの宛先となる IPv6 ネットワーク。 スタティック ホスト ルートを設定する場合は、ホスト名も設定できます。 • */prefixlength*：IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。 10 進数値の前にスラッシュ記号が必要です。 • *ipv6-address*：指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。 ネクスト ホップの IPv6 アドレスを直接接続する必要はありません。再帰処理が実行されて、直接接続されたネクスト ホップの IPv6 アドレスが検出されます。 このアドレスは RFC 2373 に記載された形式（16 ビット値を使用したコロン区切りの 16 進表記で指定）で設定する必要があります。 • *interface-id*：Point-To-Point（ポイントツーポイント）インターフェイスおよびブロードキャスト インターフェイスからのダイレクト スタティック ルートを指定します。 ポイントツーポイント インターフェイスの場合、ネクスト ホップの IPv6 アドレスを指定する必要はありません。 ブロードキャスト インターフェイスの場合は、常にネクスト ホップの IPv6 アドレスを指定するか、または指定したプレフィックスをリンクに割り当てて、リンクに対してローカルなアドレスをネクスト ホップとして指定する必要があります。 パケットの送信先となるネクスト ホップの IPv6 アドレスを指定することもできます。 （注） リンクに対してローカルなアドレスをネクスト ホップとして使用する場合は、*interface-id* を指定する必要があります（リンクに対してローカルなネクスト ホップを隣接ルータに設定する必要もあります）。 • *administrative distance*：（任意）アドミニストレーティブ ディスタンス。 指定できる範囲は 1 ～ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルート タイプよりも、スタティック ルートが優先します。 フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスを使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを使用します。
	• **show ipv6 static**[*ipv6-address* | *ipv6-prefix/prefix length*] [**interface***interface-id*] [**detail**]][**recursive**] [**detail**]
	• **show ipv6 route static**[*updated*]
	
	例：
	`Switch# show ipv6 static 2001:0DB8::/32 interface gigabitethernet2/0/1`
	または
	`Switch# show ipv6 route static`
		IPv6 ルーティング テーブルの内容を表示して、設定を確認します。
		• **interface***interface-id*：（任意）出力インターフェイスとして指定されたインターフェイスを含むスタティック ルートのみを表示します。
		• **recursive**：（任意）再帰スタティック ルートのみを表示します。**recursive** キーワードは **interface** キーワードと相互に排他的です。ただし、コマンド構文に IPv6 プレフィックスが指定されているかどうかに関係なく、使用することができます。
		• **detail**：（任意）次に示す追加情報を表示します。
		◦ 有効な再帰ルートの場合、出力パス セットおよび最大分解深度
		◦ 無効なルートの場合、ルートが無効な理由

ステップ 5	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv6 のスタティック ルーティングの設定：例, （178 ページ）

RIP for IPv6 の設定（CLI）

IPv6 RIP を実行するようにスイッチを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにして、IPv6 RIP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

IPv6 の RIP ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router rip***name* 例： `Switch(config)# ipv6 router rip cisco`	IPv6 RIP ルーティング プロセスを設定し、このプロセスに対してルータ コンフィギュレーションモードを開始します。
ステップ 3	**maximum-paths***number-paths* 例： `Switch(config-router)# maximum-paths 6`	（任意）IPv6 RIP がサポートできる等コスト ルートの最大数を定義します。 指定できる範囲は 1 ～ 32 で、デフォルトは 16 ルートです。
ステップ 4	**exit** 例： `Switch(config-router)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーションモードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 6	**ipv6 rip***name***enable** 例： `Switch(config-if)# ipv6 rip cisco enable`	指定された IPv6 RIP ルーティング プロセスをインターフェイス上でイネーブルにします。
ステップ 7	**ipv6 rip***name***default-information** {**only** | **originate**} 例： `Switch(config-if)# ipv6 rip cisco`	（任意）IPv6 デフォルト ルート（::/0）を RIP ルーティング プロセス アップデートに格納して、指定インターフェイスから送信します。

	コマンドまたはアクション	目的
	default-information only	（注） 任意のインターフェイスから IPv6 デフォルト ルート（::/0）を送信したあとに、ルーティング ループが発生しないようにするために、ルーティング プロセスは任意のインターフェイスで受信したすべてのデフォルト ルートを無視します。 • **only**：デフォルトルートを送信し、現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを抑制するように選択します。 • **originate**：デフォルト ルート、および現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを送信するように選択します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ステップ 9	次のいずれかを使用します。
	• **show ipv6 rip**[*name*] [**interface***interface-id*] [**database**] [**next-hops**]
	• **show ipv6 rip**
	例：
	`Switch# show ipv6 rip cisco interface gigabitethernet2/0/1`
	または
	`Switch# show ipv6 rip`
		• 現在の IPv6 RIP プロセスに関する情報を表示します。
		• IPv6 ルーティング テーブルの現在の内容を表示します。

ステップ 10	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv6 の RIP の設定：例, （178 ページ）

OSPF for IPv6 の設定（CLI）

ネットワークでは、IPv6 の OSPF をカスタマイズできます。 ただし、IPv6 の OSPF のデフォルト設定は、ほとんどのカスタマーおよび機能の要件を満たします。

次の注意事項に従ってください。

- IPv6 コマンドのデフォルト設定を変更する場合は注意してください。 デフォルト設定を変更すると、IPv6 ネットワークの OSPF に悪影響が及ぶことがあります。
- インターフェイスで IPv6 OSPF をイネーブルにする前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 OSPF をイネーブルにするレイヤ 3 インターフェイスで IPv6 をイネーブルにする必要があります。

IPv6 の OSPF ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPF for IPv6」の章を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router ospf***process-id* 例： `Switch(config)# ipv6 router ospf 21`	プロセスに対して OSPF ルータ コンフィギュレーション モードをイネーブルにします。 プロセス ID は、IPv6 OSPF ルーティング プロセスをイネーブルにする場合に管理上割り当てられる番号です。 この ID はローカルに割り当てられ、1 ～ 65535 の正の整数を指定できます。
ステップ 3	**area***area-id***range** {*ipv6-prefix/prefixlength*} [**advertise** | **not-advertise**] [**cost***cost*] 例： `Switch(config)# area .3 range 2001:0DB8::/32 not-advertise`	（任意）エリア境界でルートを統合および集約します。 • *area-id*：ルートをサマライズするエリアの ID。 10 進数または IPv6 プレフィックスのどちらかを指定できます。 • *ipv6-prefix/prefixlength*：宛先 IPv6 ネットワーク、およびプレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進数。 10 進値の前にスラッシュ（/）を付加する必要があります。 • **advertise**：（任意）Type 3 サマリー LSA をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。

	コマンドまたはアクション	目的
		• **not-advertise**：（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。 Type3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。 • **cost***cost*：（任意）現在のサマリー ルートのメトリックまたはコストを設定します。宛先への最短パスを判別する場合に、OSPF SPF 計算で使用します。 指定できる値は 0 ～ 16777215 です。
ステップ 4	**maximum paths***number-paths* 例： `Switch(config)# maximum paths 16`	（任意）IPv6 OSPF がルーティング テーブルに入力する必要がある、同じ宛先への等コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 32 で、デフォルトは 16 です。
ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 7	**ipv6 ospf***process-id***area***area-id* [**instance***instance-id*] 例： `Switch(config-if)# ipv6 ospf 21 area .3`	インターフェイスで IPv6 の OSPF をイネーブルにします。 • **instance***instance-id*：（任意）インスタンス ID。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。	• OSPF インターフェイスに関する情報を表示します。

	コマンドまたはアクション	目的

	• **show ipv6 ospf** [*process-id*] [*area-id*]**interface** [*interface-id*]
	• **show ipv6 ospf** [*process-id*] [*area-id*]
	
	例：
	`Switch# show ipv6 ospf 21 interface gigabitethernet2/0/1`
	または
	`Switch# show ipv6 ospf 21`
		• OSPF ルーティング プロセスに関する一般情報を表示します。

ステップ 10	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPFv3 高速コンバージェンスに対する LSA および SPF タイマーの調整

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6 router ospf***process-id*
4. **timers lsa arrival***milliseconds*
5. **timers pacing flood***milliseconds*
6. **timers pacing lsa-group***seconds*
7. **timers pacing retransmission***milliseconds*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf***process-id*	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**timers lsa arrival***milliseconds*	ソフトウェアが OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定します。
ステップ 5	**timers pacing flood***milliseconds*	LSA フラッド パケット ペーシングを設定します。
ステップ 6	**timers pacing lsa-group***seconds*	OSPFv3 LSA を収集してグループ化し、リフレッシュ、チェックサム、またはエージングを行う間隔を変更します。
ステップ 7	**timers pacing retransmission***milliseconds*	OSPFv3 での LSA 再送信パケット ペーシングを設定します。
ステップ 8	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6 router ospf***process-id*
4. **timers throttle spf***spf-start spf-hold spf-max-wait*
5. **timers throttle lsa***start-intervalhold-intervalmax-interval*
6. **timers lsa arrival***milliseconds*
7. **timers pacing flood***milliseconds*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf***process-id*	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**timers throttle spf***spf-start spf-hold spf-max-wait*	SPF スロットリングをオンにします。
ステップ 5	**timers throttle lsa***start-intervalhold-intervalmax-interval*	OSPFv3 LSA 生成に対するレート制限値を設定します。
ステップ 6	**timers lsa arrival***milliseconds*	ソフトウェアが OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定します。
ステップ 7	**timers pacing flood***milliseconds*	LSA フラッド パケット ペーシングを設定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

IPv6 の EIGRP の設定

IPv6 EIGRP を実行するようにスイッチを設定する前に、 **ip routing global configuration** グローバルコンフィギュレーションコマンドを入力してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを入力して IPv6 パケットの転送をイネーブルにして、IPv6 EIGRP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにします。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定済みのルータ ID を確認してから、**router-id** コマンドを使用します。

EIGRP IPv4 の場合と同様に、EIGRPv6 を使用して EIGRP IPv6 インターフェイスを指定し、これらのサブセットを受動インターフェイスとして選択できます。 **passive-interface** コマンドを使用してインターフェイスをパッシブに設定してから、選択したインターフェイスで **no passive-interface** コマンドを使用してこれらのインターフェイスをアクティブにします。 受動インターフェイスでは、EIGRP IPv6 を設定する必要がありません。

設定手順の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 の HSRP の設定

IPv6 の Hot Standby Router Protocol（HSRP）は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。

スイッチで IPv6 の HSRP がイネーブルである場合、IPv6 ホストは IPv6 ネイバー探索ルータのアドバタイズメント メッセージから使用可能な IPv6 ルータを学習します。 HSRP IPv6 グループには、HSRP グループ番号に基づいて作成される仮想 MAC アドレスがあります。 グループには、デフォルトで、HSRP 仮想 MAC アドレスに基づいて作成される仮想 IPv6 リンクローカル アドレスがあります。 HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。

IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2（HSRPv2）をイネーブルにする必要があります。

（注） IPv6 の HSRP グループを設定する前に、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 の HSRP グループを設定するインターフェイス上で IPv6 をイネーブルにする必要があります。

HSRP バージョン 2 のイネーブル化

IPv6 の HSRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Configuring First Hop Redundancy Protocols in IPv6」の章を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始して、スタンバイ バージョンを指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	**standbyversion** {**1** | **2**} 例： `Switch(config-if)# standby version 2`	HSRP バージョンを設定します。 HSRP バージョンを変更するには、**2** を入力します。 デフォルトは 1 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**showstandby** 例： `Switch# show standby`	設定を確認します。

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

IPv6 の HSRP グループのイネーブル化

ここでは、レイヤ 3 インターフェイス上で IPv6 の HSRP を作成するかイネーブルにする方法について説明します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、IPv6 の HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	**standby** [*group-number*] **ipv6** {*link-local-address* | **autoconfig**} 例： `Switch(config-if)# standby 2 ipv6 auto config`	IPv6 グループの HSRP を作成（またはイネーブルに）します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。 指定できる範囲は 0 ～ 4095 です。 デフォルトは 0 です。 HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • ホット スタンバイ ルータ インターフェイスのリンクローカル アドレスを入力するか、リンクローカル プレフィックスおよび変更された EUI-64 形式のインターフェイス ID から自動的に生成されるリンクローカルアドレスをイネーブルにします。この場合、EUI-64 インターフェイス ID は、関連する HSRP 仮想 MAC アドレスから作成されます。

	コマンドまたはアクション	目的
ステップ 4	**standby** [*group-number*] **preempt** [**delay** {**minimum***seconds* | **reload***seconds* | **sync***seconds*}] 例： `Switch(config-if)# standby 2 preempt delay reload 0`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとして制御を行います。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 • （任意）**delay**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600 秒です（1 時間）。 デフォルトは 0 です（引き継ぐまで遅延がない）。 • （任意）**reload**：リロード後のプリエンプション遅延（秒）を設定します。 遅延時間は、ルータのリロード後の最初のインターフェイスアップ イベントに対してだけ適用されます。 • （任意）**sync**：IP 冗長クライアントの最大同期化時間（秒）を設定します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	**standby** [*group-number*] **priority***priority* 例： `Switch(config-if)# standby 2 priority 200`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。 指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。 最大の値が、最高のプライオリティを表します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show standby** [*interface-id* [*group-number*]] 例： `Switch# show standby gigabitethernet 1/0/1 2`	設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

関連トピック

IPv6 の HSRP グループのイネーブル化：例, （176 ページ）

Multi-VRF CE の設定

スイッチ上で IP サービスまたは拡張 IP サービス フィーチャ セットが稼働している場合、スイッチはカスタマー エッジ（CE）デバイスの複数の VRF ルーティング/転送（Multi-VRF）インスタンスをサポートします（Multi-VRF CE）。 サービス プロバイダーは、Multi-VRF CE により、重複する IP アドレスで複数の VPN をサポートできます。

（注） スイッチでは、VPN のサポートのためにマルチプロトコル ラベル スイッチング（MPLS）が使用されません。

IPv6 マルチキャスト ルーティングは VRF 関連インターフェイスではサポートされません。

Multi-VRF CE のデフォルト設定

表 *16*：*VRF* のデフォルト設定

機能	デフォルト設定
VRF	ディセーブル。 VRF は定義されていません。
マップ	インポートマップ、エクスポートマップ、ルートマップは定義されていません。
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブルです。

VRF の設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 unicast-routing** 例： `Switch(config)# ipv6 unicast routing`	IPv6ユニキャストルーティングをイネーブルにします。
ステップ 3	**vrf definition***vrf-name* 例： `Switch(config)# vrf definition vpn1`	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**address family***ipv6* 例： `Switch(config)# address family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**rd***route-distinguisher* 例： `Switch(config-vrf)# rd 100:2`	ルート識別子を指定して VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 6	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `Switch(config-vrf)# route-target both 100:2`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。 AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。 *route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同一にする必要があります。
ステップ 7	**import map***route-map* 例： `Switch(config-vrf)# import map importmap1`	（任意）VRF にルート マップを対応付けます。

	コマンドまたはアクション	目的
ステップ 8	**interface***interface-id* 例： `Switch(config-vrf)# interface gigabitethernet 1/0/1`	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスにはルーテッド ポートまたは SVI を設定できます。
ステップ 9	**vrf forwarding***vrf-name* 例： `Switch(config-if)# vrf forwarding vpn1`	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 10	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： `Switch# show vrf interfaces vpn1`	設定を確認します。 設定した VRF に関する情報を表示します。
ステップ 12	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VRF 認識サービスの設定

次のサービスは、VRF 認識です。

- ARP
- ping
- 簡易ネットワーク管理プロトコル（SNMP）
- ホットスタンバイ ルータ プロトコル（HSRP）
- ユニキャスト RPF（uRPF）
- Syslog
- traceroute

- FTP および TFTP

（注） このスイッチでは、ユニキャスト RPF（uRPF）およびネットワーク タイム プロトコル（NTP）に対して VRF 認識のサービスはサポートされません。

ネイバー探索用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 neighbors vrf***vrf-name* 例： `Switch# show ipv6 neighbors vrf vpn1`	指定された VRF 内の ARP テーブルを表示します。

ping 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ping vrf***vrf-name***ipv6***ipv6-address* 例： `Switch# ping vrf vpn1 ipv6`	指定された VRF 内の ARP テーブルを表示します。

HSRP 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch# interface gigabitethernet1/0/1`	インターフェイス コンフィギュレーション モードを開始し、HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	**no switchport** 例： `Switch# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	**vrf forwarding***vrf-name* 例： `Switch# vrf forwarding vpn1`	インターフェイス上で VRF を設定します。
ステップ 5	**ipv6 address***ipv6 address* 例： `Switch# ipv6 address 2001::DB8:1/64`	インターフェイスの IPv6 アドレスを入力します。
ステップ 6	**standby 1 ipv6***ipv6 address* 例： `Switch# standby 1 ipv6 2001::DB8:1/64`	HSRP をイネーブルにし、仮想 IP アドレスを設定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

traceroute 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**traceroute vrf***vrf-nameipv6-address* 例： `Switch# traceroute vrf`**`vpn1 2001::DB8:1/64`**	宛先アドレスを取得する VPN VRF の名前を指定します。

FTP および TFTP 用 VRF 認識サービスの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch#` **`configure terminal`**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip ftp source-interface***interface-type interface-number* 例： `Switch(config)# ip ftp source-interface gigabitethernet 1/0/2`	FTP 接続の発信元 IP アドレスを指定します。
ステップ 3	**end** 例： `Switch(config)#end`	特権 EXEC モードに戻ります。
ステップ 4	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 5	**ip tftp source-interface***interface-type interface-number* 例： `Switch(config)# ip tftp source-interface gigabitethernet 1/0/2`	TFTP 接続用の送信元 IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**end** 例： `Switch(config)#end`	特権 EXEC モードに戻ります。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされるルーティング プロトコル（OSPF、EIGRP、または BGP）、またはスタティック ルーティングで設定できます。 ここで説明する設定は OSPF のものですが、その他のプロトコルでも手順は同じです。

（注） VRF インスタンス内で EIGRP ルーティング プロセスが実行されるように設定するには、**autonomous-system***autonomous-system-number* アドレス ファミリ コンフィギュレーション モード コマンドを入力して、自律システム番号を設定する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospfv3***process-id* 例： `Switch(config)# router ospfv3 1`	OSPF ルーティングをイネーブルにして VPN 転送テーブルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**router***router-id* 例： `Switch(config)# router router-id`	この OSPFv3 プロセスの OSPF ルータ ID を IP アドレス形式で指定します。

	コマンドまたはアクション	目的
ステップ 4	**log-adjacency-changes** 例： `Switch(config-router)# log-adjacency-changes`	（任意）隣接ステートの変更を記録します。 これは、デフォルトの状態です。
ステップ 5	**address-family ipv6 unicast vrf***vrf-name* 例： `Switch(config-router)# address-family ipv6 unicast vrf vpn1`	その VRF に対してアドレス ファミリ コマンド モードを開始します。
ステップ 6	**area***area-id normal* 例： `Switch(config-router)# area 2`	OSPFv3 エリア パラメータとタイプを指定します。
ステップ 7	**redistribute bgp***autonomous-system-number* 例： `Switch(config-router)# redistribute bgp 10`	BGP ルーティング プロセスから OSPF ルーティング プロセスにルートを再配布します。
ステップ 8	**end** 例： `Switch(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ospfv3 vrf***vrf-name* 例： `Switch# show ospfv3 vrf vpn1`	OSPFv3 ネットワークの設定を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP PE/CE ルーティング セッションの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system-number* 例： `Switch(config)# router bgp 2`	その他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp router id***router-id* 例： `Switch(config)# bgp router-id`	（任意）固定 32 ビット ルータ ID を、BGP を実行するローカル ルータの ID として設定します。
ステップ 4	**redistribute ospf***process-id* 例： `Switch(config-router)# redistribute ospf 1`	OSPF 内部ルートを再配布するようにスイッチを設定します。
ステップ 5	**address-family ipv6 vrf***vrf-name* 例： `Switch(config-router)# address-family ipv6 vrf vpn1`	PE/CE ルーティング セッションの BGP パラメータを定義し、VRF アドレス ファミリ モードを開始します。
ステップ 6	**network***ipv6 network-number* 例： `Switch(config-router)# network ipv6 255.255.255.0`	BGP を使用して IPv6 ネットワーク番号をアナウンスするように指定します。
ステップ 7	**neighbor***ipv6 address***remote-as***as-number* 例： `Switch(config-router)# neighbor 10.1.1.2 remote-as 2`	PE と CE ルータの間の BGP セッションを定義します。

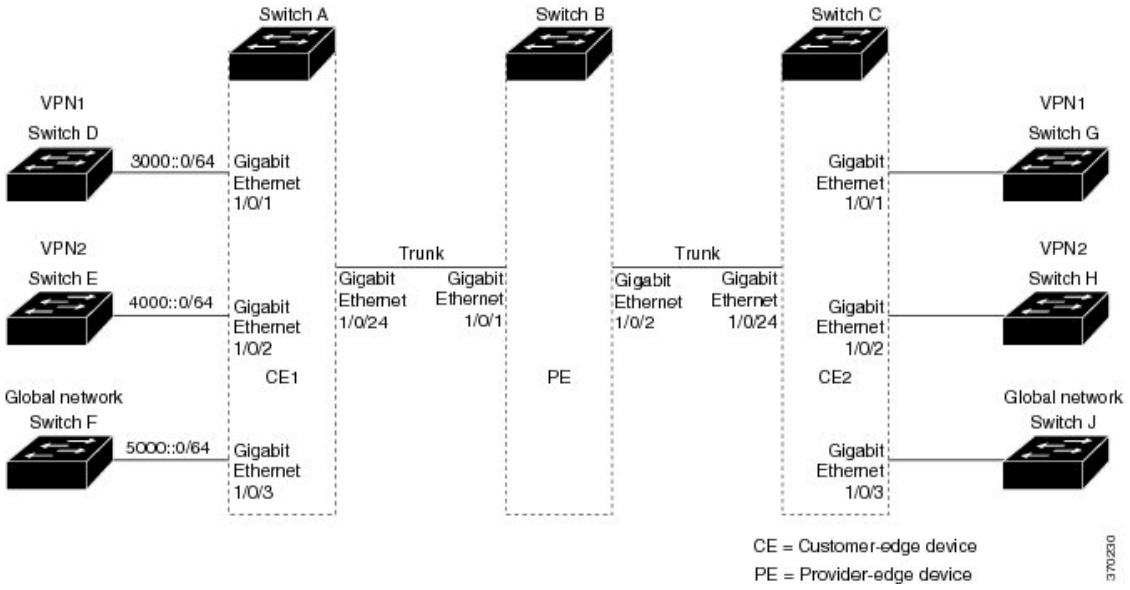
	コマンドまたはアクション	目的
ステップ 8	**neighbor***address***activate** 例： `Switch(config-router)# neighbor 10.2.1.1 activate`	IPv4 アドレス ファミリのアドバタイズメントをアクティブ化します。
ステップ 9	**end** 例： `Switch(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show bgp vrf***vrf-name* 例： `Switch# show ip bgp ipv4 neighbors`	VRF の BGP 設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Multi-VRF CE の設定例

VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。 CE/PE 接続には BGP が使用されます。 図のあとに続く出力は、スイッチを CE スイッチ A として設定する

例、およびカスタマー スイッチ D と E の VRF 設定を示しています。CE スイッチ C とその他のカスタマー スイッチを設定するコマンドは含まれていませんが、内容は同様です。

図 *2*：*Multi-VRF CE* の設定例



スイッチ A では、ルーティングをイネーブルにして VRF を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 unicast-routing
Switch(config)# vrf definition v11
Switch(config-vrf)# rd 11:1
Switch(config-vrf)# address-family ipv6
Switch(config-vrf)# exit
Switch(config-vrf)# vrf definition v12
Switch(config-vrf)# rd 12:1
Switch(config-vrf)# address-family ipv6
Switch(config-vrf-af)# end
```

スイッチ A の物理インターフェイスを設定します。ギガビット イーサネット インターフェイス 1/0/24 は PE へのトランク接続です。 ギガビット イーサネット ポート 1/0/1 と 1/0/2 は VPN に接続されます。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface GigabitEthernet 1/0/1
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# switchport access vlan 118
Switch(config-if)# no ip address
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet 1/0/24
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

スイッチ A で使用する VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。 VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。 VLAN 118 と 208 は、それぞれスイッチ E とスイッチ D を含む VPN に使用されます。

```
Switch(config)# interface vlan10
Switch(config-if)# vrf forwarding v11
Switch(config-if)# ipv6 address 1000::1/64
Switch(config-if)# exit

Switch(config)# interface vlan20
Switch(config-if)# vrf forwarding v12
Switch(config-if)# ipv6 address 2000::1/64
Switch(config-if)# exit

Switch(config)# interface vlan208
Switch(config-if)# vrf forwarding v11
Switch(config-if)# ipv6 address 3000::1/64
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# vrf forwarding v12
Switch(config-if)# ipv6 address 4000::1/64
Switch(config-if)# exit
```

VPN1 と VPN2 で OSPFv3 ルーティングを設定します。

```
Switch(config)# router ospfv3 1
Switch(config-router)# router-id 1.1.1.1
Switch(config-router)# address-family ipv6 unicast vrf v11
Switch(config-router-af)# area 0 normal
Switch(config-router-af)# redistribute bgp 800
Switch(config-router)# exit
Switch(config)# router ospfv3 2
Switch(config-router)# router-id 2.2.2.2
Switch(config-router)# address-family ipv6 unicast vrf v12
Switch(config-router-af)# area 0 normal
Switch(config-router-af)# redistribute bgp 800
Switch(config-router-af)# exit
Switch(config-router)# exit
Switch(config)# exit
```

CE/PE ルーティングに BGP を設定します。

```
Switch(config)# router bgp 800
Switch(config-router)# bgp router-id 8.8.8.8
Switch(config-router)# address-family ipv6 vrf v11
Switch(config-router-af)# redistribute ospf 1
Switch(config-router-af)# neighbor 1000::2 remote-as 100
Switch(config-router-af)# neighbor 1000::2 activate
Switch(config-router-af)# network 3000::/64
Switch(config-router-af)# exit

Switch(config)# address-family ipv6 vrf v12
Switch(config-router-af)# redistribute ospf 2
Switch(config-router-af)# neighbor 2000::2 remote-as 100
Switch(config-router-af)# neighbor 2000::2 activate
Switch(config-router-af)# network 4000::/64
```

スイッチ D は VPN 1 に属します。 次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 unicast-routing
Switch(config)# interface GigabitEthernet 5/0/16
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 3000::2/64
Switch(config-if)# exit

Switch(config-router)# router ospfv3 101
```

```
Switch(config-router)# address-family ipv6
Switch(config-router-af)# area 0 normal
Switch(config-router-af)# redistribute connected
Switch(config-router-af)# exit
Switch(config-router)# exit
```

スイッチ E は VPN 2 に属します。 次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch(config)# ipv6 unicast-routing
Switch(config)# interface GigabitEthernet 3/0/13
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
Switch(config)# interface vlan 20
Switch(config-if)# ipv6 address 4000::2/64


Switch(config)# router ospfv3 101
Switch(config-router)# address-family ipv6
Switch(config-router-af)# area 0 normal
Switch(config-router-af)# redistribute connected
Switch(config-router-af)# end
```

このコマンドをスイッチ B（PE ルータ）で使用すると、CE デバイス、スイッチ A に対する接続だけが設定されます。

```
Switch(config)# vrf definition v1
Switch(config-vrf)# rd 1:1
Switch(config-vrf)# address-family ipv6
Switch(config-vrf-af)# exit
Switch(config-vrf)# exit

Switch(config)# vrf definition v2
Switch(config-vrf)# rd 2:1
Switch(config-vrf)# address-family ipv6
Switch(config-vrf-af)# exit
Switch(config-vrf)# exit

Switch(config-if)# interface g 1/0/2
Switch(config-if)# vrf forwarding v1
Switch(config-if)# ipv6 address 1000::2/64
Switch(config-if)# exit
Switch(config)# interface g 1/0/4
Switch(config-if)# vrf forwarding v2
Switch(config-if)# ipv6 address 2000::2/64

Switch(config-if)# interface gigabitEthernet 1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk

Switch(config)# router bgp 100
Switch(config-router)# address-family ipv6 vrf v1
Switch(config-router-af)# neighbor 1000::1 remote-as 100
Switch(config-router-af)# neighbor 1000::1 activate
Switch(config-router-af)# network 3000::/64
Switch(config-router-af)# exit
Switch(config-router)# address-family ipv6 vrf v2
Switch(config-router-af)# neighbor 2000::1 remote-as 100
Switch(config-router-af)# neighbor 2000::1 activate
Switch(config-router-af)# network 4000::/64
```

Multi-VRF CE ステータスの表示

表 *17* : ***Multi-VRF CE*** 情報を表示するコマンド

コマンド	目的
show ipv6 protocols vrf*vrf -name*	VRF に対応付けられたルーティング プロトコル情報を表示します。
show ipv6 route vrf*vrf -name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**] [**supernets-only**]	VRF に対応付けられた IP ルーティング テーブル情報を表示します。
show ipv6 vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]	定義された VRF インスタンスに関する情報を表示します。

IPv6 の表示

次のコマンドの構文および使用方法の詳細については、Cisco IOS のコマンド リファレンスを参照してください。

表 *18* : ***IPv6*** をモニタリングするコマンド

コマンド	目的
show ipv6 access-list	アクセス リストのサマリーを表示します。
show ipv6 cef	IPv6 の Cisco エクスプレス フォワーディングを表示します。
show ipv6 interface*interface-id*	IPv6 インターフェイスのステータスと設定を表示します。
show ipv6 mtu	宛先キャッシュごとに IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュ エントリを表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 protocols	スイッチの IPv6 ルーティング プロトコルのリストを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。

コマンド	目的
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

関連トピック

IPv6 の表示：例, （178 ページ）

DHCP for IPv6 アドレス割り当ての設定

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトで、DHCPv6 機能はスイッチに設定されています。

DHCPv6 アドレス割り当ての設定時の注意事項

DHCPv6 アドレス割り当てを設定する場合は、次の注意事項に従ってください。

- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイス上でイネーブルである必要があります。
  - SVI：**interface vlan***vlan_id* コマンドを使用して作成された VLAN インターフェイスです。
  - レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel port-channel-number** コマンドを使用して作成されたポートチャネル論理インターフェイス。
- スイッチは、DHCPv6 クライアント、サーバ、またはリレーエージェントとして動作できます。 DHCPv6 クライアント、サーバ、およびリレー機能は、インターフェイスで相互に排他的です。

DHCPv6 サーバ機能のイネーブル化（CLI）

DHCPv6 プールの特性を変更するには、**no** 形式の DHCP プール コンフィギュレーション モード コマンドを使用します。 インターフェイスに対して DHCPv6 サーバ機能をディセーブルにするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスで DHCPv6 サーバをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 dhcp pool***poolname* 例： `Switch(config)# ipv6 dhcp pool 7`	DHCP プール コンフィギュレーション モードを開始して、IPv6 DHCP プールの名前を定義します。 プール名は、記号文字列（Engineering など）または整数（0 など）です。
ステップ 3	**address prefix***IPv6-prefix* {**lifetime**} {*t1 t1* | **infinite**} 例： `Switch(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime 3600`	（任意）アドレス割り当て用のアドレス プレフィックスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 **lifetime***t1 t1*：IPv6 アドレス プレフィックスが有効ステートを維持するタイム インターバル（秒）を指定します。 指定できる範囲は 5 ～ 4294967295 秒です。 間隔を指定しない場合は、**infinite** を指定します。
ステップ 4	**link-address***IPv6-prefix* 例： `Switch(config-dhcpv6)# link-address 2001:1002::0/64`	（任意）link-address IPv6 プレフィックスを指定します。 着信インターフェイス上のアドレスまたはパケットのリンクアドレスが指定した IPv6 プレフィックスに一致する場合、サーバは設定情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
ステップ 5	**vendor-specific***vendor-id* 例： `Switch(config-dhcpv6)# vendor-specific 9`	（任意）ベンダー固有のコンフィギュレーション モードを開始して、ベンダー固有の ID 番号を指定します。 この番号は、ベンダーの IANA プライベート エンタープライズ番号です。 指定できる範囲は 1 ～ 4294967295 です。
ステップ 6	**suboption***number* {**address***IPv6-address* | **ascii***ASCII-string* | **hex***hex-string*} 例： `Switch(config-dhcpv6-vs)# suboption`	（任意）ベンダー固有のサブオプション番号を入力します。 指定できる範囲は 1 ～ 65535 です。 IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプション パラメータで定義されているように入力します。

	コマンドまたはアクション	目的
	`1 address 1000:235D::`	
ステップ 7	**exit** 例： `Switch(config-dhcpv6-vs)# exit`	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 8	**exit** 例： `Switch(config-dhcpv6)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 10	**ipv6dhcpserver** [*poolname* | **automatic**] [**rapid-commit**] [**preference***value*] [**allow-hint**] 例： `Switch(config-if)# ipv6 dhcp server automatic`	インターフェイスに対して DHCPv6 サーバ機能をイネーブルにします。 • *poolname*：（任意）IPv6 DHCP プールのユーザ定義の名前。プール名は、記号文字列（Engineering など）または整数（0 など）です。 • **automatic**：（任意）システムが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。 • **rapid-commit**：（任意）2 つのメッセージの交換方法を許可します。 • **preference***value*：（任意）サーバによって送信されるアドバタイズメントメッセージ内のプリファレンスオプションで指定されるプリファレンス値を設定します。 有効な範囲は 0 ～ 255 です。 デフォルトのプリファレンス値は 0 です。 • **allow-hint**：（任意）サーバが、SOLICIT メッセージ内のクライアントからの指示を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントのヒントを無視します。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ステップ 12	次のいずれかを実行します。
	• **show ipv6 dhcp pool**
	• **show ipv6 dhcp interface**
	
	例：
	`Switch# show ipv6 dhcp pool`
	または
	`Switch# show ipv6 dhcp interface`
		• DHCPv6 プール設定を確認します。
		• DHCPv6 サーバ機能がインターフェイス上でイネーブルであることを確認します。

ステップ 13	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

DHCPv6 サーバ機能のイネーブル化：例, （177 ページ）

DHCPv6 クライアント機能のイネーブル化（CLI）

このタスクでは、インターフェイスに対して DHCPv6 クライアントをイネーブルにする方法を説明します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ipv6 address dhcp** [**rapid-commit**] 例： `Switch(config-if)# ipv6 address dhcp rapid-commit`	インターフェイスで DHCPv6 サーバから IPv6 アドレスを取得できるようにします。 **rapid-commit**：（任意）アドレス割り当てで、2 つのメッセージの交換方法を許可します。
ステップ 4	**ipv6 dhcp client request** [**vendor-specific**] 例： `Switch(config-if)# ipv6 dhcp client request vendor-specific`	（任意）インターフェイスでベンダー固有のオプションを要求できるようにします。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showipv6dhcpinterface** 例： `Switch# show ipv6 dhcp interface`	DHCPv6 クライアントがインターフェイスでイネーブルになっていることを確認します。

関連トピック

DHCPv6 クライアント機能のイネーブル化：例, （177 ページ）

IPv6 ユニキャスト ルーティングの設定例

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化：例

次に、IPv6 プレフィックス 2001:0DB8:c18:1::/64 に基づく、リンクに対してローカルなアドレスおよびグローバル アドレスを使用して、IPv6 をイネーブルにする例を示します。 EUI-64 インターフェイス ID が、両方のアドレスの下位 64 ビットで使用されます。 **show ipv6 interface** EXEC コマ

ンドの出力は、インターフェイスのリンクに対してローカルなプレフィックス FE80::/64 にインターフェイス ID（20B:46FF:FE2F:D940）を付加する方法を示すために追加されています。

```
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/0/11

Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/0/11
GigabitEthernet1/0/11 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

関連トピック

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化（CLI），（125 ページ）

デフォルト ルータ プリファレンスの設定：例

次に、インターフェイス上のルータに高い DRP を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

関連トピック

デフォルト ルータ プリファレンスの設定（CLI），（140 ページ）

IPv6 の HSRP グループのイネーブル化：例

次に、ポートのグループ 1 で IPv6 の HSRP をアクティブにする例を示します。 ホットスタンバイグループで使用される IP アドレスは、IPv6 の HSRP を使用して学習されます。

（注） これは、IPv6 の HSRP をイネーブルにするために必要な最小限の手順です。 その他の設定は任意です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
```

```
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ipv6 autoconfig
Switch(config-if)# end
Switch# show standby
```

関連トピック

IPv6 の HSRP グループのイネーブル化, （155 ページ）

DHCPv6 サーバ機能のイネーブル化：例

次の例では、*engineering* という IPv6 アドレス プレフィックスを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)#address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次に、3 リンクアドレスおよび IPv6 アドレス プレフィックスを持つ *testgroup* と呼ばれるプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

次の例では、*350* というベンダー固有オプションを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

関連トピック

DHCPv6 サーバ機能のイネーブル化（CLI）, （171 ページ）

DHCPv6 クライアント機能のイネーブル化：例

次に、IPv6 アドレスを取得して、rapid-commit オプションをイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

関連トピック

DHCPv6 クライアント機能のイネーブル化（CLI）, （174 ページ）

IPv6 ICMP レート制限の設定：例

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
Switch(config)#ipv6 icmp error-interval 50 20
```

関連トピック

IPv6 ICMP レート制限の設定（CLI），（142 ページ）

IPv6 のスタティック ルーティングの設定：例

次に、アドミニストレーティブ ディスタンスが 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130
```

関連トピック

IPv6 のスタティック ルーティングの設定（CLI），（143 ページ）

IPv6 の RIP の設定：例

次に、最大 8 の等コスト ルートにより RIP ルーティング プロセス *cisco* をイネーブルにし、インターフェイス上でこれをイネーブルにする例を示します。

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface gigabitethernet2/0/11
Switch(config-if)# ipv6 rip cisco enable
```

関連トピック

RIP for IPv6 の設定（CLI），（145 ページ）

IPv6 の表示：例

次に、**show ipv6 interface** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
```

```
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
<output truncated>
```

関連トピック

IPv6 の表示, （170 ページ）

第 10 章

IPv6 マルチキャストの実装

- 機能情報の確認，181 ページ
- IPv6 マルチキャスト ルーティングの実装に関する情報，181 ページ
- IPv6 マルチキャストの実装，194 ページ

機能情報の確認

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

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

IPv6 マルチキャスト ルーティングの実装に関する情報

この章では、スイッチに IPv6 マルチキャスト ルーティングを実装する方法について説明します。

従来の IP 通信では、ホストはパケットを単一のホスト（ユニキャスト伝送）またはすべてのホスト（ブロードキャスト伝送）に送信できます。 IPv6 マルチキャストは、第三の方式を提供するものであり、ホストが単一のデータ ストリームをすべてのホストのサブセット（グループ伝送）に同時に送信できるようにします。

（注） IPv6 マルチキャスト ルーティングは Cisco Catalyst 3560-CX スイッチでのみサポートされます。

IPv6 マルチキャストの概要

IPv6マルチキャスト グループは、特定のデータ ストリームを受信する受信側の任意のグループです。 このグループには、物理的境界または地理的境界はありません。受信側は、インターネット上または任意のプライベート ネットワーク内の任意の場所に配置できます。 特定のグループへのデータ フローの受信に関与する受信側は、ローカル スイッチに対してシグナリングすることによってそのグループに加入する必要があります。 このシグナリングは、MLD プロトコルを使用して行われます。

スイッチは、MLDプロトコルを使用して、直接接続されているサブネットにグループのメンバが存在するかどうかを学習します。 ホストは、MLD レポート メッセージを送信することによってマルチキャスト グループに加入します。 ネットワークでは、各サブネットでマルチキャストデータのコピーを 1 つだけ使用して、潜在的に無制限の受信側にデータが伝送されます。 トラフィックの受信を希望する IPv6 ホストはグループ メンバと呼ばれます。

グループ メンバに伝送されるパケットは、単一のマルチキャスト グループ アドレスによって識別されます。 マルチキャスト パケットは、IPv6ユニキャスト パケットと同様に、ベストエフォート型の信頼性を使用してグループに伝送されます。

マルチキャスト環境は、送信側と受信側で構成されます。 どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。 ただし、グループのメンバだけがメッセージをリッスンして受信できます。

マルチキャスト アドレスがマルチキャスト グループの受信先として選択されます。 送信者は、データグラムの宛先アドレスとしてグループのすべてのメンバに到達するためにそのアドレスを使用します。

マルチキャスト グループ内のメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。 マルチキャスト グループ内のメンバの場所または数に制約はありません。 ホストは、一度に複数のマルチキャスト グループのメンバにすることができます。

マルチキャスト グループがどの程度アクティブであるか、その期間、およびメンバーシップはグループおよび状況によって異なります。 メンバを含むグループにアクティビティがない場合もあります。

IPv6 マルチキャスト ルーティングの実装

Cisco IOS ソフトウェアでは、IPv6 マルチキャスト ルーティングを実装するため、次のプロトコルがサポートされています。

- MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャスト アドレスを宛先としたマルチキャスト パケットを受信するために使用するノード）を検出するために IPv6 スイッチで使用されます。 MLD には 2 つのバージョンがあります。MLD バージョン 1 はバージョン 2 のインターネット グループ管理プロトコル（IGMP）for IPv4 をベースとしています。MLD バージョン 2 はバージョン 3 の IGMP for IPv4 をベースとしています。 Cisco IOS ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 と MLD バージョン 1 の両方が使用されます。 MLD バージョン 2 は、MLD バージョン 1 と完全な下位互換性があります（RFC 2710 で規定）。 MLD バージョン 1 だけをサポートするホストは、

MLD バージョン 2 を実行しているスイッチと相互運用します。 MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。

- PIM-SM は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。
- PIM in Source Specific Multicast（PIM-SSM）は PIM-SM と類似していますが、IP マルチキャストアドレスを宛先とした特定の送信元アドレス（または特定の送信元アドレスを除くすべてのアドレス）からのパケットを受信する対象をレポートする機能を別途備えています。

MLD アクセス グループ

MLD アクセス グループは、Cisco IOS IPv6 マルチキャスト スイッチでの受信側アクセス コントロールを実現します。 この機能では、受信側が加入できるグループのリストを制限し、SSM チャネルへの加入に使用される送信元を許可または拒否します。

受信側の明示的トラッキング

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。 また、この機能により、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

IPv6 マルチキャスト ユーザ認証およびプロファイル サポート

IPv6 マルチキャストは、ネットワーク内の任意のホストがマルチキャスト グループの受信側または送信元になれる設計になっています。 したがって、ネットワークのマルチキャスト トラフィックを制御するには、マルチキャスト アクセス コントロールが必要です。 アクセス コントロール機能は、主に、送信元のアクセス コントロールとアカウンティング、受信側のアクセス コントロールとアカウンティング、およびこのアクセスコントロールメカニズムのプロビジョニングで構成されます。

マルチキャスト アクセス コントロールは、マルチキャストと認証、許可、アカウンティング（AAA）間のインターフェイスを提供し、ラストホップ スイッチ、マルチキャストにおける受信側アクセスコントロール機能、およびマルチキャストにおけるグループまたはチャネルディセーブル化機能でのプロビジョニング、許可、およびアカウンティングを実現します。

新しいマルチキャスト サービス環境を展開する場合、ユーザ認証を追加し、インターフェイス単位でユーザ プロファイルのダウンロードを行う必要があります。 AAA と IPv6 マルチキャストを使用すると、マルチキャスト環境でのユーザ認証とユーザ プロファイルのダウンロードがサポートされます。

RADIUS サーバからアクセス スイッチへのマルチキャスト アクセス コントロール プロファイルのダウンロードをトリガーするイベントは、アクセス スイッチへの MLD join の着信です。 このイベントが発生すると、ユーザは認可キャッシュのタイム アウトを発生させて定期的なダウンロードを要求するか、または適切な multicast clear コマンドを使用してプロファイルが変更された場合に新規ダウンロードをトリガーできます。

アカウンティングはRADIUSアカウンティングを使用して行われます。 開始および停止アカウンティング レコードは、アクセス スイッチから RADIUS サーバに送信されます。 リソースの消費をストリーム単位で追跡できるように、これらのアカウンティング レコードには、マルチキャスト送信元およびグループに関する情報が含まれています。 ラストホップ スイッチが新しい MLD レポートを受信すると、開始レコードが送信され、MLD leave を受信するか、何らかの理由によりグループまたはチャネルが削除されると、停止レコードが送信されます。

IPv6 MLD プロキシ

MLD プロキシ機能は、スイッチのアップストリーム インターフェイス上で、スイッチがすべての（*, G）および（S, G）エントリに対して MLD メンバーシップ レポートを生成するか、またはこれらのエントリのユーザ定義サブセットを生成するメカニズムを提供します。 MLD プロキシ機能により、デバイスは、プロキシグループ メンバーシップ情報を学習し、その情報に基づいてマルチキャスト パケットを転送できるようになります。

スイッチが mroute プロキシ エントリの RP として動作する場合、これらのエントリの MLD メンバーシップ レポートを、ユーザが指定したプロキシ インターフェイス上で生成できます。

Protocol Independent Multicast

プロトコル独立マルチキャスト（PIM）は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。 PIM は、ユニキャスト ルーティング プロトコルとは独立して動作し、他のプロトコルと同様に、マルチキャストルートアップデートの送受信を実行します。 ユニキャストルーティング テーブルに値を入力するために LAN でどのユニキャスト ルーティング プロトコルが使用されているかどうかにかかわらず、Cisco IOS PIM では、独自のルーティングテーブルを構築および管理する代わりに、既存のユニキャスト テーブル コンテンツを使用して、Reverse Path Forwarding（RPF）チェックを実行します。

PIM-SM または PIM-SSM のいずれかを使用するように IPv6 マルチキャストを設定することも、ネットワークで PIM-SM と PIM-SSM の両方を使用することもできます。

PIM スパース モード

IPv6 マルチキャストでは、PIM-SM を使用したドメイン内マルチキャスト ルーティングがサポートされています。 PIM-SM は、ユニキャストルーティングを使用して、マルチキャスト ツリー構築用のリバースパス情報を提供しますが、特定のユニキャストルーティングプロトコルには依存しません。

PIM-SM は、トラフィックに対して明示的な要求がある場合を除いて、各マルチキャストに関与しているスイッチの数が比較的少なく、これらのスイッチがグループのマルチキャスト パケットを転送しないときに、マルチキャスト ネットワークで使用されます。 PIM-SM は、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。 PIM-SM は最初に共有ツリーを使用しますが、これには RP の使用が必要となります。

要求は、ツリーのルート ノードに向けてホップバイホップで送信される PIM join を使用して行われます。 PIM-SM のツリーのルート ノードは、共有ツリーの場合は RP、最短パス ツリー（SPT）

の場合はマルチキャスト送信元に直接接続されているファーストホップ スイッチになります。 RP はマルチキャスト グループを追跡し、マルチキャストパケットを送信するホストはそのホストのファーストホップ スイッチによって RP に登録されます。

PIM join がツリーの上位方向に送信されると、要求されたマルチキャスト トラフィックがツリーの下位方向に転送されるように、パス上のスイッチがマルチキャスト転送ステートを設定します。マルチキャスト トラフィックが不要になったら、スイッチはルート ノードに向けてツリーの上位方向に PIM prune を送信し、不必要なトラフィックをプルーニング（削除）送信します。 この PIM prune がホップごとにツリーを上位方向に移動する際、各スイッチはその転送状態を適切に更新します。 最終的に、マルチキャスト グループまたは送信元に関連付けられている転送ステートは削除されます。

マルチキャストデータの送信側は、マルチキャスト グループを宛先としたデータを送信します。送信側の指定スイッチ（DR）は、これらのデータ パケットを受け取り、ユニキャストでカプセル化し、RP に直接送信します。 RP は、カプセル化されたこれらのデータ パケットを受信し、カプセル化を解除し、共有ツリー上に転送します。 そのあと、パケットは、RP ツリー上のスイッチの（*, G）マルチキャスト ツリー ステートに従って、RP ツリー ブランチの任意の場所に複製され、そのマルチキャスト グループのすべての受信側に最終的に到達します。 RP へのデータ パケットのカプセル化のプロセスは登録と呼ばれ、カプセル化されたパケットは PIM レジスタ パケットと呼ばれます。

指定スイッチ

Cisco スイッチは、LAN セグメント上に複数のスイッチが存在する場合、PIM-SM を使用してマルチキャスト トラフィックを転送し、選択プロセスに従って指定スイッチを選択します。

指定スイッチは、PIM register メッセージ、PIM join メッセージ、および PIM prune メッセージを RP に送信し、アクティブな送信元およびホスト グループ メンバーシップに関する情報を通知します。

LAN 上に複数の PIM-SM スイッチが存在する場合は、指定スイッチを選択して、接続されているホストに対するマルチキャスト トラフィックの重複を回避する必要があります。 ipv6 pim dr-priority コマンドを使用して DR の選択を強制することを選択しない限り、最も大きい IPv6 アドレスの PIM スイッチが LAN の DR になります。 このコマンドでは、LAN セグメント上の各スイッチの DR プライオリティ（デフォルトのプライオリティ = 1）を指定して、最もプライオリティの高いスイッチが DR として選択されるようにすることができます。 LAN セグメント上のすべてのスイッチのプライオリティが同じ場合にも、最上位 IPv6 アドレスを持つスイッチが使用されます。

DR で障害が発生した場合、PIM-SM はスイッチ A の障害を検出し、フェールオーバー DR を選択する手段を提供します。 DR（スイッチ A）が動作不能になった場合、スイッチ A とネイバーとの隣接関係がタイムアウトすると、スイッチ B はその状況を検出します。 スイッチ B はホスト A から MLD メンバーシップ レポートを受けているため、このインターフェイスでグループ A の MLD ステートをすでに持ち、新しい DR になると即座に RP に join を送信します。 この段階で、スイッチ B を経由する共有ツリーの新しいブランチの下位方向へのトラフィック フローが再び確立されます。また、ホスト A がトラフィックをソーシングしていた場合、スイッチ B は、ホスト A から次のマルチキャスト パケットを受信した直後に、新しい登録プロセスを開始します。このアクションで、RP による、スイッチ B を経由する新しいブランチを介したホスト A への SPT 加入がトリガーされます。

（注）

- 2 つの PIM スイッチが直接接続されている場合、これらのスイッチはネイバーになります。 PIM ネイバーを表示するには、show ipv6 pim neighbor 特権 EXEC コマンドを使用します。
- DR 選択プロセスは、マルチアクセス LAN のみで必要です。

Rendezvous Point

IPv6 PIM では、組み込み RP がサポートされています。 組み込み RP サポートを利用すると、スイッチは、スタティックに設定されている RP の代わりに、マルチキャスト グループ宛先アドレスを使用して RP 情報を学習できるようになります。 スイッチが RP である場合、RP としてスタティックに設定する必要があります。

スイッチは、MLD レポート内、または PIM メッセージおよびデータ パケット内の組み込み RP グループアドレスを検索します。 このようなアドレスが見つかったら、スイッチはアドレス自体からグループの RP を学習します。 この学習された RP は、グループのすべてのプロトコル アクティビティに使用されます。 スイッチが RP である場合、組み込み RP を RP として設定する必要があり、スイッチはそのようにアドバタイズされます。

組み込み RP よりも優先するスタティック RP を選択するには、特定の組み込み RP グループ範囲またはマスクをスタティック RP のアクセス リストに設定する必要があります。 PIM がスパースモードで設定されている場合は、RP として動作する 1 つ以上のスイッチを選択する必要もあります。 RP は、共有配布ツリーの選択ポイントに配置された単一の共通ルートであり、各ボックスでスタティックに設定されます。

PIM DR は、共有ツリーの下位方向に配布するために、直接接続されているマルチキャスト送信元から RP にデータを転送します。 データは次の 2 つの方法のいずれかを使用して RP に転送されます。

- データは、登録パケットにカプセル化され、DR として動作するファーストホップ スイッチによって直接 RP にユニキャストされます。
- RP 自身が送信元ツリーに加入している場合は、PIM スパース モードの項で説明したように、RPF 転送アルゴリズムに従ってマルチキャスト転送されます。

RP アドレスは、パケットをグループに送信するホストの代わりに、ファーストホップ スイッチによって PIM register メッセージを送信するために使用されます。 また、RP アドレスは、ラストホップ スイッチによって PIM join および prune メッセージを RP に送信してグループ メンバーシップについて通知するためにも使用されます。 すべてのスイッチ（RP スイッチを含む）で RP アドレスを設定する必要があります。

1 つの PIM スイッチを複数のグループの RP にすることができます。 特定のグループの PIM ドメイン内で一度に使用できる RP アドレスは 1 つだけです。 アクセス リストで指定されている条件によって、スイッチがどのグループの RP であるかが判別されます。

IPv6 マルチキャストでは、PIM accept register 機能がサポートされています。これは、RP で PIM-SM register メッセージのフィルタリングを実行するための機能です。 ユーザは、アクセス リストを

照合するか、または登録されている送信元の AS パスとルート マップに指定されている AS パスを比較できます。

PIMv6 エニーキャスト *RP* ソリューションの概要

IPv6 PIM のエニーキャスト RP ソリューションは、IPv6 ネットワークによる PIM-SM RP のエニーキャスト サービスのサポートを可能にします。 これにより、PIM のみを実行するドメイン内でエニーキャスト RP を使用できるようになります。 この機能は、ドメイン間接続が不要な場合に便利です。 エニーキャスト RP は、IPv4 および IPv6 で使用できますが、IPv4 だけで動作する Multicast Source Discovery Protocol（MSDP）には依存しません。

エニーキャスト RP は、PIM RP のデバイスに障害が発生した場合に、高速コンバージェンスを取得するために ISP ベースのバックボーンが使用するメカニズムです。 受信側および送信元が最も近くの RP にランデブーできるようにするには、送信元からのパケットがすべての RP に到達して、加入している受信側を検出する必要があります。

ユニキャスト IP アドレスは RP アドレスとして選択されます。 このアドレスは、静的に設定されるか、またはダイナミック プロトコルを使用して、ドメイン全体のすべての PIM デバイスに配信されます。 ドメイン内の一連のデバイスが、この RP アドレスの RP として動作するように選択されます。これらのデバイスは、エニーキャスト RP セットと呼ばれます。 エニーキャスト RP セット内の各デバイスは、RP アドレスを使用してループバック インターフェイスで設定されます。 また、エニーキャスト RP セット内の各デバイスには、RP 間の通信に使用する別の物理 IP アドレスも必要です。

RP アドレス、または RP アドレスに対応するプレフィックスは、ドメイン内部のユニキャスト ルーティング システムに挿入されます。 エニーキャスト RP セット内の各デバイスは、エニーキャスト RP セット内のその他すべてのデバイスのアドレスで設定されます。また、この設定は、セット内のすべての RP で一致している必要があります。

IPv6 BSR：RP マッピングの設定

ドメイン内の PIM スイッチは、各マルチキャスト グループを正しい RP アドレスにマッピングできる必要があります。 PIM-SM 対応の BSR プロトコルは、グループと RP のマッピング情報をドメイン全体に迅速に配布するためのダイナミック適応メカニズムを備えています。 IPv6 BSR 機能を使用すると、到達不能になった RP が検出され、マッピング テーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。

すべての PIM-SM マルチキャスト グループを RP の IP または IPv6 アドレスに関連付ける必要があります。 新しいマルチキャスト送信側が送信を開始すると、そのローカル DR がこれらのデータ パケットを PIM register メッセージにカプセル化し、そのマルチキャスト グループの RP に送信します。 新しいマルチキャスト受信側が加入すると、そのローカル DR がそのマルチキャスト グループの RP に PIM join メッセージを送信します。 PIM スイッチは、（*, G）join メッセージを送信するとき、RP 方向への次のスイッチを認識して、G（グループ）がそのスイッチにメッセージを送信できるようにする必要があります。 また、PIM スイッチは、（*, G）ステートを使用してデータ パケットを転送するとき、G を宛先としたパケットの正しい着信インターフェイスを認識する必要があります。これは、他のインターフェイスに着信するパケットを拒否する必要があるためです。

ドメイン内の少数のスイッチが候補ブートストラップ スイッチ（C-BSR）として設定され、単一のBSRがそのドメイン用に選択されます。 また、ドメイン内の一連のスイッチが候補RP（C-RP）として設定されます。通常、これらのスイッチは、C-BSRとして設定されているものと同じスイッチです。 候補RPは、候補RPアドバタイズメント（C-RP-Adv）メッセージをそのドメインのBSRに定期的にユニキャストし、RPになる意思をアドバタイズします。 C-RP-Advメッセージには、アドバタイズを行っているC-RPのアドレス、およびグループ アドレスとマスク長のフィールドの任意のリストが含まれています。これらのフィールドは、立候補のアドバタイズの対象となるグループ プレフィックスを示します。 BSRは、定期的に発信するブートストラップ メッセージ（BSM）にこれらの一連のC-RPとそれに対応するグループ プレフィックスを含めます。 BSMは、ドメイン全体にホップバイホップで配布されます。

双方向BSRがサポートされているため、双方向RPをC-RPメッセージおよびBSMの双方向範囲でアドバタイズできます。 システム内のすべてのスイッチは、BSMで双方向範囲を使用できる必要があります。使用できない場合は、双方向RP機能が機能しません。

PIM 送信元固有マルチキャスト

PIM-SSMは、SSMの実装をサポートするルーティング プロトコルであり、PIM-SMから派生したものです。 ただし、PIM-SMではPIM joinを受けてすべてのマルチキャスト送信元からデータが送信されるのに対し、SSM機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラム トラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネット ブロードキャスト トラフィックが拒否されます。 さらに、SSMでは、RPと共有ツリーを使用する代わりに、マルチキャスト グループの送信元アドレスで見つかった情報を使用します。 この情報は、MLDメンバーシップ レポートによってラストホップ スイッチにリレーされる送信元アドレスを通して受信側から提供されます。その結果として、送信元に直接つながる最短パス ツリーが得られます。

SSMでは、データグラムは（S, G）チャネルに基づいて配信されます。 1つの（S, G）チャネルのトラフィックは、IPv6ユニキャスト送信元アドレスSとマルチキャスト グループ アドレスGをIPv6宛先アドレスとして使用するデータグラムで構成されます。 システムは、（S, G）チャネルのメンバになることによって、このトラフィックを受信します。 シグナリングは不要ですが、受信側は特定の送信元からのトラフィックを受信する場合は（S, G）チャネルに加入し、トラフィックを受信しない場合はチャネルから脱退する必要があります。

SSMを動作させるには、MLDバージョン2が必要です。 MLDを使用すると、ホストが送信元の情報を提供できるようになります。 MLDを使用してSSMを動作させるには、Cisco IOS IPv6スイッチ、アプリケーションが実行されているホスト、およびアプリケーション自体でSSMがサポートされている必要があります。

IPv6 用の *SSM* マッピング

IPv6用のSSMマッピングでは、MLDバージョン1の受信側用にスタティックとダイナミックの両方のドメイン ネーム システム（DNS）マッピングがサポートされています。 この機能を使用すると、TCP/IPホスト スタックおよびIPマルチキャスト受信アプリケーションでMLDバージョン2サポートを提供できないホストでIPv6 SSMを展開できます。

SSMマッピングにより、スイッチは実行コンフィギュレーションまたはDNSサーバのいずれかでマルチキャストMLDバージョン1レポートの送信元を検索できるようになります。 そのあと、スイッチは送信元に対する（S, G）joinを開始できます。

PIM 共有ツリーおよびソース ツリー（最短パス ツリー）

デフォルトでは、グループのメンバは、RPをルートとする単一のデータ配布ツリーを通じて、送信側からグループへのデータを受信します。 このタイプの配布ツリーは、共有ツリーまたはランデブー ポイント ツリー（RPT）と呼ばれます（下の図を参照）。 送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。

データしきい値で保証される場合、共有ツリー上のリーフ スイッチは、送信元をルートとするデータ配布ツリーへの切り替えを開始できます。 このタイプの配布ツリーは、最短パスツリーまたはソース ツリーと呼ばれます。 デフォルトでは、Cisco IOS ソフトウェアは、送信元から最初のデータ パケットを受信した時点で、ソース ツリーへの切り替えを行います。

次に、共有ツリーからソース ツリーに切り替わるプロセスの詳細を示します。

1. 受信側がグループに加入します。リーフ スイッチ C が RP に join メッセージを送信します。
2. RP がスイッチ C へのリンクを発信インターフェイス リストに登録します。
3. 送信元がデータを送信します。スイッチ A が register にデータをカプセル化し、それを RP に送信します。
4. RP が共有ツリーの下位方向のスイッチ C にデータを転送し、送信元に join メッセージを送信します。 この時点で、データはスイッチ C に 2 回（カプセル化された状態で 1 回、ネイティブの状態で 1 回）着信する可能性があります。
5. データがネイティブの（カプセル化されていない）状態で RP に着信すると、RP はスイッチ A に register-stop メッセージを送信します。
6. デフォルトでは、最初のデータ パケット受信時に、スイッチ C が Join メッセージを送信元に送信するよう要求します。
7. スイッチ C は、（S, G）でデータを受信すると、共有ツリーの上位方向にある送信元に prune メッセージを送信します。
8. RP が（S, G）の発信インターフェイスからスイッチ C へのリンクを削除します。
9. RP が送信元への prune メッセージをトリガーします。

送信元および RP に join および prune メッセージが送信されます。 これらのメッセージはホップバイホップで送信され、送信元または RP へのパス上にある各 PIM スイッチで処理されます。 register および register-stop メッセージは、ホップバイホップで送信されません。 これらのメッセージは、送信元に直接接続されている指定スイッチによって送信され、グループの RP によって受信されます。

Reverse Path Forwarding

Reverse Path Forwarding は、マルチキャスト データグラムの転送に使用されます。 これは、次のように機能します。

- スイッチで、送信元へのユニキャスト パケットの送信に使用しているインターフェイスでデータグラムを受信すると、パケットは RPF インターフェイスに着信しています。
- パケットが RPF インターフェイスに着信した場合、スイッチは、マルチキャスト ルーティング テーブルエントリの発信インターフェイス リストに存在するインターフェイスにパケットを転送します。

- パケットがRPFインターフェイスに着信しない場合、パケットはループを回避するためにサイレントにドロップされています。

PIM では、送信元ツリーと RP をルートとする共有ツリーの両方を使用してデータグラムを転送します。RPF チェックは、次のようにそれぞれ異なる方法で実行されます。

- PIM スイッチが送信元ツリー ステートである場合（つまり、（S, G）エントリがマルチキャスト ルーティング テーブル内にある場合）、マルチキャスト パケットの送信元の IPv6 アドレスに対して RPF チェックが実行されます。
- PIM スイッチが共有ツリー ステートである場合（および送信元ツリー ステートが明示されていない場合）、（メンバがグループに加入している場合は既知である）RPのアドレスに対して RPF チェックが実行されます。

空間モード PIM では、RPF ルックアップ機能を使用して、join および prune の送信先を決定します。 （S, G）join（送信元ツリー ステート）は送信元に向けて送信されます。 （*, G）join（共有ツリー ステート）は RP に向けて送信されます。

ルーティング可能アドレスの hello オプション

IPv6 内部ゲートウェイ プロトコルを使用してユニキャスト ルーティング テーブルを構築する場合、アップストリーム スイッチ アドレスを検出するための手順では、PIM ネイバーとネクスト ホップ スイッチが同じスイッチを表しているかぎり、これらのアドレスは常に同じであるものと想定されます。 ただし、スイッチがリンク上に複数のアドレスを持つ場合は、このことが当てはまるとはかぎりません。

この状況は IPv6 において、2 つの一般的な状況で発生することがあります。 1 つめの状況は、ユニキャスト ルーティング テーブルが IPv6 内部ゲートウェイ プロトコル（マルチキャスト BGP など）によって構築されない場合に発生します。 2 つめの状況は、RP のアドレスがダウンストリーム スイッチとサブネット プレフィックスを共有している場合に発生します（RP スイッチ アドレスはドメインワイドにする必要があるため、リンクローカル アドレスにはできないことに注意してください）。

ルーティング可能アドレスの hello オプションによって、PIM プロトコルでこのような状況を回避できます。このためには、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージ オプションを追加します。 PIM スイッチが何らかのアドレスのアップストリーム スイッチを検出すると、RPF 計算の結果は、PIM ネイバーのアドレス自体に加えて、このオプションのアドレスとも比較されます。 このオプションにはそのリンク上の PIM スイッチの考えられるアドレスがすべて含まれているため、対象の PIM スイッチがこのオプションをサポートしている場合、常に RPF 計算の結果が含まれます。

PIM メッセージにサイズ制限があることと、ルーティング可能アドレスの hello オプションが単一の PIM hello メッセージ内に収まる必要があるため、インターフェイスで設定できるアドレスの制限は 16 個になっています。

双方向 PIM

双方向 PIM により、マルチキャスト スイッチは、PIM-SM の単方向共有ツリーと比較して、保持するステート情報を減らすことができます。 双方向共有ツリーは、データを送信元からランデブー ポイント アドレス（RPA）に伝送し、それらを RPA から受信側に配布します。 PIM-SM とは異なり、双方向 PIM は送信元ツリーへの切り替えは実行しません。また、送信元から RP へのデータの登録カプセル化は行われません。

指定された単一のフォワーダ（DF）が、双方向 PIM ドメイン内のすべてのリンク（マルチアクセスおよびポイントツーポイント リンクを含む）の各 RPA 用に存在しています。 唯一の例外は、DF が存在しない RPL です。 DF は、MRIB が提供するメトリックとの比較で決定される、RPA への最適なルートを持つリンク上のスイッチです。 指定された RPA の DF は、リンクにダウンストリーム トラフィックを転送し、リンクからのアップストリーム トラフィックをランデブー ポイント リンク（RPL）に転送します。 DF は、RPA にマップするすべての双方向グループに対してこの機能を実行します。 また、リンク上の DF は、リンク上のダウンストリーム スイッチからの Join メッセージを処理するとともに、MLD などのローカル メンバーシップ メカニズムによって検出されたローカル受信者にパケットが転送されることを保証します。

双方向 PIM は、中レートまたは低レートの送信元が多数存在する場合に役立ちます。 ただし、双方向共有ツリーの遅延特性は、PIM-SM で構築された送信元ツリーよりもさらに劣る可能性があります（トポロジに依存）。

IPv6 では、双方向 RP のスタティック設定だけがサポートされています。

スタティック mroute

IPv6 スタティック mroute は、RPF チェックを変化させるために使用する IPv4 スタティック mroute とほぼ同様に動作します。 IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、RPF チェックに対するスタティック ルート サポートを拡張することによって実装されます。 スタティック mroute では、等コスト マルチパス mroute がサポートされています。また、ユニキャスト専用スタティック ルートもサポートされています。

MRIB

マルチキャストルーティング情報ベース（MRIB）は、マルチキャスト ルーティング プロトコル（ルーティング クライアント）によってインスタンス化されるマルチキャスト ルーティング エントリのプロトコル非依存リポジトリです。 その主要機能は、ルーティング プロトコルとマルチキャスト転送情報ベース（MFIB）間の非依存性を実現することです。 また、クライアント間の調整および通信ポイントとしても機能します。

ルーティング クライアントは、MRIB が提供するサービスを使用して、ルーティング エントリをインスタンス化し、他のクライアントによってルーティング エントリに加えられた変更を取得します。 MRIB では、ルーティング クライアント以外に、転送クライアント（MFIB インスタンス）や特別なクライアント（MLD など）も扱われます。 MFIB は、MRIB からその転送エントリを取得し、パケットの受信に関連するイベントについて MRIB に通知します。 これらの通知は、ルーティング クライアントによって明示的に要求されることも、MFIB によって自発的に生成されることもあります。

MRIB のもう 1 つの重要な機能は、同じマルチキャスト セッション内でマルチキャスト接続を確立する際に、複数のルーティング クライアントの調整を可能にすることです。 また、MRIB では、MLD とルーティング プロトコル間の調整も可能です。

MFIB

MFIB は、IPv6 ソフトウェア用のプラットフォーム非依存およびルーティング プロトコル非依存ライブラリです。 その主な目的は、転送テーブルが変更されたときに、Cisco IOS プラットフォームに、IPv6 マルチキャスト転送テーブルおよび通知を読み取るインターフェイスを提供することです。 MFIB が提供する情報には、明確に定義された転送セマンティクスが含まれています。この情報は、プラットフォームが特定のハードウェアまたはソフトウェア転送メカニズムに容易に変換できる設計になっています。

ネットワーク内でルーティングまたはトポロジが変更されると、IPv6 ルーティング テーブルがアップデートされ、これらの変更が MFIB に反映されます。 MFIB は、IPv6 ルーティング テーブル内の情報に基づいて、ネクストホップ アドレス情報を管理します。 MFIB エントリとルーティング テーブル エントリの間には 1 対 1 の相互関係があるため、MFIB には既知のすべてのルートが含まれ、高速スイッチングや最適スイッチングなどのスイッチング パスに関連付けられているルート キャッシュ管理の必要がなくなります。

IPv6 マルチキャスト VRF Lite

IPv6 マルチキャスト VRF Lite 機能は、複数の仮想ルーティングおよび転送（VRF）コンテキストに対する IPv6 マルチキャスト サポートを提供します。 これらの VRF のスコープは、VRF が定義されているスイッチに制限されています。

この機能により、別の VRF に属するデバイス間の通信は、明示的に設定されていない限り許可されないため、より高いレベルのセキュリティでのルーティングと転送の切り分けができます。 IPv6 マルチキャスト VRF Lite 機能は、特定の VRF に属するトラフィックの管理とトラブルシューティングを容易にします。

IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング

統合 MFIB は、IPv6 マルチキャストでの PIM-SM および PIM-SSM に対するファスト スイッチングおよびプロセス スイッチングの両サポートを提供するために使用されます。 プロセス スイッチングでは、の が各パケットの調査、書き換え、および転送を行う必要があります。 最初にパケットが受信され、システム メモリにコピーされます。 次に、スイッチがルーティング テーブル内でレイヤ 3 ネットワーク アドレスを検索します。 そのあと、レイヤ 2 フレームがネクストホップの宛先アドレスで書き換えられ、発信インターフェイスに送信されます。 また、は、巡回冗長検査（CRC）も計算します。 このスイッチング方式は、IPv6 パケットをスイッチングする方式の中でスケーラビリティが最も低い方式です。

IPv6 マルチキャストの高速スイッチングを使用すると、スイッチは、プロセス スイッチングよりも高いパケット転送パフォーマンスを実現できます。 従来ルート キャッシュに格納される情報は、IPv6 マルチキャスト スイッチング用にいくつかのデータ構造に格納されます。 これらのデータ構造では、ルックアップが最適化され、パケット転送を効率的に行えるようになっています。

IPv6 マルチキャスト転送では、PIM プロトコル ロジックで許可されていれば、最初のパケットのファスト スイッチングが行われます。 IPv6 マルチキャストの高速スイッチングでは、MAC カプセル化ヘッダーが事前に計算されます。 IPv6 マルチキャストの高速スイッチングでは、MFIB を使用して、IPv6 送信先プレフィックス ベースのスイッチング判定が行われます。 IPv6 マルチキャストの高速スイッチングでは、MFIB に加えて、隣接関係テーブルを使用して、レイヤ 2 アドレッシング情報が付加されます。 隣接関係テーブルでは、すべての MFIB エントリのレイヤ 2 ネクストホップ アドレスが管理されます。

隣接が検出されると、隣接関係テーブルにそのデータが入力されます。 （ARP などを使用して）隣接エントリが作成されるたびに、その隣接ノードのリンク層ヘッダーが事前に計算され、隣接関係テーブルに格納されます。 ルートが決定されると、そのヘッダーはネクストホップおよび対応する隣接エントリを指します。 そのあと、そのヘッダーはパケット スイッチング時のカプセル化に使用されます。

ロード バランシングと冗長性の両方に対応するようにスイッチが設定されている場合など、ルートには送信先プレフィックスへの複数のパスが存在することがあります。 解決されたパスごとに、そのパスのネクストホップ インターフェイスに対応する隣接へのポインタが追加されます。 このメカニズムは、複数のパスでのロード バランシングに使用されます。

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 機能では、マルチプロトコル BGP for IPv6 拡張を提供し、IPv4 BGP と同じ機能と機能性をサポートします。 マルチキャスト BGP に対する IPv6 拡張には、IPv6 マルチキャスト アドレス ファミリ、ネットワーク層到達可能性情報（NLRI）、および IPv6 アドレスを使用するネクストホップ（宛先へのパス内の次のスイッチ）属性のサポートが含まれています。

マルチキャスト BGP は、ドメイン間 IPv6 マルチキャストの配布を可能にする、拡張された BGP です。 マルチプロトコル BGP では、複数のネットワーク層プロトコル アドレス ファミリ（IPv6 アドレス ファミリなど）および IPv6 マルチキャスト ルートに関するルーティング情報を伝送します。 IPv6 マルチキャスト アドレス ファミリには、IPv6 PIM プロトコルによる RPF ルックアップに使用される複数のルートが含まれており、マルチキャスト BGP IPv6 は、同じドメイン間転送を提供します。 ユニキャスト BGP が学習したルートは IPv6 マルチキャストには使用されないため、ユーザは、BGP で IPv6 マルチキャストを使用する場合は、マルチプロトコル BGP for IPv6 マルチキャストを使用する必要があります。

マルチキャスト BGP 機能は、個別のアドレス ファミリ コンテキストを介して提供されます。 Subsequent Address Family Identifier（SAFI）では、属性で伝送されるネットワーク層到達可能性情報のタイプに関する情報を提供します。 マルチプロトコル BGP ユニキャストでは SAFI 1 メッセージを使用し、マルチプロトコル BGP マルチキャストでは SAFI 2 メッセージを使用します。 SAFI 1 メッセージは、ルートは IP ユニキャストだけに使用でき、IP マルチキャストには使用できないことを示します。 この機能があるため、IPv6 ユニキャスト RIB 内の BGP ルートは、IPv6 マルチキャスト RPF ルックアップでは無視される必要があります。

IPv6 マルチキャスト RPF ルックアップを使用して、異なるポリシーおよびトポロジ（IPv6 ユニキャストとマルチキャストなど）を設定するよう、個別の BGP ルーティング テーブルが維持されています。 マルチキャスト RPF ルックアップは、IP ユニキャスト ルート ルックアップと非常によく似ています。

IPv6 マルチキャスト BGP テーブルと関連付けられている MRIB はありません。 ただし、必要な場合、IPv6 マルチキャスト BGP は、ユニキャスト IPv6 RIB で動作します。 マルチキャスト BGP では、IPv6 ユニキャスト RIB へのルートの挿入や更新は行いません。

IPv6 マルチキャストでの NSF と SSO のサポート

IPv6 マルチキャストでは、ノンストップ フォワーディング（NSF）およびステートフル スイッチオーバー（SSO）がサポートされています。

IPv6 マルチキャストの帯域幅ベースの CAC

IPv6 マルチキャストの帯域幅ベースのコール アドミッション制御（CAC）機能は、コスト乗数を使用してインターフェイス単位の mroute ステート リミッタをカウントする手段を実装します。この機能を使用すると、マルチキャスト フローで異なる量の帯域幅が使用されるネットワーク環境で、インターフェイス単位の帯域幅ベースの CAC を提供できます。

この機能では、IPv6 マルチキャスト ステートを詳細に制限および考慮します。 この機能を設定すると、IPv6 マルチキャスト PIM トポロジの着信インターフェイスまたは発信インターフェイスとして使用できる回数にインターフェイスを制限できます。

この機能を使用すると、スイッチ管理者はアクセス リストと一致するステートに対してグローバル制限コスト コマンドを設定して、インターフェイス制限に対してこのようなステートを考慮するときに使用するコスト乗数を指定できます。 この機能では、異なる帯域幅要件に応じてコスト乗数を適切に調整することによって、帯域幅ベースのローカル CAC ポリシーを柔軟に実装できます。

IPv6 マルチキャストの実装

IPv6 マルチキャスト ルーティングのイネーブル化

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 multicast-routing** 例： `Switch (config)# ipv6 multicast-routing`	すべての IPv6 対応インターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルになっているすべてのスイッチ インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD プロトコルのカスタマイズおよび確認

インターフェイスでの MLD のカスタマイズおよび確認

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***type number* 例： `Switch(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 3	**ipv6 mld join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]} 例： `Switch (config-if) # ipv6 mld join-group FF04::10`	指定したグループおよび送信元に対して MLD レポートを設定します。
ステップ 4	**ipv6 mld access-group***access-list-name* 例： `Switch (config-if) # ipv6 access-list acc-grp-1`	ユーザに IPv6 マルチキャストの受信側アクセス コントロールの実行を許可します。
ステップ 5	**ipv6 mld static-group** [*group-address*] [**include** | **exclude**] {*source-address* | source-list [*acl*]} 例： `Switch (config-if) # ipv6 mld static-group ff04::10 include 100::1`	指定したインターフェイスにマルチキャスト グループのトラフィックをスタティックに転送し、MLD ジョイナがインターフェイスに存在するかのようにインターフェイスが動作するようにします。

	コマンドまたはアクション	目的
ステップ 6	**ipv6 mld query-max-response-time***seconds* 例： `Switch (config-if) # ipv6 mld query-max-response-time 20`	MLD キューにアドバタイズされる最大応答時間を設定します。
ステップ 7	**ipv6 mld query-timeout***seconds* 例： `Switch (config-if) # ipv6 mld query-timeout 130`	スイッチがインターフェイスのクエリアとして引き継ぐまでのタイムアウト値を設定します。
ステップ 8	**exit** 例： `Switch (config-if) # exit`	このコマンドを2回入力して、インターフェイスコンフィギュレーションモードを終了し、特権EXECモードを開始します。
ステップ 9	**show ipv6 mldgroups [link-local]** [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**] 例： `Switch # show ipv6 mld groups GigabitEthernet 1/0/1`	スイッチに直接接続されており、MLD を介して学習したマルチキャスト グループを表示します。
ステップ 10	**show ipv6 mld groups summary** 例： `Switch # show ipv6 mld groups summary`	MLD キャッシュに存在する (*, G) および (S, G) メンバーシップ レポートの番号を表示します。
ステップ 11	**show ipv6 mldinterface** [*type number*] 例： `Switch # show ipv6 mld interface GigabitEthernet 1/0/1`	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 12	**debug ipv6 mld** [*group-name* | *group-address* | *interface-type*] 例： `Switch # debug ipv6 mld`	MLD プロトコル アクティビティに対するデバッグをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 13	**debug ipv6 mld explicit** [*group-name* | *group-address* 例： `Switch # debug ipv6 mld explicit`	ホストの明示的トラッキングに関連する情報を表示します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

MLD グループ制限の実装

インターフェイス単位の MLD 制限とグローバル MLD 制限は相互に独立して機能します。 インターフェイス単位の MLD 制限とグローバル MLD 制限の両方を同じスイッチで設定できます。 MLD 制限の数は、グローバルの場合もインターフェイス単位の場合も、デフォルトでは設定されません。ユーザが制限を設定する必要があります。 インターフェイス単位のステート制限またはグローバル ステート制限を超えるメンバーシップ レポートは無視されます。

MLD グループ制限のグローバルな実装

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6 mld** [*vrf vrf-name*] **state-limit***number*
4. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch# enable`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 mld** [*vrf vrf-name*] **state-limit***number* 例： `Switch(config)# ipv6 mld state-limit 300`	MLD ステートの数をグローバルに制限します。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD グループ制限のインターフェイス単位での実装

手順の概要

1. **enable**
2. **configureterminal**
3. **interface type***number*
4. **ipv6 mld limit***number* [**except**]*access-list*
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch# enable`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface type***number* 例： `Switch(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 mld limit***number* [**except**]*access-list* 例： `Switch(config-if)# ipv6 mld limit 100`	MLD ステートの数をインターフェイス単位で制限します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

受信側の明示的トラッキングによってホストの動作を追跡するための設定

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***type number* 例： `Switch(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 3	**ipv6 mld explicit-tracking***access-list-name* 例： `Switch(config-if)# ipv6 mld explicit-tracking list1`	ホストの明示的トラッキングをイネーブルにします。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

マルチキャスト ユーザ認証およびプロファイル サポートの設定

マルチキャストユーザ認証およびプロファイルサポートを設定する前に、次の制約事項を認識しておく必要があります。

- ポート、インターフェイス、VC、または VLAN ID がユーザまたは加入者アイデンティティになります。 ホスト名、ユーザ ID、またはパスワードを使用したユーザ アイデンティティはサポートされていません。
- IPv6 マルチキャストに対する AAA アクセス コントロールのイネーブル化
- 方式リストの指定およびマルチキャスト アカウンティングのイネーブル化
- スイッチでの未認証マルチキャスト トラフィック受信のディセーブル化
- MLD インターフェイスでの許可ステータスのリセット

IPv6 マルチキャストに対する *AAA* アクセス コントロールのイネーブル化

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA アクセス コントロール システムをイネーブルにします。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

方式リストの指定およびマルチキャスト アカウンティングのイネーブル化

次の作業では、AAA 認可およびアカウンティングに使用される方式リストを指定する方法、およびインターフェイス上の指定したグループまたはチャネルでマルチキャスト アカウンティングをイネーブルにする方法を示します。

特権 EXEC モードで次の手順を実行します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**aaa authorization multicast default** [*method3* | *method4*] 例： `Switch (config)# aaa authorization multicast default`	AAA 認可をイネーブルにし、IPv6 マルチキャスト ネットワークへのユーザアクセスを制限するパラメータを設定します。
ステップ 3	**aaa accounting multicast default** [**start-stop** | **stop- only** [**broadcast**] [*method1*] [*method2*] [*method3*] [*method2]* 例： `Switch (config)# aaa accounting multicast default`	課金、または RADIUS を使用する際のセキュリティのために、IPv6 マルチキャスト サービスの AAA アカウンティングをイネーブルにします。
ステップ 4	**interface** *type number* 例： `Switch (config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**ipv6 multicast aaa account receive access-list-name** *access-list-name*[**throttle***throttle-number*] 例： `Switch (config-if)# ipv6 multicast aaa account receive list1`	指定したグループまたはチャネルで AAA アカウンティング cha**copy running-config startup-config**nnels をイネーブルにします。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチでの未認証マルチキャスト トラフィックの受信のディセーブル化

状況によっては、アクセスコントロールプロファイルに従って加入者の認証とチャネルの認可が行われていないかぎり、マルチキャスト トラフィックの受信を防止することが必要となる場合があります。 つまり、アクセス コントロール プロファイルで特に指定がなければ、トラフィックを完全になくす必要があります。

未認証グループまたは未認可チャネルからマルチキャスト トラフィックをスイッチが受信しないようにするには、次の作業を実行します。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 multicast** [vrf*vrf-name*] **group-range** [*access-list-name* 例： `Switch (config)# ipv6 multicast group-range`	スイッチのすべてのインターフェイスで未認可グループまたはチャネルのマルチキャスト プロトコル アクションおよびトラフィック転送をディセーブルにします。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 での MLD プロキシのイネーブル化

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld host-proxy** [*group-acl*] 例： `Switch (config)# ipv6 mld host-proxy proxy-group`	MLD プロキシ機能をイネーブルにします。
ステップ 3	**ipv6 mld host-proxy interface**[*group-acl*] 例： `Switch (config)# ipv6 mld host-proxy interface Ethernet 0/0`	RP 上の指定したインターフェイス上で MLD プロキシ機能をイネーブルにします。
ステップ 4	**show ipv6 mld host-proxy**[*interface-type interface-number*] **group** [*group-address*]]	IPv6 MLD ホスト プロキシ情報を表示します。

	コマンドまたはアクション	目的
	例： `Switch (config)# show ipv6 mld host-proxy Ethernet0/0`	
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD インターフェイスでの許可ステータスのリセット

インターフェイスを指定しない場合は、すべての MLD インターフェイスで認可がリセットされます。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 multicast aaa authorization** [*interface-type interface-number*] 例： `Switch # clear ipv6 multicast aaa authorization FastEthernet 1/0`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD トラフィック カウンタのリセット

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mldtraffic** 例： `Switch # clear ipv6 mld traffic`	すべての MLD トラフィック カウンタをリセットします。

	コマンドまたはアクション	目的
ステップ 2	**show ipv6 mldtraffic** 例： `Switch # show ipv6 mld traffic`	MLD トラフィック カウンタを表示します。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD インターフェイス カウンタのクリア

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mldcounters***interface-type* 例： `Switch # clear ipv6 mld counters Ethernet1/0`	MLD インターフェイス カウンタをクリアします。
ステップ 2	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM の設定

ここでは、PIM の設定方法について説明します。

PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 pim **rp-address***ipv6-address*[*group-access-list*] 例： `Switch (config) # ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C acc-grp-1`	特定のグループ範囲の PIM RP のアドレスを設定します。
ステップ 3	**exit** 例： `Switch (config) # exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 4	**show ipv6 piminterface** [state-on] [**state-off**] [*type-number*] 例： `Switch # show ipv6 pim interface`	PIM に対して設定されたインターフェイスに関する情報を表示します。
ステップ 5	**show ipv6 pimgroup-map** [*group-name* | group-address] | [*group-range* | *group-mask*] [**info-source {bsr** | **default** | **embedded-rp** | **static**}] 例： `Switch # show ipv6 pim group-map`	IPv6 マルチキャスト グループ マッピング テーブルを表示します。
ステップ 6	**show ipv6 pimneighbor** [**detail**] [*interface-type interface-number* | **count**] 例： `Switch # show ipv6 pim neighbor`	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。
ステップ 7	**show ipv6 pimrange-list** [**config**] [*rp-address* | *rp-name*] 例： `Switch # show ipv6 pim range-list`	IPv6 マルチキャスト範囲リストに関する情報を表示します。
ステップ 8	**show ipv6 pimtunnel** [*interface-type interface-number*] 例： `Switch # show ipv6 pim tunnel`	インターフェイス上の PIM レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	**debug ipv6 pim** [*group-name* | *group-address* | **interface***interface-type* | **bsr** | **group** | **mvpn** | **neighbor**] 例： `Switch # debug ipv6 pim`	PIM プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM オプションの設定

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pimspt-threshold infinity** [**group-list***access-list-name*] 例： `Switch (config) # ipv6 pim spt-threshold infinity group-list acc-grp-1`	PIM リーフ スイッチが指定したグループの SPT に加入するタイミングを設定します。
ステップ 3	**ipv6 pimaccept-register** {**list***access-list* | **route-map***map-name*} 例： `Switch (config) # ipv6 pim accept-register route-map reg-filter`	RP のレジスタを許可または拒否します。
ステップ 4	**interface***type number* 例： `Switch (config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイスコンフィギュレーションモードにします。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 pim dr-priority***value* 例： `Switch (config-if) # ipv6 pim dr-priority 3`	PIM スイッチの DR プライオリティを設定します。
ステップ 6	**ipv6 pim hello-interval***seconds* 例： `Switch (config-if) # ipv6 pim hello-interval 45`	インターフェイスにおける PIM hello メッセージの頻度を設定します。
ステップ 7	**ipv6 pim join-prune-interval***seconds* 例： `Switch (config-if) # ipv6 pim join-prune-interval 75`	指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。
ステップ 8	**exit** 例： `Switch (config-if) # exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 9	**ipv6 pimjoin-prune statistic** [*interface-type*] 例： `Switch (config-if) # show ipv6 pim join-prune statistic`	各インターフェイスの最後の集約パケットに関する平均 join-prune 集約を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

双方向 PIM の設定および双方向 PIM 情報の表示

特権 EXEC モードで次の手順を実行します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list]* [**bidir**] 例： `Switch (config) # ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C bidir`	特定のグループ範囲の PIM RP のアドレスを設定します。 bidir キーワードを使用すると、そのグループ範囲が双方向共有ツリー転送に使用されるようになります。
ステップ 3	**exit** 例： `Switch (config-if) # exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 4	**show ipv6 pim** [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*] 例： `Switch (config) # show ipv6 pim df`	RP の各インターフェイスの Designated Forwarder（DF）選択ステートを表示します。
ステップ 5	**show ipv6 pim** [**vrf** *vrf-name*] **df winner** [*interface-type interface-number*] [*rp-address*] 例： `Switch (config-if) # show ipv6 pim df winner ethernet 1/0 200::1`	各 RP の各インターフェイスの DF 選択ウィナーを表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM トラフィック カウンタのリセット

PIM が誤動作する場合、または予想される PIM パケット数が送受信されていることを確認するために、ユーザは PIM トラフィック カウンタをクリアできます。 トラフィック カウンタがクリアされたら、ユーザは show ipv6 pim traffic コマンドを入力して、PIM が正しく機能していること、および PIM パケットが正しく送受信されていることを確認できます。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 pimtraffic** 例： `Switch # clear ipv6 pim traffic`	PIM トラフィック カウンタをリセットします。
ステップ 2	**show ipv6 pimtraffic** 例： `Switch # show ipv6 pim traffic`	PIM トラフィック カウンタを表示します。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット

MRIB を使用するのに設定は不要です。 ただし、特定の状況においては、ユーザは PIM トポロジ テーブルをクリアして MRIB 接続をリセットし、MRIB 情報を確認する必要がある場合があります。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 pimtopology** [*group-name* | *group-address*] 例： `Switch # clear ipv6 pim topology FF04::10`	PIM トポロジ テーブルをクリアします。
ステップ 2	**show ipv6 mribclient** [**filter**] [**name** {*client-name* | *client-name*: **client-id**}] 例： `Switch # show ipv6 mrib client`	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 3	**show ipv6 mribroute** {**link-local** | **summary** | [*sourceaddress-or-name* | *] [*groupname-or-address*[*prefix-length*]]]	MRIB ルート情報を表示します。

	コマンドまたはアクション	目的
	例： `Switch # show ipv6 mrib route`	
ステップ 4	**show ipv6 pimtopology** [*groupname-or-address* [*sourceaddress-or-name*] | **link-local** | **route-count** [**detail**]] 例： `Switch # show ipv6 pim topology`	特定のグループまたはすべてのグループの PIM トポロジ テーブル情報を表示します。
ステップ 5	**debug ipv6 mribclient** 例： `Switch # debug ipv6 mrib client`	MRIB クライアント管理アクティビティに対するデバッグをイネーブルにします。
ステップ 6	**debug ipv6 mribio** 例： `Switch # debug ipv6 mrib io`	MRIB I/O イベントに対するデバッグをイネーブルにします。
ステップ 7	**debug ipv6 mrib proxy** 例： `Switch # debug ipv6 mrib proxy`	分散型スイッチプラットフォームにおけるスイッチプロセッサとラインカード間の MRIB プロキシアクティビティに対するデバッグをイネーブルにします。
ステップ 8	**debug ipv6 mribroute** [*group-name* | *group-address*] 例： `Switch # debug ipv6 mrib route`	MRIB ルーティング エントリ関連のアクティビティに関する情報を表示します。
ステップ 9	**debug ipv6 mribtable** 例： `Switch # debug ipv6 mrib table`	MRIBテーブル管理アクティビティに対するデバッグをイネーブルにします。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BSR の設定

ここでの作業について、以下に説明します。

BSR の設定および BSR 情報の確認

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pimbsr candidate bsr***ipv6-address*[*hash-mask-length*] [**priority** *priority-value*] 例： `Switch (config) # ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10`	候補 BSR になるようにスイッチを設定します。
ステップ 3	**interface** *type number* 例： `Switch (config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 pim bsr border** 例： `Switch (config-if) # ipv6 pim bsr border`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**exit** 例： `Switch (config-if) # exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 6	**show ipv6 pim** bsr {**election** | **rp-cache** | **candidate-rp**} 例： `Switch (config-if) # show ipv6 pim bsr election`	PIM BSR プロトコル処理に関連する情報を表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BSR への PIM RP アドバタイズメントの送信

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pim bsr candidate rp***ipv6-address* [**group-list***access-list-name*] [**priority***priority-value*] [**interval** seconds] 例： `Switch(config) # ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0`	BSR に PIM RP アドバタイズメントを送信します。
ステップ 3	**interface***type number* 例： `Switch(config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 pim bsr border** 例： `Switch(config-if) # ipv6 pim bsr border`	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

限定スコープ ゾーン内で BSR を使用できるようにするための設定

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pim bsr candidate rp***ipv6-address* [*hash-mask-length*] [**priority** priority-value]	候補 BSR になるようにスイッチを設定します。

	コマンドまたはアクション	目的
	例： `Switch(config) # ipv6 pim bsr candidate bsr 2001:DB8:1:1:4`	
ステップ 3	**ipv6 pim bsr candidate rp***ipv6-address* [**group-list***access-list-name*] [**priority***priority-value*] [**interval** seconds] 例： `Switch(config) # ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6`	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。
ステップ 4	**interface***type number* 例： `Switch(config-if) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイスコンフィギュレーション モードにします。
ステップ 5	**ipv6 multicast boundary scope***scope-value* 例： `Switch(config-if) # ipv6 multicast boundary scope 6`	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定

IPv6 BSR スイッチは、スコープと RP のマッピングを候補 RP メッセージから学習するのではなく、直接アナウンスするようにスタティックに設定できます。 ユーザは、スコープと RP のマッピングをアナウンスするように BSR スイッチを設定して、BSR をサポートしていない RP がその BSR にインポートされるように設定できます。 この機能をイネーブルにすると、ローカルの候補 BSR スイッチの既知のリモート RP が、企業の BSR ドメインの外部に配置されている RP を学習できるようになります。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 pim bsr announced rp***ipv6-address* [**group-list***access-list-name*] [**priority***priority-value*] 例： `Switch(config)# ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0`	指定した候補 RP の BSR からスコープと RP のマッピングを直接アナウンスします。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピングの設定

SSM マッピング機能をイネーブルにすると、DNS ベースの SSM マッピングが自動的にイネーブルになります。つまり、スイッチは、マルチキャスト MLD バージョン 1 レポートの送信元を DNS サーバから検索するようになります。

スイッチ設定に応じて、DNS ベースのマッピングまたはスタティック SSM マッピングのいずれかを使用できます。 スタティック SSM マッピングを使用する場合は、複数のスタティック SSM マッピングを設定できます。 複数のスタティック SSM マッピングを設定すると、一致するすべてのアクセス リストの送信元アドレスが使用されるようになります。

（注） DNS ベースの SSM マッピングを使用するには、スイッチは正しく設定されている DNS サーバを少なくとも 1 つ見つける必要があります。スイッチは、その DNS サーバに直接接続される可能性があります。

特権 EXEC モードで次の手順を実行します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ipv6 mldssm-map enable** 例： `Switch(config) # ipv6 mld ssm-map enable`	設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。
ステップ 3	**no ipv6 mldssm-map query dns** 例： `Switch(config) # no ipv6 mld ssm-map query dns`	DNS ベースの SSM マッピングをディセーブルにします。
ステップ 4	**ipv6 mldssm-map static***access-listsource-address* 例： `Switch(config-if) # ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1`	スタティック SSM マッピングを設定します。
ステップ 5	**exit** 例： `Switch(config-if) # exit`	グローバルコンフィギュレーションモードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 6	**show ipv6 mldssm-map** [*source-address*] 例： `Switch(config-if) # show ipv6 mld ssm-map`	SSM マッピング情報を表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

スタティック mroute の設定

IPv6 のスタティック マルチキャスト ルート（mroute）は、IPv6 スタティック ルートの拡張として実装できます。スイッチを設定する際には、ユニキャストルーティング専用としてスタティック ルートを使用するか、マルチキャスト RPF 選択専用としてスタティック マルチキャスト ルートを使用するか、またはユニキャストルーティングとマルチキャストRPF選択の両方にスタティック ルートを使用するように設定できます。

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 route** {*ipv6-prefix / prefix-length ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | *unicast* | *multicast*] [**tag***tag*] 例： `Switch (config) # ipv6 route 2001:DB8::/64 6::6 100`	スタティック IPv6 ルートを確立します。 この例は、ユニキャスト ルーティングとマルチキャスト RPF 選択の両方に使用されるスタティック ルートを示しています。
ステップ 3	**exit** 例： `Switch # exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 4	**show ipv6 mroute** [link-local | [*group-name* | *group-address* [*source-address* | *source-name*]] [**summary**] [**count**] 例： `Switch # show ipv6 mroute ff07::1`	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 5	**show ipv6 mroute** [**link-local** | *group-name* | *group-address*] **active** [*kbps*] 例： `Switch (config-if) # show ipv6 mroute active`	スイッチ上のアクティブなマルチキャスト ストリームを表示します。
ステップ 6	**show ipv6 rpf** [*ipv6-prefix*] 例： `Switch (config-if) #  show ipv6 rpf 2001::1:1:2`	特定のユニキャスト ホスト アドレスおよびプレフィックスの RPF 情報を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 マルチキャストでの MFIB の使用

IPv6 マルチキャスト ルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。

IPv6 マルチキャストでの MFIB の動作の確認

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 mfib** [**link-local** | **verbose** | *group-address-name* | *ipv6-prefix / prefix-length* | *source-address-name* | **count** | **interface** | **status** | **summary**] 例： `Switch # show ipv6 mfib`	IPv6 MFIB での転送エントリおよびインターフェイスを表示します。
ステップ 2	**show ipv6 mfib** [all | linkscope | group-name | group-address [source-name | source-address]] **count** 例： `Switch # show ipv6 mfib ff07::1`	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 3	**show ipv6 mfib interface** 例： `Switch # show ipv6 mfib interface`	IPv6 マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示します。
ステップ 4	**show ipv6 mfib status** 例： `Switch # show ipv6 mfib status`	一般的な MFIB 設定と動作ステータスを表示します。
ステップ 5	**show ipv6 mfibsummary** 例： `Switch # show ipv6 mfib summary`	IPv6 MFIB エントリおよびインターフェイスの数に関するサマリー情報を表示します。
ステップ 6	**debug ipv6 mfib** [*group-name* | *group-address*] [**adjacency** | **db** | **fs** | **init** | **interface** | **mrib** [**detail**] | **nat** | **pak** | **platform** | **ppr** | **ps** | **signal** | **table**] 例： `Switch # debug ipv6 mfib FF04::10 pak`	IPv6 MFIB に対するデバッグ出力をイネーブルにします。

MFIB トラフィック カウンタのリセット

特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mfibcounters** [*group-name* | **group-address** [*source-address* | *source-name*]] 例： `Switch # clear ipv6 mfib counters FF04::10`	アクティブなすべての MFIB トラフィック カウンタをリセットします。

第 III 部

レイヤ 2

- IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定，221 ページ
- スパニングツリー プロトコルの設定，253 ページ
- 複数のスパニング ツリー プロトコルの設定，283 ページ
- オプションのスパニングツリー機能の設定，327 ページ
- 双方向フォワーディング検出の設定，353 ページ
- EtherChannel の設定，385 ページ
- リンクステート トラッキングの設定，415 ページ
- Resilient Ethernet Protocol の設定，423 ページ
- Flex Link および MAC アドレス テーブル移動更新機能の設定，443 ページ
- 単方向リンク検出の設定，465 ページ

第 11 章

IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定

- 機能情報の確認，221 ページ
- トンネリング設定の前提条件，221 ページ
- トンネリングについて，224 ページ
- トンネリングの設定方法，235 ページ
- IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定例，247 ページ
- トンネリング ステータスのモニタリング，250 ページ
- 次の作業，251 ページ

機能情報の確認

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

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

トンネリング設定の前提条件

ここでは、IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングを設定するための前提条件と考慮事項について説明します。

IEEE 802.1Q トンネリング

IEEE 802.1Q トンネリングはレイヤ 2 パケット スイッチングで適切に動作しますが、一部のレイヤ 2 機能およびレイヤ 3 スイッチングの間には非互換性があります。

- トンネル ポートはルーテッド ポートにできません。
- IEEE 802.1Q ポートを含む VLAN では IP ルーティングがサポートされません。 トンネル ポートから受信したパケットは、レイヤ 2 情報だけに基づいて転送されます。 トンネル ポートを含むスイッチ仮想インターフェイス（SVI）でルーティングがイネーブルになっている場合、トンネル ポートから受信したタグなし IP パケットは、スイッチに認識されてルーティングされます。 カスタマーは、ネイティブ VLAN を介してインターネットにアクセスできます。 このアクセスが必要ない場合は、トンネル ポートを含む VLAN で SVI を設定しないでください。
- フォールバック ブリッジングは、トンネル ポートでサポートされません。 トンネル ポートから受信したすべての IEEE 802.1Q タグ付きパケットは IP 以外のパケットとして扱われるので、トンネル ポートが設定されている VLAN でフォールバック ブリッジングがイネーブルである場合、IP パケットは VLAN を越えて不適切にブリッジングされます。 このため、トンネル ポートを含む VLAN ではフォールバック ブリッジングをイネーブルにしないでください。
- トンネル ポートでは IP アクセス コントロール リスト（ACL）がサポートされません。
- レイヤ 3 の Quality of Service（QoS）ACL およびレイヤ 3 情報に関連する他の QoS 機能は、トンネル ポートではサポートされていません。 MAC ベース QoS はトンネル ポートでサポートされます。
- IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、単一方向リンク検出（UDLD）は、IEEE 802.1Q トンネル ポートでサポートされます。
- トンネル ポートとトランク ポートで非対称リンクを手動で設定する必要があるので、ダイナミック トランキング プロトコル（DTP）には IEEE 802.1Q トンネリングとの互換性がありません。
- VLAN トランキング プロトコル（VTP）は、非対称リンクで接続されているデバイス間、またはトンネルを通して通信を行うデバイス間で動作しません。
- IEEE 802.1Q トンネル ポートでは、ループバック検出がサポートされます。
- IEEE 802.1Q トンネル ポートとしてポートを設定すると、スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）フィルタリングがインターフェイスで自動的にイネーブルになります。 Cisco Discovery Protocol（CDP）および Layer Link Discovery Protocol（LLDP）は、インターフェイスで自動的にディセーブルになります。

関連トピック

IEEE 802.1Q トンネリング ポートの設定, （235 ページ）

例：IEEE 802.1Q トンネリング ポートの設定, （247 ページ）

レイヤ 2 プロトコル トンネリング

- スイッチでは、CDP、STP（Multiple STP（MSTP）を含む）、VTP のトンネリングがサポートされます。 プロトコル トンネリングはデフォルトでディセーブルになっていますが、IEEE 802.1Q トンネル ポート、またはアクセス ポートでプロトコルごとにイネーブルにできます。
- スイッチでは、switchport モードが dynamic auto または dynamic desirable に設定されているポートにおいて、レイヤ 2 プロトコル トンネリングがサポートされません。
- DTP はレイヤ 2 プロトコル トンネリングと互換性がありません。
- サービスプロバイダー ネットワークのアウトバウンド側のエッジ スイッチでは、適切なレイヤ 2 プロトコル情報および MAC アドレス情報が復元され、同じメトロ VLAN のすべてのトンネル ポートおよびアクセス ポートにパケットが転送されます。
- サードパーティ ベンダー スイッチとの相互運用性のため、スイッチではレイヤ 2 プロトコルトンネル バイパス機能がサポートされます。 バイパス モードでは、プロトコル トンネリングの制御方法が異なるベンダー スイッチに制御 PDU が透過的に転送されます。 スイッチの入力ポートでレイヤ 2 プロトコル トンネリングがイネーブルになっている場合、出力トランク ポートは特殊なカプセル化を使用してトンネリング パケットを転送します。 出力トランク ポートでもレイヤ 2 プロトコル トンネリングをイネーブルにすると、この動作がバイパスされて、スイッチは加工や変更を行わずに制御 PDU を転送します。
- スイッチでは、ポイントツーポイント ネットワーク トポロジのエミュレートに関して PAgP、LACP、UDLD のトンネリングがサポートされます。 プロトコル トンネリングはデフォルトでディセーブルになっていますが、IEEE 802.1Q トンネル ポート、またはアクセス ポートでプロトコルごとにイネーブルにできます。
- PAgP トンネリングまたは LACP トンネリングの場合は、リンク障害検出を高速にするため、インターフェイスで UDLD もイネーブルにすることを推奨します。
- PAgP パケット、LACP パケット、UDLD パケットのレイヤ 2 プロトコル トンネリングでは、ループバック検出はサポートされません。
- IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- 独自の宛先 MAC アドレスでカプセル化された PDU が、レイヤ 2 トンネリングがイネーブルになっているトンネル ポートまたはアクセス ポートから受信される場合、トンネル ポートは、ループを防止するためにシャットダウンされます。 このポートは、プロトコル用に設定されたシャットダウンしきい値に達した場合にもシャットダウンされます。 **shutdown** コマンドに続けて **no shutdown** コマンドを入力すると、ポートを手動で再びイネーブルにできます。 errdisable recovery がイネーブルである場合は、指定された間隔で動作が再試行されます。
- カプセル化が解除された PDU だけがカスタマー ネットワークに転送されます。 サービスプロバイダーネットワーク上で動作しているスパニングツリーインスタンスでは、BPDU がトンネル ポートに転送されません。 CDP パケットはトンネル ポートから転送されません。

- インターフェイスでプロトコル トンネリングがイネーブルである場合は、カスタマー ネットワークによって生成された PDU 用に、プロトコルごとのシャットダウンしきい値やポートごとのシャットダウンしきい値を設定できます。 制限を超えると、ポートはシャットダウンされます。 QoS ACL およびポリシー マップをトンネル ポートで使用すると、BPDU レートを制限することもできます。
- インターフェイスでプロトコル トンネリングがイネーブルである場合は、カスタマー ネットワークによって生成された PDU 用に、プロトコルごとのドロップしきい値やポートごとのドロップしきい値を設定できます。 制限を超えると、ポートが PDU を受信するレートがドロップしきい値未満になるまで、ポートで PDU がドロップされます。
- トンネリングされた PDU（特に STP BPDU）は、カスタマーの仮想ネットワークが正しく動作するためにすべてのリモート サイトに配信される必要があるので、同じトンネル ポートから受信されるデータ パケットよりも PDU のプライオリティをサービスプロバイダー ネットワーク内で高くできます。 デフォルトの場合、PDU ではデータ パケットと同じ CoS 値が使用されます。

関連トピック

レイヤ 2 プロトコル トンネリングの設定, （238 ページ）

例：レイヤ 2 プロトコル トンネリングの設定, （248 ページ）

EtherChannel のレイヤ 2 トンネリング

EtherChannel の自動作成を容易にするためにレイヤ 2 ポイントツーポイント トンネリングを設定するには、サービスプロバイダー（SP）エッジ スイッチおよびカスタマー スイッチの両方を設定する必要があります。

関連トピック

レイヤ 2 プロトコル トンネリングの設定, （238 ページ）

例：レイヤ 2 プロトコル トンネリングの設定, （248 ページ）

トンネリングについて

IEEE 802.1Q およびレイヤ 2 プロトコルの概要

バーチャルプライベート ネットワーク（VPN）では、多くの場合にイーサネットベースの共有インフラストラクチャである企業規模の接続に、プライベート ネットワークと同じセキュリティ、プライオリティ、信頼性、管理の容易さが提供されます。 トンネリングは、サービス プロバイダーのネットワークを越えて複数のカスタマーのトラフィックを運び、その他のカスタマーのトラフィックに影響を与えずに、それぞれのカスタマーの VLAN およびレイヤ 2 プロトコルの設定を維持する必要があるサービス プロバイダー用に設計された機能です。

（注） IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングは Cisco Catalyst 3560-CX スイッチでのみサポートされています。

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

IEEE 802.1Q トンネリング

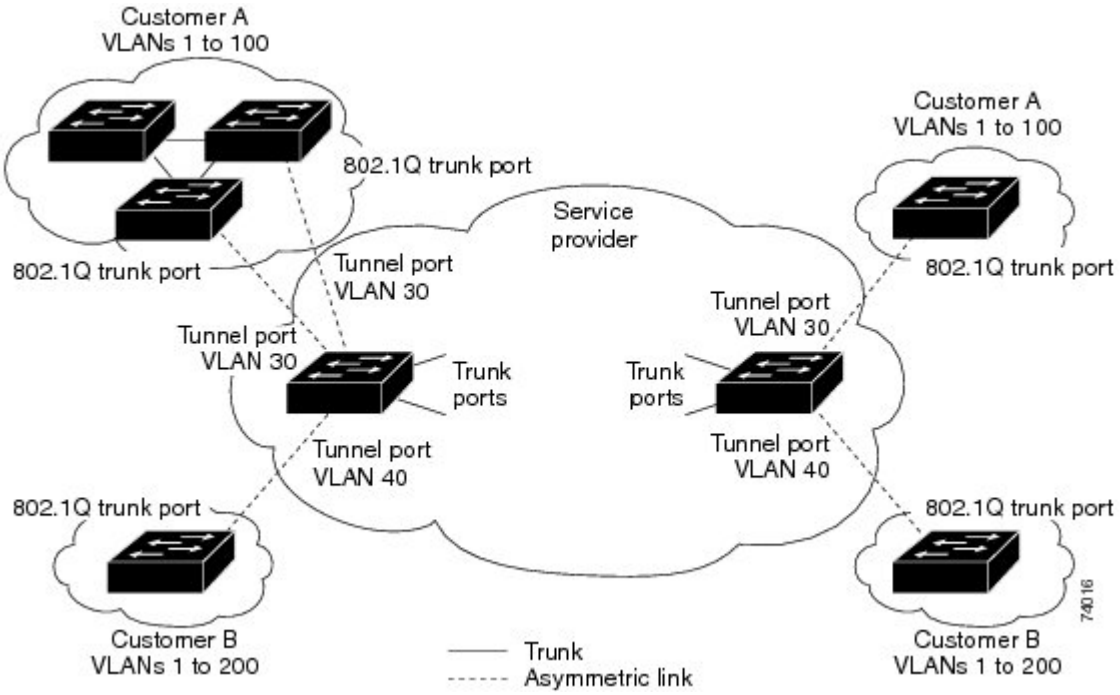
サービス プロバイダーのビジネス カスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。 同一サービスプロバイダー ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。 それぞれのカスタマーに VLAN ID の固有の範囲を割り当てると、カスタマーの設定が制限され、IEEE 802.1Q 仕様の VLAN 制限（4096）を簡単に超えてしまうことがあります。

サービス プロバイダーは、IEEE 802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含むカスタマーをサポートできます。 カスタマーの VLAN ID は、同一 VLAN にあるように見えても保護され、さまざまなカスタマーのトラフィックは、サービスプロバイダー ネットワーク内で区別されます。 IEEE 802.1Q トンネリングを使用する場合、VLAN-in-VLAN 階層構造およびタグ付きパケットへの再タグ付けによって、VLAN スペースを拡張できます。 IEEE 802.1Q トンネリングをサポートするように設定したポートは、トンネル ポートと呼ばれます。 トンネリングを設定する場合は、トンネリング専用の VLAN ID にトンネル ポートを割り当てます。 それぞれのカスタマーには別個のサービスプロバイダー VLAN ID が必要ですが、その VLAN ID ではすべてのカスタマーの VLAN がサポートされます。

適切な VLAN ID で通常どおりにタグ付けされたカスタマーのトラフィックは、カスタマー デバイスの IEEE 802.1Q トランク ポートからサービスプロバイダーのエッジ スイッチのトンネル ポートに発信されます。 カスタマー デバイスとエッジ スイッチ間のリンクは、片方が IEEE 802.1Q トランク ポートとして設定され、もう一方がトンネルポートとして設定されるため、非対称です。

それぞれのカスタマーに固有のアクセス VLAN ID には、トンネル ポート インターフェイスを割り当てます。

図 *3*：サービス プロバイダー ネットワークにおける *IEEE 802.1Q* トンネル ポート

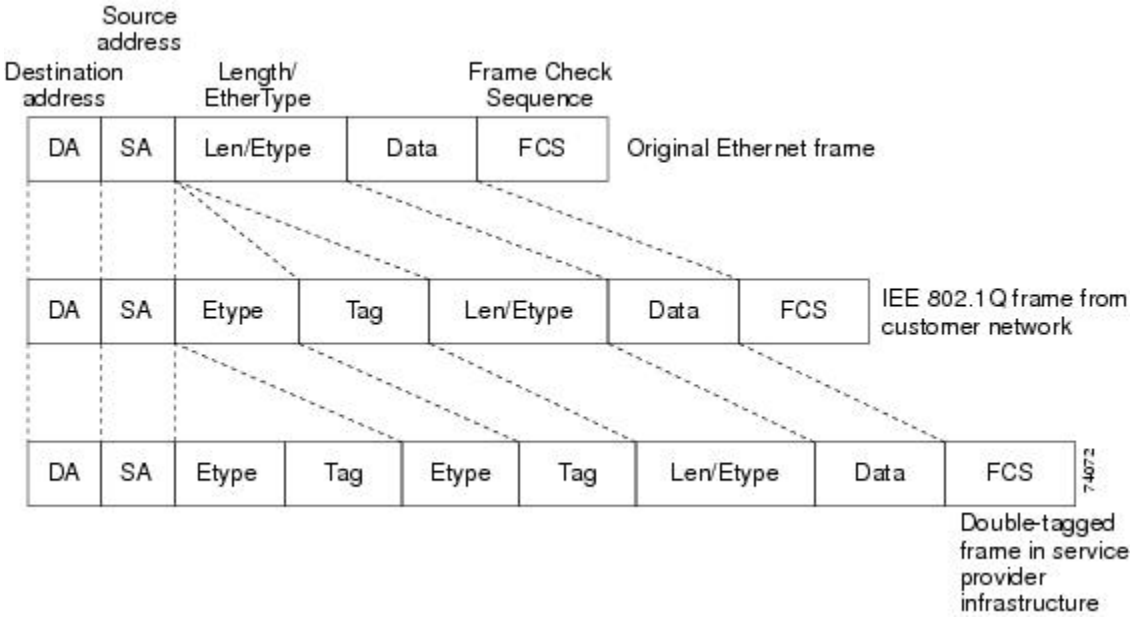


カスタマーのトランク ポートからサービス プロバイダーのエッジ スイッチのトンネル ポートに発信されるパケットには、通常、適切な VLAN ID とともに IEEE 802.1Q タグが付いています。これらのタグ付きパケットは、スイッチ内部ではそのまま保持され、トランク ポートを出てサービスプロバイダー ネットワークに入る時点で、カスタマーに固有の VLAN ID を含む、IEEE 802.1Q タグのもう 1 つのレイヤ（メトロ タグと呼ばれる）でカプセル化されます。 カスタマーの元の IEEE 802.1Q タグは、カプセル化されたパケット内で保護されます。 このため、サービスプロバイダー ネットワークに入るパケットには、カスタマーのアクセス VLAN ID を含む外部（メトロ）タグ、および着信トラフィックのものである内部 VLAN ID という、二重のタグが付きます。

二重タグ パケットがサービスプロバイダー コア スイッチの別のトランク ポートに入ると、スイッチがパケットを処理するときに外部タグが外されます。 パケットがその同じコア スイッチの別のトランク ポートを出るとき、同じメトロ タグがパケットに再び追加されます。

この図は、二重タグ付きパケットのタグ構造を示しています。

図 *4*：元の（通常）イーサネット パケット、*IEEE 802.1Q* イーサネット パケット、二重タグ イーサネット パケットの形式



パケットがサービスプロバイダー出力スイッチのトランク ポートに入ると、スイッチがパケットを内部処理する間に外部タグが再び外されます。 ただし、パケットがエッジスイッチのトンネル ポートからカスタマー ネットワークに送信されるとき、メトロ タグは追加されません。 パケットは通常の IEEE 802.1Q タグ フレームとして送信され、カスタマー ネットワーク内で元の VLAN 番号は保護されます。

上記のネットワークの図では、カスタマー A に VLAN 30、カスタマー B に VLAN 40 が割り当てられています。 エッジ スイッチのトンネル ポートに入る、IEEE 802.1Q タグが付いたパケットは、サービスプロバイダー ネットワークに入るとき、VLAN ID 30 または 40 を適切に含む外部タグ、および VLAN 100 などの元の VLAN 番号を含む内部タグが付いて二重タグになります。 カスタマー A とカスタマー B の両方が、それぞれのネットワーク内で VLAN 100 を含んでいても、外部タグが異なるので、サービスプロバイダーネットワーク内で区別されます。 それぞれのカスタマーは、その他のカスタマーが使用する VLAN 番号スペース、およびサービスプロバイダー ネットワークが使用する VLAN 番号スペースから独立した、独自の VLAN 番号スペースを制御します。

アウトバウンド トンネル ポートでは、カスタマーのネットワーク上の元の VLAN 番号が回復されます。 トンネリングとタグ付けを複数レベルにすることもできますが、このリリースのスイッチでは 1 レベルだけがサポートされます。

カスタマー ネットワークから発信されるトラフィックにタグ（ネイティブ VLAN フレーム）が付いていない場合、そのパケットのブリッジングまたはルーティングは通常パケットとして行われます。 エッジ スイッチのトンネル ポートを通ってサービスプロバイダー ネットワークに入るすべてのパケットは、タグが付いていないか、IEEE 802.1Q ヘッダーですでにタグが付いているかに関係なく、タグなしパケットとして扱われます。 パケットは、IEEE 802.1Q トランク ポートでサー

ビスプロバイダー ネットワークを通じて送信される場合、メトロ タグ VLAN ID（トンネル ポートのアクセス VLAN に設定）でカプセル化されます。 メトロ タグのプライオリティ フィールドは、トンネル ポートで設定されているインターフェイス サービス クラス（CoS）プライオリティに設定されます （設定されていない場合、デフォルトはゼロです）。

関連トピック

IEEE 802.1Q トンネリング ポートの設定, （235 ページ）

例：IEEE 802.1Q トンネリング ポートの設定, （247 ページ）

IEEE 802.1Q トンネリング設定時の注意事項

IEEE 802.1Q トンネリングを設定する場合は、カスタマー デバイスおよびエッジ スイッチの間で非対称リンクを常に使用する必要があります。カスタマー デバイスのポートを IEEE 802.1Q トランク ポートに、エッジ スイッチのポートをトンネル ポートとして設定してください。

トンネリングに使用する VLAN だけにトンネル ポートを割り当ててください。

ネイティブ VLAN および最大伝送単位（MTU）の設定要件については、次の項で説明します。

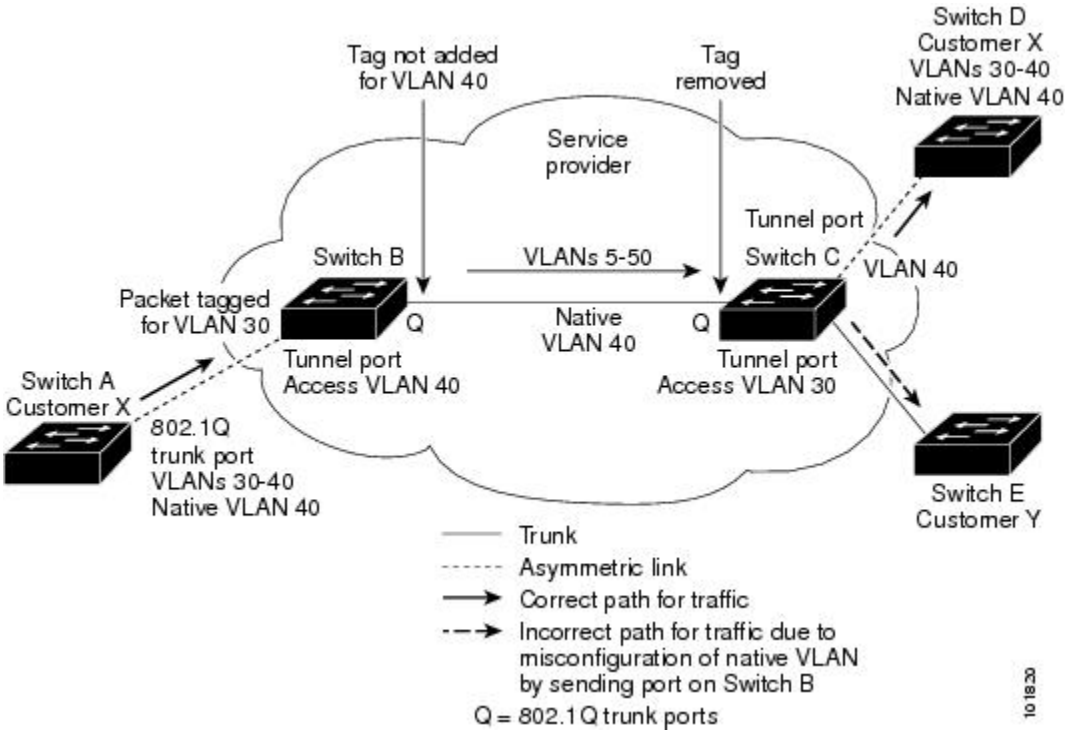
ネイティブ VLAN

エッジ スイッチで IEEE 802.1Q トンネリングを設定する場合、サービスプロバイダー ネットワークにパケットを送信するために、IEEE 802.1Q トランク ポートを使用する必要があります。 ただし、サービスプロバイダー ネットワークのコアを通過するパケットは、IEEE 802.1Q トランク、ISL トランク、非トランキング リンクのいずれかで送信できます。 コア スイッチで IEEE 802.1Q トランクを使用する場合、IEEE 802.1Q トランクのネイティブ VLAN は、同一スイッチの非トランキング（トンネリング）ポートのネイティブ VLAN と同じであってはなりません。これは、ネイティブ VLAN のトラフィックは、IEEE 802.1Q 送信トランク ポートではタグ付けされないためです。

次のネットワーク図で、VLAN 40 は、サービスプロバイダー ネットワークの入力エッジスイッチ（スイッチ B）にある、カスタマー X からの IEEE 802.1Q トランク ポートのネイティブ VLAN として設定されています。 カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダー ネットワークのスイッチ B の入力トンネル ポートに送信します。 トンネル ポートのアクセス VLAN（VLAN 40）は、エッジ スイッチのトランク ポートのネイティブ VLAN（VLAN 40）と同じであるため、トンネル ポートから受信したタグ付きパケットにメトロ タグが追加されません。 パケットには VLAN 30 タグだけが付いて、サー

ビスプロバイダーネットワークで出力エッジスイッチ（スイッチC）のトランク ポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違って送信されます。

図 5：***IEEE 802.1Q*** **トンネリングおよびネイティブ** ***VLAN*** **に潜在する問題**



この問題の解決方法は次のとおりです。

-
- **vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用することで、（ネイティブ VLAN を含む）IEEE 802.1Q トランクから発信されるすべてのパケットがタグ付けされるようにエッジ スイッチを設定します。 すべての IEEE 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットを受け入れますが、タグ付きパケットだけを送信します。
- エッジ スイッチのトランク ポートのネイティブ VLAN ID が、カスタマー VLAN 範囲に含まれないようにしてください。 たとえばトランク ポートが VLAN100 ～ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

システム MTU

スイッチ上のトラフィックに関するデフォルトのシステム MTU は、1500 バイトです。

system mtu jumbo グローバル コンフィギュレーション コマンドを使用すると、10 ギガビット イーサネット ポートおよびギガビット イーサネット ポートで 1500 バイトを超えるフレームをサポートするように設定できます。

システム MTU 値とシステム ジャンボ MTU 値には、IEEE 802.1Q ヘッダーは含まれていません。IEEE 802.1Q トンネリング機能では、メトロ タグが追加されるとフレーム サイズが 4 バイト増加するため、システム最大伝送単位サイズとシステム ジャンボ最大伝送単位サイズに最低 4 バイトを追加することによって、サービスプロバイダー ネットワークのすべてのスイッチが最大フレームを処理できるように設定する必要があります。

たとえば、スイッチは、次のいずれかの設定で、1496バイトの最大フレームサイズをサポートします。

- スイッチのシステム ジャンボ最大伝送単位値が 1500 バイトで、**switchport mode dot1q tunnel** インターフェイス コンフィギュレーション コマンドを使って 10 ギガビット イーサネットまたはギガビット イーサネット スイッチ ポートが設定されている。
- スイッチ メンバのシステム最大伝送単位値が 1500 バイトで、**switchport mode dot1q tunnel** インターフェイス コンフィギュレーション コマンドを使ってメンバのファスト イーサネット ポートが設定されている。

IEEE 802.1Q トンネリングのデフォルト設定

デフォルトでは、デフォルト switchport モードが dynamic auto であるため、IEEE 802.1Q トンネルはディセーブルです。 すべての IEEE 802.1Q トランク ポートにおける IEEE 802.1Q ネイティブ VLAN パケットのタグ付けもディセーブルです。

レイヤ 2 プロトコル トンネリングの概要

サービスプロバイダー ネットワークを越えて接続されている、さまざまなサイトに散在するカスタマーは、さまざまなレイヤ 2 プロトコルを使用してトポロジをスケールし、すべてのリモート サイトおよびローカル サイトを含める必要があります。 STP を適切に動作させる必要があり、サービスプロバイダー ネットワークを越えたローカル サイトおよびすべてのリモート サイトを含む、適切なスパニングツリーをすべての VLAN で構築する必要があります。 Cisco Discovery Protocol（CDP）では、隣接するシスコ デバイスをローカル サイトおよびリモート サイトから検出する必要があります。 VLAN トランキング プロトコル（VTP）では、カスタマー ネットワークのすべてのサイトで矛盾しないVLAN 設定を提供する必要があります。

プロトコル トンネリングがイネーブルである場合、サービスプロバイダーネットワークのインバウンド側エッジ スイッチでは、特殊 MAC アドレスでレイヤ 2 プロトコルパケットがカプセル化され、サービスプロバイダー ネットワークに送信されます。 ネットワークのコア スイッチでは、このパケットが処理されずに通常のパケットとして転送されます。 CDP、STP、VTP のレイヤ 2 プロトコル データ ユニット（PDU）は、サービスプロバイダー ネットワークをまたがり、サービスプロバイダー ネットワークのアウトバウンド側のカスタマー スイッチに配信されます。 同一パケットは同じ VLAN のすべてのカスタマー ポートで受信され、次のような結果になります。

- それぞれのカスタマー サイトのユーザは STP を適切に実行でき、すべての VLAN では（ローカル サイトだけではなく）すべてのサイトからのパラメータに基づいて、正しいスパニング ツリーが構築されます。

- CDP では、サービスプロバイダー ネットワークによって接続されているその他のシスコ デバイスに関する情報が検出されて表示されます。
- VTP ではカスタマー ネットワーク全体で一貫した VLAN 設定が提供され、サービス プロバイダーを通してすべてのスイッチに伝播されます。

（注） サードパーティ ベンダーとの相互運用性を提供するには、レイヤ 2 プロトコルトンネル バイパス機能を使用します。 バイパス モードでは、プロトコル トンネリングの制御方法が異なるベンダー スイッチに、制御 PDU が透過的に転送されます。 バイパス モードを実装するには、出力トランク ポートでレイヤ 2 プロトコル トンネリングをイネーブルにします。 レイヤ 2 プロトコル トンネリングがトランク ポートでイネーブルの場合、カプセル化された MAC アドレスが削除されて、プロトコル パケットに通常の MAC アドレスを持つようになります。

レイヤ 2 プロトコル トンネリングは個別に使用できます。レイヤ 2 プロトコル トンネリングでは、IEEE 802.1Q トンネリングを向上させることができます。 IEEE 802.1Q トンネリング ポートでプロトコル トンネリングがイネーブルになっていない場合、サービスプロバイダーネットワークの受信側のリモート スイッチでは PDU が受信されず、STP、CDP、VTP を適切に実行できません。プロトコルのトンネリングがイネーブルである場合、それぞれのカスタマーネットワークのレイヤ 2 プロトコルは、サービスプロバイダー ネットワーク内で動作しているものから完全に区別されます。 IEEE 802.1Q トンネリングでサービスプロバイダーネットワークを通してトラフィックを送信する、さまざまなサイトのカスタマー スイッチでは、カスタマー VLAN が完全に認識されます。 IEEE 802.1Q トンネリングを使用しない場合は、アクセス ポートでカスタマー スイッチに接続し、サービスプロバイダーのアクセス ポートでトンネリングをイネーブルにすることで、レイヤ 2 プロトコル トンネリングをイネーブルにできます。

たとえば、次の図（レイヤ 2 プロトコル トンネリング）では、カスタマー X の 4 つのスイッチが同じ VLAN 上にあり、サービスプロバイダー ネットワークを通して互いに接続されています。ネットワークで PDU がトンネリングされない場合、ネットワークの遠端側のスイッチでは、STP、CDP、VTP を適切に実行できません。 たとえば、カスタマー X のサイト 1 のスイッチでは、VLAN の STP は、カスタマー X のサイト 2 のスイッチに基づくコンバージェンス パラメータを考慮せずに、サイト 1 のスイッチ上にスパニングツリーを構築します。 これにより、「適切なコンバー

ジェンスを含まないレイヤ 2 ネットワーク トポロジ」の図に示されているようなトポロジになる可能性があります。

図 *6*：レイヤ *2* プロトコル トンネリング

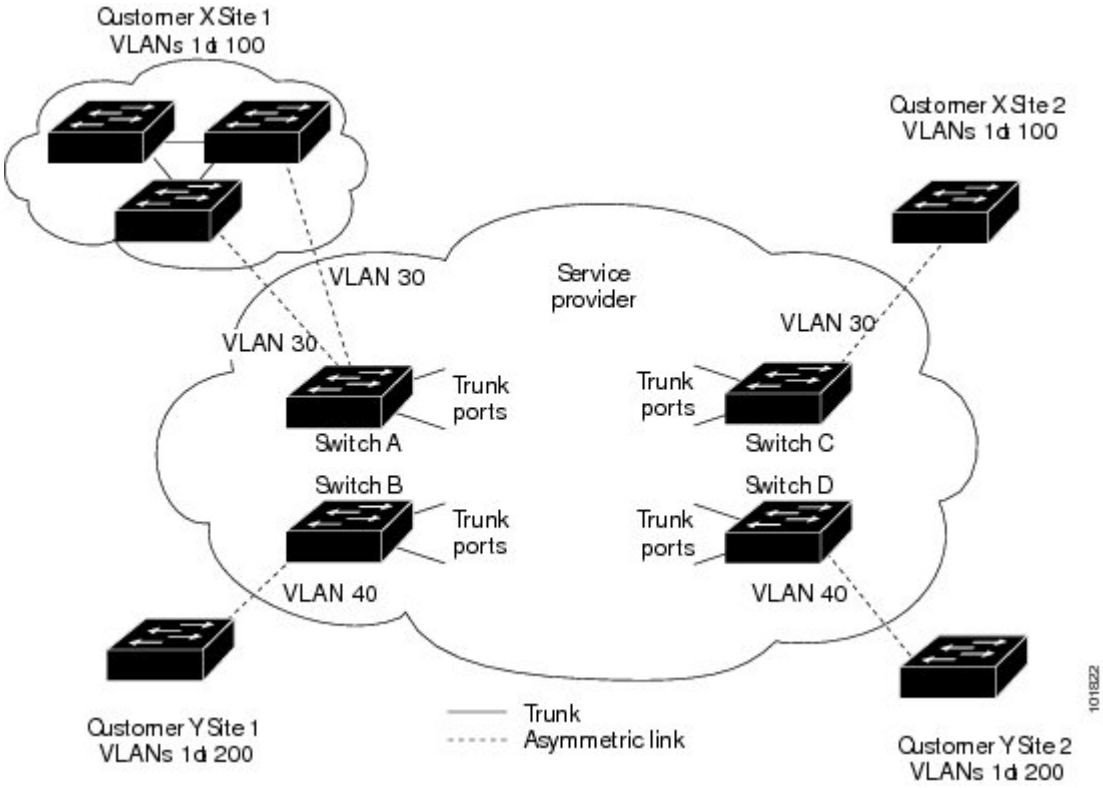
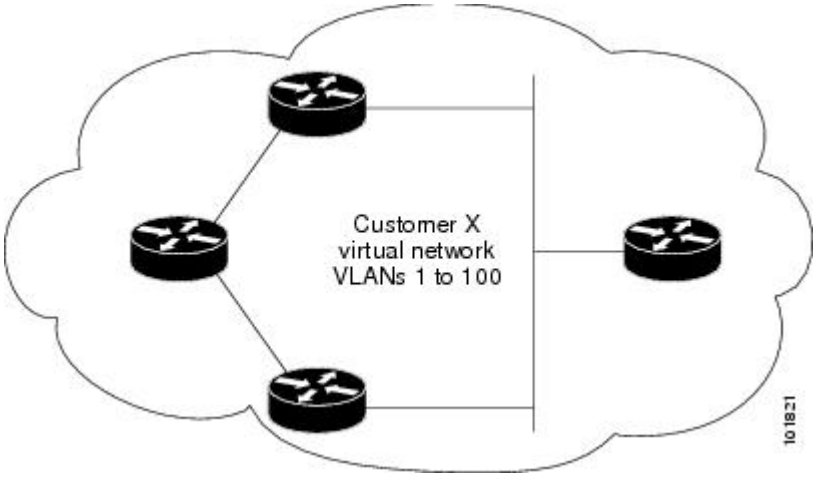


図 *7*：適切なコンバージェンスを含まないレイヤ *2* ネットワーク トポロジ

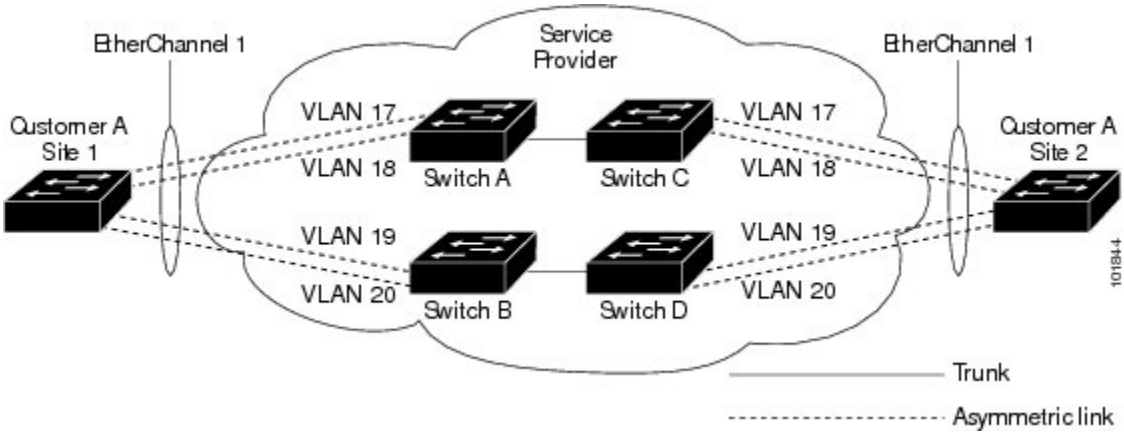


サービスプロバイダー ネットワークでは、レイヤ 2 プロトコル トンネリングを使用し、ポイント ツーポイント ネットワーク トポロジをエミュレートして、EtherChannel の作成を向上させること

ができます。 サービスプロバイダー スイッチでプロトコル トンネリング（PAgP または LACP）をイネーブルにすると、リモート カスタマー スイッチでは PDU が受信され、EtherChannel の自動作成をネゴシエーションできるようになります。

たとえば、次の図（EtherChannels のレイヤ 2 プロトコル トンネリング）では、カスタマー A の 2 つのスイッチが同じ VLAN 上にあり、サービスプロバイダー ネットワークを介して接続されています。 ネットワークで PDU がトンネリングされると、ネットワークの遠端側のスイッチでは、専用回線を必要とせずに EtherChannel の自動作成をネゴシエーションできます。

図 *8*：*EtherChannel* のレイヤ *2* プロトコル トンネリング



ポートでのレイヤ 2 プロトコル トンネリング

サービスプロバイダーネットワークのエッジスイッチで、カスタマーに接続されているポートにおいて、レイヤ 2 プロトコル トンネリングを（プロトコルごとに）イネーブルにできます。 カスタマー スイッチに接続されているサービス プロバイダー エッジ スイッチでは、トンネリング処理が実行されます。 エッジ スイッチ トンネル ポートは、カスタマーの IEEE 802.1Q トランク ポートに接続されます。 エッジ スイッチ アクセス ポートは、カスタマー アクセス ポートに接続されます。 カスタマー スイッチに接続されるエッジ スイッチでは、トンネリング処理が実行されます。

アクセス ポートまたはトンネル ポートのいずれかとして設定されているポートでは、レイヤ 2 プロトコル トンネリングをイネーブルにできます。 **switchport mode dynamic auto** モード（デフォルト モード）または **switchport mode dynamic desirable** モードに設定されているポートでは、レイヤ 2 プロトコル トンネリングをイネーブルにできません。

スイッチでは、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングがサポートされます。 ポイントツーポイント ネットワーク トポロジのエミュレートの場合は、PAgP、LACP、UDLD のプロトコルもサポートされます。 スイッチは、LLDP のレイヤ 2 プロトコル トンネリングをサポートしません。

（注） PAgP、LACP、UDLDプロトコル トンネリングでは、ポイントツーポイント トポロジのエミュレートだけが目的です。 設定を間違えたことによりトンネリング パケットが多くのポートに送信されると、ネットワーク障害が発生する可能性があります。

レイヤ 2 プロトコルがイネーブルになっているポート経由でサービスプロバイダーのインバウンド エッジ スイッチに入ったレイヤ 2 PDU が、トランク ポートからサービスプロバイダー ネットワークに出て行くとき、スイッチでは、カスタマー PDU 宛先 MAC アドレスが、周知のシスコ固有のマルチキャスト アドレス（01-00-0c-cd-cd-d0）で上書きされます。 IEEE 802.1Q トンネリングがイネーブルである場合、パケットにはタグが二重に付きます。このうち外部タグはカスタマーのメトロ タグ、内部タグはカスタマーの VLAN タグです。 コア スイッチでは内部タグが無視され、同じメトロ VLAN のすべてのトランク ポートにパケットが転送されます。 アウトバウンド側のエッジスイッチでは、適切なレイヤ2プロトコル情報およびMACアドレス情報が復元され、同じメトロ VLAN のすべてのトンネル ポートまたはすべてのアクセス ポートにパケットが転送されます。 このため、レイヤ 2 PDU はそのまま残り、サービスプロバイダー インフラストラクチャを越えてカスタマー ネットワークの反対側に配信されます。

レイヤ 2 プロトコル トンネリングの概要, （230 ページ）のレイヤ 2 プロトコル トンネリングの図を参照してください（それぞれアクセス VLAN 30、40 のカスタマー X とカスタマー Y）。 非対称リンクにより、サイト 1 のカスタマーは、サービスプロバイダー ネットワークのエッジ スイッチに接続されています。 サイト 1 のカスタマー Y からスイッチ B に発信されたレイヤ 2 PDU（たとえばBPDU）は、周知のMACアドレスが宛先MACアドレスになっている二重タグ パケットとしてインフラストラクチャに転送されます。 この二重タグ パケットには、40 というメトロ VLAN タグ、および VLAN 100 などの内部 VLAN タグが付いています。 二重タグ パケットがスイッチ D に入ると、外部 VLAN タグ 40 が外されて、周知の MAC アドレスがそれぞれのレイヤ 2 プロトコル MAC アドレスで置き換わり、パケットは、VLAN 100 の 1 重タグ フレームとしてサイト 2 のカスタマー Y に送信されます。

また、カスタマー スイッチのアクセス ポートまたはトランク ポートに接続されているエッジ スイッチのアクセス ポートでも、レイヤ 2 プロトコル トンネリングをイネーブルにできます。 この場合は、カプセル化プロセスとカプセル開放プロセスが、前の段落で説明したものと同じですが、パケットはサービスプロバイダーネットワークで二重タグになりません。 カスタマー固有のアクセス VLAN タグの 1 重タグになります。

関連トピック

レイヤ 2 プロトコル トンネリングの設定, （238 ページ）

例：レイヤ 2 プロトコル トンネリングの設定, （248 ページ）

レイヤ 2 プロトコル トンネリングのデフォルト設定

次の表に、レイヤ 2 プロトコル トンネリングのデフォルト設定を記載します。

表 *19*：レイヤ *2* イーサネット インターフェイス *VLAN* のデフォルト設定

機能	デフォルト設定
レイヤ 2 プロトコル トンネリング	ディセーブル。
シャットダウンしきい値	未設定。
ドロップしきい値	未設定。
CoS 値	インターフェイスで CoS 値が設定されている場合は、その値がレイヤ 2 プロトコル トンネリングの BPDU CoS 値を設定するために使用されます。 インターフェイス レベルで CoS 値が設定されてない場合は、L2 プロトコル トンネリング BPDU の CoS マーキングのデフォルト値は 5 になります。 これはデータ トラフィックに適用されません。

トンネリングの設定方法

IEEE 802.1Q トンネリング ポートの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport access vlan***vlan-id*
5. **switchport mode dot1q-tunnel**
6. **exit**
7. **vlan dot1q tag native**
8. **end**
9. 次のいずれかを使用します。
   - **show dot1q-tunnel**
   - **show running-config interface**
10. **show vlan dot1q tag native**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	トンネル ポートとして設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。 これは、カスタマースイッチに接続するサービスプロバイダーネットワーク内のエッジ ポートである必要があります。 有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（ポート チャネル 1 ～ 48）が含まれます。
ステップ 4	**switchport access vlan***vlan-id* 例： `Switch(config-if)# switchport access vlan 2`	インターフェイスがトランキングを停止した場合に使用されるデフォルト VLAN を指定します。 この VLAN ID は特定カスタマーに固有です。
ステップ 5	**switchport mode dot1q-tunnel** 例： `Switch(config-if)# switchport mode dot1q-tunnel`	IEEE 802.1Q トンネル ポートとしてインターフェイスを設定します。 （注） ポートを dynamic desirable デフォルト状態に戻すには、**no switchport mode dot1q-tunnel** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 6	**exit** 例： `Switch(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 7	**vlan dot1q tag native** 例： `Switch(config)# vlan dot1q tag`	（任意）すべての IEEE 802.1Q トランク ポートでネイティブ VLAN パケットのタギングがイネーブルになるようにスイッチを設定します。 これを設定せず、カスタマー VLAN ID がネイティブ VLAN と同じである場合、トランク ポートはメトロ タ

	コマンドまたはアクション	目的
	native	グを適用せず、パケットは誤った宛先に送信される可能性があります。 （注） ネイティブ VLAN パケットのタグ付けをディセーブルにするには、**no vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ステップ 9	次のいずれかを使用します。
	• **show dot1q-tunnel**
	• **show running-config interface**
	例：
	`Switch# show dot1q-tunnel`
	または
	`Switch# show running-config interface`
		IEEE 802.1Q トンネリング用に設定されたポートを表示します。
		トンネリング モードになっているポートを表示します。

ステップ 10	**show vlan dot1q tag native** 例： `Switch# show vlan dot1q native`	IEEE 802.1Q ネイティブ VLAN タギング ステータスを表示します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IEEE 802.1Q トンネリング，（225 ページ）
IEEE 802.1Q トンネリング，（222 ページ）
例：IEEE 802.1Q トンネリング ポートの設定，（247 ページ）

レイヤ 2 プロトコル トンネリングの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. 次のいずれかを使用します。
   - **switchport mode access**
   - **switchport mode dot1q-tunnel**
5. **l2protocol-tunnel** [**cdp** | **lldp** | **point-to-point** | **stp** | **vtp**]
6. **l2protocol-tunnel shutdown-threshold** [*packet_second_rate_value* | **cdp** | **lldppoint-to-point** | **stp** | **vtp**]
7. **l2protocol-tunnel drop-threshold** [*packet_second_rate_value* | **cdp** | **lldp** | **point-to-point** | **stp** | **vtp**]
8. **exit**
9. **errdisable recovery cause l2ptguard**
10. **l2protocol-tunnel cos***value*
11. **end**
12. **show l2protocol**
13. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを使用します。
	• **switchport mode access**
	• **switchport mode dot1q-tunnel**
	
	例：
	`Switch# switchport mode access`
	または
	`Switch# switchport mode dot1q-tunnel`
		アクセス ポートまたはIEEE 802.1Q トンネル ポートとしてインターフェイスを設定します。

ステップ 5	**l2protocol-tunnel** [**cdp** | **lldp** | **point-to-point** | **stp** | **vtp**] 例： `Switch# l2protocol-tunnel cdp`	目的のプロトコルに対してプロトコル トンネリングをイネーブルにします。 キーワードを入力しない場合、トンネリングは、3 つすべてのレイヤ 2 プロトコルでイネーブルになります。 （注） レイヤ 2 プロトコルのいずれか 1 つ、または 3 つすべてのプロトコル トンネリングをディセーブルにするには、**no l2protocol-tunnel** [**cdp** | **lldp** | **point-to-point** | **stp** | **vtp**] インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 6	**l2protocol-tunnel shutdown-threshold** [*packet_second_rate_value* | **cdp** | **lldppoint-to-point** | **stp** | **vtp**] 例： `Switch# l2protocol-tunnel shutdown-threshold 100 cdp`	（任意）1 秒間にカプセル化可能なパケット数を表すしきい値を設定します。 設定したしきい値を超えると、インターフェイスはディセーブルになります。 プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。 指定できる範囲は 1 ～ 4096 です。 デフォルトでは、しきい値は設定されません。 （注） このインターフェイスでドロップしきい値も設定する場合は、**shutdown-threshold** 値を **drop-threshold** の値以上にする必要があります。 （注） シャットダウンしきい値およびドロップしきい値をデフォルト設定に戻すには、**no l2protocol-tunnelshutdown-threshold** [*packet_second_rate_value* | **cdp** | **lldp**| **point-to-point** | **stp** | **vtp**]and the **no l2protocol-tunnel drop-threshold** [*packet_second_rate_value* | **cdp** | **lldp**| **point-to-point** |**stp** | **vtp**] コマンドを使用します。
ステップ 7	**l2protocol-tunnel drop-threshold** [*packet_second_rate_value* | **cdp** | **lldp** | **point-to-point** | **stp** | **vtp**]	（任意）1 秒間にカプセル化可能なパケット数を表すしきい値を設定します。 設定したしきい値を超えると、インターフェイスによってパケットがドロップされます。 プロトコル オプションを指定し

	コマンドまたはアクション	目的
	例： `Switch# l2protocol-tunnel drop-threshold 100 cdp`	ない場合、しきい値は、それぞれのトンネリングされたレイヤ2プロトコル タイプに適用されます。 指定できる範囲は 1 ～ 4096 です。 デフォルトでは、しきい値は設定されません。 （注） このインターフェイスでシャットダウンしきい値も設定する場合、**drop-threshold** 値は **shutdown-threshold** の値以下である必要があります。 （注） シャットダウンしきい値およびドロップしきい値をデフォルト設定に戻すには、**nol2protocol-tunnelshutdown-threshold** [**cdp** | **lldp**| **point-to-point** | **stp** | **vtp**]and the **no l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**] コマンドを使用します。
ステップ 8	**exit** 例： `Switch# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**errdisable recovery cause l2ptguard** 例： `Switch(config)# errdisable recovery cause l2ptguard`	（任意）インターフェイスが再びイネーブルになって再試行できるように、レイヤ 2 最大レート エラーからの復旧メカニズムを設定します。 errdisable recovery はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は300秒です。
ステップ 10	**l2protocol-tunnel cos***value* 例： `Switch(config)# l2protocol-tunnel cos value 7`	（任意）トンネリングされたすべてのレイヤ 2 PDU に対して CoS 値を設定します。 範囲は0～7です。デフォルトは、インターフェイスのデフォルト CoS 値です。 設定されていない場合、デフォルトは 5 です。
ステップ 11	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show l2protocol** 例： `Switch# show l2protocol`	スイッチのレイヤ 2 トンネル ポートを表示します（設定されているプロトコル、しきい値、カウンタを含む）。
ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

関連トピック

ポートでのレイヤ 2 プロトコル トンネリング, （233 ページ）
レイヤ 2 プロトコル トンネリング , （223 ページ）
EtherChannel のレイヤ 2 トンネリング, （224 ページ）
例：レイヤ 2 プロトコル トンネリングの設定, （248 ページ）

サービスプロバイダー エッジ スイッチの設定

はじめる前に

EtherChannels の場合は、SP（サービス プロバイダー）エッジ スイッチおよびカスタマー スイッチをレイヤ 2 プロトコル トンネリング用に設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode dot1q-tunnel**
5. **l2protocol-tunnel point-to-point** [**pagp** | **lacp** | **udld**]
6. **l2protocol-tunnel shutdown-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*
7. **l2protocol-tunnel drop-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*
8. **no cdp enable**
9. **spanning-tree bpdu filter enable**
10. **exit**
11. **errdisable recovery cause l2ptguard**
12. **l2protocol-tunnel cos***value*
13. **end**
14. **show l2protocol**
15. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch>` **`enable`**	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch#` **`configure terminal`**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)#` **`interface gigabitethernet1/0/1`**	IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode dot1q-tunnel** 例： `Switch(config-if)#` **`switchport mode dot1q-tunnel`**	IEEE 802.1Q トンネル ポートとしてインターフェイスを設定します。
ステップ 5	**l2protocol-tunnel point-to-point** [**pagp** | **lacp** | **udld**] 例： `Switch(config-if)#` **`l2protocol-tunnel point-to-point pagp`**	（任意）目的のプロトコルに関するポイントツーポイント プロトコル トンネリングをイネーブルにします。 キーワードを入力しない場合、トンネリングは、3 つすべてのプロトコルでイネーブルになります。 （注） ネットワーク障害を避けるため、ネットワークがポイントツーポイント トポロジになっていることを確認してから、PAgP パケット、LACP パケット、UDLD パケットのうちいずれかのトンネリングをイネーブルにしてください。 （注） いずれかのレイヤ 2 プロトコルまたは 3 つのすべてのレイヤ 2 プロトコルのポイントツーポイント プロトコル トンネリングをディセーブルにするには**no l2protocol-tunnel** [**point-to-point** [**pagp** | **lacp** | **udld**]] インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 6	**l2protocol-tunnel shutdown-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*	（任意）1 秒間にカプセル化可能なパケット数を表すしきい値を設定します。 設定したしきい値を超えると、インターフェイスは

	コマンドまたはアクション	目的
	例： `Switch(config-if)# l2protocol-tunnel shutdown-threshold point-to-point pagp 100`	ディセーブルになります。プロトコルオプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。 指定できる範囲は 1 ～ 4096 です。デフォルトでは、しきい値は設定されません。 （注） このインターフェイスでドロップしきい値も設定する場合は、**shutdown-threshold** 値を **drop-threshold** の値以上にする必要があります。 （注） シャットダウンしきい値およびドロップしきい値をデフォルト設定に戻すには、**no l2protocol-tunnel shutdown-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]]and the **no l2protocol-tunnel drop-threshold** [[**point-to-point** [**pagp** | lacp | **udld**]] コマンドを使用します。
ステップ 7	**l2protocol-tunnel drop-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] *value* 例： `Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 500`	（任意）1 秒間にカプセル化可能なパケット数を表すしきい値を設定します。 設定したしきい値を超えると、インターフェイスによってパケットがドロップされます。プロトコルオプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。 指定できる範囲は 1 ～ 4096 です。 デフォルトでは、しきい値は設定されません。 （注） このインターフェイスでシャットダウンしきい値も設定する場合、**drop-threshold** 値は **shutdown-threshold** の値以下である必要があります。
ステップ 8	**no cdp enable** 例： `Switch(config-if)# no cdp enable`	インターフェイス上で CDP をディセーブルにします。
ステップ 9	**spanning-tree bpdu filter enable** 例： `Switch(config-if)# spanning-tree bpdu filter enable`	インターフェイス上で BPDU フィルタリングをイネーブルにします。
ステップ 10	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**errdisable recovery cause l2ptguard** 例： `Switch(config)# errdisable recovery cause l2ptguard`	（任意）インターフェイスが再びイネーブルになって再試行できるように、レイヤ 2 最大レート エラーからの復旧メカニズムを設定します。 errdisable recovery はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は 300 秒です。
ステップ 12	**l2protocol-tunnel cos***value* 例： `Switch(config)# l2protocol-tunnel cos 2`	（任意）トンネリングされたすべてのレイヤ 2 PDU に対して CoS 値を設定します。 範囲は 0 ～ 7 です。デフォルトは、インターフェイスのデフォルト CoS 値です。 設定されていない場合、デフォルトは 5 です。
ステップ 13	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show l2protocol** 例： `Switch)# show l2protocol`	スイッチのレイヤ 2 トンネル ポートを表示します（設定されているプロトコル、しきい値、カウンタを含む）。
ステップ 15	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：サービスプロバイダー エッジ スイッチとカスタマー スイッチの設定, （248 ページ）

カスタマー スイッチの設定

はじめる前に

EtherChannel の場合は、サービスプロバイダー エッジ スイッチおよびカスタマー スイッチをレイヤ 2 プロトコル トンネリング用に設定する必要があります

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport trunk encapsulation dot1q**
5. **switchport mode trunk**
6. **udld port**
7. **channel-group***channel-group-number* **mode desirable**
8. **exit**
9. **interface port-channel port-channel***number*
10. **shutdown**
11. **no shutdown**
12. **end**
13. **show l2protocol**
14. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport trunk encapsulation dot1q** 例： `Switch(config)# switchport trunk encapsulation dot1q`	トランキング カプセル化形式を IEEE 802.1Q に設定します。

	コマンドまたはアクション	目的
ステップ 5	**switchport mode trunk** 例： `Switch(config-if)# switchport mode trunk`	インターフェイスでトランキングをイネーブルにします。
ステップ 6	**udld port** 例： `Switch(config-if)# udld port`	インターフェイス上で UDLD を通常モードでイネーブルにします。
ステップ 7	**channel-group***channel-group-number* **mode desirable** 例： `Switch(config-if)# channel-group 25 mode desirable`	チャネル グループにインターフェイスを割り当て、PAgP モードに desirable を指定します。
ステップ 8	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface port-channel port-channel***number* 例： `Switch(config)# interface port-channel port-channel 25`	ポートチャネル インターフェイス モードを開始します。
ステップ 10	**shutdown** 例： `Switch(config)# shutdown`	インターフェイスをシャットダウンします。
ステップ 11	**no shutdown** 例： `Switch(config)# no shutdown`	インターフェイスをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show l2protocol** 例： `Switch# show l2protocol`	スイッチのレイヤ 2 トンネル ポートを表示します（設定されているプロトコル、しきい値、カウンタを含む）。
ステップ 14	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 （注） インターフェイスをデフォルト設定に戻すには、**no switchport mode trunk**、**no udld enable**、および **no channel group***channel-group-number* **mode desirable** インターフェイス コンフィギュレーション コマンドを使用します。

関連トピック

例：サービスプロバイダー エッジ スイッチとカスタマー スイッチの設定, （248 ページ）

IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定例

例：IEEE 802.1Q トンネリング ポートの設定

以下の例では、トンネル ポートとしてインターフェイスを設定してネイティブ VLAN パケットのタグ付けをイネーブルにし、設定を確認する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/7
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Switch# show dot1q-tunnel interface gigabitethernet1/0/7
Port
-----
Gi1/0/1Port
-----
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

関連トピック

IEEE 802.1Q トンネリング ポートの設定, （235 ページ）

IEEE 802.1Q トンネリング, （225 ページ）

IEEE 802.1Q トンネリング, （222 ページ）

例：レイヤ 2 プロトコル トンネリングの設定

以下の例では、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングを設定し、設定を確認する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol

COS for Encapsulated Packets: 7
Port Protocol Shutdown Drop Encapsulation Decapsulation Drop
Threshold Threshold Counter Counter Counter
------- -------- --------- --------- ------------- ------------- -------------
Gi0/11 cdp 1500 1000 2288 2282 0
stp 1500 1000 116 13 0
vtp 1500 1000 3 67 0
pagp ---- ---- 0 0 0
lacp ---- ---- 0 0 0
udld ---- ---- 0 0 0
```

関連トピック

レイヤ 2 プロトコル トンネリングの設定, （238 ページ）

ポートでのレイヤ 2 プロトコル トンネリング, （233 ページ）

レイヤ 2 プロトコル トンネリング , （223 ページ）

EtherChannel のレイヤ 2 トンネリング, （224 ページ）

例：サービスプロバイダー エッジ スイッチとカスタマー スイッチの設定

以下は、サービス プロバイダーのエッジ スイッチ 1 およびエッジ スイッチ 2 を設定する方法の例です。 VLAN 17、18、19、20 はアクセス VLAN、ファスト イーサネット インターフェイス 1 および 2 は PAgP および UDLD がイネーブルになっているポイントツーポイント トンネル ポート、ドロップしきい値は 1000、ファスト イーサネット インターフェイス 3 はトランク ポートです。

サービスプロバイダー エッジ スイッチ 1 の設定は次のとおりです。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport access vlan 17
```

```
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport trunk encapsulation isl
Switch(config-if)# switchport mode trunk
```

サービスプロバイダー エッジ スイッチ 2 の設定は次のとおりです。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport trunk encapsulation isl
Switch(config-if)# switchport mode trunk
```

次は、サイト 1 のカスタマー スイッチを設定する方法の例です。ファストイーサネットインターフェイス 1、2、3、4 は IEEE 802.1Q トランキング用に設定されており、UDLD はイネーブル、EtherChannel グループ 1 はイネーブル、ポート チャネルはシャットダウンされた後でイネーブルになり EtherChannel 設定がアクティブになります。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface port-channel 1
```

```
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

関連トピック

サービスプロバイダー エッジ スイッチの設定, （241 ページ）

カスタマー スイッチの設定, （244 ページ）

トンネリング ステータスのモニタリング

次の表では、トンネリング ステータスをモニタするために使用するコマンドについて説明します。

表 *20*：トンネリングのモニタリング コマンド

コマンド	目的
clear l2protocol-tunnel counters	レイヤ 2 プロトコル トンネリング ポートのプロトコル カウンタをクリアします。
show dot1q-tunnel	スイッチの IEEE 802.1Q トンネル ポートを表示します。
show dot1q-tunnel interface*interface-id*	特定のインターフェイスがトンネル ポートであるかどうかを確認します。
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
show errdisable recovery	レイヤ 2 プロトコル トンネル エラーディセーブル ステートの回復タイマーがイネーブルかどうかを確認します。
show l2protocol-tunnel interface*interface-id*	特定のレイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
show l2protocol-tunnel summary	レイヤ 2 プロトコルのサマリー情報だけを表示します。
show vlan dot1q tag native	スイッチのネイティブ VLAN タギングのステータスを表示します。

次の作業

次の設定を行えます。

- VTP
- VLANs
- VLAN トランキング
- プライベート VLAN
- VLAN メンバーシップ ポリシー サーバ（VMPS）
- 音声 VLAN

第 12 章

スパニングツリー プロトコルの設定

- 機能情報の確認，253 ページ
- STP の制約事項，253 ページ
- スパニング ツリー プロトコルに関する情報，254 ページ
- スパニングツリー機能の設定方法，267 ページ
- スパニングツリー ステータスのモニタリング，281 ページ

機能情報の確認

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

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

STP の制約事項

- ルート スイッチとしてスイッチを設定しようとする場合、ルート スイッチにするために必要な値が 1 未満だと、失敗します。
- ネットワークが、拡張システム ID をサポートするスイッチとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするスイッチがルート スイッチになる可能性は低くなります。 古いソフトウェアを実行している接続スイッチのプライオリティより VLAN 番号が大きい場合は常に、拡張システム ID によってスイッチ プライオリティ値が増加します。

- 各スパニングツリー インスタンスのルート スイッチは、バックボーンまたはディストリビューション スイッチでなければなりません。 アクセス スイッチをスパニングツリー プライマリ ルートとして設定しないでください。

関連トピック

ルート スイッチの設定, （269 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （256 ページ）
スパニングツリー トポロジと BPDU, （255 ページ）
接続を維持するためのエージング タイムの短縮, （262 ページ）

スパニング ツリー プロトコルに関する情報

スパニングツリー プロトコル

スパニングツリー プロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ 2 リンク管理プロトコルです。 レイヤ 2 イーサネット ネットワークが正常に動作するには、任意の 2 つのステーション間で存在できるアクティブ パスは 1 つだけです。 エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。 このループがネットワークに発生すると、エンド ステーションにメッセージが重複して到着する可能性があります。 スイッチは、複数のレイヤ 2 インターフェイスのエンド ステーション MAC アドレスを学習する可能性もあります。 このような状況によって、ネットワークが不安定になります。 スパニングツリーの動作は透過的であり、エンド ステーション側で、単一 LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STP は、スパニングツリー アルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のスイッチを 1 つ選択します。 アルゴリズムは、次に基づき、各ポートにロールを割り当て、スイッチド レイヤ 2 ネットワークを介して最良のループフリー パスを算出します。 アクティブ トポロジでのポートの役割：

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているスイッチ、またはバックアップの役割が指定されているスイッチはルート スイッチです。 少なくとも *1* つのポートに役割が指定されているスイッチは、指定スイッチを意味します。

冗長データ パスはスパニングツリーによって、強制的にスタンバイ（ブロックされた）ステートにされます。 スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリーアルゴリズムがスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。 スイッチは、スパニングツリー フレーム （ブリッジ プロト

コルデータ ユニット（BPDU）と呼ばれる）を定期間隔で送受信します。 スイッチはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。 BPDU には、スイッチおよび MAC アドレス、スイッチの優先順位、ポートの優先順位、およびパス コストを含む、送信側スイッチとそのポートに関する情報が含まれます。 スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート スイッチおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

スイッチの 2 つのポートがループの一部である場合、 spanning-tree および、パス コスト設定は、どのポートがフォワーディング ステートになるか、およびどのポートがブロッキング ステートになるかを制御します。 スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。 パス コストパス コスト値は、メディア速度を表します。

（注） デフォルトではスイッチは、Small Form-Factor Pluggable（SFP）モジュールを備えていないインターフェイスにだけ、（接続が稼働していることを確認するために）キープアライブ メッセージを送信します。 [**no**] **keepalive** インターフェイス コンフィギュレーション コマンドをキーワードなしで入力すると、インターフェイスのデフォルトを変更できます。

スパニングツリー トポロジと BPDU

スイッチド ネットワーク内の安定したアクティブ スパニングツリー トポロジは、次の要素によって制御されます。

- スイッチ上の各 VLAN に関連付けられた一意のブリッジ ID（スイッチ プライオリティおよび MAC アドレス）。
- ルート スイッチに対するスパニングツリー パス コスト。
- 各レイヤ2インターフェイスに対応付けられたポート ID（ポート プライオリティおよびMAC アドレス）。

ネットワーク内のスイッチに電源が入ると、各機能はルート スイッチとして機能します。 各スイッチは、そのすべてのポートからコンフィギュレーション BPDU を送信します。 BPDU によって通信が行われ、スパニングツリー トポロジが計算されます。 各設定BPDU には、次の情報が含まれています。

- 送信スイッチがルート スイッチとして識別するスイッチの一意のブリッジ ID。
- ルートまでのスパニングツリー パス コスト
- 送信スイッチのブリッジ ID。
- メッセージ エージ
- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

スイッチは、優位な情報（より小さいブリッジID、より低いパスコストなど）が含まれているコンフィギュレーション BPDU を受信すると、そのポートに対する情報を保存します。 この BPDU をスイッチのルート ポート上で受信した場合、そのスイッチが指定スイッチとなっているすべての接続 LAN に、更新したメッセージを付けて BPDU を転送します。

スイッチは、そのポートに現在保存されている情報よりも下位の情報を含むコンフィギュレーション BPDU を受信した場合は、その BPDU を廃棄します。 スイッチが下位 BPDU を受信した LAN の指定スイッチである場合、そのポートに保存されている最新情報を含む BPDU をその LAN に送信します。 このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- ネットワーク内の1つのスイッチがとして選択されます。ルートスイッチ（スイッチドネットワークのスパニングツリー トポロジーの論理的な中心）。 箇条書きの項目の下の図を参照してください。

  VLAN ごとに、スイッチ プライオリティが最も高い（最も小さい数字の優先順位の値）スイッチがルート スイッチとして選択されます。 すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合、VLAN内でMACアドレスの最も小さいスイッチがルート スイッチになります。 スイッチのプライオリティ値は、次の図のようにブリッジ ID の最上位ビットを占めます。

- スイッチごとに（ルート スイッチを除く）、ルート ポートが 1 つ選択されます。 このポートは、スイッチからルートスイッチにパケットを転送するときに最適パス（最小コスト）を提供します。

- ルート スイッチへの最短距離は、パス コストに基づいてスイッチごとに計算されます。

- LAN セグメントごとに指定スイッチが選択されます。 指定スイッチは、その LAN からルート スイッチにパケットを転送するときの最小パス コストを提供します。 DP は、指定スイッチが LAN に接続されているポートです。

スイッチドネットワーク上のいずれの地点からもルートスイッチに到達する場合に必要のないパスはすべて、スパニングツリー ブロッキング モードになります。

関連トピック

ルート スイッチの設定, （269 ページ）
STP の制約事項, （253 ページ）

ブリッジ ID、デバイス プライオリティ、および拡張システム ID

IEEE 802.1D 標準では、それぞれのスイッチに固有のルートスイッチの選択を制御するブリッジ識別子（ブリッジ ID）が必要です。 各 VLAN は PVST+ と Rapid PVST+ によって異なる論理ブリッジと見なされるので、同一のスイッチは設定された各 VLAN とは異なるブリッジ ID を保有している必要があります。 スイッチ上の各 VLAN には一意の 8 バイト ブリッジ ID が設定されます。 上位の 2 バイトはスイッチ プライオリティに使用され、残りの 6 バイトがスイッチの MAC アドレスから取得されます。

スイッチでは IEEE 802.1t スパニングツリー拡張機能がサポートされ、従来はスイッチプライオリティに使用されていたビットの一部が VLAN ID として使用されるようになりました。 その結果、

スイッチに割り当てられる MAC アドレスが少なくなり、より広い範囲の VLAN ID をサポートできるようになり、しかもブリッジ ID の一意性を損なうこともありません。

従来はスイッチ プライオリティに使用されていた 2 バイトが、4 ビットのプライオリティ値と 12 ビットの拡張システム ID 値（VLAN ID と同じ）に割り当てられています。

表 *21*：デバイス プライオリティ値および拡張システム *ID*

プライオリティ値				拡張システム ID（VLAN ID と同設定）											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニングツリーは、ブリッジ ID を VLAN ごとに一意にするために、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用します。

拡張システム ID のサポートにより、ルート スイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチプライオリティの手動での設定方法に影響が生じます。 たとえば、スイッチのプライオリティ値を変更すると、スイッチがルート スイッチとして選定される可能性も変更されることになります。 大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。

指定された VLAN のルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチはその VLAN について、自身のプライオリティを最小のスイッチプライオリティより 4096 だけ小さい値に設定します 4096 は、表に示すように 4 ビット スイッチ スイッチ プライオリティ値の最下位ビットの値です。

関連トピック

ルート スイッチの設定, （269 ページ）
STP の制約事項, （253 ページ）
ルート スイッチの設定, （307 ページ）
ルート スイッチ, （287 ページ）
MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

ポート プライオリティとパス コスト

ループが発生した場合、スパニングツリーはポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。 最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てることができます。 すべてのインターフェイスに同じプライオリティ値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

スパニングツリー パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。 ループが発生した場合、スパニングツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。 最初に選択されるインターフェイスには低いコスト値を

割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスに同じコスト値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

スイッチがスイッチ スタックのメンバーの場合は、最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには（ポート プライオリティを調整せずに）大きいコスト値を与えます。 詳細については、関連項目を参照してください。

関連トピック

ポート プライオリティの設定, （273 ページ）
パス コストの設定, （274 ページ）

スパニングツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。 その結果、スイッチドネットワークのさまざまな時点および場所でトポロジーの変化が発生します。インターフェイスがスパニングツリートポロジに含まれていない状態からフォワーディングステートに直接移行すると、一時的にデータループが形成されることがあります。インターフェイスは新しいトポロジ情報がスイッチドLAN上で伝播されるまで待機し、フレーム転送を開始する必要があります。 インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

スパニングツリーを使用しているスイッチの各レイヤ 2 インターフェイスは、次のいずれかのステートになります。

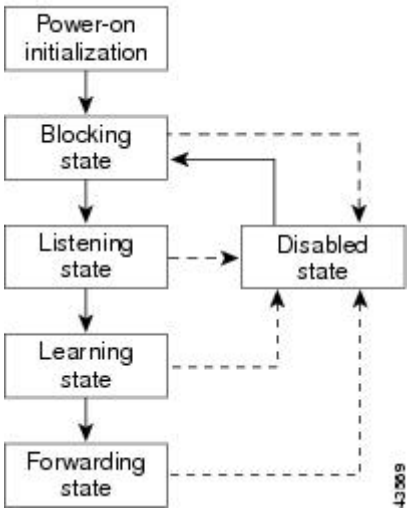
- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：インターフェイスをフレーム転送に関与させることをスパニングツリーが決定した場合、ブロッキング ステートから最初に移行するステートです。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニングツリーに含まれません。シャットダウン ポートであるか、ポート上にリンクがないか、またはポート上でスパニングツリーインスタンスが稼働していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

インターフェイスはこれらのステート間を移動します。

図 *9*：スパニングツリー インターフェイス ステート



デフォルト設定では、スイッチを起動するとスパニングツリーがイネーブルになります。その後、スイッチの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。スパニングツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. スパニングツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニング ステートになります。
2. スパニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートの間、スイッチが転送データベースのエンド ステーションの位置情報を学習しているとき、インターフェイスはフレーム転送をブロックし続けます。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 インターフェイスはフレームの転送に関与しません。 初期化後、スイッチの各インターフェイスに BPDU が送信されます。 スイッチは最初、他のスイッチと BPDU を交換するまで、ルートとして動作します。 この交換により、ネットワーク内でどのスイッチがルートまたはルート スイッチになるかが確立されます。 ネットワーク内にスイッチが 1 つしかない場合は交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニング ステートになります。 インターフェイスはスイッチの初期化後、必ずブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、ブロッキング ステートを経て、レイヤ 2 インターフェイスが最初に移行するステートです。 インターフェイスがリスニング ステートになるのは、スパニングツリーによってそのインターフェイスのフレーム転送への関与が決定された場合です。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ 2 インターフェイスは、フレームの転送に関与できるように準備します。 インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 インターフェイスは、フレームを転送します。 インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ブロッキング ステートのレイヤ 2 インターフェイスは、フレームの転送やスパニングツリーに関与しません。 ディセーブル ステートのインターフェイスは動作不能です。

ディセーブル インターフェイスは、次の機能を実行します。

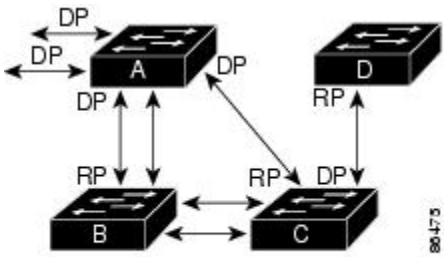
- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

スイッチ またはポートがルート スイッチまたはルート ポートになる仕組み

ネットワーク上のすべてのスイッチがデフォルトのスパニングツリー設定でイネーブルになっている場合、最小の MAC アドレスを持つスイッチがルート スイッチになります。

スイッチ A はルート スイッチとして選択されます。すべてのスイッチのスイッチのプライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最も小さいためです。 ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、スイッチ A が最適なルート スイッチとは限りません。 ルート スイッチになるように、最適なスイッチのプライオリティを引き上げる（数値を引き下げる）と、スパニングツリーの再計算が強制的に行われ、最適なスイッチをルートとした新しいトポロジが形成されます。

図 *10*：スパニングツリー トポロジ



RP = Root Port
DP = Designated Port

スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチドネットワークの送信元エンドステーションから宛先エンドステーションまでのパスが最適にならない場合があります。 たとえば、ルートポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルートポートが変更される可能性があります。 最高速のリンクをルートポートにすることが重要です。

たとえば、スイッチ B 上のあるポートがギガビット イーサネット リンクで、スイッチ B 上の別のポート（10/100 リンク）がルート ポートであると仮定します。 ネットワーク トラフィックはギガビット イーサネット リンクに流す方が効率的です。 ギガビット イーサネット ポートのスパニングツリー ポート プライオリティをルート ポートより高くする（数値を小さくする）と、ギガビット イーサネット ポートが新しいルート ポートになります。

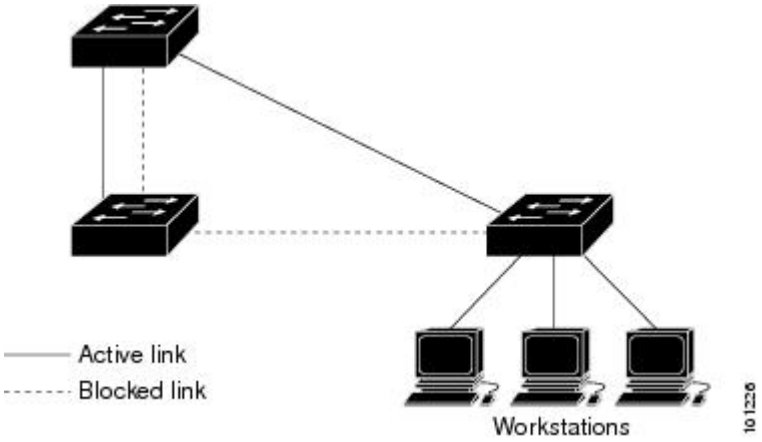
関連トピック

ポート プライオリティの設定, （273 ページ）

スパニングツリーおよび冗長接続

2 つのスイッチ インターフェイスを別の 1 台のデバイス、または 2 台の異なるデバイスに接続することにより、スパニングツリーを使用して冗長バックボーンを作成できます。 スパニングツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合にはそのディセーブルにしていた方をイネーブルにします。 一方のリンクが高速で、他方が低速の場合、必ず、低速の方のリンクがディセーブルになります。 速度が同じ場合、ポート プライオリティとポート ID が加算され、最大値を持つリンクがスパニングツリーによってディセーブルにされます。

図 *11*：スパニングツリーおよび冗長接続



EtherChannel グループを使用して、スイッチ間に冗長リンクを設定することもできます。

スパニングツリー アドレスの管理

IEEE 802.1D では、各種ブリッジ プロトコルに使用させるために、0x00180C2000000 ～ 0x0180C2000010 の範囲で 17 のマルチキャスト アドレスが規定されています。 これらのアドレスは削除できないスタティック アドレスです。

スパニングツリー ステートに関係なく、スタック内の各スイッチは 0x0180C2000000 ～ 0x0180C2000000 のアドレス宛てのパケットを受信しますが、転送は行いません。

スパニングツリーがイネーブルの場合、スイッチまたはスタック内の各スイッチの CPU は 0x0180C2000000 および 0x0180C2000010 宛てのパケットを受信します。 スパニングツリーがディセーブルの場合は、スイッチまたはスタック内の各スイッチは、それらのパケットを不明のマルチキャスト アドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミック アドレスのエージング タイムはデフォルトで 5 分です。これは、**mac-address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルトの設定です。 ただし、スパニングツリーの再構成により、多数のステーションの位置が変更されることがあります。 このよ

うなステーションは、再構成中、5分以上にわたって到達できないことがあるので、アドレステーブルからステーション アドレスを削除し、改めて学習できるように、アドレス エージング タイムが短縮されます。 スパニングツリー再構成時に短縮されるエージングタイムは、転送遅延パラメータ値（**spanning-tree vlan** *vlan-id* **forward-time** *seconds* グローバル コンフィギュレーション コマンド）と同じです。

各 VLAN はそれぞれ独立したスパニングツリー インスタンスであるため、スイッチは VLAN 単位でエージング タイムを短縮します。 ある VLAN でスパニングツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスがエージング タイム短縮の対象になります。 他の VLAN のダイナミック アドレスは影響を受けず、スイッチで設定されたエージング間隔がそのまま保持されます。

関連トピック

ルート スイッチの設定, （269 ページ）
STP の制約事項, （253 ページ）

スパニングツリー モードおよびプロトコル

このスイッチでサポートされるモードおよびプロトコルは、次のとおりです。

- PVST+：このスパニングツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。 すべてのイーサネット ポートベースの VLAN で使用されるスパニングツリーのデフォルト モードです。 PVST+ はスイッチ上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリー パスを提供します。

  PVST+ は、対象となる VLAN にレイヤ 2 ロード バランシングを提供します。 ネットワーク上の VLAN を使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリンクを使用できるようにします。 VLAN 上の PVST+ インスタンスごとに、それぞれ 1 つのルート スイッチがあります。 このルート スイッチは、その VLAN に対応するスパニングツリー情報を、ネットワーク上の他のすべてのスイッチに伝送します。 このプロセスにより、各スイッチがネットワークに関する共通の情報を持つため、ネットワーク トポロジが確実に維持されます。

- Rapid PVST+：このスパニングツリー モードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。 高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。 このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージング タイムが使用されます。

  Rapid PVST+ は PVST+ と同じ設定を使用しているので（特に明記する場合を除く）、スイッチで必要なことは最小限の追加設定のみです。 Rapid PVST+ の利点は、大規模な PVST+ のインストール ベースを Rapid PVST+ に移行する際に、複雑なマルチ スパニングツリー プロトコル（MSTP）設定の学習やネットワーク再設定の必要がないことです。 Rapid PVST+ モードでは、各 VLAN は独自のスパニングツリー インスタンスを最大数実行します。

- MSTP：このスパニングツリー モードは IEEE 802.1s 標準に準拠しています。 複数の VLAN を同一のスパニングツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要となるスパニングツリーインスタンスの数を減らすことができます。 MSTP は Rapid

Spanning-Tree Protocol（RSTP）（IEEE 802.1w 準拠）上で実行され、転送遅延を解消し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行することにより、スパニングツリーの高速コンバージェンスを可能にします。 スイッチ スタックでは、クロススタック高速移行（CSRT）機能が RSTP と同じ機能を実行します。 RSTP または CSRT を使用しなければ、MSTP は稼働できません。

関連トピック

スパニングツリー モードの変更, （267 ページ）

サポートされるスパニングツリー インスタンス

PVST+ または Rapid PVST+ モードでは、スイッチまたはスイッチ スタックは最大 128 のスパニングツリー インスタンスをサポートします。

MSTP モードでは、スイッチまたはスイッチ スタックは最大 65 の MST インスタンスをサポートします。 特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

関連トピック

スパニング ツリーのディセーブル化, （268 ページ）
スパニングツリー機能のデフォルト設定, （266 ページ）
MSTP のデフォルト設定, （303 ページ）

スパニングツリーの相互運用性と下位互換性

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree（CST）のルートは MST バックボーンの内側に配置する必要があり、PVST+ スイッチを複数の MST リージョンに接続することはできません。

ネットワーク内に Rapid PVST+ を実行しているスイッチと PVST+ を実行しているスイッチが存在する場合、Rapid PVST+ スイッチと PVST+ スイッチを別のスパニングツリーインスタンスに設定することを推奨します。 Rapid PVST+ スパニングツリー インスタンスでは、ルート スイッチは Rapid PVST+ スイッチでなければなりません。 PVST+ インスタンスでは、ルート スイッチは PVST+ スイッチでなければなりません。 PVST+ スイッチはネットワークのエッジに配置する必要があります。

すべてのスタック メンバーが、同じバージョンのスパニングツリーを実行します（すべて PVST+、すべて Rapid PVST+、またはすべて MSTP）。

表 *22*：*PVST+*、*MSTP*、*Rapid PVST+* の相互運用性と互換性

	PVST+	**MSTP**	**Rapid PVST+**
PVST+	Yes	あり（制限あり）	あり（PVST+ に戻る）
MSTP	あり（制限あり）	Yes	あり（PVST+ に戻る）
Rapid PVST+	あり（PVST+ に戻る）	あり（PVST+ に戻る）	Yes

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）
MSTP 設定時の注意事項, （286 ページ）
MST リージョン, （288 ページ）

STP および IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニングツリー ストラテジに一定の制限を設けています。 この規格では、トランク上で使用できるすべての VLAN に対して、1 つのスパニングツリー インスタンスしか認められません。 ただし、IEEE 802.1Q トランクを介して接続される Cisco スイッチのネットワークにおいて、スイッチはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。

IEEE 802.1Q トランクを介して Cisco スイッチを他社製のデバイスに接続する場合、Cisco スイッチは PVST+ を使用してスパニングツリーの相互運用性を実現します。 Rapid PVST+ がイネーブルの場合、スイッチは PVST+ ではなく Rapid PVST+ を使用します。 スイッチは、トランクの IEEE 802.1Q VLAN のスパニングツリー インスタンスと他社の IEEE 802.1Q スイッチのスパニングツリー インスタンスを結合します。

ただし、PVST+ または Rapid PVST+ の情報はすべて、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離された Cisco スイッチによって維持されます。 Cisco スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

PVST+ は IEEE 802.1Q トランクで自動的にイネーブルになるので、ユーザ側で設定する必要はありません。 アクセス ポートおよび ISL（スイッチ間リンク）トランク ポートでの外部スパニングツリーの動作は、PVST+ の影響を受けません。

VLAN ブリッジ スパニングツリー

シスコ VLAN ブリッジ スパニングツリーは、フォールバック ブリッジング機能（ブリッジ グループ）で使用し、DECnet などの IP 以外のプロトコルを 2 つ以上の VLAN ブリッジ ドメインまたはルーテッド ポート間で伝送します。 VLAN ブリッジ スパニングツリーにより、ブリッジ グループは個々の VLAN スパニングツリーの上部にスパニングツリーを形成できるので、VLAN 間で複数の接続がある場合に、ループが形成されないようにします。 また、ブリッジングされている VLAN からの個々のスパニングツリーが単一のスパニングツリーに縮小しないようにする働きもします。

VLAN ブリッジ スパニングツリーをサポートするには、一部のスパニングツリー タイマーを増やします。 フォールバック ブリッジング機能を使用するには、スイッチで IP サービス フィーチャセットをイネーブルにする必要があります。

スパニングツリー機能のデフォルト設定

表 *23*：スパニングツリー機能のデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル
スパニングツリー モード	PVST+ （Rapid PVST+ と MSTP はディセーブル）
スイッチ priority	32768
スパニングツリーポートプライオリティ（インターフェイス単位で設定可能）	128
スパニングツリーポートコスト（インターフェイス単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリーVLANポートプライオリティ（VLAN単位で設定可能）	128
スパニングツリーVLANポートコスト（VLAN単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー タイマー	hello タイム：2 秒 転送遅延時間：15 秒 最大エージング タイム：20 秒 転送保留カウント：6 BPDU

関連トピック

スパニング ツリーのディセーブル化，（268 ページ）
サポートされるスパニングツリー インスタンス，（264 ページ）

スパニングツリー機能の設定方法

スパニングツリー モードの変更

スイッチは次の 3 つのスパニングツリー モードをサポートします。Per-VLAN Spanning-Tree Plus（PVST+）、Rapid PVST+、またはマルチ スパニングツリー プロトコル（MSTP）。 デフォルトで、スイッチは PVST+ プロトコルを実行します。

デフォルト モード以外のモードをイネーブルにする場合、この手順は必須です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**}
4. **interface***interface-id*
5. **spanning-tree link-type point-to-point**
6. **end**
7. **clear spanning-tree detected-protocols**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**} 例： `Switch(config)# spanning-tree mode pvst`	スパニングツリーモードを設定します。 すべてのスタック メンバーは、同じバージョンのスパニング ツリーを実行します。 • **pvst** を選択して、PVST+ をイネーブルにします（デフォルト設定）。 • **mst** を選択して、MSTP（および RSTP）をイネーブルにします。 • **rapid-pvst** を選択して、Rapid PVST+ をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**interface***interface-id* 例： `Switch(config)# interface GigabitEthernet1/0/1`	（Rapid PVST+ モードの場合のみ推奨）設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。 VLAN ID の範囲は 1 ～ 4094 です。 指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 5	**spanning-tree link-type point-to-point** 例： `Switch(config-if)# spanning-tree link-type point-to-point`	（Rapid PVST+ モードの場合のみ推奨）このポートのリンク タイプをポイントツーポイントに指定します。 このポート（ローカル ポート）をポイントツーポイント リンクでリモート ポートと接続し、ローカル ポートが指定ポートになると、スイッチはリモート ポートとネゴシエーションし、ローカル ポートをフォワーディング ステートにすばやく変更します。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**clear spanning-tree detected-protocols** 例： `Switch# clear spanning-tree detected-protocols`	（Rapid PVST+ モードの場合のみ推奨）スイッチ上の任意のポートが IEEE 802.1D 準拠のレガシー スイッチのポートと接続されている場合に、このコマンドはスイッチ全体でプロトコル移行プロセスを再開します。 このステップは、このスイッチで Rapid PVST+ が稼働していることを指定スイッチが検出する場合のオプションです。

関連トピック

スパニングツリー モードおよびプロトコル，（263 ページ）

スパニング ツリーのディセーブル化

スパニングツリーはデフォルトで、VLAN 1 およびスパニングツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。 スパニングツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。

注意 スパニングツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **no spanning-tree vlan***vlan-id*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree vlan***vlan-id* 例： `Switch(config)# no spanning-tree vlan 300`	*vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

サポートされるスパニングツリー インスタンス，（264 ページ）
スパニングツリー機能のデフォルト設定，（266 ページ）

ルート スイッチの設定

特定の VLAN でスイッチをルートとして設定するには、**spanning-tree vlan***vlan-id***root** グローバル コンフィギュレーション コマンドを使用して、スイッチプライオリティをデフォルト値（32768）から、それより大幅に小さい値に変更します。 このコマンドを入力すると、ソフトウェアが各

VLAN について、ルート スイッチのスイッチ プライオリティを確認します。 拡張システム ID をサポートするため、スイッチは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、このスイッチを指定された VLAN のルートに設定できます。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大スイッチ ホップ カウント）を指定するには、**diameter** キーワードを使用します。ネットワーク直径を指定すると、スイッチはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。 **hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree vlan***vlan-id***root primary** [**diameter***net-diameter*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan***vlan-id***root primary** [**diameter***net-diameter* 例： `Switch(config)# spanning-tree vlan 20-24 root primary diameter 4`	指定された VLAN のルートになるように、スイッチを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • （任意）**diameter***net-diameter* には、任意の 2 つのエンド ステーション間の最大スイッチ数を指定します。 範囲は 2 ～ 7 です。

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

次の作業

ルート スイッチとしてスイッチを設定した後で、**spanning-tree vlan***vlan-id***hello-time**、**spanning-tree vlan***vlan-id***forward-time**、および **spanning-tree vlan***vlan-id***max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、および最大エージング タイムを手動で設定することは推奨できません。

関連トピック

ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （256 ページ）
スパニングツリー トポロジと BPDU, （255 ページ）
接続を維持するためのエージング タイムの短縮, （262 ページ）
STP の制約事項, （253 ページ）

セカンダリ ルート デバイスの設定

スイッチをセカンダリ ルートとして設定すると、スイッチプライオリティがデフォルト値（32768）から 28672 に変更されます。 このプライオリティでは、スイッチがプライマリ ルート スイッチが失敗した場合の、指定された VLAN のルートスイッチになる可能性があります。 ここでは、その他のネットワーク スイッチが、デフォルトのスイッチ プライオリティの 32768 を使用しているためにルート スイッチになる可能性が低いことが前提となっています。

このコマンドを複数のスイッチに対して実行すると、複数のバックアップ ルート スイッチを設定できます。 **spanning-tree vlan***vlan-id***root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree vlan***vlan-id***root secondary** [**diameter***net-diameter*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan***vlan-id***root secondary** [**diameter***net-diameter* 例： `Switch(config)# spanning-tree vlan 20-24 root secondary diameter 4`	指定された VLAN のセカンダリ ルートになるように、スイッチを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • （任意）**diameter***net-diameter* には、任意の 2 つのエンド ステーション間の最大スイッチ数を指定します。 指定できる範囲は 2 ～ 7 です。 プライマリ ルート スイッチを設定したときと同じネットワーク直径を使用してください。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ポート プライオリティの設定

（注） スイッチがスイッチ スタックのメンバである場合、**spanning-tree** [**vlan** *vlan-id*] **port-priority***priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree** [**vlan** *vlan-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させるインターフェイスには、低いコスト値を割り当て、最後に選択させるインターフェイスには高いコスト値を割り当てます。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree port-priority***priority*
5. **spanning-treevlan***vlan-id***port-priority***priority*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）です。

	コマンドまたはアクション	目的
ステップ 4	**spanning-tree port-priority***priority* 例： `Switch(config-if)# spanning-tree port-priority 0`	インターフェイスのポート プライオリティを設定します。 *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。 有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。 その他の値はすべて拒否されます。 値が小さいほど、プライオリティが高くなります。
ステップ 5	**spanning-treevlan***vlan-id***port-priority***priority* 例： `Switch(config-if)# spanning-tree vlan 20-25 port-priority 0`	VLAN のポート プライオリティを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。 有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。 その他の値はすべて拒否されます。 値が小さいほど、プライオリティが高くなります。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

ポート プライオリティとパス コスト，（257 ページ）

スイッチ またはポートがルート スイッチまたはルート ポートになる仕組み，（261 ページ）

パス コストの設定

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree cost***cost*
5. **spanning-tree vlan***vlan-id***cost***cost*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。 有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）です。
ステップ 4	**spanning-tree cost***cost* 例： `Switch(config-if)# spanning-tree cost 250`	インターフェイスのコストを設定します。 ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。 低いパス コストは高速送信を表します。 *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**spanning-tree vlan***vlan-id***cost***cost* 例： `Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300`	VLAN のコストを設定します。 ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。 低いパス コストは高速送信を表します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一

	コマンドまたはアクション	目的
		連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-treeinterface*interface-id* 特権 EXEC コマンドで情報が表示されるのは、リンクアップ動作可能の状態にあるポートに限られます。 そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティとパス コスト，（257 ページ）

VLAN のデバイス プライオリティの設定

スイッチプライオリティを設定して、スタンドアロンスイッチまたはスタックにあるスイッチがルート スイッチとして選択される可能性を高めることができます。

（注） このコマンドの使用には注意してください。 スイッチのプライオリティを変更する場合は通常、**spanning-tree vlan***vlan-id***root primary** および **spanning-tree vlan***vlan-id***root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree vlan***vlan-id***priority***priority*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan***vlan-id***priority***priority* 例： `Switch(config)# spanning-tree vlan 20 priority 8192`	VLAN のスイッチ プライオリティの設定 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。 この値が低いほど、スイッチがルート スイッチとして選択される可能性が高くなります。 有効なプライオリティ値は4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。 その他の値はすべて拒否されます。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

hello タイムの設定

helloタイムはルートスイッチによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

手順の概要

1. **enable**
2. **spanning-tree vlan***vlan-id***hello-time***seconds*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**spanning-tree vlan***vlan-id***hello-time***seconds* 例： `Switch(config)# spanning-tree vlan 20-24 hello-time 3`	VLAN の hello タイムを設定します。 hello タイムはルート スイッチによって設定メッセージが生成されて送信される時間の間隔です。 このメッセージは、スイッチが活動中であることを表します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

VLAN の転送遅延時間の設定

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree vlan***vlan-id***forward-time***seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan***vlan-id***forward-time***seconds* 例： `Switch(config)# spanning-tree vlan 20,25 forward-time 18`	VLAN の転送時間を設定します。 転送遅延時間は、スパニング ツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

VLAN の最大エージング タイムの設定

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree vlan***vlan-id***max-age***seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan***vlan-id***max-age***seconds* 例： `Switch(config)# spanning-tree vlan 20 max-age 30`	VLAN の最大エージング タイムを設定します。 最大エージング タイムは、スイッチが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

転送保留カウントの設定

転送保留カウント値を変更することで、BPDU のバースト サイズを設定できます。

（注） このパラメータをより高い値に変更すると、（特に Rapid PVST+ モードで）CPU の使用率に大きく影響します。 逆に、この値を低く設定すると、セッションによってはコンバージェンスを抑えることができます。 この値は、デフォルト設定で使用することを推奨します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree transmit hold-count***value*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree transmit hold-count***value* 例： `Switch(config)# spanning-tree transmit hold-count 6`	1 秒間停止する前に送信できる BPDU 数を設定します。 *value* に指定できる範囲は 1 ～ 20 です。デフォルト値は 6 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

スパニングツリー ステータスのモニタリング

表 *24*：スパニングツリー ステータス表示用のコマンド

show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。

show spanning-tree vlan *vlan-id*	指定した VLAN のスパニング ツリー情報を表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree interface *interface-id* **portfast**	指定したインターフェイスのスパニングツリー portfast 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。またはSTP ステートセクションのすべての行を表示します。

スパニングツリー カウンタをクリアするには、**clear spanning-tree** [**interface** i*nterface-id*] 特権 EXEC コマンドを使用します。

第 13 章

複数のスパニングツリープロトコルの設定

- 機能情報の確認，283 ページ
- MSTP の前提条件，283 ページ
- MSTP の制約事項，284 ページ
- MSTP について，285 ページ
- MSTP 機能の設定方法，304 ページ
- MST の設定およびステータスのモニタリング，324 ページ
- MSTP の機能情報，325 ページ

機能情報の確認

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

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

MSTP の前提条件

- 2 つ以上のスイッチを同じマルチ スパニングツリー（MST）リージョンに設定するには、その 2 つに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

- 2 つ以上のスタックされたスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。
- ネットワーク内の冗長パスでロード バランシングを機能させるには、すべての VLAN/インスタンスマッピングの割り当てが一致している必要があります。一致していないと、すべてのトラフィックが 1 つのリンク上で伝送されます。 パス コストを手動で設定することで、スイッチ スタック全体にわたりロード バランシングを実現できます。
- Per-VLAN Spanning-Tree Plus（PVST+）と MST クラウドの間、または Rapid- PVST+ と MST クラウドの間でロード バランシングが機能するためには、すべての MST 境界ポートがフォワーディングでなければなりません。 MST クラウドの内部スパニング ツリー（IST）マスターが共通スパニング ツリー（CST）のルートである場合、MST境界ポートはフォワーディングです。 MST クラウドが複数の MST リージョンから構成されている場合、いずれかの MST リージョンに CST ルートを含める必要があり、その他すべての MST リージョンに、PVST+ クラウドまたは高速 PVST+ クラウドを通るパスよりも、MST クラウド内に含まれるルートへのパスが良くする必要があります。 クラウド内のスイッチを手動で設定しなければならない場合もあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）
MSTP 設定時の注意事項, （286 ページ）
MST リージョン, （288 ページ）

MSTP の制約事項

- スイッチ スタックは最大 65 の MST インスタンスをサポートします。 特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。
- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは 1 つのバージョンだけです （たとえば、すべての VLAN で PVST+ を実行する、すべての VLAN で Rapid PVST+ を実行する、またはすべての VLAN で MSTP を実行します）。
- すべてのスタック メンバーは同一のスパニングツリー バージョンを実行する必要があります（すべての PVST+、Rapid PVST+、または MSTP）。
- MST コンフィギュレーションの VLAN トランキング プロトコル（VTP）伝搬はサポートされません。 ただし、コマンドライン インターフェイス（CLI）または簡易ネットワーク管理プロトコル（SNMP）サポートを通じて、MST リージョン内の各スイッチで MST コンフィギュレーション（リージョン名、リビジョン番号、およびVLANとインスタンスのマッピング）を手動で設定することは可能です。
- ネットワークを多数のリージョンに分割することは推奨できません。 ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。

- リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバーで構成されます。リージョンの各メンバーは高速スパニングツリー プロトコル（RSTP）ブリッジ プロトコルデータユニット（BPDU）を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリー インスタンスの数は 65 までです。 VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。
- スイッチをルート スイッチとして設定した後に、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定することは推奨できません。

表 *25*：***PVST+***、***MSTP***、***Rapid PVST+*** の相互運用性と互換性

	PVST+	**MSTP**	**Rapid PVST+**
PVST+	Yes	あり（制限あり）	あり（PVST+ に戻る）
MSTP	あり（制限あり）	Yes	あり（PVST+ に戻る）
Rapid PVST+	あり（PVST+ に戻る）	あり（PVST+ に戻る）	Yes

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）
MSTP 設定時の注意事項, （286 ページ）
MST リージョン, （288 ページ）
ルート スイッチの設定, （307 ページ）
ルート スイッチ, （287 ページ）
MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

MSTP について

MSTP の設定

高速コンバージェンスのために RSTP を使用する MSTP では、複数の VLAN をグループ化して同じスパニングツリーインスタンスにマッピングすることが可能で、多くの VLAN をサポートするのに必要なスパニングツリーインスタンスの数を軽減できます。 MSTP は、データ トラフィックに複数の転送パスを提供し、ロードバランシングを実現して、多数の VLAN をサポートするのに必要なスパニングツリー インスタンスの数を減らすことができます。 MSTP を使用すると、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）は影響を受けないので、ネットワークのフォールトトレランスが向上します。

（注） マルチ スパニングツリー（MST）実装は IEEE 802.1s 標準に準拠しています。

MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの導入です。 MSTP の導入により、サービス プロバイダー環境に求められる高可用性ネットワークを実現できます。

スイッチが MST モードの場合、IEEE 802.1w 準拠の RSTP が自動的にイネーブルになります。RSTP は、IEEE 802.1D の転送遅延を軽減し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行する明示的なハンドシェイクによって、スパニングツリーの高速コンバージェンスを実現します。

MSTP と RSTP は、既存のシスコ独自の Multiple Instance STP（MISTP）、および既存の Cisco PVST+ と Rapid Per-VLAN Spanning-Tree plux（Rapid PVST+）を使用して、スパニングツリーの動作を改善し、（オリジナルの）IEEE 802.1D スパニング ツリーに準拠した機器との下位互換性を保持しています。

スイッチスタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが同一のスイッチ ID を使用します。

MSTP 設定時の注意事項

- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して、MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- UplinkFast、BackboneFast、クロススタック UplinkFast の設定のガイドラインについては、関連項目のセクションの該当するセクションを参照してください。
- スイッチが MST モードの場合は、パス コスト値の計算に、ロング パス コスト計算方式（32 ビット）が使用されます。 ロング パス コスト計算方式では、次のパス コスト値がサポートされます。

速度	パス コスト値
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

MSTP の前提条件, （283 ページ）
MSTP の制約事項, （284 ページ）
スパニングツリーの相互運用性と下位互換性, （264 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast, （332 ページ）
UplinkFast, （330 ページ）

ルート スイッチ

スイッチは、マッピングされている VLAN グループのスパニングツリー インスタンスを保持しています。 スイッチ ID は、スイッチのプライオリティおよびスイッチの MAC アドレスで構成されており、各インスタンスに関連付けられます。 VLAN のグループでは、最小のスイッチ ID をもつスイッチがルート スイッチになります。

スイッチをルートとして設定する場合は、スイッチ プライオリティをデフォルト値（32768）からそれより大幅に低い値に変更し、スイッチが、指定したスパニング ツリーインスタンスのルート スイッチになるようにします。 このコマンドを入力すると、スイッチはルート スイッチのスイッチ プライオリティをチェックします。 拡張システム ID をサポートしているため、24576 という値でスイッチが指定したスパニングツリー インスタンスのルートとなる場合、そのスイッチは指定したインスタンスに対する自身のプライオリティを 24576 に設定します。

指定されたインスタンスのルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します （4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です）。 詳細については、関連項目の「Bridge ID, スイッチ Priority, and Extended System ID」リンクを参照してください。

ネットワークが、拡張システム ID をサポートするスイッチとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするスイッチがルート スイッチになる可能性は低くなります。 古いソフトウェアを実行している接続スイッチのプライオリティより VLAN 番号が大きい場合は常に、拡張システム ID によってスイッチ プライオリティ値が増加します。

各スパニングツリー インスタンスのルート スイッチは、バックボーンまたはディストリビューション スイッチでなければなりません。 アクセス スイッチをスパニングツリー プライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大スイッチ ホップ カウント）を指定するには、**diameter** キーワード（MST インスタンスが 0 の場合のみ使用できる）を指定します。 ネットワーク直径を指定すると、スイッチはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。 **hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

関連トピック

ルート スイッチの設定, （307 ページ）
MSTP の制約事項, （284 ページ）

ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （256 ページ）

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して矛盾のないようにスイッチを設定する必要があります。 同じ MST 設定の相互接続スイッチの集まりによって MST リージョンが構成されます。

MST 設定では、それぞれのスイッチが属する MST リージョンが制御されます。 この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。 その中で MST リージョンの設定を指定することにより、リージョンのスイッチを設定します。 MST インスタンスに VLAN をマッピングし、リージョン名を指定して、リビジョン番号を設定できます。 手順と例については、関連項目の「MST リージョンの設定の指定と MSTP のイネーブル化」リンクをクリックします。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。 さらに、各メンバは、RSTP ブリッジ プロトコル データ ユニット（BPDU）を処理できる必要があります。 ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は 65 までです。 インスタンスは、0 ～ 4094 の範囲の任意の番号で識別できます。 VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

関連トピック

MST リージョンの図, （291 ページ）

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

MSTP の前提条件, （283 ページ）

MSTP の制約事項, （284 ページ）

スパニングツリーの相互運用性と下位互換性, （264 ページ）

オプションのスパニングツリー設定時の注意事項

BackboneFast, （332 ページ）

UplinkFast, （330 ページ）

IST、CIST、CST

すべてのスパニングツリーインスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の 2 つのタイプのスパニングツリーを確立して保持しています。

- Internal Spanning-Tree（IST）は、1 つの MST リージョン内で稼働するスパニングツリーです。

  各 MST リージョン内の MSTP は複数のスパニングツリー インスタンスを維持しています。 インスタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。 その他すべての MSTI には、1 ～ 4094 の番号が付きます。

  IST は、BPDU を送受信する唯一のスパニングツリー インスタンスです。 他のスパニングツリーの情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されていま

す。 MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニングツリーインスタンスをサポートする処理が必要な BPDU の数を大幅に減少できます。

同一リージョン内の すべての MST インスタンスは同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポロジ パラメータ（ルート スイッチ ID、ルート パス コストなど）を持っています。 デフォルトでは、すべての VLAN が IST に割り当てられます。

MSTI はリージョンにローカルです。たとえばリージョン A およびリージョン B が相互接続されていても、リージョン A の MSTI 1 は、リージョン B の MSTI 1 に依存しません。

- Common and Internal Spanning-Tree（CIST）は、各 MST リージョン内の IST と、MST リージョンおよびシングル スパニングツリーを相互接続する Common Spanning-Tree（CST）の集合です。

  1 つのリージョン内で計算されたスパニングツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーと見なされます。 CIST は、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 標準をサポートするスイッチ間で実行されるスパニングツリーアルゴリズムによって形成されます。 MST リージョン内の CIST は、リージョン外の CST と同じです。

MST リージョン内の動作

IST は 1 つのリージョン内のすべての MSTP スイッチを接続します。 IST が収束すると、IST のルートは、CIST リージョナル ルート（IEEE 802.1s 標準が実装される以前は *IST* マスターと呼ばれた）になります。 これは、リージョン内で最も小さいスイッチ ID、および CIST ルートに対するパス コストをもつスイッチです。 ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。 CIST ルートがリージョンの外部にある場合、リージョンの境界に位置する MSTP スイッチの 1 つが CIST リージョナル ルートとして選択されます。

MSTP スイッチは初期化時に、自身が CIST のルートおよび CIST リージョナル ルートであることを主張するために CIST ルートと CIST リージョナル ルートへのパス コストがいずれもゼロに設定された BPDU を送信します。 スイッチはすべての MSTI を初期化し、そのすべてのルートであることを主張します。 スイッチは、ポート用に現在保存されているものより上位の MST ルート情報（低いスイッチ ID、低いパス コストなど）を受信した場合、CIST リージョナル ルートとしての主張を放棄します。

リージョンには、初期化中に多くのサブ リージョンが含まれて、それぞれに独自の CIST リージョナル ルートが含まれることがあります。 スイッチは、優位の IST 情報を受信すると、古いサブリージョンを脱退して、真の CIST リージョナル ルートが含まれている新しいサブリージョンに加入します。 真の CIST リージョナル ルートが含まれている以外のサブリージョンは、すべて縮小します。

正常な動作のためには、MST リージョン内のすべてのスイッチが同じ CIST リージョナル ルートを承認する必要があります。 共通の CIST リージョナル ルートに収束する場合、そのリージョン内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

関連トピック

MST リージョンの図, （291 ページ）

MST リージョン間の動作

ネットワーク内に複数のリージョンまたはレガシー IEEE 802.1D スイッチが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP スイッチから構成される CST を構築して保持します。 MSTI は、リージョンの境界にある IST と組み合わさり、CST になります。

IST はリージョン内のすべての MSTP スイッチを接続し、スイッチド ドメイン全体を囲む CIST のサブツリーとして認識されます。 サブツリーのルートは CIST リージョナル ルートです。 MST リージョンは、隣接する STP スイッチおよび MST リージョンへの仮想スイッチとして認識されます。

CST インスタンスのみが BPDU を送受信し、MST インスタンスはスパニングツリー情報を BPDU に追加して隣接するスイッチと相互作用し、最終的なスパニングツリー トポロジーを算出します。 したがって、BPDU 伝送に関連するスパニングツリー パラメータ（hello タイム、転送時間、最大エージング タイム、最大ホップ カウントなど）は、CST インスタンスだけで設定されますが、その影響はすべての MST インスタンスに及びます。 スパニングツリー トポロジに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンスと MST インスタンスの両方で設定できます。

MSTP スイッチは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、レガシー IEEE 802.1D スイッチと通信します。 MSTP スイッチは、MSTP BPDU を使用して MSTP スイッチと通信します。

関連トピック

MST リージョンの図, （291 ページ）

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部の MST 命名規則は、一部の内部パラメータまたはリージョンパラメータを識別するように変更されました。 これらのパラメータは、ネットワーク全体に関連している外部パラメータと違い、MST リージョン内でのみ影響があります。 CIST はネットワーク全体を網羅するスパニングツリーインスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル修飾子ではなく外部修飾子が必要です。

- CIST ルートは、ネットワーク全体を網羅する一意のインスタンスのためのルート スイッチです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。 このコストは MST 領域内で変化しません。 MST リージョンは、CIST への単一スイッチと見なすことに注意してください。 CIST 外部ルート パス コストは、これらの仮想スイッチ、およびどのリージョンにも属さないスイッチの間で算出されるルート パス コストです。
- CIST リージョナル ルートは、準規格の実装で IST マスターと呼ばれていました。 CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。 CIST ルートがリージョン内にない場合、CIST リージョナル ルートは、リージョン内の CIST ルートに最も近いスイッチです。 CIST リージョナル ルートは、IST のルート スイッチとして動作します。

- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。 このコストは、IST つまりインスタンス 0 だけに関連します。

表 *26*：準規格と規格の用語

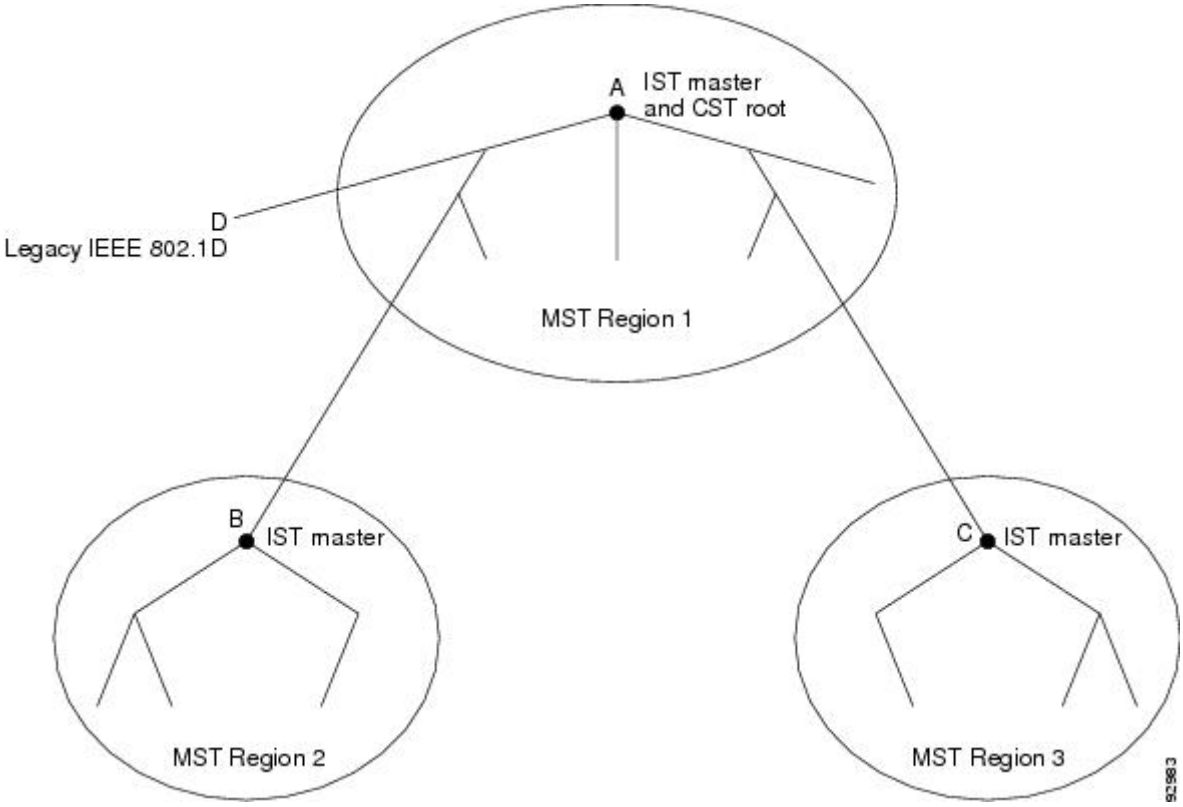
IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

MST リージョンの図

この図は、3 個の MST リージョンとレガシー IEEE 802.1D スイッチ（D）を示しています。 リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。 リージョン 2 の CIST

リージョナル ルート（B）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。 RSTP はすべてのリージョンで稼働しています。

図 *12*：***MST*** リージョン、***CIST*** マスター、および ***CST*** ルート



関連トピック

MST リージョン，（288 ページ）
MST リージョン内の動作，（289 ページ）
MST リージョン間の動作，（290 ページ）

ホップ カウント

IST および MST インスタンスは、スパニングツリー トポロジの計算に、コンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報を使用しません。 その代わりに、IP 存続可能時間（TTL）メカニズムに似た、ルートまでのパス コストおよびホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することにより、リージョン内の最大ホップを設定し、その値をリージョン内の IST インスタンスとすべての MST インスタンスに適用できます。 ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。 インスタンスのルート スイッチは、コストが 0 でホップ カウントが最大値に設定されている BPDU（M レコード）を常に送信します。 スイッチは、この BPDU を受信す

ると、受信した残りのホップカウントから1を引き、生成するBPDUで残りのホップカウントとしてこの値を伝播します。 カウントがゼロに達すると、スイッチはBPDUを廃棄し、ポート用に維持されている情報を期限切れにします。

BPDUのRSTP部分に格納されているメッセージ有効期間と最大エージングタイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTPが稼働する単一のスパニングツリー リージョン、PVST+またはRapid PVST+が稼働する単一のスパニングツリー リージョン、または異なるMSTコンフィギュレーションを持つ別のMSTリージョンにMSTリージョンを接続します。 境界ポートは、LAN、単一のスパニングツリー スイッチまたはMST設定が異なるスイッチの指定スイッチにも接続します。

IEEE 802.1s標準では、境界ポートの定義はなくなりました。 IEEE 802.1Q-2002標準では、ポートが受信できる2種類のメッセージを識別します。

- 内部（同一リージョンから）
- 外部（別のリージョンから）

メッセージが内部の場合、CISTの部分はCISTによって受信されるので、各MSTインスタンスは個々のMレコードだけを受信します。

メッセージが外部である場合、CISTだけが受信します。 CISTの役割がルートや代替ルートの場合、または外部BPDUのトポロジが変更された場合は、MSTインスタンスに影響する可能性があります。

MSTリージョンには、スイッチおよびLANの両方が含まれます。 セグメントは、DPのリージョンに属します。 そのため、セグメントの指定ポートではなく異なるリージョンにあるポートは境界ポートになります。 この定義では、リージョン内部の2つのポートが、別のリージョンに属するポートとセグメントを共有し、内部メッセージおよび外部メッセージの両方を1つのポートで受信できるようになります。

シスコ先行標準の実装との主な違いは、STP互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。

（注） レガシーSTPスイッチがセグメントに存在する場合、メッセージは常に外部と見なされます。

シスコ先行標準の実装から他に変更された点は、送信スイッチIDを持つRSTPまたはレガシーIEEE 802.1Qスイッチの部分に、CISTリージョナル ルート スイッチIDフィールドが加えられたことです。 リージョン全体は、一貫した送信者スイッチIDをネイバー スイッチに送信し、単一仮想スイッチのように動作します。 この例では、AまたはBがセグメントに指定されているかどうかに関係なく、ルートの一貫した送信者スイッチIDが同じであるBPDUをスイッチCが受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標準には含まれていない一部の（要望されている）先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的にMST標準に含まれませんでしたが、境界の概念自体はシスコの実装に投影されています。 ただし、リージョン境界にある MST インスタンスのポートは、対応する CIST ポートのステートに必ずしも従うわけではありません。 現在、2 つの境界の役割が存在しています。

- 境界ポートがCIST リージョナル ルートのルート ポートである場合：CISTインスタンス ポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わった後であれば（その後フォワーディングします）、その場合のみ合意を返信してフォワーディング ステートに移行できます。 MSTI ポートには、特別なマスターの役割があります。
- 境界ポートが CIST リージョナル ルートのルート ポートでない：MSTI ポートは、CIST ポートのステートおよび役割に従います。 標準では提供される情報が少ないため、MSTI ポートが BPDU（M レコード）を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかりにくい場合があります。 この場合、境界の役割自体は存在していませんが、**show** コマンドで見ると、出力される *type* カラムで、ポートが境界ポートとして認識されていることがわかります。

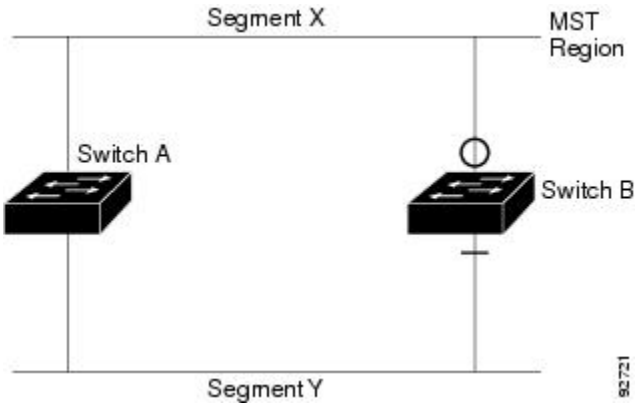
レガシーおよび規格スイッチの相互運用

準規格スイッチの自動検出はエラーになることがあるので、インターフェイス コンフィギュレーション コマンドを使用して準規格ポートを識別できます。 スイッチの規格と準規格の間にリージョンを形成することはできませんが、CIST を使用して相互運用することができます。 このような特別な方法を採用しても、失われる機能は、異なるインスタンス上のロード バランシングだけです。 ポートが先行標準の BPDU を受信すると、CLI（コマンドライン インターフェイス）にはポートの設定に応じて異なるフラグが表示されます。 スイッチが準規格 BPDU 送信用に設定されていないポートで準規格 BPDU を初めて受信したときは、Syslog メッセージも表示されます。

A が規格のスイッチで、B が準規格のスイッチとして、両方とも同じリージョンに設定されているとします。 A は CIST のルート スイッチ、B にはセグメント X にルート ポート（BX）、セグメント B に代替ポート（BY）があります。セグメント Y がフラップして BY のポートが代替になってから 1 つの準規格 BPDU を送信すると、準規格スイッチが Y に接続されていることを AY は検出できず、規格 BPDU の送信を続けます。 ポート BY は境界に固定され、A と B の間での

ロードバランスは不可能になります。セグメント X にも同じ問題がありますが、B はトポロジの変更を送信する場合があります。

図 *13*：規格および準規格のスイッチの相互運用



（注） 規格 MST 実装と準規格 MST 実装間の相互作用を最低限に抑えることを推奨します。

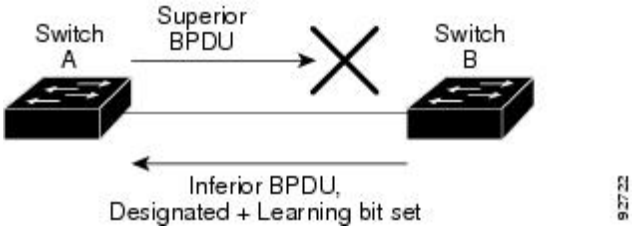
単一方向リンク障害の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフトウェアは、受信したBPDUでポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

指定ポートは、矛盾を検出すると、そのロールを維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジング ループを解決できるからです。

次の図に、ブリッジング ループの一般的な原因となる単方向リンク障害を示します。 スイッチ A はルート スイッチであり、スイッチ B へのリンクで BPDU は失われます。RSTP および MST BPDU には、送信側ポートの役割とステートが含まれます。 スイッチ A はこの情報を使用し、ルータ A が送信する上位 BPDU にスイッチ B が反応しないこと、およびスイッチ B がルート スイッチではなく指定ブリッジであることを検出できます。 この結果、スイッチ A は、そのポートをブロックし（またはブロックし続け）、ブリッジング ループが防止されます。

図 *14*：単一方向リンク障害の検出



IEEE 802.1D STP との相互運用性

MSTP が稼働しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。 このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。 また、MSTP スイッチは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、スイッチが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシースイッチが指定スイッチでない限り、レガシースイッチがリンクから削除されたかどうか検出できないためです。 このスイッチが接続するスイッチがリージョンに加入していると、スイッチはポートに境界の役割を割り当て続ける場合があります。 プロトコル移行プロセスを再開するには（強制的にネイバー スイッチと再びネゴシエーションするには）、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシー スイッチが RSTP スイッチであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。 したがって、MSTP スイッチは、バージョン 0 コンフィギュレーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで送信します。 境界ポートは、LAN、単一スパニングツリー スイッチまたは MST 設定が異なるスイッチのいずれかの指定のスイッチに接続します。

RSTP 概要

RSTP は、ポイントツーポイントの配線を利用して、スパニングツリーの高速コンバージェンスを実現します。 また、1 秒未満の間に、スパニングツリーを再構成できます（IEEE 802.1D スパニングツリーのデフォルトに設定されている 50 秒とは異なります）。

ポートの役割およびアクティブ トポロジー

RSTP は、ポートに役割を割り当てて、アクティブ トポロジを学習することによって高速コンバージェンスを実現します。 RSTP は スイッチ をルート スイッチとして最も高いスイッチ プライオリティ（プライオリティの数値が一番小さい）に選択するために、IEEE 802.1D STP 上に構築されます。 RSTP は、次のうちいずれかのポートのロールをそれぞれのポートに割り当てます。

- ルート ポート：スイッチ がルートスイッチ にパケットを転送するとき、最適なパス（最低コスト）を提供します。
- 指定ポート：指定スイッチに接続し、その LAN からルート スイッチにパケットを転送するとき、パス コストを最低にします。 DP は、指定スイッチが LAN に接続されているポートです。
- 代替ポート：現在のルート ポートが提供したパスに代わるルート スイッチへの代替パスを提供します。

- バックアップ ポート：指定ポートが提供した、スパニングツリーのリーフに向かうパスのバックアップとして機能します。 バックアップ ポートは、2 つのポートがループバック内でポイントツーポイント リンクによって接続されるか、共有 LAN セグメントとの複数の接続がスイッチにある場合に限って存在できます。
- ディセーブル ポート：スパニングツリーの動作において何も役割が与えられていません。

ルート ポートまたは指定ポートのロールを持つポートは、アクティブなトポロジに含まれます。代替ポートまたはバックアップポートのロールがあるポートは、アクティブ トポロジから除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTP は、すべてのルートポートおよび指定ポートがただちにフォワーディング ステートに移行し、代替ポートとバックアップ ポートが必ず廃棄ステート（IEEE 802.1D のブロッキング ステートと同じ）になるように保証します。 ポートのステートにより、転送処理および学習処理の動作が制御されます。

表 *27*：ポート ステートの比較

Operational Status	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	Blocking	廃棄	No
イネーブル	リスニング	廃棄	No
イネーブル	ラーニング	ラーニング	Yes
イネーブル	Forwarding	Forwarding	Yes
ディセーブル	ディセーブル	廃棄	No

Cisco STP の実装との一貫性を保つため、このマニュアルでは、ポート ステートを廃棄ではなくブロッキングとして定義します。 DP はリスニング ステートから開始します。

高速コンバージェンス

RSTP は、スイッチ、スイッチ ポート、LAN のうちいずれかの障害のあと、接続の高速回復を提供します。 エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- エッジ ポート：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して RSTP スイッチでエッジ ポートとしてポートを設定した場合、エッジ ポートはフォワーディング ステートにすぐに移行します。 エッジ ポートは Port Fast 対応ポートと同じであり、単一エンド ステーションに接続しているポートだけでイネーブルにする必要があります。

- ルート ポート：RSTP は、新しいルート ポートを選択した場合、古いルート ポートをブロックし、新しいルート ポートをフォワーディング ステートにすぐに移行します。
- ポイントツーポイント リンク：ポイントツーポイント リンクによってあるポートと別のポートを接続することでローカル ポートが指定ポートになると、提案合意ハンドシェイクを使用して他のポートと急速な移行がネゴシエートされ、トポロジにループがなくなります。

  スイッチ A がスイッチ B にポイントツーポイント リンクで接続され、すべてのポートはブロッキング ステートになっています。 スイッチ A のプライオリティがスイッチ B のプライオリティよりも数値的に小さいとします。スイッチ A は提案メッセージ（提案フラグを設定した設定 BPDU）をスイッチ B に送信し、指定スイッチとしてそれ自体を提案します。

  スイッチ B は、提案メッセージの受信後、提案メッセージを受信したポートを新しいルート ポートとして選択し、エッジ以外のすべてのポートを強制的にブロッキング ステートにして、新しいルート ポートを介して合意メッセージ（合意フラグを設定した BPDU）を送信します。

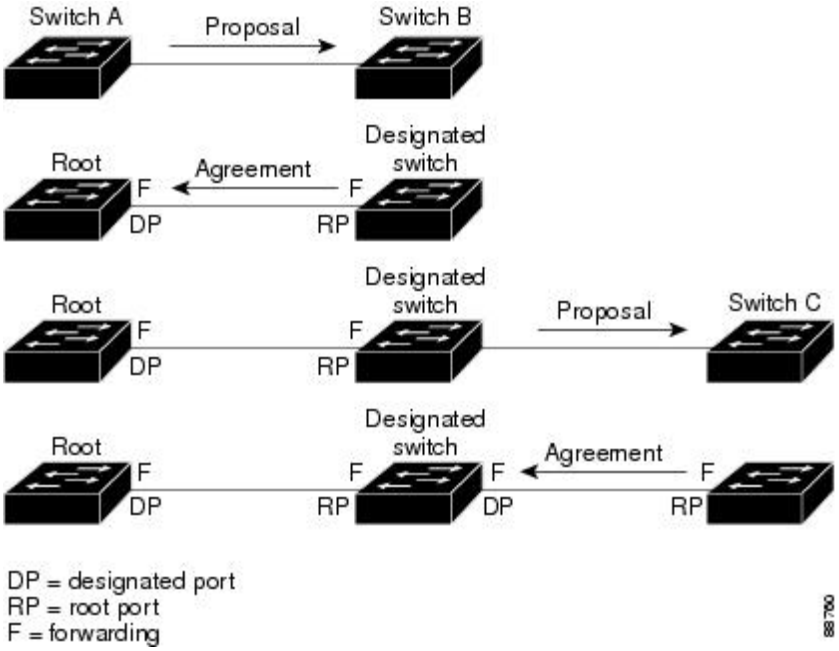
  スイッチ A も、スイッチ B の合意メッセージの受信後、指定ポートをフォワーディング ステートにすぐに移行します。 スイッチ B はすべてのエッジ以外のポートをブロックし、スイッチ A およびルータ B の間にポイントツーポイント リンクがあるので、ネットワークにループは形成されません。

  スイッチ C がスイッチ B に接続すると、同様のセットのハンドシェーク メッセージが交換されます。 スイッチ C はスイッチ B に接続されているポートをルート ポートとして選択し、両端がフォワーディング ステートにすぐに移行します。 このハンドシェーク処理を繰り返して、もう 1 つのスイッチがアクティブ トポロジーに加わります。 ネットワークが収束すると、この提案/合意ハンドシェイクがルートからスパニングツリーのリーフへと進みます。

  スイッチ スタックでは、Cross-Stack Rapid Transition（CSRT）機能を使用すると、ポートがフォワーディング ステートに移行する前に、スタック メンバで、提案/合意ハンドシェイク中にすべてのスタック メンバーから確認メッセージを受信できます。 スイッチが MST モードの場合、CSRT は自動的にイネーブルにされます。

  スイッチはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用すると、デュプレックス設定によって制御されるデフォルト設定を無効にすることができます。

図 *15*：高速コンバージェンスの提案と合意のハンドシェイク



ポート ロールの同期

スイッチがそのルータのポートの 1 つで提案メッセージを受信し、そのポートが新しいルートポートとして選択されると、RSTP によってその他すべてのポートが新しいルートの情報と強制的に同期化します。

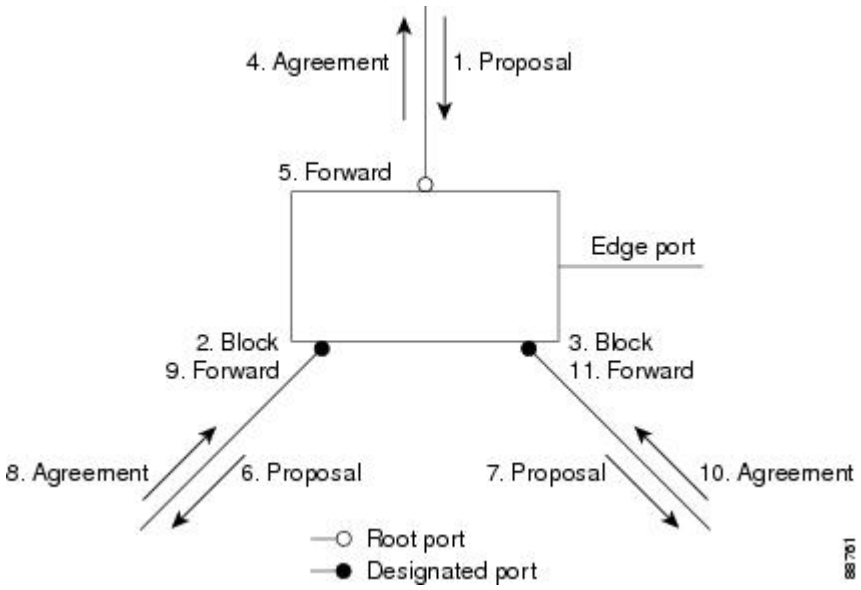
その他すべてのポートが同期化されている場合、スイッチはルート ポートで受信した上位ルート情報で同期化されます。 スイッチのそれぞれのポートは、次のような場合に同期化します。

- ポートがブロッキング ステートである。
- エッジ ポートである（ネットワークのエッジに存在するように設定されたポート）。

指定ポートがフォワーディング ステートでエッジ ポートとして設定されていない場合、RSTP によって新しいルート情報と強制的に同期されると、その指定ポートはブロッキング ステートに移行します。 一般的に RSTP がルート情報でポートを強制的に同期化し、ポートが上の条件を満たしていない場合、そのポート ステートはブロッキングに設定されます。

スイッチは、すべてのポートが同期化されたことを確認した後で、ルート ポートに対応する指定スイッチに合意メッセージを送信します。 ポイントツーポイントリンクで接続されたスイッチがポートの役割で合意すると、RSTP はポート ステートをフォワーディングにすぐに移行します。

図 *16*：高速コンバージェンス中のイベントのシーケンス



ブリッジ プロトコル データ ユニットの形式および処理

RSTP BPDU のフォーマットは、プロトコル バージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。 新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報がないことを示しています。

表 *28*：*RSTP BPDU* フラグ

ビット	機能
0	トポロジーの変化（TC）
1	提案
2 ～ 3: 00 01 10 11	ポートの役割： 不明（Unknown） Alternate port Root port Designated port
4	ラーニング

ビット	機能
5	Forwarding
6	合意
7	トポロジー変更確認応答（TCA）

送信側スイッチは RSTP BPDU の提案フラグを設定し、そのLAN の指定スイッチとして自分自身を提案します。 提案メッセージのポートの役割は、常に DP に設定されます。

送信側スイッチは、RSTP BPDU の合意フラグを設定して以前の提案を受け入れます。 合意メッセージ内のポート ロールは、常にルート ポートに設定されます。

RSTP には個別のトポロジ変更通知（TCN）BPDU はありません。 TC フラグが使用されて、TC が示されます。 ただし、IEEE 802.1D スイッチとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニング フラグおよびフォワーディング フラグは、送信側ポートのステートに従って設定されます。

優位 *BPDU* 情報の処理

ポートに現在保存されているルート情報よりも優位のルート情報（小さいスイッチ ID、低いパス コストなど）をポートが受け取ると、RSTP は再構成を開始します。 ポートが新しいルート ポートとして提案されて選択されると、RSTP は強制的にその他すべてのポートを同期化します。

受信した BPDU が、提案フラグが設定されている RSTP BPDU である場合、スイッチはその他すべてのポートが同期化されてから合意メッセージを送信します。 BPDU が IEEE 802.1D BPDU の場合、スイッチは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。 新しいルート ポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

ポートで優位の情報が受信されたために、そのポートがバックアップ ポートまたは代替ポートになる場合、RSTP はそのポートをブロッキング ステートに設定し、合意メッセージは送信しません。 DP は、転送遅延タイマーが失効するまで、提案フラグを設定して BPDU を送信し続け、転送遅延タイマーの失効時に、ポートはフォワーディング ステートに移行します。

下位 *BPDU* 情報の処理

指定ポートの役割を持つ下位BPDU（そのポートに現在保存されている値より大きいスイッチ ID、高いパス コストなど）を指定ポートが受信した場合、その指定ポートはただちに現在の自身の情報で応答します。

トポロジの変更

ここでは、スパニングツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出：IEEE 802.1D では、どのようなブロッキング ステートとフォワーディング ステートとの間の移行でもトポロジの変更が発生しますが、RSTP でトポロジの変更が発生するのは、

ブロッキング ステートからフォワーディング ステートに移行する場合だけです（トポロジの変更と見なされるのは、接続数が増加する場合だけです）。エッジポートにおけるステート変更は、TC の原因になりません。 RSTP スイッチは、TC を検出すると、TCN を受信したポートを除く、エッジ以外のすべてのポートで学習した情報を削除します。

- 通知：IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。 ただし、IEEE 802.1D との相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。
- 確認：RSTP スイッチは、指定ポートで IEEE 802.1D スイッチから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。 ただし、IEEE 802.1D スイッチに接続されたルート ポートで TC 時間タイマー（IEEE 802.1D のトポロジ変更タイマーと同じ）がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

  この処理は、IEEE 802.1D スイッチをサポートする目的でのみ必要とされます。 RSTP BPDU は TCA ビットが設定されていません。
- 伝播：RSTP スイッチは、DP またはルート ポートを介して別のスイッチから TC メッセージを受信すると、エッジ以外のすべての DP、およびルート ポート（TC メッセージを受信したポートを除く）に変更を伝播します。 スイッチはこのようなすべてのポートで TC-while タイマーを開始し、そのポートで学習した情報を消去します。
- プロトコルの移行：IEEE 802.1D スイッチとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU が送信される最低時間を指定）、RSTP BPDU が送信されます。 このタイマーがアクティブである間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコル タイプを無視します。

  スイッチはポートの移行遅延タイマーが満了した後に IEEE 802.1D BPDU を受信した場合、IEEE 802.1D スイッチに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。 ただし、RSTP スイッチが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了した後に RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用が開始されます。

プロトコル移行プロセス

MSTP が稼働しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。 このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。 また、MST スイッチは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RST BPDU（バージョン2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、スイッチが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシースイッチが指定スイッチでない限り、レガシースイッチがリンクから削

除されたかどうか検出できないためです。 また、接続するスイッチがリージョンに加入していると、スイッチはポートに境界の役割を割り当て続ける場合があります。

関連トピック

プロトコルの移行プロセスの再開, （323 ページ）

MSTP のデフォルト設定

表 *29* : ***MSTP*** のデフォルト設定

機能	デフォルト設定
スパニングツリー モード	MSTP
スイッチプライオリティ（CIST ポートごとに設定可能）	32768
スパニングツリー ポート プライオリティ（CIST ポート単位で設定可能）	128
スパニングツリー ポート コスト（CIST ポート単位で設定可能）	1000 Mb/s：20000 100 Mb/s：20000 10 Mb/s：20000 1000 Mb/s：20000 100 Mb/s：20000 10 Mb/s：20000
hello タイム	3 秒
転送遅延時間	20 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

関連トピック

サポートされるスパニングツリー インスタンス, （264 ページ）
MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

MSTP 機能の設定方法

MST リージョン設定の指定と MSTP のイネーブル化

2 つ以上のスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/インスタンスマッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

リージョンには、MST 設定が同一である、1 つ以上のメンバーを含めることができます。各メンバーでは、RSTP BPDU を処理できる必要があります。 ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は65までです。 VLAN には、一度に 1 つのスパニングツリーインスタンスのみ割り当てることができます。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst configuration**
4. **instance***instance-id* **vlan***vlan-range*
5. **name***name*
6. **revision***version*
7. **show pending**
8. **exit**
9. **spanning-tree mode mst**
10. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree mst configuration** 例： `Switch(config)# spanning-tree mst configuration`	MST コンフィギュレーション モードを開始します。
ステップ 4	**instance***instance-id***vlan***vlan-range* 例： `Switch(config-mst)# instance 1 vlan 10-20`	VLAN を MSTI にマップします。 • *instance-id* に指定できる範囲は、0 ～ 4094 です。 • **vlan***vlan-range* に指定できる範囲は、1 ～ 4094 です。 VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN の範囲を指定するには、ハイフンを使用します。たとえば **instance 1 vlan 1-63** では、VLAN 1 ～ 63 が MST インスタンス 1 にマップされます。 一連の VLAN を指定するには、カンマを使用します。たとえば **instance 1 vlan 10, 20, 30** と指定すると、VLAN 10、20、30 が MST インスタンス 1 にマップされます。
ステップ 5	**name***name* 例： `Switch(config-mst)# name region1`	コンフィギュレーション名を指定します。 *name* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。
ステップ 6	**revision***version* 例： `Switch(config-mst)# revision 1`	設定リビジョン番号を指定します。 指定できる範囲は 0 ～ 65535 です。
ステップ 7	**show pending** 例： `Switch(config-mst)# show pending`	保留中の設定を表示し、設定を確認します。
ステップ 8	**exit** 例： `Switch(config-mst)# exit`	すべての変更を適用し、グローバルコンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**spanning-tree mode mst** 例： `Switch(config)# spanning-tree mode mst`	MSTP をイネーブルにします。 RSTP もイネーブルになります。 スパニングツリー モードを変更すると、すべてのスパニングツリーインスタンスは以前のモードであるため停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。 MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 10	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MSTP 設定時の注意事項, （286 ページ）
MST リージョン, （288 ページ）
MSTP の前提条件, （283 ページ）
MSTP の制約事項, （284 ページ）
スパニングツリーの相互運用性と下位互換性, （264 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast, （332 ページ）
UplinkFast, （330 ページ）
MSTP のデフォルト設定, （303 ページ）
ルート スイッチの設定, （307 ページ）
MSTP の制約事項, （284 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （256 ページ）
セカンダリ ルート スイッチの設定, （308 ページ）
ポート プライオリティの設定, （309 ページ）
パス コストの設定, （312 ページ）
スイッチ プライオリティの設定, （313 ページ）
hello タイムの設定, （315 ページ）
転送遅延時間の設定, （316 ページ）
最大エージング タイムの設定, （318 ページ）
最大ホップ カウントの設定, （319 ページ）
高速移行を確実にするためのリンク タイプの指定, （320 ページ）

ネイバー タイプの設定, （321 ページ）
プロトコルの移行プロセスの再開, （323 ページ）

ルート スイッチの設定

この手順は任意です。

はじめる前に

マルチスパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。 この例のステップ 2 では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst***instance-id***root primary**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst***instance-id***root primary** 例： `Switch(config)# spanning-tree mst 0 root primary`	ルート スイッチとしてスイッチを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 指定できる範囲は 0 ～ 4094 です。

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

関連トピック

ルート スイッチ, （287 ページ）

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

MSTP の制約事項, （284 ページ）

ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （256 ページ）

セカンダリ ルート スイッチの設定, （308 ページ）

セカンダリ ルート スイッチの設定

拡張システム ID をサポートするスイッチをセカンダリ ルートとして設定する場合、スイッチ プライオリティはデフォルト値（32768）から 28672 に修正されます。 プライマリ ルート スイッチで障害が発生した場合は、このスイッチが指定インスタンスのルート スイッチになる可能性があります。 ここでは、その他のネットワーク スイッチが、デフォルトのスイッチ プライオリティの 32768 を使用しているためにルート スイッチになる可能性が低いことが前提となっています。

このコマンドを複数のスイッチに対して実行すると、複数のバックアップルートスイッチを設定できます。 **spanning-tree mst***instance-id***root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。 この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst***instance-id***root secondary**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst***instance-id***root secondary** 例： `Switch(config)# spanning-tree mst 0 root secondary`	セカンダリ ルート スイッチとしてスイッチを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 指定できる範囲は 0 ～ 4094 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）
ルート スイッチの設定, （307 ページ）

ポート プライオリティの設定

ループが発生した場合、MSTP はポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。 最初に選択されるインターフェイスには高いプライオリ

ティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てることができます。 すべてのインターフェイスに同じプライオリティ値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

（注） スイッチがスイッチ スタックのメンバーの場合、**spanning-tree mst** [*instance-id*] **port-priority***priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree mst** [*instance-id*] **cost***cost* インターフェイス コンフィギュレーション コマンドを使用し、フォワーディング ステートにするインターフェイスを選択する必要があります。 最初に選択させたいポートには、より小さいコスト値を割り当て、最後に選択させたいポートには、より大きいコスト値を割り当てることができます。 詳細については、関連項目の下に表示されるパス コストのトピックを参照してください。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。 この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree mst***instance-id***port-priority***priority*
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree mst***instance-id***port-priority***priority* 例： `Switch(config-if)# spanning-tree mst 0 port-priority 64`	ポート プライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 指定できる範囲は 0 ～ 4094 です。 • *priority* 値の範囲は 0 ～ 240 で、16 ずつ増加します。 デフォルト値は 128 です。 値が小さいほど、プライオリティが高くなります。 使用可能な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 だけです。 その他の値はすべて拒否されます。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-tree mstinterface*interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。 ポートがリンクアップ動作状態になっていない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認できます。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）
パス コストの設定, （312 ページ）

パス コストの設定

MSTP パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。 ループが発生した場合、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択します。 最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。 すべてのインターフェイスに同じコスト値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。 この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree mst***instance-id***cost***cost*
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートとポート チャネル論理インターフェイスがあります。 指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**spanning-tree mst***instance-id***cost***cost* 例： `Switch(config-if)# spanning-tree mst 0 cost 17031970`	コストを設定します。 ループが発生した場合、MSTP はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。 低いパス コストは高速送信を表します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 指定できる範囲は 0 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-tree mst interface*interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。 そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティの設定, （309 ページ）
MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

スイッチ プライオリティの設定

スイッチのプライオリティを変更すると、スタンドアロン スイッチまたはスタック内のスイッチであるかに関係なく、ルートスイッチとして選択される可能性が高くなります。

（注） このコマンドの使用には注意してください。 通常のネットワーク設定では、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** グローバル コンフィギュレーション コマンドを使用して、スイッチをルートまたはセカンダリ ルート スイッチとして指定することをお勧めします。 これらのコマンドが動作しない場合にのみスイッチプライオリティを変更する必要があります。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

使用する指定された MST インスタンス ID も把握する必要があります。 この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst** *instance-id* **priority** *priority*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **priority** *priority* 例： `Switch(config)# spanning-tree mst 0 priority 40960`	スイッチのプライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 指定できる範囲は 0 ～ 4094 です。

	コマンドまたはアクション	目的
		• *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。 この値が低いほど、スイッチがルート スイッチとして選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。 これらは唯一の許容値です。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

hello タイムの設定

hello タイムはルート スイッチによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst hello-time***seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst hello-time***seconds* 例： `Switch(config)# spanning-tree mst hello-time 4`	すべての MST インスタンスについて、hello タイムを設定します。 hello タイムはルート スイッチによって設定メッセージが生成されて送信される時間の間隔です。 このメッセージは、スイッチが活動中であることを表します。 *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 3 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

転送遅延時間の設定

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst forward-time***seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst forward-time***seconds* 例： `Switch(config)# spanning-tree mst forward-time 25`	すべての MST インスタンスについて、転送時間を設定します。 転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、ポートが待機する秒数です。 *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

最大エージング タイムの設定

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst max-age***seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst max-age***seconds* 例： `Switch(config)# spanning-tree mst max-age 40`	すべての MST インスタンスについて、最大経過時間を設定します。 最大エージング タイムは、スイッチが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

最大ホップ カウントの設定

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree mst max-hops***hop-count*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst max-hops***hop-count* 例： `Switch(config)# spanning-tree mst max-hops 25`	BPDU を廃棄してポート用に保持していた情報を期限切れにするまでの、リージョンでのホップ数を設定します。 *hop-count* に指定できる範囲は 1 ～ 255 です。デフォルト値は 20 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

高速移行を確実にするためのリンク タイプの指定

ポイントツーポイント リンクでポート間を接続し、ローカル ポートが DP になると、RSTP は提案と合意のハンドシェークを使用して別のポートと高速移行をネゴシエーションし、ループがないトポロジーを保証します。

デフォルトの場合、リンク タイプはインターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続、半二重ポートは共有接続と見なされます。 MSTP を実行しているリモート スイッチの単一ポートに、半二重リンクを物理的にポイントツーポイントで接続した場合は、リンク タイプのデフォルト設定を無効にして、フォワーディング ステートへの高速移行をイネーブルにすることができます。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。 この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree link-type point-to-point**
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイスコンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポート、VLAN、およびポートチャネル論理インターフェイスがあります。 VLAN ID の範囲は 1 ～ 4094 です。 指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**spanning-tree link-type point-to-point** 例： `Switch(config-if)# spanning-tree link-type point-to-point`	ポートのリンクタイプがポイントツーポイントであることを指定します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

ネイバー タイプの設定

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることができます。 デフォルトの場合、ポートは準規格デバイスを自動的に検出できますが、規格 BPDU および準規格 BPDU の両方を受信できます。 デバイスとそのネイバーの間に不一致がある場合は、CIST だけがインターフェイスで動作します。

準規格 BPDU だけを送信するようにポートを設定できます。 ポートが STP 互換モードになっていても、すべての **show** コマンドで準規格フラグが表示されます。

この手順は任意です。

はじめる前に

マルチスパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree mst pre-standard**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**spanning-tree mst pre-standard** 例： `Switch(config-if)# spanning-tree mst pre-standard`	ポートが準規格 BPDU だけを送信できることを指定します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）

プロトコルの移行プロセスの再開

この手順では、プロトコル移行プロセスを再開し、ネイバー スイッチとの再ネゴシエーションを強制します。 また、スイッチを MST モードに戻します。 これは、IEEE 802.1D BPDU の受信後にスイッチがそれらを受信しない場合に必要です。

スイッチでプロトコルの移行プロセスを再開する（隣接するスイッチで再ネゴシエーションを強制的に行う）手順については、これらの手順に従ってください。

はじめる前に

マルチ スパニングツリー（MST）が、スイッチで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

コマンドのインターフェイス バージョンを使用する場合は、使用する MST インターフェイスが分かっている必要があります。 この例では、インターフェイスとして GigabitEthernet1/0/1 を使用します。それが「関連項目」で示されている手順によって設定されたインターフェイスであるからです。

手順の概要

1. **enable**
2. 次のいずれかのコマンドを入力します。
   - **clear spanning-tree detected-protocols**
   - **clear spanning-tree detected-protocolsinterface***interface-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかのコマンドを入力します。 • **clear spanning-tree detected-protocols** • **clear spanning-tree detected-protocolsinterface***interface-id* 例： `Switch# clear spanning-tree detected-protocols`	スイッチが MSTP モードに戻り、プロトコルの移行プロセスが再開されます。

	コマンドまたはアクション	目的
	または `Switch# clear spanning-tree detected-protocols interface GigabitEthernet1/0/1`	

次の作業

この手順は、スイッチでさらにレガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定された BPDU）を受信する場合に、繰り返しが必要なことがあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化，（304 ページ）
プロトコル移行プロセス，（302 ページ）

MST の設定およびステータスのモニタリング

表 *30*：*MST* ステータスを表示するコマンド

show spanning-tree mst configuration	MST リージョンの設定を表示します。
show spanning-tree mst configuration digest	現在の MSTCI に含まれる MD5 ダイジェストを表示します。
このコマンドは、リンク アップ動作可能状態のポートの情報を表示します。	すべてのインスタンスの MST 情報を表示します。 （注） このコマンドは、リンク アップ動作可能状態のポートの情報を表示します。 このコマンドは、リンク アップ動作可能状態のポートの情報を表示します。
show spanning-tree mst*instance-id*	指定インスタンスの MST 情報を表示します。 （注） このコマンドは、ポートがリンク アップ動作可能状態の場合にのみ情報を表示します。
show spanning-tree mstinterface*interface-id*	指定インターフェイスの MST 情報を表示します。

MSTP の機能情報

リリース	変更内容
Cisco IOS 15.0(2)EX	この機能が導入されました。

第 14 章

オプションのスパニングツリー機能の設定

- 機能情報の確認，327 ページ
- オプションのスパニング ツリー機能の制約事項，327 ページ
- オプションのスパニングツリー機能について，328 ページ
- オプションのスパニングツリー機能の設定方法，337 ページ
- スパニングツリー ステータスのモニタリング，350 ページ

機能情報の確認

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

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

オプションのスパニング ツリー機能の制約事項

- PortFast は、スパニング ツリーがコンバージェンスするまでにインターフェイスが待機する時間を最短にするため、これはエンドステーションに接続されているインターフェイスで使用される場合のみ有用です。 他のスイッチに接続するインターフェイスで PortFast をイネーブルにすると、スパニングツリーのループが生じることがあります。

関連トピック

PortFast のイネーブル化，（337 ページ）

PortFast, （328 ページ）

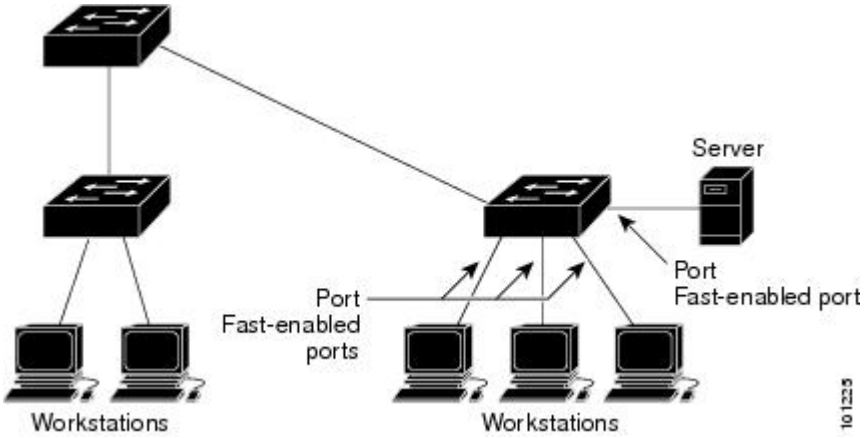
オプションのスパニングツリー機能について

PortFast

PortFast機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートから直接フォワーディング ステートに移行します。

1 台のワークステーションまたはサーバに接続されているインターフェイス上でPortFastを使用すると、スパニングツリーが収束するのを待たずにデバイスをすぐにネットワークに接続できます。

図 *17*：*PortFast* がイネーブルなインターフェイス



1 台のワークステーションまたはサーバに接続されたインターフェイスがブリッジ プロトコル データ ユニット（BPDU）を受信しないようにする必要があります。 スイッチを再起動すると、PortFast がイネーブルに設定されているインターフェイスは通常のスパニングツリー ステータスの遷移をたどります。

インターフェイスまたはすべての非トランク ポートでイネーブルにして、この機能をイネーブルにできます。

関連トピック

PortFast のイネーブル化, （337 ページ）

オプションのスパニング ツリー機能の制約事項, （327 ページ）

BPDU ガード

ブリッジ プロトコル データ ユニット（BPDU）ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

PortFast 対応ポート上でグローバル レベルで BPDU ガードをイネーブルにすると、スパニングツリーは、BPDU が受信されると、PortFast 動作ステートのポートをシャット ダウンします。 設定が有効であれば、PortFast 対応ポートは BPDU を受信しません。 PortFast 対応ポートが BPDU を受信した場合は、認可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは errdisable ステートになります。 この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

PortFast 機能もイネーブルにせずにインターフェイス レベルでポート上の BPDU ガードをイネーブルにした場合、ポートが BPDU を受信すると、errdisable ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。 サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

関連トピック

BPDU ガードのイネーブル化, （338 ページ）

BPDU フィルタリング

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルで PortFast がイネーブルなインターフェイス上の BPDU フィルタリングをイネーブルにすると、PortFast 動作状態にあるインターフェイスでの BPDU の送信または受信が防止されます。 ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。 これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。 BPDU を受信した PortFast がイネーブルなインターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

PortFast 機能をイネーブルにせずに、インターフェイスで BPDU フィルタリングをイネーブルにすると、インターフェイスでの BPDU の送信または受信が防止されます。

注意 BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチ全体または 1 つのインターフェイスで BPDU フィルタリング機能をイネーブルにできます。

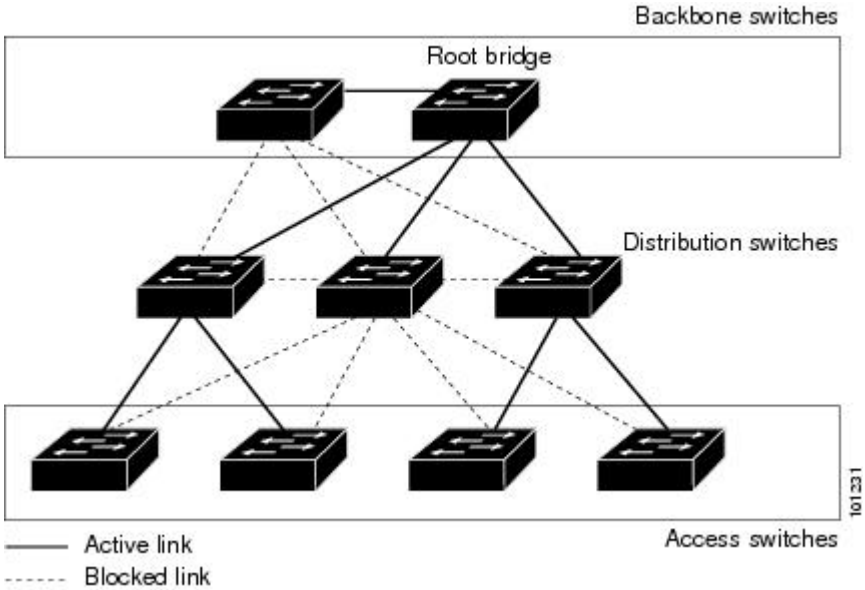
関連トピック

BPDU フィルタリングのイネーブル化, （340 ページ）

UplinkFast

階層型ネットワークに配置されたスイッチは、バックボーン スイッチ、ディストリビューション スイッチ、およびアクセス スイッチに分類できます。 この複雑なネットワークには、ディストリビューション スイッチとアクセス スイッチがあり、ループを防止するために、スパニング ツリーがブロックする冗長リンクが少なくとも 1 つあります。

図 *18*：階層型ネットワークのスイッチ



スイッチの接続が切断されると、スイッチはスパニングツリーが新しいルート ポートを選択すると同時に代替パスの使用を開始します。 リンクやスイッチに障害が発生した場合、またはスパニングツリーが UplinkFast のイネーブル化によって自動的に再設定された場合に、新しいルート ポートを短時間で選択できます。 ルート ポートは、通常のスパニングツリー手順とは異なり、リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

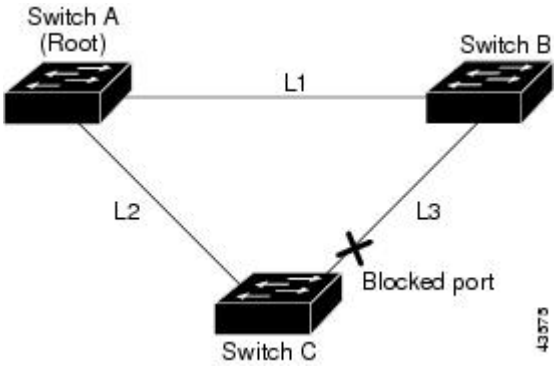
スパニングツリーが新規ルート ポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッディングし、インターフェイス上で学習した各アドレスにパケットを送信します。 max-update-rate パラメータの値を小さくすることで、これらのマルチキャスト トラフィックのバーストを制限できます（このパラメータはデフォルトで毎秒 150 パケットです）。 ただし、0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。

（注） UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのスイッチで非常に有効です。 バックボーン デバイスには適していません。 他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロード バランシングを実行します。 アップリンク グループは、（VLAN ごとの）レイヤ 2 インターフェイスの集合であり、いかなるときも、その中の 1 つのインターフェイスだけが転送を行います。 つまり、アップリンク グループは、（転送を行う）ルート ポートと、（セルフループを行うポートを除く）ブロックされたポートの集合で構成されます。 アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

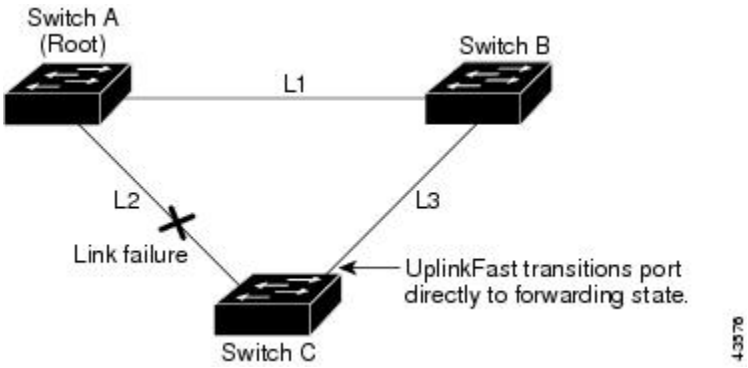
このトポロジにはリンク障害がありません。 ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。 スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 *19*：直接リンク障害が発生する前の *UplinkFast* の例



スイッチ C が、ルート ポートの現在のアクティブ リンクである L2 でリンク障害（直接リンク障害）を検出すると、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、直接フォワーディング ステートに移行させます。 この切り替えに必要な時間は、約 1 ～ 5 秒です。

図 *20*：直接リンク障害が発生したあとの *UplinkFast* の例



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （304 ページ）
MSTP 設定時の注意事項, （286 ページ）

MST リージョン, （288 ページ）
冗長リンクで使用するための UplinkFast のイネーブル化, （342 ページ）
高速コンバージェンスを発生させるイベント

BackboneFast

BackboneFastは、バックボーンのコアにおける間接障害を検出します。 BackboneFastは、UplinkFast機能を補完するテクノロジーです。UplinkFast は、アクセス スイッチに直接接続されたリンクの障害に対応します。 BackboneFast は、最大エージング タイマーを最適化します。最大エージングタイマーによって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御されます。 スイッチが別のスイッチの指定ポートから下位 BPDU を受信した場合、BPDUは他のスイッチでルートまでのパスが失われた可能性を示すシグナルとなり、BackboneFastはルートまでの別のパスを見つけようとします。

スイッチのルートポートまたはブロックされたインターフェイスが、指定スイッチから下位BPDUを受け取ると、BackboneFast が開始します。 下位 BPDU は、ルート ブリッジと指定スイッチの両方を宣言しているスイッチを識別します。 スイッチが下位 BPDU を受信した場合、そのスイッチが直接接続されていないリンク（間接リンク）で障害が発生したことを意味します（指定スイッチとルートスイッチ間の接続が切断されています）。 スパニングツリーのルールに従い、スイッチは最大エージング タイム（デフォルトは 20 秒）の間、下位 BPDU を無視します。

スイッチは、ルートスイッチへの代替パスの有無を判別します。 下位BPDUがブロックインターフェイスに到達した場合、スイッチ上のルート ポートおよび他のブロック インターフェイスがルート スイッチへの代替パスになります （セルフループ ポートはルート スイッチの代替パスとは見なされません）。 下位 BPDU がルート ポートに到達した場合には、すべてのブロック インターフェイスがルートスイッチへの代替パスになります。 下位BPDUがルートポートに到達し、しかもブロックインターフェイスがない場合、スイッチはルートスイッチへの接続が切断されたものと見なし、ルートポートの最大エージングタイムが経過するまで待ち、通常のスパニングツリー ルールに従ってルート スイッチになります。

スイッチが代替パスでルート スイッチに到達できる場合、スイッチはその代替パスを使用して、Root Link Query（RLQ）要求を送信します。 スイッチは、スタック メンバーがルート スイッチへの代替ルートを持つかどうかを学習するために、すべての代替パスにRLQ要求を送信し、ネットワーク内およびスタック内の他のスイッチからの RLQ 応答を待機します。 スイッチは、すべての代替パスにRLQ要求を送信し、ネットワーク内の他のスイッチからのRLQ応答を待機します。

スタック メンバが、ブロック インターフェイス上の非スタック メンバから RLQ 応答を受信し、その応答が他の非スタックスイッチ宛てのものであった場合、そのスタックメンバは、スパニングツリー インターフェイス ステートに関係なく、その応答パケットを転送します。

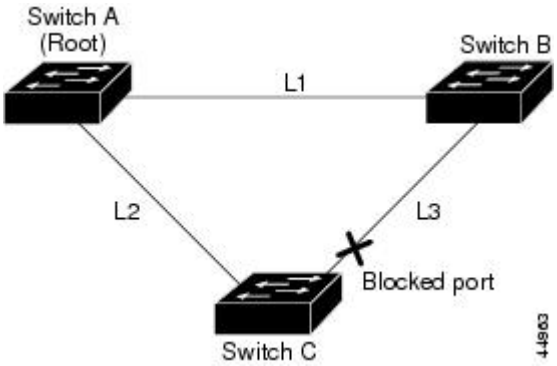
スタック メンバが非スタック メンバから RLQ 応答を受信し、その応答がスタック宛てのものであった場合、そのスタックメンバは、他のすべてのスタックメンバがその応答を受信するようにその応答を転送します。

ルートへの代替パスがまだ存在していると判断したスイッチは、下位 BPDU を受信したインターフェイスの最大エージング タイムが経過するまで待ちます。 ルート スイッチへのすべての代替パスが、スイッチとルート スイッチ間の接続が切断されていることを示している場合、スイッチは RLQ 応答を受信したインターフェイスの最大エージング タイムを満了させます。 1 つまたは

複数の代替パスからルート スイッチへ引き続き接続できる場合、スイッチは下位 BPDU を受信したすべてのインターフェイスを指定ポートにして、（ブロッキング ステートになっていた場合）ブロッキング ステートを解除し、リスニング ステート、ラーニング ステートを経てフォワーディング ステートに移行させます。

これは、リンク障害が発生していないトポロジー例です。 ルート スイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。 スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

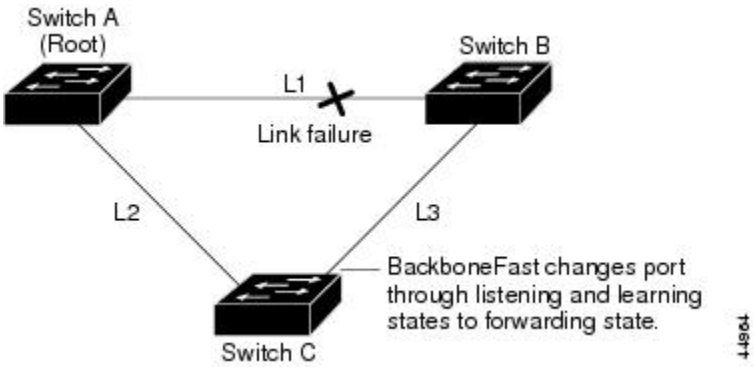
図 *21*：間接リンク障害が発生する前の *BackboneFast* の例



リンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、この障害を検出できません。 一方スイッチ B は、L1 によってルート スイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。 スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。 この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。 BackboneFast は、次に、スイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを提供します。ルートスイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に

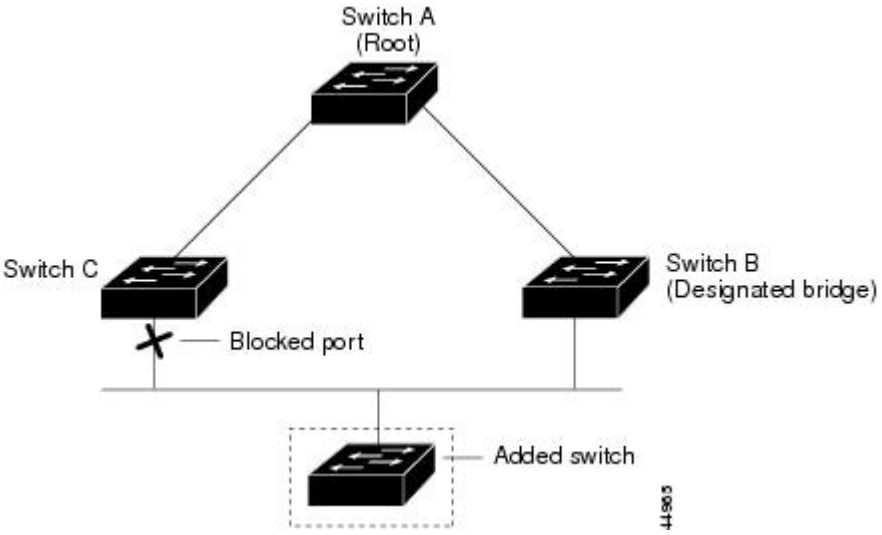
設定されていればその倍の時間です。 BackboneFast がリンク L1 で発生した障害に応じてトポロジーを再設定します。

図 *22*：間接リンク障害が発生したあとの ***BackboneFast*** の例



新しいスイッチがメディア共有型トポロジーに組み込まれた場合、認識された指定スイッチ（スイッチ B）から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。 新しいスイッチは、自身がルートスイッチであることを伝える下位 BPDU の送信を開始します。 ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルートスイッチであるスイッチ A への指定スイッチであることを学習します。

図 *23*：メディア共有型トポロジにおけるスイッチの追加



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化，（304 ページ）
MSTP 設定時の注意事項，（286 ページ）
MST リージョン，（288 ページ）
BackboneFast をイネーブル化，（345 ページ）

EtherChannel ガード

EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。 スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾が発生します。 また、EtherChannel の両端でチャネルのパラメータが異なる場合にも、設定の矛盾が発生します。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのインターフェイスを errdisable ステートにし、エラー メッセージを表示します。

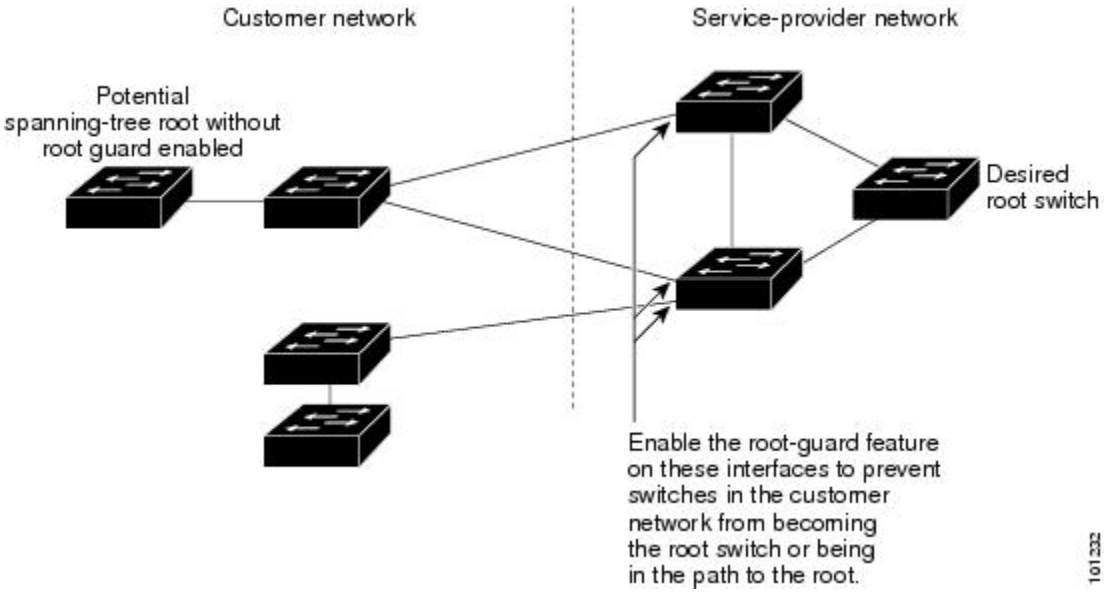
関連トピック

EtherChannel ガードのイネーブル化, （346 ページ）

ルート ガード

サービス プロバイダー（SP）のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多く含まれている場合があります。 このようなトポロジでは、スパニングツリーが再構成され、カスタマー スイッチをルート スイッチとして選択する可能性があります。 この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルート ガード機能をイネーブルに設定します。 スパニングツリーの計算によってカスタマー ネットワーク内のインターフェイスがルート ポートとして選択されると、ルート ガードがそのインターフェイスを root-inconsistent（ブロッキング）ステートにして、カスタマーのスイッチがルート スイッチにならないようにするか、ルートへのパスに組み込まれないようにします。

図 *24* : サービス プロバイダー ネットワークのルート ガード



SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ（root-inconsistent ステートになり）、スパニングツリーが新しいルート スイッチを選択します。カスタマーのスイッチがルート スイッチになることはありません。ルートへのパスに組み込まれることもありません。

スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定ポートにします。 また、境界ポートがルート ガードによって Internal Spanning-Tree（IST）インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インスタンスでもブロックされます。 境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。 VLAN は、MST インスタンスに対してグループ化された後、マッピングされます。

注意 ルート ガード機能を誤って使用すると、接続が切断されることがあります。

関連トピック

ルート ガードのイネーブル化, （347 ページ）

ループ ガード

ループ ガードを使用すると、代替ポートまたはルートポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。 この機能は、スイッチド ネットワーク全体でイネーブルにした場合に最も効果があります。 ループ ガードによって、代替ポートおよびルートポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルートポートまたは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされている場合でのみ、非境界ポートで BPDU を送信しません。境界ポートでは、ループ ガードがすべての MST インスタンスでインターフェイスをブロックします。

関連トピック

ループ ガードのイネーブル化, （349 ページ）

オプションのスパニングツリー機能の設定方法

PortFast のイネーブル化

PortFast機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、すぐにスパニングツリー フォワーディング ステートに移行されます。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。 音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

⚠

注意 PortFast を使用するのは、1 つのエンド ステーションがアクセス ポートまたはトランク ポートに接続されている場合に限定されます。 スイッチまたはハブに接続するインターフェイス上でこの機能をイネーブルにすると、スパニングツリーがネットワーク ループを検出または阻止できなくなり、その結果、ブロードキャスト ストームおよびアドレス ラーニングの障害が起きる可能性があります。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree portfast** [**trunk**]
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree portfast** [**trunk**] 例： `Switch(config-if)# spanning-tree portfast trunk`	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で PortFast をイネーブルにします。 **trunk** キーワードを指定すると、トランク ポート上で PortFast をイネーブルにできます。 （注） トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランク ポート上では機能しないためです。 トランク ポート上で PortFast をイネーブルにする場合は、事前に、トランク ポートとワークステーションまたはサーバの間にループがないことを確認してください。 デフォルトでは、PortFast はすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

次の作業

spanning-tree portfast default グローバル コンフィギュレーション コマンドを使用すると、すべての非トランク ポート上で PortFast 機能をグローバルにイネーブルにできます。

関連トピック

PortFast, （328 ページ）
オプションのスパニング ツリー機能の制約事項, （327 ページ）

BPDU ガードのイネーブル化

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU ガード機能をイネーブルにできます。

⚠

注意 PortFast は、エンド ステーションに接続するポートのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree portfast bpduguard default**
4. **interface***interface-id*
5. **spanning-tree portfast**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree portfast bpduguard default** 例： `Switch(config)# spanning-tree portfast bpduguard default`	BPDU ガードをグローバルにイネーブルにします。 BPDU ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	エンド ステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**spanning-tree portfast** 例： `Switch(config-if)# spanning-tree portfast`	PortFast 機能をイネーブルにします。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

次の作業

ポートのシャットダウンを防ぐには、**errdisable detect cause bpduguard shutdown vlan** グローバルコンフィギュレーションコマンドを使用すると、違反の発生時にポートで問題になっている VLAN のみをシャットダウンできます。

PortFast 機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにすることもできます。 BPDU を受信したポートは、errdisable ステートになります。

関連トピック

BPDU ガード, （328 ページ）

BPDU フィルタリングのイネーブル化

PortFast 機能をイネーブルにしなくても、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイスで BPDU フィルタリングをイネーブルにすることもできます。 このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。

注意 BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU フィルタリング機能をイネーブルにできます。

⚠

注意 PortFast は、エンド ステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree portfast bpdufilter default**
4. **interface***interface-id*
5. **spanning-tree portfast**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree portfast bpdufilter default** 例： `Switch(config)# spanning-tree portfast bpdufilter default`	BPDU フィルタリングをグローバルにイネーブルにします。 BPDU フィルタリングは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	エンド ステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**spanning-tree portfast** 例： `Switch(config-if)# spanning-tree portfast`	指定したインターフェイスで PortFast 機能をイネーブルにします。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

BPDU フィルタリング，（329 ページ）

冗長リンクで使用するための UplinkFast のイネーブル化

（注） UplinkFast をイネーブルにすると、スイッチまたはスイッチ スタックのすべての VLAN に影響します。 個々の VLAN について UplinkFast を設定することはできません。

Rapid PVST+ または MSTP に対して UplinkFast または Cross-Stack UplinkFast（CSUF）機能を設定できますが、この機能は、スパニングツリーのモードを PVST+ に変更するまではディセーブル（非アクティブ）になったままです。

この手順は任意です。 UplinkFast および CSUF をイネーブルにするには、次の手順に従います。

はじめる前に

スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにすることはできません。 スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにする場合は、最初に **no spanning-tree vlan***vlan-id***priority** グローバル コンフィギュレーション コマンドを使用することによって、VLAN のスイッチ プライオリティをデフォルト値に戻す必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree uplinkfast** [**max-update-rate***pkts-per-second*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree uplinkfast** [**max-update-rate***pkts-per-second*] 例： `Switch(config)# spanning-tree uplinkfast max-update-rate 200`	UplinkFast をイネーブルにします。 （任意）*pkts-per-second* に指定できる範囲は毎秒 0 ～ 32000 パケットです。デフォルト値は 150 です。 0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。 このコマンドを入力すると、すべての非スタック ポート インターフェイス上で CSUF もイネーブルになります。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティは 49152 に設定されます。 UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します（パス コストを 3000 以上の値に変更した場合、パスコストは変更されません）。スイッチプライオリティおよびパスコストを変更すると、スイッチがルート スイッチになる可能性が低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をイネーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにイネーブルになります。

関連トピック

UplinkFast, （330 ページ）
クロススタック UplinkFast
クロススタック UplinkFast の動作
高速コンバージェンスを発生させるイベント

UplinkFast のディセーブル化

この手順は任意です。

UplinkFast および Cross-Stack UplinkFast（SUF）をディセーブルにするには、次の手順に従います。

はじめる前に

UplinkFast を有効にする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **no spanning-tree uplinkfast**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree uplinkfast** 例： `Switch(config)# no spanning-tree uplinkfast`	スイッチおよびそのスイッチのすべての VLAN で UplinkFast および CSUF をディセーブルにします。

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

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をディセーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにディセーブルになります。

BackboneFast をイネーブル化

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニングツリーの再構成をより早く開始できます。

Rapid PVST+ または MSTP に対して BackboneFast 機能を設定できます。ただし、スパニングツリーモードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

この手順は任意です。 スイッチ上で BackboneFast をイネーブルにするには、次の手順に従います。

はじめる前に

BackboneFast を使用する場合は、ネットワーク上のすべてのスイッチでイネーブルする必要があります。 BackboneFast は、トークンリング VLAN ではサポートされません。 この機能は他社製スイッチでの使用にサポートされています。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree backbonefast**
4. **end**

手順の詳細

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

関連トピック

BackboneFast, （332 ページ）

EtherChannel ガードのイネーブル化

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、EtherChannel の設定の矛盾を検出する EtherChannel ガード機能をイネーブルにできます。

この手順は任意です。

スイッチで EtherChannel ガードをイネーブルにするには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **spanning-tree etherchannel guard misconfig**
4. **end**

手順の詳細

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

次の作業

show interfaces status err-disabled 特権 EXEC コマンドを使用することで、EtherChannel の設定矛盾が原因でディセーブルになっているスイッチ ポートを表示できます。 リモート デバイス上では、**show etherchannel summary** 特権 EXEC コマンドを使用して、EtherChannel の設定を確認できます。

設定を修正した後、誤って設定していたポート チャネル インターフェイス上で、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してください。

関連トピック

EtherChannel ガード, （335 ページ）

ルート ガードのイネーブル化

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。 UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。 UplinkFast を使用すると、障害発生時に

（ブロック ステートの）バックアップ インターフェイスがルート ポートになります。 ただし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。

（注） ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。

スイッチ上でルート ガードをイネーブルにするには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **spanning-tree guard root**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**spanning-tree guard root** 例： `Switch(config-if)# spanning-tree guard root`	インターフェイス上でルートガードをイネーブルにします。 デフォルトでは、ルートガードはすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

ルート ガード, （335 ページ）

ループ ガードのイネーブル化

ループガードを使用すると、代替ポートまたはルートポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチドネットワーク全体に設定した場合に最も効果があります。ループガードは、スパニングツリーがポイントツーポイントと見なすインターフェイス上でのみ動作します。

（注） ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。スイッチでループガードをイネーブルにするには、次の手順に従います。

手順の概要

1. 次のいずれかのコマンドを入力します。
   - **show spanning-tree active**
   - **show spanning-tree mst**
2. **configure terminal**
3. **spanning-tree loopguard default**
4. **end**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	次のいずれかのコマンドを入力します。
	• **show spanning-tree active**
	• **show spanning-tree mst**
	
	例：
	`Switch# show spanning-tree active`
	または
	`Switch# show spanning-tree mst`
		どのインターフェイスが代替ポートまたはルート ポートであるかを確認します。

ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree loopguard default** 例： `Switch(config)# spanning-tree loopguard default`	ループ ガードをイネーブルにします。 ループ ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ループ ガード, （336 ページ）

スパニングツリー ステータスのモニタリング

表 *31*：スパニングツリー ステータスをモニタリングするコマンド

コマンド	目的
show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。

コマンド	目的
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface*interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree mst interface*interface-id*	指定インターフェイスの MST 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。またはスパニングツリー ステート セクションのすべての行を表示します。

第 15 章

双方向フォワーディング検出の設定

- 機能情報の確認，353 ページ
- 双方向フォワーディング検出の前提条件，353 ページ
- 双方向フォワーディング検出の制約事項，354 ページ
- 双方向フォワーディング検出について，354 ページ
- 双方向フォワーディング検出の設定方法，359 ページ
- 双方向フォワーディング検出の設定例，374 ページ

機能情報の確認

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

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

双方向フォワーディング検出の前提条件

BFD の前提条件は次のとおりです。

- スイッチのフィーチャ セットは、IP Base またはそれ以上です。 IP Base フィーチャ セットは EIGRP スタブ ルーティングのみをサポートします。BFD は使用しません。 IP Service フィーチャ セットは BFD を使用して EIGRP をサポートします。
- IP ルーティングは、参加しているすべてのスイッチでイネーブルにする必要があります。

- BFD を導入する前に、BFD でサポートされる IP ルーティング プロトコルのいずれかをスイッチで設定しておくこと。 使用する予定のルーティング プロトコルの高速コンバージェンスを実装する必要があります。 高速コンバージェンスの設定については、お使いのバージョンの Cisco IOS ソフトウェアの IP ルーティングのマニュアルを参照してください。

双方向フォワーディング検出の制約事項

BFD の制約事項は次のとおりです。

- BFD は直接接続されたネイバーだけに対して動作します。 BFD のネイバーは 1 ホップ以内に限られます。 マルチホップのコンフィギュレーションはサポートされません。
- スイッチでは、最小 hello 間隔 100 ms、倍率 3 で最大 100 の BFD セッションがサポートされます。 この倍率は、セッションがダウンしたと宣言される前に失われた可能性のある連続するパケットの最小数を指定します。
- エコー モードをイネーブルにするには、ピア システムを no ip redirects コマンドで設定する必要があります。

双方向フォワーディング検出について

BFD の動作

BFD は、インターフェイス、データリンク、および転送プレーンを含めて、2 つの隣接ルータ間の転送パスで、オーバーヘッドの少ない短期間の障害検出方法を提供します。

BFD はインターフェイス レベルおよびルーティング プロトコル レベルでイネーブルにする検出プロトコルです。 シスコではBFD非同期モードをサポートしています。これは、ルータ間のBFDネイバー セッションをアクティブにして維持するための、2 台のシステム間の BFD 制御パケットの送信に依存します。 したがって、BFDセッションを作成するには、両方のシステムで（または BFD ピアで）BFD を設定する必要があります。 適切なルーティング プロトコルに対して、インターフェイス レベルおよびルータ レベルで BFD がイネーブルになっている場合、BFD セッションが作成されて BFD タイマーがネゴシエートされ、ネゴシエートされた間隔で BFD ピアが互いに BFD 制御パケットの送信を開始します。

シスコは、BFD エコー モードをサポートしています。 エコー パケットはフォワーディング エンジンによって送信され、検出を実行するために同じパスに沿って返信されます。 もう一方のBFDセッションは、エコー パケットの実際のフォワーディングに参加しません。

ここでは、次の内容について説明します。

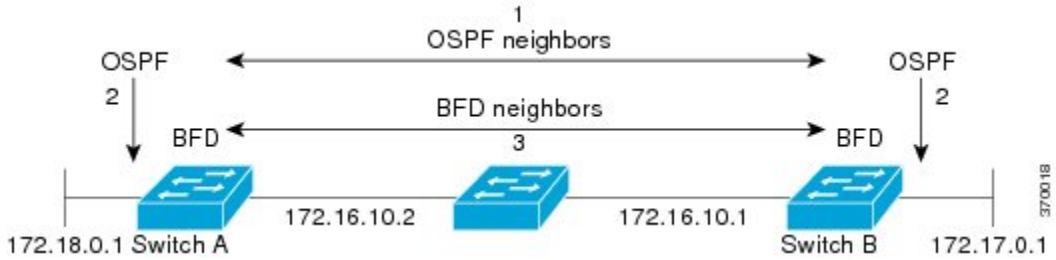
関連トピック

BFD エコー モードの設定, （371 ページ）
インターフェイスでの BFD セッション パラメータの設定, （359 ページ）
BFD のモニタリングとトラブルシューティング, （373 ページ）

ネイバー関係

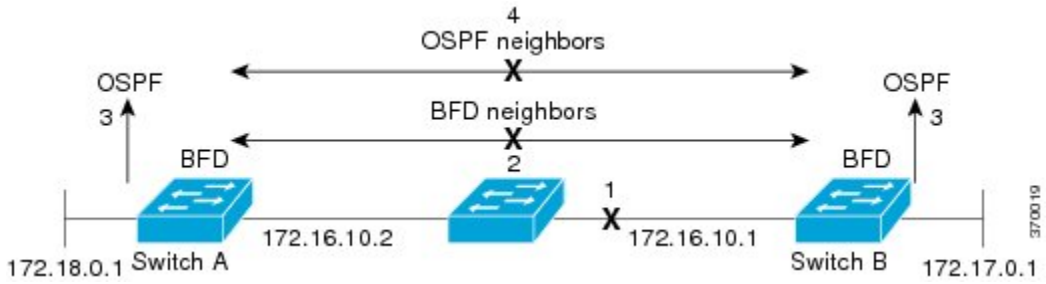
BFDはあらゆるメディアタイプ、カプセル化、トポロジ、ルーティングプロトコルBGP、EIGRP、IS-IS、およびOSPFの個別の高速BFDピア障害検出時間を提供します。 ローカル ルータのルーティングプロトコルに高速障害検出通知を送信して、ルーティングテーブル再計算プロセスを開始すると、BFDはネットワーク コンバージェンス時間全体を大幅に短縮できます。 下の図に、OSPFとBFDを実行する2台のルータがある単純なネットワークを示します。 OSPFがネイバー（1）を検出すると、OSPFネイバー ルータ（2）でBFDネイバー セッションを開始する要求が、ローカルBFDプロセスに送信されます。 OSPFネイバー ルータでのBFDネイバー セッションが確立されます（3）。

図 *25*：*BFD* ネイバー関係の確立



以下の図に、ネットワークで障害が発生した場合を示します（1）。 OSPFネイバー ルータでのBFDネイバー セッションが停止されます（2）。 BFDはローカルOSPFプロセスにBFDネイバーに接続できなくなったことを通知します（3）。 ローカルOSPFプロセスはOSPFネイバー関係を解除します（4）。 代替パスを使用できる場合、ルータはただちにコンバージェンスを開始します。

図 *26*：*OSPF* ネイバー関係の解除



ルーティングプロトコルでは、取得したネイバーそれぞれについて、BFDで登録する必要があります。 ネイバーが登録されると、セッションがまだ存在していない場合、BFDによって、ネイバーとのセッションが開始されます。

次のとき、OSPFでは、BFDを使用して登録が行われます。

- ネイバーの有限状態マシン（FSM）は、Fullステートに移行します。
- OSPF BFDとBFDの両方がイネーブルにされます。

ブロードキャスト インターフェイスでは、OSPF によって、指定ルータ（DR）とバックアップ指定ルータ（BDR）とともにのみ、BFD セッションが確立されますが、DROTHER ステートのすべての 2 台のルータ間では確立されません。

BFD の障害検出

BFD セッションが確立され、タイマーの取り消しが完了すると、BFD ピアは IGP hello プロトコルと同様に動作する（ただし、より高速な）、BFD 制御パケットを送信して状態を検出します。次の点に注意する必要があります。

- BFD はフォワーディング パスの障害検出プロトコルです。 BFD は障害を検出しますが、障害が発生したピアをバイパスするには、ルーティング プロトコルがアクションを実行する必要があります。
  - 通常、BFD はどのプロトコル レイヤでも使用できます。 ただし、シスコの BFD 実装では、特に BGP、EIGRP、IS-IS、および OSPF ルーティング プロトコル、およびスタティック ルーティングのレイヤ 3 クライアントだけがサポートされます。
- シスコの BFD 実装では、シスコ デバイスが複数のクライアント プロトコルに 1 つの BFD セッションを使用します。 たとえば、同じピアへの同じリンクを介してネットワークでOSPF および EIGRP を実行している場合、1 つの BFD セッションだけが確立され、BFD で両方のルーティング プロトコルとセッション情報を共有します。 ただし、IPv4 および IPv6 クライアントは BFD セッションを共有できません。

BFD バージョンの相互運用性

スイッチは、BFD バージョン 1 および BFD バージョン 0 をサポートします。 デフォルトでは、すべての BFD セッションがバージョン 1 で実行され、バージョン 0 と相互運用可能です。 システムで自動的に FD バージョン検出が実行される場合、ネイバー間の BFD セッションがネイバー間の最も一般的な BFD バージョンで実行されます。 たとえば、BFD ネイバーが BFD バージョン 0 を実行し、他の BFD ネイバーがバージョン 1 を実行している場合、セッションで BFD バージョン 0 が実行されます。 **showbfdneighbors** [**details**] コマンドの出力で、BFD ネイバーが実行している BFD バージョンを確認できます。

BFDバージョンの検出の例については、エコーモードがデフォルトでイネーブルになったEIGRPネットワークでの BFD の設定の例を参照してください。

関連トピック

例：エコー モードがデフォルトでイネーブルになった EIGRP ネットワークでの BFD の設定, (374 ページ)

BFD セッションの制限

作成できる BFD セッションの最小数は、「hello」間隔によって異なることがあります。 100 ms の「hello」間隔では、100 セッションが許可されます。 より大きい hello 間隔では、より多くのセッションが許可されます。 VLAN インターフェイスでは、最小「hello」間隔は 600 ms です。

非ブロードキャスト メディア インターフェイスに対する BFD サポート

BFD 機能はスイッチの VLAN インターフェイスでサポートされています。

bfd interval コマンドは、BFD モニタリングを開始するインターフェイスで設定する必要があります。

ステートフル スイッチオーバーでのノンストップ フォワーディングの BFD サポート

通常、ネットワーキングデバイスを再起動すると、そのデバイスのすべてのルーティング ピアがデバイスの終了および再起動を検出します。 この遷移によってルーティング フラップが発生し、そのために複数のルーティング ドメインに分散される可能性があります。 ルーティングの再起動によって発生したルーティング フラップによって、ルーティングが不安定になります。 これはネットワーク全体のパフォーマンスに悪影響を及ぼします。 ノンストップ フォワーディング（NSF）は、ステートフル スイッチオーバー（SSO）がイネーブルになっているデバイスのルーティング フラップを抑制するのに役立ち、それによってネットワークの不安定さが減少します。

NSF では、ルーティング プロトコル情報がスイッチオーバー後に保存されるとき、既知のルータでデータ パケットのフォワーディングを継続できます。 NSF を使用すると、ピア ネットワーキング デバイスでルーティング フラップが発生しません。 データ トラフィックはインテリジェント ラインカードまたはデュアル フォワーディング プロセッサを介して転送されますが、スタンバイ RP では、スイッチオーバー中に障害が発生したアクティブな RP からの制御と見なされます。 ラインカードおよびフォワーディング プロセッサの機能はスイッチオーバーによって維持され、アクティブな RP の転送情報ベース（FIB）が NSF 動作で最新状態が維持されます。

デュアル RP をサポートするデバイスでは、SSO が RP の 1 つをアクティブなプロセッサとして確立し、他の RP はスタンバイ プロセッサに割り当てられ、それらの間で情報が同期されます。 アクティブな RP に障害が発生したとき、ネットワーキング デバイスから削除されたとき、または手動でメンテナンスから排除されたときに、アクティブなプロセッサとスタンバイ プロセッサからのスイッチオーバーが発生します。

ステートフル スイッチオーバーの BFD サポート

BFD プロトコルでは、隣接するフォワーディング エンジン間でパスに短期間の障害検出が行われます。 デュアル RP スイッチ（冗長性のため）を使用するネットワーク導入では、スイッチにグレースフル リスタート メカニズムがあり、アクティブな RP とスタンバイ RP の間のスイッチオーバー時にフォワーディング状態が保護されます。

スタンバイ *RP* のステートフル *BFD*

スタンバイ RP へのスイッチオーバーを成功させるために、BFD プロトコルでチェックポイント メッセージを使用して、アクティブな RP Cisco IOS インスタンスからセッション情報をスタンバイ RP Cisco IOS インスタンスに送信します。 セッション情報には、ローカル識別子およびリモート識別子、隣接ルータのタイマー情報、BFD セットアップ情報、およびセッション固有の情報（セッションのタイプやセッションのバージョンなど）が含まれます。 さらに、BFD プロトコルはセッションの作成および削除のチェックポイント メッセージを送信して、スタンバイ RP でセッションを作成または削除します。

スタンバイ RP の BFD セッションはパケットの送受信を行わず、期限切れになったタイマーを処理しません。 このようなセッションは、スイッチオーバーの発生を待ってからアクティブ セッションのパケットを送信し、セッションが隣接スイッチでタイム アウトにならないようにします。

スタンバイ RP の BFD プロトコルはスイッチオーバーの通知を受けると、状態をアクティブに変更し、自分自身をシスコエクスプレスフォワーディングに登録することで、パケットを受信し、期限切れになったすべての要素にパケットを送信できるようにします。

また、BFD ではチェックポイント メッセージを使用して、アクティブな RP でクライアントによって作成されたセッションをスイッチオーバー時に維持します。 スイッチオーバーが発生すると、BFD は SSO 再要求タイマーを起動します。 クライアントは再要求タイマーによって指定された期間内のセッションを再要求する必要があります。そうしないと、セッションが削除されます。

タイマーの値は、BFD セッションの数およびプラットフォームによって異なります。

表 *32*：スイッチの *BFD* タイマー値

BFD セッションの最大数	BFD セッションタイプ	最小タイマー値（ms）	クライアント	注
100	非同期/エコー	100 x 3	すべて（All）	SSO スイッチでは、5 の倍数の使用が推奨されます。

スタティック ルーティングの BFD サポート

OSPF や BGP などの動的なルーティング プロトコルとは異なり、スタティック ルーティングにはピア検出の方法がありません。 したがって、BFD が設定されると、ゲートウェイの到達可能性は完全に指定されたネイバーへの BFD セッションの状態に依存します。 BFD セッションが開始されない限り、スタティック ルートのゲートウェイは到達不能と見なされ、したがって、影響を受けるルートが適切なルーティング情報ベース（RIB）にインストールされません。

BFD セッションが正常に確立されるように、ピア上のインターフェイスで BFD を設定し、ピア上の BFD クライアントに BFD ネイバーのアドレスを登録する必要があります。 インターフェイスがダイナミック ルーティング プロトコルで使用される場合、後者の要件は通常、BFD の各ネイバーでルーティング プロトコル インスタンスを設定することによって満たされます。 インターフェイスがスタティック ルーティングに排他的に使用される場合、この要件はピア上でスタティック ルートを設定することによって満たす必要があります。

BFD セッションが起動状態のときに BFD 設定がリモート ピアから削除された場合、BFD セッションの最新状態がスタティック スタティックに送信されません。 その結果、スタティック ルートが RIB に残ります。 唯一の回避策は、IPv4 スタティック BFD ネイバー設定を削除して、スタティック ルートが BFD セッション状態を追跡しないようにすることです。

関連トピック

例：スタティック ルーティングに対する BFD サポートの設定, （383 ページ）

障害検出に BFD を使用することの利点

機能を導入するときは、あらゆる代替策を検討し、トレードオフに注意することが重要です。

EIGRP、BGP、および OSPF の通常の導入で BFD に最も近い代替策は、EIGRP、BGP、および OSPF ルーティング プロトコルの変更された障害検出メカニズムを使用することです。

EIGRP の hello およびホールド タイマーを絶対最小値に設定する場合、EIGRP の障害検出速度が 1～2 秒程度に下がります。

BGP または OSPF に fast hello を使用する場合、これらの Interior Gateway Protocol（IGP）プロトコルによって障害検出メカニズムが最小 1 秒に減少します。

ルーティング プロトコルの減少したタイマー メカニズムで BFD を実装すると、いくつかの利点があります。

- EIGRP、BGP、および OSPF タイマーによって 1 秒または 2 秒の最小検出タイマーを実現できますが、障害検出が 1 秒未満になる場合もあります。
- BFD は特定のルーティング プロトコルに関連付けられていないため、EIGRP、BGP、および OSPF の汎用の整合性のある障害検出メカニズムとして使用できます。
- BFD の一部をデータ プレーンに分散できるため、コントロール プレーンに全体が存在する分散 EIGRP、BGP、および OSPF タイマーよりも CPU の負荷を軽くすることができます。

双方向フォワーディング検出の設定方法

インターフェイスで BFD を設定して、BFD プロセスを開始します。 BFD プロセスが開始されると、隣接するデータベースにエントリが作成されません。つまり、BFD 制御パケットが送受信されません。 BFD バージョン 1 でサポートされる BFD エコー モード。

BFD 制御パケットに加えて、BFD エコー パケットが送受信されます。 適用可能なルーティング プロトコルの BFD サポートを設定すると、隣接作成が実行されます。 ここでは、次の手順について説明します。

インターフェイスでの BFD セッション パラメータの設定

この手順では、インターフェイスで基本 BFD セッション パラメータを設定することによって、インターフェイスで BFD を設定する方法を示します。 BFD ネイバーに対して BFD セッションを実行するインターフェイスごとに、この手順を繰り返します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Switch(config)# interface GigabitEthernet 6/1`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。

ステップ 4	**bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier*
	
	例：
	`Switch(config-if)# bfd interval 50 min_rx 50 multiplier 5`
	`Switch(config-if)# no bfd echo`
		インターフェイスで BFD をイネーブルにします。
		ハードウェア オフロードをイネーブルにするために、BFD エコー モードをディセーブルにします。

関連トピック

BFD エコー モードの設定，（371 ページ）
EIGRP に対する BFD サポートの設定，（362 ページ）
BGP に対する BFD サポートの設定，（361 ページ）
BFD の動作，（354 ページ）
OSPF に対する BFD サポートの設定，（364 ページ）
1 つ以上のインターフェイスの OSPF に対する BFD サポートの設定，（367 ページ）
BFD のモニタリングとトラブルシューティング，（373 ページ）
すべてのインターフェイスの OSPF に対する BFD サポートの設定，（365 ページ）

ダイナミック ルーティング プロトコルに対する BFD サポートの設定

ルータ レベルでダイナミック ルーティング プロトコルの BFD サポートをイネーブルにして、すべてのインターフェイスに対してグローバルに BFD サポートをイネーブルにするか、またはインターフェイス レベルでインターフェイスごとに BFD を設定することができます。

ここでは、次の手順について説明します。

BGP に対する BFD サポートの設定

ここでは、BGP が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、BGP に対する BFD サポートを設定する手順について説明します。

はじめる前に

BGP は、参加しているすべてのスイッチで実行されている必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでのBFDセッション パラメータの設定」の項を参照してください。

（注） **showbfdneighborsdetails** コマンドの出力には、設定された間隔が表示されます。ハードウェアオフロードされた BFD セッションが 50 ms の倍数でない Tx および Rx 間隔で設定されていたために変更された間隔は出力に表示されません。

手順の概要

1. **enable**
2. **configureterminal**
3. **routerbgp***as-tag*
4. **neighbor***ip-address***fall-overbfd**
5. **end**
6. **showbfdneighbors**[**details**]
7. **showipbgpneighbor**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**routerbgp***as-tag* 例： `Switch(config)# router bgp tag1`	BGP プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor***ip-address***fall-overbfd** 例： `Switch(config-router)# neighbor 172.16.10.2 fall-over bfd`	フェールオーバーに対する BFD サポートをイネーブルにします。
ステップ 5	**end** 例： `Switch(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**showbfdneighbors**[**details**] 例： `Switch# show bfd neighbors detail`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されることを確認します。
ステップ 7	**showipbgpneighbor** 例： `Switch# show ip bgp neighbor`	（任意）ネイバーへの BGP および TCP 接続についての情報を表示します。

関連トピック

インターフェイスでの BFD セッション パラメータの設定，（359 ページ）
BFD のモニタリングとトラブルシューティング，（373 ページ）
すべてのインターフェイスの OSPF に対する BFD サポートの設定，（365 ページ）

EIGRP に対する BFD サポートの設定

ここでは、EIGRP が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、EIGRP に対する BFD サポートを設定する手順について説明します。 EIGRP に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して、EIGRP がルーティングしているすべてのインターフェイスに対して BFD をイネーブルにできます。

- ルータ コンフィギュレーション モードで **bfdinterface***typenumber* コマンドを使用して、EIGRP がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

はじめる前に

EIGRP は、関連するすべてのスイッチで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。 詳細については、「インターフェイスでの BFD セッション パラメータの設定」を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **routereigrp***as-number*
4. 次のいずれかを実行します。
   - **bfdall-interfaces**
   - **bfdinterface***typenumber*
5. **end**
6. **showbfdneighbors**[**details**]
7. **showipeigrpinterfaces** [*typenumber*] [*as-number*] [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**routereigrp***as-number* 例： `Switch(config)# router eigrp 123`	EIGRP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを実行します。
	• **bfdall-interfaces**
	• **bfdinterface***typenumber*
	
	例：
	`Switch(config-router)# bfd all-interfaces`
	
	例：
	`Switch(config-router)# bfd interface FastEthernet 6/1`
		EIGRP ルーティング プロセスに関連付けられたすべてのインターフェイスで、BFD をグローバルにイネーブルにします。
		または
		EIGRP ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルにします。

ステップ 5	**end** 例： `Switch(config-router) end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**showbfdneighbors**[**details**] 例： `Switch# show bfd neighbors details`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティングプロトコルが表示されることを確認します。
ステップ 7	**showipeigrpinterfaces** [*typenumber*] [*as-number*] [**detail**] 例： `Switch# show ip eigrp interfaces detail`	（任意）EIGRP に対する BFD サポートがイネーブルになっているインターフェイスを表示します。

関連トピック

OSPF に対する BFD サポートの設定，（364 ページ）
インターフェイスでの BFD セッション パラメータの設定，（359 ページ）
BFD のモニタリングとトラブルシューティング，（373 ページ）
すべてのインターフェイスの OSPF に対する BFD サポートの設定，（365 ページ）

OSPF に対する BFD サポートの設定

ここでは、OSPF が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、OSPF に対する BFD サポートを設定する手順について説明します。 すべてのイン

ターフェイスでグローバルに OSPF に対する BFD を設定するか、または 1 つ以上のインターフェイスで選択的に設定することができます。

OSPF に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して、OSPF がルーティングしているすべてのインターフェイスに対して BFD をイネーブルにできます。 インターフェイス コンフィギュレーション モードで **ipospfbfd** [**disable**] コマンドを使用して、個々のインターフェイスで BFD をディセーブルにできます。
- インターフェイス コンフィギュレーション モードで **ipospfbfd** コマンドを使用して、OSPF がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

OSPF に対する BFD サポートのタスクについては、次の項を参照してください。

関連トピック

EIGRP に対する BFD サポートの設定, （362 ページ）
インターフェイスでの BFD セッション パラメータの設定, （359 ページ）
BFD のモニタリングとトラブルシューティング, （373 ページ）
すべてのインターフェイスの OSPF に対する BFD サポートの設定, （365 ページ）

すべてのインターフェイスの *OSPF* に対する *BFD* サポートの設定

すべての OSPF インターフェイスに BFD を設定するには、この項の手順に従います。

すべての OSPF インターフェイスに対して BFD を設定するのではなく、特定の 1 つ以上のインターフェイスに対して BFD サポートを設定する場合は、「Configuring OSPF Support for BFD over IPv4 for One or More Interfaces」の項を参照してください。

はじめる前に

OSPF は、参加しているすべてのスイッチで実行されている必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。 詳細については、「インターフェイスでの BFD セッション パラメータの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **switchospf***process-id*
4. **bfdall-interfaces**
5. **end**
6. **showbfdneighbors**[**details**]
7. **showiospf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**switchospf***process-id* 例： `Switch(config)# router ospf 4`	OSPF プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**bfdall-interfaces** 例： `Switch(config-router)# bfd all-interfaces`	OSPF ルーティング プロセスに関連付けられたすべてのインターフェイスで、BFD をグローバルにイネーブルにします。
ステップ 5	**end** 例： `Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、デバイスが特権 EXEC モードに戻ります。
ステップ 6	**showbfdneighbors**[**details**] 例： `Switch# show bfd neighbors detail`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されるかどうかの検証に使用できる情報を表示します。
ステップ 7	**showipospf** 例： `Switch# show ip ospf`	（任意）OSPF に対して BFD がイネーブルになっているかどうかを検証するために使用できる情報を表示します。

関連トピック

OSPF に対する BFD サポートの設定，（364 ページ）
インターフェイスでの BFD セッション パラメータの設定，（359 ページ）

EIGRP に対する BFD サポートの設定, （362 ページ）
BGP に対する BFD サポートの設定, （361 ページ）
1 つ以上のインターフェイスの OSPF に対する BFD サポートの設定, （367 ページ）

1 つ以上のインターフェイスの *OSPF* に対する *BFD* サポートの設定

すべての OSPF インターフェイスに BFD を設定するには、この項の手順に従います。

すべての OSPF インターフェイスに対して BFD を設定するのではなく、特定の 1 つ以上のインターフェイスに対して BFD サポートを設定する場合は、「Configuring OSPF Support for BFD over IPv4 for One or More Interfaces」の項を参照してください。

はじめる前に

OSPF は、参加しているすべてのスイッチで実行されている必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでのBFDセッション パラメータの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **ipospfbfd**[**disable**]
5. **end**
6. **showbfdneighbors**[**details**]
7. **showipospf**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface***typenumber* 例： `Switch(config)# interface fastethernet 6/1`	（任意）インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipospfbfd**[**disable**] 例： `Switch(config-if)# ip ospf bfd`	（任意）OSPF ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルまたはディセーブルにします。 （注） ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して OSPF が関連付けられたすべてのインターフェイスで BFD をイネーブルにした場合にだけ、**disable** キーワードを使用する必要があります。
ステップ 5	**end** 例： `Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、デバイスが特権 EXEC モードに戻ります。
ステップ 6	**showbfdneighbors**[**details**] 例： `Switch# show bfd neighbors detail`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されるかどうかの検証に使用できる情報を表示します。
ステップ 7	**showipospf** 例： `Switch# show ip ospf`	（任意）OSPF に対して BFD がイネーブルになっているかどうかを検証するために使用できる情報を表示します。

関連トピック

インターフェイスでの BFD セッション パラメータの設定，（359 ページ）
BFD のモニタリングとトラブルシューティング，（373 ページ）
すべてのインターフェイスの OSPF に対する BFD サポートの設定，（365 ページ）

スタティック ルーティングに対する BFD サポートの設定

スタティック ルーティングのための BFD サポートを設定するには、このタスクを実行します。各 BFD ネイバーに対してこの手順を繰り返します。 詳細については、「例：スタティック ルーティングのための BFD サポートの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **no switchport**
5. **ipaddress***ip-addressmask*
6. **bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier*
7. **exit**
8. **iproutestaticbfd***interface-typeinterface-numberip-address* [**group***group-name* [**passive**]]
9. **iproute** [**vrf***vrf-name*] *prefixmask* {*ip-address* | *interface-typeinterface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name***next-hop-name*] [**permanent** | **track***number*] [**tag***tag*]
10. **exit**
11. **showipstaticroute**
12. **showipstaticroutebfd**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Switch(config)# interface gigabitethernet 6/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**no switchport** 例： `Switch(config)# no switchport`	レイヤ 3 にインターフェイスを変更します。
ステップ 5	**ipaddress***ip-addressmask* 例： `Switch(config-if)# ip address 10.201.201.1 255.255.255.0`	インターフェイスに IP アドレスを設定します。
ステップ 6	**bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier* 例： `Switch(config-if)# bfd interval 500 min_rx 500 multiplier 5`	インターフェイスで BFD をイネーブルにします。
ステップ 7	**exit** 例： `Switch(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**iproutestaticbfd***interface-typeinterface-numberip-address* [**group***group-name* [**passive**]] 例： `Switch(config)# ip route static bfd serial 2/0 10.1.1.1 group group1 passive`	スタティック ルートの BFD ネイバーを指定します。 • BFD が直接接続されたネイバーだけでサポートされているため、*interface-type*、*interface-number*、および *ip-address* 引数は必須です。
ステップ 9	**iproute** [**vrf***vrf-name*] *prefixmask* {*ip-address* | *interface-typeinterface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name***next-hop-name*] [**permanent** | **track***number*] [**tag***tag*] 例： `Switch(config)# ip route 10.0.0.0 255.0.0.0 Gi6/1 10.201.201.2`	スタティック ルートの BFD ネイバーを指定します。
ステップ 10	**exit** 例： `Switch(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**showipstaticroute** 例： `Switch# show ip static route`	（任意）スタティック ルート データベース情報を表示します。
ステップ 12	**showipstaticroutebfd** 例： `Switch# show ip static route bfd`	（任意）設定された BFD グループおよび non-group エントリからスタティック BFD の設定に関する情報を表示します。

BFD エコー モードの設定

デフォルトではBFDエコーモードがイネーブルになっていますが、方向ごとに個別に実行できるように、ディセーブルにすることもできます。

BFD エコー モードは非同期 BFD で動作します。 エコー パケットはフォワーディング エンジンによって送信され、検出を実行するために、同じパスで転送されます。反対側のBFDセッションはエコーパケットの実際のフォワーディングに関与しません。 エコー機能およびフォワーディング エンジンが検出プロセスを処理するため、2 つの BFD ネイバー間で送信される BFD 制御パケットの数が減少します。 また、フォワーディング エンジンが、リモート システムを介さずにリモート（ネイバー）システムの転送パスをテストするため、パケット内遅延が向上する可能性があり、それによって BFD バージョン 0 を BFD セッションの BFD 制御パケットで使用する場合に、障害検出時間を短縮できます。

エコー モードを両端で実行している（両方の BFD ネイバーがエコー モードを実行している）場合は、非対称性がないと表現されます。

関連トピック

インターフェイスでの BFD セッション パラメータの設定, （359 ページ）
BFD の動作, （354 ページ）

前提条件

BFD は、参加しているすべてのスイッチで実行されている必要があります。

CPU 使用率の上昇を避けるために、BFD エコー モードを使用する前に、**noipredirects** コマンドを入力して、インターネット制御メッセージ プロトコル（ICMP）リダイレクト メッセージの送信をディセーブルにする必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。 詳細については、「インターフェイスでのBFDセッション パラメータの設定」の項を参照してください。

制限事項

BFD バージョン 1 でサポートされる BFD エコー モード。

（注） BFD エコー モードは、ユニキャスト リバース パス転送（uRPF）の設定との組み合わせでは動作しません。 BFD エコー モードと uRPF の設定がイネーブルの場合、セッションはフラップします。

BFD 低速タイマーの設定

この手順では、BFD の slow timer 値を変更する方法を示します。 各 BFD スイッチに対してこの手順を繰り返します。

手順の概要

1. **enable**
2. **configureterminal**
3. **bfdslow-timer***milliseconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bfdslow-timer***milliseconds* 例： `Switch(config)# bfd slow-timer 12000`	BFD の slow timer を設定します。

非対称性のない *BFD* エコー モードのディセーブル化

この手順では、非対称性のないBFDエコーモードをディセーブルにする方法を示します。スイッチからエコーパケットが送信されず、スイッチはネイバースイッチが受信したBFDエコーパケットを転送しません。

各 BFD スイッチに対してこの手順を繰り返します。

手順の概要

1. **enable**
2. **configureterminal**
3. **nobfdecho**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**nobfdecho** 例： `Switch(config)# no bfd echo`	BFD エコー モードをディセーブルにします。 • **no** 形式を使用すると、BFD エコー モードをディセーブルにできます。
ステップ 4	**end** 例： `Switch(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

BFD のモニタリングとトラブルシューティング

ここでは、維持とトラブルシューティングのために BFD 情報を取得する方法について説明します。 これらのタスクのコマンドを必要に応じて任意の順序で入力できます。

BFD のモニタリングとトラブルシューティングを行うには、次の手順を実行します。

手順の概要

1. **enable**
2. **showbfdneighbors**[**details**]
3. **debugbfd**[**packet** | **event**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showbfdneighbors**[**details**] 例： `Switch# show bfd neighbors details`	（任意）BFD 隣接関係データベースを表示します。 • **details** キーワードを指定すると、すべての BFD プロトコル パラメータとネイバーごとにタイマーが表示されます。
ステップ 3	**debugbfd**[**packet** | **event**] 例： `Switch# debug bfd packet`	（任意）BFD パケットのデバッグ情報を表示します。

関連トピック

インターフェイスでの BFD セッション パラメータの設定，（359 ページ）
EIGRP に対する BFD サポートの設定，（362 ページ）
BGP に対する BFD サポートの設定，（361 ページ）
BFD の動作，（354 ページ）
OSPF に対する BFD サポートの設定，（364 ページ）
1 つ以上のインターフェイスの OSPF に対する BFD サポートの設定，（367 ページ）

双方向フォワーディング検出の設定例

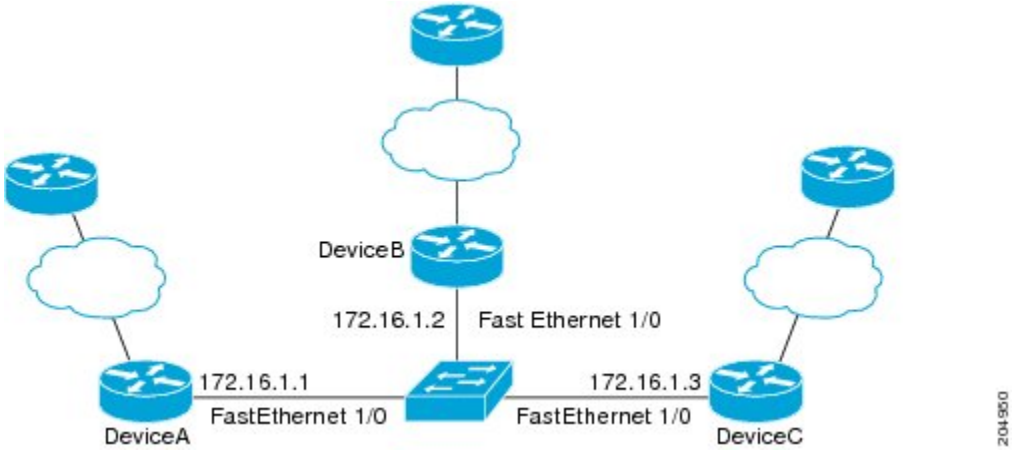
ここでは、次の設定例について説明します。

例：エコー モードがデフォルトでイネーブルになった EIGRP ネットワークでの BFD の設定

次の例では、EIGRP ネットワークにデバイス A、デバイス B およびデバイス C が含まれています。 デバイス A のファスト イーサネット インターフェイス 1/0 がデバイス B のファスト イーサネット インターフェイス 1/0 と同じネットワークに接続されています。デバイス B のファスト イーサネット 1/0 が デバイス C のファスト イーサネット インターフェイス 1/0 と同じネットワークに接続されています。

デバイス A とデバイス B はエコー モードをサポートする BFD バージョン 1 を実行しており、デバイス C はエコー モードをサポートしない BFD バージョン 0 を実行しています。 エコー モードはデバイス A とデバイス B の転送パスで動作するため、デバイス C とその BFD ネイバーの間の BFD セッションは非対称のエコー モードで実行されます。BFD セッションおよび障害検出のため、エコー パケットは同じパスで返されます。また、BFD ネイバー デバイス C は BFD バージョン 0 を実行し、BFD セッションおよび障害検出のために BFD 制御パケットを使用します。

下の図に、複数のデバイスがある大規模な EIGRP ネットワークを示します。その中の 3 台は、ルーティング プロトコルとして EIGRP を実行している BFD ネイバーです。



この例は、グローバル コンフィギュレーション モードから開始し、BFD の設定を示します。

デバイス A の設定

```
interface Fast Ethernet0/0
no shutdown
ip address 10.4.9.14 255.255.255.0
duplex auto
speed auto
!
interface Fast Ethernet1/0
ip address 172.16.1.1 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
no shutdown
duplex auto
speed auto
!
router eigrp 11
network 172.16.0.0
bfd all-interfaces
auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
```

```
line con 0
exec-timeout 30 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
!
end
```

デバイス B の設定

```
!
interface Fast Ethernet0/0
no shutdown
ip address 10.4.9.34 255.255.255.0
duplex auto
speed auto
!
interface Fast Ethernet1/0
ip address 172.16.1.2 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
no shtdown
duplex auto
speed auto
!
router eigrp 11
network 172.16.0.0
bfd all-interfaces
auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
exec-timeout 30 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
!
end
```

デバイス C の設定

```
!
!
interface Fast Ethernet0/0
no shutdown
ip address 10.4.9.34 255.255.255.0
duplex auto
speed auto
!
interface Fast Ethernet1/0
ip address 172.16.1.2 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
no shutdown
duplex auto
```

```
speed auto
!
router eigrp 11
network 172.16.0.0
bfd all-interfaces
auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
exec-timeout 30 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
!
end
```

デバイス A からの **show bfd neighbors details** コマンドの出力で、3 台のすべてのデバイス間に BFD セッションが作成され、EIGRP が BFD サポートに登録されることを確認できます。 出力の最初のグループは、IP アドレスが 172.16.1.3 のデバイス C が BFD バージョン 0 を実行しているため、エコーモードを使用しないことを示します。 出力の 2 番目のグループは、IP アドレスが 172.16.1.2 のデバイス B が BFD バージョン 1 を実行していて、50 ミリ秒の BFD interval パラメータが使用されていることを示します。 この出力では、対応するコマンド出力が太字で表示されています。

```
DeviceA# show bfd neighbors details

OurAddr
       NeighAddr
      LD/RD  RH/RS    Holdown(mult)  State     Int
172.16.1.1    172.16.1.3
     5/3    1(RH)    150 (3 )       Up   Fa1/0
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(1364284)
Rx Count: 1351813, Rx Interval (ms) min/max/avg: 28/64/49 last: 4 ms ago
Tx Count: 1364289, Tx Interval (ms) min/max/avg: 40/68/49 last: 32 ms ago
Registered protocols: EIGRP
Uptime: 18:42:45
Last packet: Version: 0
            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 3          - Your Discr.: 5
             Min tx interval: 50000    - Min rx interval: 50000
             Min Echo interval: 0
OurAddr       NeighAddr
     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.1    172.16.1.2

    6/1    Up        0    (3 )   Up        Fa1/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
```

```
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(317)
Rx Count: 305, Rx Interval (ms) min/max/avg: 1/1016/887 last: 448 ms ago
Tx Count: 319, Tx Interval (ms) min/max/avg: 1/1008/880 last: 532 ms ago
Registered protocols: EIGRP
Uptime: 00:04:30
Last packet: Version: 1

         - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 1          - Your Discr.: 6
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
```

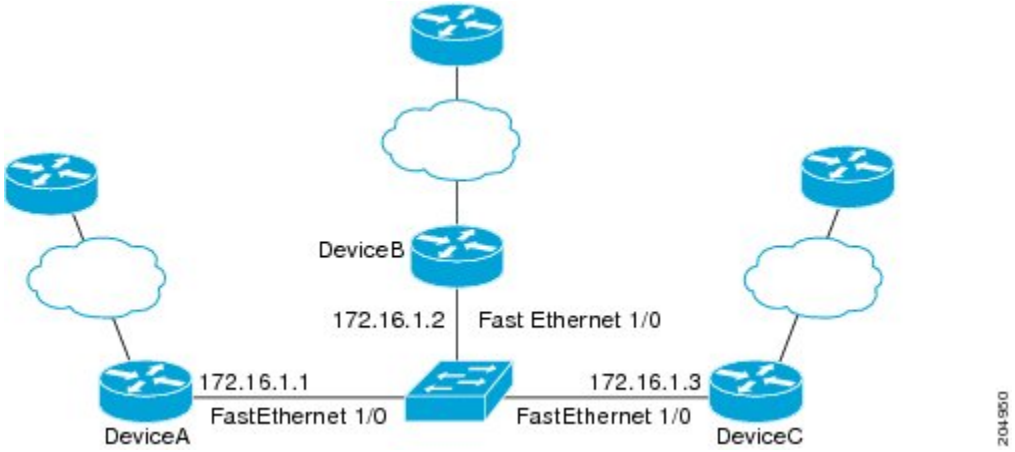
デバイスBの**showbfdneighborsdetails**コマンドによる出力で、BFDセッションが作成され、EIGRPがBFDサポートに対して登録されていることを確認できます。前述のように、デバイスAはBFDバージョン1を実行するため、エコー モードを実行しており、デバイスCはBFDバージョン0を実行するため、エコーモードを実行しません。この出力では、対応するコマンド出力が太字で表示されています。

```
DeviceB# show bfd neighbors details

OurAddr       NeighAddr
     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.2    172.16.1.1
    1/6    Up        0    (3 )   Up        Fa1/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1
           - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
OurAddr       NeighAddr

 LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.2    172.16.1.3
     3/6    1(RH)     118  (3 )   Up        Fa1/0
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(5735)
Rx Count: 5731, Rx Interval (ms) min/max/avg: 32/72/49 last: 32 ms ago
Tx Count: 5740, Tx Interval (ms) min/max/avg: 40/64/50 last: 44 ms ago
Registered protocols: EIGRP
Uptime: 00:04:45
Last packet: Version: 0
            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 3
             Min tx interval: 50000    - Min rx interval: 50000
             Min Echo interval: 0
```

下の図は、デバイス B のファスト イーサネット インターフェイス 1/0 に障害が発生したことを示しています。 デバイス B でファスト イーサネット インターフェイス 1/0 をシャット ダウンした場合、デバイス A とデバイス B の対応する BFD セッションの BFD 統計情報が少なくなります。



デバイス B のファスト イーサネット インターフェイス 1/0 に障害が発生すると、BFD はデバイス A またはデバイス C の BFD ネイバーとしてデバイス B を検出しなくなります。 この例では、デバイス B でファスト イーサネット インターフェイス 1/0 が管理的上の理由でシャット ダウンされています。

デバイス A での **showbfdneighbors** コマンドによる次の出力では、EIGRP ネットワークのデバイス A の唯一の BFD ネイバーが表示されます。 この出力では、対応するコマンド出力が太字で表示されています。

```
DeviceA# show bfd neighbors
OurAddr       NeighAddr

    LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.1    172.16.1.3

    5/3    1(RH)     134  (3 )   Up        Fa1/0
```

デバイス C での **showbfdneighbors** コマンドによる次の出力では、EIGRP ネットワークのデバイス C の唯一の BFD ネイバーが表示されます。 この出力では、対応するコマンド出力が太字で表示されています。

```
DeviceC# show bfd neighbors

OurAddr       NeighAddr

   LD/RD RH  Holdown(mult)  State     Int
172.16.1.3    172.16.1.1

    3/5  1   114  (3 )      Up        Fa1/0
```

関連トピック

BFD バージョンの相互運用性, （356 ページ）

例：OSPF ネットワークでの BFD の設定

次に、OSPF インターフェイスで BFD を設定する例を示します。 次の例では、デバイス A とデバイス B でシンプルな OSPF ネットワークが構成されています。デバイス A のファスト イーサネット インターフェイス 1/0 はデバイス B のファスト イーサネット インターフェイス 6/0 と同じネットワークに接続されています。グローバルコンフィギュレーションモードで始まるこの例には、BFD の設定が示されています。 デバイス A と B に対して、OSPF プロセスに関連付けられたすべてのインターフェイスで、BFD がグローバルに設定されます。

デバイス A の設定

```
!
interface Fast Ethernet 0/1
ip address 172.16.10.1 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 3/0.1
ip address 172.17.0.1 255.255.255.0
!
router ospf 123
log-adjacency-changes detail
network 172.16.0.0 0.0.0.255 area 0
network 172.17.0.0 0.0.0.255 area 0
bfd all-interfaces
```

デバイス B の設定

```
!
interface Fast Ethernet 6/0
 ip address 172.16.10.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 6/1
 ip address 172.18.0.1 255.255.255.0
!
router ospf 123
 log-adjacency-changes detail
 network 172.16.0.0 0.0.255.255 area 0
 network 172.18.0.0 0.0.255.255 area 0
 bfd all-interfaces
```

show bfd neighbors details コマンドによる出力で、BFD セッションが作成され、BFD サポートに対して OSPF が登録されることを確認できます。

デバイス A

```
DeviceA# show bfd neighbors details

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.1   172.16.10.2    1/2  1   532  (3 )      Up        Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
Registered protocols: OSPF

Uptime: 02:18:49
Last packet: Version: 0
            - Diagnostic: 0
```

```
            I Hear You bit: 1     - Demand bit: 0
            Poll bit: 0           - Final bit: 0
            Multiplier: 3         - Length: 24
            My Discr.: 2          - Your Discr.: 1
            Min tx interval: 50000    - Min rx interval: 1000
            Min Echo interval: 0
```

デバイス B からの **showbfdneighborsdetails** コマンドによる出力で、BFD セッションが作成されたことを確認します。

デバイス B

```
DeviceB# attach 6
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!

Device> show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    8/1  1   1000 (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0            - Diagnostic: 0
I Hear You bit: 1     - Demand bit: 0
Poll bit: 0           - Final bit: 0
Multiplier: 5         - Length: 24
My Discr.: 1          - Your Discr.: 8
Min tx interval: 200000    - Min rx interval: 200000
Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
IPC Tx Failure Count: 0
IPC Rx Failure Count: 0
Total Adjs Found: 1
```

showipospf コマンドによる出力で、BFD が OSPF に対してイネーブルになっていることを確認できます。

デバイス A

```
DeviceA# show ip ospf

 Routing Process "ospf 123" with ID 172.16.10.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

```
 External flood list length 0
 BFD is enabled

    Area BACKBONE(0)
        Number of interfaces in this area is 2 (1 loopback)
        Area has no authentication
        SPF algorithm last executed 00:00:08.828 ago
        SPF algorithm executed 9 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x028417
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

デバイス B

```
DeviceB# show ip ospf

 Routing Process "ospf 123" with ID 172.18.0.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x0
 Number of opaque AS LSA 0. Checksum Sum 0x0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 BFD is enabled

    Area BACKBONE(0)
        Number of interfaces in this area is 2 (1 loopback)
        Area has no authentication
        SPF algorithm last executed 02:07:30.932 ago
        SPF algorithm executed 7 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x28417
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

show ip ospf interface コマンドによる出力で、デバイス A とデバイス B を接続しているインターフェイスで OSPF に対して BFD がイネーブルになっていることを確認できます。

デバイス A

```
DeviceA# show ip ospf interface Fast Ethernet 0/1

show ip ospf interface Fast Ethernet 0/1
Fast Ethernet0/1 is up, line protocol is up
Internet Address 172.16.10.1/24, Area 0
Process ID 123, Router ID 172.16.10.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1, BFD enabled
Designated Router (ID) 172.18.0.1, Interface address 172.16.10.2
```

```
Backup Designated router (ID) 172.16.10.1, Interface address 172.16.10.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:03
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 172.18.0.1  (Designated Router)
Suppress hello for 0 neighbor(s)
```

デバイス B

```
DeviceB# show ip ospf interface Fast Ethernet 6/1

Fast Ethernet6/1 is up, line protocol is up
Internet Address 172.18.0.1/24, Area 0
Process ID 123, Router ID 172.18.0.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1, BFD enabled
Designated Router (ID) 172.18.0.1, Interface address 172.18.0.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

例：スタティック ルーティングに対する BFD サポートの設定

次の例では、ネットワークはデバイス A とデバイス B で構成されています。デバイス A のシリアル インターフェイス 2/0 は、デバイス B のシリアル インターフェイス 2/0 と同じネットワークに接続されています。BFD セッションを起動するには、デバイス B を設定する必要があります。

デバイス A

```
configure terminal
interface Serial 2/0
ip address 10.201.201.1 255.255.255.0
bfd interval 500 min_rx 500 multiplier 5
ip route static bfd Serial 2/0 10.201.201.2
ip route 10.0.0.0 255.0.0.0 Serial 2/0 10.201.201.2
```

デバイス B

```
configure terminal
interface Serial 2/0
ip address 10.201.201.2 255.255.255.0
bfd interval 500 min_rx 500 multiplier 5
ip route static bfd Serial 2/0 10.201.201.1
ip route 10.1.1.1 255.255.255.255 Serial 2/0 10.201.201.1
```

デバイス B のスタティック ルートが単独で存在していて、10.201.201.1 と 10.201.201.2 の間で BFD セッションをイネーブルにすることに注意してください。 設定する必要のある有益なスタティッ

ク ルートがない場合、パケットの転送に影響しないプレフィックス、たとえば、ローカルで設定されたループバック インターフェイスを選択します。

次の例では、BFD グループ testgroup のイーサネット インターフェイス 0/0 を介して 209.165.200.225 に到達するアクティブなスタティック BFD 設定があります。 設定されたスタティック BFD によってトラッキングされるスタティック ルートが設定されるとすぐに、単一のホップ BFD セッションがイーサネット インターフェイス 0/0 を介して 209.165.200.225 に開始されます。 BFD セッションが正常に確立されると、プレフィックス 10.0.0.0/8 が RIB に追加されます。

```
configure terminal
ip route static bfd Ethernet 0/0 209.165.200.225 group testgroup
ip route 10.0.0.0 255.255.255.224 Ethernet 0/0 209.165.200.225
```

次の例では、イーサネット インターフェイス 0/0.1001 を介した 209.165.200.226 への BFD セッションがグループ testgroup を使用するようにマークされます。 つまり、この設定はパッシブなスタティック BFD です。 2 つ目の BFD 設定によってトラッキングされるスタティック ルートがあるものの、209.165.200.226 に対する BFD セッションはイーサネット インターフェイス 0/0.1001 を介しては開始されません。 プレフィックス 10.1.1.1/8 と 10.2.2.2/8 の存在は、アクティブなスタティック BFD セッション（イーサネット インターフェイス 0/0 209.165.200.225）によって制御されます。

```
configure terminal
ip route static bfd Ethernet 0/0 209.165.200.225 group testgroup
ip route 10.0.0.0 255.255.255.224 Ethernet 0/0 209.165.200.225
ip route static bfd Ethernet 0/0.1001 209.165.200.226 group testgroup passive
ip route 10.1.1.1 255.255.255.224 Ethernet 0/0.1001 209.165.200.226
ip route 10.2.2.2 255.255.255.224 Ethernet 0/0.1001 209.165.200.226
```

関連トピック

スタティック ルーティングの BFD サポート, （358 ページ）

第 16 章

EtherChannel の設定

- 機能情報の確認，385 ページ
- EtherChannel の制約事項，385 ページ
- EtherChannel について，386 ページ
- EtherChannel の設定方法，404 ページ
- EtherChannel、PAgP、および LACP ステータスのモニタ，413 ページ
- EtherChannel の設定例，414 ページ

機能情報の確認

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

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

EtherChannel の制約事項

- EtherChannel のすべてのポートは同じ VLAN に割り当てるか、またはトランク ポートとして設定する必要があります。
- EtherChannel のポートがトランク ポートとして設定されている場合、すべてのポートを同じモード（Inter-Switch Link（ISL）または IEEE 802.1Q）で設定する必要があります。
- Port Aggregation Protocol（PAgP）は単一スイッチの EtherChannel 設定でのみイネーブルにできます。PAgP はクロススタック EtherChannel ではイネーブルにできません。

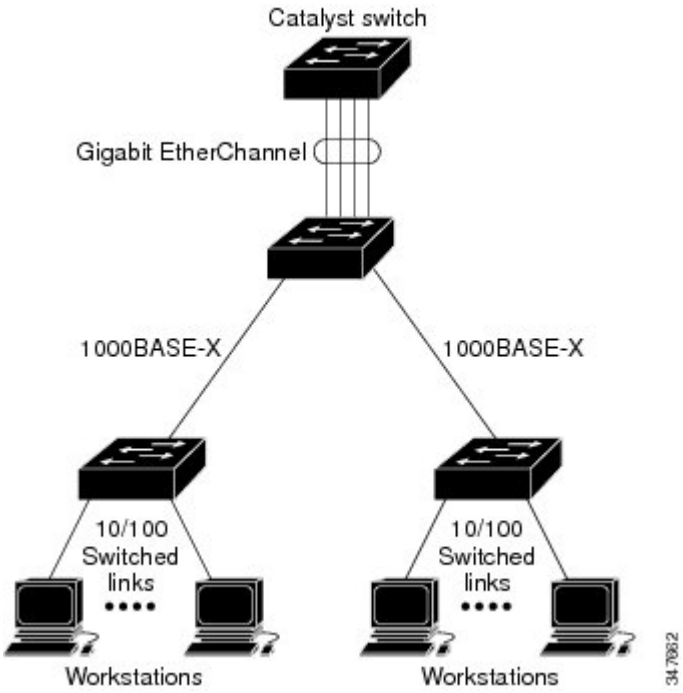
EtherChannel について

EtherChannel の概要

EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供します。 EtherChannel を使用して、ワイヤリング クローゼットとデータセンター間の帯域幅を増やすことができます。さらに、ボトルネックが発生しやすいネットワーク上のあらゆる場所に EtherChannel を配置できます。 EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。 リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャネル内の他のリンクにトラフィックをリダイレクトします。

EtherChannel は、単一の論理リンクにバンドルする個別のイーサネット リンクで構成されます。

図 *27*：一般的な *EtherChannel* 構成



EtherChannel は、スイッチ間またはスイッチとホスト間に、最大 8 Gb/s（ギガビット EtherChannel）または 80 Gb/s（10 ギガビット EtherChannel）の全二重帯域幅を提供します。

各 EtherChannel は、互換性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

LAN Lite フィーチャ セットでは、最大 6 個の EtherChannel をサポートします。 LAN Base フィーチャ セットでは、最大 24 個の EtherChannel をサポートします。

関連トピック

レイヤ 2 EtherChannel の設定, （404 ページ）

EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

EtherChannel のモード

EtherChannel は、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、またはOnのいずれかのモードに設定できます。 EtherChannelの両端は同じモードで設定します。

- EtherChannel の一方の端を PAgP または LACP モードに設定すると、システムはチャネルのもう一方の端とネゴシエーションし、アクティブにするポートを決定します。 リモートポートがEtherChannelとネゴシエーションができない場合、ローカルポートは独立ステートになり、他の単一リンクと同様にデータ トラフィックを引き続き伝送します。 ポート設定は変更されませんが、ポートは EtherChannel に参加しません。
- EtherChannel を **on** モードに設定すると、ネゴシエーションは実行されません。 スイッチは EtherChannel 内で互換性のあるすべてのポートを強制的にアクティブにします。 EtherChannel のもう一方の端（他のスイッチ上）も、同じように **on** モードに設定する必要があります。それ以外を設定した場合、パケットの損失が発生します。

関連トピック

レイヤ 2 EtherChannel の設定, （404 ページ）
EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

スイッチ上の EtherChannel

スイッチ上、スタックの単一スイッチ上、またはスタックの複数スイッチ上（クロススタック EtherChannel とも呼ぶ）で EtherChannel を作成できます。

図 *28*：単一スイッチ *EtherChannel*

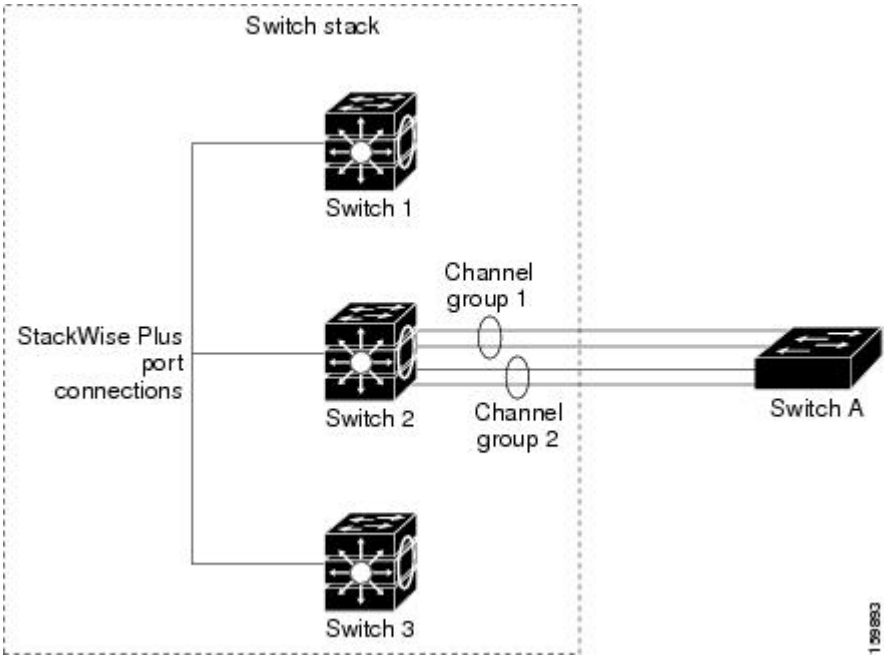
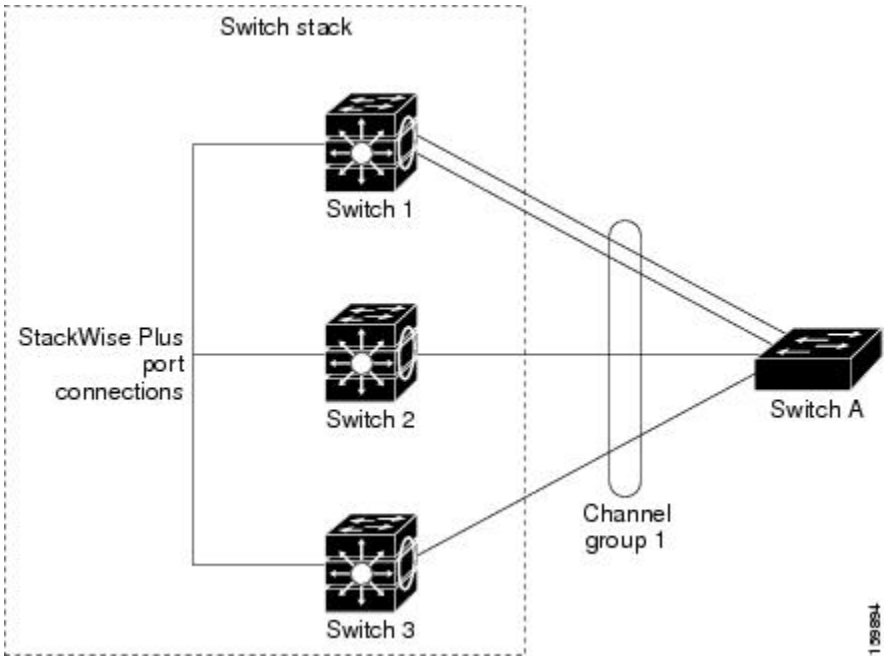


図 *29*：クロススタック *EtherChannel*



関連トピック

レイヤ 2 EtherChannel の設定, （404 ページ）
EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

EtherChannel リンクのフェールオーバー

EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが EtherChannel 内の残りのリンクに切り替えられます。 スイッチでトラップがイネーブルになっている場合、スイッチ、EtherChannel、および失敗したリンクを区別したトラップが送信されます。 EtherChannel の 1 つのリンク上の着信ブロードキャストおよびマルチキャスト パケットは、EtherChannel の他のリンクに戻らないようにブロックされます。

関連トピック

レイヤ 2 EtherChannel の設定, （404 ページ）
EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

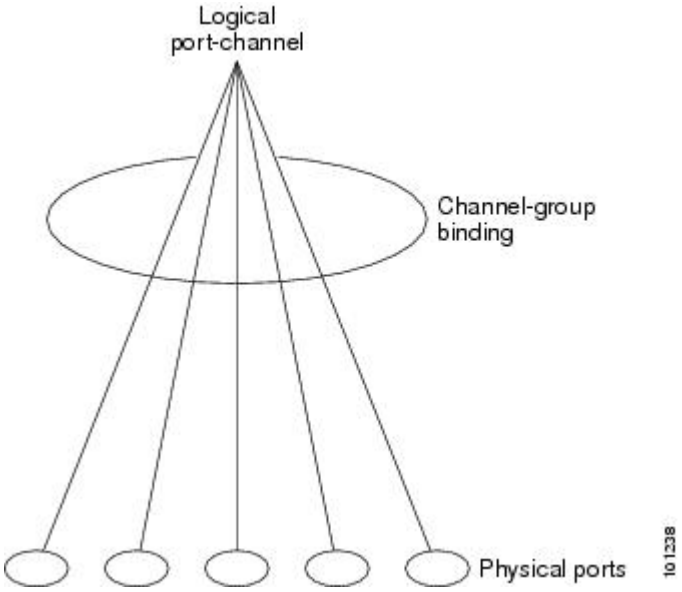
チャネル グループおよびポートチャネル インターフェイス

EtherChannel は、チャネル グループとポートチャネル インターフェイスから構成されます。 チャネル グループはポートチャネル インターフェイスに物理ポートをバインドします。 ポートチャ

ネルインターフェイスに適用した設定変更は、チャネルグループにまとめてバインドされるすべての物理ポートに適用されます。

channel-group コマンドは、物理ポートおよびポートチャネル インターフェイスをまとめてバインドします。 各 EtherChannel には 1 ～ 24 までの番号が付いたポートチャネル論理インターフェイスがあります。 このポートチャネル インターフェイス番号は、**channel-group** インターフェイス コンフィギュレーション コマンドで指定した番号に対応しています。

図 *30*：物理ポート、チャネル グループおよびポートチャネル インターフェイスの関係



- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル インターフェイスを動的に作成します。

  また、**interface port-channel***port-channel-number* グローバル コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group** *channel-group-number* コマンドを使用する必要があります。 *channel-group-number* は *port-channel-number* と同じ値に設定することも、違う値を使用することもできます。 新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

関連トピック

ポートチャネル論理インターフェイスの作成

EtherChannel 設定時の注意事項, （401 ページ）

EtherChannel のデフォルト設定, （399 ページ）

レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

物理インターフェイスの設定

EtherChannel 設定時の注意事項, （401 ページ）

EtherChannel のデフォルト設定, （399 ページ）

レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

ポート集約プロトコル

ポート集約プロトコル（PAgP）はシスコ独自のプロトコルで、Cisco スイッチおよび PAgP をサポートするベンダーによってライセンス供与されたスイッチでのみ稼働します。 PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチまたはスイッチ スタックは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。 次に、設定が類似している（スタック内の単一スイッチ上の）ポートを、単一の論理リンク（チャネルまたは集約ポート）に動的にグループ化します。 設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。 たとえば、PAgP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。 リンクを EtherChannel にグループ化した後で、PAgP は単一スイッチ ポートとして、スパニングツリーにそのグループを追加します。

PAgP モード

PAgP モードは、PAgP ネゴシエーションを開始する PAgP パケットをポートが送信できるか、または受信した PAgP パケットに応答できるかを指定します。

表 *33* : ***EtherChannel PAgP*** モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 これにより、PAgP パケットの送信は最小限に抑えられます。 EtherChannel メンバが、スイッチ スタックにある異なるスイッチから（クロススタック EtherChannel）の場合、このモードはサポートされません。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 EtherChannel メンバが、スイッチ スタックにある異なるスイッチから（クロススタック EtherChannel）の場合、このモードはサポートされません。

スイッチ ポートは、**auto** モードまたは **desirable** モードに設定された相手ポートとだけ PAgP パケットを交換します。 **on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

PAgP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。 次に例を示します。

- **desirable** モードのポートは、**desirable** モードまたは **auto** モードの別のポートとともに EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートとともに EtherChannel を形成できます。

どのポートも PAgP ネゴシエーションを開始しないため、**auto** モードのポートは、**auto** モードの別のポートとは EtherChannel を形成できません。

関連トピック

レイヤ 2 EtherChannel の設定, （404 ページ）
EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

ポートチャネル論理インターフェイスの作成

EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

物理インターフェイスの設定

EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

サイレント モード

PAgP 対応のデバイスにスイッチを接続する場合、**non-silent** キーワードを使用すると、非サイレント動作としてスイッチ ポートを設定できます。 **auto** モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレント モードが指定されていると見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにスイッチを接続する場合です。 サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。 この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼働させると、このスイッチ ポートが動作しなくなります。 ただし、サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

関連トピック

レイヤ 2 EtherChannel の設定, （404 ページ）
EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

ポートチャネル論理インターフェイスの作成

EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

物理インターフェイスの設定

EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

PAgP 学習方式およびプライオリティ

ネットワーク デバイスは、PAgP 物理ラーナーまたは集約ポート ラーナーに分類されます。 物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。 集約（論理）ポートによってアドレスを学習するデバイスは、集約ポート ラーナーです。 学習方式は、リンクの両端で同一の設定にする必要があります。

デバイスとそのパートナーが両方とも集約ポート ラーナーの場合、論理ポートチャネル上のアドレスを学習します。 デバイスは EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。 集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポート ラーナーの場合には自動検出できません。 したがって、物理ポートでアドレスを学習するには、ローカルデバイスに手動で学習方式を設定する必要があります。 また、負荷の分散方式を送信元ベース分散に設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要もあります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホット スタンバイに使用することもできます。 選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。 パケット伝送用に常に選択されるようにポートを設定するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。 プライオリティが高いほど、そのポートが選択される可能性が高まります。

（注） CLI で **physical-port** キーワードを指定した場合でも、スイッチがサポートするのは、集約ポート上でのアドレス ラーニングのみです。 **pagp learn-method** コマンドおよび **pagp port-priority** コマンドは、スイッチのハードウェアには作用しませんが、Catalyst 1900 スイッチなどの物理ポートによるアドレス ラーニングだけをサポートするデバイスと PAgP の相互運用性を確保するために必要です。

スイッチのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポート ラーナーとしてスイッチを設定することを推奨します。 送信元 MAC アドレスに基づいて負荷の分散方式を設定するには、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用します。 すると、スイッチは送信元アドレスを学習した EtherChannel 内の同じポートを使用して、物理ラーナーにパケットを送信します。 **pagp learn-method** コマンドは、このような場合のみ使用してください。

関連トピック

PAgP 学習方式およびプライオリティの設定, （408 ページ）
EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ, （413 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

PAgP と仮想スイッチとの相互作用およびデュアルアクティブ検出

仮想スイッチは、仮想スイッチ リンク（VSL）により接続された複数のコア スイッチであり、それらのスイッチ間で制御情報とデータ トラフィックを伝送します。 スイッチのうちの 1 つはアクティブ モードです。 その他のスイッチはスタンバイ モードです。 冗長性のため、リモート スイッチはリモート サテライト リンク（RSL）によって仮想スイッチに接続されます。

2 つのスイッチ間の VSL に障害が発生すると、一方のスイッチは他方のスイッチのステータスを認識しません。 両方のスイッチがアクティブモードになり、ネットワークを、重複したコンフィギュレーション（IP アドレスおよびブリッジ ID の重複を含む）を伴うデュアルアクティブの状態にする可能性があります。 ネットワークがダウンする場合もあります。

デュアルアクティブの状態を防止するために、コア スイッチは PAgP プロトコル データ ユニット（PDU）を RSL を介してリモート スイッチに送信します。 PAgP PDU はアクティブ スイッチを識別し、リモート スイッチは、コア スイッチが同期化するように PDU をコア スイッチに転送します。 アクティブ スイッチに障害が発生した場合、またはアクティブ スイッチがリセットされた場合は、スタンバイ スイッチがアクティブスイッチの役割を引き継ぎます。 VSL がダウンした場合は、1 つのコア スイッチが他のコア スイッチのステータスを認識し、その状態を変更しません。

PAgP と他の機能との相互作用

ダイナミック トランキング プロトコル（DTP）および Cisco Discovery Protocol（CDP）は、EtherChannel の物理ポートを使用してパケットを送受信します。 トランク ポートは、番号が最も小さい VLAN 上で PAgP プロトコル データ ユニット（PDU）を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。 このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼働状態のポート上だけです。

Link Aggregation Control Protocol

LACP は IEEE 802.3ad で定義されており、Cisco スイッチが IEEE 802.3ad プロトコルに適合したスイッチ間のイーサネット チャネルを管理できるようにします。 LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチまたはスイッチ スタックはLACPを使用することによって、LACPをサポートできるパートナーの識別情報、および各ポートの機能を学習します。 次に、設定が類似しているポートを単一の倫理リンク（チャネルまたは集約ポート）に動的にグループ化します。 設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。 たとえば、LACP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。 リンクをまとめて EtherChannel を形成した後で、LACP は単一スイッチ ポートとして、スパニング ツリーにそのグループを追加します。

LACP モード

LACPモードでは、ポートがLACPパケットを送信できるか、LACPパケットの受信のみができるかどうかを指定します。

表 *34*：*EtherChannel LACP* モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートはLACPパケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。 これにより、LACPパケットの送信を最小限に抑えます。

active モードおよび **passive LACP** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

LACP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。 次に例を示します。

- **active** モードのポートは、**active** モードまたは **passive** モードの別のポートとともに EtherChannel を形成できます。
- 両ポートとも LACP ネゴシエーションを開始しないため、**passive** モードのポートは、**passive** モードの別のポートと EtherChannel を形成することはできません。

関連トピック

レイヤ 2 EtherChannel の設定, （404 ページ）
EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

LACP と他の機能との相互作用

DTP および CDP は、EtherChannel の物理ポートを介してパケットを送受信します。 トランク ポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。 このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

LACP が LACP PDU を送受信するのは、LACP が active モードまたは passive モードでイネーブルになっている稼働状態のポートとの間だけです。

EtherChannel の On モード

EtherChannel の **on** モードは、EtherChannel の手動設定に使用します。 **on** モードを使用すると、ポートはネゴシエーションせずに強制的に EtherChannel に参加します。 リモート デバイスが PAgP や LACP をサポートしていない場合にこの **on** モードが役立ちます。 **on** モードでは、リンクの両端のスイッチが **on** モードに設定されている場合のみ EtherChannel を使用できます。

同じチャネル グループの **on** モードで設定されたポートは、速度やデュプレックスのようなポート特性に互換性を持たせる必要があります。 **on** モードで設定されている場合でも、互換性のないポートは suspended ステートになります。

注意 **on** モードの使用には注意が必要です。 これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。 グループの設定を誤ると、パケット損失またはスパニング ツリー ループが発生することがあります。

ロードバランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル内の 1 つのリンクを選択する数値に縮小することによって、チャネル内のリンク間でトラフィックのロード バランシングを行います。 MAC アドレス、IP アドレス、送信元アドレス、宛先アドレス、または送信元と宛先両方のアドレスに基づいた負荷分散など、複数の異なるロード バランシング モードから 1 つを指定できます。 選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。

ロードバランシングおよび転送方式を設定するには、**port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

EtherChannel ロードバランシングの設定
EtherChannel 設定時の注意事項, （401 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）
EtherChannel のデフォルト設定, （399 ページ）

MAC アドレス転送

送信元MACアドレス転送の場合、EtherChannelに転送されたパケットは、着信パケットの送信元MAC アドレスに基づいてチャネル ポート間で分配されます。 したがって、ロード バランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャネル ポートを使用しますが、送信元ホストが同じパケットは同じチャネル ポートを使用します。

宛先MACアドレス転送の場合、EtherChannelに転送されたパケットは、着信パケットの宛先ホストの MAC アドレスに基づいてチャネル ポート間で分配されます。 したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネル ポートに転送されます。

送信元および宛先MACアドレス転送の場合、EtherChannelに転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャネル ポート間で分配されます。 この転送方式は、負荷分散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のスイッチに対して送信元MACアドレス転送と宛先MACアドレス転送のどちらが適切であるかが不明な場合に使用できます。 送信元および宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

EtherChannel ロードバランシングの設定
EtherChannel 設定時の注意事項, （401 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）
EtherChannel のデフォルト設定, （399 ページ）

IP アドレス転送

送信元 IP アドレスベース転送の場合、パケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。 ロードバランシングを行うために、IP アドレスが異なるパケットはチャネルでそれぞれ異なるポートを使用しますが、IP アドレスが同じパケットはチャネルで同じポートを使用します。

宛先 IP アドレスベース転送の場合、パケットは着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。 ロードバランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、チャネルの異なるチャネルポートに送信できます。 異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常にチャネルの同じポートに送信されます。

送信元と宛先 IP アドレスベース転送の場合、パケットは着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。 この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたもので、特定のスイッチに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切であるか不明な場合に使用できます。 この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

EtherChannel ロードバランシングの設定
EtherChannel 設定時の注意事項, （401 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）
EtherChannel のデフォルト設定, （399 ページ）

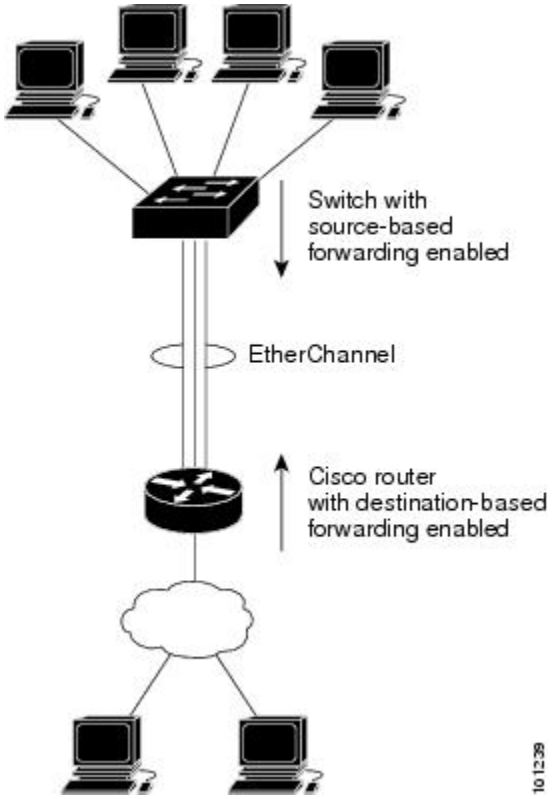
ロードバランシングの利点

ロードバランシング方式には異なる利点があるため、ネットワーク内のスイッチの位置、および負荷分散が必要なトラフィックの種類に基づいて特定のロードバランシング方式を選択する必要があります。

次の図では、4 台のワーク ステーションの EtherChannel がルータと通信します。 ルータは単一 MAC アドレス デバイスであるため、スイッチ EtherChannel で送信元ベース転送を行うことにより、スイッチが、ルータで使用可能なすべての帯域幅を使用することが保証されます。 ルータ

は、宛先アドレスベース転送を行うように設定されます。これは、多数のワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっているためです。

図 *31*：負荷の分散および転送方式



設定で一番種類が多くなるオプションを使用してください。たとえば、チャネル上のトラフィックが単一MACアドレスを宛先とする場合、宛先MACアドレスを使用すると、チャネル内の同じリンクが常に選択されます。ただし、送信元アドレスまたはIPアドレスを使用した方が、ロードバランシングの効率がよくなる場合があります。

関連トピック

EtherChannel ロードバランシングの設定
EtherChannel 設定時の注意事項，（401 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（403 ページ）
EtherChannel のデフォルト設定，（399 ページ）

EtherChannel のデフォルト設定

EtherChannel のデフォルト設定を、次の表に示します。

表 *35*：*EtherChannel* のデフォルト設定

機能	デフォルト設定
チャネル グループ	割り当てなし
ポートチャネル論理インターフェイス	未定義
PAgP モード	デフォルトなし。
PAgP 学習方式	すべてのポートで集約ポート ラーニング
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし。
LACP 学習方式	すべてのポートで集約ポート ラーニング
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768
LACP システム ID	LACP システムのプライオリティ、スイッチまたはスタックの MAC アドレス。
ロード バランシング	スイッチ上での負荷分散は着信パケットの送信元 MAC アドレスに基づきます。

関連トピック

レイヤ 2 EtherChannel の設定, （404 ページ）
EtherChannel の概要, （386 ページ）
EtherChannel のモード, （387 ページ）
スイッチ上の EtherChannel, （388 ページ）
EtherChannel リンクのフェールオーバー, （389 ページ）
LACP モード, （395 ページ）
PAgP モード , （391 ページ）
サイレント モード, （392 ページ）
ポートチャネル論理インターフェイスの作成
チャネル グループおよびポートチャネル インターフェイス, （389 ページ）
PAgP モード , （391 ページ）
サイレント モード, （392 ページ）
物理インターフェイスの設定

チャネル グループおよびポートチャネル インターフェイス, （389 ページ）
PAgP モード , （391 ページ）
サイレント モード, （392 ページ）
EtherChannel ロードバランシングの設定
ロードバランシングおよび転送方式, （397 ページ）
MAC アドレス転送, （397 ページ）
IP アドレス転送, （398 ページ）
ロードバランシングの利点, （398 ページ）
PAgP 学習方式およびプライオリティの設定, （408 ページ）
PAgP 学習方式およびプライオリティ, （393 ページ）
LACP システム プライオリティの設定, （410 ページ）
LACP ポート プライオリティの設定, （411 ページ）

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワーク ループおよびその他の問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。 設定上の問題を回避するために、次の注意事項に従ってください。

- 同じタイプのイーサネット ポートを最大で 8 個備えた PAgP EtherChannel を設定してください。
- 同じタイプのイーサネット ポートを最大で 16 個備えた LACP EtherChannel を設定してください。 最大で 8 個のポートを active モードにし、最大で 8 個のポートを standby モードにできます。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックス モードで動作するように設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。 **shutdown** インターフェイス コンフィギュレーション コマンドによってディセーブルにされた EtherChannel 内のポートは、リンク障害として扱われます。そのポートのトラフィックは、EtherChannel 内の他のポートの 1 つに転送されます。
- グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。 次のパラメータのいずれかで設定を変更した場合は、グループ内のすべてのポートでも変更する必要があります。
  - 許可 VLAN リスト
  - 各 VLAN のスパニングツリー パス コスト
  - 各 VLAN のスパニングツリー ポート プライオリティ
  - スパニングツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバになるように設定しないでください。

- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。 PAgP および LACP を実行している EtherChannel グループはスタックの同一スイッチ、または異なるスイッチで共存できます。 個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。
- EtherChannel の一部としてセキュア ポートを設定したり、セキュア ポートの一部として EtherChannel を設定したりしないでください。
- アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。 EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。
- EtherChannel がスイッチ インターフェイス上に設定されている場合、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、IEEE 802.1x をスイッチ上でグローバルにイネーブルにする前に、EtherChannel の設定をインターフェイスから削除します。
- クロススタック EtherChannel 設定では、EtherChannel のターゲットとなるすべてのポートが LACP に設定されているか、または、**channel-group***channel-group-number***mode on** インターフェイス コンフィギュレーション コマンドを使用してチャネル グループに手動で設定されていることを、確認します。 PAgP プロトコルは、クロススタック EtherChannel 上ではサポートされません。

関連トピック

レイヤ 2 EtherChannel の設定, （404 ページ）
EtherChannel の概要, （386 ページ）
EtherChannel のモード, （387 ページ）
スイッチ上の EtherChannel, （388 ページ）
EtherChannel リンクのフェールオーバー, （389 ページ）
LACP モード, （395 ページ）
PAgP モード , （391 ページ）
サイレント モード, （392 ページ）
ポートチャネル論理インターフェイスの作成
チャネル グループおよびポートチャネル インターフェイス, （389 ページ）
PAgP モード , （391 ページ）
サイレント モード, （392 ページ）
物理インターフェイスの設定
チャネル グループおよびポートチャネル インターフェイス, （389 ページ）
PAgP モード , （391 ページ）
サイレント モード, （392 ページ）
EtherChannel ロードバランシングの設定
ロードバランシングおよび転送方式, （397 ページ）
MAC アドレス転送, （397 ページ）

IP アドレス転送, （398 ページ）
ロードバランシングの利点, （398 ページ）
PAgP 学習方式およびプライオリティの設定, （408 ページ）
PAgP 学習方式およびプライオリティ, （393 ページ）
LACP システム プライオリティの設定, （410 ページ）
LACP ポート プライオリティの設定, （411 ページ）

レイヤ 2 EtherChannel 設定時の注意事項

レイヤ 2 EtherChannels を設定する場合は、次の注意事項に従ってください。

- EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。 複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。
- EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。 VLAN 許容範囲が一致していないと、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
- スパニングツリー パス コストが異なるポートは、設定上の矛盾がない限り、EtherChannel を形成できます。 異なるスパニングツリー パス コストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。

関連トピック

レイヤ 2 EtherChannel の設定, （404 ページ）
EtherChannel の概要, （386 ページ）
EtherChannel のモード, （387 ページ）
スイッチ上の EtherChannel, （388 ページ）
EtherChannel リンクのフェールオーバー, （389 ページ）
LACP モード, （395 ページ）
PAgP モード , （391 ページ）
サイレント モード, （392 ページ）
ポートチャネル論理インターフェイスの作成
チャネル グループおよびポートチャネル インターフェイス, （389 ページ）
PAgP モード , （391 ページ）
サイレント モード, （392 ページ）
物理インターフェイスの設定
チャネル グループおよびポートチャネル インターフェイス, （389 ページ）
PAgP モード , （391 ページ）
サイレント モード, （392 ページ）
EtherChannel ロードバランシングの設定

ロードバランシングおよび転送方式, （397 ページ）
MAC アドレス転送, （397 ページ）
IP アドレス転送, （398 ページ）
ロードバランシングの利点, （398 ページ）
PAgP 学習方式およびプライオリティの設定, （408 ページ）
PAgP 学習方式およびプライオリティ, （393 ページ）
LACP システム プライオリティの設定, （410 ページ）
LACP ポート プライオリティの設定, （411 ページ）

EtherChannel の設定方法

EtherChannel の設定後、ポートチャネルインターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。

レイヤ 2 EtherChannel の設定

レイヤ 2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャネルグループにポートを割り当てます。 このコマンドにより、ポートチャネル論理インターフェイスが自動的に作成されます。

ポート上で、**auto** モードまたは **desirable** モードで PAgP をイネーブルにした場合、このポートをクロススタック EtherChannel に追加する前に、**on** モードまたは LACP モードのいずれかになるように再設定する必要があります。 PAgP では、クロススタック EtherChannel はサポートされません。

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. **switchport mode** {**access** | **trunk**}
4. **switchport access vlan***vlan-id*
5. **channel-group***channel-group-number***mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive**}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスは、物理ポートです。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。 最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 3	**switchport mode** {**access** | **trunk**} 例： `Switch(config-if)# switchport mode access`	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセスポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。 指定できる範囲は 1 ～ 4094 です。
ステップ 4	**switchport access vlan***vlan-id* 例： `Switch(config-if)# switchport access vlan 22`	ポートをスタティックアクセスポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。 指定できる範囲は 1 ～ 4094 です。
ステップ 5	**channel-group***channel-group-number***mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive**} 例： `Switch(config-if)# channel-group 5 mode auto`	チャネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 *channel-group-number* の範囲は 1 ～ 24 です。 **mode** には、次のキーワードのいずれか 1 つを選択します。 • **auto**：PAgP デバイスが検出された場合にのみ、PAgP をイネーブルにします。 ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。このキーワードは、EtherChannel メンバがスイッチ スタックの異なるスイッチのものである場合にはサポートされません。

	コマンドまたはアクション	目的
		• **desirable**：PAgP を無条件でイネーブルにします。 ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 このキーワードは、EtherChannel メンバがスイッチ スタックの異なるスイッチのものである場合にはサポートされません。 • **on**：PAgP または LACP を使用せずにポートが強制的にチャネル化されます。 **on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**：（任意）スイッチ が PAgP 対応のパートナーに接続されている場合、ポートが **auto** または **desirable** モードになると非サイレント動作を行うようにスイッチ ポートを設定します。 **non-silent** を指定しないと、サイレントが想定されます。 サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。 サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。 • **active**：LACP デバイスが検出された場合にのみ、LACP をイネーブルにします。 ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive**：ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel の概要, （386 ページ）
EtherChannel のモード, （387 ページ）
スイッチ上の EtherChannel, （388 ページ）

EtherChannel リンクのフェールオーバー, （389 ページ）
LACP モード, （395 ページ）
PAgP モード , （391 ページ）
サイレント モード, （392 ページ）
EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）

EtherChannel ロード バランシングの設定

送信元ベースまたは宛先ベースの転送方式を使用することによって、EtherChannel のロード バランシングを設定できます。

このタスクはオプションです。

手順の概要

1. **configureterminal**
2. **port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}** 例： `Switch(config)# port-channel load-balance src-mac`	EtherChannel のロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **src-dst-ip**：送信元および宛先ホストの IP アドレスを指定します。 • **src-dst-mac**：送信元および宛先ホストの MAC アドレスを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。

	コマンドまたはアクション	目的
		• **src-mac**：着信パケットの送信元 MAC アドレスを指定します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

PAgP 学習方式およびプライオリティの設定

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **pagp learn-methodphysical-port**
4. **pagp port-priority***priority*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/2`	伝送ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**pagp learn-methodphysical-port** 例： `Switch(config-if)# pagp`	PAgP 学習方式を選択します。 デフォルトでは、**aggregation-port learning** が選択されています。つまり、EtherChannel 内のポートのいずれかを使用して、スイッ

	コマンドまたはアクション	目的
	learn-method physical port	チがパケットを送信元に送信します。 集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。 物理ポート ラーナーである別のスイッチに接続する**物理ポート**を選択します。 **port-channel load-balance** グローバル コンフィギュレーション コマンドを **src-mac** に設定してください。 学習方式はリンクの両端で同じ方式に設定する必要があります。
ステップ 4	**pagp port-priority***priority* 例： `Switch(config-if)# pagp port-priority 200`	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 *priority* に指定できる範囲は 0 ～ 255 です。 デフォルト値は 128 です。 プライオリティが高いほど、ポートが PAgP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

PAgP 学習方式およびプライオリティ，（393 ページ）
EtherChannel 設定時の注意事項，（401 ページ）
EtherChannel のデフォルト設定，（399 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ，（413 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（403 ページ）

LACP ホット スタンバイ ポートの設定

イネーブルの場合、LACP はチャネル内の LACP 互換ポート数を最大に設定しようとします（最大 16 ポート）。 同時にアクティブになれる LACP リンクは 8 つだけです。 リンクが追加されるとソフトウェアによってホット スタンバイモードになります。 アクティブ リンクの 1 つが非アクティブになると、ホット スタンバイ モードのリンクが代わりにアクティブになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリティに基づいてアクティブにするホット スタンバイ ポートを決定します。 ソフトウェアは、LACP を操作するシステム間のすべてのリンクに、次の要素（プライオリティ順）で構成された一意のプライオリティを割り当てます。

- LACP システム プライオリティ

- システム ID（スイッチ MAC アドレス）
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。 プライオリティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバイ モードにするポートを決定します。

アクティブ ポートかホット スタンバイ ポートかを判別するには、次の（2 つの）手順を使用します。 まず、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。 次に、ポート プライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートとホット スタンバイ ポートを決定します。 他のシステムのポート プライオリティとポート番号の値は使用されません。

ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響を与えるように、LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更できます。

LACP システム プライオリティの設定

lacp system-priority グローバル コンフィギュレーション コマンドを使用して、LACP をイネーブルにしているすべての EtherChannel に対してシステム プライオリティを設定できます。 LACP を設定済みの各チャネルに対しては、システム プライオリティを設定できません。 デフォルト値を変更すると、ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響します。

show etherchannel summary 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが H になっています）。

LACP システム プライオリティを設定するには、次の手順に従います。 この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **lacp system-priority***priority*
4. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lacp system-priority***priority* 例： `Switch(config)# lacp system-priority 32000`	LACP システム プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。 デフォルトは 32768 です。 値が小さいほど、システム プライオリティは高くなります。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ, （413 ページ）

LACP ポート プライオリティの設定

デフォルトでは、すべてのポートは同じポート プライオリティです。 ローカル システムのシステム プライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さな値に変更して、最初にアクティブになるホットスタンバイ リンクを変更できます。 ホット スタンバイ ポートは、番号が小さい方が先にチャネルでアクティブになります。 **show etherchannel summary** 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが H になっています）。

（注） LACP がすべての互換ポートを集約できない場合（たとえば、ハードウェアの制約が大きいリモート システム）、EtherChannel 中でアクティブにならないポートはすべてホット スタンバイ ステートになり、チャネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP ポート プライオリティを設定するには、次の手順に従います。 この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **lacp port-priority***priority*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lacp port-priority***priority* 例： `Switch(config-if)# lacp port-priority 32000`	LACP ポート プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。 デフォルトは 32768 です。 値が小さいほど、ポートが LACP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項, （401 ページ）
EtherChannel のデフォルト設定, （399 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （403 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ, （413 ページ）

EtherChannel、PAgP、および LACP ステータスのモニタ

この表に記載されているコマンドを使用して EtherChannel、PAgP、および LACP ステータスを表示できます。

表 *36* : ***EtherChannel*、*PAgP*、および *LACP* ステータスのモニタ用コマンド**

コマンド	説明
clear lacp {*channel-group-number* **counters** | **counters**}	LACP チャネル グループ情報およびトラフィック カウンタをクリアします。
clear pagp {*channel-group-number* **counters** | **counters**}	PAgP チャネル グループ情報およびトラフィック カウンタをクリアします。
show etherchannel[*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}] [**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**]	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。 ロード バランシング方式またはフレーム配布方式、ポート、ポートチャネル、プロトコルの情報も表示されます。
show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 PAgP 設定、ネイバー情報などの PAgP 情報が表示されます。
show pagp [*channel-group-number*] **dual-active**	デュアルアクティブ検出ステータスが表示されます。
show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**}	トラフィック情報、内部 LACP 設定、ネイバー情報などの LACP 情報が表示されます。
show running-config	設定エントリを確認します。
show etherchannel load-balance	ポート チャネル内のポート間のロード バランシング、またはフレーム配布方式を表示します。

関連トピック

PAgP 学習方式およびプライオリティの設定，（408 ページ）
PAgP 学習方式およびプライオリティ，（393 ページ）
LACP システム プライオリティの設定，（410 ページ）
LACP ポート プライオリティの設定，（411 ページ）

EtherChannel の設定例

レイヤ 2 EtherChannel の設定：例

この例では、スタック内の 1 つのスイッチに EtherChannel を設定する例を示します。 2 つのポートを VLAN 10 のスタティック アクセス ポートとして、PAgP モードが **desirable** であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

この例では、スタック内の 1 つのスイッチに EtherChannel を設定する例を示します。 2 つのポートは VLAN 10 のスタティックアクセス ポートとして、LACP モードが **active** であるチャネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

次の例では、クロススタック EtherChannel を設定する方法を示します。 LACP パッシブ モードを使用して、VLAN 10 内のスタティックアクセス ポートとしてスタック メンバ 1 のポートを 2 つ、スタック メンバ 2 のポートを 1 つチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode passive
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# channel-group 5 mode passive
Switch(config-if)# exit
```

第 17 章

リンクステート トラッキングの設定

- 機能情報の確認，415 ページ
- リンク ステート トラッキングの設定の制約事項，415 ページ
- リンクステート トラッキングの概要，416 ページ
- リンクステート トラッキングの設定方法，419 ページ
- リンクステート トラッキングのモニタリング，421 ページ
- リンクステート トラッキングの設定：例，421 ページ

機能情報の確認

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

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

リンク ステート トラッキングの設定の制約事項

- スイッチ 1 つにつき、設定できるリンクステート グループは 2 つだけです。
- インターフェイスは、複数のリンクステート グループのメンバにはなれません。
- リンクステート グループ内でアップストリーム インターフェイスとして定義されているインターフェイスを、リンクステート グループ内でダウンストリーム インターフェイスとして定義することはできません。

- ダウンストリームの EtherChannel インターフェイスの一部となる個々のインスターフェイスでリンクステート トラッキングをイネーブルにしないでください。

関連トピック

リンクステート トラッキングの概要, （416 ページ）
リンクステート トラッキングの設定方法, （419 ページ）
リンクステート トラッキング ステータスのモニタリング

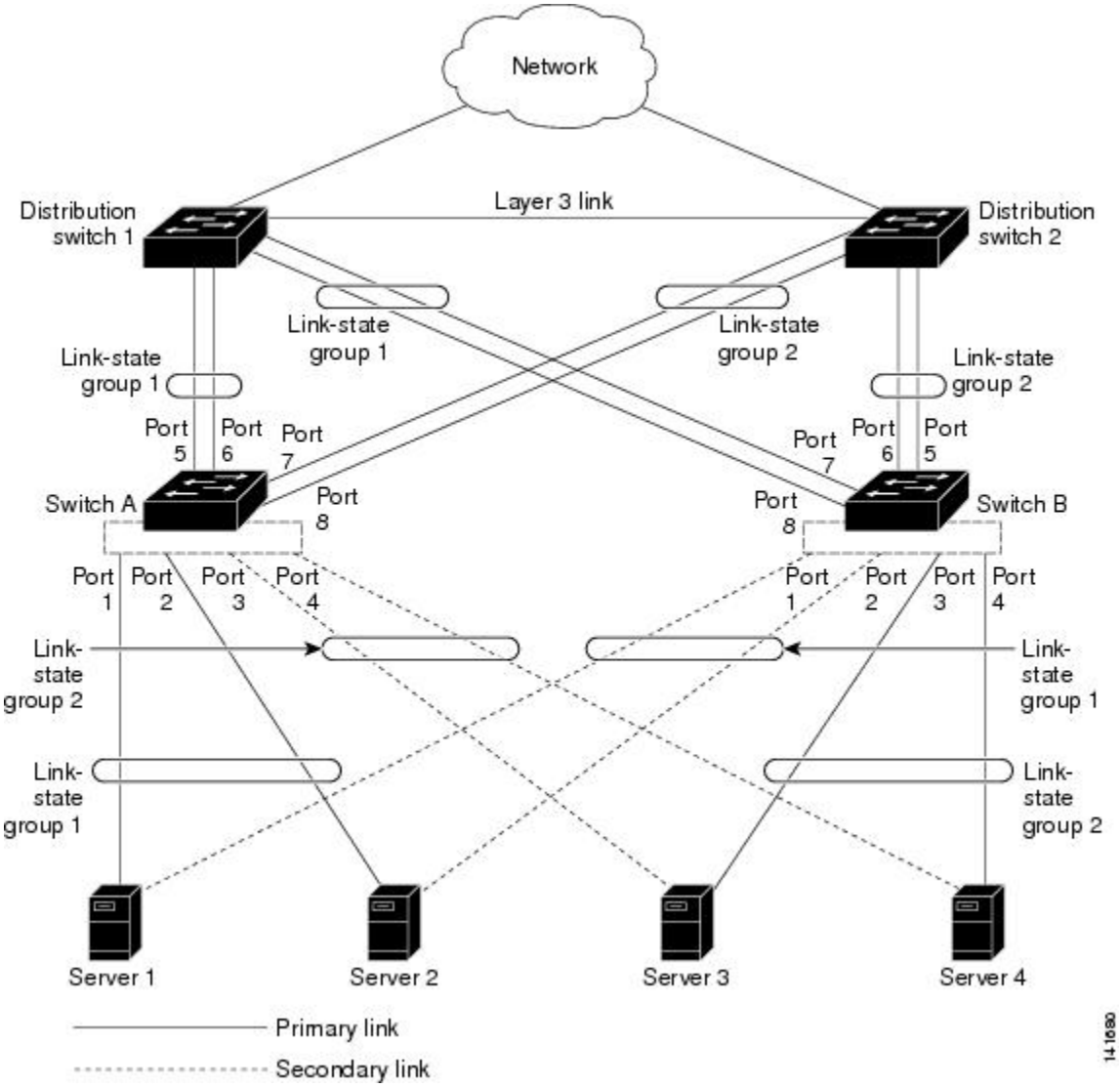
リンクステート トラッキングの概要

リンクステートトラッキングは、トランク フェールオーバーとも呼ばれ、複数のインターフェイスのリンクステートをバインドします。 リンクステート トラッキングはサーバ NIC アダプタのチーミングと連動させることができ、ネットワークに冗長性を提供します。 サーバ NIC アダプタがプライマリまたはセカンダリの関係で設定されており、プライマリ インターフェイスでリンクが失われた場合は、ネットワーク接続が透過的にセカンダリ インターフェイスに切り替えられます。

（注） ポートの集合（EtherChannel）またはアクセス モードかトランク モードのいずれかの単一の物理ポートをインターフェイスに指定できます。

次の図の設定では、ネットワーク トラフィック フローのバランスが確実に保たれます。

図 *32*：一般的なリンクステート トラッキングの設定



- スイッチと他のネットワーク デバイスへのリンクの場合
  - サーバ 1 とサーバ 2 は、プライマリ リンクにスイッチ A を使用し、セカンダリ リンクにスイッチ B を使用しています。
  - サーバ 3 とサーバ 4 は、プライマリ リンクにスイッチ B を使用し、セカンダリ リンクにスイッチ A を使用しています。
- スイッチ A のリンクステート グループ 1

- スイッチ A はリンクステート グループ 1 を介して、プライマリ リンクをサーバ 1 および サーバ 2 に使用します。 ポート 1 はサーバ 1 に、ポート 2 はサーバ 2 にそれぞれ接続されます。 ポート 1 およびポート 2 はリンクステート グループ 1 でダウンストリーム インターフェイスとして使用します。
- ポート 5 およびポート 6 は、リンクステート グループ 1 を介して分散スイッチ 1 に接続されます。 ポート 5 およびポート 6 は、リンクステート グループ 1 でアップストリーム インターフェイスとして使用します。

• スイッチ A のリンクステート グループ 2

- スイッチ A はリンクステートグループ 2 を介して、セカンダリ リンクをサーバ 3 および サーバ 4 に使用します。 ポート 3 はサーバ 3 に、ポート 4 はサーバ 4 にそれぞれ接続されます。 ポート 3 およびポート 4 はリンクステート グループ 2 でダウンストリーム インターフェイスとして使用します。
- ポート 7 およびポート 8 は、リンクステート グループ 2 を介して分散スイッチ 2 に接続されます。 ポート 7 およびポート 8 は、リンクステート グループ 2 でアップストリーム インターフェイスとして使用します。

• スイッチ B のリンクステート グループ 2

- スイッチ B はリンクステートグループ 2 を介して、プライマリ リンクをサーバ 3 および サーバ 4 に使用します。 ポート 3 はサーバ 3 に、ポート 4 はサーバ 4 にそれぞれ接続されます。 ポート 3 およびポート 4 はリンクステート グループ 2 でダウンストリーム インターフェイスとして使用します。
- ポート 5 およびポート 6 は、リンクステート グループ 2 を介して分散スイッチ 2 に接続されます。 ポート 5 およびポート 6 は、リンクステート グループ 2 でアップストリーム インターフェイスとして使用します。

• スイッチ B のリンクステート グループ 1

- スイッチ B はリンクステート グループ 1 を介して、セカンダリ リンクをサーバ 1 および サーバ 2 に使用します。 ポート 1 はサーバ 1 に、ポート 2 はサーバ 2 にそれぞれ接続されます。 ポート 1 およびポート 2 はリンクステート グループ 1 でダウンストリーム インターフェイスとして使用します。
- ポート 7 およびポート 8 は、リンクステート グループ 1 を介して分散スイッチ 1 に接続されます。 ポート 7 およびポート 8 は、リンクステート グループ 1 でアップストリーム インターフェイスとして使用します。

分散スイッチやルータに障害が発生したり、ケーブルが切断されたり、リンクが失われたために、リンクステート グループ内でアップストリーム ポートが利用不能や接続不能になる場合があります。 これらは、リンクステート トラッキングがイネーブルの際の、ダウンストリーム インターフェイスとアップストリーム インターフェイス間の相互作用です。

- アップストリーム インターフェイスがリンクアップ ステートの場合、ダウンストリーム インターフェイスをリンクアップ ステートに変更したり、リンクアップ ステートのままにしたりすることができます。
- すべてのアップストリーム インターフェイスが利用不能になった場合、リンクステート トラッキングが自動的にダウンストリーム インターフェイスを errdisable ステートにします。サーバ間の接続は、自動的にプライマリ サーバ インターフェイスからセカンダリ サーバ インターフェイスに変更されます。 たとえば、前の図で、ポート 6 のアップストリーム リンクが切断されても、ダウンストリーム ポート 1 および 2 のリンク ステートは変わりません。ただし、アップストリーム ポート 5 のリンクも切断された場合、ダウンストリーム ポートのリンク ステートがリンクダウン ステートに変更されます。 サーバ 1 およびサーバ 2 の接続については、リンクステート グループ 1 からリンクステート グループ 2 へ変更します。ダウンストリーム ポート 3 およびダウンストリーム ポート 4 は、リンクグループ 2 であるためステートを変更しません。
- リンクステート グループが設定されている場合、リンクステート トラッキングはディセーブルで、アップストリーム インターフェイスが切断され、ダウンストリーム インターフェイスのリンク ステートは変更されないままになります。 サーバはこのアップストリーム接続が切断されたことを認識せず、セカンダリ インターフェイスにフェールオーバーしません。

障害のあるダウンストリーム ポートをリンクステート グループから削除することで、ダウンストリーム インターフェイスのリンクダウン状態から復旧できます。 複数のダウンストリーム インターフェイスを復旧させるには、リンクステート グループをディセーブルにします。

関連トピック

リンクステート トラッキングの設定方法, （419 ページ）
リンクステート トラッキング ステータスのモニタリング
リンクステート トラッキングの設定：例, （421 ページ）
リンク ステート トラッキングの設定の制約事項, （415 ページ）

リンクステート トラッキングの設定方法

リンクステート トラッキングをイネーブルにするには、リンク ステート グループを作成し、そのグループに割り当てるインターフェイスを指定します。 このタスクはオプションです。

手順の概要

1. **configureterminal**
2. **linkstatetrack***number*
3. **interface***interface-id*
4. **link state group**[*number*]{**upstream** | **downstream**}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**linkstatetrack***number* 例： `Switch(config)# link state track 2`	リンクステート グループを作成して、リンクステート トラッキングをイネーブルにします。 グループ番号は 1 または 2 です。デフォルトは 1 です。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定する物理インターフェイスまたはインターフェイスの範囲を指定して、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、アクセスまたはトランクモード（IEEE 802.1q）のスイッチ ポートかルーテッド ポートが含まれます。 （注） Etherchannelインターフェイスの一部となる個々のインスターフェイスでリンクステート トラッキングをイネーブルにしないでください。
ステップ 4	**link state group**[*number*]{**upstream** | **downstream**} 例： `Switch(config-if)# link state group 2 upstream`	リンクステート グループを指定し、グループ内のインターフェイスを upstream または downstream インターフェイスに設定します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

リンクステート トラッキングの概要, （416 ページ）
リンクステート トラッキングの設定：例, （421 ページ）
リンク ステート トラッキングの設定の制約事項, （415 ページ）

リンクステート トラッキングのモニタリング

次の表のコマンドを使用してリンクステート トラッキングのステータスを表示できます。

表 *37*：リンクステート トラッキング ステータスをモニタするコマンド

コマンド	説明
show link state group [*number*] **[detail]**	リンクステート グループ情報を表示します。

リンクステート トラッキングの設定：例

次に、リンクステート グループ 1 を作成してリンクステート グループにインターフェイスを設定する例を示します。

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config-if)# interface range gigabitethernet1/0/21-22
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet1/0/3
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet1/0/5
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

関連トピック

リンクステート トラッキングの概要，（416 ページ）
リンクステート トラッキングの設定方法，（419 ページ）
リンクステート トラッキング ステータスのモニタリング

第 18 章

Resilient Ethernet Protocol の設定

- 機能情報の確認，423 ページ
- REP の概要，423 ページ
- REP の設定方法，430 ページ
- REP のモニタリング，439 ページ
- REP の設定例，439 ページ

機能情報の確認

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

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

REP の概要

Resilient Ethernet Protocol（REP）はシスコ独自のプロトコルで、スパニングツリー プロトコル（STP）に代わるプロトコルとして、ネットワーク ループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。 REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジング ループを作成するのを防ぎ、セグメント内のリンク障害に応答します。 REP は、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。

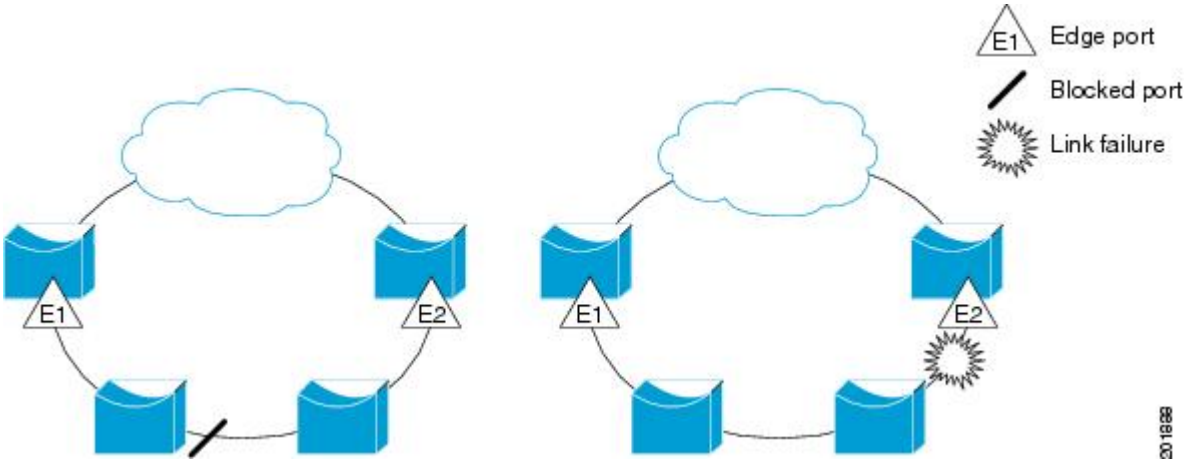
（注） REP は IP Base、IP Services、または IP Lite のライセンスを実行している Catalyst スイッチでサポートされます。 REP は LAN Base ライセンスではサポートされません。

REP は Cisco Catalyst 3560-CX スイッチのみでサポートされています。

REP セグメントは、相互接続されたポートのチェーンで、セグメント ID が設定されます。 各セグメントは、標準（非エッジ）セグメント ポートと、2 つのユーザ設定エッジ ポートで構成されています。 1 ルータは同じセグメントに属するポートを複数持たず、各セグメント ポートにある外部ネイバーは 1 つだけです。 セグメントは共有メディアを通過できますが、どのリンクであっても同じセグメントに属することができるのは 2 ポートだけです。 REP はトランクのイーサネット フロー ポイント（EFP）インターフェイスでのみサポートされます。

次の図に、4 つのスイッチにまたがる 6 つのポートで構成されているセグメントの例を示します。ポート E1 および E2 がエッジ ポートとして設定されています。 （左側のセグメントのように）すべてのポートが動作可能の場合、斜線で表しているように単一ポートがブロックされます。ネットワークに障害が発生した場合、ブロックされたポートがフォワーディング ステートに戻り、ネットワークの中断を最小限に抑えます。

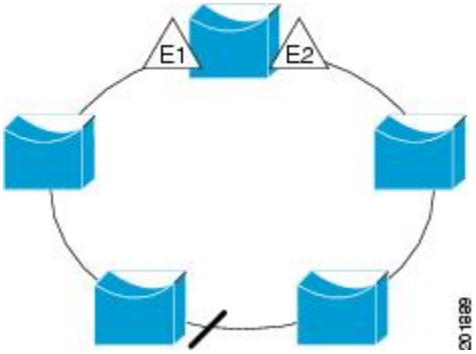
図 *33*：*REP* オープン セグメント



上の図に示されたセグメントは、オープン セグメントで、2 つのエッジ ポート間は接続されていません。 REP セグメントはブリッジング ループの原因とならないため、セグメント エッジを安全に任意のネットワークに接続できます。 セグメント内のルータに接続されているすべてのホストには、エッジ ポートを通じて残りのネットワークに接続する方法が 2 つありますが、いつでもアクセス可能なのは 1 つだけです。 いずれかのセグメントまたは REP セグメントのいずれかのポートに障害が発生した場合、REP はすべてのポートのブロックを解除し、他のゲートウェイ経由で接続できるようにします。

下の図に示すセグメントはリングセグメントであり、同じルータ上に両方のエッジポートがあります。 この設定を使用すると、セグメント内の任意の 2 ルータ間で冗長接続を形成することができます。

図 *34* : *REP* リング セグメント



REP セグメントには、次のような特徴があります。

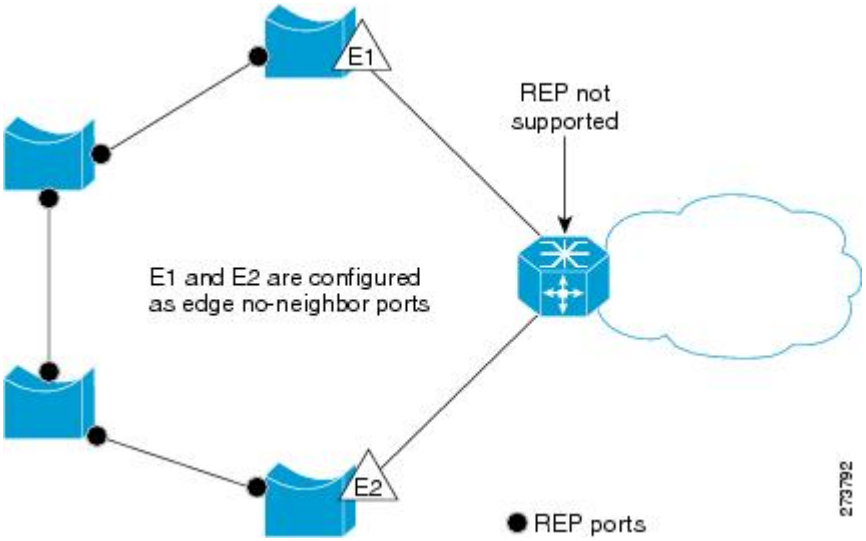
- セグメント内の全ポートが動作可能な場合、1 ポート（代替ポートと呼ばれる）が各 VLAN でブロック ステートとなります。 VLAN ロード バランシングが設定されている場合は、セグメント内の 2 つのポートが VLAN のブロック ステートを制御します。
- セグメント内の 1 つまたは複数のポートが動作不能になると、リンク障害が発生して、すべてのポートがすべての VLAN トラフィックを転送して、接続性を確保します。
- リンク障害の場合、できるだけ早期に代替ポートのブロックが解除されます。 障害リンクが復旧すると、ネットワークの中断を最小限に抑えるようにVLAN単位で論理的にブロックされたポートが選択されます。

REP セグメントに基づいて、ほとんどのネットワーク タイプを構成することができます。 また REPはプライマリ エッジポートで制御され、セグメント内の任意のポートで発生するVLANロード バランシングをサポートします。

アクセス リング トポロジでは、下の図に示すように、ネイバー スイッチで REP がサポートされない場合があります。 この場合、そのスイッチ側のポート（E1 と E2）を非ネイバー エッジ ポートとして設定できます。 これらのポートは、エッジポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。たとえば、STP や REP のトポロジ変更通知を集約ス

イッチに送信するように設定することもできます。 この場合、送信される STP トポロジ変更通知（TCN）は、Multiple Spanning-Tree（MST）STP メッセージです。

図 *35*：非ネイバー エッジ ポート



REP には次のような制限事項があります。

- 各セグメント ポートを設定する必要があります。設定を間違えると、ネットワーク内でフォワーディング ループが発生します。
- REP はセグメント内の単一障害ポートだけを管理できます。REP セグメント内の複数ポート障害の場合、ネットワークの接続が中断します。
- 冗長ネットワーク内だけに REP を設定します。 冗長性のないネットワークに REP を設定すると、接続が失われます。

リンク完全性

REP は、リンク完全性の確認にエッジポート間でエンドツーエンドポーリング機能を使用しません。 ローカル リンク障害検出を実装しています。 REP リンク ステータス レイヤ（LSL）が REP 対応ネイバーを検出して、セグメント内の接続性を確立します。 すべての VLAN は、ネイバーが検出されるまでインターフェイス上でブロックされます。 ネイバーが特定されたあと、REP が代替ポートとなるネイバー ポートと、トラフィックを転送するポートを決定します。

セグメント内のポートごとに、一意のポート ID が割り当てられます。 ポート ID フォーマットは、スパニングツリー アルゴリズムで使用されるものと類似しており、ポート番号（ブリッジ上で一意）と、関連 MAC アドレス（ネットワーク内で一意）から構成されます。 セグメント ポートが起動すると、ポートの LSL がセグメント ID およびポート ID を含むパケットの送信を開始します。 ポートは、同じセグメント内のネイバーとのスリーウェイ ハンドシェイクを実行したあとで、動作可能と宣言されます。

次のような場合、セグメント ポートは動作可能になりません。

- ネイバーに同じセグメント ID がない
- 複数のネイバーに同じセグメント ID がある
- ネイバーがピアとして、ローカル ポートに確認応答しない

各ポートは、直近のネイバーと隣接関係を確立します。 ネイバー関係が確立されると、ポートがセグメントの1つのブロックされたポート（代替ポート）を決定するようにネゴシエートします。その他のポートのブロックは解除されます。 デフォルトで、REP パケットは BPDU クラス MAC アドレスに送信されます。 パケットは、シスコ マルチキャスト アドレスにも送信できますが、セグメントに障害が発生した場合にブロックされたポートのアドバタイズ（BPA）メッセージの送信だけに使用されます。 パケットは、REP が動作していない装置によって廃棄されます。

高速コンバージェンス

REP は、物理リンク ベースで動作し、VLAN 単位ベースでは動作しません。 すべての VLAN に対して 1 つの hello メッセージしか必要ないため、プロトコル上の負荷が軽減されます。 指定セグメント内の全スイッチで継続的に VLAN を作成し、REP トランク ポート上に同じ許容 VLAN を設定することを推奨します。 ソフトウェアでのメッセージのリレーによって発生する遅延を回避するために、REP ではいくつかのパケットを通常のマルチキャスト アドレスにフラッディングすることも可能です。 これらのメッセージはハードウェア フラッド レイヤ（HFL）で動作し、REP セグメントだけではなくネットワーク全体にフラッディングされます。 セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。 ドメイン全体で専用の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

ファイバ インターフェイスのコンバージェンス復旧時間の推定値は、200 の VLAN が設定されたローカル セグメントで 50 ミリ秒から 200 ミリ秒までです。 VLAN ロード バランシングのコンバージェンスは 300 ミリ秒以下です。

VLAN ロード バランシング

REP セグメント内の 1 つのエッジ ポートがプライマリ エッジ ポートとして機能し、もう一方がセカンダリ エッジ ポートとなります。 セグメント内の VLAN ロード バランシングに常に参加しているのがプライマリ エッジ ポートです。 REP VLAN バランシングは、設定された代替ポートでいくつかの VLAN をブロックし、プライマリ エッジ ポートでその他の全 VLAN をブロックすることで実行されます。 VLAN ロード バランシングを設定する際に、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

- インターフェイスにポート ID を入力します。 セグメント内のポート ID を識別するには、ポートの **show interface rep** detail インターフェイス コンフィギュレーション コマンドを入力します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジ ポートのダウンストリーム ネイバー ポートを識別するものです。 ネイバー オフセット番号の範囲は、-256 ～ +256 で、0 値は無効です。 プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。 負

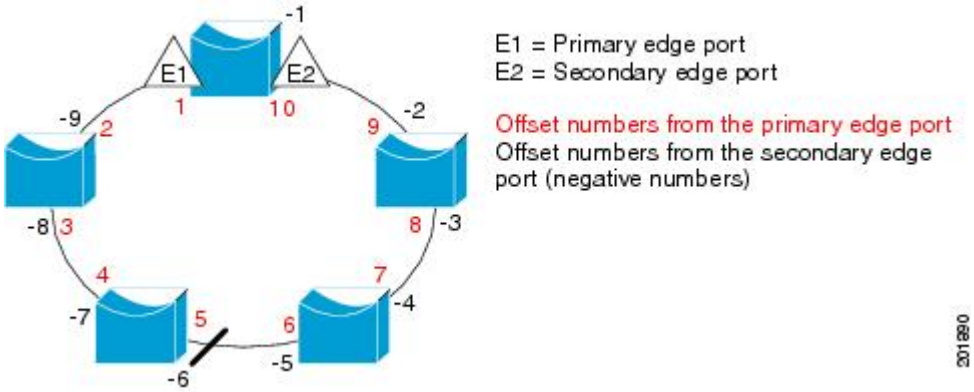
数は、セカンダリ エッジ ポート（オフセット番号 -1）とそのダウンストリーム ネイバーを示します。

（注） プライマリ（またはセカンダリ）エッジ ポートからポートのダウンストリーム位置を識別することで、プライマリ エッジ ポートのオフセット番号を設定します。 番号 1 はプライマリ エッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

下の図に、E1 がプライマリ エッジ ポートで E2 がセカンダリ エッジ ポートの場合の、セグメントのネイバー オフセット番号を示します。 リングの内側にある赤い番号は、プライマリ エッジ ポートからのオフセット番号で、リングの外側にある黒い番号がセカンダリエッジポートからのオフセット番号です。 正のオフセット番号（プライマリ エッジ ポートからのダウンストリーム位置）または負のオフセット番号（セカンダリエッジポートからのダウンストリーム位置）のいずれかにより、（プライマリ エッジ ポートを除く）全ポートを識別できます。 E2 がプライマリ エッジ ポートになるとオフセット番号 1 となり、E1 のオフセット番号が -1 になります。

- **preferred** キーワードを入力します。これにより、**rep segment***segment-id***preferred** インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。

図 *36*：セグメント内のネイバー オフセット番号



REP セグメントが完了すると、すべての VLAN がブロックされます。 VLAN ロード バランシングを設定する際には、次の 2 種類の方法のいずれかを使用してトリガーを設定する必要もあります。

- プライマリ エッジ ポートのあるスイッチ上で **rep preempt segment***segment-id* 特権 EXEC コマンドを入力することで、いつでも手動で VLAN ロード バランシングをトリガーすることができます。
- **rep preempt delay***seconds* インターフェイス コンフィギュレーション コマンドを入力すると、プリエンプション遅延時間を設定できます。 リンク障害が発生して回復すると、設定されたプリエンプション期間の経過後に VLAN ロード バランシングが開始されます。 設定時間が

経過する前に別のポートで障害が発生した場合、遅延タイマーが再開されることに注意してください。

（注） VLAN ロード バランシングが設定されている場合、手動での介入またはリンク障害および回復によってトリガーされるまで、動作が開始されません。

VLAN ロード バランシングがトリガーされると、プライマリ エッジ ポートがメッセージを送信して、セグメント内の全インターフェイスにプリエンプションについて警告します。 メッセージがセカンダリ ポートで受信されると、これがネットワークに反映され、メッセージ内で指定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジ ポートに通知します。

またすべての VLAN をブロックするために、セグメント内の特定ポートを設定できます。 プライマリ エッジ ポートだけによって VLAN ロード バランシングが開始され、セグメントが各エンドでエッジ ポートによって終端されていない場合開始することができません。 プライマリ エッジ ポートは、ローカル VLAN ロード バランシング設定を決定します。

ロード バランシングを再設定するには、プライマリ エッジ ポートを再設定します。 ロード バランシング設定を変更すると、プライマリ エッジ ポートでは、再び **rep preempt segment** コマンドが実行されるか、ポート障害および復旧のあとで設定済みプリエンプト遅延期間が経過してから、新規設定が実行されます。 エッジ ポートを通常セグメント ポートに変更しても、既存の VLAN ロード バランシング ステータスは変更されません。 新規エッジ ポートを設定すると、新規トポロジ設定になる可能性があります。

関連トピック

REP インターフェイスの設定, （433 ページ）

スパニングツリー インタラクション

REP は、STP とも Flex Link 機能とも対話しませんが、どちらとも共存できます。 セグメントに属しているポートはスパニングツリーの制御から削除されるため、セグメント ポートでは STP BPDU の送受信は行われません。 したがって、STP はセグメント上で実行できません。

STP リング コンフィギュレーションから REP セグメント コンフィギュレーションに移行するには、まずリング内の単一ポートをセグメントの一部として設定し、次にセグメント数を最小限にするように隣接するポートを設定します。 各セグメントには、常にブロックされたポートが含まれているので、セグメントが複数になるとブロックされたポートも複数になり、接続が失われる可能性があります。 セグメントがエッジ ポートの場所まで両方向に設定されたら、次にエッジ ポートを設定します。

REP ポート

REP セグメントは、障害ポート、オープン ポート、および代替ポートで構成されます。

- 標準セグメント ポートとして設定されたポートは、障害ポートとして起動します。

- ネイバーとの隣接関係が確立されると、ポートは代替ポートステートに移行して、インターフェイス内の全 VLAN をブロックします。 ブロックされたポートのネゴシエーションが発生して、セグメントが安定すると、ブロックされたポートのうちの 1 つが代替ロールのままになって他のすべてのポートがオープン ポートになります。
- リンク内に障害が発生すると、すべてのポートが障害ステートに移行します。 代替ポートは、障害通知を受信すると、すべての VLAN を転送するオープン ステートに遷移します。

通常セグメント ポートをエッジ ポートに変換しても、エッジ ポートを通常セグメント ポートに変換しても、必ずトポロジ変更が発生するわけではありません。エッジポートを通常セグメントポートに変更する場合、設定されるまで VLAN ロード バランシングは実装されません。 VLAN ロード バランシングの場合、セグメント内に 2 つのエッジ ポートを設定する必要があります。

スパニングツリーポートとして再設定されたセグメントポートは、スパニングツリー設定に従って再起動します。 デフォルトでは、これは指定ブロッキング ポートです。 PortFast が設定されていたり、STP がディセーブルの場合、ポートはフォワーディング ステートになります。

REP の設定方法

セグメントは、チェーンで相互接続しているポートの集合で、セグメント ID が設定されています。 REP セグメントを設定するには、REP 管理 VLAN を設定し（またはデフォルト VLAN 1 を使用し）、次にインターフェイスコンフィギュレーションモードを使用してセグメントにポートを追加します。 2 つのエッジ ポートをセグメント内に設定して、1 つをプライマリ エッジ ポート、もう 1 つをデフォルトでセカンダリ エッジ ポートにします。 1 セグメント内のプライマリ エッジ ポートは 1 つだけです。 別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。 オプションで、セグメント トポロジ変更通知（STCN）および VLAN ロード バランシングを送信する場所を設定することもできます。

REP のデフォルト設定

REP はすべてのインターフェイス上でディセーブルです。 イネーブルにする際に、エッジポートとして設定されていなければインターフェイスは通常セグメント ポートになります。

REP をイネーブルにする際に、STCN の送信はディセーブルで、すべての VLAN はブロックされ、管理 VLAN は VLAN 1 になります。

VLAN ロード バランシングがイネーブルの場合、デフォルトは手動でのプリエンプションで、遅延タイマーはディセーブルになっています。 VLAN ロード バランシングが設定されていない場合、手動でのプリエンプション後のデフォルト動作は、プライマリ エッジ ポートで全 VLAN がブロックとなります。

REP 設定時の注意事項

REP の設定時には、次の注意事項に従ってください。

- まず 1 ポートの設定から始めて、セグメント数とブロックされたポートの数を最小限に抑えるように隣接するポートを設定することを推奨します。
- 外部ネイバーが設定されておらずセグメント内では 3 つ以上のポートに障害が発生した場合、1 ポートがデータ パス用のフォワーディング ステートになり、設定中の接続性の維持に役立ちます。 **showrepinterface** コマンド出力では、このポートのポート ロールは「Fail Logical Open」と表示され、他の障害ポートのポート ロールは「Fail No Ext Neighbor」と表示されます。 障害ポートの外部ネイバーが設定されている場合、ポートは代替ポート ステートに移行して、代替ポート選択メカニズムに基づいて最終的にオープン ステートになるか、代替ポートのままになります。
- REP ポートは、レイヤ 2 IEEE 802.1Q またはトランク ポートのいずれかである必要があります。
- 同じ許可 VLAN のセットでセグメント内のすべてのトランク ポートを設定することを推奨します。
- Telnet 接続を通じて REP を設定する際には注意してください。 これは、別の REP インターフェイスがブロック解除のメッセージを送信するまで、REP はすべての VLAN をブロックするためです。 同じインターフェイス経由でルータにアクセスする Telnet セッションで REP をイネーブルにすると、ルータへの接続が失われることがあります。
- REP と STP または REP と Flex Link を同じセグメントやインターフェイスで実行できません。
- STP ネットワークを REP セグメントに接続する場合、接続はセグメント エッジであることを確認してください。 エッジで実行されていない STP 接続は、REP セグメントでは STP が実行されないため、ブリッジング ループが発生する可能性があります。 すべての STP BPDU は、REP インターフェイスで廃棄されます。
- 同じ許容 VLAN セットでセグメント内のすべてのトランク ポートを設定する必要があります。そうでない場合、設定ミスが発生します。
- REP がスイッチの 2 ポートでイネーブルの場合、両方のポートが通常セグメント ポートまたはエッジ ポートである必要があります。 REP ポートは以下の規則に従います。
  - スイッチ上の REP ポートの数に制限はありませんが、同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
  - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジ ポートとなります。
  - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジ ポートであるか、両方のポートが通常セグメント ポートであるか、一方が通常ポートでもう一方が非ネイバー エッジ ポートである必要があります。 スイッチ上のエッジ ポートと通常セグメント ポートが同じセグメントに属することはできません。
  - スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジ ポートとして設定され、もう 1 つが通常セグメント ポートに設定されている場合（設定ミス）、エッジ ポートは通常セグメント ポートとして扱われます。

- REPインターフェイスはブロックされた状態になり、ブロック解除できるようになるまでブロックされた状態のまま残ります。 突然の接続切断を避けるために、このステータスを認識しておく必要があります。
- REP はネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。 シスコ マルチキャスト アドレスに送信された BPA メッセージは、管理 VLAN で送信されます。 これはデフォルトで VLAN 1 です。
- ネイバーからの hello が受信されないままどのくらいの時間が経過すると REP インターフェイスがダウンするかを設定できます。 **rep lsl-age-timer** value インターフェイス コンフィギュレーション コマンドを使用して、120 ～ 10000 ミリ秒の時間を設定します。 LSL hello タイマーは、このエージング タイマーの値を 3 で割った値に設定されます。 通常の動作では、ピア スイッチのエージング タイマーが満了になって hello メッセージが確認されるまでに LSL hello が 3 回送信されます。
  - EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。 ポート チャネルで 1000 ミリ秒未満の値を設定しようとすると、エラー メッセージが表示されてコマンドが拒否されます。
- REP ポートは、次のポート タイプのいずれかに設定できません。
  - スイッチド ポート アナライザ（SPAN）宛先ポート
  - トンネル ポート
  - アクセス ポート
- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別のポートではサポートされません。
- スイッチごとに最大 64 の REP セグメントを設定できます。

REP 管理 VLAN の設定

リンク障害によるソフトウェアでのメッセージのリレーやロードバランシング時のVLANブロッキング通知によって発生する遅延を回避するため、REP はハードウェア フラッド レイヤ（HFL）で通常のマルチキャスト アドレスにパケットをフラッディングします。 これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。 ドメイン全体の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- スイッチとセグメントで 1 つの管理 VLAN だけが可能です。 ただし、これはソフトウェアによって強制的に設定されません。
- 管理 VLAN は RSPAN VLAN になりません。

REP 管理 VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **repadminvlan***vlan-id*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**repadminvlan***vlan-id* 例： `Switch(config)# rep admin vlan 100`	管理 VLAN を指定します。 指定できる範囲は 2 ～ 4094 です。 デフォルトは VLAN 1 です。 管理 VLAN を 1 に設定するには、**no rep admin vlan** グローバル コンフィギュレーション コマンドを入力します。
ステップ 3	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

REP インターフェイスの設定

REP 動作の場合、各セグメント インターフェイスで REP をイネーブルにして、セグメント ID を指定する必要があります。 このタスクは必須で、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。その他のステップはすべて任意です。

インターフェイスで REP をイネーブルにし、設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode trunk**
5. **repsegment***segment-id* [**edge**[**no-neighbor**][[**primary**]] [**preferred**]
6. **repstcn** {**interface***interface id*| **segment***id-list* | **stp**}
7. **repblockport**{**id***port-id*| *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
8. **reppreemptdelay***seconds*
9. **rep lsl-age-timer***value*
10. **end**
11. **showinterface**[*interface-id*]**rep** [**detail**]
12. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch>` **`enable`**	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id*	インターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。 インターフェイスは物理レイヤ2インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。 指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**switchport mode trunk**	インターフェイスをレイヤ 2 トランク ポートとして設定します。
ステップ 5	**repsegment***segment-id* [**edge**[**no-neighbor**][[**primary**]] [**preferred**]	インターフェイス上でREPをイネーブルにして、セグメント番号を特定します。 指定できるセグメント ID の範囲は 1 ～ 1024 です。 これらの任意のキーワードは利用可能です。 （注） 各セグメントに 1 つのプライマリ エッジ ポートを含めて、2 つのエッジ ポートを設定する必要があります。 • （任意）**edge**：エッジ ポートとしてポートを設定します。 各セグメントにあるエッジ ポートは 2 つだけです。 **primary** キーワードなしで **edge** を入力すると、ポートがセカンダリ エッジ ポートとして設定されます。

	コマンドまたはアクション	目的
		• （任意）**primary**：プライマリ エッジ ポート（VLAN ロード バランシングを設定できるポート）としてポートを設定します。 • （任意）**no-neighbor**：エッジ ポートとして外部 REP ネイバーを使用せずにポートを設定します。 そのポートはエッジ ポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。 （注） 各セグメントにあるプライマリ エッジ ポートは 1 つだけですが、2 つの異なるスイッチにエッジ ポートを設定して **primary** キーワードを両方のスイッチに入力しても、その設定は有効です。 ただし、REP ではセグメント プライマリ エッジ ポートとして 1 つのポートだけが選択されます。 **showreptopology** 特権 EXEC コマンドを入力すると、セグメントのプライマリ エッジ ポートを特定することができます。 • （任意）**preferred**：ポートが優先代替ポートであるか、VLAN ロード バランシングの優先ポートであるかを示します。 （注） ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。 通常、前に障害が発生したポートが、代替ポートとなります。
ステップ 6	**repstcn** {**interface***interface id*| **segment***id-list* | **stp**}	（任意）STCN を送信するようにエッジ ポートを設定します。 • **interface***interface -id*：物理インターフェイスまたはポート チャネルを指定して、STCN を受け取ります。 • **segment***id-list*：STCN を受け取る 1 つ以上のセグメントを特定します。 有効な範囲は 1 ～ 1024 です。 • **stp**：STCN を STP ネットワークに送信します。
ステップ 7	**repblockport**{**id***port-id*| *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}	（任意）プライマリ エッジ ポートに VLAN ロード バランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し、代替ポートでブロックされるように VLAN を設定します。 • **id***port-id*：ポート ID で代替ポートを特定します。 セグメント内の各ポートにポート ID が自動的に生成されます。 **showinterface***type number***rep** [**detail**] 特権 EXEC コマンドを入力して、インターフェイス ポート ID を表示できます。 • *neighbor_offset*：エッジ ポートからのダウンストリーム ネイバーとして代替ポートを特定するための番号。 有効範囲は -256 ～ 256 で、負数はセカンダリ エッジ ポートからのダウンストリーム ネイバーを示します。 値 **0** は無効です。 **-1** を入力して、セカンダリ エッジ

	コマンドまたはアクション	目的
		ポートを代替ポートとして識別します。 ネイバー オフセット番号付けの例については、図 36：セグメント内のネイバー オフセット番号，（428 ページ） を参照してください。 （注） プライマリ エッジ ポート（オフセット番号 1）にこのコマンドを入力するので、代替ポートを特定するのにオフセット値 1 を入力できません。 • **preferred**：すでに VLAN ロード バランシングの優先代替ポートとして指定されている通常セグメント ポートを選択します。 • **vlan***vlan-list*：1 つの VLAN または VLAN の範囲をブロックします。 • **vlanall**：すべての VLAN をブロックします。 （注） REP プライマリ エッジ ポート上にだけこのコマンドを入力します。
ステップ 8	**reppreemptdelay***seconds*	（任意）プリエンプト遅延時間を設定します。 • リンク障害が発生して復旧した後に、VLAN ロード バランシングを自動的にトリガーするには、このコマンドを使用します。 • 遅延時間の範囲は 15 ～ 300 秒です。 デフォルトは、遅延時間のない手動によるプリエンプションです。 （注） REP プライマリ エッジ ポート上にだけこのコマンドを入力します。
ステップ 9	**rep lsl-age-timer***value*	（任意）ネイバーからの hello が受信されないままどのくらいの時間（ミリ秒）が経過すると REP インターフェイスがダウンするかを設定します。 指定できる範囲は 120 ～ 10000 ミリ秒（40 ミリ秒単位）です。 デフォルト値は 5000 ミリ秒（5 秒）です。 （注） • EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。 • リンクのフラップを避けるため、リンクの両方のポートに同じ LSL エージが設定されている必要があります。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**showinterface**[*interface-id*]**rep** [**detail**]	（任意）REP インターフェイスの設定を表示します。

	コマンドまたはアクション	目的
ステップ 12	**copyrunning-configstartup-config**	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN ロード バランシング，（427 ページ）

VLAN ロード バランシングの手動によるプリエンプションの設定

プライマリ エッジ ポートで **rep preempt delay***seconds* インターフェイス コンフィギュレーション コマンドを入力しないで、プリエンプション時間遅延を設定する場合、デフォルトではセグメントで VLAN ロード バランシングを手動でトリガーします。 手動で VLAN ロード バランシングをプリエンプトする前に、他のすべてのセグメント設定が完了しているかどうか確認してください。 **rep preempt delay***segment-id* コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

手順の概要

1. **rep preempt segment***segment-id*
2. **show rep topology***segment-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**rep preempt segment***segment-id*	手動により、セグメント上の VLAN ロード バランシングをトリガーします。 実行前にコマンドを確認する必要があります。
ステップ 2	**show rep topology***segment-id*	REP トポロジ情報を表示します。

REP の SNMP トラップ設定

REP 固有のトラップを送信して、簡易ネットワーク管理プロトコル（SNMP）サーバにリンクの動作状態の変更およびすべてのポート役割の変更を通知するようにルータを設定できます。

手順の概要

1. **configureterminal**
2. **snmpmibreptrap-rate***value*
3. **end**
4. **showrunning-config**
5. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**snmpmibreptrap-rate***value* 例： `Switch(config)# snmp mib rep trap-rate 500`	スイッチで REP トラップの送信をイネーブルにして、1 秒あたりのトラップの送信数を設定します。 • 1 秒あたりのトラップの送信数を入力します。範囲は 0 ～ 1000 です。デフォルトは 0（制限なし、発生するたびにトラップが送信される）です。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**showrunning-config** 例： `Switch# show running-config`	（任意）実行コンフィギュレーションを表示します。これを使用して REP トラップ コンフィギュレーションを検証できます。
ステップ 5	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

REP のモニタリング

手順の概要

1. **show interface**[*interface-id*]**rep**[**detail**]
2. **show rep topology**[**segment***segment-_id*][**archive**][**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show interface**[*interface-id*]**rep**[**detail**]	特定のインターフェイスまたはすべてのインターフェイスのREPの設定とステータスを表示します。 • （任意）**detail**：インターフェイス固有の REP 情報を表示します。
ステップ 2	**show rep topology**[**segment***segment-_id*][**archive**][**detail**]	セグメント内のプライマリおよびセカンダリ エッジ ポートを含む、1 セグメントまたは全セグメントの REP トポロジ情報を表示します。 • （任意）**archive**：最後の安定したトポロジを表示します。 （注） アーカイブのトポロジは、スイッチをリロードすると保持されません。 • （任意）**detail**：詳細なアーカイブ情報を表示します。

REP の設定例

REP 管理 VLAN の設定：例

次に、管理 VLAN を VLAN 100 として設定して、REP インターフェイスの 1 つに **show interface rep detail**show interface rep detail コマンドを入力して設定を確認する例を示します。

```
Switch# configure terminal
Switch (conf)# rep admin vlan 100
Switch (conf-if)# end
Switch# show interface gigabitethernet1/1 rep details
GigabitEthernet1/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
```

```
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

REP インターフェイスの設定：例

次に、インターフェイスをセグメント 1 のプライマリ エッジ ポートに設定し、STCN をセグメント 2 ～ 5 に送信し、代替ポートをポート ID 0009001818D68700 のポートとして設定して、セグメント ポート障害および回復後の 60 秒のプリエンプション遅延後にすべての VLAN をブロックする例を示します。 このインターフェイスは、ネイバーからの hello が受信されないまま 6000 ミリ秒が経過するとダウンするように設定されています。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
Switch (conf-if)# end
```

次に、インターフェイスに外部 REP ネイバーがない場合の同じ設定の例を示します。

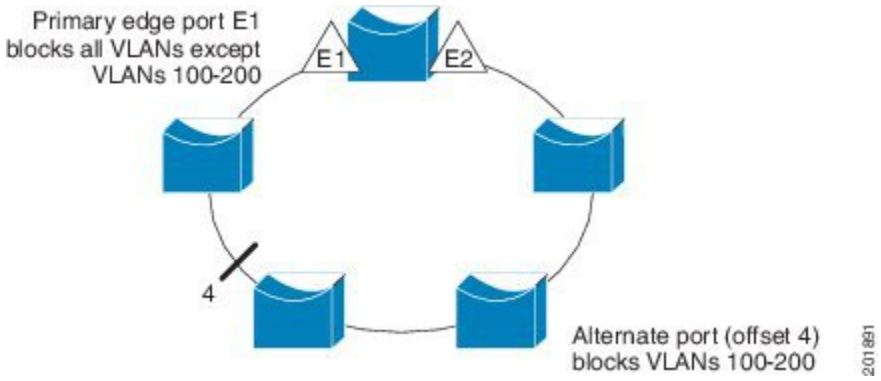
```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge no-neighbor primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
Switch (conf-if)# end
```

次に、下の図のように VLAN ブロッキングを設定する例を示します。 代替ポートは、ネイバー オフセット番号 4 のネイバーです。 手動によるプリエンプションのあと、VLAN 100 ～ 200 がこのポートでブロックされ、その他のすべての VLAN がプライマリ エッジ ポート E1（ギガビット イーサネット ポート 1/1）でブロックされます。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge primary
```

```
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end
```

図 *37* : ***VLAN*** ブロッキングの例



第 19 章

Flex Link および MAC アドレス テーブル移動更新機能の設定

- 機能情報の確認，443 ページ
- Flex Link および MAC アドレス テーブル移動更新設定の制約事項，443 ページ
- Flex Link および MAC アドレス テーブル移動更新に関する情報，444 ページ
- Flex Link および MAC アドレス テーブル移動更新機能の設定方法，451 ページ
- Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタリング，458 ページ
- Flex Link の設定例，459 ページ

機能情報の確認

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

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

Flex Link および MAC アドレス テーブル移動更新設定の制約事項

- Flex Link はレイヤ 2 ポートおよびポート チャネルだけでサポートされます。
- 最大 16 のバックアップ リンクを設定できます。

- アクティブ リンクには、Flex Link バックアップ リンクを 1 つだけ設定できます。バックアップ リンクは、アクティブ インターフェイスとは異なるインターフェイスにする必要があります。
- インターフェイスは 1 つの Flex Link ペアだけに属します。 インターフェイスは、1 つだけのアクティブ リンクのバックアップ リンクにすることができます。 アクティブ リンクは、別の Flex Link ペアに属することができません。
- どちらのリンクも、EtherChannel に属するポートには設定できません。 ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定でき、ポート チャネルおよび物理インターフェイスを Flex Link として設定して、ポート チャネルか物理インターフェイスのどちらかをアクティブ リンクにすることができます。
- バックアップ リンクはアクティブ リンクと同じタイプ（ギガビット イーサネットまたはポート チャネル）にする必要はありません。 ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の Flex Link を同様の特性で設定する必要があります。
- Flex Link ポートでは STP がディセーブルになります。 ポート上にある VLAN が STP 用に設定されている場合でも、Flex Link ポートは STP に参加しません。 STP がイネーブルでない場合は、設定されているトポロジでループが発生しないようにしてください。

関連トピック

Flex Link ペアのプリエンプション方式の設定，（452 ページ）
Flex Link の設定，（451 ページ）
Flex Link の設定：例，（459 ページ）
Flex Link の VLAN ロード バランシングの設定，（454 ページ）
Flex Link における VLAN ロード バランシングの設定：例，（460 ページ）
MAC アドレス テーブル移動更新メッセージの取得および処理用のスイッチ設定，（457 ページ）
MAC アドレス テーブル移動更新の設定，（456 ページ）
MAC アドレス テーブル移動更新の設定：例，（461 ページ）

Flex Link および MAC アドレス テーブル移動更新に関する情報

Flex Link

Flex Link は、レイヤ 2 インターフェイス（スイッチ ポートまたはポート チャネル）のペアで、一方のインターフェイスが他方のインターフェイスのバックアップとして機能するように設定されます。 この機能は、スパニングツリー プロトコル（STP）の代替ソリューションです。 ユーザは、STP をディセーブルにしても、基本的リンク冗長性を保つことができます。 Flex Link は、通常、ユーザがスイッチで STP を実行したくない場合に、サービス プロバイダーまたは企業ネット

ワークで設定されます。 スイッチが STP を実行中の場合は、STP がすでにリンクレベルの冗長性またはバックアップを提供しているため、Flex Link は不要です。

別のレイヤ 2 インターフェイスを Flex Link またはバックアップ リンクとして割り当てることで、1 つのレイヤ 2 インターフェイス（アクティブ リンク）に Flex Link を設定します。 スイッチ では、Flex Link を同じスイッチまたはスタックの別のスイッチ上で使用できます。 リンクの 1 つがアップでトラフィックを転送しているときは、もう一方のリンクがスタンバイ モードで、このリンクがシャットダウンした場合にトラフィックの転送を開始できるように準備しています。 どの時点でも、1 つのインターフェイスのみがリンクアップ ステートでトラフィックを転送しています。 プライマリ リンクがシャットダウンされると、スタンバイ リンクがトラフィックの転送を開始します。 アクティブ リンクがアップに戻った場合はスタンバイ モードになり、トラフィックが転送されません。 STP は Flex Link インターフェイス上ではディセーブル化されています。

関連トピック

Flex Link ペアのプリエンプション方式の設定 ,（452 ページ）

Flex Link の設定,（451 ページ）

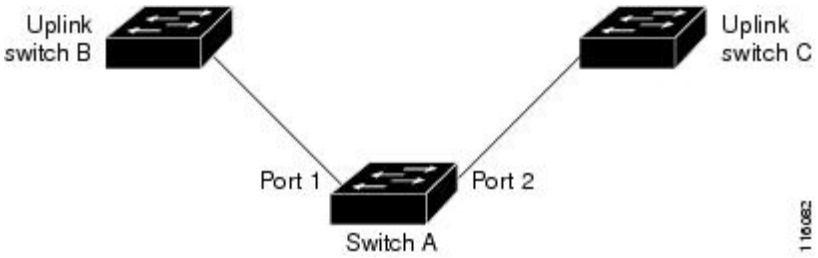
Flex Link の設定：例,（459 ページ）

Flex Link の設定

次の図では、スイッチ 上のポート 1 と 2 がアップリンク スイッチ B と C に接続されています。これらのスイッチは Flex Link として設定されているので、どちらかのインターフェイスがトラフィックを転送し、もう一方のインターフェイスはスタンバイ モードになります。 ポート 1 がアクティブ リンクになる場合、ポート 1 とスイッチ B との間でトラフィックの転送を開始し、ポート 2（バックアップ リンク）とスイッチ C との間のリンクでは、トラフィックは転送されません。ポート 1 がダウンすると、ポート 2 がアップ状態になってスイッチ C へのトラフィックの転送を開始します。ポート 1 が再びアップ状態に戻ってもスタンバイ モードになり、トラフィックを転送しません。ポート 2 がトラフィック転送を続けます。

また、トラフィックを転送する優先ポートを指定して、プリエンプション機能を設定できます。たとえば、プリエンプション モードと Flex Link ペアを設定できます。 図のシナリオでは、ポート 1 がバックアップとなって、ポート 2 より帯域幅が大きい場合、ポート 1 は 60 秒後にパケットの転送を開始します。 ポート 2 がスタンバイとなります。 これを行うには、**switchport backup interface preemption mode bandwidth** および **switchport backup interface preemption delay** インターフェイス コンフィギュレーション コマンドを入力します。

図 ***38*** : ***Flex Link*** の設定例



プライマリ（転送）リンクがダウンすると、トラップによってネットワーク管理ステーションが通知を受けます。 スタンバイ リンクがダウンすると、トラップによってユーザが通知を受けます。

Flex Link はレイヤ 2 ポートおよびポート チャネルだけでサポートされ、VLAN またはレイヤ 3 ポートではサポートされません。

関連トピック

Flex Link ペアのプリエンプション方式の設定 ，（452 ページ）

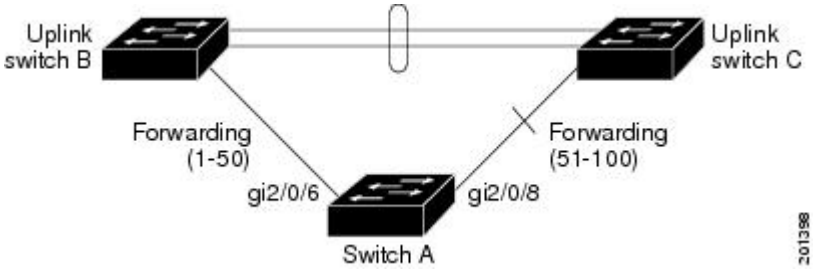
Flex Link の設定，（451 ページ）

VLAN Flex Link ロード バランシングおよびサポート

VLAN Flex Link ロード バランシングにより、ユーザは相互排他的な VLAN のトラフィックを両方のポートで同時に転送するように Flex Link ペアを設定できます。 たとえば、Flex Link ポートが 1 ～ 100 の VLAN に対して設定されている場合、最初の 50 の VLAN のトラフィックを 1 つのポートで転送し、残りの VLAN のトラフィックをもう一方のポートで転送できます。 どちらかのポートで障害が発生した場合には、もう一方のアクティブ ポートがすべてのトラフィックを転送します。 障害が発生したポートが元に戻ると、優先 VLAN のトラフィックの転送を再開します。 冗長性を提供する以外に、この Flex Link のペアはロード バランシングに使用できます。 Flex Link VLAN ロード バランシングによってアップリンク スイッチが制約を受けることはありません。

次の図に、Flex Link の VLAN ロードバランシング設定を示します。

図 *39*：*VLAN Flex Link* ロード バランシングの設定例



Flex Link フェールオーバーによるマルチキャスト高速コンバージェンス

Flex Link マルチキャスト高速コンバージェンスにより、Flex Link 障害発生後のマルチキャスト トラフィック コンバージェンス時間が短縮されます。 マルチキャスト高速コンバージェンスは mrouter ポートとしてのバックアップ リンクの学習、IGMP レポートの生成、および IGMP レポートのリークを組み合わせて実行されます。

関連トピック

Flex Link フェールオーバーによるマルチキャスト高速コンバージェンスの設定: 例，（462 ページ）

その他の Flex Link ポートを mrouter ポートとして学習

通常のマルチキャスト ネットワークでは、個々の VLAN について 1 つのクエリアが選定されます。 ネットワーク エッジに展開されたスイッチには、クエリーを受信するいずれかの Flex Link ポートが存在します。 Flex Link ポートは常に、転送状態になります。

クエリーを受信するポートが、スイッチの mrouter ポートとして追加されます。 mrouter ポートは、スイッチが学習したすべてのマルチキャスト グループの 1 つとして認識されます。 切り替えの後、クエリーは別の Flex Link ポートによって受信されます。 この別の Flex Link ポートは mrouter ポートとして認識されるようになります。 切り替えの後、マルチキャスト トラフィックは別の Flex Link ポートを介して流れます。 トラフィック コンバージェンスを高速化するために、いずれかの Flex Link ポートが mrouter ポートとして学習されると、両方の Flex Link ポートが mrouter ポートとして認識されます。 いずれの Flex Link ポートも常に、マルチキャスト グループの一部として扱われます。

通常の動作モードではいずれの Flex Link ポートもグループの一部として認識されますが、バックアップ ポートを通過するトラフィックはすべてブロックされます。 mrouter ポートとしてバックアップ ポートを追加しても、通常のマルチキャスト データ フローが影響を受けることはありません。 切り替えが生じると、バックアップ ポートのブロックが解除され、トラフィックが流れるようになります。 この場合、バックアップ ポートのブロックが解除されるとただちに、アップストリーム データが流れ始めます。

IGMP レポートの生成

切り替えの後、バックアップ リンクがアップ状態になると、アップストリームでの新しいディストリビューション スイッチでのマルチキャストデータの転送は開始されません。これは、ブロックされた Flex Link ポートに接続されているアップストリーム ルータのポートが、マルチキャスト グループの一部として認識されないからです。 マルチキャスト グループのレポートは、バックアップ リンクがブロックされているため、ダウンストリーム スイッチで転送されませんでした。 このポートのデータは、マルチキャスト グループが学習されるまで流れません。マルチキャスト グループの学習は、レポートを受信した後にだけ行われます。

レポートは、一般クエリーが受信されると、ホストより送信されます。一般クエリーは、通常のシナリオであれば 60 秒以内に送信されます。 バックアップ リンクが転送を開始し、マルチキャストデータの高速コンバージェンスを達成できるようになると、ダウンストリーム スイッチが一般クエリーを待つことなく、ただちにこのポート上のすべての学習済みグループに対し、プロキシ レポートを送信します。

IGMP レポートのリーク

マルチキャスト トラフィック コンバージェンスを最小限の損失で達成できるように、Flex Link のアクティブ リンクがダウンする前に冗長データ パスを設定しておく必要があります。 これは、Flex Link バックアップ リンクで IGMP レポート パケットだけをリークさせることで行えます。 こうしてリークさせた IGMP レポート メッセージがアップストリームのディストリビューション ルータで処理されるため、マルチキャストデータのトラフィックはバックアップ インターフェイスに転送されます。 バックアップ インターフェイスの着信トラフィックはすべてアクセス スイッチの入り口部分でドロップされるため、ホストが重複したマルチキャスト トラフィックを受信す

ることはありません。 Flex Link のアクティブ リンクに障害が発生した場合、ただちにアクセス スイッチがバックアップ リンクからのトラフィックを受け入れ始めます。 このスキームの唯一の欠点は、ディストリビューション スイッチ間のリンク、およびディストリビューションとアクセス スイッチの間のバックアップ リンクで帯域幅が大幅に消費される点です。 この機能はデフォルトでディセーブルになっています。**switchport backup interface** *interface-id* **multicast fast-convergence** コマンドを使用して、設定を変更できます。

切り替え時にこの機能がイネーブルになっている場合、スイッチで転送ポートに設定されたバックアップ ポート上でプロキシ レポートは生成されません。

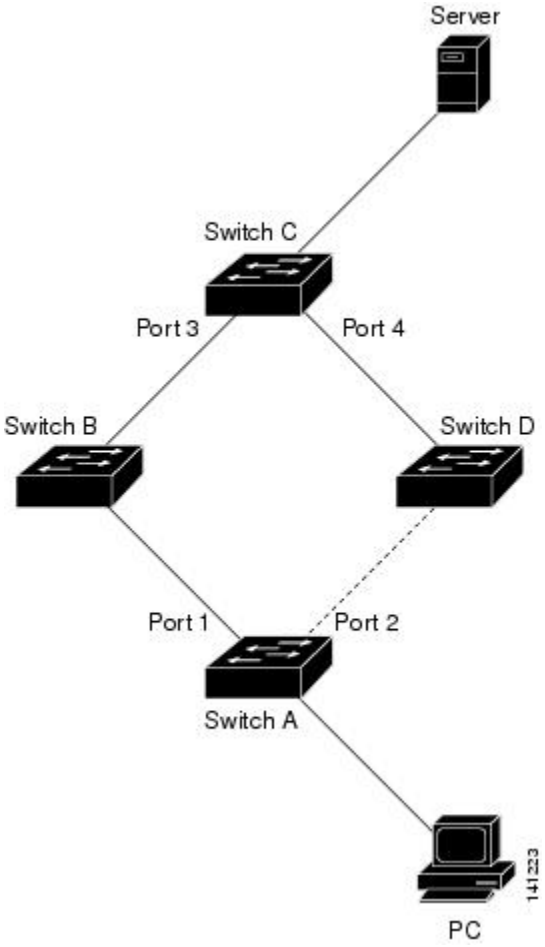
MAC アドレス テーブル移動更新

MAC アドレス テーブル移動更新機能により、プライマリ（転送）リンクがダウンしてスタンバイ リンクがトラフィックの転送を開始したときに、スイッチで高速双方向コンバージェンスが提供されます。

次の図では、スイッチ A がアクセス スイッチで、スイッチ A のポート 1 および 2 が Flex Link ペア経由でアップリンク スイッチ B および D に接続されます。 ポート 1 はトラフィックの転送中で、ポート 2 はバックアップ ステートです。 PC からサーバへのトラフィックはポート 1 からポー

ト 3 に転送されます。 PC の MAC アドレスはスイッチ C のポート 3 で学習されています。サーバから PC へのトラフィックはポート 3 からポート 1 に転送されます。

図 *40* : *MAC* アドレス テーブル移動更新の例



MAC アドレス テーブル移動更新機能が設定されておらず、ポート 1 がダウンした場合は、ポート 2 がトラフィックの転送を開始します。 しかし、少しの間、スイッチ C がポート 3 経由でサーバから PC にトラフィックを転送し続けるため、ポート 1 がダウンしていることにより、PC へのトラフィックが途切れます。 スイッチ C がポート 3 で PC の MAC アドレスを削除し、ポート 4 で再度学習した場合は、トラフィックはポート 2 経由でサーバから PC へ転送される可能性があります。

スイッチで MAC アドレス テーブル移動更新機能が設定されイネーブル化されていると、ポート 1 がダウンした場合、ポート 2 が PC からサーバへのトラフィックの転送を開始します。 スイッチは、ポート 2 から MAC アドレス テーブル移動更新パケットを送信します。 スイッチ C はこのパケットをポート 4 で受信し、ただちにポート 4 で PC の MAC アドレスを学習します。これにより、再コンバージェンス時間が短縮されます。

スイッチ、スイッチ A のアクセスを設定して、MAC アドレス テーブル移行更新メッセージを送信できます。 また、アップリンク スイッチ B、C、および D を設定して、MAC アドレス テーブ

ル移動更新メッセージの取得および処理を行うこともできます。 スイッチ C が スイッチ A から MAC アドレス テーブル移動更新メッセージを取得すると、スイッチ C はポート 4 で PC の MAC アドレスを学習します。 スイッチ C は、PC の転送テーブル エントリ転送を含め、MAC アドレス テーブルをアップデートします。

スイッチ A が、MAC アドレス テーブル移動更新を待機する必要はありません。 スイッチ はポート 1 上の障害を検出して、ただちに新しい転送ポートであるポート 2 からのサーバ トラフィックの転送を開始します。 この変更は 100 ミリ秒 (ms) 未満で発生します。 PC はスイッチ A に直接接続され、その接続状態に変更はありません。 スイッチ A による、MAC アドレス テーブルで PC エントリの更新は必要ありません。

関連トピック

MAC アドレス テーブル移動更新メッセージの取得および処理用のスイッチ設定 , （457 ページ）

MAC アドレス テーブル移動更新の設定, （456 ページ）

MAC アドレス テーブル移動更新の設定：例, （461 ページ）

Flex Link の VLAN ロード バランシング設定時の注意事項

- Flex Link VLAN ロード バランシングでは、バックアップ インターフェイス上で優先される VLAN を選択する必要があります。
- 同じ Flex Link ペアに対して、プリエンプション メカニズムと VLAN ロード バランシングを設定することはできません。

関連トピック

Flex Link の VLAN ロード バランシングの設定 , （454 ページ）

Flex Link における VLAN ロード バランシングの設定：例, （460 ページ）

MAC アドレス テーブル移動更新設定時の注意事項

- アクセス スイッチでこの機能のイネーブル化と設定を行うと、MAC アドレス テーブル移動更新を送信（*send*）できます。
- MAC アドレス テーブル移動更新メッセージを取得（*get*）する場合、この機能をアップリンク スイッチでイネーブルにして設定します。

デフォルトの Flex Link および MAC アドレス テーブル移動更新の設定

- Flex Link は設定されておらず、バックアップ インターフェイスは定義されていません。
- プリエンプション モードはオフです。
- プリエンプション遅延は 35 秒です。

- MAC アドレス テーブル移動更新機能は、 スイッチ上で設定されません。

関連トピック

Flex Link ペアのプリエンプション方式の設定 , （452 ページ）
Flex Link の設定, （451 ページ）
Flex Link の設定：例, （459 ページ）

Flex Link および MAC アドレス テーブル移動更新機能の設定方法

Flex Link の設定

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. **switchport backup interface***interface-id*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(conf)# interface gigabitethernet1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。 インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。 ポートチャネル範囲は 1 ～ 24 です。
ステップ 3	**switchport backup interface***interface-id* 例： `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2`	物理レイヤ 2 インターフェイス（ポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。

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

関連トピック

Flex Link, （444 ページ）
デフォルトの Flex Link および MAC アドレス テーブル移動更新の設定, （450 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （443 ページ）
Flex Link の設定：例, （459 ページ）
Flex Link の設定, （445 ページ）
Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタリング, （458 ページ）
Flex Link の設定：例, （459 ページ）

Flex Link ペアのプリエンプション方式の設定

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport backup interface** *interface-id*
4. **switchport backup interface** *interface-id* **preemption mode** [**forced** | **bandwidth** | **off**]
5. **switchport backup interface** *interface-id* **preemption delay** *delay-time*
6. **end**
7. **show interface** [*interface-id*] **switchport backup**
8. **copy running-config startup config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Switch(conf)# interface gigabitethernet1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。 ポートチャネル範囲は 1 ～ 24 です。
ステップ 3	**switchport backup interface** *interface-id* 例： `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2`	物理レイヤ 2 インターフェイス（ポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**switchport backup interface** *interface-id* **preemption mode** [**forced** | **bandwidth** | **off**] 例： `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption mode forced`	Flex Link インターフェイス ペアのプリエンプション メカニズムおよび遅延を設定します。 次のプリエンプション モードを設定することができます。 • **forced**：（任意）アクティブ インターフェイスはバックアップを常にプリエンプトします。 • **bandwidth**：（任意）より大きい帯域幅のインターフェイスが常にアクティブ インターフェイスとして動作します。 • **off**：アクティブからバックアップへのプリエンプトは発生しません。
ステップ 5	**switchport backup interface** *interface-id* **preemption delay** *delay-time* 例： `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption delay 50`	ポートが他のポートより先に使用されるまでの遅延時間を設定します。 （注） 遅延時間の設定は、forced モードおよび bandwidth モードでのみ有効です。
ステップ 6	**end** 例： `Switch(conf-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interface** [*interface-id*] **switchport backup** 例： `Switch# show interface`	設定を確認します。

	コマンドまたはアクション	目的
	`gigabitethernet1/0/2 switchport backup`	
ステップ 8	**copy running-config startup config** 例： `Switch# copy running-config startup config`	（任意）スイッチスタートアップコンフィギュレーションファイルに設定を保存します。

関連トピック

Flex Link, （444 ページ）
デフォルトの Flex Link および MAC アドレス テーブル移動更新の設定, （450 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （443 ページ）
Flex Link の設定：例, （459 ページ）
Flex Link の設定, （445 ページ）
Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタリング, （458 ページ）
Flex Link の設定：例, （459 ページ）

Flex Link の VLAN ロード バランシングの設定

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **switchport backupinterface***interface-id***prefer vlan***vlan-range*
4. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface***interface-id* 例： `Switch (config)# interface gigabitethernet2/0/6`	インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポートチャネル範囲は 1 ～ 24 です。
ステップ 3	**switchport backupinterface***interface-id***prefer vlan***vlan-range* 例： `Switch (config-if)# switchport backup interface gigabitethernet2/0/8 prefer vlan 2`	物理レイヤ 2 インターフェイス（またはポート チャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定し、インターフェイス上の VLAN を指定します。VLAN ID の範囲は 1 ～ 4094 です。
ステップ 4	**end** 例： `Switch (config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

Flex Link の VLAN ロード バランシング設定時の注意事項, （450 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （443 ページ）
Flex Link における VLAN ロード バランシングの設定：例, （460 ページ）
Flex Link における VLAN ロード バランシングの設定：例, （460 ページ）
Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタリング, （458 ページ）

MAC アドレス テーブル移動更新の設定

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. 次のいずれかを使用します。
   - **switchport backupinterface***interface-id*
   - **switchport backupinterface***interface-id***mmu primary vlan***vlan-id*
4. **end**
5. **mac address-table move update transmit**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch#interface gigabitethernet1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスは物理レイヤ2インターフェイスまたはポートチャネル（論理インターフェイス）に設定できます。 ポートチャネル範囲は 1 ～ 24 です。
ステップ 3	次のいずれかを使用します。 • **switchport backupinterface***interface-id* • **switchport backupinterface***interface-id***mmu primary vlan***vlan-id* 例： `Switch(config-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 2`	物理レイヤ2インターフェイス（またはポートチャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定します。 MAC アドレス テーブル移動更新 VLAN はインターフェイスで最も低い VLAN ID です。 物理レイヤ2インターフェイス（ポートチャネル）を設定し、MAC アドレス テーブル移動更新の送信に使用される VLAN ID をインターフェイスで指定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**mac address-table move update transmit** 例： `Switch(config)# mac address-table move update transmit`	プライマリ リンクがダウンし、スタンバイ リンクを介してスイッチがトラフィックの転送を開始すると、アクセス スイッチで、ネットワークの他のスイッチにMACアドレステーブル移動更新を送信できます。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MAC アドレス テーブル移動更新の設定：例, （461 ページ）
Flex Link、マルチキャスト高速コンバージェンス、およびMAC アドレス テーブル移動更新のモニタリング, （458 ページ）
MAC アドレス テーブル移動更新, （448 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （443 ページ）
MAC アドレス テーブル移動更新の設定：例, （461 ページ）

MAC アドレス テーブル移動更新メッセージの取得および処理用のスイッチ設定

手順の概要

1. **configure terminal**
2. **mac address-table move update receive**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**mac address-table move update receive** 例： `Switch (config)# mac address-table move update receive`	スイッチで MAC アドレス テーブル移動更新の取得と処理を可能にします。
ステップ 3	**end** 例： `Switch (config)# end`	特権 EXEC モードに戻ります。

関連トピック

Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタリング, （458 ページ）
MAC アドレス テーブル移動更新の設定：例, （461 ページ）
MAC アドレス テーブル移動更新, （448 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （443 ページ）
MAC アドレス テーブル移動更新の設定：例, （461 ページ）

Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタリング

コマンド	目的
show interface [*interface-id*] **switchport backup**	インターフェイス用に設定された Flex Link バックアップ インターフェイス、または設定されたすべての Flex Link と、各アクティブ インターフェイスおよびバックアップ インターフェイスの状態（アップまたはスタンバイ モード）を表示します。

コマンド	目的
show ip igmp profile address-table move update *profile-id*	特定の IGMP プロファイルまたはスイッチ上で定義されているすべての IGMP プロファイルを表示します。
show mac address-table move update	スイッチに関する MAC アドレス テーブル移動更新情報を表示します。

関連トピック

Flex Link ペアのプリエンプション方式の設定，（452 ページ）

Flex Link の設定，（451 ページ）

Flex Link の設定例

Flex Link の設定：例

この例では、バックアップ インターフェイスでインターフェイスを設定した後に、設定を確認する方法を示します。

```
Switch# show interface switchport backup

Switch Backup Interface Pairs:
Active Interface Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/0/1 GigabitEthernet1/0/2 Active Up/Backup Standby
```

この例では、バックアップ インターフェイス ペアにプリエンプション モードを強制として設定した後に、設定を確認する方法を示します。

```
Switch# show interface switchport backup detail

Switch Backup Interface Pairs:

Active Interface Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/0/211 GigabitEthernet1/0/2 Active Up/Backup Standby
Interface Pair : Gi1/0/1, Gi1/0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi1/0/1), 100000 Kbit (Gi1/0/2)
Mac Address Move Update Vlan : auto
```

関連トピック

Flex Link ペアのプリエンプション方式の設定，（452 ページ）

Flex Link の設定，（451 ページ）

Flex Link，（444 ページ）

デフォルトの Flex Link および MAC アドレス テーブル移動更新の設定，（450 ページ）

Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （443 ページ）
Flex Link ペアのプリエンプション方式の設定 , （452 ページ）
Flex Link の設定, （451 ページ）

Flex Link における VLAN ロード バランシングの設定：例

次の例では、スイッチに VLAN 1 ～ 50、60、および 100 ～ 120 を設定する例を示します。

```
Switch(config)# interface gigabitethernet 2/0/6
Switch(config-if)# switchport backup interface gigabitethernet 2/0/8 prefer vlan 60,100-120
```

両方のインターフェイスが起動しているとき、Gi2/0/8 は VLAN 60 および 100 ～ 120 のトラフィックを転送し、Gi2/0/6 は VLAN 1 ～ 50 のトラフィックを転送します。

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがダウンすると（LINK_DOWN）、このインターフェイスで優先される VLAN は、Flex Link ペアのピア インターフェイスに移動します。 この例では、インターフェイス Gi2/0/6 がダウンして、Gi2/0/8 が Flex Link ペアのすべての VLAN を引き継ぎます。

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

FlexLink インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートに移動します。 次に、インターフェイス Gi2/0/6 が起動すると、このインターフェイスの優先 VLAN は、ピア インターフェイス Gi2/0/8 ではブロックされ、Gi2/0/6 で転送されます。

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

Switch# show interfaces switchport backup detail
```

```
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet1/0/3       FastEthernet1/0/4       Active Down/Backup Up

Vlans Preferred on Active Interface: 1-2,5-4094
Vlans Preferred on Backup Interface: 3-4
Preemption Mode  : off
Bandwidth : 10000 Kbit (Fa1/0/3), 100000 Kbit (Fa1/0/4)
Mac Address Move Update Vlan : auto
```

関連トピック

Flex Link の VLAN ロード バランシングの設定，（454 ページ）
Flex Link の VLAN ロード バランシング設定時の注意事項，（450 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項，（443 ページ）
Flex Link の VLAN ロード バランシングの設定，（454 ページ）

MAC アドレス テーブル移動更新の設定：例

この例では、MAC アドレス テーブル移動更新を送信するようにアクセス スイッチを設定した後に設定を確認する方法を示します。

```
Switch# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

関連トピック

MAC アドレス テーブル移動更新の設定，（456 ページ）
MAC アドレス テーブル移動更新メッセージの取得および処理用のスイッチ設定，（457 ページ）
MAC アドレス テーブル移動更新メッセージの取得および処理用のスイッチ設定，（457 ページ）
MAC アドレス テーブル移動更新の設定，（456 ページ）
MAC アドレス テーブル移動更新，（448 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項，（443 ページ）

Flex Link フェールオーバーによるマルチキャスト高速コンバージェンスの設定: 例

次に、Flex Link を GigabitEthernet1/0/11 および GigabitEthernet1/0/12 に設定したときに他の Flex Link ポートを mrouter ポートとして学習する例と、**show interfaces switchport backup** コマンドの出力を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface GigabitEthernet1/0/12
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/0/12
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet1/0/11 GigabitEthernet1/0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto
```

この出力は、GigabitEthernet1/0/11 を介してスイッチに到達するクエリーのある、VLAN 1 および 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier

Vlan   IP Address     IGMP Version      Port
-----------------------------------------------------------
1      1.1.1.1        v2      Gi1/0/11
401    41.41.41.1     v2      Gi1/0/11
```

この例では、VLAN 1 および VLAN 401 用の **show ip igmp snooping mrouter** コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter

Vlan   ports
----   -----
1     Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401   Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

同様に、両方の Flex Link ポートが学習されたグループに属しています。 次の例では、GigabitEthernet2/0/11 は VLAN 1 のレシーバ/ホストであり、2 つのマルチキャスト グループに関連しています。

```
Switch# show ip igmp snooping groups

Vlan   Group    Type   Version    Port List
------------------------------------------------------------------------
1   228.1.5.1    igmp   v2    Gi1/0/11, Gi1/0/12, Gi2/0/11
1   228.1.5.2    igmp   v2    Gi1/0/11, Gi1/0/12, Gi2/0/11
```

ホストが一般クエリーに応答するときに、スイッチはすべてのマルチキャストルータ ポートに関するこのレポートを転送します。 次の例では、ホストがグループ 228.1.5.1 のレポートを送信するとき、バックアップ ポート GigabitEthernet1/0/12 はブロックされているので、レポートは

GigabitEthernet1/0/11 でだけ送信されます。 アクティブ リンク GigabitEthernet1/0/11 がダウンすると、バックアップ ポート GigabitEthernet1/0/12 が転送を開始します。

このポートが転送を開始すると、ただちにスイッチがホストに代わり、228.1.5.1 と 228.1.5.2 のグループにプロキシ レポートを送信します。 アップストリーム ルータはグループを学習し、マルチキャスト データの転送を開始します。 これは、Flex Link のデフォルトの動作です。 ユーザが **switchport backup interface gigabitEthernet 1/0/12 multicast fast-convergence** コマンドを使用して高速コンバージェンスを設定すると、この動作は変更されます。 次に、この機能をオンにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 1/0/11
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/12 multicast
fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:
Active       Interface       Backup Interface State
------------------------------------------------------------------------------
GigabitEthernet1/0/11  GigabitEthernet1/0/12  Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto
```

この出力は、GigabitEthernet1/0/11 を介してスイッチに到達するクエリーのある、VLAN 1 および 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier

Vlan    IP Address     IGMP Version     Port
-----------------------------------------------------------------
1      1.1.1.1        v2     Gi1/0/11
401    41.41.41.1     v2     Gi1/0/11
```

次に VLAN 1 と 401 に対する **show ip igmp snooping mrouter** コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter

Vlan    ports
----    -----
1    Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401    Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

同様に、両方の Flex Link ポートが学習されたグループに属しています。 次の例では、GigabitEthernet2/0/11 は VLAN 1 のレシーバ/ホストであり、2 つのマルチキャスト グループに関連しています。

```
Switch# show ip igmp snooping groups

Vlan   Group    Type   Version    Port List
------------------------------------------------------------------------
1   228.1.5.1    igmp   v2    Gi1/0/11, Gi1/0/12, Gi2/0/11
1   228.1.5.2    igmp   v2    Gi1/0/11, Gi1/0/12, Gi2/0/11
```

一般クエリーに対してあるホストが応答すると必ず、スイッチがすべての mrouter ポートに関するこのレポートを転送します。 コマンドライン ポートを使用してこの機能をオンにすると、レポートは、GigabitEthernet1/0/11 上のスイッチによって転送されるときにバックアップ ポート

GigabitEthernet1/0/12 にも送信されます。 アップストリーム ルータはグループを学習し、マルチキャストデータの転送を開始します。GigabitEthernet1/0/12 はブロックされているので、このデータは入力でドロップされます。 アクティブ リンク GigabitEthernet1/0/11 がダウンすると、バックアップ ポート GigabitEthernet1/0/12 が転送を開始します。 マルチキャストデータはアップストリームルータによりすでに転送されているため、いずれのプロキシレポートも送信する必要がありません。 レポートをバックアップ ポートにリークすると冗長マルチキャスト パスが設定され、マルチキャスト トラフィック コンバージェンス用の時間が最小限になります。

関連トピック

Flex Link フェールオーバーによるマルチキャスト高速コンバージェンス, （446 ページ）

第 20 章

単方向リンク検出の設定

- 機能情報の確認，465 ページ
- UDLD 設定の制約事項，465 ページ
- UDLD について，466 ページ
- UDLD の設定方法，469 ページ
- UDLD のモニタおよびメンテナンス，472 ページ

機能情報の確認

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

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

UDLD 設定の制約事項

次に、単方向リンク検出（UDLD）設定の制約事項を示します。

- UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。
- モード（通常またはアグレッシブ）を設定する場合、リンクの両側に同じモードを設定します。

⚠

注意 ループ ガードは、ポイントツーポイント リンクでのみサポートされます。 リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

UDLD について

UniDirectional Link Detection（UDLD）は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニタリングしたり、単一方向リンクの存在を検出できるようにするためのレイヤ 2 プロトコルです。 このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。 UDLD は単一方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。 単一方向リンクは、スパニングツリー トポロジループをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。通常モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できます。 アグレッシブ モードの UDLD は、光ファイバ リンクおよびツイストペア リンク上の片方向トラフィックと、光ファイバ リンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ 1 のメカニズムを使用して、リンクの物理ステータスを学習します。 レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。 UDLD は、ネイバー ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。 自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合に、単一方向リンクが発生します。

通常モード

通常モードの UDLD は、光ファイバ ポートの光ファイバが誤って接続されている場合に単一方向リンクを検出しますが、レイヤ 1 メカニズムは、この誤った接続を検出しません。 ポートが正しく接続されていてもトラフィックが片方向である場合、単一方向リンクを検出するはずのレイヤ 1 メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。 この場合、論理リンクは不確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ 1 メカニズムがリンクの物理的な問題を検出するため、リンクは稼働状態でなくなります。 この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされます。

関連トピック

UDLD のグローバルなイネーブル化, （469 ページ）
インターフェイスでの UDLD のイネーブル化, （471 ページ）

Aggressive Mode

アグレッシブ モードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。 アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイント リンクの単一方向リンクも検出できます。 また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがトラフィックを送受信できない。
- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがダウンし、残りのインターフェイスが稼働している。
- ケーブルのうち 1 本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイント リンクでは、UDLD hello パケットをハートビートと見なすことができ、ハートビートがあればリンクは正常です。 逆に、ハートビートがないということは、双方向リンクを再確立できない限り、リンクをシャットダウンする必要があることを意味しています。

レイヤ 1 の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブ モードの UDLD はそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。 自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは自動ネゴシエーションでは実行できません。

関連トピック

UDLD のグローバルなイネーブル化, （469 ページ）
インターフェイスでの UDLD のイネーブル化, （471 ページ）

単一方向の検出方法

UDLD は、2 つの方法で動作します。

- ネイバー データベース メンテナンス
- イベントドリブン検出およびエコー

関連トピック

UDLD のグローバルなイネーブル化, （469 ページ）
インターフェイスでの UDLD のイネーブル化, （471 ページ）

ネイバー データベース メンテナンス

UDLDは、アクティブな各ポート上でhelloパケット（別名アドバタイズまたはプローブ）を定期的に送信して、他のUDLD対応ネイバーに関して学習し、各デバイスがネイバーに関する情報を常に維持できるようにします。

スイッチがhelloメッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、情報をキャッシュします。 古いキャッシュ エントリの期限が切れる前に、スイッチが新しいhelloメッセージを受信すると、スイッチが古いエントリを新しいエントリで置き換えます。

UDLDの実行中にポートがディセーブルになったり、ポート上でUDLDがディセーブルになったり、またはスイッチをリセットした場合、UDLDは設定変更の影響を受けるポートの既存のキャッシュ エントリをすべてクリアします。 UDLDは、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを1つまたは複数送信します。 このメッセージは、キャッシュを継続的に同期するためのものです。

イベントドリブン検出およびエコー

UDLDは検出動作としてエコーを利用します。 UDLDデバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続のUDLDデバイス側の検出ウィンドウを再起動して、エコーメッセージを返送します。 この動作はすべてのUDLDネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLDモードに応じてシャットダウンされることがあります。 UDLDが通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。 UDLDがアグレッシブ モードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

関連トピック

UDLDのグローバルなイネーブル化, （469ページ）
インターフェイスでのUDLDのイネーブル化, （471ページ）

UDLD リセット オプション

インターフェイスがUDLDでディセーブル化された場合、次のオプションの1つを使用してUDLDをリセットできます。

- **udld reset** インターフェイス コンフィギュレーション コマンド。
- **shutdown** インターフェイス コンフィギュレーション コマンドに続いて **no shutdown** インターフェイス コンフィギュレーション コマンドを入力すると、ディセーブル化されたポートを再起動できます。
- **no udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドの後に **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを実行すると、ディセーブル化されたポートが再びイネーブルになります。

- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port [aggressive]** インターフェイス コンフィギュレーション コマンドを実行すると、ディセーブル化された光ファイバ ポートが再びイネーブルになります。
- **errdisable recovery cause udld** グローバル コンフィギュレーション コマンドを入力すると、UDLD の errdisable ステートから自動回復するタイマーをイネーブルにできます。さらに、**errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンドを入力すると、UDLD の errdisable ステートから回復する時間を指定できます。

関連トピック

UDLD のグローバルなイネーブル化, （469 ページ）
インターフェイスでの UDLD のイネーブル化, （471 ページ）

UDLD のデフォルト設定

表 *38* : ***UDLD*** のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ ポート上でディセーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX ポート上でディセーブル
UDLD アグレッシブ モード	ディセーブル

関連トピック

UDLD のグローバルなイネーブル化, （469 ページ）
インターフェイスでの UDLD のイネーブル化, （471 ページ）

UDLD の設定方法

UDLD のグローバルなイネーブル化

アグレッシブ モードまたは通常モードで UDLD をイネーブルにし、スイッチ上のすべての光ファイバ ポートに設定可能なメッセージ タイマーを設定するには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **udld**{**aggressive** | **enable** | **message time***message-timer-interval*}
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**udld**{**aggressive** | **enable** | **message time***message-timer-interval*} 例： `Switch(config)# udld enable message time 10`	UDLD モードの動作を指定します。 • **aggressive**：すべての光ファイバ ポート上で、UDLD をアグレッシブ モードでイネーブルにします。 • **enable**：スイッチ上のすべての光ファイバ ポート上で、UDLD を通常モードでイネーブルにします。 UDLD はデフォルトでディセーブルです。 個々のインターフェイスの設定は、**udld enable** グローバル コンフィギュレーション コマンドの設定を上書きします。 • **message time***message-timer-interval*：アドバタイズ フェーズに存在し、双方向と検出されたポートにおける UDLD プローブ メッセージ間の時間間隔を設定します。 有効な範囲は 1 ～ 90 秒です。デフォルト値は 15 です。 （注） このコマンドが作用するのは、光ファイバ ポートだけです。 他のポート タイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。 UDLD をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

UDLD のモニタおよびメンテナンス
Aggressive Mode, （467 ページ）
通常モード, （466 ページ）
単一方向の検出方法, （467 ページ）
イベントドリブン検出およびエコー, （468 ページ）
UDLD リセット オプション, （468 ページ）
UDLD のデフォルト設定, （469 ページ）

インターフェイスでの UDLD のイネーブル化

アグレッシブ モードまたは通常モードをイネーブルにする、またはポート上でUDLDをディセーブルにするには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **udld port** [**aggressive**]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	UDLD用にイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**udld port** [**aggressive**] 例： `Switch(config-if)# udld port aggressive`	UDLD はデフォルトでディセーブルです。 • **udld port**：指定されたポート上で、UDLD を通常モードでイネーブルにします。 • **udld port aggressive**：（任意）指定されたポート上でアグレッシブ モードで UDLD をイネーブルにします。

	コマンドまたはアクション	目的
		（注） 特定の光ファイバ ポート上で UDLD をディセーブルにする場合は、**no udld port** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

UDLD のモニタおよびメンテナンス
Aggressive Mode, （467 ページ）
通常モード, （466 ページ）
単一方向の検出方法, （467 ページ）
イベントドリブン検出およびエコー, （468 ページ）
UDLD リセット オプション, （468 ページ）
UDLD のデフォルト設定, （469 ページ）

UDLD のモニタおよびメンテナンス

コマンド	目的
show udld [*interface-id* | **neighbors**]	指定されたポートまたはすべてのポートの UDLD ステータスを表示します。

第 IV 部

High Availability（高可用性）

- HSRP および VRRP の設定，475 ページ
- サービス レベル契約の設定，501 ページ
- 拡張オブジェクト トラッキングの設定，525 ページ

第 21 章

HSRP および VRRP の設定

- HSRP の設定，475 ページ

HSRP の設定

この章では、ホット スタンバイ ルータ プロトコル（HSRP）を使用する方法について説明します。これによって、IP トラフィック ルーティングに冗長性を提供し、個々のルータのアベイラビリティに依存しないルーティングを実現します。

レイヤ 2 モードの HSRP のバージョンを使用すると、クラスタ コマンド スイッチが故障した場合、クラスタ管理を引き継ぐ冗長コマンド スイッチを設定することもできます。

（注） HSRP および VRRP 機能は Cisco Catalyst 3560-CXスイッチでのみサポートされます。

機能情報の確認

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

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

HSRP の設定に関する情報

HSRP の概要

HSRP は、デフォルト ゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファースト ホップ冗長性を確保することでネットワークのアベイラビリティを高めるシスコの標準方式です。 HSRP を使用すると、特定のルータのアベイラビリティに依存せず IP トラフィックをルーティングできます。 また、一連のルータ インターフェイスを組み合わせることで、1 台の仮想ルータ、または LAN 上のホストへのデフォルト ゲートウェイのように機能させることができます。 ネットワークまたはセグメント上に HSRP を設定すると、仮想 MAC（メディア アクセス コントロール）アドレス、および設定されたルータ グループ間で共有される IP アドレスを使用できるようになり HSRP が設定された複数のルータは、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスを使用できるようになります。 仮想ルータは、実際には存在しません。仮想ルータは、相互にバックアップ機能を提供するように設定されている複数のルータの共通のターゲットを表します。 1 台のルータがアクティブなルータとして、もう 1 台のルータがスタンバイ ルータとして選択されます。スタンバイ ルータは、指定されたアクティブ ルータが故障した場合に、グループの MAC アドレスおよび IP アドレスを制御するルータです。

（注） HSRP グループ内のルータには、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）など、HSRP をサポートする任意のルータ インターフェイスを指定できます。

HSRP は、ネットワーク上のホストからの IP トラフィックに冗長性を提供することで、ネットワークのアベイラビリティを高めます。 アクティブ ルータは、ルータ インターフェイスのグループ内でパケットのルーティングを実行するために選択されたルータです。スタンバイ ルータは、アクティブ ルータが故障した場合、または事前に設定した条件が満たされた場合に、ルーティング作業を引き継ぐルータです。

HSRP は、ホストがルータ ディスカバリ プロトコルをサポートしておらず、選択されたルータのリロードや電源故障時に新しいルータに切り替えることができない場合に有効です。 HSRP をネットワーク セグメントに設定すると、HSRP は仮想 MAC アドレスと IP アドレスを 1 つずつ提供します。このアドレスは、HSRP が動作するルータ インターフェイス グループ内のルータ インターフェイス間で共有できます。 プロトコルによってアクティブ ルータとして選択されたルータは、グループの MAC アドレス宛てのパケットを受信し、ルーティングします。 n 台のルータで HSRP が稼働している場合、n +1 個の IP アドレスおよび MAC アドレスが割り当てられます。

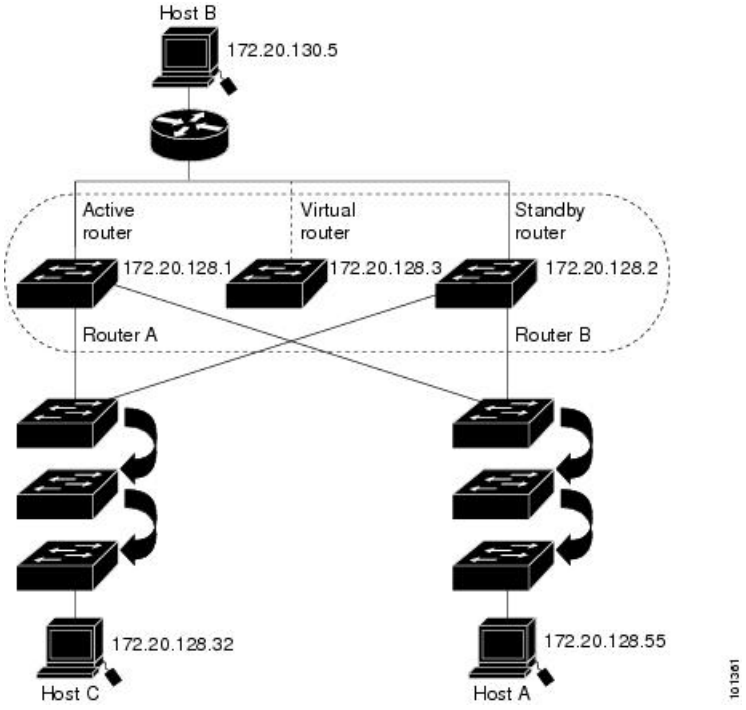
指定されたアクティブ ルータの故障を HSRP が検出すると、選択されているスタンバイ ルータがホットスタンバイ グループの MAC アドレスおよび IP アドレスの制御を引き継ぎます。 この時点で新しいスタンバイ ルータも選択されます。 HSRP が稼働しているデバイスは、マルチキャスト UDP ベースの hello パケットを送受信することにより、ルータ障害の検出、アクティブ ルータおよびスタンバイ ルータの指定を行います。 インターフェイスに HSRP が設定されている場合、そのインターフェイスではインターネット制御メッセージプロトコル（ICMP）のリダイレクトメッセージが自動的にイネーブルになっています。

レイヤ 3 で動作するスイッチおよびスイッチ スタック間で複数のホット スタンバイ グループを設定すると、冗長ルータをさらに活用できます。 そのためには、インターフェイスに設定するホットスタンバイ コマンド グループごとにグループ番号を指定します。 たとえば、スイッチ 1

のインターフェイスをアクティブ ルータ、スイッチ 2 のインターフェイスをスタンバイ ルータとして設定できます。また、スイッチ 2 の別のインターフェイスをアクティブ ルータ、スイッチ 1 の別のインターフェイスをスタンバイ ルータとして設定することもできます。

次の図に、HSRP 用に設定されたネットワークのセグメントを示します。 各ルータには、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスが設定されています。 ルータ A の IP アドレスをネットワーク上のホストに設定する代わりに、デフォルトルータとして仮想ルータの IP アドレスを設定します。 ホスト C からホスト B にパケットが送信される場合、ホスト C は仮想ルータの MAC アドレスにパケットを送信します。 何らかの理由により、ルータ A がパケットの転送を停止すると、ルータ B が仮想 IP アドレスおよび仮想 MAC アドレスに応答してアクティブ ルータとなり、アクティブ ルータの作業を行います。 ホスト C は引き続き仮想ルータの IP アドレスを使用し、ホスト B 宛のパケットをアドレッシングします。ルータ B はそのパケットを受信し、ホスト B に送信します。ルータ B は HSRP の機能を使用し、ルータ A が動作を再開するまで、ホスト B のセグメント上のユーザと通信する必要があるホスト C のセグメント上のユーザに連続的にサービスを提供します。また、ホスト A セグメントとホスト B の間で、引き続き通常のパケット処理機能を実行します。

図 *41*：*HSRP* の一般的な構成



レイヤ 3 で動作するスイッチおよびスイッチ スタック間で複数のホット スタンバイ グループを設定すると、冗長ルータをさらに活用できます。 そのためには、インターフェイスに設定するホットスタンバイ コマンド グループごとにグループ番号を指定します。 たとえば、スイッチ 1 のインターフェイスをアクティブ ルータ、スイッチ 2 のインターフェイスをスタンバイ ルータとして設定できます。また、スイッチ 2 の別のインターフェイスをアクティブ ルータ、スイッチ 1 の別のインターフェイスをスタンバイ ルータとして設定することもできます。

HSRP のバージョン

Cisco IOS XE Release 3.3SE 以降の製品は、下記のホットスタンバイ ルータ プロトコル（HSRP）バージョンをサポートしています。

スイッチでは、次の HSRP バージョンがサポートされます。

- HSRPv1：HSRP のバージョン 1（デフォルトのバージョン）。 次の機能があります。
  - HSRP グループ番号は 0 ～ 255 まで使用できます。
  - HSRPv1 は 224.0.0.2 のマルチキャスト アドレスを使用して hello パケットを送信しますが、これは Cisco Group Management Protocol（CGMP）の脱退処理と競合します。 HSRPv1 と CGMP は相互に排他的なため、同時には使用できません。
- HSRPv2：HSRP のバージョン 2。このバージョンには次の機能があります。
  - HSRPv2 は 224.0.0.102 のマルチキャスト アドレスを使用して hello パケットを送信します。 HSRPv2 と CGMP 脱退処理は相互に排他的ではありません。同時に使用できます。
  - HSRPv2 のパケット形式は、HSRPv1 とは異なります。

HSRPv1 を実行しているスイッチは、ルータの送信元 MAC アドレスが仮想 MAC アドレスのため、hello パケットを送信した物理的なルータを特定できません。

HSRPv2 のパケット形式は、HSRPv1 とは異なります。 HSRPv2 パケットは、パケットを送信した物理ルータの MAC アドレスを格納できる 6 バイトの識別子フィールドを持った、Type Length Value（TLV）形式を使用します。

HSRPv1 を実行しているインターフェイスが HSRPv2 パケットを取得した場合、このタイプ フィールドは無視されます。

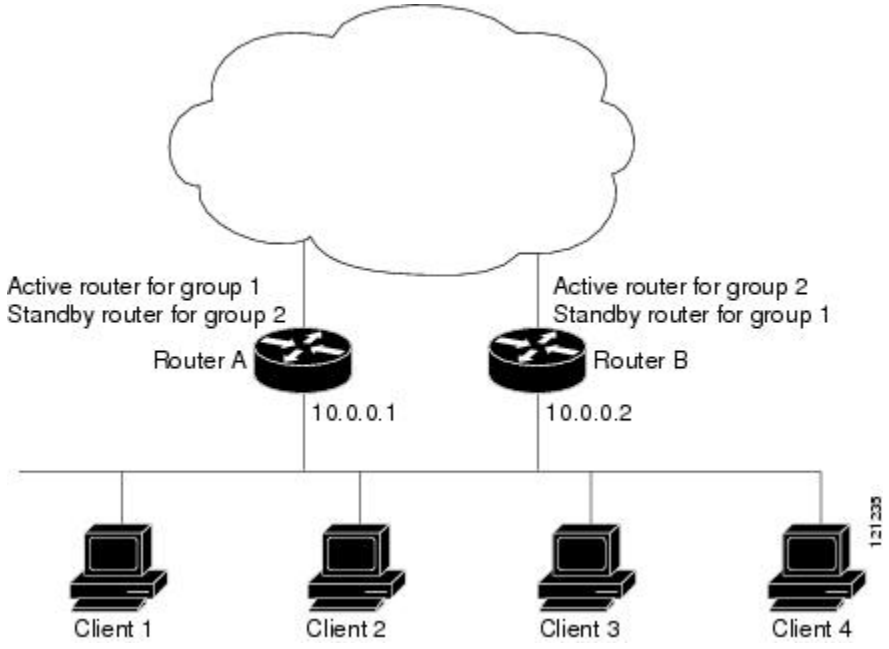
MHSRP

スイッチは、Multiple HSRP（MHSRP）をサポートします。MHSRP は HSRP の拡張版で、複数の HSRP グループ間でのロード シェアリングが可能です。 ホスト ネットワークからサーバ ネットワークまで、ロードバランシングを実現して複数のスタンバイ グループ（およびパス）を使用するために、MHSRP を設定できます。

下の図では、半分のクライアントがルータ A に設定されており、もう半分はルータ B に設定されています。ルータ A およびルータ B の設定により、合計 2 つの HSRP グループが確立されています。 グループ 1 では、ルータ A に最高のプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブ ルータになり、ルータ B がスタンバイ ルータとなります。 グループ 2 では、ルータ B に最も高いプライオリティが割り当てられているため、ルータ B がデフォルトのアクティブ ルータであり、ルータ A がスタンバイ ルータです。 通常の運用では、2 つのルータが IP トラフィック負荷を分散します。いずれかのルータが使用できなくなると、もう一方のルータがアクティブになり、使用できないルータのパケット転送機能を引き継ぎます。

（注） MHSRP では、ルータに障害が発生して正常に戻った場合にプリエンプションによりロードシェアリングを復元するために、**standby preempt** インターフェイス コンフィギュレーションコマンドを HSRP インターフェイスで入力する必要があります。

図 *42* : ***MSHRP*** ロード シェアリング



関連トピック

MHSRP の設定, （486 ページ）

SSO HSRP

SSO HSRP は、冗長なルート プロセッサ（RP）を装備したデバイスがステートフル スイッチオーバー（SSO）冗長モード用に設定されているときの HSRP の動作を変更します。 ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。

この機能を使用すると、HSRP の SSO 情報がスタンバイ RP に同期されるため、HSRP 仮想 IP アドレスを使用して送信されるトラフィックをスイッチオーバー中も引き続き転送できるほか、データの損失やパスの変更も発生しません。 さらに、HSRP アクティブ デバイスの両方の RP に障害が発生しても、スタンバイ状態の HSRP デバイスが HSRP アクティブ デバイスとして処理を引き継ぎます。

この機能は、動作の冗長モードが SSO に設定されている場合にデフォルトでイネーブルになっています。

HSRP の設定方法

HSRP のデフォルト設定

表 *39* : ***HSRP*** のデフォルト設定

機能	デフォルト設定
HSRP バージョン	Version 1
HSRP グループ	未設定
スタンバイ グループ番号	0
スタンバイ MAC アドレス	0000.0c07.acXX に指定されたシステム。XX は、HSRP グループ番号
スタンバイプライオリティ	100
スタンバイ遅延	0（遅延なし）
スタンバイでのインターフェイスプライオリティの追跡	10
スタンバイ hello 時間	3 秒
スタンバイ ホールドタイム	10 秒

HSRP HSRP 設定時の注意事項

- HSRPv2 および HSRPv1 は相互に排他的です。 HSRPv2 は、同じインターフェイス上で HSRPv1 と一緒には動作しません（その逆も同様）。
- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - ルーテッド ポート：インターフェイス コンフィギュレーション モードで **no switchport** コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。
  - SVI：グローバル コンフィギュレーション モードで **interface vlan***vlan_id* によって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
  - レイヤ 3 モードの Etherchannel ポート チャネル：グローバル コンフィギュレーション モードで **interface port-channel***port-channel-number* を使用し、イーサネット インターフェイスをチャネル グループにバインドして作成されたポートチャネル論理インターフェイスです。
- すべてのレイヤ 3 インターフェイスに IP アドレスを割り当てる必要があります。
-

- インターフェイスの HSRP バージョンを変更する場合、HSRP グループは新しい MAC アドレスを持つことになるため、リセットされます。

HSRP のイネーブル化

インターフェイス コンフィギュレーション コマンド **standby ip** は、設定されているインターフェイスで HSRP をアクティブ化します。 IP アドレスを指定した場合は、IP アドレスがホットスタンバイ グループの指定アドレスとして使用されます。 IP アドレスを指定しなかった場合は、スタンバイ機能によってアドレスが学習されます。 指定アドレスを使用し、LAN 上に少なくとも 1 つのレイヤ 3 ポートを設定する必要があります。 IP アドレスを設定すると、常に、現在使用されている別の指定アドレスが、設定した IP アドレスに変更されます。

standby ip コマンドがインターフェイス上でイネーブルに設定され、プロキシ ARP がイネーブルの場合、インターフェイスのホットスタンバイ ステートがアクティブになると、プロキシ ARP 要求に対する応答は、ホットスタンバイ グループの MAC アドレスを使用して実行されます。 インターフェイスが別のステートの場合、プロキシ ARP の応答は抑制されます。

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **standby version**{**1**| **2**}
4. **standby**[*group-number*] **ip**[*ip-address* [**secondary**]]
5. **end**
6. **show standby**[*interface-id*[*group*]]
7. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	インターフェイス コンフィギュレーション モードを開始し、HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	**standby version**{**1**| **2**} 例： `Switch(config-if)# standby version 1`	（任意）インターフェイスに HSRP バージョンを設定します。 • 1：HSRPv1 を選択します。 • 2：HSRPv2 を選択します。

	コマンドまたはアクション	目的
		このコマンドを入力しない場合、またはキーワードを指定しない場合、インターフェイスはデフォルトのHSRPバージョンであるHSRPv1を実行します。
ステップ 4	**standby**[*group-number*] **ip**[*ip-address* [**secondary**]] 例： `Switch(config-if)# standby 1 ip`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）group-number：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。 指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。 HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）ip-address：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。 少なくとも 1 つのインターフェイスに対して仮想IPアドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。 ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります
ステップ 6	**show standby**[*interface-id*[*group*]] 例： `Switch # show standby`	スタンバイ グループの設定を確認します。
ステップ 7	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

HSRP のイネーブル化：例, （498 ページ）

HSRP のプライオリティの設定

standby priority, **standby preempt**、および **standby track** インターフェイス コンフィギュレーション コマンドはいずれも、アクティブ ルータとスタンバイ ルータを検索するための特性、および新しいアクティブ ルータが処理を引き継いだ場合の動作を設定するために使用できます。

HSRP プライオリティを設定する場合の注意事項は、次のとおりです。

- プライオリティを割り当てておくと、アクティブ ルータおよびスタンバイ ルータを選択できます。 プリエンプションがイネーブルの場合は、プライオリティが最高のルータがアクティブ ルータになります。 プライオリティが等しい場合は、現在アクティブなルータに変更はありません。
- 最大の値（1～255）が、最高のプライオリティ（アクティブ ルータになる確率が最も高い）を表します。
- プライオリティ、プリエンプト、またはその両方を設定するときは、少なくとも 1 つのキーワード（**priority**、**preempt**、または両方）を指定する必要があります。
- インターフェイスが **standby track** コマンドによって設定されている場合、ルータ上の別のインターフェイスがダウンすると、デバイスのプライオリティが動的に変更されることもあります。
- **standby track** インターフェイス コンフィギュレーション コマンドを実行すると、ルータのホットスタンバイ プライオリティとインターフェイスのアベイラビリティが関連付けられます。この機能は、HSRP 用に設定されていないインターフェイスを追跡する場合に有効です。追跡対象のインターフェイスが故障すると、トラッキングが設定されているデバイスのホットスタンバイ プライオリティが 10 減少します。 追跡対象でないインターフェイスの場合は、そのステートが変わっても、設定済みデバイスのホットスタンバイ プライオリティは変わりません。 ホットスタンバイ用に設定されたインターフェイスごとに、追跡するインターフェイスのリストを個別に設定できます。
- **standby track***interface-priority* インターフェイス コンフィギュレーション コマンドを実行すると、追跡対象のインターフェイスがダウンした場合のホットスタンバイ プライオリティの減少幅を指定できます。 インターフェイスが稼働状態に戻ると、プライオリティは同じ分だけ増加します。
- *interface-priority* 値が設定されている場合に、複数の追跡対象インターフェイスがダウンすると、設定済みプライオリティの減少幅が累積されます。 プライオリティ値が設定されていない追跡対象インターフェイスが故障した場合、デフォルトの減少幅は 10 です。この値は累積されません。
- インターフェイスに対してルーティングを最初にイネーブルにした時点で、完全なルーティング テーブルは存在しません。 このインターフェイスがプリエンプトに設定されている場合はアクティブ ルータになりますが、十分なルーティング処理はできません。 この問題を解決するには、ルータがルーティングテーブルを更新できるように遅延時間を設定します。

インターフェイスに HSRP プライオリティ特性を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **standby** [*group-number*] **priority***priority*
4. **standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
5. **standby** [*group-number*] **track** *type number*[*interface-priority*]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	インターフェイス コンフィギュレーション モードを開始し、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3	**standby** [*group-number*] **priority***priority* 例： `Switch(config-if)# standby 120 priority 50`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。 指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。 最大の値が、最高のプライオリティを表します。 • （任意）group-number：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 4	**standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間

	コマンドまたはアクション	目的
		を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカルルータがリロードの後アクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカルルータがアクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ **5**	**standby** [*group-number*] **track** *type number*[*interface-priority*] 例： `Switch(config-if)# standby track interface gigabitethernet1/1/1`	他のインターフェイスを追跡するようにインターフェイスを設定します。この設定により、他のインターフェイスの 1 つがダウンした場合は、そのデバイスのホットスタンバイ プライオリティが減少します。 • （任意）group-number：コマンドが適用されるグループ番号です。 • type：追跡対象のインターフェイスタイプを（インターフェイス番号とともに）入力します。 • number：追跡対象のインターフェイス番号を（インターフェイスタイプとともに）入力します。 • （任意）interface-priority：インターフェイスがダウンした場合、または稼働状態に戻った場合に、ルータのホットスタンバイ プライオリティを減少または増加させる幅を入力します。 デフォルト値は 10 です。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

HSRP のプライオリティの設定：例, （498 ページ）

MHSRP の設定

MHSRP およびロード バランシングをイネーブルにするには、MHSRP の項の *MHSRP* ロード シェアリングの図に示したように、グループのアクティブ ルータとして 2 つのルータを設定し、スタンバイ ルータとして仮想ルータを設定します。 ルータに障害が発生して正常に戻った場合、プリエンプションを発生させてロードバランシングを復元するために、**standby preempt** インターフェイス コンフィギュレーション コマンドをそれぞれの HSRP インターフェイスで入力する必要があります。

ルータ A はグループ 1 のアクティブ ルータとして、ルータ B はグループ 2 のアクティブ ルータとして設定されています。 ルータ A の HSRP インターフェイスの IP アドレスは 10.0.0.1、グループ 1 のスタンバイ プライオリティは 110（デフォルトは 100）です。 ルータ B の HSRP インターフェイスの IP アドレスは 10.0.0.2、グループ 2 のスタンバイ プライオリティは 110 です。

グループ 1 は仮想 IP アドレス 10.0.0.3 を使用し、グループ 2 は仮想 IP アドレス 10.0.0.4 を使用します。

関連トピック

MHSRP, （478 ページ）

ルータ *A* の設定

手順の概要

1. **configure terminal**
2. **interface***type number*
3. **no switchport**
4. **ip address***ip-address mask*
5. **standby**[*group-number*]**ip**[*ip-address*[**secondary**]]
6. **standby** [*group-number*] **priority***priority*
7. **standby**[*group-number*] **preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
8. **standby**[*group-number*]**ip**[*ip-address*[**secondary**]]
9. **standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***type number* 例： `Switch (config)# interface gigabitethernet1/0/1`	インターフェイスタイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** 例： `Switch (config)# no switchport`	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 4	**ip address***ip-address mask* 例： `Switch (config-if)# 10.0.0.1 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby**[*group-number*]**ip**[*ip-address*[**secondary**]] 例： `Switch (config-if)# standby 1 ip 10.0.0.3`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。 指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。 HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。

	コマンドまたはアクション	目的
		• （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。 ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 6	**standby** [*group-number*] **priority***priority* 例： `Switch(config-if)# standby 1 priority 110`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。 指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。 最大の値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 7	**standby**[*group-number*] **preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指

	コマンドまたはアクション	目的
		定できる範囲は0～3600（1時間）で、デフォルトは0です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは0です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ **8**	**standby**[*group-number*]**ip**[*ip-address*[**secondary**]] 例： `Switch (config-if)# standby 2 ip 10.0.0.4`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。 指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。 HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。 ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。

	コマンドまたはアクション	目的
ステップ 9	**standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] 例： `Switch(config-if)# standby 2 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

MHSRP の設定：例, （499 ページ）

ルータ *B* の設定

手順の概要

1. **configure terminal**
2. **interface***type number*
3. **no switchport**
4. **ip address***ip-address mask*
5. **standby**[*group-number*]**ip**[*ip-address*[**secondary**]]
6. **standby** [*group-number*] **priority***priority*
7. **standby**[*group-number*] **preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
8. **standby**[*group-number*]**ip**[*ip-address*[**secondary**]]
9. **standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***type number* 例： `Switch (config)# interface gigabitethernet1/0/1`	インターフェイスタイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** 例： `Switch (config)# no switchport`	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 4	**ip address***ip-address mask* 例： `Switch (config-if)# 10.0.0.2 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby**[*group-number*]**ip**[*ip-address*[**secondary**]] 例： `Switch (config-if)# standby 1 ip 10.0.0.3`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。 指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。 HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。

	コマンドまたはアクション	目的
		• （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。 ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 6	**standby** [*group-number*] **priority***priority* 例： `Switch(config-if)# standby 1 priority 110`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。 指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。 最大の値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 7	**standby**[*group-number*] **preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指

	コマンドまたはアクション	目的
		定できる範囲は0～3600（1時間）で、デフォルトは0です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは0です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ **8**	**standby**[*group-number*]**ip**[*ip-address*[**secondary**]] 例： `Switch (config-if)# standby 2 ip 10.0.0.4`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。 指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。 HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。 ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。

	コマンドまたはアクション	目的
ステップ 9	**standby**[*group-number*]**preempt**[**delay**[**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] 例： `Switch(config-if)# standby 2 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

MHSRP の設定：例, （499 ページ）

HSRP 認証およびタイマーの設定

HSRP 認証ストリングを設定したり、hello タイム インターバルやホールドタイムを変更することもできます。

これらの属性を設定する場合の注意事項は次のとおりです。

- 認証ストリングはすべての HSRP メッセージで暗号化されずに送信されます。 相互運用できるように、接続されたすべてのルータおよびアクセス サーバに同じ認証ストリングを設定する必要があります。 認証ストリングが一致しないと、HSRP によって設定された他のルータから、指定されたホットスタンバイ IP アドレスおよびタイマー値を学習できません。
- スタンバイ タイマー値が設定されていないルータまたはアクセス サーバは、アクティブ ルータまたはスタンバイ ルータからタイマー値を学習できます。 アクティブ ルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。
- ホットスタンバイ グループのすべてのルータで、同じタイマー値を使用する必要があります。 通常、*holdtime* は *hellotime* の 3 倍以上です。

インターフェイスに HSRP の認証とタイマーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface***interface-id*
3. **standby**[*group-number*] **authentication***string*
4. **standby**[*group-number*]**timers***hellotimeholdtime*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config) # interface gigabitethernet1/0/1`	インターフェイス コンフィギュレーション モードを開始し、プライオリティを設定する HSRP インターフェイスを入力します。

	コマンドまたはアクション	目的
ステップ 3	**standby**[*group-number*] **authentication***string* 例： `Switch(config-if) # standby 1 authentication word`	（任意）**authentication***string*：すべての HSRP メッセージで伝達されるストリングを入力します。 認証ストリングには8文字までを指定できます。デフォルトのストリングは **cisco** です。 （任意）*group-number*：コマンドが適用されるグループ番号です。
ステップ 4	**standby**[*group-number*]**timers***hellotimeholdtime* 例： `Switch(config-if) # standby 1 timers 5 15`	（任意）hello パケット間隔、およびアクティブ ルータのダウンを他のルータが宣言するまでの時間を設定します。 • *group-number*：コマンドが適用されるグループ番号です。 • （任意）*hellotime*：ローカルルータがアクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • *holdtime*：ローカルルータがリロードの後アクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。 指定できる範囲は0～3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。
ステップ 5	**end** 例： `Switch(config-if) # end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

HSRP 認証およびタイマーの設定：例, （499 ページ）

ICMP リダイレクト メッセージの HSRP サポートのイネーブル化

HSRP が設定されたインターフェイスでは、ICMP リダイレクトメッセージが自動的にイネーブルになります。 ICMP は、エラーをレポートするためのメッセージパケットや IP 処理に関連する他

の情報を提供する、ネットワーク層インターネット プロトコルです。 ICMP には、ホストへのエラー パケットの方向付けや送信などの診断機能があります。 この機能は、HSRP を介した発信 ICMP リダイレクト メッセージをフィルタリングします。HSRP では、ネクスト ホップ IP アドレスが HSRP 仮想 IP アドレスに変更される可能性があります。 詳細については、『Cisco IOS IP Configuration Guide, Release 12.4』を参照してください。

HSRP グループおよびクラスタリングの設定

デバイスが HSRP スタンバイ ルーティングに参加し、クラスタリングがイネーブルの場合は、同じスタンバイ グループを使用して、コマンド スイッチの冗長性および HSRP の冗長性を確保できます。 同じ HSRP スタンバイ グループをイネーブルにし、コマンド スイッチおよびルーティングの冗長性を確保するには、**cluster standby-group***HSRP-group-name* [**routing-redundancy**] グローバル コンフィギュレーション コマンドを使用します。 **routing-redundancy** キーワードを指定せずに同じ HSRP スタンバイ グループ名でクラスタを作成すると、そのグループに対する HSRP スタンバイ ルーティングはディセーブルになります。

関連トピック

HSRP グループおよびクラスタリングの設定：例, （500 ページ）

HSRP のトラブルシューティング

次の表で説明されている状況のいずれかが発生した場合、以下のメッセージが表示されます。

```
%FHRP group not consistent with already configured groups on the switch stack - virtual MAC
reservation failed
```

表 *40*：*HSRP* のトラブルシューティング

状況	アクション
32 個を超える HSRP グループ インスタンスを設定する。	最大 32 個のグループ インスタンスに設定されるように HSRP グループを削除します。

HSRP の確認

HSRP コンフィギュレーションの確認

HSRP 設定を表示するには、次の特権 EXEC モードで次のコマンドを使用します。

show standby[*interface-id*[*group*]][**brief**][**detail**]

スイッチ全体、特定のインターフェイス、HSRP グループ、またはインターフェイスの HSRP グループに関する HSRP 情報を表示できます。 HSRP 情報の概要または詳細のいずれを表示するかを指定することもできます。 デフォルト表示は **detail** です。 多数の HSRP グループがある場合

に、修飾子を指定しないで **show standby** コマンドを使用すると、正確に表示されないことがあります。

```
Switch #show standby
VLAN1 - Group 1
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.182
Hot standby IP address is 172.20.128.3 configured
Active router is 172.20.128.1 expires in 00:00:09
Standby router is local
Standby virtual mac address is 0000.0c07.ac01
Name is bbb

VLAN1 - Group 100
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.262
Hot standby IP address is 172.20.138.51 configured
Active router is 172.20.128.1 expires in 00:00:09
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac64
Name is test
```

HSRP の設定例

HSRP のイネーブル化：例

次に、インターフェイスのグループ 1 で HSRP をアクティブにする例を示します。 ホットスタンバイ グループで使用される IP アドレスは、HSRP を使用して学習されます。

（注） これは、HSRP をイネーブルにするために必要な最小限の手順です。 その他の設定は任意です。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch # show standby
```

関連トピック

HSRP のイネーブル化, （481 ページ）

HSRP のプライオリティの設定：例

次に、ポートをアクティブにして、IP アドレスおよびプライオリティ 120（デフォルト値よりも高いプライオリティ）を設定して、アクティブ ルータになるまで 300 秒（5 分間）待機する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
Switch # show standby
```

関連トピック

HSRP のプライオリティの設定, （483 ページ）

MHSRP の設定：例

次に、*MHSRP* ロードシェアリングの図で示した MHSRP 設定をイネーブルにする例を示します。

ルータ A の設定

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

ルータ B の設定

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 1 priority 110
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

関連トピック

ルータ A の設定, （487 ページ）
ルータ B の設定, （491 ページ）

HSRP 認証およびタイマーの設定：例

次に、グループ 1 のホットスタンバイ ルータを相互運用させるために必要な認証ストリングとして、word を設定する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

次に、hello パケット間隔が 5 秒、ルータがダウンしたと見なされるまでの時間が 15 秒となるように、スタンバイ グループ 1 のタイマーを設定する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

関連トピック

HSRP 認証およびタイマーの設定, （495 ページ）

HSRP グループおよびクラスタリングの設定：例

次に、スタンバイ グループ my_hsrp をクラスタにバインドし、同じ HSRP グループをイネーブルにしてコマンドスイッチおよびルータの冗長性に使用する例を示します。 このコマンドを実行できるのは、コマンド スイッチに対してだけです。 スタンバイ グループの名前または番号が存在しない場合、またはスイッチがクラスタ メンバー スイッチである場合は、エラー メッセージが表示されます。

```
Switch # configure terminal
Switch(config) # cluster standby-group my_hsrp routing-redundancy
Switch(config-if)# end
```

関連トピック

HSRP グループおよびクラスタリングの設定 , （497 ページ）

VRRP の概要

VRRP の設定

Virtual Router Redundancy Protocol（VRRP）は、ルータのグループを使用して単一の仮想ルータを形成し、冗長性を実現する選択プロトコルです。 VRRP の設定では、1 つのルータが仮想ルータマスターとして選択され、もう 1 つのルータが障害発生時のバックアップとして機能します。 LAN クライアントは、デフォルト ゲートウェイとして仮想ルータを使用して設定でき、マルチアクセス リンク上の複数のルータが同じ仮想 IP アドレスを使用できるようにします。 ルータのグループを表す仮想ルータは、VRRP グループを形成します。

HSRP も VRRP も、同じ機能を実行します。 スイッチまたはスイッチに、IETF 標準 VRRP を設定するか、シスコのより強力な HSRP を設定するかを選択できます。

VRRP の制約事項

- スイッチの VRRP 実装は、RFC 2787 で指定された MIB をサポートしません。
- スイッチの VRRP 実装は、テキストベースの認証だけをサポートします。

第 22 章

サービス レベル契約の設定

この章では、スイッチで Cisco IOS IP サービス レベル契約（SLA）を使用する方法について説明します。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチまたはスイッチ スタックを意味します。

- 機能情報の確認，501 ページ
- SLA の制約事項，501 ページ
- SLA について，502 ページ
- IP SLA 動作の設定方法，508 ページ
- IP SLA 動作のモニタリング，522 ページ
- IP SLA 動作のモニタリングの例，523 ページ

機能情報の確認

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

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

SLA の制約事項

ここでは、SLA の制約事項を示します。

次に示すのは、IP SLA ネットワーク パフォーマンス測定の制約事項です。

- スイッチは、ゲートキーパー登録遅延動作測定を使用した Voice over IP（VoIP）サービス レベルはサポートしていません。
- Cisco IOS デバイスだけが宛先 IP SLA Responder の送信元になります。
- 他社製のデバイスに IP SLA Responder を設定することはできません。また、Cisco IOS IP SLA はこれらのデバイス固有のサービスに対してだけ動作パケットを送信できます。

関連トピック

IP SLA ネットワーク パフォーマンス測定の実装, （511 ページ）

Cisco IOS IP SLA でのネットワーク パフォーマンスの測定, （503 ページ）

IP SLA レスポンダおよび IP SLA 制御プロトコル, （504 ページ）

SLA について

Cisco IOS IP サービス レベル契約（SLA）

Cisco IOS IP SLA はネットワークにデータを送信し、複数のネットワーク ロケーション間あるいは複数のネットワーク パス内のパフォーマンスを測定します。 Cisco IOS IP SLA は、ネットワーク データおよび IP サービスをシミュレーションし、ネットワーク パフォーマンス情報をリアルタイムで収集します。 Cisco IOS IP SLA は、Cisco IOS デバイス間のトラフィックまたは Cisco IOS デバイスからネットワーク アプリケーション サーバのようなリモート IP デバイスへのトラフィックを生成し、分析します。 さまざまな Cisco IOS IP SLA 動作で評価を実行し、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用します。

Cisco IOS IP SLA 動作に応じてシスコ デバイスのネットワーク パフォーマンス統計情報がモニタリングされ、コマンドライン インターフェイス（CLI）MIB および簡易ネットワーク管理プロトコル（SNMP）MIB に格納されます。 IP SLA パケットには設定可能な IP レイヤおよびアプリケーション層のオプションがあります。たとえば、発信元および宛先 IP アドレス、ユーザデータグラム プロトコル（UDP）/TCP ポート番号、タイプ オブ サービス（ToS）バイト（DiffServ コードポイント（DSCP）および IP プレフィックス ビットを含む）、VPN ルーティング/転送インスタンス（VRF）、URL Web アドレスなどが設定できます。

Cisco IP SLA はレイヤ 2 転送に依存していないので、異なるネットワーク間にエンドツーエンド動作を設定してエンド ユーザが経験しそうなメトリックを最大限に反映させることができます。IP SLA は、次のパフォーマンス メトリックを収集して分析するために、。

- 遅延（往復および一方向）
- ジッタ（方向性あり）
- パケット損失（方向性あり）
- パケット シーケンス（パケット順序）
- パス（ホップ単位）

- 接続（方向性あり）
- サーバまたは Web サイトのダウンロード時間

Cisco IP SLA は SNMP によるアクセスが可能なので、Cisco Prime Internetwork Performance Monitor（IPM）やサードパーティ製パフォーマンス管理製品などのパフォーマンス モニタリング アプリケーションでも使用できます。

IP SLA を使用すると、次の利点が得られます。

- SLA モニタリング、評価、検証。
- ネットワーク パフォーマンス モニタリング。
  - ネットワークのジッター、遅延、パケット損失の測定。
  - 連続的で信頼性のある予測可能な測定。
- IP サービス ネットワーク ヘルス アセスメントにより、既存の QoS が新しい IP サービスに適していることを確認できる。
- 端末間のネットワーク アベイラビリティをモニタリングして、ネットワーク リソースをあらかじめ検証し接続をテストできる（たとえば、ビジネス上の重要なデータを保存する NFS サーバのネットワーク アベイラビリティをリモート サイトから確認できる）。
- 問題をすぐに認識し、トラブルシューティングにかかる時間を短縮できる一貫性のある信頼性の高い測定によるネットワーク動作のトラブルシューティング。
- マルチプロトコル ラベル スイッチング（MPLS）パフォーマンス モニタリングとネットワークの検証を行う（スイッチが MPLS をサポートする場合）。

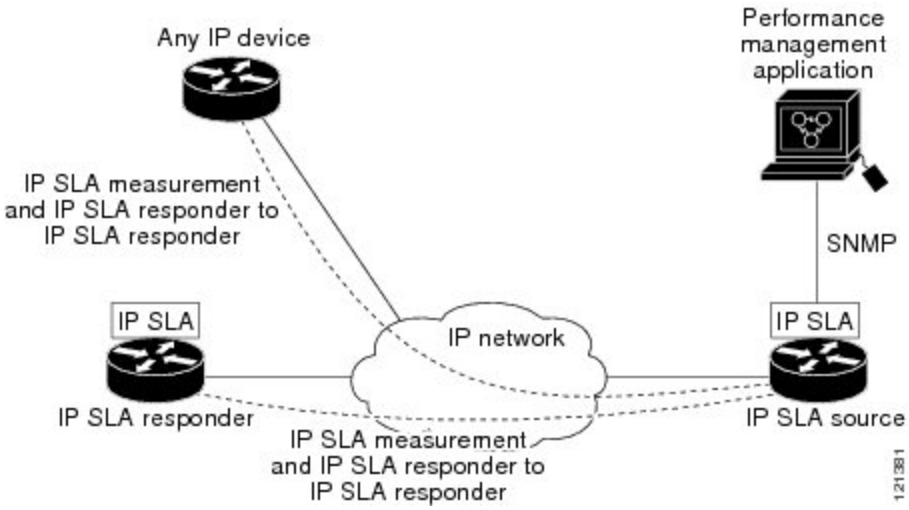
Cisco IOS IP SLA でのネットワーク パフォーマンスの測定

IP SLA を使用して、プローブを物理的に配置せずに、コア、分散、エッジといったネットワーク内の任意のエリア間のパフォーマンスをモニタリングすることができます。 2 つのネットワーク デバイス間のネットワーク パフォーマンスは、生成トラフィックで測定します。

次の図に、送信元デバイスが宛先デバイスに生成パケットを送信するときに IP SLA が開始される手順を示します。 宛先デバイスがパケットを受信すると、IP SLA 動作の種類によって、送信元のタイム スタンプ情報に応じてパフォーマンス メトリックを算出します。 IP SLA 動作は、特定の

プロトコル（UDP など）を使用してネットワークの送信元から宛先へのネットワーク測定を行います。

図 *43*：*Cisco IOS IP SLA* 動作



関連トピック

IP SLA ネットワーク パフォーマンス測定の実装，（511 ページ）

SLA の制約事項，（501 ページ）

IP SLA レスポンダおよび IP SLA 制御プロトコル

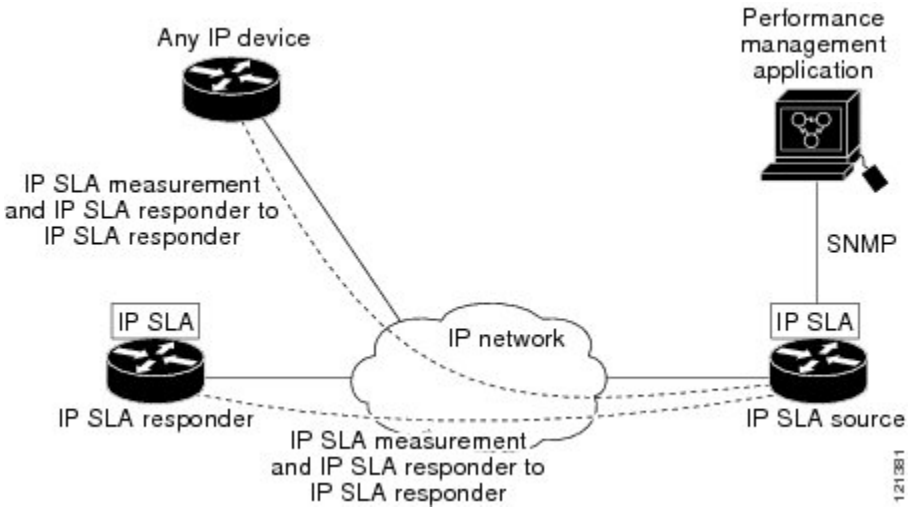
IP SLA レスポンダは宛先 Cisco デバイスに組み込まれたコンポーネントで、システムが IP SLA 要求パケットを予想して応答します。 Responder は専用プローブなしで正確な測定を行います。 レスポンダは、受信および応答するポートが通知されるメカニズムを Cisco IOS IP SLA コントロール プロトコルを通じて実現します。

（注） IP SLA レスポンダはレスポンダ設定可能なスイッチである Cisco IOS レイヤ 2 にすることもできます。 レスポンダは、IP SLA 機能を全面的にサポートする必要はありません。

次の図は、IP ネットワーク内での Cisco IOS IP SLA レスポンダの配置場所を示します。 レスポンダは、IP SLA 動作から送信されたコントロール プロトコル メッセージを指定されたポートで受信します。 コントロール メッセージを受信したら、指定された UDP または TCP ポートを指定された時間だけイネーブルにします。 この間に、レスポンダは要求を受け付け、応答します。 レス

ポンダは、IP SLA パケットに応答した後または指定の時間が経過したら ポートをディセーブルにします。 セキュリティの向上のために、コントロール メッセージでは MD5 認証が利用できます。

図 *44*：*Cisco IOS IP SLA* 動作



すべての IP SLA 動作に対して宛先デバイスのレスポンダをイネーブルにする必要はありません。たとえば、宛先ルータが提供しているサービス（Telnet や HTTP など）は Responder では必要ありません。

関連トピック

SLA の制約事項, （501 ページ）

IP SLA の応答時間の計算

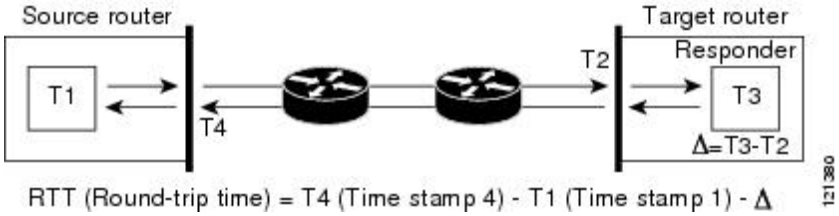
スイッチ、コントローラ、ルータは、他のハイ プライオリティ プロセスがあるために、着信パケットの処理に数十ミリ秒かかることがあります。 この遅延により応答時間が影響を受けます。テストパケットの応答が処理待ちのキューに入っていることもあるからです。 この場合、応答時間は正しいネットワーク遅延を反映しません。 IP SLA はソース デバイスとターゲット デバイス（レスポンダが使用されている場合）の処理遅延を最小化し、正しいラウンドトリップ時間（RTT）を識別します。 IP SLA テスト パケットは、タイム スタンプによって処理遅延を最小化します。

IP SLA レスポンダがイネーブルの場合、パケットが割り込みレベルでインターフェイスに着信したときおよびパケットが出て行くときにターゲットデバイスでタイムスタンプを付け、処理時間は含めません。 タイム スタンプはサブミリ秒単位で構成されます。

次の図に、レスポンダの動作を示します。 RTT を算出するためのタイム スタンプが 4 つ付けられます。 ターゲット ルータでレスポンダ機能がイネーブルの場合、タイム スタンプ 3（TS3）からタイムスタンプ 2（TS2）を引いてテストパケットの処理にかかった時間を求め、デルタ（Δ）で表します。 次に全体の RTT からこのデルタの値を引きます。 IP SLA により、この方法はソース

ルータにも適用されます。その場合、着信タイム スタンプ 4（TS4）が割り込みレベルで付けられ、より正確な結果を得ることができます。

図 45：***Cisco IOS IP SLA*** **レスポンダ タイム スタンプ**



この他にも、ターゲット デバイスに 2 つのタイム スタンプがあれば一方向遅延、ジッタ、方向性を持つパケット損失がトラッキングできるという利点があります。 大半のネットワーク動作は非同期なので、このような統計情報があるのは問題です。 ただし一方向遅延測定を取り込むには、ソース ルータとターゲット ルータの両方にネットワーク タイム プロトコル（NTP）を設定し、両方のルータを同じくロック ソースに同期させる必要があります。 一方向ジッタ測定にはクロック同期は不要です。

IP SLA 動作のスケジューリング

IP SLA 動作を設定する場合、統計情報の取り込みとエラー情報の収集から開始するように動作をスケジューリングする必要があります。 スケジューリングは、すぐに動作を開始する、または特定の月、日、時刻に開始するように設定できます。 また、*pending* オプションを使用して、あとで動作を開始するように設定することもできます。 pending オプションは動作の内部状態に関するもので、SNMP で表示できます。 トリガーを待機する反応（しきい値）動作の場合も pending オプションを使用します。 一度に 1 つの IP SLA 動作をスケジューリングしたり、グループの動作をスケジューリングすることもできます。

Cisco IOS CLI または CISCO RTTMON-MIB で 1 つのコマンドを使用して、複数の IP SLA 動作をスケジューリングできます。 等間隔で動作を実行するようにスケジューリングすると、IP SLA モニタリング トラフィックの数を制御できます。 IP SLA 動作をこのように分散させると CPU 使用率を最小限に抑え、ネットワーク スケーラビリティを向上させることができます。

IP SLA 複数動作のスケジューリング機能の詳細については、『*Cisco IOS IP SLA Configuration Guide*』の「IP SLAs—Multiple Operation Scheduling」の章を参照してください。

IP SLA 動作のしきい値のモニタリング

サービス レベル契約モニタリングを正しくサポートするには、違反が発生した場合にすぐに通知されるメカニズムにする必要があります。 IP SLA は次のような場合にイベントによってトリガーされる SNMP トラップを送信できます。

- 接続の損失
- タイムアウト
- RTT しきい値

- 平均ジッタしきい値
- 一方向パケット損失
- 一方向ジッタ
- 一方向平均オピニオン評点（MOS）
- 一方向遅延

IP SLA しきい値違反が発生した場合も、あとで分析するために別の IP SLA 動作がトリガーされます。 たとえば、回数を増やしたり、Internet Control Message Protocol（ICMP）パス エコーや ICMP パス ジッター動作を開始してトラブルシューティングを行うことができます。

ICMP Echo

ICMP エコー動作は、シスコ デバイスと IP を使用するその他のデバイス間のエンドツーエンド応答時間を測定します。 応答時間は、ICMP エコー要求メッセージを宛先に送信し、ICMP エコー応答を受信するのにかかる時間を測定して算出されます。 多くのお客様は、IP SLA ICMP ベース動作、社内 ping テスト、またはこの応答所要時間を測定するために ping ベース専用プローブを使用します。 IP SLA ICMP エコー動作は、ICMP ping テストと同じ仕様に準拠しており、どちらの方法でも同じ応答所要時間になります。

関連トピック

ICMP エコー動作を使用した IP サービス レベルの分析, （519 ページ）

UDP Jitter

ジッターとは、パケット間遅延の差異を説明する簡単な用語です。 複数のパケットが送信元から宛先まで 10 ミリ秒の間隔で継続的に送信される場合、宛先は 10 ミリ秒間隔で受信します（ネットワークが正常に動作している場合）。 しかし、ネットワークに遅延がある場合（キューイングや代替ルートを通じた到着など）、パケットの着信の間隔が 10 ミリ秒を超える場合や 10 ミリ秒未満になる場合があります。 正のジッター値は、パケットが 10 ミリ秒を超える間隔で到着することを示します。 負のジッター値は、パケットが 10 ミリ秒未満の間隔で到着することを示します。 パケットの到着が 12 ミリ秒間隔の場合、正のジッター値は 2 ミリ秒です。8 ミリ秒間隔で到着する場合、負のジッター値は 2 ミリ秒です。 遅延による影響を受けやすいネットワークの場合、正のジッタ値は望ましくありません。ジッタ値 0 が理想的です。

ジッターのモニタリング以外にも、IP SLA UDP ジッター動作を多目的データ収集動作に使用できます。 IP SLA によって生成されるパケットは、データを送受信するパケットを含めて、送信元および動作ターゲットからシーケンス情報とタイム スタンプを伝送します。 このデータに基づいて、UDP ジッター動作は次を測定します。

- 方向別ジッター（送信元から宛先へ、宛先から送信元へ）
- 方向別パケット損失
- 方向別遅延（一方向遅延）
- ラウンドトリップ遅延（平均 RTT）

データを送受信するパスが異なる場合もあるので（非同期）、方向別データを使用すればネットワークで発生している輻輳や他の問題の場所を簡単に突き止めることができます。

UDP ジッタ動作では合成（シミュレーション）UDP トラフィックを生成し、送信元ルータからターゲット ルータに多数の UDP パケットを送信します。その際の各パケットのサイズ、パケット同士の間隔、送信間隔は決められています。 デフォルトでは、10 バイトのペイロード サイズのパケット フレームを 10 ミリ秒で 10 個生成し、60 秒間隔で送信します。 これらのパラメータは、提供する IP サービスを最適にシミュレートするように設定できます。

一方向遅延を正確に測定する場合、（NTP によって提供される）送信元デバイスとターゲットデバイス間のクロック同期が必要です。 一方向ジッタおよびパケット損失を測定する場合は、クロック同期は不要です。 送信元デバイスとターゲットデバイスの間でクロックが同期していない場合、一方向ジッターとパケット損失のデータは戻されますが、UDP ジッター動作による一方向遅延測定は 0 の値が戻ります。

関連トピック

UDP ジッター動作を使用した IP サービス レベルの分析, （515 ページ）

IP SLA 動作の設定方法

ここでは、利用可能なすべての動作の設定情報について説明されているわけではありません。設定情報の詳細については『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。 ここでは、応答側の設定、UDP ジッター動作の設定（応答側が必要）、ICMP エコー動作の設定（応答側が不要）などの動作例を説明します。 他の動作の設定の詳細については、次の URL の『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。

デフォルト設定

IP SLA 動作は設定されていません。

設定時の注意事項

IP SLA のコマンドについては、『*Cisco IOS IP SLA Command Reference, Release 12.4T*』のコマンドリファレンスを参照してください。

説明と設定手順の詳細については、『*Cisco IOS IP SLAs Configuration Guide, Release 12.4TL*』を参照してください。

ガイドに記載されている IP SLA コマンドまたは動作の中にはスイッチでサポートされないものもあります。 スイッチでは、UDP ジッター、UDP エコー、HTTP、TCP 接続、ICMP エコー、ICMP パス エコー、ICMP パス ジッター、FTP、DNS、DHCP を使用する IP サービス レベル分析がサポートされます。また、複数動作スケジューリングおよび事前に設定されたしきい値のモニタリングもサポートされます。 ゲートキーパー登録遅延動作測定を使用した Voice over IP（VoIP）サービス レベルはサポートしていません。

IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用してソフトウェアイメージで動作タイプがサポートされていることを確認してください。 コマンド出力例は次のとおりです。

```
Switch# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

IP SLA レスポンダの設定

IP SLA レスポンダは、Cisco IOS ソフトウェアベース デバイスだけで利用可能です。これには、IP SLA 機能をフルにサポートしていない一部のレイヤ 2 スイッチも含まれます。

ターゲット デバイス（動作ターゲット）上の IP SLA 応答側を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sla responder** {**tcp-connect** |**udp-echo**}**ipaddress***ip-address***port***port-number*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sla responder** {**tcp-connect** |**udp-echo**} **ipaddress***ip-address* **port***port-number* 例： `Switch(config)# ip sla responder udp-echo 172.29.139.134 5000`	スイッチを IP SLA レスポンダとして設定します。 キーワードの意味は次のとおりです。 • **tcp-connect**：レスポンダの TCP 接続動作をイネーブルにします。 • **udp-echo**：レスポンダの User Datagram Protocol（UDP）エコー動作またはジッター動作をイネーブルにします。 • **ipaddress***ip-address*：宛先 IP アドレスを入力します。 • **port***port-number*：宛先ポート番号を入力します。 （注） IP アドレスとポート番号は、IP SLA 動作のソース デバイスに設定した IP アドレスおよびポート番号と一致している必要があります。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA ネットワーク パフォーマンス測定の実装

スイッチ上でIP SLAネットワーク パフォーマンス測定を実施するには、次の手順を実行します。

はじめる前に

show ip sla application 特権 EXEC コマンドを使用して、ソフトウェア イメージで目的の動作タイプがサポートされていることを確認してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sla***operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port***port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval***interpacket-interval*]
5. **frequency***seconds*
6. **threshold***milliseconds*
7. **exit**
8. **ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**]
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip sla***operation-number* 例： `Switch(config)# ip sla 10`	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port***port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval***interpacket-interval*] 例： `Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000`	IP SLA 動作を目的の動作タイプとして設定して（例では UDP ジッター動作が使用されています）、そのコンフィギュレーションモードを開始します（例ではUDP ジッターコンフィギュレーションモードが使用されています）。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • *destination-port*：宛先ポート番号を 1 ～ 65535 の範囲で指定します。 •（任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。 送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 •（任意）**source-port***port-number*：送信元ポート番号を 1 ～ 65535 の範囲で指定します。 ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 •（任意）**control**：IP SLA 制御メッセージの IP SLA レスポンダへの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA 制御メッセージは宛先デバイスに送信され、IP SLA レスポンダとの接続が確立されます。 •（任意）**num-packets***number-of-packets*：生成するパケット数を入力します。 指定できる範囲は 1 ～ 6000 です。デフォルトは 10 です。 •（任意）**interval***inter-packet-interval*：パケットの送信間隔をミリ秒で入力します。 指定できる範囲は 1 ～ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 5	**frequency***seconds* 例： `Switch(config-ip-sla-jitter)# frequency 45`	（任意）SLA 動作のオプションを設定します。 次の例では、指定された IP SLA 動作が繰り返されるレートを設定します。 指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。

	コマンドまたはアクション	目的
ステップ 6	**threshold***milliseconds* 例： `Switch(config-ip-sla-jitter)#` **`threshold 200`**	（任意）しきい値条件を設定します。 次の例では、指定された IP SLA 動作のしきい値が 200 に設定されます。 有効な範囲は 0 ～ 60000 ミリ秒です。
ステップ 7	**exit** 例： `Switch(config-ip-sla-jitter)#` **`exit`**	SLA 動作コンフィギュレーション モード（この例では UDP ジッター コンフィギュレーション モード）を終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**] 例： `Switch(config)#` **`ip sla schedule 10 start-time now life forever`**	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 • （任意）**life**：動作の実行を無制限（**forever**）に指定するか、特定の秒数（*seconds*）を指定します。 指定できる範囲は 0 ～ 2147483647 です。 デフォルトは 3600 秒（1 時間）です。 • （任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24 時間表記）、月日を入力します。 月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すると、開始時刻を指定するまでは情報を収集しません。 **now** と入力すると、ただちに動作を開始します。 **after***hh:mm:ss* と入力すると、指定した時刻の経過後に動作を開始します。 • （任意）**ageout***seconds*：情報を収集していないときのメモリの動作を保存する秒数を指定します。 指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 9	**end** 例： `Switch(config)#` **`end`**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

UDP ジッター コンフィギュレーション

次に、UDP ジッター IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

関連トピック

Cisco IOS IP SLA でのネットワーク パフォーマンスの測定, （503 ページ）

SLA の制約事項, （501 ページ）

UDP ジッター動作を使用した IP サービス レベルの分析

送信元デバイス上の UDP ジッタ動作を設定するには、次の手順を実行します。

はじめる前に

送信元デバイス上でUDPジッター動作を設定するには、ターゲットデバイス（動作ターゲット）で、IP SLA レスポンダをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sla***operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port***port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval***interpacket-interval*]
5. **frequency***seconds*
6. **exit**
7. **ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**]
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip sla***operation-number* 例： `Switch(config)# ip sla 10`	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port***port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval***interpacket-interval*] 例： `Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000`	IP SLA 動作を UDP ジッター動作として設定し、UDP ジッター コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • *destination-port*：宛先ポート番号を 1 ～ 65535 の範囲で指定します。 • （任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。 送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 • （任意）**source-port***port-number*：送信元ポート番号を 1 ～ 65535 の範囲で指定します。 ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 • （任意）**control**：IP SLA 制御メッセージの IP SLA レスポンダへの送信をイネーブルまたはディセーブルにします。 デフォルトでは、IP SLA 制御メッセージは宛先デバイスに送信され、IP SLA レスポンダとの接続が確立されます。 • （任意）**num-packets***number-of-packets*：生成するパケット数を入力します。 指定できる範囲は 1 ～ 6000 です。デフォルトは 10 です。 • （任意）**interval***inter-packet-interval*：パケットの送信間隔をミリ秒で入力します。 指定できる範囲は 1 ～ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 5	**frequency***seconds* 例： `Switch(config-ip-sla-jitter)# frequency 45`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。 指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Switch(config-ip-sla-jitter)# exit`	UDP ジッター コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**] 例： `Switch(config)# ip sla schedule 10 start-time now life forever`	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 • （任意）**life**：動作の実行を無制限（**forever**）に指定するか、特定の秒数（*seconds*）を指定します。 指定できる範囲は 0 ～ 2147483647 です。 デフォルトは 3600 秒（1 時間）です。 • （任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24 時間表記）、月日を入力します。 月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すると、開始時刻を指定するまでは情報を収集しません。 **now** と入力すると、ただちに動作を開始します。 **after***hh:mm:ss* と入力すると、指定した時刻の経過後に動作を開始します。 • （任意）**ageout***seconds*：情報を収集していないときのメモリの動作を保存する秒数を指定します。 指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

UDP ジッター IP SLA 動作の設定

次に、UDP ジッター IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

関連トピック

UDP Jitter, （507 ページ）

ICMP エコー動作を使用した IP サービス レベルの分析

送信元デバイス上の ICMP エコー動作を設定するには、次の手順を実行します。

はじめる前に

この動作では、IP SLA レスポンダ側を有効にしておく必要はありません。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sla***operation-number*
4. **icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface***interface-id*]
5. **frequency***seconds*
6. **exit**
7. **ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**]
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sla***operation-number* 例： `Switch(config)# ip sla 10`	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface***interface-id*] 例： `Switch(config-ip-sla)# icmp-echo 172.29.139.134`	IP SLA 動作を ICMP エコー動作として設定し、ICMP エコー コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 •（任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。 送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 •（任意）**source-interface***interface-id*：動作に対する送信元インターフェイスを指定します。
ステップ 5	**frequency***seconds* 例： `Switch(config-ip-sla-echo)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。 指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 6	**exit** 例： `Switch(config-ip-sla-echo)# exit`	UDP エコー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip sla schedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm*[*:ss*] [*month day* | *day month*] | **pending** | **now** | **after***hh:mm:ss*] [**ageout***seconds*] [**recurring**] 例： `Switch(config)# ip sla schedule 5 start-time now life forever`	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 •（任意）**life**：動作の実行を無制限（**forever**）に指定するか、特定の秒数（*seconds*）を指定します。 指定できる範囲は 0 ～ 2147483647 です。 デフォルトは 3600 秒（1 時間）です。 •（任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24時間表記）、月日を入力します。 月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すると、開始時刻を指定するまでは情報を収集しません。 **now** と入力すると、ただちに動作を開始します。

	コマンドまたはアクション	目的
		after *hh:mm:ss* と入力すると、指定した時刻の経過後に動作を開始します。 • （任意）**ageout***seconds*：情報を収集していないときのメモリの動作を保存する秒数を指定します。 指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ICMP エコー IP SLA 動作の設定

次に、ICMP エコー IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
```

```
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

関連トピック

IP SLA 動作のしきい値のモニタリング，（506 ページ）

IP SLA 動作のモニタリング

次の表で、IP SLA 動作の設定と結果を表示するために使用するコマンドについて説明します。

表 *41*：*IP SLA* 動作のモニタリング

show ip sla application	Cisco IOS IP SLA のグローバル情報を表示します。
show ip sla authentication	IP SLA 認証情報を表示します。
show ip sla configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA 動作に関する、デフォルト値をすべて含めた設定値を表示します。
show ip sla enhanced-history {**collection-statistics** | **distribution statistics**} [*entry-number*]	収集した履歴バケットの拡張履歴統計情報、あるいはすべての IP SLA 動作または特定の IP SLA 動作に関する分散統計情報を表示します。
show ip sla ethernet-monitor configuration [*entry-number*]	IP SLA 自動イーサネット設定を表示します。
show ip sla group schedule [*schedule-entry-number*]	IP SLA グループ スケジューリング設定と個別情報を表示します。

show ip sla history [*entry-number* | **full** | **tabular**]	すべての IP SLA 動作について収集した履歴を表示します。
show ip sla mpls-lsp-monitor {**collection-statistics** | **configuration** | **ldp operational-state** | **scan-queue** | **summary** [*entry-number*] | **neighbors**}	MPLS ラベルスイッチドパス（LSP）ヘルス モニタ動作を表示します。
show ip sla reaction-configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA動作に関する、予防的しきい値のモニタリングの設定を表示します。
show ip sla reaction-trigger [*entry-number*]	すべての IP SLA 動作または特定の IP SLA動作に関する反応トリガー情報を表示します。
show ip sla responder	IP SLA レスポンダ側の情報を表示します。
show ip sla statistics [*entry-number* | **aggregated** | **details**]	動作ステータスおよび統計情報の現在値または合計値を表示します。

IP SLA 動作のモニタリングの例

次の例は、アプリケーションごとのすべての IP SLA を示しています。

```
Switch# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

次の例は、すべての IP SLA ディストリビューション統計情報を示しています。

```
Switch# show ip sla enhanced-history distribution-statistics

Point by point Enhanced History
Entry    = Entry Number
Int      = Aggregation Interval
BucI     = Bucket Index
```

```
StartT   = Aggregation Start Time
Pth      = Path index
Hop      = Hop in path index
Comps    = Operations completed
OvrTh    = Operations completed over thresholds
SumCmp   = Sum of RTT (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry Int BucI StartT     Pth Hop Comps OvrTh SumCmp     SumCmp2L   SumCmp2H   T
Max    TMin
```

第 23 章

拡張オブジェクト トラッキングの設定

- 機能情報の確認，525 ページ
- 拡張オブジェクト トラッキングに関する情報，525 ページ
- 拡張オブジェクト トラッキングの設定方法，528 ページ
- 拡張オブジェクト トラッキングのモニタリング，547 ページ

機能情報の確認

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

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

拡張オブジェクト トラッキングに関する情報

拡張オブジェクト トラッキングの概要

拡張オブジェクト トラッキング機能が導入される前は、ホットスタンバイ ルータ プロトコル（HSRP）に単純なトラッキング メカニズムが内蔵されていますた。このメカニズムでは、インターフェイスのラインプロトコルのステートしか追跡することができませんでした。 インターフェイスのラインプロトコル ステートがダウンになった場合、ルータの HSRP 優先度は削減され、より高い優先度のもう 1 つの HSRP ルータがアクティブになることができます。

拡張オブジェクト トラッキング機能は、HSRP からトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP 以外のプロセスがこのトラッ

キングプロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコルのステートに加えて他のオブジェクトも追跡できます。

HSRP、仮想ルータ冗長プロトコル（VRRP）、Gateway Load Balancing Protoco（GLBP）などのクライアントプロセスで、トラッキングオブジェクトに対する興味を登録し、追跡対象オブジェクトの状態が変化したときに通知を受け取るようにすることができます。

（注） 拡張オブジェクト トラッキングは、LAN Base イメージを実行しているスイッチではサポートされていません。

拡張オブジェクト トラッキングは Cisco Catalyst 3560-CX スイッチのみでサポートされています。

各追跡対象オブジェクトには、トラッキング コマンドライン インターフェイス（CLI）で指定される一意の番号があります。クライアントプロセスは、この番号を使用して特定のオブジェクトを追跡します。トラッキングプロセスは、追跡対象オブジェクトに値の変化がないかどうかを定期的にポーリングし、（アップまたはダウン値など）変化があれば登録されているクライアントプロセスに通知します。ただちに通知する場合と、指定された時間遅延後に通知する場合があります。同じオブジェクトを複数のクライアントが追跡して、オブジェクトのステートが変化した場合に、それぞれが異なるアクションを実行できます。

複数のオブジェクトを組み合わせて 1 つのリストにして追跡することもできます。このリストの状態判定には、重みしきい値またはパーセンテージを使用します。オブジェクトの組み合わせには、ブールロジックを使用できます。「AND」ブール関数を使用する追跡リストの場合、リスト内の各オブジェクトがアップ ステートでないと追跡対象オブジェクトはアップになりません。「OR」ブール関数を使用する追跡リストの場合、リスト内の 1 つのオブジェクトだけがアップ ステートであれば追跡対象オブジェクトはアップになります。

インターフェイス ラインプロトコルまたは IP ルーティング ステートのトラッキング

インターフェイス ラインプロトコル ステートまたはインターフェイス IP ルーティング ステートのいずれかを追跡できます。IP ルーティング ステートを追跡する場合、オブジェクトをアップするには次の 3 つの条件が必要です。

- インターフェイス上で IP ルーティングがイネーブル、かつアクティブになっている。
- インターフェイス ラインプロトコル ステートが使用可能な状態（アップ）にある。
- 既知のインターフェイス IP アドレスを使用している。

この 3 つの条件がすべて合致しないと、IP ルーティング ステートはダウンになります。

関連トピック

インターフェイスでのライン ステート プロトコルまたは IP ルーティング ステートのトラッキングの設定, （528 ページ）

追跡リスト

オブジェクトの追跡リストは、ブール式、重みしきい値、またはパーセントしきい値を使用して設定できます。 追跡リストには1つまたは複数のオブジェクトが含まれます。 オブジェクトは存在していないと追跡リストに追加できません。

- 設定にブール式による演算を指定する場合は、「AND」または「OR」演算子を使用します。
- 追跡リストのステートを重みしきい値で判定する場合は、追跡リスト内の各オブジェクトに重み番号を割り当てます。 追跡リストのステートは、このしきい値に合致したかどうかで判定されます。 各オブジェクトのステートは、すべてのオブジェクトの重みの合計と各オブジェクトのしきい値の重みを比較して判定されます。
- 追跡リストをパーセントしきい値で判定する場合は、追跡リスト内のすべてのオブジェクトにパーセントしきい値を割り当てます。 各オブジェクトのステートは、各オブジェクトに割り当てたパーセンテージとリストを比較して判定されます。

関連トピック

ブール式による追跡リストの設定
重みしきい値による追跡リストの設定, （530 ページ）
パーセントしきい値による追跡リストの設定, （532 ページ）

他の特性のトラッキング

拡張オブジェクト トラッキングを使用して他の特性を追跡することもできます。

- **track ip route reachability** グローバル コンフィギュレーション コマンドを使用すると、IP ルートの到達可能性を追跡できます。
- **track ip route metric threshold** グローバル コンフィギュレーション コマンドを使用すると、ルートがしきい値を超えているか下回っているかを確認できます。
- **track resolution** グローバル コンフィギュレーション コマンドを使用すると、ルーティング プロトコルのメトリック解決のデフォルト値を変更できます。
- **track timer tracking** コンフィギュレーション コマンドを使用すると、追跡対象オブジェクトを定期的にポーリングするようにトラッキング プロセスを設定できます。

拡張オブジェクト トラッキング設定を確認する場合は、**show track** 特権 EXEC コマンドを使用してください。

IP SLA オブジェクト トラッキング

Cisco IOS IP サービス レベル契約（SLA）は、ネットワーク パフォーマンスの測定と診断を行うツールです。ネットワーク パフォーマンスを測定するためのトラフィック生成には、アクティブ

モニタリングが使用されます。 Cisco IP SLA 動作は、ネットワークのトラブルシューティングや設計、分析に使用できるリアルタイム メトリックを収集します。

IP SLA 動作のオブジェクト トラッキングを活用すると、クライアントは IP SLA オブジェクトの出力を追跡して、その情報をアクションのトリガーに使用できます。 各 IP SLA 動作は、OK または OverThreshold のような簡易ネットワーク管理プロトコル（SNMP）動作の戻りコード値を保持しているため、トラッキング プロセス側で解釈できます。 ステートと到達可能性という IP SLA 動作の 2 つの側面をトラッキングできます。 ステートの場合、戻りコードが OK のとき、トラック ステートがアップします。リターン コードが OK ではないとき、トラック ステートはダウンします。 到達可能性の場合、戻りコードが OK または OverThreshold のとき、到達可能性がアップします。リターン コードが OK ではないとき、到達可能性はダウンします。

関連トピック

IP SLA オブジェクト トラッキングの設定, （538 ページ）

スタティック ルート オブジェクト トラッキング

拡張オブジェクト トラッキングを使用したスタティック ルーティング サポートにより、スイッチで Internet Control Message Protocol（ICMP）ping を使用して、設定済みのスタティック ルートまたは DHCP ルートのダウン時を特定できます。 トラッキングを有効にしている場合、システムはルート ステートを追跡し、ステートの変化をクライアントに通知できます。 スタティック ルート オブジェクト トラッキングは、プライマリ ゲートウェイへの接続状態をモニタするために、Cisco IP SLA を使用して ICMP ping を生成します。

この機能は、IP サービス イメージのみでサポートされています。

関連トピック

スタティック ルーティング用のプライマリ インターフェイスの設定 , （540 ページ）

DHCP のプライマリ インターフェイスの設定, （541 ページ）

IP SLA モニタリング エージェントの設定, （542 ページ）

ルーティング ポリシーおよびデフォルト ルートの設定, （545 ページ）

拡張オブジェクト トラッキングの設定方法

インターフェイスでのライン ステート プロトコルまたは IP ルーティング ステートのトラッキングの設定

インターフェイスのラインプロトコル ステートまたは IP ルーティング ステートを追跡するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **track***object-number***interface***interface-id***line-protocol**
4. **delay** { *object-number***up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
5. **exit**
6. **track***object-number***interface***interface-id***ip routing**
7. **delay** { *object-number***up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
8. **end**
9. **show track***object-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**track***object-number***interface***interface-id***line-protocol** 例： `Switch(config)# track 33 interface gigabitethernet 1/0/1 line-protocol`	（任意）インターフェイスのラインプロトコルステートを追跡するための追跡リストを作成し、トラッキングコンフィギュレーション モードを開始します。 • object-number：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。 • **interface**：追跡されるインターフェイスです。
ステップ 4	**delay** { *object-number***up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。 指定できる範囲は 1 ～ 180 秒です。

	コマンドまたはアクション	目的
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**track***object-number***interface***interface-id***ip routing** 例： `Switch(config)# track 33 interface gigabitethernet 1/0/1 ip routing`	（任意）インターフェイスの IP ルーティング ステートを追跡するための追跡リストを作成し、トラッキング コンフィギュレーション モードを開始します。 IP ルート追跡では、ルーティング テーブル内の IP ルートおよびインターフェイスの IP パケット ルーティング機能を追跡します。 • object-number：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。 • **interface**：追跡されるインターフェイスです。
ステップ 7	**delay** { *object-number***up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。 指定できる範囲は 1 ～ 180 秒です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。

関連トピック

インターフェイス ラインプロトコルまたは IP ルーティング ステートのトラッキング, （526 ページ）

追跡リストの設定

重みしきい値による追跡リストの設定

重みしきい値による追跡を行うには、複数オブジェクトを含んだ追跡リストを作成し、重みをしきい値として使用することを指定したあと、各オブジェクトに重み値を設定します。 各オブジェクトのステートは、アップであるすべてのオブジェクトの重み合計と各オブジェクトのしきい値の重みを比較して判定されます。

重みしきい値のリストには、「NOT」ブール演算子を使用できません。

重みしきい値を使用してオブジェクトの追跡リストを作成し、各オブジェクトに重み値を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **track***track-number***list threshold**{**weight**}
4. **object***object-number*[**weight***weight-number*]
5. **threshold weight** {**up***number*|[**down***number*]}
6. **delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
7. **end**
8. **show track***object-number*
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track***track-number***list threshold**{**weight**} 例： `Switch(config)# track 4 list threshold weight`	トラッキング対象リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。 指定できる track-number の範囲は 1 ～ 500 です。 • **threshold**：追跡リストのステートがしきい値に基づくことを指定します。 • **weight**：しきい値が重みに基づくことを指定します。
ステップ 4	**object***object-number*[**weight***weight-number*] 例： `Switch(config)# object 2 weight 15`	追跡対象のオブジェクトを指定します。 指定できる範囲は 1 ～ 500 です。 任意の **weight***weight-number* には、オブジェクトのしきい値の重みを指定します。 範囲は 1 ～ 255 です。

	コマンドまたはアクション	目的
		（注） オブジェクトは存在していないと追跡リストに追加できません。
ステップ 5	**threshold weight** {**up***number*|[**down***number*]} 例： `Switch(config-track)# threshold weight up 30 down 10`	（任意）重みしきい値を指定します。 • **up***number*：有効範囲は 1 ～ 255 です。 • **down***number*：（任意）指定できる範囲は、**up***number* で指定した数により異なります。**up***number* を 25 に設定すると、down number の範囲は 0 ～ 24 です。
ステップ 6	**delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。 指定できる範囲は 1 ～ 180 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

追跡リスト，（527 ページ）

パーセントしきい値による追跡リストの設定

パーセントしきい値による追跡を行うには、複数オブジェクトを含んだ追跡リストを作成し、パーセンテージをしきい値として使用することを指定したあと、リスト内のすべてのオブジェクトにパーセンテージを指定します。 リストのステートは、各オブジェクトに割り当てたパーセンテージとリストを比較して判定されます。

パーセントしきい値のリストには、「NOT」ブール演算子を使用できません。

パーセントしきい値を使用してオブジェクトの追跡リストを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **track***track-number***list threshold**{**percentage**}
4. **object***object-number*
5. **threshold percentage** {**up***number*|[**down***number*]}
6. **delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
7. **end**
8. **show track***object-number*
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**track***track-number***list threshold**{**percentage**} 例： `Switch(config)# track 4 list threshold percentage`	トラッキング対象リスト オブジェクトを設定し、トラッキング コンフィギュレーションモードを開始します。 指定できる track-number の範囲は 1 ～ 500 です。 • **threshold**：追跡リストのステートがしきい値に基づくことを指定します。 • **percentage**：しきい値がパーセンテージに基づくことを指定します。
ステップ 4	**object***object-number* 例： `Switch(config)# object 1`	追跡対象のオブジェクトを指定します。 指定できる範囲は 1 ～ 500 です。 （注） オブジェクトは存在していないと追跡リストに追加できません。

	コマンドまたはアクション	目的
ステップ 5	**threshold percentage** {**up***number*|[**down***number*]} 例： `Switch(config)# threshold percentage up 51 down 10`	（任意）パーセントしきい値を指定します。 • **up***number*：有効範囲は 1 ～ 100 です。 • **down***number*：（任意）指定できる範囲は、**up***number* で指定した数により異なります。**up***number* を 25 に設定すると、down number の範囲は 0 ～ 24 です。
ステップ 6	**delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。 指定できる範囲は 1 ～ 180 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

追跡リスト，（527 ページ）

HSRP オブジェクト トラッキングの設定

特定のオブジェクトを追跡し、そのオブジェクトのステートに基づいて HSRP プライオリティを変更できるようにスタンバイ HSRP グループを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **track***object-number*{**interface***interface-id*{**line-protocol**|**ip routing**}|**ip route***ip address/prefix-length*{**metric threshold**|**reachability**}**list**{**boolean**{**and**|**or**}}|{**threshold**{**weight**|**percentage**}}}
4. **exit**
5. **interface** { *interface-id*
6. **standby**[*group-number*]**ip**[*ip-address***secondary**]]
7. **standby**[*group-number*]**track**[*object-number*[**decrement***priority-decrement*]]
8. **end**
9. **show standby**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track***object-number*{**interface***interface-id*{**line-protocol**|**ip routing**}|**ip route***ip address/prefix-length*{**metric threshold**|**reachability**}**list**{**boolean**{**and**|**or**}}|{**threshold**{**weight**|**percentage**}}}	（任意）設定されたステートを追跡するための追跡リストを作成し、トラッキング コンフィギュレーション モードを開始します。 • object-number：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。 • 追跡するインターフェイスを選択するには、**interface***interface-id* を入力します。 • インターフェイス ラインプロトコル ステートを追跡するに

	コマンドまたはアクション	目的
		は **line-protocol** を入力します。また、インターフェイス IP ルーティング ステートを追跡するには、**ip routing** を入力します。 • IP ルートのステートを追跡するには、**ip route***ip-address/prefix-length* を入力します。 • しきい値メトリックを追跡する場合は **metric threshold**、ルートが到達できるかどうかを追跡するには **reachability** を入力します。 デフォルトの up しきい値は 254、デフォルトの down しきい値は 255 です。 • リスト内の一連のオブジェクトを追跡するには、**list** を入力します。 （注） 追跡するインターフェイスごとにこの手順を繰り返してください。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** { *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**standby**[*group-number*]**ip**[*ip-address***secondary**]]	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を入力します。 指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。 HSRP グループが 1

	コマンドまたはアクション	目的
		つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。 このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ **7**	**standby**[*group-number*]**track**[*object-number*[**decrement***priority-decrement*]]	特定のオブジェクトを追跡し、そのオブジェクト ステートに基づいてホットスタンバイ プライオリティを変更できるように HSRP を設定します。 • （任意）*group-number*：追跡が適用されるグループ番号を入力します。 • *object-number*：追跡対象のオブジェクト番号を入力します。 指定できる範囲は 1 ～ 500 で、デフォルトは1です。 • （任意）**secondary**：IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。 このキーワードが省略された場

	コマンドまたはアクション	目的
		合、設定されたアドレスはプライマリ IP アドレスになります。 • （任意）**decrement***priority-decrement*：追跡対象のオブジェクトがダウンになった場合（またはアップに戻った場合）に、ルータのホットスタンバイ プライオリティを減少（または増加）させる幅を指定します。 指定できる範囲は 1 ～ 255 で、デフォルトは 10 です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show standby**	スタンバイ ルータの IP アドレスおよび追跡ステートを確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA オブジェクト トラッキングの設定

IP SLA 動作のステートまたは IP SLA IP ホストの到達可能性を追跡するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **track***object-number***rtr***operation-number***state**
4. **delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
5. **exit**
6. **track***object-number***rtr***operation-number***state**
7. **end**
8. **show track***object-number*
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track***object-number***rtr***operation-number***state** 例： `Switch(config)# track 2 200 state`	トラッキング コンフィギュレーション モードを開始し、IP SLA 動作のステートを追跡します。 • *object-number* の範囲は 1 ～ 500 です。 • *operation-number* の範囲は 1 ～ 2147483647 です。
ステップ 4	**delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。 指定できる範囲は 1 ～ 180 秒です。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**track***object-number***rtr***operation-number***state**	トラッキング コンフィギュレーション モードを開始し、IP SLA 動作のステートを追跡します。 • *object-number* の範囲は 1 ～ 500 です。

	コマンドまたはアクション	目的
		• *operation-number* の範囲は 1 ～ 2147483647 です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IP SLA オブジェクト トラッキング，（527 ページ）

スタティック ルート オブジェクト トラッキングの設定

スタティック ルーティング用のプライマリ インターフェイスの設定

スタティック ルーティングのプライマリ インターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **description***string*
5. **ip address***ip-address mask*[**secondary**]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id*	プライマリまたはセカンダリ インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**description***string*	インターフェイスに説明を追加します。
ステップ 5	**ip address***ip-address mask*[**secondary**]	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。

関連トピック

スタティック ルート オブジェクト トラッキング, （528 ページ）

DHCP のプライマリ インターフェイスの設定

DHCP のプライマリ インターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **description***string*
5. **ip dhcp client route track***number*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id*	プライマリまたはセカンダリ インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**description***string*	インターフェイスに説明を追加します。
ステップ 5	**ip dhcp client route track***number*	DHCP クライアントを設定し、追加されたルートを指定の追跡番号に関連付けます。 有効な数値は 1 ～ 500 です。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。

関連トピック

スタティック ルート オブジェクト トラッキング, （528 ページ）

IP SLA モニタリング エージェントの設定

プライマリ インターフェイスおよびエージェント状態をモニタするトラック オブジェクトを使用して、IP アドレスの ping を実行するように IP SLA エージェントを設定することができます。

Cisco IP SLA でネットワーク モニタリングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sla***operation number*
4. **icmp-echo**{ *destination ip-address*|*destination hostname*[**source -ipaddr**{*ip-address*|*hostname***source-interface***interface-id*]
5. **timeout***milliseconds*
6. **frequency***seconds*
7. **threshold***milliseconds*
8. **exit**
9. **ip sla schedule***operation-number*[**life**{**forever**|*seconds*}]**start-time***time*|**pending**|**now**|**after***time*]**ageout***seconds*][**recurring**]
10. **track***object-number***rtr***operation-number***statereachability**
11. **end**
12. **show track***object-number*
13. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sla***operation number*	Cisco IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**icmp-echo**{ *destination ip-address*|*destination hostname*[**source -ipaddr**{*ip-address*|*hostname***source-interface***interface-id*]	Cisco IP SLA エンドツーエンド ICMP エコー

	コマンドまたはアクション	目的
		答時間動作を設定し、IP SLA ICMP エコー コンフィギュレーション モードを開始します。
ステップ 5	**timeout***milliseconds*	要求パケットの応答に対する動作の待機時間を設定します。
ステップ 6	**frequency***seconds*	動作がネットワークに送信される頻度を設定します。
ステップ 7	**threshold***milliseconds*	反応イベントを生成し、その動作の履歴情報を保存するしきい値（ヒステリシス）の上限を設定します。
ステップ 8	**exit**	IP SLA ICMP エコー コンフィギュレーション モードを終了します。
ステップ 9	**ip sla schedule***operation-number*[**life**{**forever**|*seconds*}]**start-time***time*|**pending**|**now**|**after***time*]**ageout***seconds*][**recurring**] 例： `Switch(config)# track 2 200 state`	単一の IP SLA 動作のスケジューリング パラメータを設定します。 • *object-number* の範囲は 1 ～ 500 です。 • *operation-number* の範囲は 1 ～

	コマンドまたはアクション	目的
		2147483 です。
ステップ 10	**track***object-number***rtr***operation-number***statereachability**	Cisco IOS IP S 動作の状態を 跡し、トラッ ング コンフ ギュレーショ モードを開始 ます。
ステップ 11	**end**	特権 EXEC モ ドに戻ります
ステップ 12	**show track***object-number*	指定したオブ ジェクトが追 されているか うかを確認し す。
ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コン フィギュレー ション ファイ に設定を保存 ます。

関連トピック

スタティック ルート オブジェクト トラッキング，（528 ページ）

ルーティング ポリシーおよびデフォルト ルートの設定

オブジェクト トラッキングを使用してバックアップ スタティック ルーティングのルーティング ポリシーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **access-list***access-list-number*
4. **route-map***map tag*[**permit**|**deny**][*sequence-number*]
5. **match ip address**{*access-list number*[**permit**|**deny**][*sequence-number*]
6. **set ip next-hop dynamic dhcp**
7. **set interface***interface-id*
8. **exit**
9. **ip local policy route-map***map tag*
10. **ip route***prefix mask*{*ip address*|*interface-id*[*ip address*]}[*distance*][*name*][**permanent**|**track***track-number*][*tag tag*]
11. **end**
12. **show ip route track table**
13. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list***access-list-number*	拡張 IP アクセス リストを定義します。 オプションの文字を設定します。
ステップ 4	**route-map***map tag*[**permit**|**deny**][*sequence-number*]	ルートマップ コンフィギュレーション モードを開始し、特定のルーティングから別のルーティングへの再配信ルートの条件を定義します。
ステップ 5	**match ip address**{*access-list number*[**permit**|**deny**][*sequence-number*]	標準または拡張アクセス リストに許可された宛先ネットワーク番号アドレスを持つルートを配信し、パケットのポリシー ルーティングを実行します。 複数の番号または名前を入力できます。

	コマンドまたはアクション	目的
ステップ 6	**set ip next-hop dynamic dhcp**	DHCP ネットワーク専用。 DHCP クライアントが学んだ最新のゲートウェイへのネクスト ホップを設定します。
ステップ 7	**set interface***interface-id*	スタティック ルーティング ネットワーク専用。 ポリシー ルーティングのルート マップ一致条件をパスした出力パケットの送信場所を指定します。
ステップ 8	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**ip local policy route-map***map tag*	ルート マップを特定し、ローカル ポリシー ルーティングに使用します。
ステップ 10	**ip route***prefix mask*{*ip address*|*interface-id*[*ip address*]}[*distance*][*name*][**permanent**|**track***track-number*][*tag tag*]	スタティック ルーティング ネットワーク専用。 スタティック ルートを確立します。 **track***track-number* を入力し、設定したトラック オブジェクトがアップした場合に限り、スタティック ルートがインストールされるように指定します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ip route track table**	IP ルート トラック テーブルの情報を表示します。
ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

スタティック ルート オブジェクト トラッキング, （528 ページ）

拡張オブジェクト トラッキングのモニタリング

下の表に示す特権 EXEC コマンドまたはユーザ EXEC コマンドを使用して、拡張オブジェクトの追跡情報を表示します。

.

表 *42*：追跡情報を表示するコマンド

コマンド	目的
show ip route track table	IP ルート トラック テーブルの情報を表示します。
show track *[object-number]*	すべての追跡リストまたは指定リストの情報を表示します。
show track brief	すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。
show track interface [brief]	追跡対象のインターフェイス オブジェクトに関する情報を表示します。
show track ip [*object-number*][**brief**]**route**	追跡対象 IP ルート オブジェクトの情報を表示します。
show track resolution	追跡対象パラメータの解像度を表示します。
show track timer	追跡対象のポーリング インターバル タイマーを表示します。

第 V 部

Network Management

- Cisco IOS Configuration Engine の設定，551 ページ
- Cisco Discovery Protocol の設定，575 ページ
- 簡易ネットワーク管理プロトコルの設定，587 ページ
- SPAN および RSPAN の設定，619 ページ
- RMON の設定，667 ページ
- Embedded Event Manager の設定，677 ページ
- NetFlow Lite の設定，685 ページ
- Web Cache Communication Protocol を使用したキャッシュ サービスの設定，715 ページ

第 24 章

Cisco IOS Configuration Engine の設定

- 機能情報の確認，551 ページ
- Configuration Engine を設定するための前提条件，551 ページ
- Configuration Engine の設定に関する制約事項，552 ページ
- Configuration Engine の設定について，552 ページ
- Configuration Engine の設定方法，559 ページ
- CNS 設定のモニタリング，573 ページ

機能情報の確認

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

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

Configuration Engine を設定するための前提条件

- ユーザが接続している設定エンジン インスタンスの名前を取得します。
- CNS は、イベント バスとコンフィギュレーション サーバの両方を使用してデバイスに設定を提供するので、設定済みのスイッチごとに ConfigID と DeviceID の両方を定義する必要があります。
- **cns config partial** グローバル コンフィギュレーション コマンドを使用して設定したすべてのスイッチがイベント バスにアクセスする必要があります。スイッチを起源とする DeviceID

は、Cisco Configuration Engine 内の対応するスイッチ定義の DeviceID と一致する必要があります。 ユーザが接続しているイベント バスのホスト名を把握する必要があります。

関連トピック

Cisco Networking Service ID およびデバイスのホスト名, （554 ページ）
DeviceID, （555 ページ）

Configuration Engine の設定に関する制約事項

- コンフィギュレーション サーバの 1 つのインスタンスでは、設定済みの 2 つのスイッチが同じ ConfigID 値を共有できません。
- イベント バスの 1 つのインスタンスでは、設定済みの 2 つのスイッチが同じ DeviceID 値を共有できません。

関連トピック

Cisco Networking Service ID およびデバイスのホスト名, （554 ページ）

Configuration Engine の設定について

Cisco Configuration Engine ソフトウェア

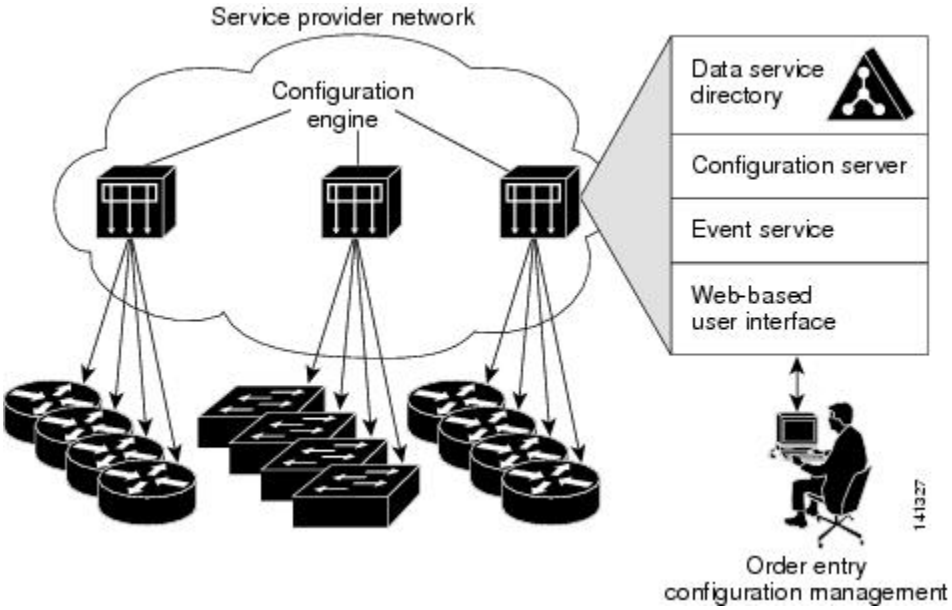
Cisco Configuration Engine は、ネットワーク管理ユーティリティ ソフトウェアで、ネットワーク デバイスおよびサービスの配置と管理を自動化するためのコンフィギュレーション サービスとして機能します。 各 Cisco Configuration Engine は、シスコ デバイス（スイッチとルータ）のグループとデバイスが提供するサービスを管理し設定を保存して、必要に応じて配信します。 Cisco Configuration Engine は、デバイス固有のコンフィギュレーション変更を生成してデバイスに送信し、コンフィギュレーション変更を実行して結果をログに記録することにより、初期設定とコンフィギュレーションの更新を自動化します。

Cisco Configuration Engine は、スタンドアロン モードとサーバ モードをサポートし、次の Cisco Networking Service（CNS）コンポーネントがあります。

- コンフィギュレーション サービス
  - Web サーバ
  - ファイル マネージャ
  - ネームスペース マッピング サーバ
- イベント サービス（イベント ゲートウェイ）
- データ サービス ディレクトリ（データ モデルおよびスキーマ）

スタンドアロン モードでは、内部に組み込まれたディレクトリ サービスがサポートされます。このモードでは、外部ディレクトリまたはその他のデータ ストアは必要ありません。 サーバ モードでは、ユーザが定義した外部ディレクトリの使用がサポートされます。

図 *46*：*Cisco Configuration Engine* のアーキテクチャの概要



コンフィギュレーション サービス

コンフィギュレーション サービスは、Cisco Configuration Engine の中核コンポーネントです。 スイッチ上にある Cisco IOS CNS エージェントと連携して動作するコンフィギュレーション サーバで構成されています。 コンフィギュレーションサービスは、初期設定と論理グループによる大規模な再設定のために、デバイスとサービスの設定をスイッチに配信します。 スイッチはネットワーク上で初めて起動するときに、コンフィギュレーション サービスから初期設定を受信します。

コンフィギュレーション サービスは CNS イベント サービスを使用して設定変更イベントを送受信し、成功および失敗の通知を送信します。

コンフィギュレーション サーバは Web サーバであり、コンフィギュレーション テンプレートと組み込み型ディレクトリ（スタンドアロン モード）またはリモート ディレクトリ（サーバ モード）に保存されているデバイス固有の設定情報を使用します。

コンフィギュレーション テンプレートは、CLI（コマンドライン インターフェイス）コマンド形式で静的な設定情報を含んだテキスト ファイルです。 テンプレートでは、変数は、Lightweight Directory Access Protocol（LDAP）URL を使用して指定します。この URL はディレクトリに保存されているデバイス固有の設定情報を参照します。

Cisco IOS エージェントは受信したコンフィギュレーション ファイルの構文をチェックし、イベントを発行して構文チェックが成功または失敗したかを表示します。 コンフィギュレーションエー

ジェントは設定をただちに適用することも、あるいは同期化イベントをコンフィギュレーションサーバから受信するまで適用を遅らせることもできます。

イベント サービス

Cisco Configuration Engine は、設定イベントの受信および生成にイベント サービスを使用します。イベント サービスはイベント エージェント、イベント ゲートウェイから構成されます。 イベント エージェントはスイッチ上にあり、スイッチと Cisco Configuration Engine のイベント ゲートウェイ間の通信を容易にします。

イベント サービスは、非常に有効なパブリッシュ サブスクライブ通信方式です。 イベント サービスは、サブジェクトベースのアドレス指定を使用して、メッセージを宛先に送信します。 サブジェクトベースのアドレス表記法では、メッセージおよび宛先には簡単で均一な名前空間を定義します。

関連トピック

CNS イベント エージェントのイネーブル化, （559 ページ）

名前空間マッパー

Cisco Configuration Engine はネームスペース マッパー（NSM）を備えています。これは、アプリケーション、デバイスまたはグループ ID、およびイベントに基づいてデバイスの論理グループを管理するための検索サービスを提供します。

Cisco IOS デバイスは、たとえば cisco.cns.config.load といった、Cisco IOS ソフトウェアで設定されたサブジェクト名と一致するイベント サブジェクト名のみを認識します。 ネームスペース マッピング サービスを使用すると、希望する命名規則を使用することでイベントを指定できます。 サブジェクト名でデータ ストアにデータを入力した場合、NSM はイベント サブジェクト名ストリングを、Cisco IOS が認識するものに変更します。

サブスクライバの場合、一意のデバイス ID とイベントが指定されると、ネームスペース マッピング サービスは、サブスクライブ対象のイベント セットを返します。 同様にパブリッシャの場合、一意のグループ ID、デバイス ID、およびイベントが指定されると、マッピング サービスは、パブリッシュ対象のイベント セットを返します。

Cisco Networking Service ID およびデバイスのホスト名

Cisco Configuration Engine は、設定対象の各スイッチに一意の識別子が関連付けられていることを前提としています。 一意の識別子は複数の同義語を持つことができますが、各同義語は特定のネームスペース内で一意です。イベント サービスは、ネームスペースの内容を使用してメッセージのサブジェクトベース アドレス指定を行います。

Cisco Configuration Engine は、イベント バス用とコンフィギュレーション サーバ用の 2 つの名前空間を交差します。 コンフィギュレーション サーバのネームスペースでは、*ConfigID* という用語がデバイスの一意な識別子です。 イベント バスのネームスペースでは、*DeviceID* という用語がデバイスの CNS 一意識別子です。

関連トピック

Configuration Engine を設定するための前提条件, （551 ページ）

Configuration Engine の設定に関する制約事項, （552 ページ）

ConfigID

設定対象のスイッチはそれぞれ固有の ConfigID を持ちます。これは Cisco Configuration Engine ディレクトリからスイッチ CLI 属性の対応するセットを取得するためのキーとなります。 スイッチで定義された ConfigID は、Cisco Configuration Engine 上の対応するスイッチ定義の ConfigID と一致する必要があります。

ConfigID は起動時に固定され、スイッチ ホスト名を再設定した場合でもデバイスを再起動するまで変更できません。

DeviceID

イベント バスに参加している設定済みのスイッチごとに一意の DeviceID があります。これはスイッチの送信元アドレスに似ているので、スイッチをバス上の特定の宛先として指定できます。

DeviceID の発信元は、スイッチの Cisco IOS ホスト名によって定義されます。 ただし、DeviceID 変数およびその使用は、スイッチに隣接するイベント ゲートウェイ内にあります。

イベント バス上の Cisco IOS の論理上の終点は、イベント ゲートウェイに組み込まれ、それがスイッチの代わりにプロキシとして動作します。イベント ゲートウェイはイベント バスに対して、スイッチおよび対応する DeviceID を表示します。

スイッチは、イベント ゲートウェイとの接続が成功するとすぐに、そのホスト名をイベント ゲートウェイに宣言します。 接続が確立されるたびに、イベント ゲートウェイは DeviceID 値を Cisco IOS ホスト名に組み合わせます。 イベント ゲートウェイは、スイッチと接続している間、この DeviceID 値を保持します。

関連トピック

Configuration Engine を設定するための前提条件, （551 ページ）

ホスト名および DeviceID

DeviceID は、イベント ゲートウェイと接続したときに固定され、スイッチ ホスト名を再設定した場合でも変更されません。

スイッチでスイッチ ホスト名を変更するとき、DeviceID を更新する唯一の方法は、スイッチとイベント ゲートウェイ間の接続を切断することです。 DeviceID 更新の手順については、以下の「関連項目」を参照してください。

接続が再確立されると、スイッチは変更したホスト名をイベント ゲートウェイに送信します。 イベント ゲートウェイは DeviceID を新しい値に再定義します。

⚠ **注意** Cisco Configuration Engine ユーザ インターフェイスを使用するときは、最初に DeviceID フィールドを、スイッチが前ではなく後に取得するホスト名値に設定する必要があります。Cisco IOS CNS エージェント用に設定を再初期化する必要があります。 そのようにしないと、後続の部分的なコンフィギュレーション コマンド操作で誤動作が発生する可能性があります。

関連トピック

DeviceID の更新, （569 ページ）

ホスト名、DeviceID、および ConfigID

スタンドアロン モードでは、ホスト名の値をスイッチに設定すると、コンフィギュレーション サーバはイベントをホスト名に送信する場合、そのホスト名を DeviceID として使用します。 ホスト名が設定されていない場合、イベントはデバイスの cn=<*value*>で送信されます。

サーバモードでは、ホスト名は使用されません。 このモードでは、バス上のイベント送信には常に一意の DeviceID 属性が使用されます。この属性が設定されていない場合はスイッチを更新できません。

Cisco Configuration Engine で **Setup** を実行する場合、これらの属性および関連する属性（タグ値のペア）を設定します。

Cisco IOS CNS エージェント

CNS イベント エージェント機能によって、スイッチはイベント バス上でイベントにパブリッシュおよびサブスクライブを行い、Cisco IOS CNS エージェントと連携できます。 スイッチ Cisco IOS ソフトウェアに組み込まれているこれらのエージェントでは、スイッチを接続して、自動的に設定できます。

関連トピック

Cisco IOS CNS エージェントのイネーブル化, （561 ページ）

初期設定

スイッチが最初に起動すると、ネットワークで Dynamic Host Configuration Protocol（DHCP）要求をブロードキャストすることで IP アドレスを取得しようとします。 サブネット上には DHCP サーバがないものと想定し、ディストリビューション スイッチは DHCP リレー エージェントとして動作し、要求を DHCP サーバに転送します。 DHCP サーバは要求を受信すると、新しいスイッチに IP アドレスを割り当て、Trivial File Transfer Protocol（TFTP）サーバのインターネット プロトコル（IP）アドレス、ブートストラップ コンフィギュレーション ファイルへのパス、デフォルト ゲートウェイの IP アドレスを、DHCP リレー エージェントに対するユニキャスト応答に組み入れます。 DHCP リレー エージェントは、この応答をスイッチに転送します。

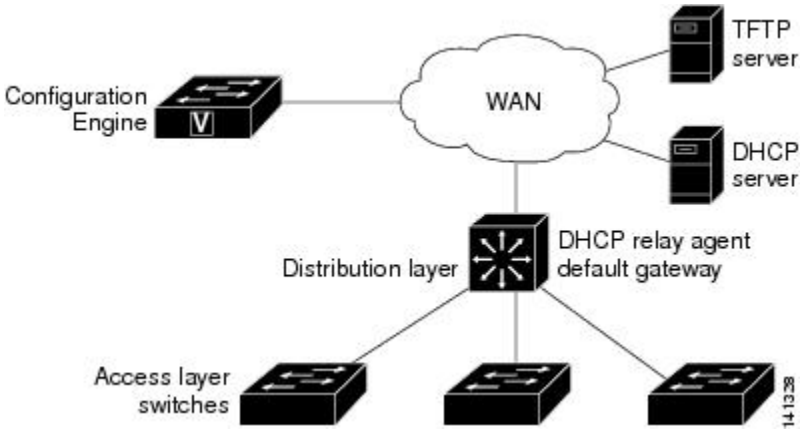
スイッチは、割り当てられた IP アドレスを自動的にインターフェイス VLAN 1（デフォルト）に設定し、TFTP サーバからブートストラップ コンフィギュレーション ファイルをダウンロードし

ます。 ブートストラップ コンフィギュレーション ファイルが正常にダウンロードされると、スイッチはそのファイルを実行コンフィギュレーションにロードします。

Cisco IOS CNS エージェントは、該当する ConfigID および EventID を使用して Configuration Engine との通信を開始します。 Configuration Engine はこの ConfigID をテンプレートにマッピングして、スイッチに完全なコンフィギュレーション ファイルをダウンロードします。

次の図に、DHCP ベースの自動設定を使用して初期ブートストラップ コンフィギュレーション ファイルを取得するためのネットワーク構成例を示します。

図 *47*：初期設定



関連トピック

Cisco IOS CNS エージェントの初期設定のイネーブル化, （563 ページ）
CNS 設定のモニタリング, （573 ページ）

差分（部分的）設定

ネットワークが稼働すると、Cisco IOS CNS エージェントを使用して新しいサービスを追加できます。 差分（部分）設定は、スイッチに送信できます。 実際の設定を、イベント ペイロードとしてイベントゲートウェイを介して（プッシュ処理）送信するか、スイッチにプルオペレーションを開始させる信号イベントとして送信できます。

スイッチは、適用する前に設定の構文をチェックできます。 構文が正しい場合は、スイッチは差分設定を適用し、コンフィギュレーション サーバに成功を信号で伝えるイベントを発行します。 スイッチが差分設定を適用しない場合、エラーステータスを示すイベントを発行します。 スイッチが差分設定を適用した場合、不揮発性 RAM（NVRAM）に書き込むか、または書き込むように指示されるまで待つことができます。

関連トピック

Cisco IOS CNS エージェントの部分的設定のイネーブル化, （571 ページ）
CNS 設定のモニタリング, （573 ページ）

コンフィギュレーションの同期

スイッチは、設定を受信した場合、書き込み信号イベントの受信時に設定の適用を遅らせることができます。 書き込み信号イベントは、更新された設定を NVRAM に保存しないようにスイッチに指示します。 スイッチは更新された設定を実行コンフィギュレーションとして使用します。 これによりスイッチの設定は、次のリブート時の使用のために NVRAM に設定を保存する前に、他のネットワーク アクティビティと同期化されます。

自動 CNS 設定

スイッチの自動CNS設定をイネーブルにするには、まずこのトピックに示す前提条件を完了する必要があります。 条件設定を完了したらスイッチの電源を入れます。 **setup** プロンプトでは何も入力しません。スイッチが初期設定を開始します。 コンフィギュレーション ファイル全体がスイッチにロードされると作業は完了です。

初期設定中の動作については、「関連項目」を参照してください。

表 *43*：自動設定イネーブル化の条件

デバイス	必要な設定
アクセス スイッチ	出荷時の設定（コンフィギュレーション ファイルなし）
ディストリビューション スイッチ	• IP ヘルパー アドレス • DHCP リレー エージェントをイネーブルにする[1] • IP ルーティング（デフォルト ゲートウェイとして使用する場合）
DHCP サーバ	• IP アドレスの割り当て • TFTP サーバの IP アドレス • TFTP サーバのブートストラップ コンフィギュレーション ファイルへのパス • デフォルト ゲートウェイの IP アドレス

デバイス	必要な設定
TFTP サーバ	• スイッチと Configuration Engine との通信を可能にする CNS コンフィギュレーション コマンドを含むブートストラップ コンフィギュレーション ファイル • （デフォルトのホスト名の代わりに）スイッチ MAC アドレスまたはシリアル番号のいずれかを使用して ConfigID および EventID を生成するように設定されたスイッチ • スイッチにコンフィギュレーション ファイルをプッシュするように設定された CNS イベント エージェント
CNS Configuration Engine	デバイス タイプ別の 1 つまたは複数のテンプレートで、テンプレートにデバイスの ConfigID がマッピングされています。

[1] DHCP リレーは、DHCP サーバがクライアントとは異なるサブネット上にある場合にのみ必要です。

Configuration Engine の設定方法

CNS イベント エージェントのイネーブル化

（注） スイッチ上で CNS イベント エージェントをイネーブルにしてから、CNS 設定エージェントをイネーブルにする必要があります。

スイッチ上で CNS イベント エージェントをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cns event** {*hostname* | *ip-address*} [*port-number*] [[**keepalive***secondsretry-count*] [**failover-time***seconds*] [**reconnect-time***time*] | **backup**]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cns event** {*hostname* | *ip-address*} [*port-number*] [[**keepalive***secondsretry-count*] [**failover-time***seconds*] [**reconnect-time***time*] | **backup**] 例： `Switch(config)# cns event 10.180.1.27 keepalive 120 10`	イベントエージェントをイネーブルにして、ゲートウェイ パラメータを入力します。 • {*hostname* | *ip-address*} に、イベント ゲートウェイのホスト名または IP アドレスを入力します。 • （任意）*port number* に、イベント ゲートウェイのポート番号を入力します。 デフォルトのポート番号は 11011 です。 • （任意）**keepalive***seconds* に、スイッチがキープアライブ メッセージを送信する間隔を入力します。 *retry-count* に、キープアライブ メッセージへの応答がない場合に接続を終了するまでのスイッチのメッセージ送信回数を入力します。 デフォルト値はいずれも 0 です。 • （任意）**failover-time***seconds* に、バックアップ ゲートウェイが確立された後にスイッチがプライマリ ゲートウェイ ルートを待つ時間を入力します。 • （任意）**reconnect-time***time* に、スイッチがイベント ゲートウェイに再接続しようとする前の最大時間間隔を入力します。 • （任意）バックアップ ゲートウェイであることを示す場合は、**backup** を入力します （省略した場合は、プライマリ ゲートウェイになります）。 （注） **encrypt** キーワードおよび **clock-timeout***time* キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

イベント エージェントに関する情報を確認するには、**show cns event connections** コマンドを特権 EXEC モードで使用します。

CNS イベント エージェントをディセーブルにするには、**no cns event** { *ip-address* | *hostname* } グローバル コンフィギュレーション コマンドを使用します。

関連トピック

イベント サービス, （554 ページ）

Cisco IOS CNS エージェントのイネーブル化

スイッチ上で Cisco IOS CNS エージェントをイネーブルにするには、次の手順を実行します。

はじめる前に

このエージェントをイネーブルにする前に、スイッチで CNS イベント エージェントをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **cns config initial** {*hostname* | *ip-address*} [*port-number*]
4. **cns config partial** {*hostname* | *ip-address*} [*port-number*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**
8. Cisco IOS CNS エージェントを、スイッチで開始します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cns config initial** {*hostname* | *ip-address*} [*port-number*] 例： `Switch(config)# cns config initial 10.180.1.27 10`	Cisco IOS CNS エージェントをイネーブルにし、コンフィギュレーション サーバ パラメータを入力します。 • {*hostname* | *ip-address*} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。 このコマンドが Cisco IOS CNS エージェントをイネーブルにして、スイッチで初期設定を開始します。
ステップ 4	**cns config partial** {*hostname* | *ip-address*} [*port-number*] 例： `Switch(config)# cns config partial 10.180.1.27 10`	Cisco IOS CNS エージェントをイネーブルにし、コンフィギュレーション サーバ パラメータを入力します。 • {*hostname* | *ip-address*} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。

	コマンドまたはアクション	目的
		Cisco IOS CNS エージェントをイネーブルにして、スイッチで部分的設定を開始します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 8	Cisco IOS CNS エージェントを、スイッチで開始します。	

次の作業

リモートで差分設定をスイッチに送信するために、Cisco Configuration Engine を使用できるようになりました。

関連トピック

Cisco IOS CNS エージェント，（556 ページ）

Cisco IOS CNS エージェントの初期設定のイネーブル化

スイッチ上で、CNS コンフィギュレーション エージェントをイネーブルにして初期設定を開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cns template connect***name*
4. **cli***config-text*
5. 別の CNS 接続テンプレートを設定する場合は、ステップ 3 ～ 4 を繰り返します。
6. **exit**
7. **cns connect***name* [**retries***number*] [**retry-interval***seconds*] [**sleep***seconds*] [**timeout***seconds*]
8. **discover** {**controller***controller-type* | **dlci** [**subinterface***subinterface-number*] | **interface** [*interface-type*] | **line***line-type*}
9. **template***name* [*... name*]
10. ステップ 8 ～ 9 を繰り返し、CNS 接続プロファイルにさらに多くのインターフェイスパラメータと CNS 接続テンプレートを指定します。
11. **exit**
12. **hostname***name*
13. **ip route***network-number*
14. **cns id***interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]
15. **cns id** {**hardware-serial** | **hostname** | **string***string* | **udi**} [**event**] [**image**]
16. **cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page***page*] [**source***ip-address*] [**syntax-check**]
17. **end**
18. **show running-config**
19. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**cns template connect***name* 例： `Switch(config)# cns template connect template-dhcp`	CNS テンプレート接続コンフィギュレーションモードを開始して、CNS 接続テンプレートの名前を指定します。
ステップ 4	**cli***config-text* 例： `Switch(config-tmpl-conn)# cli ip address dhcp`	CNS 接続テンプレートにコマンドラインを入力します。 テンプレート内の各コマンドラインにこの手順を繰り返します。
ステップ 5	別の CNS 接続テンプレートを設定する場合は、ステップ 3 ～ 4 を繰り返します。	
ステップ 6	**exit** 例： `Switch(config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**cns connect***name* [**retries***number*] [**retry-interval***seconds*] [**sleep***seconds*] [**timeout***seconds*] 例： `Switch(config)# cns connect dhcp`	CNS 接続コンフィギュレーション モードを開始し、CNS 接続プロファイルの名前を指定し、プロファイルパラメータを定義します。 スイッチは CNS 接続プロファイルを使用して Configuration Engine に接続します。 • CNS 接続プロファイルの *name* を入力します。 • （任意）**retries***number* に、接続のリトライ回数を入力します。 指定できる範囲は 1 ～ 30 です。 デフォルト値は 3 です。 • （任意）**retry-interval***seconds* に、Configuration Engine への連続する接続の試行間隔を入力します。 指定できる範囲は 1 ～ 40 秒です。 デフォルトは 10 秒です。 • （任意）**sleep***seconds* に、最初の接続試行を実行するまで待機する時間を入力します。 指定できる範囲は 0 ～ 250 秒です。 デフォルト値は 0 です。 • （任意）**timeout***seconds* に、接続試行が終了するまでの時間を入力します。 値の範囲は 10 ～ 2000 秒です。 デフォルト値は 120 です。
ステップ 8	**discover** {**controller***controller-type* | **dlci** [**subinterface***subinterface-number*] | **interface** [*interface-type*] | **line***line-type*}	CNS 接続プロファイル内のインターフェイス パラメータを入力します。 • **controller***controller-type* に、コントローラ タイプを入力します。

	コマンドまたはアクション	目的
	例： `Switch(config-cns-conn)# discover interface gigabitethernet`	• **dlci** に、アクティブなデータリンク接続識別子（DLCI）を入力します。 （任意）**subinterface***subinterface-number* に、アクティブな DLCI の検索に使用するポイントツーポイント サブインターフェイス番号を指定します。 • **interface** [*interface-type*] に、インターフェイスのタイプを入力します。 • **line***line-type* に、回線タイプを入力します。
ステップ 9	**template***name* [... *name*] 例： `Switch(config-cns-conn)# template template-dhcp`	スイッチの設定に適用する CNS 接続プロファイル内の CNS 接続テンプレートのリストを指定します。 複数のテンプレートを指定できます。
ステップ 10	ステップ 8 ～ 9 を繰り返し、CNS 接続プロファイルにさらに多くのインターフェイス パラメータと CNS 接続テンプレートを指定します。	
ステップ 11	**exit** 例： `Switch(config-cns-conn)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**hostname***name* 例： `Switch(config)# hostname device1`	スイッチのホスト名を入力します。
ステップ 13	**ip route***network-number* 例： `RemoteSwitch(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1`	（任意）IP アドレスが *network-number* の Configuration Engine へのスタティック ルートを確立します。
ステップ 14	**cns id***interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]	（任意）Configuration Engine が使用する一意の EventID または ConfigID を設定します。 このコマンドを入力する場合は、**cns id** {**hardware-serial** | **hostname** | **string***string* | **udi**} [**event**] [**image**] コマンドを入力しないでください。

	コマンドまたはアクション	目的
	例： `RemoteSwitch(config)# cns id GigabitEthernet1/0/1 ipaddress`	• *interface num* に、インターフェイスのタイプを入力します。 たとえば、ethernet、group-async、loopback、virtual-template を入力します。 この設定では、一意の ID を定義するためにどのインターフェイスから IP アドレスまたは MAC アドレスを取得するかを指定します。 • {**dns-reverse** | **ipaddress** | **mac-address**} では、ホスト名を取得してそのホスト名を一意の ID として割り当てるには **dns-reverse** を入力し、IP アドレスを使用するには **ipaddress** を入力し、MAC アドレスを一意の ID として使用するには **mac-address** を入力します。 • （任意）ID をスイッチの識別に使用する event-id 値になるように設定するには、**event** を入力します。 • （任意）ID をスイッチの識別に使用する image-id 値になるように設定するには、**image** を入力します。 （注） **event** と **image** キーワードの両方を省略した場合は、スイッチの識別には image-id 値が使用されます。
ステップ 15	**cns id** {**hardware-serial** | **hostname** | **string***string* | **udi**} [**event**] [**image**] 例： `RemoteSwitch(config)# cns id hostname`	（任意）Configuration Engine が使用する一意の EventID または ConfigID を設定します。 このコマンドを入力する場合は、**cns id***interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] コマンドを入力しないでください。 • {**hardware-serial** | **hostname** | **string** *string*| **udi**} で、**hardware-serial** を入力してスイッチのシリアル番号を一意の ID として設定するか、**hostname**（デフォルト）を入力してスイッチのホスト名を一意の ID として選択するか、**string***string* に任意のテキスト ストリングを一意の ID として入力するか、または **udi** を入力して Unique Device Identifier（UDI）を一意の ID として設定します。
ステップ 16	**cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page***page*] [**source***ip-address*] [**syntax-check**] 例： `RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist`	Cisco IOS エージェントをイネーブルにして、初期設定を開始します。 • {*hostname* | *ip-address*} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。 デフォルトのポート番号は 80 です。 • （任意）設定が完了したときの設定の成功、失敗、または警告のメッセージ用に **event** をイネーブルにします。

	コマンドまたはアクション	目的
		• （任意）**cns config initial** グローバル コンフィギュレーション コマンドの入力結果によってプルされた設定の NVRAM への自動書き込みを抑制するには、**no-persist** を入力します。**no-persist** キーワードを入力しない場合、**cns config initial** コマンドを使用すると、その結果の設定が自動的に NVRAM に書き込まれます。 • （任意）**page***page* に、初期設定の Web ページを入力します。デフォルトは /Config/config/asp です。 • （任意）送信元 IP アドレスに使用するには、**source***ip-address* を入力します。 • （任意）このパラメータを使用したときの構文をチェックするには、**syntax-check** をイネーブルにします。 （注） コマンドラインのヘルプ ストリングに表示されますが、**encrypt**、**status***url*、**inventory** キーワードはサポートされていません。
ステップ 17	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 18	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 19	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

コンフィギュレーション エージェントに関する情報を確認するには、**show cns config connections** コマンドを特権 EXEC モードで使用します。

CNS Cisco IOS エージェントをディセーブルにするには、**no cns config initial** { *ip-address* | *hostname* } グローバル コンフィギュレーション コマンドを使用します。

関連トピック

初期設定, （556 ページ）
CNS 設定のモニタリング, （573 ページ）

DeviceID の更新

スイッチ上でホスト名を変更するときに DeviceID を更新するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show cns config connections**
3. CNS イベント エージェントがイベント ゲートウェイに正しく接続されていることを確認します。
4. **show cns event connections**
5. ステップ 4 の出力に基づいて、次に示す現在接続されている接続に関する情報を記録します。この手順の以降のステップで IP アドレスとポート番号を使用します。
6. **configure terminal**
7. **no cns event***ip-addressport-number*
8. **cns event***ip-addressport-number*
9. **end**
10. **show cns event connections** からの出力を調べて、スイッチとイベント接続間の接続が再確立されていることを確認します。
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**show cns config connections** 例： `Switch# show cns config connections`	CNS イベント エージェントがゲートウェイに接続しているか、接続されているか、またはアクティブか、およびイベントエージェントに使用されているゲートウェイ、その IP アドレス、およびポート番号を表示します。

	コマンドまたはアクション	目的
ステップ 3	CNS イベント エージェントがイベント ゲートウェイに正しく接続されていることを確認します。	次のように **show cns config connections** の出力を確認します。 • 接続がアクティブになっている。 • 接続で現在設定されているスイッチ ホスト名を使用している。 DeviceID はこれらの手順を使用して、新しいホスト名の設定に対応するように更新されます。
ステップ 4	**show cns event connections** 例： `Switch# show cns event connections`	スイッチのイベント接続情報を表示します。
ステップ 5	ステップ 4 の出力に基づいて、次に示す現在接続されている接続に関する情報を記録します。 この手順の以降のステップで IP アドレスとポート番号を使用します。	
ステップ 6	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 7	**no cns event***ip-addressport-number* 例： `Switch(config)# no cns event 172.28.129.22 2012`	このコマンドで、ステップ 5 で記録した IP アドレスとポート番号を指定します。 このコマンドで、スイッチとイベント ゲートウェイ間の接続が解除されます。 最初に接続を解除し、次にこの接続を再確立して、DeviceID を更新する必要があります。
ステップ 8	**cns event***ip-addressport-number* 例： `Switch(config)# cns event 172.28.129.22 2012`	このコマンドで、ステップ 5 で記録した IP アドレスとポート番号を指定します。 このコマンドで、スイッチとイベント ゲートウェイ間の接続が再確立されます。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show cns event connections** からの出力を調べて、スイッチとイベント接続間の接続が再確立されていることを確認します。	
ステップ 11	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

ホスト名および DeviceID, （555 ページ）

Cisco IOS CNS エージェントの部分的設定のイネーブル化

スイッチ上で Cisco IOS CNS エージェントをイネーブルにして部分設定を開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source***ip-address*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source***ip-address*] 例： `Switch(config)# cns config partial 172.28.129.22 2013`	コンフィギュレーション エージェントをイネーブルにし、部分設定を開始します。 • {*ip-address* | *hostname*} に、コンフィギュレーション サーバの IP アドレスまたはホスト名を入力します。 • （任意）*port number* に、コンフィギュレーション サーバのポート番号を入力します。 デフォルトのポート番号は 80 です。 • （任意）送信元 IP アドレスに使用するには、**source***ip-address* を入力します。 （注） **encrypt** キーワードは、コマンドラインのヘルプストリングに表示されますが、サポートされていません。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

次の作業

コンフィギュレーション エージェントに関する情報を確認するには、**show cns config stats** または **show cns config outstanding** コマンドのいずれかを特権 EXEC モードで使用します。

Cisco IOS エージェントをディセーブルにするには、**no cns config partial** { *ip-address* | *hostname* } グローバル コンフィギュレーション コマンドを使用します。 部分設定を取り消すには、**cns config cancel** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

差分（部分的）設定，（557 ページ）
CNS 設定のモニタリング，（573 ページ）

CNS 設定のモニタリング

表 *44*：***CNS show*** コマンド

コマンド	目的
show cns config connections `Switch# show cns config connections`	CNS Cisco IOS CNS エージェントの接続のステータスを表示します。
show cns config outstanding `Switch# show cns config outstanding`	開始されたがまだ終了していない差分（部分）CNS 設定に関する情報を表示します。
show cns config stats `Switch# show cns config stats`	Cisco IOS CNS エージェントに関する統計情報を表示します。
show cns event connections `Switch# show cns event connections`	CNS イベント エージェントの接続のステータスを表示します。
show cns event gateway `Switch# show cns event gateway`	スイッチのイベント ゲートウェイ情報を表示します。
show cns event stats `Switch# show cns event stats`	CNS イベント エージェントに関する統計情報を表示します。

コマンド	目的
show cns event subject `Switch# show cns event subject`	アプリケーションによってサブスクライブされたイベントエージェントのサブジェクト一覧を表示します。

関連トピック

Cisco IOS CNS エージェントの部分的設定のイネーブル化, （571 ページ）
差分（部分的）設定, （557 ページ）
Cisco IOS CNS エージェントの初期設定のイネーブル化, （563 ページ）
初期設定, （556 ページ）

第 25 章

Cisco Discovery Protocol の設定

- 機能情報の確認，575 ページ
- CDP に関する情報，575 ページ
- CDP の設定方法，577 ページ
- CDP のモニタおよびメンテナンス，585 ページ

機能情報の確認

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

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

CDP に関する情報

CDP の概要

CDP はすべてのシスコ デバイス（ルータ、ブリッジ、アクセス サーバ、コントローラ、およびスイッチ）のレイヤ 2（データリンク層）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスにネイバー シスコ デバイスを検出できます。 また、下位レイヤのトランスペアレントプロトコルが稼働しているネイバーデバイスのデバイス タイプや、簡易ネットワーク管理プロトコル（SNMP）エージェント アドレスを学習することもできます。 この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDP は、サブネットワーク アクセス プロトコル（SNAP）をサポートしているすべてのメディアで動作します。 CDP はデータリンク層でのみ動作するため、異なるネットワーク層プロトコルをサポートする 2 つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャストアドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。 このアドバタイズには、受信側デバイスで CDP 情報を廃棄せずに保持する時間を表す存続可能時間、つまりホールドタイム情報も含まれます。 各デバイスは他のデバイスから送信されたメッセージも待ち受けて、ネイバー デバイスについて学習します。

CDP はスイッチ上で Network Assistant をイネーブルにすることで、ネットワークをグラフィカルに表示できます。 スイッチは CDP を使用してクラスタ候補を検出し、クラスタ メンバ、およびコマンド スイッチから最大 3 台（デフォルト）離れたクラスタ対応の他のデバイスについての情報を維持します。

関連トピック

CDP 特性の設定, （577 ページ）

CDP のモニタおよびメンテナンス, （585 ページ）

CDP のデフォルト設定

この表は、CDP のデフォルト設定を示します。

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP タイマー（パケット更新頻度）	60 秒
CDP ホールドタイム（廃棄までの時間）	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

関連トピック

CDP のイネーブル化, （580 ページ）

CDP のディセーブル化, （579 ページ）

インターフェイス上での CDP のイネーブル化, （583 ページ）

インターフェイス上での CDP のディセーブル化, （582 ページ）

CDP の設定方法

CDP 特性の設定

次の CDP 特性を設定できます。

- CDP 更新の頻度
- 破棄するまで情報を保持する時間の長さ
- バージョン 2 アドバタイズを送信するかどうか

（注） ステップ 3 ～ 5 はすべて任意であり、どの順番で実行してもかまいません。

CDP 特性を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cdp timer***seconds*
4. **cdp holdtime***seconds*
5. **cdp advertise-v2**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**cdp timer***seconds* 例： `Switch(config)# cdp timer 20`	（任意）CDP 更新の送信頻度を秒単位で設定します。 指定できる範囲は 5 ～ 254 です。デフォルトは 60 秒です。
ステップ 4	**cdp holdtime***seconds* 例： `Switch(config)# cdp holdtime 60`	（任意）受信デバイスがこのデバイスから送信された情報を破棄せずに保持する時間を指定します。 指定できる範囲は 10 ～ 255 秒です。デフォルトは 180 秒です。
ステップ 5	**cdp advertise-v2** 例： `Switch(config)# cdp advertise-v2`	（任意）バージョン 2 アドバタイズを送信するように CDP を設定します。 これは、デフォルトの状態です。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

デフォルト設定に戻すには、CDP コマンドの **no** 形式を使用します。

関連トピック

CDP の概要，（575 ページ）

CDP のモニタおよびメンテナンス，（585 ページ）

CDP のディセーブル化

CDP はデフォルトで有効になっています。

（注） スイッチ クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。 CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

CDP デバイス検出機能をディセーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no cdp run**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no cdp run** 例： `Switch(config)# no cdp run`	CDP をディセーブルにします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

CDP を使用するには、再びイネーブルにする必要があります。

関連トピック

CDP のイネーブル化，（580 ページ）

CDP のデフォルト設定，（576 ページ）

CDP のイネーブル化

CDP はデフォルトで有効になっています。

（注） スイッチ クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。 CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

無効になっている CDP を有効にするには、次の手順を実行します。

はじめる前に

CDP を無効にする必要があります。そのようにしないと有効にできません。

手順の概要

1. **enable**
2. **configureterminal**
3. **cdp run**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cdp run** 例： `Switch(config)# cdp run`	無効にされている場合は、CDP を有効にします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

CDP が有効になっていることを示すには、**showrunall** コマンドを使用します。 **showrun** だけを入力した場合、CDP の有効化が表示されないことがあります。

関連トピック

CDP のデフォルト設定, （576 ページ）

CDP のディセーブル化, （579 ページ）

インターフェイス上での CDP のディセーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。

（注） スイッチ クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。 CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

ポート上で CDP をディセーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **no cdp enable**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	CDP をディセーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no cdp enable** 例： `Switch(config-if)# no cdp enable`	ステップ 3 で指定したインターフェイスで CDP をディセーブルにします。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

インターフェイス上での CDP のイネーブル化，（583 ページ）

CDP のデフォルト設定，（576 ページ）

インターフェイス上での CDP のイネーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。

（注） スイッチ クラスタと他のシスコ デバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。 CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

ポート上でディセーブルになっている CDP をイネーブルにするには、次の手順を実行します。

はじめる前に

CDP をイネーブルにしようとしているポートで、CDP をディセーブルになっている必要があります。そうでない場合は、イネーブルにできません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **cdp enable**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	CDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cdp enable** 例： `Switch(config-if)# cdp enable`	ディセーブルにされているインターフェイスで CDP をイネーブルにします。

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

関連トピック

CDP のデフォルト設定, （576 ページ）
インターフェイス上での CDP のディセーブル化, （582 ページ）

CDP のモニタおよびメンテナンス

表 *45*：*CDP* 情報を表示するためのコマンド

コマンド	説明
clear cdp counters	トラフィック カウンタを 0 にリセットします。
clear cdp table	ネイバー デバイスに関する情報を収めた CDP テーブルを削除します。
show cdp	送信間隔、送信したパケットの保持時間などのグローバル情報を表示します。

コマンド	説明
show cdp entry *entry-name* [**version**] [**protocol**]	特定のネイバーに関する情報を表示します。 アスタリスク（*）を入力してすべてのCDPネイバーを表示することも、情報が必要なネイバーの名前を入力することもできます。 また、指定されたネイバー上でイネーブルになっているプロトコルの情報や、デバイス上で稼働しているソフトウェアのバージョン情報が表示されるように、表示内容を制限することもできます。
show cdp interface [*interface-id*]	CDP がイネーブルに設定されているインターフェイスの情報を表示します。 必要なインターフェイスの情報だけを表示できます。
show cdp neighbors [*interface-id*] [*detail*]	装置タイプ、インターフェイス タイプ、インターフェイス番号、保持時間の設定値、機能、プラットフォーム、ポート ID を含めたネイバー情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show cdp traffic	CDP カウンタ（送受信されたパケット数およびチェックサム エラーを含む）を表示します。

関連トピック

CDP 特性の設定，（577 ページ）

CDP の概要，（575 ページ）

第 26 章

簡易ネットワーク管理プロトコルの設定

- 機能情報の確認，587 ページ
- SNMP の前提条件，587 ページ
- SNMP の制約事項，590 ページ
- SNMP に関する情報，591 ページ
- SNMP の設定方法，596 ページ
- SNMP ステータスのモニタリング，616 ページ
- SNMP の例，617 ページ

機能情報の確認

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

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

SNMP の前提条件

サポートされている SNMP バージョン

このソフトウェア リリースは、次の SNMP バージョンをサポートしています。

- SNMPv1：RFC1157 に規定された SNMP（完全インターネット標準）。

- SNMPv2C は、SNMPv2Classic のバルク検索機能を残し、エラー処理を改善したうえで、SNMPv2Classic のパーティ ベースの管理およびセキュリティ フレームワークをコミュニティ ストリング ベースの管理フレームワークに置き換えたものです。 次の機能があります。
  - SNMPv2：RFC 1902 ～ 1907 に規定された SNMP バージョン 2（ドラフト版インターネット標準）
  - SNMPv2C：RFC 1901 に規定された SNMPv2 のコミュニティ ストリング ベースの管理フレームワーク（試験版インターネット プロトコル）
- SNMPv3：SNMP のバージョン 3 は、RFC 2273 ～ 2275 に規定されている相互運用可能な標準ベース プロトコルです。 SNMPv3 は、ネットワーク上のパケットを認証、暗号化することでデバイスへのアクセスに対するセキュリティを提供します。SNMPv3 は、次のセキュリティ機能を備えています。
  - メッセージの完全性：パケットが伝送中に改ざんされないようにします。
  - 認証：有効な送信元からのメッセージであるかどうかを判別します。
  - 暗号化：パッケージの内容をミキシングし、許可されていない送信元に内容が読まれることを防止します。

（注） 暗号化を選択するには、**priv** キーワードを入力します。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。 エージェントの MIB にアクセスできるマネージャのコミュニティが、IP アドレス アクセス コントロール リストおよびパスワードによって定義されます。

SNMPv2C にはバルク検索機能が組み込まれ、より詳細なエラー メッセージを管理ステーションに報告します。 バルク検索機能は、テーブルや大量の情報を検索し、必要な往復回数を削減します。 SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラーコードが使用されています。これらのエラーは、SNMPv1 では単一のエラー コードで報告されます。 SNMPv2 では、エラー リターン コードでエラー タイプが報告されるようになりました。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。 セキュリティ モデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。 セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。 セキュリティ レベルとセキュリティ モデルの組み合わせにより、SNMP パケットを扱うときに使用するセキュリティ方式が決まります。 使用可能なセキュリティ モデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

次の表では、この特性を識別し、セキュリティモデルとセキュリティ レベルの異なる組み合わせを比較します。

表 *46* : ***SNMP*** セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
SNMPv3	noAuthNoPriv	[Username]	No	ユーザ名の照合を使用して認証します。
SNMPv3	authNoPriv	Message Digest 5（MD5）または Secure Hash Algorithm（SHA）	No	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。

モデル	レベル	認証	暗号化	結果
SNMPv3	authPriv	MD5 または SHA	データ暗号規格（DES）または Advanced Encryption Standard（AES）	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。 次の暗号化アルゴリズムで、User-based Security Model（USM）を指定できます。 • CBC-DES（DES-56）規格に基づく認証に加えた DES 56 ビット暗号化 • 3DES 168 ビット暗号化 • AES 128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化

管理ステーションでサポートされている SNMP バージョンを使用するには、SNMP エージェントを設定する必要があります。 エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、および SNMPv3 を使用する通信をサポートするようにソフトウェアを設定できます。

SNMP の制約事項

バージョンの制約事項

- SNMPv1 は informs をサポートしていません。

SNMP に関する情報

SNMP の概要

SNMP は、マネージャとエージェント間の通信のメッセージ フォーマットを提供するアプリケーションレイヤ プロトコルです。 SNMP システムは、SNMP マネージャ、SNMP エージェント、および管理情報ベース（MIB）で構成されます。 SNMP マネージャは、Cisco Prime Infrastructure などのネットワーク管理システム（NMS）に統合できます。 エージェントおよび MIB は、スイッチに常駐します。 スイッチ 上で SNMP を設定するには、マネージャとエージェント間の関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。 マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。 エージェントは、デバイス パラメータやネットワーク データの保存場所である MIB から値を収集します。 また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。 トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。 トラップは不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、次の表に示す動作を実行します。

表 *47*：*SNMP* の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。[2]
get-bulk-request[3]	テーブルの複数の行など、通常はサイズの小さい多数のデータ ブロックに分割して送信する必要がある巨大なデータ ブロックを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

[2] この動作を使用した場合、SNMP マネージャは厳密な変数名を知る必要はありません。 テーブル内を順に検索して、必要な変数を検出します。

[3] get-bulk コマンドを使用できるのは、SNMPv2 以上に限られます。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。 エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。 SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップメッセージも送信します。 トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニングツリー トポロジが変更された場合、認証に失敗した場合などがあります。

関連トピック

SNMP エージェントのディセーブル化, （596 ページ）

SNMP ステータスのモニタリング, （616 ページ）

エージェント コンタクトおよびロケーションの設定, （613 ページ）

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。 NMS が スイッチ にアクセスするには、NMS 上のコミュニティ ストリング定義が スイッチ 上の 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致しなければなりません。

コミュニティ ストリングの属性は、次のいずれかです。

- 読み取り専用（RO）：コミュニティ ストリングを除き MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りアクセス権を与えますが、書き込みアクセスは許可しません。
- 読み取り-書き込み（RW）：MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りおよび書き込みアクセス権を与えますが、コミュニティ ストリングへのアクセスは許可しません。
- クラスタを作成すると、コマンド スイッチがメンバ スイッチと SNMP アプリケーション間のメッセージ交換を管理します。 Network Assistant ソフトウェアは、コマンド スイッチ上で最初に設定された RW および RO コミュニティ ストリングにメンバ スイッチ番号（@esN、N はスイッチ番号）を追加し、これらのストリングをメンバ スイッチに伝播します。

関連トピック

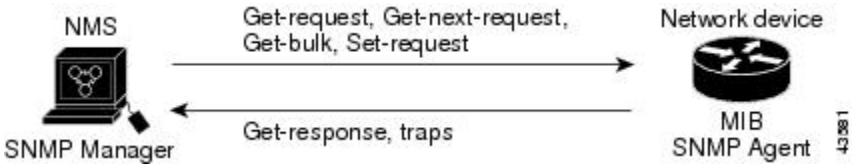
コミュニティ ストリングの設定, （598 ページ）

SNMP MIB 変数アクセス

NMS の例として、Cisco Prime Infrastructure ネットワーク管理ソフトウェアがあります。 Cisco Prime Infrastructure 2.0 ソフトウェアは、スイッチ MIB 変数を使用して装置変数を設定し、ネットワーク上の装置をポーリングして特定の情報を取得します。 ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

次の図に示すように、SNMP エージェントは MIB からデータを収集します。 エージェントは SNMP マネージャに対し、トラップ（特定イベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。 トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス トラッキングなどの状況を SNMP マネージャに通知します。 SNMP エージェントはさらに、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送信される MIB 関連のクエリに応答します。

図 *48*：*SNMP* ネットワーク



SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、スイッチから SNMP マネージャに通知を送信できます。 SNMP 通知は、トラップまたは情報要求として送信できます。 コマンド構文では、トラップまたは情報を選択するオプションがコマンドにない限り、キーワード traps はトラップ、情報、またはその両方を表します。 **snmp-server host** コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

（注） SNMPv1 は informs をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうかが送信側にわからないからです。 情報要求の場合、受信した SNMP マネージャは SNMP 応答プロトコル データ ユニット（PDU）でメッセージを確認します。 送信側が応答を受信しなかった場合は、再び情報要求を送信できます。 再送信できるので、情報の方がトラップより意図した宛先に届く可能性が高くなります。

情報の方がトラップより信頼性が高いのは、スイッチおよびネットワークのリソースを多く消費するという特性にも理由があります。 送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。 トラップの送信は 1 回限りですが、情報は数回にわたって再送信つまり再試行が可能です。 再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。

したがって、トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。 SNMP マネージャですべての通知を受信することが重要な場合は、情報要求を使用してください。ネットワークまたはスイッチのメモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

関連トピック

SNMP 通知の設定, （606 ページ）

SNMP ステータスのモニタリング, （616 ページ）

SNMP ifIndex MIB オブジェクト値

NMS の IF-MIB は、物理インターフェイスまたは論理インターフェイスを識別する、ゼロより大きい一意の値である interface index（ifIndex）オブジェクト値の生成および割り当てを行います。スイッチの再起動またはスイッチ ソフトウェアのアップグレード時に、スイッチは、インターフェイスにこれと同じ値を使用します。 たとえば、スイッチのポート 2 に 10003 という ifIndex 値が割り当てられていると、スイッチの再起動後も同じ値が使用されます。

スイッチは、次の表内のいずれかの値を使用して、インターフェイスに ifIndex 値を割り当てます。

表 *48*：*ifIndex* 値

インターフェイス タイプ	ifIndex 範囲
SVI[4]	1 ～ 4999
EtherChannel	5001 ～ 5048
トンネル	5078 ～ 5142
タイプとポート番号に基づく物理（ギガビット イーサネットまたは SFP[5] モジュール インターフェイスなど）	10000 ～ 14500
ヌル	14501
ループバックおよびトンネル	24567+

4 SVI = スイッチ仮想インターフェイス
5 SFP = Small Form-Factor Pluggable

SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル[6]
SNMP トラップ レシーバ	未設定

機能	デフォルト設定
SNMP トラップ	TCP 接続のトラップ（tty）以外は、イネーブルではありません。
SNMP バージョン	バージョン キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで **noauth**（noAuthNoPriv）になります。
SNMP 通知タイプ	タイプが指定されていない場合、すべての通知が送信されます。

6 これは、スイッチが起動し、スタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが設定されていない場合のデフォルトです。

SNMP 設定時の注意事項

スイッチが起動し、スイッチのスタートアップ コンフィギュレーションに少なくとも 1 つの **snmp-server** グローバル コンフィギュレーション コマンドが設定されている場合、SNMP エージェントはイネーブルになります。

SNMP グループは、SNMP ユーザを SNMP ビューに対応付けるテーブルです。 SNMP ユーザは、SNMP グループのメンバです。 SNMP ホストは、SNMP トラップ動作の受信側です。 SNMP エンジン *ID* は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP グループを設定するときには、次の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しません。 **snmp-server host** グローバル コンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザを対応するグループに追加します。 グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。
- リモートユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応する IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモート ユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドを **remote** オプションとともに使用して、SNMP エンジン ID を設定してください。 リモート エージェントの SNMP エンジン ID およびユーザ パスワードを使用して認証およびプライバシー ダイジェストが算出されます。 先にリモート エンジン ID を設定しておかないと、コンフィギュレーション コマンドがエラーになります。
- SNMP 情報を設定するときには、プロキシ要求または情報の送信先となるリモート エージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。
- ローカル ユーザがリモート ホストと関連付けられていない場合、スイッチは **auth**（authNoPriv）および **priv**（authPriv）の認証レベルの情報を送信しません。
- SNMP エンジン ID の値を変更すると、重大な影響が生じます。 （コマンド ラインで入力された）ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて、MD5 または SHA セキュリティ ダイジェストに変換されます。 コマンド ラインのパスワードは、

RFC 2274 の規定に従って廃棄されます。 このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合は SNMPv3 ユーザのセキュリティ ダイジェストが無効となり、**snmp-server user***username* グローバル コンフィギュレーション コマンドを使用して、SNMP ユーザを再設定する必要があります。 エンジン ID を変更した場合は、同様の制限によってコミュニティ ストリングも再設定する必要があります。

関連トピック

SNMP グループおよびユーザの設定, （601 ページ）

SNMP ステータスのモニタリング, （616 ページ）

SNMP の設定方法

SNMP エージェントのディセーブル化

no snmp-server グローバル コンフィギュレーション コマンドは、デバイス上で実行している SNMP エージェントのすべてのバージョン（バージョン 1、バージョン 2C、バージョン 3）をディセーブルにします。 入力した最初の **snmp-server** グローバル コンフィギュレーション コマンドによって、SNMP エージェントのすべてのバージョンを再度イネーブルにします。 特に SNMP をイネーブルにするために指定された Cisco IOS コマンドはありません。

SNMP エージェントをディセーブルにするには、次の手順を実行します。

はじめる前に

SNMP エージェントをディセーブルにする前にイネーブルにする必要があります。 デバイス上で入力した最初の **snmp-server** グローバル コンフィギュレーション コマンドによって SNMP エージェントがイネーブルになります。

手順の概要

1. **enable**
2. **configureterminal**
3. **no snmp-server**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no snmp-server** 例： `Switch(config)# no snmp-server`	SNMP エージェント動作をディセーブルにします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

SNMP エージェント機能，（592 ページ）

SNMP ステータスのモニタリング，（616 ページ）

コミュニティ ストリングの設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティストリングは、スイッチ上のエージェントへのアクセスを許可する、パスワードと同様の役割を果たします。 ストリングに対応する次の特性を 1 つまたは複数指定することもできます。

- コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限

スイッチ上でコミュニティ ストリングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server community***string*[**view***view-name*][**ro**|**rw**][*access-list-number*]
4. **access-list***access-list-number*{**deny**|**permit**}*source*[*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server community***string*[**view***view-name*][**ro**|**rw**][*access-list-number*]	コミュニティ ストリングを設定します。

	コマンドまたはアクション	目的
	例： `Switch(config)# snmp-server community comaccess ro 4`	（注） コンテキスト情報を区切るには @ 記号を使用します。 このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。 • *string* には、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。 任意の長さのコミュニティ ストリングを 1 つまたは複数設定できます。 • （任意）**view** には、コミュニティがアクセスできるビュー レコードを指定します。 • （任意）許可された管理ステーションで MIB オブジェクトを取得する場合は読み取り専用（**ro**）、許可された管理ステーションで MIB オブジェクトを取得および変更する場合は読み書き（**rw**）を指定します。 デフォルトでは、コミュニティ ストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 • （任意）*access-list-number* には、1 ～ 99 および 1300 ～ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 4	**access-list***access-list-number*{**deny**|**permit**}*source*[*source-wildcard*] 例： `Switch(config)# access-list 4 deny any`	（任意）ステップ 3 で標準 IP アクセス リスト番号を指定してリストを作成した場合は、必要に応じてコマンドを繰り返します。 • *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、コミュニティ ストリングを使用してエージェントにアクセスできる

	コマンドまたはアクション	目的
		SNMP マネージャの IP アドレスを入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します（コミュニティ ストリングに値を入力しないでください）。

特定のコミュニティ ストリングを削除するには、**no snmp-server** コミュニティ ストリング グローバル コンフィギュレーション コマンドを使用します。

スイッチのローカルまたはリモート SNMP サーバ エンジンを表す識別名（エンジン ID）を指定できます。 SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

関連トピック

SNMP コミュニティ ストリング，（592 ページ）

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモート SNMP サーバ エンジンを表す識別名（エンジン ID）を指定できます。 SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

スイッチ上の SNMP グループとユーザを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server engineID** {**local***engineid-string*|**remote***ip-address*[**udp-port***port-number*]*engineid-string*}
4. **snmp-server group***group-name*{**v1**|**v2c**|**v3**{**auth**|**noauth**|**priv**}}[**read***readview*][**write***writeview*][**notify***notifyview*][**access***access-list*]
5. **snmp-server user***username group-name*{**remote***host*[**udp-port***port*]}{**v1**[**access***access-list*]|**v2c**[**access***access-list*]|**v3**[**encrypted**][**access***access-list*]{**auth**{**md5**|**sha**}*auth-password*}[**priv**{**des**|**3des**|**aes**{**128**|**192**|**256**}}*priv-password*]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション
ステップ 1	**enable** 例： `Switch> enable`
ステップ 2	**configureterminal** 例： `Switch# configure terminal`
ステップ 3	**snmp-server engineID** {**local***engineid-string*|**remote***ip-address*[**udp-port***port-number*]*engineid-string*} 例： `Switch(config)# snmp-server engineID local 1234`

	コマンドまたはアクション
ステップ 4	**snmp-server group***group-name*{**v1**|**v2c**|**v3**{**auth**|**noauth**|**priv**}}[**read***readview*][**write***writeview*][**notify***notifyview*][**access***access-list*] 例： `Switch(config)# snmp-server group public v2c access lmnop`

	コマンドまたはアクション

	コマンドまたはアクション
ステップ 5	**snmp-server user***usernamegroup-name*{**remote***host*[**udp-port***port*]}{**v1**[**access***access-list*]|**v2c**[**access***access-list*]|**v3**[**encrypted**][**access***access-list*][**au** 例： `Switch(config)#  snmp-server user Pat public v2c`

	コマンドまたはアクション
ステップ 6	**end** 例： `Switch(config)# end`

	コマンドまたはアクション
ステップ 7	**show running-config** 例： `Switch# show running-config`
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`

関連トピック

SNMP 設定時の注意事項，（595 ページ）

SNMP ステータスのモニタリング，（616 ページ）

SNMP 通知の設定

トラップマネージャは、トラップを受信して処理する管理ステーションです。 トラップは、特定のイベントが発生したときにスイッチが生成するシステム アラートです。 デフォルトでは、トラップ マネージャは定義されず、トラップは送信されません。 この Cisco IOS Release が稼働しているスイッチでは、トラップ マネージャを無制限に設定できます。

（注） コマンド構文で **traps** というワードを使用するコマンドは多数あります。 トラップまたは情報を選択するオプションがコマンドにない限り、キーワード **traps** はトラップ、情報のいずれか、またはその両方を表します。 **snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

snmp-server host グローバル コンフィギュレーション コマンドを組み合わせて使用することによって、次の表に示す通知タイプを特定のホストで受信できます。 これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定できます。

表 *49*：デバイスの通知タイプ

通知タイプのキーワード	説明
bgp	ボーダー ゲートウェイ プロトコル（BGP）状態変化トラップを生成します。 このオプションは、IP サービス フィーチャ セットがイネーブルになっている場合にだけ使用できます。

通知タイプのキーワード	説明
bridge	STP ブリッジ MIB トラップを生成します。
cluster	クラスタ設定が変更された場合に、トラップを生成します。
config	SNMP 設定が変更された場合に、トラップを生成します。
copy-config	SNMP コピー設定が変更された場合に、トラップを生成します。
cpu threshold	CPU に関連したトラップをイネーブルにします。
entity	SNMP エンティティが変更された場合に、トラップを生成します。
envmon	環境モニタ トラップを生成します。 ファン（fan）、シャットダウン（shutdown）、ステータス（status）、電源（supply）、温度（temperature）の環境トラップのいずれかまたはすべてをイネーブルにできます。
flash	SNMP FLASH 通知を生成します。 スイッチ スタックでは、オプションとして、フラッシュの追加または削除に関する通知をイネーブルにできます。このようにすると、スタックからスイッチを削除するか、またはスタックにスイッチを追加した場合に（物理的な取り外し、電源の再投入、またはリロードの場合に）、トラップが発行されます。
fru-ctrl	エンティティ現場交換可能ユニット（FRU）制御トラップを生成します。 スイッチスタックでは、このトラップはスタックにおけるスイッチの挿入/取り外しを意味します。
hsrp	ホットスタンバイルータプロトコル（HSRP）が変更された場合に、トラップを生成します。
ipmulticast	IP マルチキャストルーティングが変更された場合に、トラップを生成します。
mac-notification	MAC アドレス通知のトラップを生成します。
msdp	Multicast Source Discovery Protocol（MSDP）が変更された場合に、トラップを生成します。
ospf	Open Shortest Path First（OSPF）が変更された場合に、トラップを生成します。 シスコ固有、エラー、リンクステート アドバタイズ、レート制限、再送信、ステート変更に関するトラップを任意にイネーブルにできます。

通知タイプのキーワード	説明
pim	Protocol-Independent Multicast（PIM）が変更された場合に、トラップを生成します。 無効な PIM メッセージ、ネイバー変更、およびランデブー ポイント（RP）マッピングの変更に関するトラップを任意にイネーブルにできます。
port-security	SNMP ポート セキュリティ トラップを生成します。 1 秒あたりの最大トラップ速度も設定できます。 指定できる範囲は 0 ～ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。 （注） 通知タイプ **port-security** を使用してトラップを設定する際に、まずポートセキュリティ トラップを設定して、次に以下のポートセキュリティ トラップ レートを設定します。 **1 snmp-server enable trapsport-security** **2 snmp-server enable trapsport-securitytrap-rate***rate*
rtr	SNMP Response Time Reporter（RTR）のトラップを生成します。
snmp	認証、コールド スタート、ウォーム スタート、リンク アップ、またはリンク ダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。 1 分あたりの最大トラップ速度も設定できます。 指定できる範囲は 0 ～ 1000 です。デフォルトは 0 に設定されています（制限なしの状態では、発生ごとにトラップが送信されます）。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP の Syslog トラップを生成します。
tty	TCP 接続のトラップを生成します。 このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバーシップが変更された場合に、トラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN トランキング プロトコル（VTP）が変更された場合に、トラップを生成します。

ホストにトラップまたは情報を送信するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server engineID remote***ip-addressengineid-string*
4. **snmp-server user***usernamegroup-name*{**remote***host*[**udp-port***port*]}{**v1**[**access***access-list*]|**v2c**[**access***access-list*]|**v3**[**encrypted**][**access***access-list*][**auth**{**md5**|**sha**}*auth-password*]}
5. **snmp-server group***group-name*{**v1**|**v2c**|**v3**{**auth**|**noauth**|**priv**}}[**read***readview*][**write***writeview*][**notify***notifyview*][**access***access-list*]
6. **snmp-server host***host-addr*[**informs**|**traps**][**version**{**1**|**2c**|**3**{**auth**|**noauth**|**priv**}}]*community-string*[*notification-type*]
7. **snmp-server enable traps***notification-types*
8. **snmp-server trap-source***interface-id*
9. **snmp-server queue-length***length*
10. **snmp-server trap-timeout***seconds*
11. **end**
12. **show running-config**
13. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション
ステップ 1	**enable** 例： `Switch> enable`
ステップ 2	**configureterminal** 例： `Switch# configure terminal`
ステップ 3	**snmp-server engineID remote***ip-addressengineid-string* 例： `Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b`
ステップ 4	**snmp-server user***usernamegroup-name*{**remote***host*[**udp-port***port*]}{**v1**[**access***access-list*]|**v2c**[**access***access-list*]|**v3**[**encrypted**][**access***access-lis* 例： `Switch(config)# snmp-server user Pat public v2c`

	コマンドまたはアクション
ステップ 5	**snmp-server group***group-name*{**v1**|**v2c**|**v3**{**auth**|**noauth**|**priv**}}[**read***readview*][**write***writeview*][**notify***notifyview*][**access***access-list*] 例： `Switch(config)# snmp-server group public v2c access lmnop`
ステップ 6	**snmp-server host***host-addr*[**informs**|**traps**][**version**{**1**|**2c**|**3**{**auth**|**noauth**|**priv**}}]*community-string*[*notification-type*] 例： `Switch(config)# snmp-server host 203.0.113.1 comaccess snmp`

	コマンドまたはアクション
ステップ 7	**snmp-server enable traps***notification-types* 例： `Switch(config)# snmp-server enable traps snmp`
ステップ 8	**snmp-server trap-source***interface-id* 例： `Switch(config)# snmp-server trap-source GigabitEthernet1/0/1`

	コマンドまたはアクション
ステップ 9	**snmp-server queue-length***length* 例： `Switch(config)# snmp-server queue-length 20`
ステップ 10	**snmp-server trap-timeout***seconds* 例： `Switch(config)# snmp-server trap-timeout 60`
ステップ 11	**end** 例： `Switch(config)# end`
ステップ 12	**show running-config** 例： `Switch# show running-config`
ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`

次の作業

snmp-server host コマンドでは、通知を受信するホストを指定します。 **snmp-server enable trap** コマンドによって、指定された通知方式（トラップおよび情報）がグローバルでイネーブルになります。 ホストが情報を受信できるようにするには、そのホストに対応する **snmp-server host informs** コマンドを設定し**snmp-server enable traps** コマンドを使用して情報をグローバルにイネーブルにする必要があります。

指定したホストがトラップを受信しないようにするには、**no snmp-server host***host* グローバル コンフィギュレーション コマンドを使用します。 キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。 情報をディセーブルにするには、**no snmp-server host informs** グローバル コンフィギュレーション コマンドを使用してください。 特定のトラップ タイプをディセーブルにするには、**no snmp-server enable traps***notification-types* グローバル コンフィギュレーション コマンドを使用します。

関連トピック

SNMP 通知, （593 ページ）

SNMP ステータスのモニタリング, （616 ページ）

エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム接点およびロケーションを設定して、コンフィギュレーションファイルからこれらの記述にアクセスできるようにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server contact***text*
4. **snmp-server location***text*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server contact***text* 例： `Switch(config)# snmp-server contact Dial System Operator at beeper 21555`	システムの連絡先文字列を設定します。
ステップ 4	**snmp-server location***text* 例： `Switch(config)# snmp-server location Building 3/Room 222`	システムの場所を表す文字列を設定します。

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

関連トピック

SNMP エージェント機能, （592 ページ）

SNMP を通して使用する TFTP サーバの制限

SNMP を介したコンフィギュレーション ファイルの保存とロードに使用する TFTP サーバを、アクセス リストで指定されたサーバに限定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server tftp-server-list***access-list-number*
4. **access-list***access-list-number*{**deny**|**permit**}*source*[*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server tftp-server-list***access-list-number* 例： `Switch(config)# snmp-server tftp-server-list 44`	SNMP を介したコンフィギュレーション ファイルのコピーに使用する TFTP サーバを、アクセス リストのサーバに限定します。 *access-list-number* には、1 ～ 99 および 1300 ～ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 4	**access-list***access-list-number*{**deny**|**permit**}*source*[*source-wildcard*] 例： `Switch(config)# access-list 44 permit 10.1.1.2`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。 *source* には、スイッチにアクセスできる TFTP サーバの IP アドレスを入力します。 （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。

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

SNMP ステータスのモニタリング

不正なコミュニティストリングエントリ、エラー、要求変数の数など、SNMP の入出力統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。 また、次の表にリストされたその他の特権 EXEC コマンドを使用して、SNMP 情報を表示することもできます。

表 *50*：*SNMP* 情報を表示するためのコマンド

コマンド	目的
show snmp	SNMP 統計情報を表示します。
	デバイスに設定されているローカル SNMP エンジンおよびすべてのリモートエンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求の情報を表示します。
show snmp sessions	現在の SNMP セッションの情報を表示します。

コマンド	目的
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。 （注） このコマンドは、**auth** | **noauth** | **priv** モードの SNMPv3 設定情報を表示するときに使用する必要があります。 この情報は、**show running-config** の出力には表示されません。

関連トピック

SNMP エージェントのディセーブル化, （596 ページ）

SNMP エージェント機能, （592 ページ）

SNMP グループおよびユーザの設定, （601 ページ）

SNMP 設定時の注意事項, （595 ページ）

SNMP 通知の設定, （606 ページ）

SNMP 通知, （593 ページ）

SNMP の例

次に、SNMP のすべてのバージョンをイネーブルにする例を示します。 この設定では、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。 この設定では、スイッチ はトラップを送信しません。

```
Switch(config)# snmp-server community public
```

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。 スイッチはさらに、SNMPv1 を使用してホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に VTP トラップを送信します。 コミュニティ ストリング *public* は、トラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。 その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。 SNMP 認証障害トラップは、SNMPv2C がコミュニティ ストリング *public* を使用してホスト *cisco.com* に送信します。

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。 コミュニティ ストリングは制限されます。 1 行めで、スイッチ はすでにイネーブルになっているトラップ以外

に、エンティティ MIB トラップを送信できるようになります。 2 行目はこれらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の **snmp-server** ホスト コマンドを無効にします。

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```

次に、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

次に、ユーザとリモートホストを関連付けて、ユーザがグローバルコンフィギュレーションモードのときに **auth**（authNoPriv）認証レベルで情報を送信する例を示します。

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5 mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

第 27 章

SPAN および RSPAN の設定

- 機能情報の確認，619 ページ
- SPAN および RSPAN の前提条件，619 ページ
- SPAN および RSPAN の制約事項，620 ページ
- SPAN および RSPAN について，623 ページ
- SPAN および RSPAN の設定方法，637 ページ
- SPAN および RSPAN 動作のモニタリング，664 ページ
- SPAN および RSPAN の設定例，664 ページ

機能情報の確認

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

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

SPAN および RSPAN の前提条件

SPAN

- SPAN トラフィックを特定の VLAN に制限するには、**filter vlan** キーワードを使用します。トランク ポートをモニタしている場合、このキーワードで指定された VLAN 上のトラフィッ

クのみがモニタされます。 デフォルトでは、トランク ポート上のすべての VLAN がモニタされます。

RSPAN

- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。

SPAN および RSPAN の制約事項

SPAN

- 各スイッチにつき、最大 4 つの送信元セッション（スイッチが Catalyst 2960-S スイッチでスタック構成されている場合は最大 2 つ）および 64 の RSPAN 宛先セッションを設定できます。 送信元セッションは、ローカル SPAN セッションまたは RSPAN 送信元セッションのどちらかになります。
- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックをモニタできます。 1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- スイッチ ポートを SPAN 宛先ポートとして設定すると、通常のスイッチ ポートではなくなります。SPAN 宛先ポートを通過するのは、監視対象トラフィックのみになります。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。 設定されている SPAN パラメータを削除するには、**no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなしまたは IEEE 802.1Q）を伝送します。 このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。
- ディセーブルのポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN がイネーブルになってからです。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。
- スタックは、LAN Base イメージを実行しているスイッチのみでサポートされています。

SPAN セッションのトラフィック モニタリングには次の制約事項があります。

- ポートまたはVLANを送信元にできますが、同じセッション内に送信元ポートと送信元VLANを混在させることはできません。
- スイッチは、最大4つのローカルSPANまたはRSPAN送信元セッションをサポートします。ただし、このスイッチが Catalyst 2960-S スイッチでスタック構成されている場合は、2 つのローカル SPAN または RSPAN 送信元セッションに制限されます。
  - 同じスイッチまたはスイッチ スタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。 スイッチまたはスイッチ スタックは合計 64 の送信元および RSPAN 宛先セッションをサポートします。
  - 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。 スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つの スイッチ スタックあたりに設定できる宛先ポートは最大で 64 個です。
- SPAN セッションがスイッチの通常の動作を妨げることはありません。 ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN がイネーブルの場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。 多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- スイッチは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じスイッチまたはスイッチ スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

RSPAN

- RSPAN は、BPDU パケット モニタリングまたは他のレイヤ 2 スイッチ プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。 不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのスイッチで VLAN RSPAN 機能がサポートされていることを確認してください。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。 また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。 ただし、スイッチはスパンされたト

ラフィックをモニタしないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパニングがサポートされません。

- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがプルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラッディングが防止されます。

フローベースの SPAN（FSPAN）およびフローベースの RSPAN（FRSPAN）

- ACL は、一度に 1 つの SPAN または RSPAN にしか接続できません。
- FSPAN ACL が接続されていない場合、FSPAN はディセーブルで、すべてのトラフィックが SPAN 宛先ポートにコピーされます。
- SPAN セッションに空の FSPAN ACL を接続すると、パケットはフィルタリングされず、すべてのトラフィックが監視されます。
- FSPAN ACL は、ポート単位 VLAN 単位のセッションに適用できません。 ポート単位 VLAN 単位のセッションは、最初にポートベースのセッションを設定し、次にセッションに特定の VLAN を設定することにより設定できます。 次に例を示します。

```
Switch(config)# monitor session session_number source interface interface-id
Switch(config)# monitor session session_number filter vlan vlan-id
Switch(config)# monitor session session_number filter ip access-group {access-list-number|
name}
```

（注） **filter vlan** および **filter ip access-group** の両方のコマンドを同時に設定できません。 一方を設定すると、他方が拒否されます。

- EtherChannel は FSPAN セッションでサポートされていません。
- TCP フラグまたは **log** キーワードが付いている FSPAN ACL はサポートされていません。
- スイッチで拡張 IP サービス フィーチャ セットを稼働中に IPv6 FSPAN ACL を設定し、のちに異なるフィーチャ セットを稼働した場合、スイッチのリブート後、スイッチでの IPv6 FSPAN ACL 設定が失われる可能性があります。
- IPv6 FSPAN ACL は、IPv6 対応の SDM テンプレートでだけサポートされています。 IPv6 対応の SDM テンプレートを稼働中に IPv6 FSPAN ACL を設定し、のちに非 IPv6 SDM テンプレートを設定してスイッチをリブートすると、IPv6 FSPAN ACL 設定が失われます。

SPAN および RSPAN について

SPAN および RSPAN

ポートまたはVLANを通過するネットワーク トラフィックを解析するには、SPANまたはRSPANを使用して、そのスイッチ上、またはネットワーク アナライザやその他のモニタデバイス、あるいはセキュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。 SPANは送信元ポート上または送信元VLAN上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。 SPANは送信元ポートまたはVLAN上のネットワーク トラフィックのスイッチングには影響しません。 宛先ポートはSPAN専用にする必要があります。 SPANまたはRSPANセッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPANを使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元VLANに出入りするトラフィックだけです。送信元VLANにルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別のVLANから送信元VLANにルーティングされているトラフィックはモニタできません。ただし、送信元VLANで受信し、別のVLANにルーティングされるトラフィックは、モニタできます。

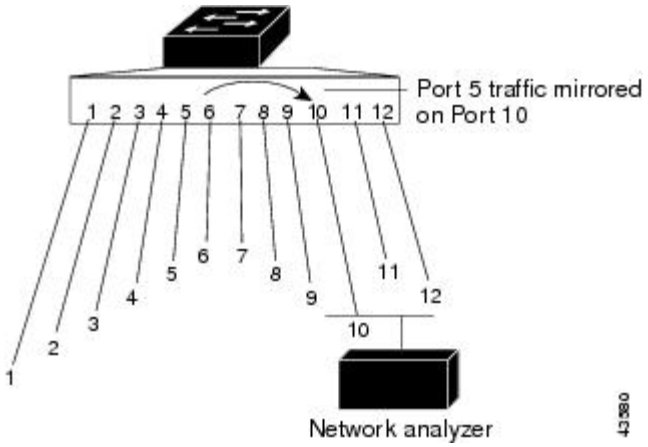
ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPANまたはRSPAN宛先ポートを使用できます。 たとえば、Cisco侵入検知システム（IDS）センサー装置を宛先ポートに接続した場合、IDSデバイスはTCPリセットパケットを送信して、疑わしい攻撃者のTCPセッションを停止させることができます。

ローカル SPAN

ローカルSPANは1つのスイッチ内のSPANセッション全体をサポートします。すべての送信元ポートまたは送信元VLAN、および宛先ポートは、同じスイッチまたはスイッチ スタック内にあります。 ローカルSPANは、任意のVLAN上の1つまたは複数の送信元ポートからのトラフィック、あるいは1つまたは複数のVLANからのトラフィックを解析するために宛先ポートへコピーします。

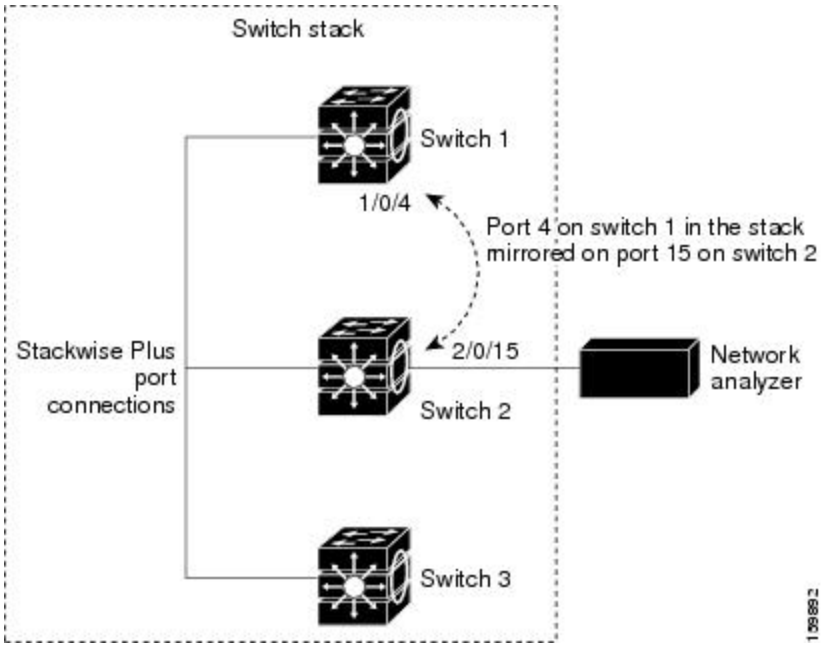
ポート 5（送信元ポート）上のすべてのトラフィックがポート 10（宛先ポート）にミラーリングされます。 ポート 10 のネットワーク アナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 からのすべてのネットワーク トラフィックを受信します。

図 *49*：単一デバイスでのローカル *SPAN* の設定例



これは、スイッチ スタック内のローカル SPAN の例です。送信元ポートと宛先ポートは異なるスタック メンバにあります。

図 *50*：デバイス スタックでのローカル *SPAN* の設定例



関連トピック

ローカル SPAN セッションの作成, （637 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定, （640 ページ）

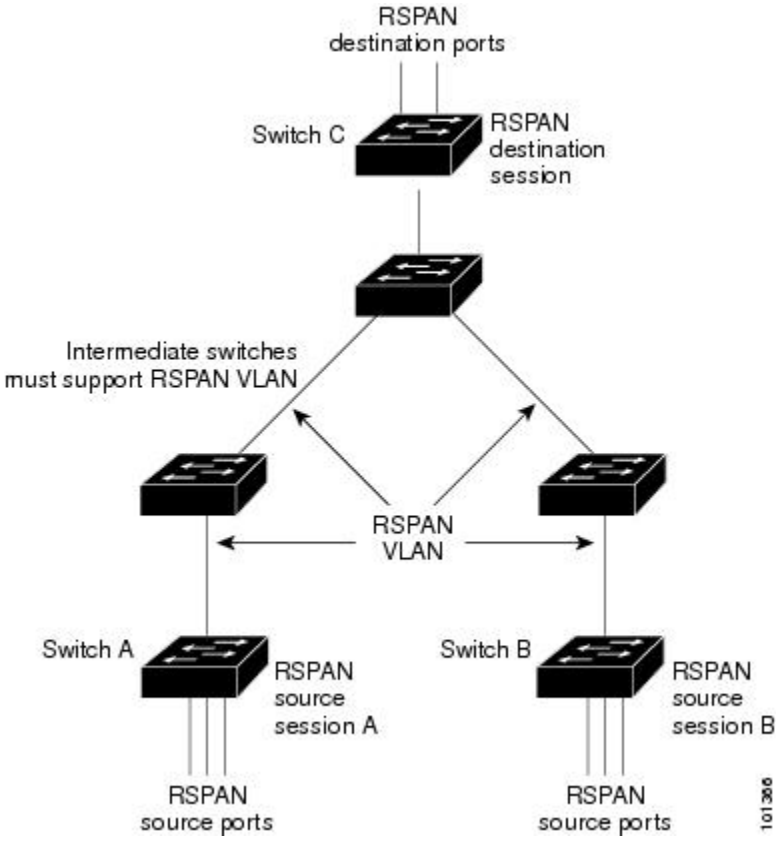
例：ローカル SPAN の設定，（664 ページ）

リモート SPAN

RSPANは、異なるスイッチ（または異なるスイッチスタック）上の送信元ポート、送信元VLAN、および宛先ポートをサポートしているので、ネットワーク上で複数のスイッチをリモートモニタリングできます。

下の図にスイッチAとスイッチBの送信元ポートを示します。各RSPANセッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチの RSPAN セッション専用です。 送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介して、RSPAN VLAN をモニタする宛先セッションに転送されます。 各 RSPAN 送信元スイッチには、ポートまたは VLAN のいずれかが RSPAN 送信元として必要です。 図中のスイッチ C のように、宛先は常に物理ポートになります。

図 *51*：*RSPAN* の設定例



関連トピック

RSPAN 送信元セッションの作成，（647 ページ）
RSPAN 宛先セッションの作成，（652 ページ）

RSPAN 宛先セッションの作成および着信トラフィックの設定, （654 ページ）
例：RSPAN VLAN の作成, （665 ページ）

SPAN と RSPAN の概念および用語

- SPAN セッション
- モニタ対象トラフィック
- 送信元ポート
- 送信元 VLAN
- VLAN フィルタリング
- 宛先ポート
- RSPAN VLAN

SPAN セッション

SPANセッション（ローカルまたはリモート）を使用すると、1つまたは複数のポート上、あるいは 1 つまたは複数の VLAN 上でトラフィックをモニタし、そのモニタしたトラフィックを 1 つまたは複数の宛先ポートに送信できます。

ローカルSPANセッションは、宛先ポートと送信元ポートまたは送信元VLAN（すべて単一のネットワーク デバイス上にある）を結び付けたものです。 ローカル SPAN には、個別の送信元および宛先のセッションはありません。 ローカル SPAN セッションはユーザが指定した入力および出力のパケット セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は少なくとも 1 つの RSPAN 送信元セッション、1 つの RSPAN VLAN、および少なくとも 1 つの RSPAN 宛先セッションで構成されています。 RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。 デバイスに RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。 このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。 別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN に関連付けます。 宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームが転送される点を除き、ローカル SPAN セッションに非常に似ています。 RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再設定され、通常のトランク ポートを介して宛先スイッチに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットを取得し、VLAN のタギングを除去し、宛先ポートに送ります。 セッションは、（レイヤ 2 制御パケットを除く）すべての RSPAN VLAN パケットのコピーを分析のためにユーザに提供します。

同じ RSPAN VLAN 内で、複数の送信元セッションと複数の宛先セッションをアクティブにできます。 中間スイッチは RSPAN 送信元セッションと宛先セッションを分離することもできます。 これらのスイッチは RSPAN を実行できませんが、RSPAN VLAN の要求に応答する必要があります。

SPAN セッションでのトラフィックのモニタには、次のような制約があります。

- ポートまたはVLANを送信元にできますが、同じセッション内に送信元ポートと送信元VLANを混在させることはできません。
- スイッチは、最大2つのローカルSPANまたはRSPAN送信元セッションをサポートします。
  - 同じスイッチまたはスイッチ スタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。 スイッチまたはスイッチ スタックは合計 64 の送信元および RSPAN 宛先セッションをサポートします。
  - 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。 スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つのスイッチ スタックあたりに設定できる宛先ポートは最大で 64 個です。
- SPAN セッションがスイッチの通常の動作を妨げることはありません。 ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN がイネーブルの場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。 したがって、多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- スイッチは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じスイッチまたはスイッチ スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

関連トピック

ローカル SPAN セッションの作成, （637 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定, （640 ページ）
例：ローカル SPAN の設定, （664 ページ）

モニタ対象トラフィック

SPAN セッションは、次のトラフィック タイプを監視できます。

- 受信（Rx）SPAN：受信（または入力）SPAN は、スイッチが変更または処理を行う前に、送信元インターフェイスまたはVLANが受信したすべてのパケットをできるだけ多くモニタリングします。 送信元が受信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。

Diffserv コード ポイント（DSCP）の変更など、ルーティングや Quality of Service（QoS）が原因で変更されたパケットは、変更される前にコピーされます。

受信処理中にパケットをドロップする可能性のある機能は、入力 SPAN には影響を与えません。宛先ポートは、実際の着信パケットがドロップされた場合でも、パケットのコピーを受信します。 パケットをドロップする可能性のある機能は、標準および拡張 IP 入力アクセス コントロール リスト（ACL）、入力 QoS ポリシング、VLAN ACL、および出力 QoS ポリシングです。

- 送信（Tx）SPAN：送信（または出力）SPAN は、スイッチによる変更または処理がすべて実行されたあとに、送信元インターフェイスから送信されたすべてのパケットをできる限り多くモニタリングします。 送信元が送信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。 コピーはパケットの変更後に用意されます。

  ルーティングが原因で変更されたパケット（存続可能時間（TTL）、MAC アドレス、QoS 値の変更など）は、宛先ポートで（変更されて）コピーされます。

  送信処理中にパケットをドロップする可能性のある機能は、SPAN 用の複製コピーにも影響します。 これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングがあります。

- 両方：SPAN セッションで、受信パケットと送信パケットの両方について、ポートまたは VLAN をモニタすることもできます。 これはデフォルトです。

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。 通常、SPAN は Cisco Discovery Protocol（CDP）、VLAN トランキング プロトコル（VTP）、Dynamic Trunking Protocol（DTP）、スパニングツリー プロトコル（STP）、ポート集約プロトコル（PAgP）などのブリッジ プロトコル データ ユニット（BPDU）パケットおよびレイヤ 2 プロトコルをモニタしません。 ただし、宛先ポートを設定するときに **encapsulation replicate** キーワードを入力すると、次の変更が発生します。

- 送信元ポートと同じカプセル化設定（タグなしまたは IEEE 802.1Q）を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコル パケットを含むすべてのタイプのパケットがモニタされます。

したがって、カプセル化レプリケーションがイネーブルにされたローカル SPAN セッションでは、タグなし、および IEEE 802.1Q タグ付きパケットが宛先ポートに混在することがあります。

スイッチの輻輳により、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットがドロップされることがあります。 一般に、これらの特性は互いに無関係です。 次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因でモニタされないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- スイッチの輻輳が原因でドロップされた出力パケットは、出力 SPAN からもドロップされます。

SPAN の設定によっては、同一送信元のパケットのコピーが複数、SPAN 宛先ポートに送信されます。 たとえば、ポート A での RX モニタ用とポート B での TX モニタ用に双方向（RX と TX）SPAN セッションが設定されているとします。パケットがポート A からスイッチに入ってポート B にスイッチされると、着信パケットも発信パケットも宛先ポートに送信されます。 このため、両方のパケットは同じものになります。レイヤ 3 書き換えが行われた場合には、パケット変更のため異なるパケットになります。

送信元ポート

送信元ポート（別名監視対象ポート）は、ネットワーク トラフィック分析のために監視するスイッチド ポートまたはルーテッド ポートです。 1 つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向でモニタできます。 スイッチは、任意の数の送信元ポート（スイッチで利用可能なポートの最大数まで）と任意の数の送信元 VLAN（サポートされている VLAN の最大数まで）をサポートしています。 ただし、スイッチが送信元ポートまたは VLAN でサポートするセッション数には上限（4 つ。スイッチが Catalyst 2960-S スイッチのスタック内にある場合は 2 つ）（ローカルまたは RSPAN）があります。 単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- 複数の SPAN セッションでモニタできます。
- モニタする方向（入力、出力、または両方）を指定して、各送信元ポートを設定できます。
- すべてのポート タイプ（EtherChannel、ギガビット イーサネットなど）が可能です。
- EtherChannel 送信元の場合、EtherChannel 全体のトラフィック、またはポート チャネルに含まれる物理ポートごとのトラフィックをモニタできます。
- アクセス ポート、トランク ポート、ルーテッド ポート、または音声 VLAN ポートに指定できます。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニタすることが可能です。

送信元 *VLAN*

VLAN ベースの SPAN（VSPAN）では、1 つまたは複数の VLAN のネットワーク トラフィックをモニタできます。 VSPAN 内の SPAN または RSPAN 送信元インターフェイスが VLAN ID となり、トラフィックはその VLAN のすべてのポートでモニタされます。

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブ ポートは送信元ポートとして含まれ、単一方向または双方向でモニタできます。
- 指定されたポートでは、モニタ対象の VLAN 上のトラフィックのみが宛先ポートに送信されます。
- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、モニタされません。

- ポートが送信元VLANに追加または削除されると、これらのポートで受信された送信元VLANのトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニタできるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブなすべてのVLANがモニタされます。 VLANフィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニタ対象を特定の VLAN に制限できます。

- VLAN フィルタリングが適用されるのは、トランク ポートまたは音声 VLAN ポートのみです。
- VLANフィルタリングはポートベースセッションにのみ適用され、VLAN送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセスポートではリスト内の該当 VLAN のみがモニタされます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートおよび VLAN からのトラフィックのコピーを受信し、SPANパケットをユーザ（通常はネットワーク アナライザ）に送信する宛先ポート（別名モニタ側ポート）が必要です。

宛先ポートの特性は、次のとおりです。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチまたはスイッチ スタックに存在している必要があります。 RSPANセッションの場合は、RSPAN宛先セッションを含むスイッチ上にあります。 RSPAN 送信元セッションのみを実行するスイッチまたはスイッチ スタックには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。 SPAN 宛先設定を削除すると、ポートは以前の設定に戻ります。 ポートがSPAN宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。

（注） SPAN の宛先ポートに QoS が設定されている場合、QoS はただちに有効になります。

- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。 削除されたポートがルーテッド ポートであった場合、このポートはルーテッド ポートでなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにすることはできません。
- 送信元ポートにすることはできません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。 ポートは SPAN セッションに必要なトラフィック以外は送信しません。 宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- スイッチまたはスイッチ スタックの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化で次のように動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、各パケットに元のカプセル化が使用されます（タグなし、ISL、または IEEE 802.1Q）。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。 したがって、**encapsulation replicate** がイネーブルになっているローカル SPAN セッションの出力に、タグなし、ISL、または IEEE 802.1Q タグ付きパケットが混在することがあります。
- RSPAN の場合は、元の VLAN ID は RSPAN VLAN ID で上書きされるため失われます。 したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

RSPAN VLAN は、RSPAN の送信元セッションと宛先セッション間で SPAN トラフィックを伝送します。 RSPAN VLAN には、次の特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上のみです。
- RSPAN VLAN は、**remote-span** VLAN コンフィギュレーション モード コマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。

- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN を、プライベート VLAN のプライマリまたはセカンダリ VLAN にはできません。

VLAN トランキング プロトコル（VTP）に対して可視である VLAN 1 ～ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。 拡張 VLAN 範囲（1006 ～ 4094）内の RSPAN VLAN ID を割り当てる場合は、すべての中間スイッチを手動で設定する必要があります。

通常は、ネットワークに複数の RSPAN VLAN を配置し、それぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。 つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションで、パケットを RSPAN セッションに送信できます。 また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN をモニタしたり、ユーザにトラフィックを送信したりできます。 セッションは RSPAN VLAN ID によって区別されます。

関連トピック

RSPAN 送信元セッションの作成, （647 ページ）
RSPAN 宛先セッションの作成, （652 ページ）
RSPAN 宛先セッションの作成および着信トラフィックの設定, （654 ページ）
例：RSPAN VLAN の作成, （665 ページ）

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッド トラフィックを監視しません。 VSPAN が監視するのはスイッチに出入りするトラフィックに限られ、VLAN 間でルーティングされるトラフィックは監視しません。 たとえば、VLAN が受信モニタされ、スイッチが別の VLAN から監視対象 VLAN にトラフィックをルーティングする場合、そのトラフィックは監視されず、SPAN 宛先ポートで受信されません。
- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。 SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。 送信元ポートでは、SPAN は STP ステータスに影響を与えません。 STP は RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。
- CDP：SPAN セッションがアクティブな間、SPAN 宛先ポートは CDP に参加しません。 SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。
- VTP：VTP を使用すると、スイッチ間で RSPAN VLAN のプルーニングが可能です。
- VLAN およびトランキング：送信元ポート、または宛先ポートの VLAN メンバーシップまたはトランクの設定値を、いつでも変更できます。 ただし、宛先ポートの VLAN メンバーシップまたはトランクの設定値に対する変更が有効になるのは、SPAN 宛先設定を削除してから

です。 送信元ポートの VLAN メンバーシップまたはトランクの設定値に対する変更は、ただちに有効になり、対応する SPAN セッションが変更に応じて自動的に調整されます。

- EtherChannel：EtherChannelグループを送信元ポートとして設定することはできますが、SPAN 宛先ポートとして設定することはできません。 グループが SPAN 送信元として設定されている場合、グループ全体がモニタされます。

  モニタ対象の EtherChannel グループに物理ポートを追加すると、SPAN 送信元ポート リストに新しいポートが追加されます。 モニタ対象の EtherChannel グループからポートを削除すると、送信元ポート リストからそのポートが自動的に削除されます。

  EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。 この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータはモニタされます。 ただし、EtherChannel グループに含まれる物理ポートを SPAN 宛先として設定した場合、その物理ポートはグループから削除されます。 SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。 EtherChannel グループから削除されたポートは、グループ メンバのままですが、inactive または suspended ステートになります。

  EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが送信元の場合、ポートは EtherChannel グループおよびモニタ対象ポート リストから削除されます。

- マルチキャスト トラフィックをモニタできます。 出力ポートおよび入力ポートのモニタでは、未編集のパケットが 1 つだけ SPAN 宛先ポートに送信されます。 マルチキャスト パケットの送信回数は反映されません。

- プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。

- セキュア ポートを SPAN 宛先ポートにすることはできません。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。 RSPAN 送信元セッションでは、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。

- IEEE 802.1x ポートは SPAN 送信元ポートにできます。 SPAN 宛先ポート上で IEEE 802.1x をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブルに設定されます。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。 RSPAN 送信元セッションでは、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。

フローベースの SPAN

送信元ポートで監視されるトラフィックにアクセス コントロール リスト（ACL）を適用するフローベース SPAN（FSPAN）またはフローベース RSPAN（FRSPAN）を使用して、SPAN または RSPAN で監視するネットワーク トラフィックのタイプを制御できます。 FSPAN ACL は、IPv4、IPv6、および監視される非 IP トラフィックをフィルタリングするように設定できます。

インターフェイスを通して ACL を SPAN セッションに適用します。 ACL は SPAN セッション内のすべてのインターフェイスで監視されるすべてのトラフィックに適用されます。この ACL によって許可されるパケットは、SPAN 宛先ポートにコピーされます。 ほかのパケットは SPAN 宛先ポートにコピーされません。

元のトラフィックは継続して転送され、接続している任意のポート、VLAN、およびルータ ACL が適用されます。 FSPAN ACL は転送の決定に影響を与えることはありません。 同様に、ポート、VLAN、およびルータ ACL は、トラフィックのモニタリングに影響を与えません。 セキュリティ入力 ACL がパケットを拒否したために転送されない場合でも、FSPAN ACL が許可すると、パケットは SPAN 宛先ポートにコピーされます。 しかし、セキュリティ出力 ACL がパケットを拒否したために転送されない場合、パケットは SPAN 宛先ポートにコピーされません。 ただし、セキュリティ出力 ACL がパケットの送信を許可した場合だけ、パケットは、FSPAN ACL が許可した場合 SPAN 宛先ポートにコピーされます。 これは RSPAN セッションについてもあてはまります。

SPAN セッションには、次の 3 つのタイプの FSPAN ACL を接続できます。

- IPv4 FSPAN ACL：IPv4 パケットだけをフィルタリングします。
- IPv6 FSPAN ACL：IPv6 パケットだけをフィルタリングします。
- MAC FSPAN ACL：IP パケットだけをフィルタリングします。

セキュリティ ACL は、スイッチ上の FSPAN ACL よりも高いプライオリティをもっています。 FSPAN ACL が適用され、その後ハードウェア メモリに収まらないセキュリティ ACL を追加する場合、適用された FSPAN ACL は、セキュリティ ACL のスペースを確保するためにメモリから削除されます。 この処理（アンローディングと呼ばれる）は、システム メッセージにより通知されます。 メモリ内に常駐するスペースが確保できたら、スイッチ上のハードウェア メモリに FSPAN ACL が追加されます。 この処理（リローディングと呼ばれる）は、システム メッセージにより通知されます。 IPv4、IPv6、および MAC FSPAN ACL は、別個にアンロードまたはリロードできます。

スタックに設定された VLAN ベースの FSPAN セッションが 1 つまたは複数のスイッチ上のハードウェア メモリに収まらない場合、セッションはこれらのスイッチ上でアンロードされたものとして処理され、スイッチでの FSPAN ACL およびソーシングのためのトラフィックは、SPAN 宛先ポートにコピーされません。 FSPAN ACL は継続して正しく適用され、トラフィックは FSPAN ACL がハードウェア メモリに収まるスイッチの SPAN 宛先ポートにコピーされます。

空の FSPAN ACL が接続されると、一部のハードウェア機能により、その ACL の SPAN 宛先ポートにすべてのトラフィックがコピーされます。 十分なハードウェア リソースが使用できない場合、空の FSPAN ACL もアンロードされる可能性があります。

IPv4 および MAC FSPAN ACL は、すべてのフィーチャ セットでサポートされています。 IPv6 FSPAN ACL は、拡張 IP Services フィーチャ セットでだけサポートされています。

関連トピック

FSPAN セッションの設定, （657 ページ）
FRSPAN セッションの設定, （660 ページ）

SPAN および RSPAN のデフォルト設定

表 *51*：*SPAN* および *RSPAN* のデフォルト設定

機能	デフォルト設定
SPAN のステート（SPAN および RSPAN）	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィックの両方（**both**）
カプセル化タイプ（宛先ポート）	ネイティブ形式（タグなしパケット）
入力転送（宛先ポート）	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。
RSPAN VLAN	未設定

設定時の注意事項

SPAN 設定時の注意事項

- SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。 宛先インターフェイスの場合、このコマンドの **no** 形式では、**encapsulation** オプションは無視されます。
- トランク ポート上のすべての VLAN をモニタするには、**no monitor session** *session_number* **filter** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

ローカル SPAN セッションの作成，（637 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定，（640 ページ）
例：ローカル SPAN の設定，（664 ページ）

RSPAN 設定時の注意事項

- すべての SPAN 設定時の注意事項が RSPAN に適用されます。

- RSPAN VLAN には特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定のパケットを選択的にフィルタリングまたはモニタできます。 RSPAN 送信元スイッチ内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数のスイッチに分散させることができます。
- RSPAN VLAN 上のアクセス ポート（音声 VLAN ポートを含む）は、非アクティブ ステートになります。
- 次の条件を満たす限り、任意の VLAN を RSPAN VLAN として設定できます。
  - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
  - 参加しているすべてのスイッチで RSPAN がサポートされている。

関連トピック

RSPAN 送信元セッションの作成, （647 ページ）
RSPAN 宛先セッションの作成, （652 ページ）
RSPAN 宛先セッションの作成および着信トラフィックの設定, （654 ページ）
例：RSPAN VLAN の作成, （665 ページ）

FSPAN および FRSPAN 設定時の注意事項

- 少なくとも 1 つの FSPAN ACL が接続されている場合、FSPAN はイネーブルになります。
- SPAN セッションに空ではない FSPAN ACL を少なくとも 1 つ接続し、ほかの 1 つまたは複数の FSPAN ACL を接続しなかった場合（たとえば、空ではない IPv4 ACL を接続し、IPv6 と MAC ACL を接続しなかった場合）、FSPAN は、接続されていない ACL によってフィルタリングされたと思われるトラフィックをブロックします。 したがって、このトラフィックは監視されません。

関連トピック

FSPAN セッションの設定, （657 ページ）
FRSPAN セッションの設定, （660 ページ）

SPAN および RSPAN の設定方法

ローカル SPAN セッションの作成

SPANセッションを作成し、送信元（モニタ対象）ポートまたはVLAN、および宛先（モニタ側）ポートを指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***source** {**interface***interface-id* |**vlan** *vlan-id*} [**,** | **-**] [**both** |**rx** | **tx**]
5. **monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**encapsulation replicate**]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session all`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPANセッションを削除します。

	コマンドまたはアクション	目的
ステップ 4	**monitor session***session_number***source** {**interface***interface-id* |**vlan** *vlan-id*} [**,** | **-**] [**both** |**rx** | **tx**] 例： `Switch(config)# monitor session 1 source interface gigabitethernet1/0/1`	SPANセッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタする送信元ポートを指定します。 有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）があります。 有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタする送信元 VLAN を指定します。 指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （任意）**[,|-]** は、一連または一定範囲のインターフェイスを指定します。 カンマの前後およびハイフンの前後にスペースを1つずつ入力します。 • （任意）**both** | **rx** | **tx**：モニタするトラフィックの方向を指定します。 トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 ◦ **both**：受信トラフィックと送信トラフィックの両方をモニタします。 ◦ **rx**：受信トラフィックをモニタします。 ◦ **tx**：送信トラフィックをモニタします。 （注） **monitor session***session_number***source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。

	コマンドまたはアクション	目的
ステップ 5	**monitor session***session_number***destination**{**interface***interface-id*[**,** | -] [**encapsulation replicate**]} 例： `Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate`	SPANセッションおよび宛先ポート（モニタ側ポート）を指定します。 （注） ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *interface-id* には、宛先ポートを指定します。 宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）**[,|-]** は、一連または一定範囲のインターフェイスを指定します。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。 選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 （注） **monitor session***session_number***destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

ローカル SPAN, （623 ページ）
SPAN セッション, （626 ページ）
SPAN 設定時の注意事項, （635 ページ）

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成し、さらに送信元ポートまたは VLAN および宛先ポートを指定した後、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置等）用に着信トラフィックをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***source** {**interface***interface-id* |**vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**encapsulation replicate**][**ingress** {**dot1q vlan***vlan-id* |**isl** |**untagged vlan***vlan-id*|**vlan***vlan-id*}]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session all`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。

	コマンドまたはアクション	目的
		• **local**：すべてのローカルセッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number***source** {**interface***interface-id* |**vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx`	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。
ステップ 5	**monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**encapsulation replicate**][**ingress** {**dot1q vlan***vlan-id* |**isl** |**untagged vlan***vlan-id*|**vlan***vlan-id*}]} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6`	SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *interface-id* には、宛先ポートを指定します。 宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 •（任意）**[,|-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。 カンマまたはハイフンの前後にスペースを 1 つずつ入力します。 •（任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。 選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 • **ingress** は、宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。 ◦ **dot1q vlan***vlan-id*：デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受信します。 ◦ **isl**：ISL カプセル化を使用して入力パケットを転送します。

	コマンドまたはアクション	目的
		◦ **untagged vlan***vlan-id* または **vlan***vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受信します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

ローカル SPAN,（623 ページ）
SPAN セッション,（626 ページ）
SPAN 設定時の注意事項,（635 ページ）
例：ローカル SPAN の設定,（664 ページ）

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number* **source interface***interface-id*
5. **monitor session***session_number***filter vlan***vlan-id*[**,** | **-**]
6. **monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**encapsulation replicate**]}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session all`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number* **source interface***interface-id* 例： `Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx`	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。 指定したインターフェイス

	コマンドまたはアクション	目的
		は、あらかじめトランク ポートとして設定しておく必要があります。
ステップ 5	**monitor session***session_number***filter vlan***vlan-id*[**,** | **-**] 例： `Switch(config)# monitor session 2 filter vlan 1 - 5 , 9`	SPAN 送信元トラフィックを特定の VLAN に制限します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* に指定できる範囲は 1 ～ 4094 です。 • （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 6	**monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**encapsulation replicate**]} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1`	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）[**,** | **-**] は、一連のまたは一定範囲のインターフェイスを指定します。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。 選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

RSPAN VLAN としての VLAN の設定

新しい VLAN を作成し、RSPAN セッション用の RSPAN VLAN になるように設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vlan***vlan-id*
4. **remote-span**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan***vlan-id* 例： `Switch(config)# vlan 100`	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。 指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN 専用）にすることはできません。
ステップ 4	**remote-span** 例： `Switch(config-vlan)# remote-span`	VLAN を RSPAN VLAN として設定します。
ステップ 5	**end** 例： `Switch(config-vlan)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

RSPAN に参加するすべてのスイッチに RSPAN VLAN を作成する必要があります。 RSPAN VLAN ID が標準範囲（1005 未満）であり、VTP がネットワーク内でイネーブルである場合は、1 つのスイッチに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するように設定できます。 拡張範囲 VLAN（1005 を超える ID）の場合、送信元と宛先の両方のスイッチ、および中間スイッチに RSPAN VLAN を設定する必要があります。

VTP プルーニングを使用して、RSPAN トラフィックが効率的に流れるようにするか、または RSPAN トラフィックの伝送が不要なすべてのトランクから、RSPAN VLAN を手動で削除します。

VLAN からリモート SPAN 特性を削除して、標準 VLAN に戻すように変換するには、**no remote-span** VLAN コンフィギュレーション コマンドを使用します。

SPAN セッションから送信元ポートまたは VLAN を削除するには、**no monitor session***session_number***source** {**interface***interface-id* |**vlan** *vlan-id*} グローバル コンフィギュレーション コマンドを使用します。 セッションから RSPAN VLAN を削除するには、**no monitor session***session_number***destination remote vlan***vlan-id* コマンドを使用します。

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを作成および開始し、モニタ対象の送信元および宛先 RSPAN VLAN を指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***source** {**interface***interface-id*| **vlan***vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session***session_number***destinationremote vlan***vlan-id*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。

	コマンドまたはアクション	目的
	例： `Switch(config)# no monitor session 1`	• **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number***source** {**interface***interface-id*| **vlan***vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx`	RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。 ◦ *interface-id* には、モニタリングする送信元ポートを指定します。 有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）があります。有効なポートチャネル番号は 1 ～ 48 です。 ◦ *vlan-id* には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。 • （任意）**[,|-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**both** | **rx** | **tx**：モニタするトラフィックの方向を指定します。 トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 ◦ **both**：受信トラフィックと送信トラフィックの両方をモニタします。 ◦ **rx**：受信トラフィックをモニタします。 ◦ **tx**：送信トラフィックをモニタします。

	コマンドまたはアクション	目的
ステップ 5	**monitor session***session_number***destinationremote vlan***vlan-id* 例： `Switch(config)# monitor session 1 destination remote vlan 100`	RSPAN セッション、宛先 RSPAN VLAN、および宛先ポート グループを指定します。 • *session_number* には、ステップ 4 で指定した番号を入力します。 • *vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

リモート SPAN, （625 ページ）
RSPAN VLAN, （631 ページ）
RSPAN 設定時の注意事項, （635 ページ）

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するように RSPAN 送信元セッションを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number* **source interface***interface-id*
5. **monitor session***session_number***filter vlan***vlan-id*[**,** | **-**]
6. **monitor session***session_number***destinationremote vlan***vlan-id*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number* **source interface***interface-id* 例： `Switch(config)# monitor session 2`	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。 指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。

	コマンドまたはアクション	目的
	source interface gigabitethernet1/0/2 rx	
ステップ 5	**monitor session***session_number***filter vlan***vlan-id*[**,** | **-**] 例： `Switch(config)# monitor session 2 filter vlan 1 - 5 , 9`	SPAN 送信元トラフィックを特定の VLAN に制限します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* に指定できる範囲は 1 ～ 4094 です。 •（任意）**,** | **-**：カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 6	**monitor session***session_number***destinationremote vlan***vlan-id* 例： `Switch(config)# monitor session 2 destination remote vlan 902`	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは、別のスイッチまたはスイッチ スタック（送信元セッションが設定されていないスイッチまたはスイッチ スタック）に設定します。

このスイッチ上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vlan***vlan-id*
4. **remote-span**
5. **exit**
6. **no monitor session** {*session_number* | **all** | **local** | **remote**}
7. **monitor session***session_number***sourceremote vlan***vlan-id*
8. **monitor session***session_number***destination interface***interface-id*
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan***vlan-id* 例： `Switch(config)# vlan 901`	送信元スイッチで作成された RSPAN VLAN の VLAN ID を指定し、VLAN コンフィギュレーション モードを開始します。 両方のスイッチが VTP に参加し、RSPAN VLAN ID が 2 ～ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 3 ～ 5 は不要です。

	コマンドまたはアクション	目的
ステップ 4	**remote-span** 例： `Switch(config-vlan)# remote-span`	VLAN を RSPAN VLAN として識別します。
ステップ 5	**exit** 例： `Switch(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 1`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 7	**monitor session***session_number***source remote vlan***vlan-id* 例： `Switch(config)# monitor session 1 source remote vlan 901`	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 8	**monitor session***session_number***destination interface***interface-id* 例： `Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1`	RSPAN セッションと宛先インターフェイスを指定します。 • *session_number* には、ステップ 7 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 • *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 • **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。 元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

リモート SPAN, （625 ページ）
RSPAN VLAN, （631 ページ）
RSPAN 設定時の注意事項, （635 ページ）

RSPAN 宛先セッションの作成および着信トラフィックの設定

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定し、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置等）用に着信トラフィックをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***sourceremote vlan***vlan-id*
5. **monitor session***session_number***destination**{**interface***interface-id*[**,** | **-**] [**ingress**{**dot1q vlan***vlan-id* | **isl** | **untaggedvlan***vlan-id*|**vlan***vlan-id*}]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカルセッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number***sourceremote vlan***vlan-id* 例： `Switch(config)# monitor session 2 source remote vlan 901`	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 5	**monitor session***session_number***destination** {**interface***interface-id*[**,** | **-**] [**ingress** {**dot1q vlan***vlan-id* | **isl** | **untaggedvlan***vlan-id*|**vlan***vlan-id*}]} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6`	SPAN セッション、宛先ポート、パケット カプセル化、および着信 VLAN とカプセル化を指定します。 • *session_number* には、ステップ 5 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 • *interface-id* には、宛先インターフェイスを指定します。 宛先インターフェイスは物理インターフェイスでなければなりません。

	コマンドまたはアクション	目的
		• **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。 元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。 • （任意）[**,**|**-**] は、一連のまたは一定範囲のインターフェイスを指定します。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress** を追加のキーワードと一緒に入力します。 ◦ **dot1q vlan***vlan-id*：デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを転送します。 ◦ **isl**：ISL カプセル化を使用して入力パケットを転送します。 ◦ **untagged vlan***vlan-id* または **vlan***vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを転送します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

リモート SPAN, （625 ページ）
RSPAN VLAN, （631 ページ）
RSPAN 設定時の注意事項, （635 ページ）
例：RSPAN VLAN の作成, （665 ページ）

FSPAN セッションの設定

SPAN セッションを作成し、送信元（監視対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定し、セッションに FSPAN を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***source** {**interface***interface-id*| **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** |**tx**]
5. **monitor session***session_number***destination**{**interface***interface-id* [**,** | **-**] [**encapsulation replicate**]}
6. **monitor session***session_number***filter**{**ip** | **ipv6**| **mac**} **access-group**{*access-list-number* | *name*}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカルセッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number***source** {**interface***interface-id*| **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** |**tx**] 例： `Switch(config)# monitor session 2 source interface gigabitethernet1/0/1`	SPANセッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。 有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）があります。 有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタリングする送信元 VLAN を指定します。 指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （任意）**[,** | **-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意） **[both** | **rx** | **tx]**：モニタリングするトラフィックの方向を指定します。 トラフィックの方向を指定しなかった場合、SPANは送信トラフィックと受信トラフィックの両方をモニタします。 ◦ **both**：送信トラフィックと受信トラフィックの両方をモニタします。 これはデフォルトです。 ◦ **rx**：受信トラフィックをモニタします。

	コマンドまたはアクション	目的
		◦ **tx**：送信トラフィックをモニタします。 （注） **monitor session***session_number***source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。
ステップ 5	**monitor session***session_number***destination**{**interface***interface-id* [**,** | **-**] [**encapsulation replicate**]} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate`	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • **destination** には、次のパラメータを指定します。 ◦ *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 ◦（任意）**[,** | **-]** は、一連または一定範囲のインターフェイスを指定します。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 ◦（任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 （注） ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 **monitor session***session_number***destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 6	**monitor session***session_number***filter**{**ip** | **ipv6**| **mac**} **access-group**{*access-list-number* | *name*} 例： `Switch(config)# monitor session 2 filter ipv6 access-group 4`	SPAN セッション、フィルタリングするパケットのタイプ、および FSPAN セッションで使用する ACL を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *access-list-number* には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。

	コマンドまたはアクション	目的
		• *name*には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

フローベースの SPAN, （633 ページ）
FSPAN および FRSPAN 設定時の注意事項, （636 ページ）

FRSPAN セッションの設定

RSPAN 送信元セッションを開始し、監視対象の送信元および宛先 RSPAN VLAN を指定し、セッションに FRSPAN を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session***session_number***source** {**interface***interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session***session_number***destinationremote vlan***vlan-id*
6. **vlan***vlan-id*
7. **remote-span**
8. **exit**
9. **monitor session***session_number***filter**{**ip** | **ipv6**| **mac**} **access-group**{*access-list-number* | *name*}
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session***session_number***source** {**interface***interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。

	コマンドまたはアクション	目的
	例： `Switch(config)# monitor session 2 source interface gigabitethernet1/0/1`	• *interface-id* には、モニタリングする送信元ポートを指定します。 有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel***port-channel-number*）があります。 有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、モニタリングする送信元 VLAN を指定します。 指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたはVLAN）を含めることができます。ただし、1つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （任意）**[,|-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意） **[both | rx | tx]**：モニタリングするトラフィックの方向を指定します。 トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。 • **both**：送信トラフィックと受信トラフィックの両方をモニタします。 これはデフォルトです。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。 （注） **monitor session***session_number***source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。
ステップ **5**	**monitor session***session_number***destinationremote vlan***vlan-id* 例： `Switch(config)# monitor session 2 destination remote vlan 5`	RSPAN セッションと宛先 RSPAN VLAN を指定します。 • *session_number* には、ステップ 4 で指定した番号を入力します。 • *vlan-id* には、モニタリングする宛先 RSPAN VLAN を指定します。

	コマンドまたはアクション	目的
ステップ 6	**vlan***vlan-id* 例： `Switch(config)# vlan 10`	VLAN コンフィギュレーション モードを開始します。 *vlan-id* には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 7	**remote-span** 例： `Switch(config-vlan)# remote-span`	ステップ 5 で指定した VLAN が RSPAN VLAN の一部であることを指定します。
ステップ 8	**exit** 例： `Switch(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**monitor session***session_number***filter** {**ip** | **ipv6**| **mac**} **access-group** {*access-list-number* | *name*} 例： `Switch(config)# monitor session 2 filter ip access-group 7`	RSPAN セッション、フィルタリングするパケットのタイプ、および FRSPAN セッションで使用する ACL を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *access-list-number* には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • *name* には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 10	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

フローベースの SPAN, （633 ページ）
FSPAN および FRSPAN 設定時の注意事項, （636 ページ）

SPAN および RSPAN 動作のモニタリング

次の表で、SPAN および RSPAN 動作の設定と結果を表示して動作をモニタするために使用するコマンドについて説明します。

表 *52*：*SPAN* および *RSPAN* 動作のモニタリング

コマンド	目的
show monitor	現在の SPAN、RSPAN、FSPAN、または FRSPAN 設定を表示します。

SPAN および RSPAN の設定例

例：ローカル SPAN の設定

次に、SPAN セッション 1 を設定し、宛先ポートへ向けた送信元ポートのトラフィックをモニタする例を示します。 最初に、セッション 1 の既存の SPAN 設定を削除し、カプセル化方式を維持しながら、双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 にミラーリングします。

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
Switch(config)# end
```

次に、SPAN セッション 1 の SPAN 送信元としてのポート 1 を削除する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# end
```

次に、双方向モニタが設定されていたポート 1 で、受信トラフィックのモニタをディセーブルにする例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx
```

ポート 1 で受信するトラフィックのモニタはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ～ 3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィックを宛先ポート GigabitEthernet 2 に送信する例を示します。 さらに、この設定は VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするよう変更されます。

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、送信元ポート GigabitEthernet 1 上で受信されるトラフィックをモニタするように SPAN セッション 2 を設定し、送信元ポートと同じ出力カプセル化方式を使用してそれを宛先ポート GigabitEthernet 2 に送信し、VLAN 6 をデフォルトの入力 VLAN として IEEE 802.1Q カプセル化を使用する入力転送をイネーブルにする例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 replicate ingress dot1q vlan 6
Switch(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、トランク ポート GigabitEthernet 2 で受信されたトラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先ポート GigabitEthernet 1 に送信する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1
Switch(config)# end
```

関連トピック

ローカル SPAN セッションの作成および着信トラフィックの設定, （640 ページ）
ローカル SPAN, （623 ページ）
SPAN セッション, （626 ページ）
SPAN 設定時の注意事項, （635 ページ）

例：RSPAN VLAN の作成

この例は、RSPAN VLAN 901 の作成方法を示しています。

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 901
```

```
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

次に、セッション 1 に対応する既存の RSPAN 設定を削除し、複数の送信元インターフェイスをモニタするように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1
Switch(config)# end
```

次に、RSPAN セッション 2 で送信元リモート VLAN として VLAN 901 を設定し、送信元ポート GigabitEthernet 2 を宛先インターフェイスとして設定し、VLAN 6 をデフォルトの受信 VLAN として着信トラフィックの転送をイネーブルにする例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6
Switch(config)# end
```

関連トピック

RSPAN 宛先セッションの作成および着信トラフィックの設定, （654 ページ）
リモート SPAN, （625 ページ）
RSPAN VLAN, （631 ページ）
RSPAN 設定時の注意事項, （635 ページ）

第 28 章

RMON の設定

- 機能情報の確認，667 ページ
- RMON について，667 ページ
- RMON の設定方法，669 ページ
- RMON ステータスのモニタリング，675 ページ

機能情報の確認

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

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

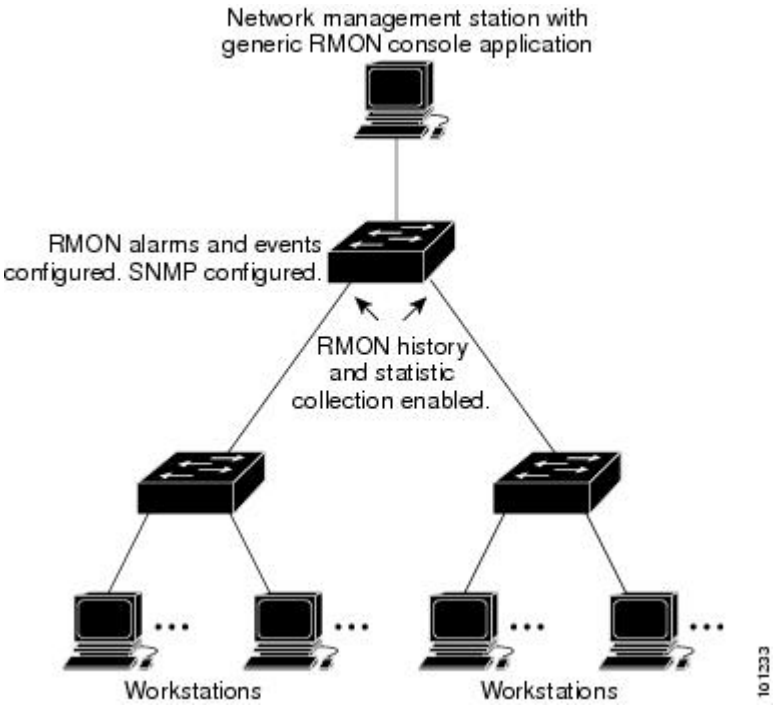
RMON について

RMON の概要

RMON とは Internet Engineering Task Force（IETF）の標準モニタリング仕様の 1 つで、RMON 準拠のコンソールシステムとネットワークプローブ間で交換可能な一連の統計情報と機能を定義します。 RMONによって、総合的なネットワーク障害診断、プランニング、パフォーマンスチューニングに関する情報が得られます。

次の図に、スイッチでの RMON 機能と Simple Network Management Protocol（SNMP）エージェントの構成例を示します。 この例では、接続されているすべての LAN セグメント上のすべてのスイッチ間のすべてのトラフィックをモニタします。

図 *52*：リモート モニタリングの例



スイッチは次の RMON グループ（RFC 1757 で規定）をサポートしています。

- 統計情報（RMON グループ 1）：インターフェイス上のイーサネットの統計情報（スイッチ タイプとサポートされているインターフェイスに応じた、ファスト イーサネットやギガビット イーサネット統計情報など）を収集します。
- 履歴（RMON グループ 2）：指定されたポーリング間隔で、イーサネット ポート上（スイッチ タイプおよびサポートされるインターフェイスに応じた、ファスト イーサネットおよびギガビット イーサネット統計情報を含む）の統計情報グループの履歴を収集します。
- アラーム（RMON グループ 3）：指定された期間、特定の管理情報ベース（MIB）オブジェクトをモニタリングし、指定された値（上限しきい値）でアラームを発生し、別の値（下限しきい値）でアラームをリセットします。 アラームはイベントと組み合わせて使用できます。アラームがイベントを発生させ、イベントによってログエントリまたはSNMP トラップが生成されるようにできます。
- イベント（RMON グループ 9）：アラームによってイベントが発生したときのアクションを指定します。 アクションは、ログ エントリまたは SNMP トラップを生成できます。

このソフトウェア リリースがサポートするスイッチは、RMON データの処理にハードウェア カウンタを使用するので、モニタが効率的になり、処理能力はほとんど必要ありません。

（注） RMON をサポートするのは、Cisco Catalyst 3560-CX スイッチのみです。

RMON をサポートするのは、IP Base ライセンスおよび IP Services ライセンスを実行する Catalyst スイッチのみです。

64 ビット カウンタは、RMON アラームではサポートされていません。

関連トピック

RMON アラームおよびイベントの設定，（669 ページ）

RMON ステータスのモニタリング，（675 ページ）

RMON の設定方法

RMON のデフォルト設定

RMONは、デフォルトではディセーブルに設定されています。アラームまたはイベントは設定されていません。

関連トピック

RMON アラームおよびイベントの設定，（669 ページ）

RMON ステータスのモニタリング，（675 ページ）

RMON アラームおよびイベントの設定

はじめる前に

スイッチを RMON 対応として設定するには、コマンドライン インターフェイス（CLI）または SNMP 準拠のネットワーク管理ステーションを使用します。

（注） 64 ビット カウンタは、RMON アラームではサポートされていません。

RMON アラームおよびイベントをイネーブルにするには、次の手順を実行します。

- ネットワーク管理ステーション（NMS）上で汎用 RMON コンソール アプリケーションを使用し、RMON のネットワーク管理機能を利用することを推奨します。
- RMON MIB オブジェクトにアクセスするために、スイッチ上で SNMP を設定することも必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **rmon alarm** {*number variable interval***absolute** | **delta** } **rising-threshold***value [event-number]***falling-threshold** *value [event-number]* [**owner***string*]
4. **rmon event***number* [**description***string*] [**log**] [**owner***string*] [**trap***community*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switchconfigure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**rmon alarm** {*number variable interval***absolute** | **delta** } **rising-threshold***value [event-number]***falling-threshold** *value [event-number]* [**owner***string*] 例： `Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner jjohnson`	MIB オブジェクトにアラームを設定します。 *number* には、アラーム番号を指定します。 指定できる範囲は 1 ～ 65535 です。 *variable* には、モニタ対象の MIB オブジェクトを指定します。 *interval* には、アラームが MIB 変数をモニタする時間を秒数で指定します。 値の範囲は 1 ～ 4294967295 秒です。 各 MIB 変数を直接テストする場合は、**absolute** キーワードを指定します。 MIB 変数のサンプル間の変動をテストする場合は、**delta** キーワードを指定します。 *value* には、アラームを発生させる値およびアラームがリセットされる値を指定します。 **rising threshold** および **falling threshold** の値の範囲は -2147483648 ～ 2147483647 です。 （任意）*event-number* には、上限および下限しきい値が限度を超えた場合に発生させるイベントの番号を指定します。 （任意）**owner***string* には、アラームの所有者を指定します。

	コマンドまたはアクション	目的
ステップ 4	**rmon event***number* [**description***string*] [**log**] [**owner***string*] [**trap***community*] 例： `Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner jjones`	RMON イベント テーブルで RMON イベント番号に関連付けられたイベントを追加します。 *number* には、イベント番号を割り当てます。 指定できる範囲は 1 ～ 65535 です。 （任意）**description***string* には、イベントの説明を指定します。 （任意）イベント発生時に RMON ログエントリを生成する場合は、**log** キーワードを使用します。 （任意）**owner***string* には、イベントの所有者を指定します。 （任意）**trap***community* には、このトラップ用の SNMP コミュニティ ストリングを入力します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

アラームをディセーブルにするには、設定した各アラームに対して、**no rmon alarm***number* グローバル コンフィギュレーション コマンドを使用します。 設定したすべてのアラームを一度にディセーブルにすることはできません。 イベントをディセーブルにするには、**no rmon event***number* グローバル コンフィギュレーション コマンドを使用します。

関連トピック

RMON の概要, （667 ページ）

RMON のデフォルト設定, （669 ページ）

RMON ステータスのモニタリング, （675 ページ）

インターフェイス上でのグループ履歴統計情報の収集

インターフェイス上でグループ履歴統計情報を収集するには、次の手順を実行します。 この手順は任意です。

はじめる前に

収集情報を表示するには、最初に RMON アラームおよびイベントを設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **rmon collection history***index* [**buckets***bucket-number*] [**interval***seconds*] [**owner***ownername*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	履歴を収集するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**rmon collection history***index* [**buckets***bucket-number*] [**interval***seconds*] [**owner***ownername*] 例：	指定したバケット数と期間での履歴収集をイネーブルにします。 *index* には、RMON 統計グループを指定します。指定できる範囲は 1 ～ 65535 です。 （任意）**buckets***bucket-number* には、RMON 統計グループ履歴収集に必要な最大バケット数を指定します。 指定できる範囲は 1 ～ 65535 です。 デフォルトのバケット数は 50 です。

	コマンドまたはアクション	目的
		（任意）**interval***seconds* には、それぞれのポーリング サイクルを秒数で指定します。 指定できる範囲は 1 ～ 3600 です。デフォルトは 1,800 秒です。 （任意）**owner***ownername* には、RMON 統計グループの所有者名を入力します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

履歴収集をディセーブルにするには、**no rmon collection history***index* インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイス上でのイーサネット グループ統計情報の収集

インターフェイス上でグループ イーサネット統計情報を収集するには、次の手順を実行します。この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **rmon collection stats***index* [**owner***ownername*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	統計情報を収集するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**rmon collection stats***index* [**owner***ownername*] 例： `Switch(config-if)# rmon collection stats 2 owner root`	インターフェイスの RMON 統計情報収集をイネーブルにします。 *index* には、RMON 統計グループを指定します。 有効な範囲は 1 ～ 65535 です。 （任意）**owner***ownername* には、RMON 統計グループの所有者名を入力します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

イーサネット統計グループの収集をディセーブルにするには、**no rmon collection stats***index* インターフェイス コンフィギュレーション コマンドを使用します。

RMON ステータスのモニタリング

表 *53*：*RMON* ステータスを表示するコマンド

コマンド	目的
show rmon	汎用RMON統計情報を表示します。
show rmon alarms	RMON アラーム テーブルを表示します。
show rmon events	RMON イベント テーブルを表示します。
show rmon history	RMON履歴テーブルを表示します。
show rmon statistics	RMON統計情報テーブルを表示します。

関連トピック

RMON アラームおよびイベントの設定，（669 ページ）

RMON の概要，（667 ページ）

RMON のデフォルト設定，（669 ページ）

第 29 章

Embedded Event Manager の設定

- Embedded Event Manager について，677 ページ
- Embedded Event Manager の設定方法，680 ページ
- Embedded Event Manager のモニタリング，683 ページ
- Embedded Event Manager の設定例，684 ページ

Embedded Event Manager について

Embedded Event Manager の概要

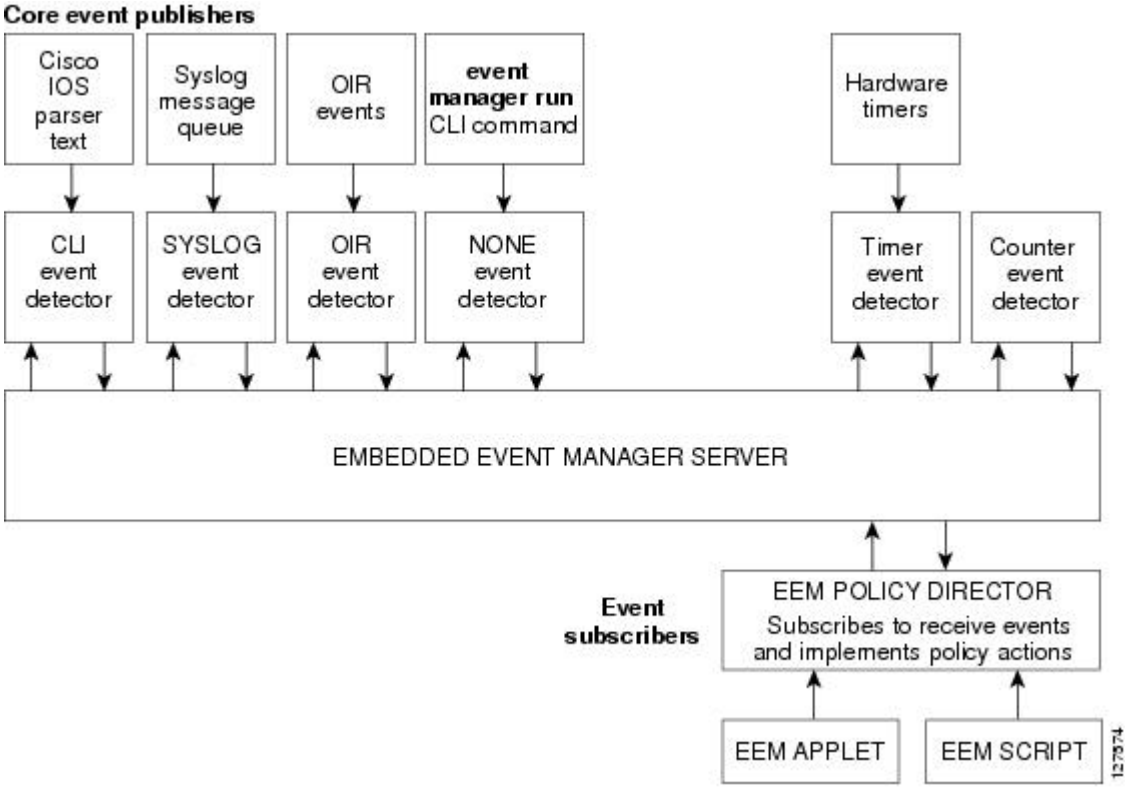
Embedded Event Manager（EEM）は、Cisco IOS デバイス内でイベント検出および回復のために配布されカスタマイズされたアプローチです。 EEM はイベントを監視する機能を提供します。また、監視されたイベントが発生するかしきい値に達した場合に情報を得たり、是正措置を行ったり、または他の EEM 処理を実行したりする機能も提供します。 EEM ポリシーは、イベントおよびイベントが発生した場合に行う処理を定義します。

EEM はキー システムのイベントを監視し、セット ポリシーを通してイベントに作用します。 このポリシーはプログラムされたスクリプトで、これを使用して、発生した特定の一連のイベントに基づいて処理を呼び出すように、スクリプトをカスタマイズできます。 このスクリプトは、カスタム Syslog または簡易ネットワーク管理プロトコル（SNMP）トラップの生成、CLI（コマンドライン インターフェイス）コマンドの呼び出し、フェールオーバーの強制などの処理を生成します。 スイッチからすべてのイベント管理を管理できるわけではなく、何らかの問題によって、スイッチと外部ネットワーク管理デバイス間の通信に障害が発生することがあるため、EEM のイベント管理機能は役立ちます。 スイッチをリブートすることなく自動回復処理が行われる場合、ネットワークのアベイラビリティは向上します。

次に、EEM サーバ、コア イベント パブリッシャ（イベント検出器）、およびイベント サブスクライバ（ポリシー）の関係の例を示します。 イベントパブリッシャはイベントを選別し、イベント サブスクライバによって提供されたイベント仕様と一致するイベントがいつ発生するかを決定します。 イベントが発生すると、イベント検出器が EEM サーバに通知します。 次に、システム

の現在の状態と特定のイベントに対してポリシーで指定された処理に基づいて、EEMポリシーが回復を実行します。

図 *53*：*Embedded Event Manager* コア イベント検出器



（注） EEM をサポートするのは、Cisco Catalyst 3560-CX スイッチのみです。

EEM をサポートするのは、IP Base ライセンスおよび IP Services ライセンスを実行する Catalyst スイッチのみです。

Embedded Event Manager のアクション

イベントに応答して次の処理が発生します。

- 名前付きカウンタの修正。
- アプリケーション特有のイベントのパブリッシュ。
- SNMP トラップの生成。
- 優先化された syslog メッセージの生成。
- Cisco IOS ソフトウェアのリロード。

- スイッチ スタックのリロード。
- マスター切り替え時のマスター スイッチのリロード。 この場合、新しいマスター スイッチが選択されます。

Embedded Event Manager ポリシー

EEMはイベントを監視して情報を提供するか、または監視されたイベントが発生するかしきい値に達した場合に是正措置を行うことができます。 EEMポリシーは、イベントおよびイベントが発生した場合に行う処理を定義するエンティティです。

EEM ポリシーにはアプレットとスクリプトの 2 つのタイプがあります。 アプレットは、CLI 設定内で定義される簡易なポリシーです。 イベントの選別基準とイベントが発生した場合に行う処理を定義する簡易な方法です。 スクリプトは、ASCII エディタを使用して、ネットワーキング デバイス上で定義されます。 スクリプト（バイトコード（.tbc）とテキスト（.tcl）スクリプトで作成できます）は、次に、ネットワーキング デバイスにコピーされ、EEM によって登録されます。 さらに、1 つの .tcl ファイルに複数のイベントを登録できます。

EEM を使用して、EEM ポリシー ツール コマンド言語（TCL）スクリプトを使用する独自のポリシーを記述して実行します。 マスター スイッチで TCL スクリプトを設定すると、ファイルはメンバー スイッチに自動的に送信されます。 マスター スイッチが変わった場合に TCL スクリプト ポリシーが機能し続けるように、メンバースイッチでユーザ定義のTCLスクリプトが使用できる必要があります。

キーワード拡張という形のシスコの TCL 機能拡張は、EEM ポリシーの開発を容易にします。 これらのキーワードは、検出されたイベント、その後の処理、ユーティリティ情報、カウンタ値、およびシステム情報を識別します。

関連トピック

Embedded Event Manager アプレットの登録と定義, （680 ページ）
例：SNMP 通知の生成, （684 ページ）
例：EEM イベントへの応答, （684 ページ）

Embedded Event Manager の環境変数

EEM は EEM ポリシーで環境変数を使用します。 この環境変数は、CLI コマンドおよび **event manager environment** コマンドを実行して、EEM ポリシー Tool Command Language（TCL）スクリプトで定義します。

- ユーザ定義の変数：ユーザ定義のポリシーに対して、ユーザにより定義されます。
- シスコ定義の変数：特定のサンプル ポリシーに対してシスコにより定義されます。
- シスコ組み込み変数（EEMアプレットで利用可能）：シスコにより定義され、読み取り専用または読み取りと書き込みに設定できます。 読み取り専用変数は、アプレットが実行を開始する前に、システムによって設定されます。 1 つの読み取りと書き込み変数 *_exit_status* により、同期イベントからトリガーされるポリシーの終了ステータスを設定できます。

シスコ定義の環境変数とシスコ システム定義の環境変数は、特定の 1 つのイベント ディテクタまたはすべてのイベント ディテクタに適用されます。 ユーザ定義の環境変数またはサンプル ポリシーでシスコにより定義される環境変数は、event manager environment グローバル コンフィギュレーション コマンドを使用して設定されます。 ポリシーを登録する前に、変数を EEM ポリシーに定義する必要があります。

Embedded Event Manager 3.2

Embedded Event Manager 3.2 では次のイベント ディテクタがサポートされています。

- ネイバー探索：ネイバー探索イベント検出器によって、次の場合に自動ネイバー検出に応答するポリシーをパブリッシュできます。
  - Cisco Discovery Protocol（CDP）のキャッシュ エントリが追加、削除、または更新された場合。
  - リンク層検出プロトコル（LLDP）キャッシュ エントリが追加、削除、または更新された場合。
  - インターフェイスのリンク ステータスが変更された場合。
  - インターフェイスのライン ステータスが変更された場合。
- ID：ID イベント検出器は、AAA の許可および認証が成功した場合、障害が発生した場合、またはポート上で通常のユーザ トラフィックの送信が許可された後にイベントを生成します。
- Mac-Address-Table：Mac-Address-Table イベント検出器は、MAC アドレスが MAC アドレス テーブルで学習された場合にイベントを生成します。

（注） Mac-Address-Table イベント検出器は、スイッチ プラットフォームでだけサポートされており、MAC アドレスが学習されたレイヤ 2 インターフェイスだけで使用できます。 レイヤ 3 インターフェイスはアドレスを学習せず、ルータは通常、学習された MAC アドレスを EFM に通知するために必要な MAC アドレス テーブル インフラストラクチャをサポートしません。

EEM 3.2 では、新しいイベント検出器で動作するアプレットをサポートするための CLI コマンドも導入されています。

Embedded Event Manager の設定方法

Embedded Event Manager アプレットの登録と定義

EEM にアプレットを登録し、**event applet** および **action applet** コンフィギュレーション コマンドを使用して EEM アプレットを定義するには、特権 EXEC モードで次の手順を実行します。

（注） EEM アプレットでは、1 つのイベント アプレット コマンドしか使用できません。 複数の処理アプレット コマンドが使用できます。 **no event** および **no action** コマンドを指定しない場合、コンフィギュレーション モードを終了すると、アプレットは削除されます。

手順の概要

1. **configure terminal**
2. **event manager applet***applet-name*
3. **event snmp oid***oid-value***get-type** {**exact**|**next**} **entry-op** { **eq**|**ge**|**gt**|**le**|**lt**|**ne**} **entry-val***entry-val* [**exit-comb** {**or**|**and**}] [**exit-op**{**eq**|**ge**|**gt**|**le**|**lt**|**nc**}] [**exit-val***exit-val*] [**exit-time***exit-time-val*] **poll interval***poll-int-val*
4. **action label syslog** [**priority***priority-level*] **msg***msg-text*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**event manager applet***applet-name*	EEM でアプレットを登録し、アプレット コンフィギュレーション モードを開始します。
ステップ 3	**event snmp oid***oid-value***get-type** {**exact**|**next**} **entry-op** { **eq**|**ge**|**gt**|**le**|**lt**|**ne**} **entry-val***entry-val* [**exit-comb** {**or**|**and**}] [**exit-op**{**eq**|**ge**|**gt**|**le**|**lt**|**nc**}] [**exit-val***exit-val*] [**exit-time***exit-time-val*] **poll interval***poll-int-val*	EEM アプレットを実行する要因となるイベント基準を指定します。 （任意）終了基準。 終了基準を指定しない場合、イベント モニタリングがすぐに再イネーブル化されます。
ステップ 4	**action label syslog** [**priority***priority-level*] **msg***msg-text*	EEM アプレットがトリガーされたときの処理を指定します。この処理を繰り返して、アプレットに他の CLI コマンドを追加します。 • （任意）プライオリティ キーワードは、Syslog メッセージのプライオリティ レベルを指定します。 選択した場合、プライオリティ レベル引数を定義する必要があります。 • *msg-text* の場合、引数は文字テキスト、環境変数、またはこの 2 つを組み合わせたものになります。
ステップ 5	**end**	アプレット コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次に、SNMP オブジェクト ID によって指定されたフィールドの 1 つが、定義されたしきい値を超えた場合の EEM での出力例を示します。

```
Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
 lt entry-val 5120000 poll-interval 10
```

次に、EEM イベントに応答して行われる処理の例を示します。

```
Switch(config-applet)# action 1.0 syslog priority critical msg "Memory exhausted; current
available memory is $_snmp_oid_val bytes"
Switch (config-applet)# action 2.0 force-switchover
```

関連トピック

Embedded Event Manager ポリシー, （679 ページ）
例：SNMP 通知の生成, （684 ページ）
例：EEM イベントへの応答, （684 ページ）

Embedded Event Manager TCL スクリプトの登録と定義

EEM で TCL スクリプトを登録し、TCL スクリプトとポリシー コマンドを定義するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **show event manager environment** [**all** | *variable-name*]
3. **configure terminal**
4. **event manager environment variable-name string**
5. **event manager policy policy-file-name** [**type system**] [**trap**]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**show event manager environment** [**all** | *variable-name*]	（任意）**show event manager environment** コマンドは、EEM 環境変数の名前と値を表示します。 （任意）**all** キーワードは、EEM 環境変数を表示します。 （任意）*variable-name* 引数は、指定された環境変数に関する情報を表示します。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**event manager environment variable-name string**	指定された EEM 環境変数の値を設定します。 要求されたすべての環境変数でこのステップを繰り返します。
ステップ 5	**event manager policy policy-file-name** [**type system**] [**trap**]	ポリシー内で定義された指定イベントが発生した場合に、EEM ポリシーを実行するよう、定義します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次に、show event manager environment コマンドの出力例を示します。

```
Switch# show event manager environment all
No.   Name                Value
1     _cron_entry         0-59/2 0-23/1 * * 0-6
2     _show_cmd           show ver
3     _syslog_pattern     .*UPDOWN.*Ethernet1/0.*
```

次に、ソフトウェアによって割り当てられた CRON タイマー環境変数を毎日の毎時間、毎分、毎秒に設定する方法を示します。

```
Switch (config)# event manager environment_cron_entry 0-59/2 0-23/1 * * 0-6
```

次に、システム ポリシーとして登録された tm_cli_cmd.tcl という名前の EEM ポリシーの例を示します。 システム ポリシーは Cisco IOS イメージの一部です。 ユーザ定義の TCL スクリプトは、最初にフラッシュ メモリにコピーする必要があります。

```
Switch (config)# event manager policy tm_cli_cmd.tcl type system
```

関連トピック

例：EEM 環境変数の表示, （684 ページ）

Embedded Event Manager のモニタリング

Embedded Event Manager 情報の表示

表 *54*：*EEM* 情報を表示するためのコマンド

コマンド	目的
show event manager environment[**all**| *variable-name*]	すべての EEM 環境変数の名前および値を表示します。

EEM 登録済みポリシーや EEM 履歴データなど、EEM に関する情報の表示については、『Cisco IOS Network Management Command Reference』を参照してください。

Embedded Event Manager の設定例

例：SNMP 通知の生成

次に、SNMP オブジェクト ID によって指定されたフィールドの 1 つが定義されたしきい値を超えた場合の EEM での出力例を示します。

```
Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
 lt entry-val 5120000 poll-interval 10
```

関連トピック

Embedded Event Manager ポリシー, （679 ページ）
Embedded Event Manager アプレットの登録と定義, （680 ページ）

例：EEM イベントへの応答

次に、EEM イベントに応答して行われる処理の例を示します。

```
Switch(config-applet)# action 1.0 syslog priority critical msg "Memory exhausted; current
available memory is $_snmp_oid_val bytes"
Switch(config-applet)# action 2.0 force-switchover
```

関連トピック

Embedded Event Manager ポリシー, （679 ページ）
Embedded Event Manager アプレットの登録と定義, （680 ページ）

例：EEM 環境変数の表示

次に、show event manager environment コマンドの出力例を示します。

```
Switch# show event manager environment all
No.   Name                    Value
1     _cron_entry             0-59/2 0-23/1 * * 0-6
2     _show_cmd               show ver
3     _syslog_pattern         .*UPDOWN.*Ethernet1/0.*
4     _config_cmd1 interface  Ethernet1/0
5     _config_cmd2            no shut
```

次に、ソフトウェアによって割り当てられた CRON タイマー環境変数を毎日の毎時間、毎分、毎秒に設定する方法を示します。

```
Switch(config)# event manager environment_cron_entry 0-59/2 0-23/1 * * 0-6
```

次に、システム ポリシーとして登録された tm_cli_cmd.tcl という名前の EEM ポリシーの例を示します。 システム ポリシーは Cisco IOS イメージの一部です。 ユーザ定義の TCL スクリプトは、最初にフラッシュ メモリにコピーする必要があります。

```
Switch(config)# event manager policy tm_cli_cmd.tcl type system
```

関連トピック

Embedded Event Manager TCL スクリプトの登録と定義, （682 ページ）

第 30 章

NetFlow Lite の設定

- 機能情報の確認，685 ページ
- NetFlow Lite の前提条件，685 ページ
- NetFlow Lite の制約事項，686 ページ
- NetFlow Lite について，687 ページ
- NetFlow Lite の設定方法，697 ページ
- Flexible NetFlow のモニタリング，711 ページ
- NetFlow Lite の設定例，712 ページ

機能情報の確認

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

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

NetFlow Lite の前提条件

NetFlow Lite を接続するために、次の 2 つのターゲットがサポートされています。

- ポート：EtherChannel などの論理インターフェイスではなく、物理インターフェイスのみでサポートされるモニタ接続。 物理インターフェイスは、ルーテッド ポートまたはスイッチド ポートです。

- VLAN：モニタ接続は、レイヤ2 VLANではなく、VLANインターフェイス（SVI）のみでサポートされます。

NetFlow Lite の制約事項

次に、NetFlow Lite の制約事項を示します。

- フロー レコードの制約事項：

  フロー モニタで **collect interface output** がフロー レコードの collect フィールドとして指定されている場合、以下のいずれかのアドレスのフローが作成されると、このフィールドは**NULL**の値を返します。

  - L3 ブロードキャスト
  - L2 ブロードキャスト
  - L3 マルチキャスト
  - L2 マルチキャスト
  - L2 の不明な宛先。

- モニタの制約事項：

  - モニタ接続は、入力方向に限りサポートされます。
  - エクスポータはインターフェイスごとに複数サポートされますが、モニタはインターフェイスごとに 1 つサポートされます。
  - モニタでは永続キャッシュと標準キャッシュのみサポートされます。即時キャッシュはサポートされません。
  - モニタ パラメータがインターフェイスまたは VLAN に適用される場合は、それらのモニタ パラメータは変更できません。
  - ポートおよび VLAN の両方がモニタに接続されている場合、ポートに着信するトラフィックについて VLAN モニタはポート モニタを上書きします。
  - フロー モニタ タイプとトラフィック タイプ（タイプとは、IPv4、IPv6、およびデータリンクを意味します）は、作成するフローで同じである必要があります。
  - スイッチ では、インターフェイスに IP およびポート ベースのモニタを同時に接続できません。 48 ポートのスイッチは最大 48 台のモニタ（IP またはポート ベース）をサポートし、256 SVI は最大 256 台のモニタ（IP またはポート ベース）を設定できます。
  - **show flow monitor***flow_name***cache** コマンドを実行すると、スイッチはそれ以前のスイッチ ソフトウェア バージョン（Catalyst 2960-S）からのキャッシュ情報を、すべてのフィールドにゼロが入力された状態で表示します。 これらのフィールドはスイッチに適用できないため、無視します。

- サンプラーの制限事項：

- サンプリングされた NetFlow のみがサポートされます。
- ポートと VLAN の両方について、スイッチでは合計 4 つのサンプラー（ランダムまたは確定）がサポートされます。
- 両方のモードのサンプリング最小レートは、32 個のフローの中から 1 つで、両方のモードのサンプリング最大レートは 1022 個のフローから 1 つです。
- サンプラーをインターフェイスに接続している間、サンプラーをモニタと関連付けておく必要があります。 これを行わないと、コマンドは拒否されます。 このタスクを実行するには、**ip flow monitor***monitor_name* sampler s*ampler_name***input** インターフェイス コンフィギュレーション コマンドを使用します。
- 確定サンプラーを使用してモニタを接続する場合は、同じサンプラーを使用するすべての接続で、4 個の使用可能なサンプラーの中から 1 つの新しいフリー サンプラーをスイッチ（ハードウェア）から使用します。 サンプラーによるモニタの接続は4つまで許容されます。

  ランダム サンプラーを使用してモニタを接続する場合は、最初の接続のみがスイッチ（ハードウェア）からの新しいサンプラーを使用します。 同じサンプラーを使用する残りのすべての接続は、同じサンプラーを共有します。

  この動作のため、確定サンプラーを使用する場合は、サンプリング レートとスイッチが送信した内容を比較することによって、サンプリングされたフローの正確な数を確認できます。 同じランダム サンプラーを複数のインターフェイスで使用する場合は、任意のインターフェイスからのフローを常にサンプリングし、他のインターフェイスからのフローは常にスキップすることができます。

- ネットワーク フローおよび統計情報はライン レートで収集されます。
- ACL ベースの NetFlow はサポートされていません。
- NetFlow バージョン 9 のみが *export-protocol* コマンド オプションを使用した Flexible NetFlow エクスポータでサポートされます。 NetFlow バージョン 5 を設定した場合、このバージョンは受け入れられますが、現在、NetFlow バージョン 5 のエクスポート機能は利用できず、サポートもされていません。
- スイッチは同種スタック構成をサポートしますが、混合スタック構成はサポートしません。

NetFlow Lite について

NetFlow Lite の概要

NetFlow Lite ではフローを使用して、アカウンティング、ネットワーク モニタリング、およびネットワーク プランニングに関連する統計情報を提供します。

フローは送信元インターフェイスに届く単方向のパケット ストリームで、キーの値は同じです。キーは、パケット内のフィールドを識別する値です。 フローを作成するには、フロー レコードを使用して、フロー固有のキーを定義します。

スイッチは、ネットワーク異常とセキュリティ問題の高度な検出をイネーブルにする NetFlow Lite 機能をサポートします。 NetFlow Lite により、大量の定義済みフィールドの集合からキーを選択して、特定のアプリケーションに最適なフロー レコードを定義できます。

1 つのフローと見なされるパケットでは、すべてのキー値が一致している必要があります。 フローは、設定したエクスポートレコードバージョンに基づいて、関係のある他のフィールドを集めることもあります。 フローはNetFlow Lite キャッシュに格納されます。

エクスポータを使用してNetFlow Liteがフローのために収集するデータをエクスポートし、NetFlow Lite コレクタなどのリモート システムにこのデータをエクスポートできます。 NetFlow Lite コレクタは、IPv4 アドレスを使用できます。

モニタを使用してフローのために収集するデータのサイズを定義します。 モニタで、フロー レコードおよびエクスポータを NetFlow Lite キャッシュ情報と結合します。

Flexible NetFlow のコンポーネント

Flexible NetFlow は、いくつかのバリエーションで一緒に使用して、トラフィック分析およびデータ エクスポートに使用できるコンポーネントで構成されます。 Flexible NetFlow のユーザ定義のフロー レコードおよびコンポーネントの構造では、最小限の数のコンフィギュレーション コマンドで、ネットワーキングデバイスでのトラフィック分析およびデータエクスポートのためのさまざまなコンフィギュレーションの作成が容易になります。 各フローモニタに、フロー レコード、フロー エクスポータ、およびキャッシュ タイプの固有の組み合わせを設定できます。 フロー エクスポータの宛先IPアドレスなどのパラメータを変更する場合、フローエクスポータを使用するすべてのフロー モニタに対して自動的に変更されます。 同じフロー モニタを複数のフロー サンプラと組み合わると、さまざまなインターフェイス上でさまざな速度の同じタイプのネットワーク トラフィックをサンプリングできます。 ここでは、Flexible NetFlow コンポーネントのその他の情報を提供します。

フロー レコード

Flexible NetFlow では、キー フィールドと非キー フィールドの組み合わせをレコードと呼びます。 Flexible NetFlow のレコードは Flexible NetFlow フロー モニタに割り当てられ、フロー データの格納に使用されるキャッシュが定義されます。

フロー レコードでは、フロー内のパケットを識別するために Flexible NetFlow で使用するキーとともに、Flexible NetFlow がフローについて収集する他の関連 フィールドを定義します。 キーと関連フィールドを任意の組み合わせで指定して、フロー レコードを定義できます。 スイッチは、幅広いキー セットをサポートします。 フロー レコードでは、フロー単位で収集するカウンタのタイプも定義します。 64 ビットのパケットまたはバイト カウンタを設定できます。 スイッチは、フロー レコードの作成時に、デフォルトとして次の match フィールドをイネーブルにします。

- match datalink：レイヤ 2 属性
- match ipv4：IPv4 属性
- match ipv6：IPv6 属性
- match transport：トランスポート層フィールド

- match wireless：ワイヤレス フィールド

関連トピック

フロー レコードの作成，（697 ページ）

例：フローの設定，（712 ページ）

NetFlow の事前定義済みのレコード

Flexible NetFlow には事前定義済みのレコードがいくつか含まれ、それを使用してネットワーク トラフィックの監視を開始できます。 事前定義済みのレコードは、Flexible NetFlow を迅速に導入するために役立ち、ユーザ定義のフロー レコードよりも簡単に使用できます。 ネットワーク モニタリングのニーズを満たす定義済みのレコードのリストから選択できます。 Flexible NetFlow が改良されると、一般的なユーザ定義のフロー レコードを事前定義済みレコードとして使用でき、簡単に導入できるようになります。

事前定義済みレコードにより、エクスポートされるデータのために既存の NetFlow コレクタ コンフィギュレーションとの下位互換性が確保されます。 事前定義済みレコードは、それぞれ固有の key および nonkey フィールドの組み合わせを持ち、ルータで Flexible NetFlow をカスタマイズしなくても、ネットワーク内のさまざまなタイプのトラフィックを監視する、内蔵機能を提供します。

2 つの事前定義済みレコード（NetFlow original と NetFlow IPv4/IPv6 original output）は機能的に同等で、以前の（入力）NetFlow、および以前の NetFlow の 出力 NetFlow アカウンティング機能をそれぞれエミュレートします。 その他の Flexible NetFlow の事前定義済みレコードのいくつかは、以前の NetFlow で利用できる集約キャッシュ方式に基づきます。 以前の NetFlow で利用できる集約キャッシュ方式に基づく Flexible NetFlow の事前定義済みレコードでは、集約を実行しません。 代わりに、事前定義済みレコードによって各フローが個別に追跡されます。

ユーザ定義レコード

Flexible NetFlow では、key および nonkey フィールドを指定し、実際の要件に合わせてデータ収集をカスタマイズすることで、Flexible NetFlow フロー モニタ キャッシュ用の独自のレコードを定義できます。 Flexible NetFlow フロー モニタ キャッシュに対して独自のレコードを定義する場合、ユーザ定義レコードと呼ばれます。 nonkey フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。 nonkey フィールドの値の変更によって新しいフローが作成されることはありません。 ほとんどの場合、nonkey フィールドの値はフロー内の最初のパケットからのみ取得されます。 Flexible NetFlow を使用すると、nonkey フィールドとして、フロー内のバイト数やパケット数などのカウンター値をキャプチャできます。

Flexible NetFlow では、ヘッダーおよびパケット セクションのタイプに新しいバージョン 9 エクスポート フォーマット フィールド タイプが追加されます。 Flexible NetFlow は NetFlow コレクタに、対応するバージョン 9 エクスポート テンプレート フィールドで設定されたセクション サイズを通知します。 ペイロードセクションには、対応する長さフィールドがあり、収集されるセクションの実際のサイズを収集するために使用できます。

*NetFlow Lite*の *match* パラメータ

フロー レコードの次のキー フィールドを照合できます。

- IPv4 または IPv6 宛先アドレス

- Datalink フィールド（送信元および宛先 MAC アドレス、ならびに MAC EtherType（ネットワーク プロトコルのタイプ））。
- アプリケーションのタイプ（ICMP、IGMP、または TCP トラフィック）を識別するトランスポート フィールドの送信元および宛先ポート。

次の表で、NetFlow Lite の match パラメータについて説明します。 フロー レコードごとに、次の match パラメータを 1 つ以上設定する必要があります。

表 *55*：*match* パラメータ

コマンド	目的
match datalink {**ethertype** | **mac** {**destinationaddressinput** | **sourceaddressinput**}}	データ リンクまたはレイヤ2フィールドとの一致を指定します。 次のコマンド オプションが使用可能です。 • **ethertype**：パケットの ethertype と一致します。 • **mac**：入力時のパケットの送信元または宛先 MAC アドレスと一致します。 （注） データリンク フロー モニタがインターフェイスまたは VLAN に割り当てられている場合、非 IPv6 または非 IPv4 トラフィック用のフローだけが作成されます。
match ipv4{**destination** {**address**} | **protocol** | **source** {**address**} | **tos**}	IPv4 フィールドとの一致を指定します。 次のコマンド オプションが使用可能です。 • **destination**：IPv4 宛先アドレス ベースのフィールドと一致します。 • **protocol**：IPv4 プロトコルと一致します。 • **source**：IPv4 送信元アドレス ベースのフィールドと一致します。 • **tos**：IPv4 タイプ オブ サービス フィールドと一致します。

コマンド	目的
match ipv6 {**destination** {**address**} | **flow-label** | **protocol** | **source** {**address**} | **traffic-class**}	IPv6 フィールドとの一致を指定します。 次のコマンド オプションが使用可能です。 • **destination**：IPv6 宛先アドレス ベースのフィールドと一致します。 • **flow-label**：IPv6 フローラベル フィールドと一致します。 • **protocol**：IPv6 ペイロード プロトコル フィールドと一致します。 • **source**：IPv6 送信元アドレス ベースのフィールドと一致します。 • **traffic-class**：IPv6 トラフィック クラスと一致します。
match transport {**destination-port** | **source-port**}	トランスポート層フィールドとの一致を指定します。 次のコマンド オプションが使用可能です。 • **destination-port**：転送先ポートと一致します。 • **source-port**：転送元ポートと一致します。
	フロー レコードのキー フィールドとして SSID のワイヤレス ネットワークの使用を指定します。

NetFlow Lite の collect パラメータ

フロー レコードの次のキー フィールドを収集できます。

- 合計バイト数、エクスポータによって送信されるまたはフローまたはパケット（exporter）、または 64 ビット カウンタのバイト数またはパケット数（long）。
- 最初のパケットの送信時間または最新（最後）のパケットが見つかった時間からのシステム稼働時間に基づくタイムスタンプ。
- 入力インターフェイスの SNMP インデックス。 サービス モジュールに着信するトラフィックのインターフェイスは、スイッチの転送キャッシュに基づいています。 このフィールドは、一般にデータ リンク、IPv4 および IPv6 アドレスとともに使用され、直接接続されたホストの実際のファースト ホップのインターフェイスを提供します。
  - 値 0 は、インターフェイス情報がキャッシュにないことを意味します。

- 一部の NetFlow コレクタでは、フロー レコードにこの情報が必要です。

次の表で、NetFlow Lite の collect パラメータについて説明します。

表 56：***collect* パラメータ**

コマンド	目的
collect counter {**bytes** {**long** | **permanent** } | **packets** { **long** | **permanent**}}	カウンタ フィールドの合計バイト数と合計パケット数を収集します。
collect flow {**sampler**}	フローサンプラー識別子（ID）を収集します。
collect interface {**input**}	入力インターフェイスからフィールドを収集します。
collect timestamp sys-uptime {**first** | **last**}	最初のパケットが確認された時刻、または最新のパケットが最後に確認された時刻のフィールドを収集します（ミリ秒）。
collect transport tcp flags	次の転送 TCP フラグを収集します。 • **ack**：TCP 確認応答フラグ • **cwr**：TCP 輻輳ウィンドウ縮小フラグ • **ece**：TCP ECN エコー フラグ • **fin**：TCP 終了フラグ • **psh**：TCP プッシュ フラグ • **rst**：TCP リセット フラグ • **syn**：TCP 同期フラグ • **urg**：TCP 緊急フラグ
	ワイヤレスクライアントが関連付けられているアクセス ポイントの MAC アドレスを収集します。

フロー エクスポータ

フローエクスポータでは、フローモニタ キャッシュ内のデータをリモートシステム（たとえば、分析および保管のために NetFlow コレクタを実行するサーバ）にエクスポートします。 フローエクスポータは、コンフィギュレーションで別のエンティティとして作成されます。フローエクスポータは、フロー モニタにデータ エクスポート機能を提供するためにフロー モニタに割り当て

られます。 複数のフロー エクスポータを作成して、1 つまたは複数のフロー モニタに適用すると、いくつかのエクスポート先を指定することができます。 1 つのフロー エクスポータを作成し、いくつかのフロー モニタに適用することができます。

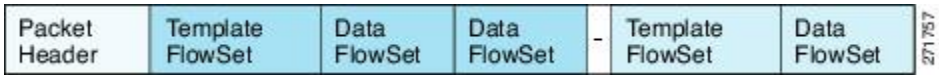
NetFlow データ エクスポート フォーマットのバージョン 9

NetFlow の基本出力はフロー レコードです。 NetFlow が改良され、フロー レコードのいくつかのフォーマットが向上しました。 NetFlow エクスポート フォーマットの最新の進化は、バージョン 9 と呼ばれます。 NetFlow Version 9 エクスポート フォーマットの識別機能は、テンプレートがベースとなります。 テンプレートは、レコード フォーマットの設計を拡張可能なものにします。 NetFlow サービスが将来拡張されても、基本フロー レコード フォーマットを変更し続ける必要がありません。 テンプレートを使用すると、次のいくつかの利点があります。

- NetFlow のコレクタを提供したり、サービスを表示したりするアプリケーションを作成するサードパーティ ビジネスパートナーは、新規の NetFlow 機能が追加されるたびにアプリケーションを再コンパイルする必要はありません。 代わりに、既知のテンプレート フォーマットを記述する外部のデータ ファイルを使用することができます。
- 新規機能は、現在の導入環境を損ねることなく、NetFlow に迅速に追加できます。
- バージョン 9 フォーマットは新しいプロトコルや開発中のプロトコルに適応できるため、NetFlow はこれらのプロトコルに対して「将来的に対応」します。

バージョン 9 のエクスポート フォーマットは、パケット ヘッダーとそれに続く 1 つ以上のテンプレート フロー セットまたはデータ フロー セットで構成されています。 テンプレート フロー セットでは、将来のデータ フロー セットに表示されるフィールドの説明が提供されます。 このようなデータ フロー セットは、後で同じエクスポート パケットまたは後続のエクスポート パケットで発生する可能性があります。 テンプレート フロー セットおよびデータ フロー セットは、次の図に示すように、単一のエクスポート パケットに混在させることができます。

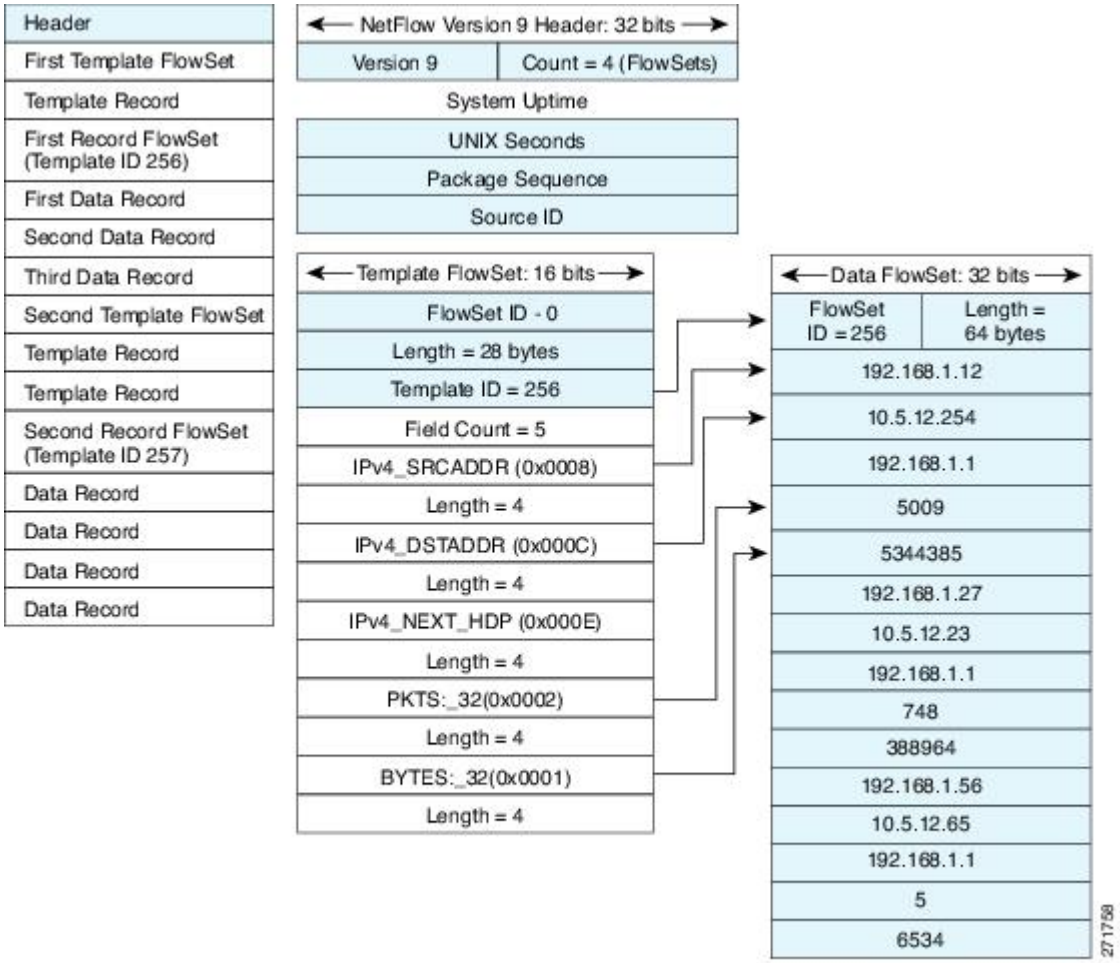
図 *54* : バージョン *9* エクスポート パケット



NetFlow Version 9 では、送信されるデータを NetFlow コレクタが理解できるように、テンプレート データを定期的にエクスポートします。また、テンプレートのデータ フロー セットもエクスポートします。 Flexible NetFlow の主な利点は、ユーザがフロー レコードを設定すると、バージョン 9 テンプレートに効率的に変換され、コレクタに転送されることです。 下の図に、ヘッダー、

テンプレート フロー セットおよびデータ フロー セットを含めて、NetFlow Version 9 エクスポート フォーマットの詳細な例を示します。

図 *55*：*NetFlow* バージョン *9* エクスポート フォーマットの詳細例



バージョン9エクスポート フォーマットの詳細については、ホワイト ペーパー『Cisco IOS NetFlow Version 9 Flow-Record Format』を参照してください。次の URL から入手できます。http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml

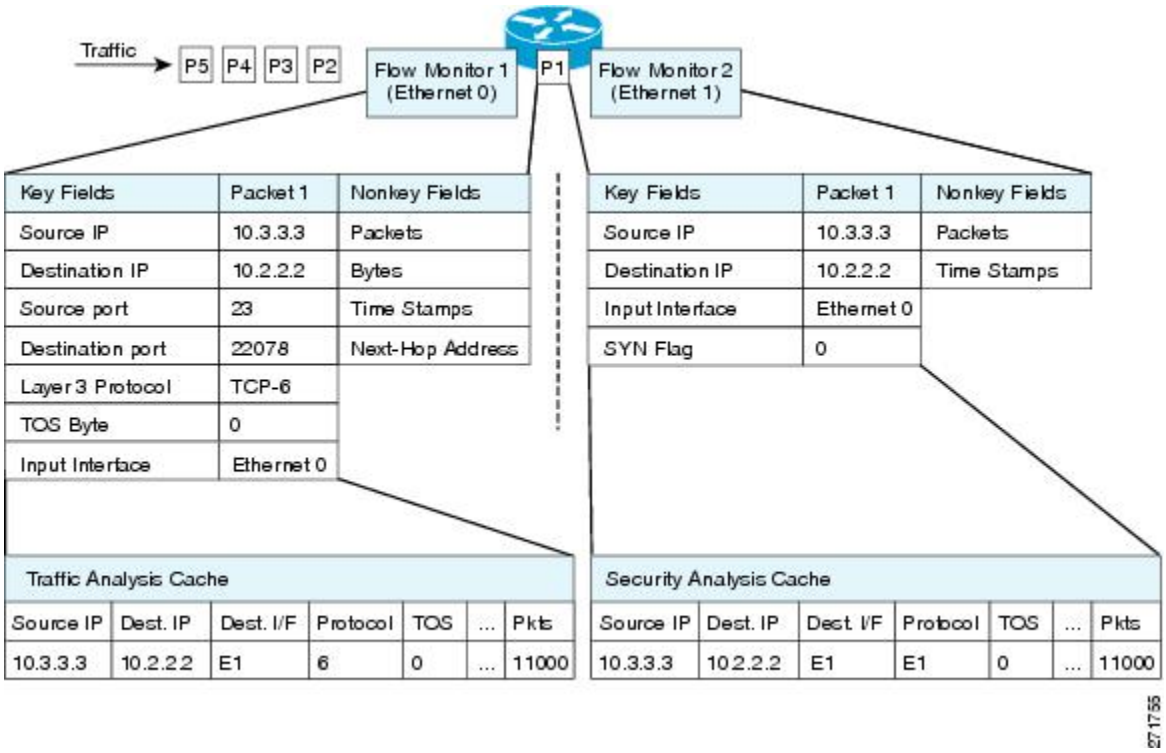
フロー モニタ

フロー モニタは Flexible NetFlow のネットワーク トラフィックの監視を実行するコンポーネントで、インターフェイスに適用されます。

フローデータはネットワーク トラフィックから収集され、フロー レコードの key フィールドおよび nonkey フィールドに基づいて監視プロセス中にフロー モニタ キャッシュに追加されます。

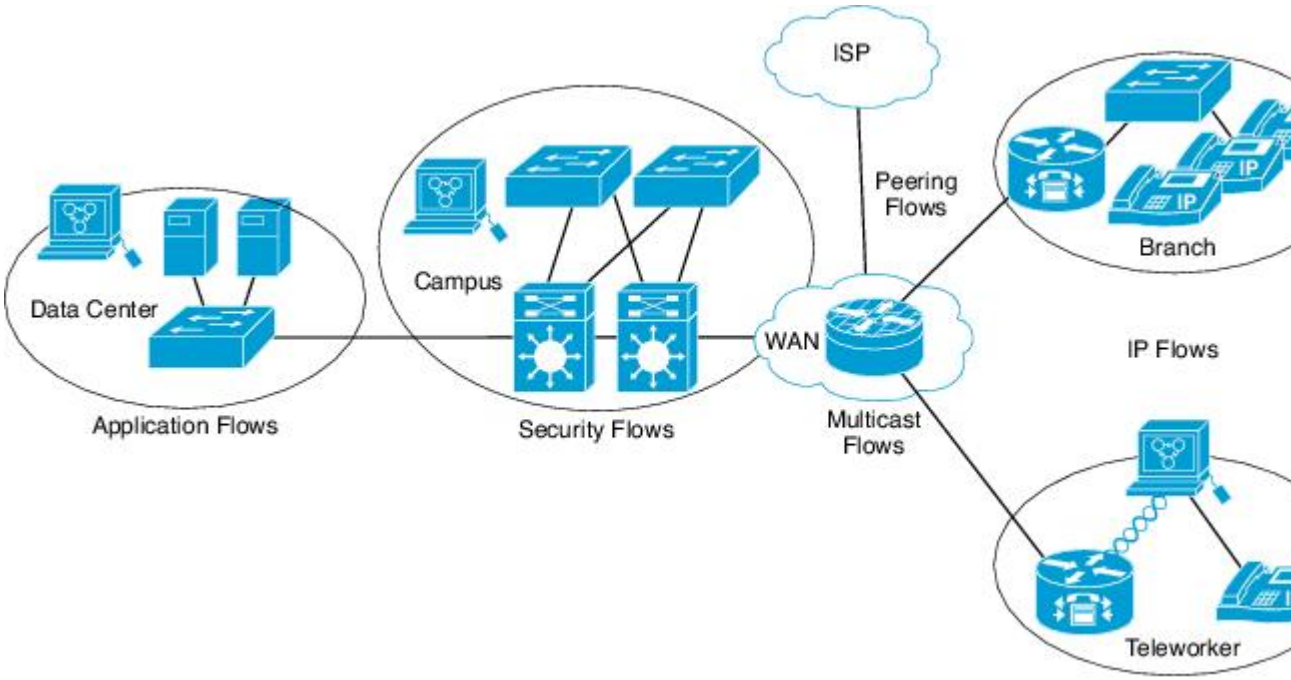
Flexible NetFlow は、同じトラフィックのさまざまなタイプの分析を実行するために使用できます。 下の図では、入力インターフェイス上の標準トラフィック分析のために設計されたレコードと、出力インターフェイス上のセキュリティ分析のために設計されたレコードを使用してパケット 1 が分析されます。

図 *56* : *2* つのフロー モニタを使用した同じトラフィックの分析例



下の図に、カスタム レコードを使用して複数のタイプのフローモニタを適用するより複雑な方法の例を示します。

図 *57*：カスタム レコードでの複数のタイプのフロー モニタの複雑な使用例



Normal

デフォルトのキャッシュ タイプは「normal」です。 このモードでは、キャッシュ内のエントリが timeout active 設定と timeout inactive 設定に従って期限切れになります。 キャッシュ エントリは、期限切れになるとキャッシュから削除され、設定されている何らかのエクスポータによってエクスポートされます。

フロー サンプラー

フロー サンプラーは、ルータのコンフィギュレーションで別のコンポーネントとして作成されます。 フロー サンプラーは、分析用に選択されるパケットの数を制限することで、 NetFlow Lite を実行しているデバイス上の負荷を減らすために使用されます。

サンプラーはランダム サンプリング技術（モード）を使用します。つまり、サンプルを取得するときに、ランダムに選択したサンプリング位置が毎回使用されます。

フロー サンプリングでは、ルータのパフォーマンスに対するモニタリング精度が交換されます。サンプラーをフローモニタに適用すると、フローモニタが分析する必要のあるパケット数が減少するため、ルータでフロー モニタを実行するためのオーバーヘッド負荷が低下します。 フローモニタで分析されるパケット数が減少すると、フロー モニタのキャッシュに格納される情報の精度が、それに応じて低下します。

ip flow monitor コマンドを使用してインターフェイスに適用する場合、サンプラーとフロー モニタを組み合わせます。

デフォルト設定

次の表に、スイッチの NetFlow Lite のデフォルト設定を示します。

表 *57* : ***NetFlow Lite*** のデフォルト設定

設定	デフォルト
フロー アクティブ タイムアウト	1800 秒 （注） この設定のデフォルト値は特定の NetFlow Lite 設定では高すぎる場合があります。 低い値（180 または 300 秒）への変更を検討してください。
フロー タイムアウトの非アクティブ化	イネーブル、30 秒
フロー アップデート タイムアウト	1800 秒
デフォルト キャッシュ サイズ	16640 ビット

NetFlow Lite の設定方法

NetFlow Lite を設定するには、次の一般的な手順に従います。

1. フローにキー フィールドおよび非キー フィールドを指定して、フロー レコードを作成します。
2. プロトコルを指定して任意のフローエクスポータを作成し、宛先ポート、宛先、およびその他のパラメータを転送します。
3. フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを作成します。
4. 任意のサンプラーを作成します。
5. レイヤ 2 ポート、レイヤ 3 ポート、または VLAN にフロー モニタを適用します。

フロー レコードの作成

フロー レコードを作成し、照合するキー、および収集するフィールドをフロー内に追加できます。

手順の概要

1. **configureterminal**
2. **flow record***name*
3. **description***string*
4. **match***type*
5. **collect***type*
6. **end**
7. **show flow record** [**name***record-name*]
8. **copy running-config startup-config**

手順の詳細

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

ステップ 2	**flow record***name*
	
	例：
	
	`Switch(config)# flow record test`
	`Switch(config-flow-record)#`
		フロー レコードを作成し、フロー レコード コンフィギュレーション モードを開始します。

ステップ 3	**description***string* 例： `Switch(config-flow-record)# description Ipv4Flow`	（任意）最大63文字で、このフローの説明を指定します。

ステップ 4	**match***type*
	
	例：
	
	`Switch(config-flow-record)# match ipv4 source address`
	`Switch(config-flow-record)# match ipv4 destination address`
	`Switch(config-flow-record)# match flow direction`
		一致キーを指定します。 使用できる match キーの値については、Flexible NetFlow の match パラメータ を参照してください。

	コマンドまたはアクション	目的

ステップ 5	**collect***type*
	
	例：
	
	`Switch(config-flow-record)# collect counter bytes layer2 long`
	`Switch(config-flow-record)# collect counter bytes long`
	`Switch(config-flow-record)# collect timestamp absolute first`
	`Switch(config-flow-record)# collect transport tcp flags`
	`Switch(config-flow-record)#` collect interface output
		コレクションフィールドを指定します。使用できるコレクションフィールドの値については、Flexible NetFlow の collect パラメータ を参照してください。
		
		（注） フロー レコードの collect フィールドとしての **collect interface output** がフロー モニタにある場合は、スイッチの宛先アドレスに基づいて出力インターフェイスが検出されます。そのため、他のフロー モニタの場合は、次の設定が必要です。
		
		• ipv4 フロー モニタの場合は「**match ip destination address**」を設定します。
		• ipv6 フロー モニタの場合は「**match ipv6 destination address**」を設定します。
		• データリンク フロー モニタの場合は、「**match datalink mac output**」を設定します。
		
		次のアドレスのいずれかにフローが作成された場合、**collect interface output** フィールドに **NULL** の値が返されます。
		
		• L3 ブロードキャスト
		• L2 ブロードキャスト
		• L3 マルチキャスト
		• L2 マルチキャスト
		• L2 の不明な宛先。

ステップ 6	**end** 例： `Switch(config-flow-record)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show flow record** [**name***record-name*] 例： `Switch show flow record test`	（任意）NetFlow のフロー レコード情報を表示します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

エクスポート フォーマット、プロトコル、宛先、およびその他のパラメータを指定することによって、任意でフロー エクスポータを定義します。

関連トピック

フロー レコード, （688 ページ）

例：フローの設定, （712 ページ）

フロー エクスポータの作成

フロー エクスポートを作成して、フローのエクスポート パラメータを定義できます。

（注） フロー エクスポータごとに、1 つ宛先のみがサポートされます。 複数の宛先にデータをエクスポートする場合は、複数のフロー エクスポータを設定してフロー モニタに割り当てる必要があります。

IPv4 アドレスを使用して宛先にエクスポートできます。

手順の概要

1. **configureterminal**
2. **flow exporter***name*
3. **description***string*
4. **destination** {*ipv4-address*}[**vrf** *vrf-name*]
5. **dscp***value*
6. **source** { *source type* }
7. **transportudp***number*
8. **ttl** *seconds*
9. **export-protocol** {**netflow-v9**}
10. **end**
11. **show flow exporter** [**name***record-name*]
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flow exporter***name* 例： `Switch(config)# flow exporter ExportTest`	フロー エクスポータを作成し、フロー エクスポータ コンフィギュレーション モードを開始します。
ステップ 3	**description***string* 例： `Switch(config-flow-exporter)# description ExportV9`	（任意）最大 63 文字で、このフローの説明を指定します。
ステップ 4	**destination** {*ipv4-address*}[**vrf** *vrf-name*] 例： `Switch(config-flow-exporter)# destination 192.0.2.1 (IPv4 destination)`	このエクスポータに IPv4 宛先アドレスまたはホスト名を設定します。

	コマンドまたはアクション	目的
ステップ 5	**dscp***value* 例： `Switch(config-flow-exporter)# dscp 0`	（任意）DiffServ コードポイント値を指定します。 範囲は 0 ～ 63 です。 デフォルトは 0 です。
ステップ 6	**source** { *source type* } 例： `Switch(config-flow-exporter)# source gigabitEthernet1/0/1`	（任意）設定された宛先で NetFlow コネクタに到達するために使用するインターフェイスを指定します。 送信元として次のインターフェイスを設定できます。
ステップ 7	**transportudp***number* 例： `Switch(config-flow-exporter)# transport udp 200`	（任意）NetFlow コレクタに到達するために使用する UDP ポートを指定します。 範囲は1 ~ 65536 です。
ステップ 8	**ttl** *seconds* 例： `Switch(config-flow-exporter)# ttl 210`	（任意）エクスポータによって送信されるデータグラムの存続可能時間（TTL）値を設定します。 範囲は 1 ～ 255 秒です。 デフォルトは 255 です。
ステップ 9	**export-protocol** {**netflow-v9**} 例： `Switch(config-flow-exporter)# export-protocol netflow-v9`	エクスポータで使用される NetFlow エクスポート プロトコルのバージョンを指定します。
ステップ 10	**end** 例： `Switch(config-flow-record)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show flow exporter** [**name***record-name*] 例： `Switch show flow exporter ExportTest`	（任意）NetFlow のフローエクスポータ情報を表示します。
ステップ 12	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを定義します。

関連トピック

エクスポータ
例：フローの設定, （712 ページ）

フロー モニタの作成

フロー モニタを作成して、フロー レコードおよびフロー エクスポータと関連付けることができます。

手順の概要

1. **configureterminal**
2. **flow monitor** *name*
3. **description** *string*
4. **exporter** *name*
5. **record** *name*
6. **cache** { **timeout** {**active** | **inactive**} *seconds* | **type normal** }
7. **end**
8. **show flow monitor** [**name** *record-name*]
9. **copy running-config startup-config**

手順の詳細

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

ステップ 2	**flow monitor** *name*
	
	例：
	
	`Switch(config)# flow monitor MonitorTest`
	`Switch (config-flow-monitor)#`
		フローモニタを作成し、フローモニタ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**description** *string* 例： `Switch(config-flow-monitor)# description Ipv4Monitor`	（任意）最大 63 文字で、このフローの説明を指定します。
ステップ 4	**exporter** *name* 例： `Switch(config-flow-monitor)# exporter ExportTest`	フローエクスポータとこのフローモニタを関連付けます。
ステップ 5	**record** *name* 例： `Switch(config-flow-monitor)# record test`	フロー レコードを指定したフローモニタと関連付けます。
ステップ 6	**cache** { **timeout** {**active** | **inactive**} *seconds* | **type normal** } 例： `Switch(config-flow-monitor)# cache timeout active 15000`	指定したフローモニタとフローキャッシュを関連付けます。
ステップ 7	**end** 例： `Switch(config-flow-monitor)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show flow monitor** [**name** *record-name*] 例： `Switch show flow monitor name MonitorTest`	（任意）NetFlow のフロー モニタ情報を表示します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、または VLAN にフロー モニタを適用します。

関連トピック

モニタ
例：フローの設定，（712 ページ）

サンプラーの作成

サンプラーを作成し、フローの NetFlow サンプリング レートを定義できます。

手順の概要

1. **configureterminal**
2. **sampler** *name*
3. **description** *string*
4. **mode** { **deterministic** { *m* - *n* } | **random** { *m* - *n* }}
5. **end**
6. **show sampler** [*name*]
7. **copy running-config startup-config**

手順の詳細

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

ステップ 2	**sampler** *name*
	
	例：
	
	`Switch(config)# sampler SampleTest`
	`Switch(config-flow-sampler)#`
		サンプラーを作成し、サンプラー コンフィギュレーション モードを開始します。

ステップ 3	**description** *string* 例： `Switch(config-flow-sampler)# description samples`	（任意）最大 63 文字で、このフローの説明を指定します。

	コマンドまたはアクション	目的
ステップ 4	**mode** { **deterministic** { *m* - *n* } | **random** { *m* - *n* }} 例： `Switch(config-flow-sampler)#` **`mode random 1 out-of 1022`**	ランダム サンプル モードを定義します。 インターフェイスに対してランダム サンプラーまたは確定的サンプラーのいずれも設定できます。 *n* パケット ウィンドウから *m* 個のパケットを選択します。 ウィンドウ サイズには、32～1022 の範囲のパケットを選択します。 インターフェイスにサンプラーを設定する際は、次の点に注意してください。 • 確定的サンプラー（s1 など）を使用してモニタを接続する場合、同じサンプラー s1 との接続ごとにスイッチ（ハードウェア）から 4 つの使用可能なサンプラーのうちの新しい空きサンプラーの 1 つを使用します。 したがって、サンプラーとモニタの接続は、4 つを超えて行うことができません。 • これとは逆に、ランダムサンプラー（たとえば、この場合も s1 など）を使用してモニタを接続する場合、最初の接続だけがスイッチ（ハードウェア）の新しいサンプラーを使用します。 同じサンプラー s1 を使用するすべての接続のうちの残りは同じサンプラーを共有します。 この動作により、確定的サンプラーを使用する際は、サンプリングレートとスイッチが何を送信するかを比較して、適切な数のフローがサンプリングされているかを常に確認することができます。 複数のインターフェイスに同じランダム サンプラーを使用している場合は、インターフェイスからのフローを常にサンプリングすることができ、他のインターフェイスからのフローは常にスキップできます。
ステップ 5	**end** 例： `Switch(config-flow-sampler)#` **`end`**	特権 EXEC モードに戻ります。
ステップ 6	**show sampler** [*name*] 例： `Switch` **`show sample SampleTest`**	（任意）NetFlow サンプラに関する情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `Switch#` **`copy running-config startup-config`**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

ソース インターフェイス、または VLAN にフロー モニタを適用します。

インターフェイスへのフローの適用

フロー モニタおよびオプションのサンプラーをインターフェイスに適用できます。

手順の概要

1. **configureterminal**
2. **interface***type*
3. {**ip flow monitor** | **ipv6 flow monitor**}*name* [|**sampler***name*] { **input** |**output**}
4. **end**
5. **show flow interface** [*interface-typenumber*]
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***type* 例： `Switch(config)# interface GigabitEthernet1/0/1`	インターフェイス コンフィギュレーション モードを開始し、インターフェイスを設定します。 インターフェイス コンフィギュレーションのコマンド パラメータは次のとおりです。 ポート チャネル インターフェイスには NetFlow モニタを接続できません。 両方のサービス モジュール インターフェイスが EtherChannel の一部である場合、両方の物理インターフェイスにモニタを接続する必要があります。
ステップ 3	{**ip flow monitor** | **ipv6 flow monitor**}*name* [|**sampler***name*] { **input** |**output**} 例： `Switch(config-if)# ip flow`	入力または出力パケットに対応するインターフェイスに、IPv4 または IPv6 フロー モニタ、およびオプションのサンプラーを関連付けます。 データリンク L2 トラフィック フローをモニタリングするには、**datalink flow monitor***name***sampler***sampler-name*{**input**} インターフェイス コマンドを使用します。 この特定のコマンドは、データリン

	コマンドまたはアクション	目的
	monitor MonitorTest input	ク L2 フロー モニタおよび必須のサンプラーを入力パケットのインターフェイスに関連付けます。 データリンク フロー モニタがインターフェイスまたは VLAN レコードに割り当てられている場合、非 IPv6 または非 IPv4 トラフィック用のフローだけが作成されます。 （注） フロー モニタをインターフェイスに割り当てる場合は、常にサンプラーを設定する必要があります。 サンプラーがない場合、エラー メッセージが表示されます。
ステップ 4	**end** 例： `Switch(config-flow-monitor)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show flow interface** [*interface-typenumber*] 例： `Switch# show flow interface`	（任意）インターフェイスの NetFlow 情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN 上でのブリッジ型 NetFlow の設定

フロー モニタおよびオプションのサンプラーを VLAN に適用できます。

手順の概要

1. **configureterminal**
2. **vlan** [**configuration**] *vlan-id*
3. **interface** {**vlan**} *vlan-id*
4. **ip flow monitor***monitor name* [**sampler***sampler name*] {**input**|**output**}
5. **copy running-config startup-config**

手順の詳細

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

ステップ 2	**vlan** [**configuration**] *vlan-id*
	
	例：
	
	`Switch(config)# vlan configuration 30`
	`Switch(config-vlan-config)#`
		VLAN または VLAN コンフィギュレーションモードを開始します。

ステップ 3	**interface** {**vlan**} *vlan-id* 例： `Switch(config)# interface vlan 30`	設定のために SVI を指定します。
ステップ 4	**ip flow monitor***monitor name* [**sampler***sampler name*] {**input**|**output**} 例： `Switch(config-vlan-config)# ip flow monitor MonitorTest input`	入力または出力パケットに対応する VLAN に、フロー モニタおよびオプションのサンプラーを関連付けます。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

レイヤ 2 NetFlow の設定

NetFlow Lite レコード内でレイヤ 2 キーを定義できます。このレコードを使用して、レイヤ 2 インターフェイスのフローをキャプチャできます。

手順の概要

1. **configureterminal**
2. **flow record** *name*
3. **match datalink** { **ethertype** | **mac** { **destination** { **address input** } | **source** { **address input** } } }
4. **match** { **ipv4** {**destination** | **protocol** | **source** | **tos** } | **ipv6** {**destination** | **flow-label**| **protocol**| **source**| **traffic-class** } | **transport** {**destination-port** | **source-port**} }
5. **end**
6. **show flow record** [*name*]
7. **copy running-config startup-config**

手順の詳細

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

ステップ 2	**flow record** *name*
	
	例：
	
	`Switch(config)# flow record L2_record`
	`Switch(config-flow-record)#`
		フロー レコード コンフィギュレーション モードを開始します。

ステップ 3	**match datalink** { **ethertype**	**mac** { **destination** { **address input** }	**source** { **address input** } } }
			
			例：
			
			`Switch(config-flow-record)# match datalink mac source address input`
			`Switch(config-flow-record)# match datalink mac destination address input`
				レイヤ 2 属性をキーとして指定します。 この例では、入力時のパケットの送信元および宛先の MAC アドレスがキーです。
				
				（注） データリンク フロー モニタがインターフェイスまたは VLAN レコードに割り当てられている場合、非 IPv4 または非 IPv6 トラフィック用のフローだけが作成されます。

ステップ 4	**match** { **ipv4** {**destination**	**protocol**	**source**	**tos** }	**ipv6** {**destination**	**flow-label**| **protocol**| **source**| **traffic-class** }	**transport** {**destination-port**	**source-port**} }
								
								例：
								
								`Switch(config-flow-record)# match ipv4 protocol`
								`Switch(config-flow-record)# match ipv4 tos`
									追加のレイヤ 2 属性をキーとして指定します。 この例では、IPv4 プロトコルと ToS がキーです。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config-flow-record)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show flow record** [*name*] 例： `Switch# show flow record`	（任意）インターフェイスの NetFlow 情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

Flexible NetFlow のモニタリング

次の表にあるコマンドを使用して、Flexible NetFlow をモニタリングできます。

表 *58*：*Flexible NetFlow* のモニタリング コマンド

コマンド	目的
show flow exporter [**broker** | **export-ids** | **name** | *name* | **statistics** | **templates**]	NetFlow のフロー エクスポータ情報と統計情報を表示します。
show flow exporter [**name***exporter-name*]	NetFlow のフロー エクスポータ情報と統計情報を表示します。
show flow interface	NetFlow インターフェイスに関する情報を表示します。
show flow monitor [**name***exporter-name*]	NetFlow のフロー モニタ情報と統計情報を表示します。
show flow monitor statistics	フロー モニタの統計情報を表示します。
show flow monitor cache format {**table** | **record** | **csv**}	指定された形式でフローモニタのキャッシュの内容を表示します。

コマンド	目的
show flow record [**name***record-name*]	NetFlow のフロー レコード情報を表示します。
show flow ssid	WLAN の NetFlow モニタのインストール ステータスを表示します。
show sampler [**broker** | **name** | *name*]	NetFlow サンプラに関する情報を表示します。
show wlan*wlan-name*	デバイスで設定された WLAN を表示します。

NetFlow Lite の設定例

例：フローの設定

（注） フローを設定する場合、フロー レコードで定義されたプロトコル、送信元ポート、宛先ポート、最初と最後のタイムスタンプ、パケットおよびバイト カウンタが必要です。 これらがないと、「Warning: Cannot set protocol distribution with this Flow Record. Require protocol, source and destination ports, first and last timestamps and packet and bytes counters.」というエラー メッセージが表示されます。

次に、フローを作成し、そのフローをインターフェイスに適用する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# flow exporter export1
Switch(config-flow-exporter)# destination 10.0.101.254
Switch(config-flow-exporter)# transport udp 2055
Switch(config-flow-exporter)# template data timeout 60
Switch(config-flow-exporter)# exit
Switch(config)# flow record record1
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# match ipv4 protocol
Switch(config-flow-record)# match transport source-port
Switch(config-flow-record)# match transport destination-port
Switch(config-flow-record)# collect counter bytes long
Switch(config-flow-record)# collect counter packets long
Switch(config-flow-record)# collect timestamp sys-uptime first
Switch(config-flow-record)# collect timestamp sys-uptime last
Switch(config-flow-record)# exit
Switch(config)# sampler SampleTest
Switch(config-sampler)# mode random 1 out-of 100
Switch(config-sampler)# exit
Switch(config)# flow monitor monitor1
Switch(config-flow-monitor)# cache timeout active 300
Switch(config-flow-monitor)# cache timeout inactive 120
Switch(config-flow-monitor)# record record1
Switch(config-flow-monitor)# exporter export1
Switch(config-flow-monitor)# exit
```

```
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# ip flow monitor monitor1 sampler SampleTest input
Switch(config-if)# end
```

関連トピック

フロー レコードの作成, （697 ページ）

フロー レコード, （688 ページ）

フロー エクスポータの作成, （700 ページ）

エクスポータ

フロー モニタの作成, （703 ページ）

モニタ

サンプラーの作成

サンプラー

第 31 章

Web Cache Communication Protocol を使用したキャッシュ サービスの設定

- 機能情報の確認，715 ページ
- WCCP の前提条件，715 ページ
- WCCP に関する制約事項，716 ページ
- WCCP に関する情報，717 ページ
- WCCP の設定方法，721 ページ

機能情報の確認

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

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

WCCP の前提条件

スイッチで WCCP を設定する前に、次の設定要件に従ってください。

- 同じサービス グループ内のアプリケーション エンジンおよびスイッチは、WCCP 対応のスイッチに直接接続された同一サブネットワーク内に存在する必要があります。
- クライアント、アプリケーションエンジン、およびレイヤ3インターフェイスとしてのサーバ（ルーテッド ポートおよびスイッチ仮想インターフェイス（SVI））に接続されたスイッ

チ インターフェイスを設定します。 WCCP パケットのリダイレクトが機能するためには、サーバ、アプリケーションエンジン、およびクライアントが、異なるサブネット上に存在する必要があります。

- 各アプリケーション エンジンに 1 つのマルチキャスト アドレスを設定するときは、予約されていないマルチキャスト アドレスだけを使用します。
- WCCP エントリおよび PBR エントリは、同じ TCAM リージョンを使用します。 WCCP は、PBR（アクセス、ルーティング、デュアル IPv4/v6 ルーティング）をサポートするテンプレート上でだけサポートされます。
- TCAM エントリを WCCP エントリの追加に使用できない場合、パケットはリダイレクトされず、標準ルーティング テーブルを使用して転送されます。
- 使用可能な PBR ラベルの数は、WCCP 入力方法でイネーブルになるインターフェイスが増えるにつれて減っていきます。 サービス グループをサポートする各インターフェイスでは、ラベルが 1 つ消費されます。 WCCP ラベルは PBR ラベルから取得されます。 PBR と WCCP 間で使用可能なラベルを監視および管理する必要があります。 ラベルが使用できないと、スイッチはサービス グループを追加できなくなります。 ただし、別のインターフェイスに同じ一連のサービス グループがある場合、新しいラベルは必要にならず、グループをインターフェイスに追加できます。
- スタック メンバー スイッチで設定されたルーティング最大伝送単位（MTU）サイズは、クライアント MTU サイズより長い必要があります。 アプリケーション エンジンに接続されたポートで設定された MAC レイヤ MTU サイズは、GRE トンネル ヘッダー バイトを考慮する必要があります。

WCCP に関する制約事項

サポートされない WCCP 機能

次の WCCP 機能は、このソフトウェア リリースでサポートされていません。

- **ip wccp redirect out** インターフェイス コンフィギュレーション コマンドを使用して設定された発信インターフェイスでのパケットのリダイレクト
- パケット リダイレクトの GRE 転送方式
- GRE リダイレクトおよび GRE リターン
- ロードバランシング用のハッシュ割り当て方式
- WCCP の SNMP サポート
- ハードウェアでのハッシュ割り当て マスク割り当てのみを使用したロード バランスの実行
- フラグメント化されたパケットのリダイレクト。 これは、セキュリティ機能です。

一般的な制約事項

- サービス グループの最大数：8 入力および 8 出力。
- 同じスイッチ インターフェイス上では、WCCP と VPN ルーティングおよび転送（VRF）を設定できません。
- 同じスイッチ インターフェイス上では、WCCP および PBR を設定できません。
- 同じスイッチ インターフェイス上では、WCCP およびプライベート VLAN（PVLAN）を設定できません。
- **ip wccp redirect exclude in** コマンドは、出力 WCCP 方式から入力パケットを除外できるようにします。 これは、CE へのインターフェイスでは必要ではありません。
- キャッシュ エンジンが使用できない場合は、一致するパケットはドロップされます。 これは、クローズ グループのサポートです。 VRF 認識 WCCP のサポート、IPv6 WCCP のサポートはありません。
- デバイスを **ip wccp check services all** コマンドで設定すると、リダイレクト ACL がパケットと一致しなかった場合、次のプライオリティのサービス グループと照合されます。

WCCP に関する情報

WCCP の概要

（注） この機能を使用するには、デバイス上で IP Services フィーチャー セットが稼働している必要があります。

WCCP をサポートするのは、Cisco Catalyst 3560-CX スイッチのみです。

WCCP はシスコが開発したコンテンツ ルーティング技術です。WCCP を使用すると広域アプリケーション エンジン（以降、アプリケーション エンジンと呼ぶ）をネットワーク インフラストラクチャに統合できます。アプリケーションエンジンは、頻繁にアクセスのあるコンテンツを透過的に格納し、その同じコンテンツへの要求を満たし、サーバから繰り返し伝送されることを防ぎます。アプリケーションエンジンは、コンテンツ配信を加速させ、最大限のスケーラビリティとコンテンツの可用性を実現します。 サービスプロバイダー ネットワークのアクセス ポイント（POP）で、WCCPおよびアプリケーションエンジン ソリューションを展開できます。エンタープライズ ネットワークでは、地域サイトまたは小規模ブランチ オフィスで WCCP およびアプリケーション エンジン ソリューションを展開できます。

WCCPおよびシスコのキャッシュ エンジン（またはWCCPが稼働している他のアプリケーション エンジン）は、ネットワークでのトラフィック パターンをローカライズし、コンテンツ要求がローカルで実現されるようにします。

WCCP により、サポート対象のシスコ ルータおよびスイッチは、コンテンツ要求を透過的にリダイレクトできます。透過リダイレクトを使用すると、ユーザは使用しているブラウザが Web プロ

キシを使用するように設定する必要がありません。 代わりに、ターゲット URL を使用してコンテンツを要求でき、その要求は自動的にアプリケーションエンジンにリダイレクトされます。 透過という用語は、エンドユーザが、自分の要求したファイル（Web ページなど）が、もとの指定したサーバからではなくアプリケーション エンジンから送信されるのを知らないという意味です。

アプリケーションエンジンが要求を受け取ると、自身のローカルキャッシュからサービスしようとします。 要求された情報が存在しない場合、アプリケーションエンジンは別個の要求をエンドサーバに送信し、要求された情報を取得します。 取得した情報は、アプリケーションエンジンが要求元のクライアントに転送するとともに、その後の要求に応えるため、情報をキャッシュします。

WCCP では、アプリケーションエンジンクラスタ（一連のアプリケーションエンジン）は、複数のルータまたはスイッチにサービスできます。

WCCP メッセージ交換

次の一連のイベントは、WCCP メッセージ交換について説明します。

1. アプリケーション エンジンは、WCCP を使用して IP アドレスを WCCP 対応スイッチに送信し、Here I am メッセージを通して自己の存在を伝えます。 スイッチおよびアプリケーション エンジンは、UDP ポート 2048 に基づき、制御チャネルを介して互いに通信します。
2. WCCP 対応スイッチは、アプリケーション エンジンの IP 情報を使用してクラスタ ビュー（クラスタ内のアプリケーションエンジンのリスト）を作成します。 このビューが、I see you メッセージでクラスタ内の各アプリケーション エンジンに送信すると、本質的にすべてのアプリケーション エンジンが互いの存在を認識するようになります。 クラスタのメンバーシップが一定時間同じままになった後で、安定したビューが確立されます。
3. 安定したビューが確立されると、クラスタ内の低い IP アドレスを持つアプリケーション エンジンが指定アプリケーション エンジンとして選択されます。

WCCP ネゴシエーション

WCCP プロトコル メッセージを交換する際、指定アプリケーション エンジンおよび WCCP 対応スイッチは次の項目をネゴシエートします。

- 転送方式（スイッチがパケットをアプリケーションエンジンに転送するときに使用される方式）。 スイッチは、パケット宛先 MAC アドレスをターゲット アプリケーション エンジン MAC アドレスに置き換えて、レイヤ 2 ヘッダーを書き換えます。 次にスイッチは、パケットをアプリケーション エンジンに転送します。 この転送方式では、ターゲット アプリケーション エンジンがレイヤ 2 でスイッチに直接接続されている必要があります。
- 割り当て方式（パケットをクラスタ内のアプリケーションエンジン間に配信するときに使用される方式）。 スイッチは宛先 IP アドレス、送信元 IP アドレス、宛先レイヤ 4 ポート、および送信元レイヤ 4 ポートの一部のビットを使用して、リダイレクトされたパケットを受け取るアプリケーション エンジンを判別します。

- パケット戻し方式（パケットをアプリケーションエンジンから通常の転送用スイッチに戻すときに使用される方式）。 アプリケーション エンジンがパケットを拒否し、パケット戻し機能を起動するのには以下の理由があります。
  - アプリケーション エンジンが過負荷となり、パケットにサービスする余裕がない。
  - アプリケーション エンジンがサーバからエラー メッセージ（プロトコル エラーや認証エラーなど）を受け取り、ダイナミック クライアント バイパス機能を使用している。 バイパスは、クライアントがアプリケーションエンジンをバイパスし、サーバに直接接続できるようにします。

アプリケーション エンジンはパケットを WCCP 対応スイッチに戻し、アプリケーション エンジンが存在しないかのようにサーバに転送します。 アプリケーションエンジンは、再接続試行を代行受信しません。 このようにして、アプリケーション エンジンは効率的にアプリケーション エンジンへのパケットのリダイレクトをキャンセルし、バイパスフローを作成します。 戻し方式がレイヤ 2 書き換えである場合、パケットはハードウェア内でターゲット サーバに転送されます。 サーバが情報に応答しているとき、スイッチは通常のレイヤ 3 転送を使用して、情報を要求しているクライアントに戻します。

MD5 セキュリティ

WCCPは各プロトコルメッセージでオプションのセキュリティコンポーネントを提供し、スイッチとアプリケーション エンジン間のメッセージで MD5 認証をスイッチが使用できるようにします。 （スイッチの認証がイネーブルになっているとき）MD5 で認証されないメッセージは、スイッチによって廃棄されます。 パスワード文字列は、MD5 値と組み合され、スイッチとアプリケーション エンジン間の接続のセキュリティを確立します。 各アプリケーション エンジンで同じパスワードを設定する必要があります。

パケットのリダイレクトおよびサービス グループ

WCCP を設定して、FTP、プロキシ Web キャッシュ処理、音声およびビデオアプリケーションなど、リダイレクト用トラフィックを分類できます。 この分類はサービス グループと呼ばれ、プロトコル タイプ（TCP または UDP）およびレイヤ 4 送信元ポート番号と宛先ポート番号に基づきます。 サービス グループは、TCP ポート 80 を意味する、Web キャッシュなどの Well-known 名または 0 ～ 99 のサービス番号のいずれかで識別されます。 サービス グループは、プロトコルおよびレイヤ 4 ポート番号にマッピングするように設定され、独立して確立および維持されます。 WCCPは、アプリケーションエンジンに加入して分類基準を動的に提供するダイナミック サービス グループを許可します。

スイッチまたはスイッチ スタックでは最大 8 つまでのサービス グループを、サービス グループごとに 32 までのキャッシュ エンジンを設定できます。 WCCP のグループ定義には、サービス グループのプライオリティがあります。 WCCP は、プライオリティを使用して、スイッチ ハードウェアのサービス グループを設定します。 たとえば、サービス グループ 1 はプライオリティ 100 で、宛先ポート 80 を探していて、サービス グループ 2 はプライオリティ 50 で、送信元ポート 80 を探している場合、送信元および宛先ポート 80 の着信パケットは、サービス グループ 1 を使用して転送されます。 これは、サービス グループ 1 の方がプライオリティが高いためです。

WCCP は各サービス グループのアプリケーション エンジンのクラスタをサポートします。 リダイレクトされたトラフィックは、アプリケーション エンジンの 1 つに送信可能です。 スイッチは、サービスグループのクラスタ内のアプリケーションエンジン間で、トラフィックのロードバランシングのマスク割り当て方式をサポートします。

WCCP がスイッチ上で設定された後、スイッチはクライアントから受信したすべてのサービス グループ パケットをアプリケーション エンジンに転送します。 ただし、次のパケットはリダイレクトされません。

- アプリケーションエンジンから発信され、サーバに宛てられたパケット
- アプリケーション エンジンから発信され、クライアントに宛てられたパケット
- アプリケーションエンジンにより返送または拒否されたパケット。 これらのパケットはサーバに送信されます。

プロトコル メッセージの送受信用に、サービス グループにつき 1 つのマルチキャスト アドレスを設定できます。 マルチキャスト アドレスが 1 つの場合、アプリケーション エンジンは通知を 1 つのアドレスに送信することになり、たとえば 225.0.0.0 など、サービス グループのすべてのルータにカバレッジを提供します。 ルータを動的に追加および削除する場合、1 つのマルチキャストアドレスを使用することで、コンフィギュレーションが簡単になります。これは、特に WCCP ネットワークのすべてのデバイスのアドレスを入力する必要がないためです。

ルータ グループ リストを使用すれば、アプリケーション エンジンから受け取ったプロトコル パケットを検証できます。 グループ リストのアドレスに一致するパケットは処理され、グループ リスト アドレスに一致しないパケットはドロップされます。

特定クライアント、サーバ、またはクライアントとサーバのペアのキャッシングをディセーブルにするには、WCCP リダイレクト アクセス コントロール リスト（ACL）を使用します。 リダイレクト ACL に一致しないパケットはキャッシュをバイパスし、通常通りに転送されます。

WCCP パケットがリダイレクトされる前、スイッチはインターフェイス上に設定されているすべての着信機能に関連した ACL をテストし、パケットが ACL 内のエントリと一致するかどうかによって、パケットの転送を許可または拒否します。

（注） WCCP リダイレクト リストでは、許可と拒否の両方の ACL エントリがサポートされます。

パケットがリダイレクトされると、リダイレクトされたインターフェイスに関連付けられた出力 ACL がパケットに適用されます。 元のポートに関連付けられた ACL は、リダイレクトされたインターフェイス上で必須出力 ACL を特に設定しない限り適用されません。

WCCP の設定方法

WCCP のデフォルト設定

機能	デフォルト設定
WCCP イネーブル ステート	WCCP サービスはディセーブルです。
プロトコル バージョン	WCCPv2
インターフェイス上で受信したトラフィックのリダイレクト	ディセーブル

関連トピック

キャッシュ サービスのイネーブル化, （721 ページ）

キャッシュ サービスのイネーブル化

WCCP パケット リダイレクトが機能するために、クライアントに接続されたスイッチ インターフェイスが着信パケットをリダイレクトするように設定する必要があります。

この手順では、ルーテッド ポートでこれらの機能を設定する方法を示します。 これらの機能を SVI で設定するには、手順に従った設定例を参照してください。

キャッシュ サービスをイネーブルにしたり、マルチキャスト グループ アドレスまたはグループ リストを設定したり、ルーテッド インターフェイスを設定したり、クライアントから受信した着信パケットをアプリケーションエンジンにリダイレクトしたり、マルチキャストアドレスを受信するようにインターフェイスをイネーブルにしたり、パスワードを設定したりするには、次の手順を実行します。 この手順は必須です。

はじめる前に

SDM テンプレートを設定し、デバイスをリブートします。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip wccp** {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]
4. **interface** *interface-id*
5. **no switchport**
6. **ip address** *ip-address subnet-mask*
7. **no shutdown**
8. **exit**
9. **interface** *interface-id*
10. **no switchport**
11. **ip address** *ip-address subnet-mask*
12. **no shutdown**
13. **ip wccp** {**web-cache** | *service-number*} **redirect in**
14. **ip wccp** {**web-cache** | *service-number*} **group-listen**
15. **exit**
16. **end**
17. **show running-config**
18. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip wccp** {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]	キャッシュ サービスをイネーブルにし、アプリケーション エンジンで定義されたダイナミック サービスに対応するサービス番号を指定します。 デフォルトでは、この機能はディセーブルになっています。

	コマンドまたはアクション	目的
	例： `Switch(config)# ip wccp web-cache`	（任意）**group-address** *groupaddress* には、スイッチおよびアプリケーション エンジンがサービス グループに加入するときに使用するマルチキャスト グループ アドレスを指定します。 （任意）**group-list** *access-list* には、マルチキャスト グループ アドレスが使用されない場合、サービス グループに加入しているアプリケーション エンジンに対応する有効な IP アドレスのリストを指定します。 （任意）**redirect-list** *access-list* には、特定ホストのリダイレクト サービスまたはホストから特定パケットを指定します。 （任意）**password** *encryption-number password* には、暗号化番号を指定します。 指定できる範囲は 0 ～ 7 です。 暗号化しない場合は 0、独自の場合は 7 を使用します。 7 文字以内でパスワード名を指定します。 スイッチは、パスワードと MD5 認証値を組み合わせて、スイッチとアプリケーション エンジンとの接続にセキュリティを確保します。 デフォルトでは、パスワードは設定されておらず、認証も実行されていません。 各アプリケーション エンジンで同じパスワードを設定する必要があります。 認証がイネーブルになっている場合、スイッチは認証されないメッセージを廃棄します。
ステップ 4	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	アプリケーションエンジンまたはサーバに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ 3 モードを開始します。
ステップ 6	**ip address** *ip-address subnet-mask* 例： `Switch(config-if)# ip address 172.20.10.30 255.255.255.0`	IP アドレスとサブネット マスクを設定します。
ステップ 7	**no shutdown** 例： `Switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。 各アプリケーション エンジンおよびサーバにステップ 4 ～ 8 を繰り返します。
ステップ 9	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	クライアントに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ 3 モードを開始します。
ステップ 11	**ip address** *ip-address subnet-mask* 例： `Switch(config-if)# ip address 175.20.20.10 255.255.255.0`	IP アドレスとサブネット マスクを設定します。
ステップ 12	**no shutdown** 例： `Switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 13	**ip wccp** {**web-cache** | *service-number*} **redirect in** 例： `Switch(config-if)# ip wccp web-cache redirect in`	クライアントから受信したパケットをアプリケーション エンジンにリダイレクトします。 クライアントに接続されているインターフェイス上でイネーブルにします。
ステップ 14	**ip wccp** {**web-cache** | *service-number*} **group-listen** 例： `Switch(config-if)# ip wccp web-cache group-listen`	（任意）マルチキャスト グループ アドレスを使用するとき、**group-listen** キーワードはインターフェイスをイネーブルにしてマルチキャスト アドレスをリッスンします。 アプリケーションエンジンに接続されているインターフェイス上でイネーブルにします。
ステップ 15	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。 各クライアントにステップ 9 ～ 15 を繰り返します。

	コマンドまたはアクション	目的
ステップ 16	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 17	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 18	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

設定例

次に、ルーテッド インターフェイスを設定し、マルチキャスト グループ アドレスとリダイレクト アクセス リストでキャッシュ サービスをイネーブルにする例を示します。 ギガビット イーサネット ポート 1 はアプリケーション エンジンに接続され、IP アドレス 172.20.10.30 のルーテッド ポートとして設定され、再イネーブル化されています。 ギガビット イーサネット ポート 2 はインターネット経由でサーバに接続され、IP アドレス 175.20.20.10 のルーテッド ポートとして設定され、再イネーブル化されています。 ギガビット イーサネット ポート 3 ～ 6 はクライアントに接続され、IP アドレス 175.20.30.20、175.20.40.30、175.20.50.40、および 175.20.60.50 のルーテッド ポートとして設定されています。 スイッチはマルチキャスト トラフィックを受信し、クライアントインターフェイスから受信したパケットをアプリケーションエンジンにリダイレクトします。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache group-address 224.1.1.100 redirect list 12
Switch(config)# access-list 12 permit host 10.1.1.1
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.10.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache group-listen
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.30.20 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
```

```
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.40.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/5
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.50.40 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/6
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.60.50 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
```

次に、SVI を設定し、マルチキャスト グループ リストでキャッシュ サービスをイネーブルにする例を示します。 VLAN 299 は、IP アドレス 175.20.20.10 で作成および設定されています。 ギガビット イーサネットのポート 1 をインターネット経由でサーバに接続し、VLAN 299 のアクセス ポートとして設定します。 VLAN 300 は、IP アドレス 172.20.10.30 で作成および設定されています。 ギガビット イーサネット ポート 2 はアプリケーション エンジンに接続され、VLAN 300 のアクセス ポートとして設定されています。 VLAN 301 を作成し、IP アドレス 175.20.30.50 に設定します。 クライアントに接続されているファスト イーサネット ポート 3 ～ 6 は、VLAN 301 のアクセス ポートとして設定されています。 スイッチは、クライアント インターフェイスから受信したパケットをアプリケーション エンジンにリダイレクトします。

（注） WCCP リダイレクト リストでは、許可と拒否の両方の ACL エントリがサポートされます。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache group-list 15
Switch(config)# access-list 15 permit host 171.69.198.102
Switch(config)# access-list 15 permit host 171.69.198.104
Switch(config)# access-list 15 permit host 171.69.198.106
Switch(config)# vlan 299
Switch(config-vlan)# exit
Switch(config)# interface vlan 299
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 299
Switch(config)# vlan 300
Switch(config-vlan)# exit
Switch(config)# interface vlan 300
Switch(config-if)# ip address 171.69.198.100 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 300
Switch(config-if)# exit
Switch(config)# vlan 301
Switch(config-vlan)# exit
Switch(config)# interface vlan 301
Switch(config-if)# ip address 175.20.30.20 255.255.255.0
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface range gigabitethernet1/0/3 - 6
Switch(config-if-range)# switchport mode access
```

```
Switch(config-if-range)# switchport access vlan 301
Switch(config-if-range)# exit
```

次の作業

キャッシュ サービスをディセーブルにするには、**no ip wccp web-cache** グローバル コンフィギュレーション コマンドを使用します。 着信パケット リダイレクトをディセーブルにするには、**no ip wccp web-cache redirect in** インターフェイス コンフィギュレーション コマンドを使用します。この手順を完了した後、ネットワークでアプリケーション エンジンを設定します。

関連トピック

WCCP のデフォルト設定, （721 ページ）

第 VI 部

QoS

- QoS の設定，731 ページ
- auto-QoS の設定，843 ページ

第 32 章

QoS の設定

- 機能情報の確認，731 ページ
- QoS の前提条件，731 ページ
- QoS の制約事項，733 ページ
- QoS の概要，734 ページ
- QoS の設定方法，764 ページ
- 標準 QoS のモニタリング，830 ページ
- QoS の設定例，831 ページ
- 次の作業，842 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD> を参照してください。

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

QoS の前提条件

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 使用するアプリケーションのタイプおよびネットワークのトラフィック パターン

- トラフィックの特性およびネットワークのニーズ。 たとえば、ネットワークのトラフィックがバーストであるかどうか。 音声およびビデオ ストリーム用の帯域幅確保の必要性
- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

QoS ACL の注意事項

アクセスコントロールリスト（ACL）を使用してQoS設定する場合は、次のガイドラインに従ってください。

- IP フラグメントと設定されている IP 拡張 ACL を照合することによって、QoS を実施することはできません。 IP フラグメントはベストエフォート型として送信されます。 IP フラグメントは IP ヘッダーのフィールドで示されます。
- 1 つのクラス マップごとに使用できる ACL は 1 つだけ、使用できる **match** クラスマップ コンフィギュレーション コマンドは 1 つだけです。 ACL には、フィールドとパケットの内容を照合する ACE を複数指定できます。
- ポリシー マップの信頼ステートメントには、1 つの ACL 行につき複数のハードウェア エントリが必要になります。 入力サービス ポリシー マップの ACL に信頼ステートメントが含まれている場合、アクセス リストが大きくなりすぎて使用可能な QoS ハードウェア メモリに収容できない可能性があり、ポリシーマップをポートに適用したときにエラーになることがあります。 QoS ACL の行数はできる限り少なくする必要があります。

関連トピック

IPv4 トラフィック用の IP 標準 ACL の作成, （778 ページ）

IPv4 トラフィック用の IP 拡張 ACL の作成, （779 ページ）

IPv6 トラフィック用の IPv6 ACL の作成, （781 ページ）

非 IP トラフィック用のレイヤ 2 MAC ACL の作成, （784 ページ）

ポリシングの注意事項

- 複数の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個のシステムの内部使用向けに予約されたポリサー）をサポートします。 ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。 ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよびASICの限界によって制約されます。

  ポートごとにポリサーを確保することはできません。ポートがいずれかのポリサーに割り当てられる保証はありません。
- 入力ポートでは 1 つのパケットに適用できるポリサーは 1 つだけです。 設定できるのは、平均レート パラメータおよび認定バースト パラメータだけです。

- QoS 対応として設定されているポートを介して受信したすべてのトラフィックは、そのポートに結合されたポリシーマップに基づいて分類、ポリシング、およびマーキングが行われます。 QoS が設定されたトランク ポートでは、そのポートを通じて受信されるすべての VLAN 内トラフィックは、ポートに付加されたポリシーマップに従って分類、ポリシング、およびマーキングが行われます。
- スイッチ上で EtherChannel ポートが設定されている場合、EtherChannel を形成する個々の物理ポートに QoS の分類、ポリシング、マッピング、およびキューイングを設定する必要があります。 また、QoS の設定を EtherChannel のすべてのポートで照合するかどうかを決定する必要があります。
- 既存の QoS ポリシーのポリシー マップを変更する必要がある場合は、最初にすべてのインターフェイスからポリシー マップを削除し、その後ポリシー マップを変更またはコピーします。 変更が終了したら、変更したポリシー マップをインターフェイスに適用します。 最初にすべてのインターフェイスからポリシーマップを削除しなかった場合、CPU 使用率が高くなり、コンソールが長期間停止する可能性があります。

一般的な QoS の注意事項

一般的な QoS の注意事項を次に示します。

- QoS を設定できるのは物理ポートだけです。VLAN のレベルでは QoS はサポートされていません。
- スイッチで受信された制御トラフィック（スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）やルーティング アップデート パケットなど）には、入力 QoS 処理がすべて行われます。
- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小のときに設定を変更するようにしてください。
- スイッチは同種スタックおよび混合スタック構成をサポートします。 混合スタック構成は、Catalyst 2960-S スイッチだけでサポートされます。 同種スタックは 8 つまで、混合スタックは4つまでのスタック メンバを持つことができます。 スイッチ スタック内のすべてのスイッチが LAN Base イメージを実行している必要があります。

QoS の制約事項

以下は、QoS の制約事項を示しています。

- 次の機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。スタック構成、DSCP、自動 QoS、信頼境界、ポリシング、マーキング、マッピング テーブル、および重み付けテール ドロップ。
- 入力キューイングはサポートされません。

- スイッチには 4 つのデフォルトの出力キューをサポートし、さらに 4 つの出力キューを追加して合計 8 つをイネーブルにするオプションがあります。 このオプションは、LAN Base イメージを実行しているスタンドアロン スイッチにのみ使用できます。
- 設定で次の機能を実行する場合は、**mls qos srr-queue output queues 8** を使用して 8 つの出力キューをイネーブルにしないことを推奨します。
  - Auto-QoS
  - Auto SmartPort
  - EnergyWise

  スイッチでは、8 つの出力キューを単一の設定でイネーブルにしてこれらの機能を実行することはできません。
- QoS を設定できるのは物理ポートのみです。 VLAN-based QoS はサポートされません。 分類、キューイングおよびスケジューリングのようなQoSが設定できます。また、ポートにポリシー マップも適用できます。 物理ポートに QoS を設定した場合は、非階層型のポリシー マップをポートに適用します。
- スイッチが LAN Lite イメージを実行中の場合、ACL を設定できますが、その ACL を物理インターフェイスに接続できません。 ACL を VLAN インターフェイスに接続して CPU へのトラフィックをフィルタリングします。
- 次の QoS 機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
  - ポリシー マップ
  - ポリシングおよびマーキング
  - マッピング テーブル
  - WTD

QoS の概要

QoS の実装

ネットワークは通常、ベストエフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、正しいタイミングで配信される可能性も同じです。輻輳が発生すると、すべてのトラフィックが等しくドロップされます。

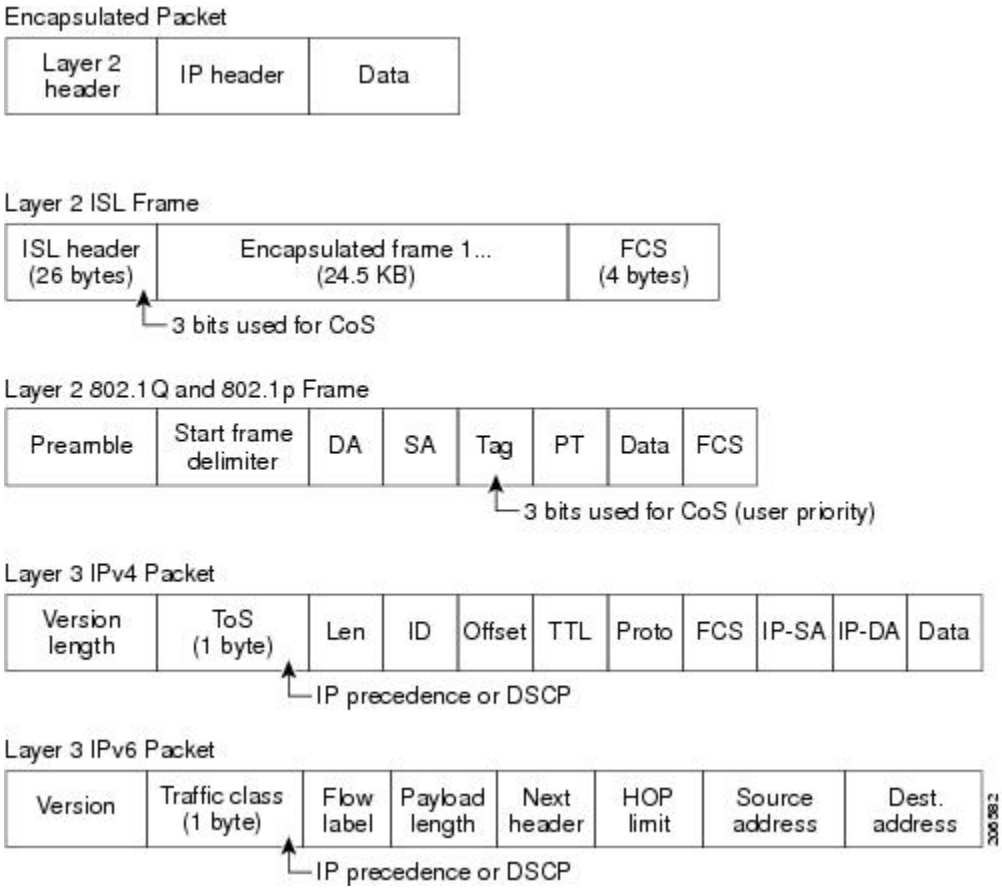
QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、相対的な重要性に応じてそのトラフィックに優先度を指定し、輻輳管理および輻輳回避技術を使用して、優先処理を実行できます。 ネットワークに QoS を実装すると、ネットワーク パフォーマンスがさらに予測しやすくなり、帯域幅をより効率的に利用できるようになります。

QoS は、インターネット技術特別調査委員会（IETF）の規格である Differentiated Services（Diff-Serv）アーキテクチャに基づいて実装されます。 このアーキテクチャでは、ネットワークに入るときに各パケットを分類することが規定されています。

この分類はIPパケットヘッダーに格納され、推奨されないIPタイプオブサービス（ToS）フィールドの 6 ビットを使用して、分類（クラス）情報として伝達されます。 分類情報をレイヤ 2 フレームでも伝達できます。

次の図にレイヤ 2 フレームまたはレイヤ 3 パケットの特殊ビットを示します。

図 *58*：フレームおよびパケットにおける *QoS* 分類レイヤ



レイヤ 2 フレームのプライオリティ ビット

レイヤ 2 の ISL（スイッチ間リンク）フレーム ヘッダーには、下位 3 ビットで IEEE 802.1p サービス クラス（CoS）値を伝達する 1 バイトのユーザ フィールドがあります。 レイヤ 2 ISL トランクとして設定されたポートでは、すべてのトラフィックが ISL フレームに収められます。

レイヤ 2 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット（ユーザ プライオリティ ビット）で CoS 値が伝達されます。 レイヤ 2 802.1Q トランクとして設定されたポートでは、ネイティブ Virtual LAN（VLAN）のトラフィックを除くすべてのトラフィックが 802.1Q フレームに収められます。

他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。

レイヤ 2 CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

レイヤ 3 パケットのプライオリティ ビット

レイヤ 3 IP パケットは、IP precedence 値または Diffserv コード ポイント（DSCP）値のいずれかを伝送できます。 DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値も使用できます。

IP precedence 値の範囲は 0 ～ 7 です。 DSCP 値の範囲は 0 ～ 63 です。

分類を使用したエンドツーエンドの QoS ソリューション

インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。 パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンド ホストが割り当てるか、または伝送中にスイッチまたはルータで割り当てることができます。 パケットの詳細な検証は、コア スイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィック クラスに割り当てるリソースの量を制限できます。 Diff-Serv アーキテクチャでトラフィックを処理するときの、各デバイスの動作をホップ単位動作といいます。 パス上のすべてのデバイスに一貫性のあるホップ単位動作をさせることによって、エンドツーエンドの QoS ソリューションを構築できます。

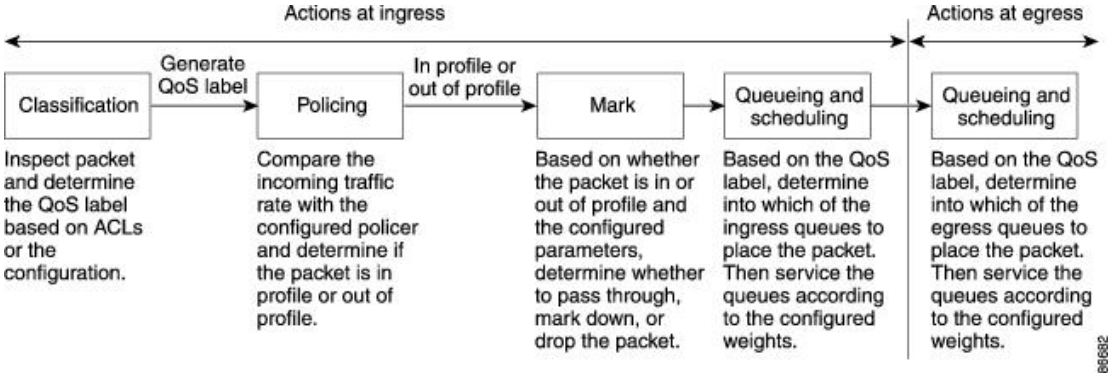
ネットワーク上で QoS を実装する作業は、インターネットワーキング デバイスが提供する QoS 機能、ネットワークのトラフィック タイプおよびパターン、さらには着信および発信トラフィックに求める制御のきめ細かさによって、簡単にも複雑にもなります。

QoS 基本モデル

QoS を実装するには、スイッチ上でパケットまたはフローを相互に区別し（分類）、パケットがスイッチを通過するときに所定の QoS を表すラベルを割り当て、設定されたリソース使用率制限にパケットを適合させ（ポリシングおよびマーキング）、リソース競合が発生する状況に応じて異なる処理（キューイングおよびスケジューリング）を行う必要があります。 また、スイッチか

ら送信されたトラフィックが特定のトラフィック プロファイルを満たすようにする必要もあります（シェーピング）。

図 *59*： ***QoS*** 基本有線モデル



入力ポートでのアクション

入力ポートでのアクションには、トラフィックの分類、ポリシング、マーキング、およびスケジューリングがあります。

- パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。 スイッチはパケット内の CoS または DSCP を QoS ラベルにマッピングして、トラフィックの種類を区別します。 生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを識別します。
- ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。 ポリサーは、トラフィック フローで消費される帯域幅を制限します。 その判別結果がマーカーに渡されます。
- マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットの QoS ラベルをマークダウンするか、またはパケットをドロップするか）を決定します。

（注） キューイングおよびスケジューリングは、スイッチの出力でのみサポートされ、入力ではサポートされません。

出力ポートでのアクション

出力ポートでのアクションには、キューイングおよびスケジューリングがあります。

- 4 つの出力キューのどれを使用するかを選択する前に、キューイングでは、QoS パケット ラベルおよび対応する DSCP または CoS 値を評価します。 複数の入力ポートが 1 つの出力ポートに同時にデータを送信すると輻輳が発生することがあるため、WTD を使用してトラフィッ

ク クラスを区別し、QoS ラベルに基づいてパケットに別々のしきい値を適用します。 しきい値を超過している場合、パケットはドロップされます。

- スケジューリングでは、設定されている SRR の共有重みまたはシェーピング重みに基づいて、4 つの出力キューを処理します。 キューの 1 つ（キュー 1）は、他のキューの処理前に空になるまで処理される緊急キューにできます。

分類の概要

分類とは、パケットのフィールドを検証して、トラフィックの種類を区別するプロセスです。 QoS がスイッチ上でグローバルにイネーブルになっている場合のみ、分類はイネーブルです。 デフォルトでは、QoS はグローバルにディセーブルになっているため、分類は実行されません。

分類中に、スイッチは検索処理を実行し、パケットに QoS ラベルを割り当てます。 QoS ラベルは、パケットに対して実行するすべての QoS アクション、およびパケットの送信元キューを識別します。

QoS ラベルは、パケット内の DSCP または CoS 値に基づいて、パケットに実行されるキューイングおよびスケジューリング アクションを決定します。 QoS ラベルは信頼設定およびパケット タイプに従ってマッピングされます（分類フローチャート，（741 ページ）を参照）。

着信トラフィックの分類に、フレームまたはパケットのどのフィールドを使用するかは、ユーザ側で指定します。

関連トピック

入力ポートのアクティビティ
出力ポートのアクティビティ
QoS ポリシーの設定，（777 ページ）

Non-IP のトラフィック分類

次の表は、QoS 設定の非 IP トラフィックの分類オプションを示しています。

表 *59*：非 *IP* トラフィックの分類

Non-IP のトラフィック分類	説明
CoS 値の信頼	着信フレーム内の CoS 値を信頼し（CoS を信頼するようにポートを設定）、設定可能な CoS/DSCP マップを使用してパケットの DSCP 値を生成します。 レイヤ 2 の ISL フレーム ヘッダーは、1 バイトのユーザ フィールドの下位 3 ビットで CoS 値を伝達します。 レイヤ 2 802.1Q フレームのヘッダーは、タグ制御情報フィールドの上位 3 ビットで CoS 値を伝達します。CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

Non-IP のトラフィック分類	説明
DSCP を信頼するか、または IP precedence 値を信頼します。	着信フレームの DSCP または IP precedence 値を信頼します。 これらの設定は、非 IP トラフィックの場合は無意味です。 これらのいずれかの方法で設定されているポートに非 IP トラフィックが着信した場合は、CoS 値が割り当てられ、CoS/DSCP マップから内部 DSCP 値が生成されます。 スイッチは内部 DSCP 値を使用して、トラフィックのプライオリティを表示する CoS 値を生成します。
設定されたレイヤ 2 の MAC ACL に基づいた分類	設定されたレイヤ 2 の MAC アクセス コントロール リスト（ACL）に基づいて分類を実行します。レイヤ 2 の MAC ACL は、MAC 送信元アドレス、MAC 宛先アドレス、およびその他のフィールドを調べることができます。 ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。 ACL が設定されている場合は、ポリシーマップ アクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

分類されたパケットは、ポリシングおよびマーキングの各段階に送られます。

IP のトラフィック分類

次の表は、QoS 設定の IP トラフィック分類オプションを示します。

表 *60*：*IP* のトラフィック分類

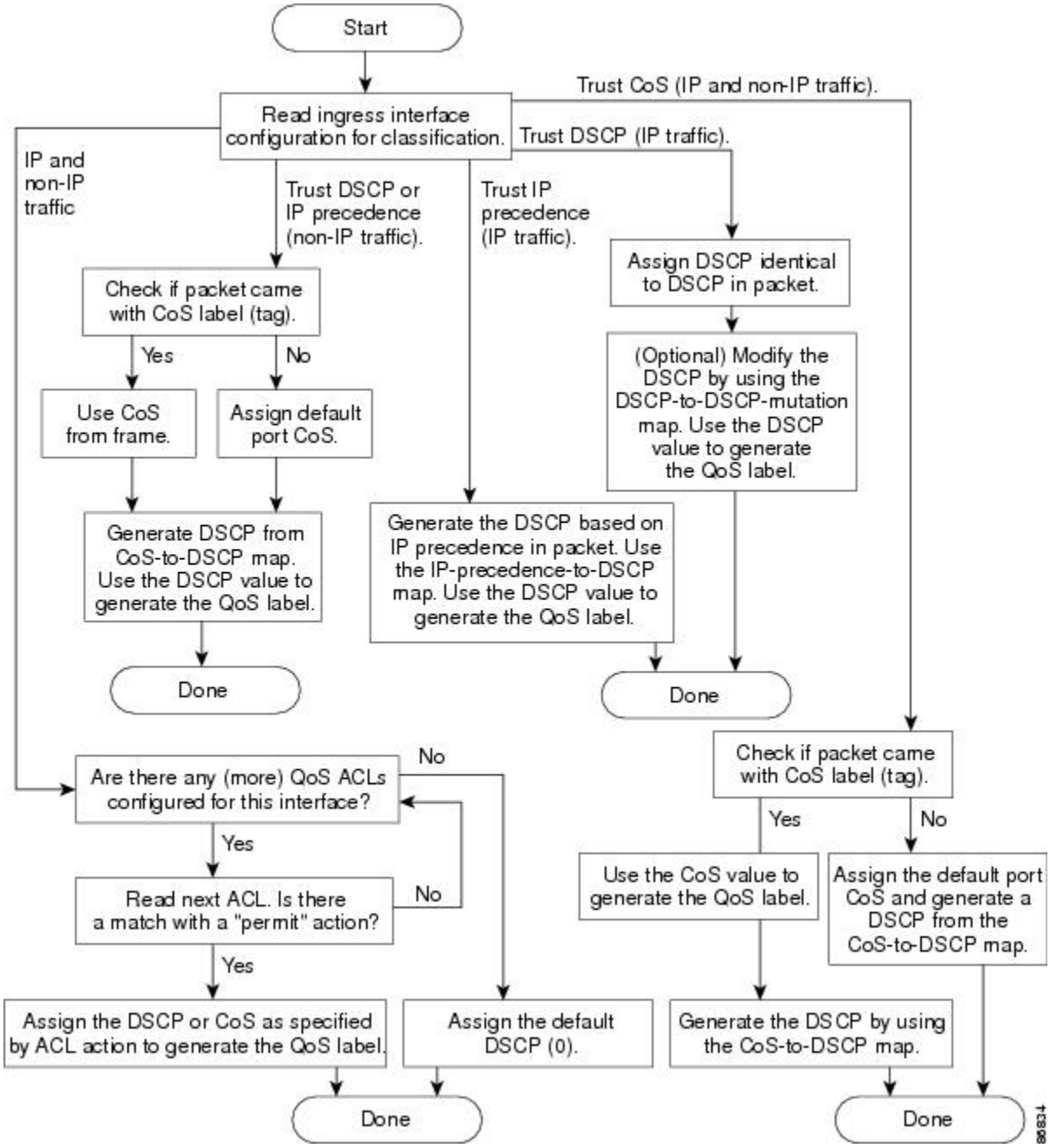
IP のトラフィック分類	説明
DSCP 値の信頼	着信パケットの DSCP 値を信頼し（DSCP を信頼するようにポートを設定し）、同じ DSCP 値をパケットに割り当てます。 IETF は、1 バイトの ToS フィールドの上位 6 ビットを DSCP として定義しています。 特定の DSCP 値が表すプライオリティは、設定可能です。 DSCP 値の範囲は 0 ～ 63 です。 また IPv6 DSCP に基づいて IP トラフィックを分類することもできます。 2 つの QoS 管理ドメインの境界上にあるポートの場合は、設定可能な DSCP/DSCP 変換マップを使用して、DSCP を別の値に変更できます。

IP のトラフィック分類	説明
IP precedence 値の信頼	着信パケットの IP precedence 値を信頼し（IP precedence を信頼するようにポートを設定し）、設定可能な IP precedence/DSCP マップを使用してパケットの DSCP 値を生成します。 IP バージョン 4 仕様では、1 バイトの ToS フィールドの上位 3 ビットが IP precedence として定義されています。 IP precedence 値の範囲は 0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。 また IPv6 precedence に基づいて IP トラフィックを分類することもできます。
CoS 値の信頼	着信パケットに CoS 値がある場合には、その CoS 値を信頼し、CoS/DSCP マップを使用してパケットの DSCP 値を生成します。 CoS 値が存在しない場合は、デフォルトのポート CoS 値を使用します。
IP 標準または拡張 ACL	設定された IP 標準 ACL または IP 拡張 ACL（IP ヘッダーの各フィールドを調べる）に基づいて、分類を実行します。 ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。 ACL が設定されている場合は、ポリシーマップ アクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。
設定された CoS の上書き	着信パケットに設定された CoS を上書きし、デフォルトのポート CoS 値を適用します。 IPv6 パケットの場合、DSCP 値は CoS/DSCP マップとポートのデフォルトの CoS を使用して書き換えられます。 これは、IPv4 と IPv6 の両方のトラフィックに対して実行できます。

分類されたパケットは、ポリシングおよびマーキングの各段階に送られます。

分類フローチャート

図 *60*：分類フローチャート



アクセス コントロール リスト

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用すると、同じ特性を備えたパケットグループ（クラス）を定義できます。 また IPv6 ACL に基づいて IP トラフィックを分類することもできます。

QoS のコンテキストでは、アクセス コントロール エントリ（ACE）の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なります。

- 許可アクションとの一致が検出されると（最初の一致の原則）、指定の QoS 関連アクションが実行されます。
- 拒否アクションと一致した場合は、処理中の ACL がスキップされ、次の ACL が処理されます。
- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットでは QoS 処理は実行されず、スイッチによってベストエフォート型サービスが実行されます。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの一致が見つかると、それ以降の検索処理は中止され、QoS 処理が開始されます。

（注） アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

ACL でトラフィック クラスを定義した後で、そのトラフィック クラスにポリシーを結合できます。 ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。 ポリシーには、特定の集約としてクラスを分類する（DSCP を割り当てるなど）コマンドまたはクラスのレート制限を実施するコマンドを含めることができます。 このポリシーを特定のポートに結合すると、そのポートでポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類する場合は、**access-list** グローバル コンフィギュレーション コマンドを使用します。 レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

IPv4 トラフィック用の IP 標準 ACL の作成, （778 ページ）

IPv4 トラフィック用の IP 拡張 ACL の作成, （779 ページ）

IPv6 トラフィック用の IPv6 ACL の作成, （781 ページ）

非 IP トラフィック用のレイヤ 2 MAC ACL の作成, （784 ページ）

クラス マップおよびポリシー マップに基づく分類

ポリシーマップを使用するには、スイッチが LAN Base イメージを実行している必要があります。

クラスマップは、特定のトラフィック フロー（またはクラス）に名前を付けて、他のすべてのトラフィックと区別するためのメカニズムです。 クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。 この条件には、ACL で定義されたアクセス グループとの照合、または DSCP 値や IP precedence 値の特定のリストとの照合を含めることができます。 複数のトラフィック タイプを分類する場合は、別のクラスマップを作成し、異なる名前を使用できます。 パケットをクラス マップ条件と照合した後で、ポリシー マップを使用してさらに分類します。

ポリシー マップでは、作用対象のトラフィック クラスを指定します。 トラフィック クラスの CoS、DSCP、または IP precedence 値を信頼するアクションや、トラフィック クラスに特定の DSCP または IP precedence 値を設定するアクション、またはトラフィック帯域幅の制限やトラフィックが不適合な場合の対処法を指定するアクションなどを指定できます。 ポリシーマップを効率的に機能させるには、ポートにポリシー マップを結合する必要があります。

クラス マップを作成するには、**class-map** グローバル コンフィギュレーション コマンドまたは **class** ポリシー マップ コンフィギュレーション コマンドを使用します。 多数のポート間でマップを共有する場合には、**class-map** コマンドを使用する必要があります。 **class-map** コマンドを入力すると、クラス マップ コンフィギュレーション モードが開始されます。 このモードで、**match** クラス マップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

class class-default ポリシー マップ コンフィギュレーション コマンドを使用して、デフォルト クラスを設定できます。 分類されていないトラフィック（ポリシー マップで設定された他のトラフィック クラスで指定されているトラフィック）は、デフォルト トラフィックとして処理されます。

ポリシーマップは、**policy-map** グローバル コンフィギュレーション コマンドを使用して作成し、名前を付けます。 このコマンドを入力すると、ポリシー マップ コンフィギュレーション モードが開始されます。 このモードでは、**class**、**trust**、または **set** ポリシー マップ コンフィギュレーション コマンドおよびポリシー マップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行するアクションを指定します。

ポリシー マップには、ポリサー、トラフィックの帯域幅限度、および限度を超えた場合のアクションを定義する **police** および **police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを含めることもできます。

ポリシーマップをイネーブルにするには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用してポートにマップを結合します。

ポリシングおよびマーキングの概要

パケットを分類し、DSCP または CoS に基づいて QoS ラベルを割り当てたあとで、ポリシングおよびマーキング プロセスを開始できます。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。 制限を超えるパケットは、「アウト オブ プロファイル」または「不適合」になります。 各ポリサーはパケットごとに、パケットが適合か不適合かを判別し、パケットに対するアクションを指定します。 これらのアクションはマーカーによって実行されます。パケットを変更しないで通過させるアクション、パケットをドロップするアクション、またはパケットに割り当てられた DSCP 値を変更（マークダウン）してパケットの通過を許可するアクションなどがあります。 設定可能なポリシング済み DSCP マップを使用すると、パケットに新しい DSCP ベース QoS ラベルが設定されます。 マークダウンされたパケットは、元の QoS ラベルと同じキューを使用して、フロー内のパケットの順番が崩れないようにします。

（注） すべてのトラフィックは、ブリッジングされるかルーティングされるかに関係なく、ポリサーの影響を受けます（ポリサーが設定されている場合）。その結果、ブリッジングされたパケットは、ポリシングまたはマーキングが行われたときにドロップされたり、DSCP または CoS フィールドが変更されたりすることがあります。

ポリシングは物理ポートに対して設定できます。 ポリシー マップおよびポリシング アクションを設定した後で、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、ポリシーを統合します。

関連トピック

入力ポートのアクティビティ
クラス マップ
ポリシー マップ
QoS ポリシーの設定, （777 ページ）
ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング, （791 ページ）
階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング
集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング, （796 ページ）

物理ポートのポリシング

物理ポートのポリシー マップでは、次のポリサー タイプを作成できます。

- Individual：QoS はポリサーに指定された帯域幅限度を、一致したトラフィック クラスごとに別々に適用します。 このタイプのポリサーは、**police** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップの中で設定します。
- Aggregate：QoS はポリサーで指定された帯域幅限度を、一致したすべてのトラフィック フローに累積的に適用します。 このタイプのポリサーは、**police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップ内で集約ポリサー名を指定することにより設定します。 ポリサーの帯域幅限度を指定するには、**mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。 このようにして、集約ポリサーはポリシー マップ内にある複数のトラフィック クラスで共有されます。

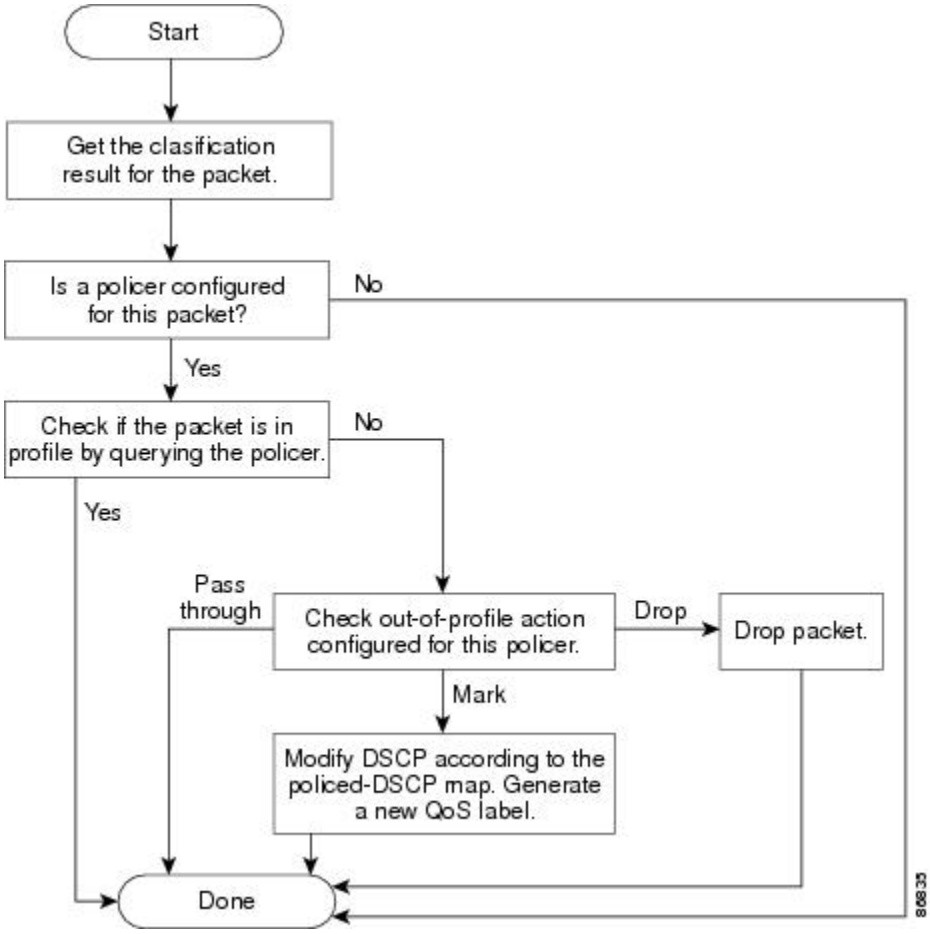
ポリシングはトークンバケット アルゴリズムを使用します。 各フレームがスイッチに着信すると、バケットにトークンが追加されます。バケットにはホールがあり、平均トラフィック レートとして指定されたレート（ビット/秒）で送信されます。 バケットにトークンが追加されるたびに、スイッチは、バケット内に十分なスペースがあるかを確認します。 十分なスペースがなければ、パケットは不適合とマーキングされ、指定されたポリサー アクション（ドロップまたはマークダウン）が実行されます。

バケットが満たされる速度は、バケット深度（burst-byte）、トークンが削除されるレート（rate-bps）、および平均レートを上回るバースト期間によって決まります。 バケットのサイズによってバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バースト期間が短い場合、バケットはオーバーフローせず、トラフィック フローに何のアクショ

ンも実行されません。 ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシング アクションが実行されます。

バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの burst-byte オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。 トークンがバケットから削除される速度（平均速度）を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの *rate-bps* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。

図 *61*：物理ポートのポリシングおよびマーキング フローチャート



関連トピック

ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング，（791 ページ）

マッピング テーブルの概要

QoS を処理している間、すべてのトラフィック（非 IP トラフィックを含む）のプライオリティは、分類段階で取得された DSCP または CoS 値に基づいて、QoS ラベルで表されます。

次の表は、QoS 処理とマッピング テーブルについて説明しています。

表 *61*：*QoS* 処理およびマッピング テーブル

QoS 処理段階	マッピング テーブルの使用
分類	分類段階で、QoS は設定可能なマッピング テーブルを使用して、受信された CoS、DSCP、または IP precedence 値から、対応する DSCP または CoS 値を取得します。 これらのマップには、CoS/DSCP マップや IP precedence/DSCP マップなどがあります。 これらのマップを設定するには、**mls qos map cos-dscp** および **mls qos map ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。 DSCP 信頼状態で設定された入力ポートの DSCP 値が QoS ドメイン間で異なる場合は、2 つの QoS ドメイン間の境界にあるポートに、設定可能な DSCP/DSCP 変換マップを適用できます。 このマップを設定するには、**mls qos map dscp-mutation** グローバル コンフィギュレーション コマンドを使用します。
ポリシング	ポリシング段階で、QoS は IP パケットまたは非 IP パケットに別の DSCP 値を割り当てることができます（パケットが不適合で、マークダウン値がポリサーによって指定されている場合）。 この設定可能なマップは、ポリシング済み DSCP マップといいます。 このマップを設定するには、**mls qos map policed-dscp** グローバル コンフィギュレーション コマンドを使用します。
プレスケジュール	トラフィックがスケジューリング段階に達する前に、QoS は QoS ラベルに従って、出力キューにパケットを格納します。 QoS ラベルはパケット内の DSCP または CoS 値に基づいており、DSCP 出力キューしきい値マップまたは CoS 出力キューしきい値マップを使用してキューを選択します。 出力のキューに加えて、QOS ラベルは WTD しきい値も識別します。 これらのマップを設定するには、**mls qos srr-queue** { **output**} **dscp-map** および **mls qos srr-queue** { **output**} **cos-map** グローバル コンフィギュレーション コマンドを使用します。

CoS/DSCP、DSCP/CoS、および IP precedence/DSCP マップのデフォルト値は、使用しているネットワークに適する場合と適さない場合があります。

デフォルトの DSCP/DSCP 変換マップおよびデフォルトのポリシング済み DSCP マップは、空のマップです。これらのマップでは、着信した DSCP 値が同じ DSCP 値にマッピングされます。

DSCP/DSCP 変換マップは、特定のポートに適用できる唯一のマップです。 その他のすべてのマップはスイッチ全体に適用されます。

関連トピック

DSCP マップの設定, （799 ページ）

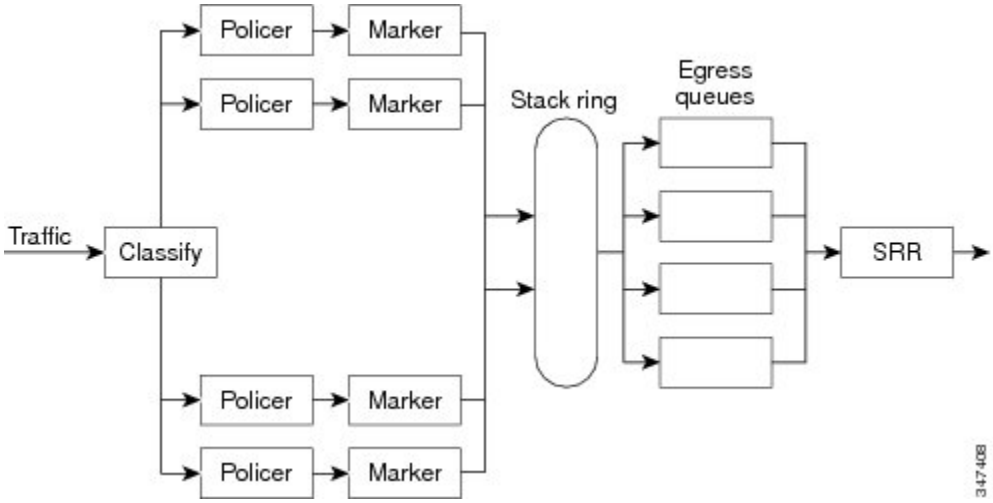
入力キューでのキューイングおよびスケジューリング

出力キューでのキューイングおよびスケジューリング

キューイングおよびスケジューリングの概要

スイッチは、輻輳を防ぐために特定の場所にキューがあります。

図 *62*：スイッチの出力キューの位置



（注） スイッチはデフォルトで 4 つの出力キューをサポートしますが、合計 8 つの出力キューを有効にするオプションがあります。 8 出力キューの設定はスタンドアロン スイッチでのみサポートされます。

WTD

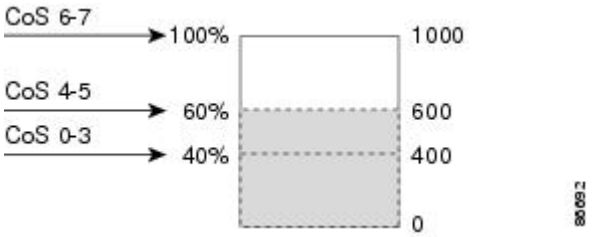
出力キューは、重み付けテール ドロップ（WTD）と呼ばれるテール ドロップ輻輳回避メカニズムの拡張バージョンを使用します。 WTD はキュー長を管理したり、トラフィック分類ごとにドロップ優先順位を設定したりするために実装されています。

フレームが特定のキューにキューイングされると、WTD はフレームに割り当てられた QoS ラベルを使用して、それぞれ異なるしきい値を適用します。 この QoS ラベルのしきい値を超えると（宛先キューの空きスペースがフレーム サイズより小さくなると）、フレームはドロップされます。

各キューには 3 つのしきい値があります。 QoS ラベルは、3 つのしきい値のうちのどれがフレームの影響を受けるかを決定します。 3 つのしきい値のうち、2 つは設定可能（明示的）で、1 つは設定不可能（暗示的）です。

次の図は、サイズが 1000 フレームであるキューでの WTD の動作の例を示しています。 ドロップ割合は次のように設定されています。40%（400 フレーム）、60%（600 フレーム）、および 100%（1000 フレーム）です。 これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレームをキューイングできるという意味です。

図 *63*：*WTD* およびキューの動作



この例では、CoS 値 6 および 7 は他の CoS 値よりも重要度が高く、100% ドロップしきい値に割り当てられます（キューフル ステート）。 CoS 値 4 および 5 は 60% しきい値に、CoS 値 0 ～ 3 は 40% しきい値に割り当てられます。

600 個のフレームが格納されているキューに、新しいフレームが着信したとします。 このフレームの CoS 値は 4 および 5 で、60% のしきい値が適用されます。 このフレームがキューに追加されると、しきい値を超過するため、フレームは廃棄されます。

関連トピック

入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定, （808 ページ）

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定, （816 ページ）

出力キューおよびしきい値 ID への DSCP または CoS 値のマッピング, （820 ページ）

WTD しきい値, （751 ページ）

キューおよび WTD しきい値, （754 ページ）

SRR のシェーピングおよび共有

出力キューはシェーピング ラウンド ロビン（SRR）で処理され、SRR によってパケットの送信レートが制御されます。 出力キューでは、SRR によってパケットが出力ポートに送信されます。

出力キューでは、SRR を共有またはシェーピング用に設定できます。

シェーピング モードでは、出力キューの帯域幅割合が保証され、この値にレートが制限されます。 リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を超えて使用できません。 シェーピングを使用すると、時間あたりのトラフィック フローがより均一になり、バースト トラフィックの最高時と最低時を削減します。 シェーピングの場合は、各重みの絶対値を使用して、キューに使用可能な帯域幅が計算されます。

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。 このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。 たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有できます。 共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。 シェーピングおよび共有は、インターフェイスごとに設定されます。 各インターフェイスは、一意に設定できます。

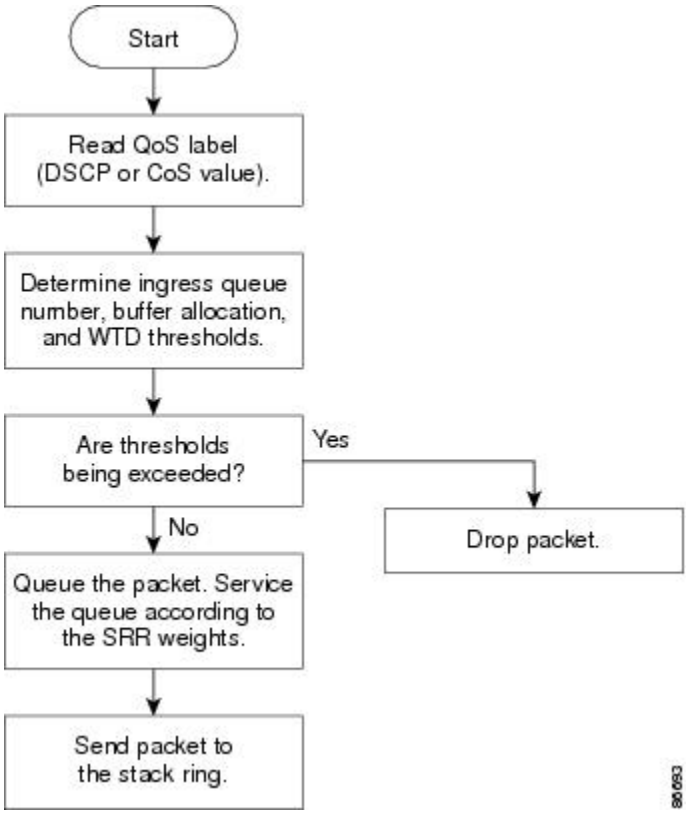
関連トピック

入力ポートのアクティビティ
入力キュー間の帯域幅の割り当て, （812 ページ）
出力キューでの SRR シェーピング重みの設定, （822 ページ）
出力キューでの SRR 共有重みの設定, （824 ページ）
シェーピング モードまたは共有モード, （755 ページ）

入力キューでのキューイングおよびスケジューリング

次の図は、スイッチの入力ポートのキューイングおよびスケジューリングのフロー チャートを示しています。

図 *64*：スイッチの入力ポートのキューイングおよびスケジューリング フロー チャート



（注） 共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

設定可能な入力キュー タイプ

スイッチは、共有モードの SRR によってのみ処理される、2 つのタイプの設定可能な入力キューをサポートしています。

（注） スイッチも、設定不可能なトラフィック用キューが 2 つ使用されます。これらのキューは、ネットワークおよびスタックを適切に動作させるために重要です。

次の表に、これら 2 つの設定可能な入力キューの説明を示します。

表 *62*：設定可能な入力キュー タイプ

キュー タイプ	機能
標準	標準プライオリティと見なされるユーザ トラフィック。 各フローを区別するために、3 つの異なるしきい値を設定できます。 次のグローバル コンフィギュレーション コマンドを使用します。 • **mls qos srr-queue input threshold** • **mls qos srr-queue input dscp-map** • **mls qos srr-queue input cos-map**
緊急	Differentiated Services（DF）緊急転送または音声トラフィックなどのハイプライオリティ ユーザ トラフィック。 このトラフィックに必要な帯域幅は、**mls qos srr-queue input priority-queue** グローバル コンフィギュレーション コマンドを使用して、スイッチ上のトラフィック合計またはスタック トラフィック合計の割合として設定できます。 緊急キューには帯域幅が保証されています。

キューおよびしきい値にスイッチを通過する各パケットを割り当てます。 特に、入力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。 **mls qos srr-queue input dscp-map queue queue-id** {*dscp1...dscp8* | **threshold threshold-id** *dscp1...dscp8*} または **mls qos srr-queue input cos-map queue queue-id** {*cos1...cos8* | **threshold threshold-id** *cos1...cos8*} グローバル コンフィギュレーション コマンドを使用します。 DSCP 入力キューしきい値マップおよび CoS 入力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

WTD しきい値

キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能（明示的）な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能（暗示的）なしきい値です。

入力キューに 2 つの明示的 WTD しきい値の割合（しきい値 ID 1 および ID 2 用）を割り当てるには、**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2* グローバル コンフィギュレーション コマンドを使用します。 各しきい値は、キューに割り当てられたバッファの合計値に対する割合です。 しきい値 ID 3 のドロップしきい値は、キューフル ステートに設定済みで、変更できません。

関連トピック

WTD, （747 ページ）

バッファおよび帯域幅の割り当て

2 つのキュー間の入力バッファを分割する比率を定義する（スペース量を割り当てる）には、**mls qos srr-queue input buffers** *percentage1 percentage2* グローバル コンフィギュレーション コマンドを使用します。 バッファ割り当てと帯域幅割り当てを組み合わせることにより、パケットがドロップされる前にバッファに格納して送信できるデータ量が制御されます。 帯域幅を割合として割り当てるには、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドを使用します。 重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

プライオリティ キューイング

1 つの入力キューをプライオリティ キューとして設定するには、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドを使用します。 プライオリティ キューはスタックまたは内部リングの負荷にかかわらず帯域幅の一部が保証されているため、確実な配信を必要とするトラフィック（音声など）に使用する必要があります。

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューを処理します。 次に、SRR は **mls qos srr-queue input bandwidth** *weight1 weight2* グローバルコンフィギュレーションコマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

上記のコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。

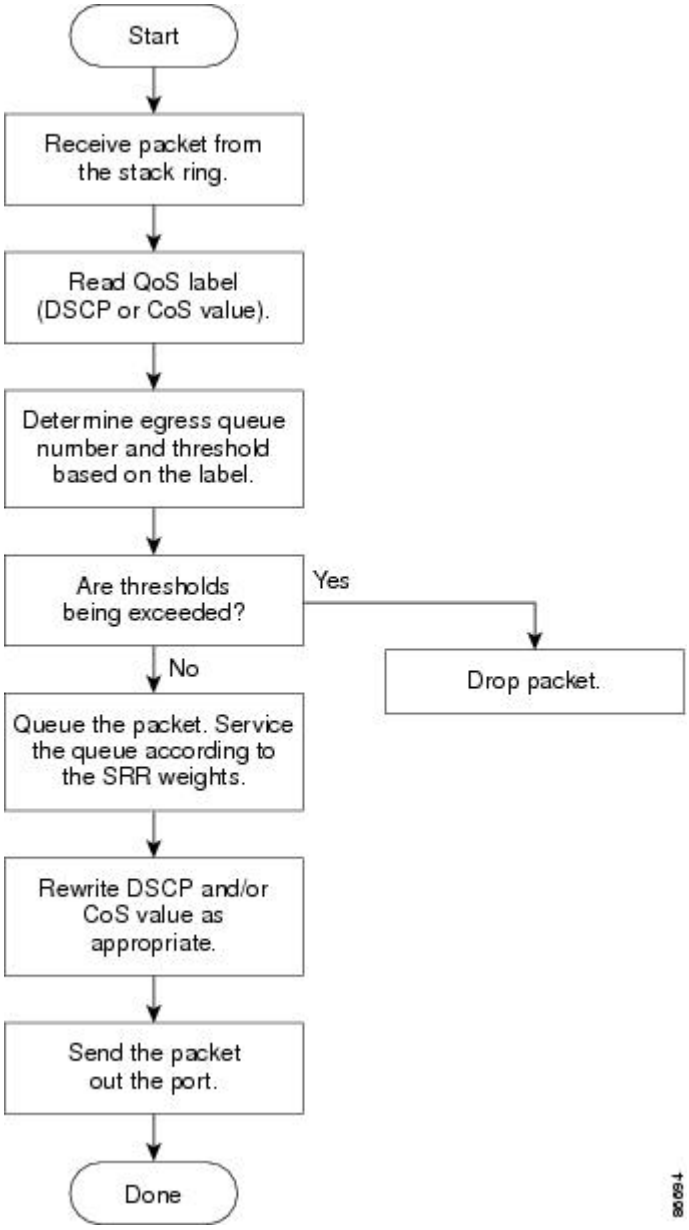
関連トピック

入力キューの特性の設定, （807 ページ）

出力キューでのキューイングおよびスケジューリング

次の図は、スイッチの出力ポートのキューイングおよびスケジューリングのフロー チャートを示しています。

図 *65* : スイッチの出力ポートのキューイングおよびスケジューリング フロー チャート



（注） 緊急キューがイネーブルの場合、SRRによって空になるまで処理されてから、他の3つのキューが処理されます。

出力緊急キュー

各ポートは、そのうち1つ（キュー1）を出力緊急キューにできる、4つの出力キューをサポートしています。 これらのキューはキューセットに割り当てられます。 スイッチに存在するすべてのトラフィックは、パケットに割り当てられたQoSラベルに基づいて、これらの4つのキューのいずれかを通過し、しきい値の影響を受けます。

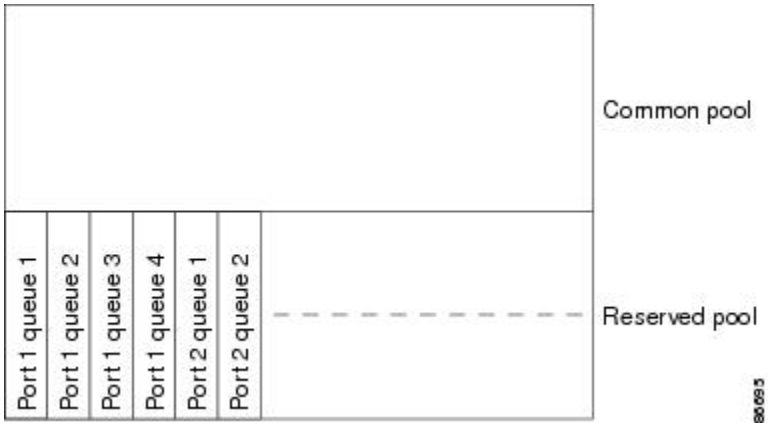
（注） 緊急キューがイネーブルの場合、SRRによって空になるまで処理されてから、他の3つのキューが処理されます。

出力キューのバッファ割り当て

次の図は、出力キューのバッファを示しています。

バッファスペースは共通プールと専用プールで構成されます。 スイッチはバッファ割り当て方式を使用して、出力キューごとに最小バッファサイズを確保します。 これにより、いずれかのキューまたはポートがすべてのバッファを消費して、その他のキューのバッファが不足することがなくなり、要求元のキューにバッファスペースを割り当てるかどうかが制御されます。 スイッチは、ターゲットキューが予約量を超えるバッファを消費していないかどうか（アンダーリミット）、その最大バッファをすべて消費したかどうか（オーバーリミット）、共通のプールが空（空きバッファがない）か空でない（空きバッファ）かを判断します。 キューがオーバーリミットでない場合は、スイッチは予約済みプールまたは共通のプール（空でない場合）からバッファスペースを割り当てることができます。 共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームをドロップします。

図 *66*：出力キューのバッファ割り当て



バッファおよびメモリの割り当て

バッファのアベイラビリティの保証、ドロップしきい値の設定、およびキューセットの最大メモリ割り当ての設定を行うには、**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* グローバル コンフィギュレーション コマンドを使用します。 各しきい値はキューに割り当てられたメモリの割合です。このパーセント値を指定するには、**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* グローバル コンフィギュレーションコマンドを使用します。割り当てられたすべてのバッファの合計が専用プールになります。残りのバッファは共通プールの一部になります。

バッファ割り当てを行うと、ハイプライオリティ トラフィックを確実にバッファに格納できます。 たとえば、バッファ スペースが 400 の場合、バッファ スペースの 70% をキュー 1 に割り当てて、10% をキュー 2 ～ 4 に割り当てることができます。 キュー 1 には 280 バッファが割り当てられ、キュー 2 ～ 4 にはそれぞれ 40 バッファが割り当てられます。

割り当てられたバッファをキューセット内の特定のキュー用に確保するよう保証できます。 たとえば、キュー用として 100 バッファがある場合、50%（50 バッファ）を確保できます。 残りの 50 バッファは共通プールに戻されます。 また、最大しきい値を設定することにより、いっぱいになったキューが確保量を超えるバッファを取得できるようにすることもできます。 共通プールが空でない場合、必要なバッファを共通プールから割り当てることができます。

（注） スイッチはデフォルトで 4 つの出力キューをサポートしますが、合計 8 つの出力キューをイネーブルにするオプションがあります。 8 つの出力キューをすべてイネーブルにするには、**mls qos srr-queue output queues 8** グローバル コンフィギュレーション コマンドを使用します。 8 出力キューがイネーブルになったら、8 つすべてのキューのしきい値およびバッファを設定できます。 8 出力キューの設定はスタンドアロン スイッチでのみサポートされます。

キューおよび *WTD* しきい値

スイッチを通過する各パケットをキューおよびしきい値に割り当てることができます。

特に、出力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。 **mls qos srr-queue output dscp-map queue** *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*} または **mls qos srr-queue output cos-map queue** *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*} グローバル コンフィギュレーション コマンドを使用します。 DSCP 出力キューしきい値マップおよび CoS 出力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。 各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能（明示的）な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能（暗示的）なしきい値です。 しきい値 ID 1 および ID 2 用の 2 つの WTD しきい値割合を割り当てます。 しきい値 ID 3 のドロップしきい値は、キューフルステートに設定済みで、変更できません。 キューセットにポートをマッピングするには、**queue-set qset-id** インターフェイス コンフィギュレーション コマンドを使用します。 WTD しきい値の割合を変更するには、キューセット設定を変更します。

（注） スイッチはデフォルトで 4 つの出力キューをサポートしますが、合計 8 つの出力キューをイネーブルにするオプションがあります。 8 つの出力キューをすべてイネーブルにするには、**mls qos srr-queue output queues 8** グローバル コンフィギュレーション コマンドを使用します。 8 出力キューがイネーブルになったら、8 つすべてのキューのしきい値およびバッファを設定できます。 8 出力キューの設定はスタンドアロン スイッチでのみサポートされます。

関連トピック

WTD, （747 ページ）

シェーピング モードまたは共有モード

SRR は、シェーピング モードまたは共有モードでキューセットを処理します。 キューセットにポートをマッピングするには、**queue-set** *qset-id* インターフェイス コンフィギュレーション コマンドを使用します。 ポートに共有重みまたはシェーピング重みを割り当てるには、**srr-queue bandwidth share** *weight1 weight2 weight3 weight4* または **srr-queue bandwidth shape** *weight1 weight2 weight3 weight4* インターフェイス コンフィギュレーション コマンドを使用します。

バッファ割り当てと SRR 重み比率を組み合わせることにより、パケットがドロップされる前にバッファに格納して送信できるデータ量が制御されます。 重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

緊急キューがイネーブルでない限り、4 つのキューはすべて SRR に参加し、この場合、1 番めの帯域幅重みは無視されて比率計算に使用されません。 緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。 緊急キューをイネーブルにするには、**priority-queue out** インターフェイス コンフィギュレーション コマンドを使用します。

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。 出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

（注） スイッチはデフォルトで 4 つの出力キューをサポートしますが、合計 8 つの出力キューをイネーブルにするオプションがあります。 8 つの出力キューをすべてイネーブルにするには、**mls qos srr-queue output queues 8** グローバル コンフィギュレーション コマンドを使用します。 8 つの出力キューがイネーブルになると、8 つすべてのキューのしきい値、バッファ、帯域幅の共有重みおよび帯域幅シェーピング重みを設定できます。 8出力キューの設定はスタンドアロン スイッチでのみサポートされます。

関連トピック

出力キューの特性の設定，（815 ページ）

SRR のシェーピングおよび共有，（748 ページ）

パケットの変更

QoS を設定するには、パケットの分類、ポリシング、キューイングを行います。 QoS を提供するプロセス中に次のパケットの変更が発生することがあります。

- IP パケットおよび非 IP パケットの分類では、受信パケットの DSCP または CoS に基づいて、パケットに QoS ラベルが割り当てられます。 ただし、この段階ではパケットは変更されません。割り当てられた DSCP または CoS 値の指定のみがパケットとともに伝達されます。
- ポリシング中は、IP および非 IP パケットに別の DSCP を割り当てることができます（これらのパケットが不適合で、ポリサーがマークダウン DSCP を指定している場合）。 この場合も、パケット内の DSCP は変更されず、マークダウン値の指定がパケットとともに伝達されます。 IP パケットの場合は、この後の段階でパケットが変更されます。非 IP パケットの場合は、DSCP が CoS に変換され、キューイングおよびスケジューリングの決定に使用されます。
- フレームに割り当てられた QoS ラベル、および選択された変換マップに応じて、フレームの DSCP および CoS 値が書き換えられます。 テーブルマップを設定しない場合、および着信フレームの DSCP を信頼するようにポートが設定されている場合、フレーム内の DSCP 値は変更されませんが、CoS は、DSCP/CoS マップに基づいて書き換えられます。 着信フレームの CoS を信頼するようにポートが設定されていて、着信フレームが IP パケットの場合、フレーム内の CoS 値は変更されないで、CoS/DSCP マップに従って DSCP が変更されることがあります。

  入力変換が行われると、選択された新しい DSCP 値に応じて DSCP が書き換えられます。 ポリシー マップの設定アクションによっても、DSCP が書き換えられます。

標準 QoS のデフォルト設定

標準 QoS はデフォルトでディセーブルになっています。

パケットが変更されないため、信頼できるポートまたは信頼できないポートといった概念はありません。 パケット内の CoS、DSCP、および IP precedence 値は変更されません。

トラフィックは Pass-Through モードでスイッチングされます。 パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます。

mls qos グローバル コンフィギュレーション コマンドを使用して QoS をイネーブルにし、その他のすべての QoS 設定がデフォルトである場合、トラフィックはポリシングを伴わないベストエフォート型として分類されます（DSCP および CoS 値は 0 に設定されます）。 ポリシー マップは設定されません。 すべてのポート上のデフォルト ポートの信頼性は、信頼性なし（untrusted）の状態です。

関連トピック

QoS のグローバルなイネーブル化, （764 ページ）
出力キューのデフォルト設定, （758 ページ）
入力キューのデフォルト設定, （757 ページ）

入力キューのデフォルト設定

次の表は、入力キューのデフォルト設定について説明しています。

次の表は、QoS がイネーブルの場合のデフォルトの入力キューの設定を示しています。 帯域幅割り当て機能では、帯域幅はキューに均等に分配されます。 SRR は共有モードでのみパケットを送信します。 キュー 2 はプライオリティ キューです。 共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

表 *63*：入力キューのデフォルト設定

機能	キュー 1	キュー 2
バッファ割り当て	90%	10%
帯域幅割り当て	4	4
プライオリティ キューの帯域幅	0	10
WTD ドロップしきい値 1	100%	100%
WTD ドロップしきい値 2	100%	100%

次の表は、QoS がイネーブルの場合のデフォルトの CoS 入力キューしきい値マップを示しています。

表 *64*：デフォルトの *CoS* 入力キューしきい値マップ

CoS 値	キュー ID-しきい値 ID
0 ～ 4	1 - 1
5	2 - 1
6、7	1 - 1

次の表は、QoS がイネーブルの場合のデフォルトの DSCP 入力キューしきい値マップを示しています。

表 *65*：デフォルトの *DSCP* 入力キューしきい値マップ

DSCP 値	キュー ID-しきい値 ID
0 ～ 39	1 - 1
40 ～ 47	2 - 1
48 ～ 63	1 - 1

関連トピック

QoS のグローバルなイネーブル化，（764 ページ）

標準 QoS のデフォルト設定，（756 ページ）

出力キューのデフォルト設定

次の表は、出力キューのデフォルト設定について説明しています。

（注） スイッチはデフォルトで 4 つの出力キューをサポートしますが、合計 8 つの出力キューをイネーブルにするオプションがあります。 8 つの出力キューをすべてイネーブルにするには、**mls qos srr-queue output queues 8** グローバル コンフィギュレーション コマンドを使用します。 8 出力キューがイネーブルになったら、8 つすべてのキューのしきい値およびバッファを設定できます。 8 出力キューの設定はスタンドアロン スイッチでのみサポートされます。

次の表は、QoS がイネーブルの場合の各キュー セットに対するデフォルトの出力キューを示しています。 すべてのポートはキューセット 1 にマッピングされます。 ポートの帯域幅限度は 100% に設定され、レートは制限されません。 SRR シェーピング重み（絶対）機能では、ゼロのシェーピング重みはキューが共有モードで動作していることを示しています。 SRR 共有重み機能では、帯域幅の 4 分の 1 が各キューに割り当てられます。

表 *66*：出力キューのデフォルト設定

機能	キュー 1	キュー 2	キュー 3	キュー 4
バッファ割り当て	25%	25%	25%	25%
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
予約済みしきい値	50%	50%	50%	50%
最大しきい値	400%	400%	400%	400%

機能	キュー 1	キュー 2	キュー 3	キュー 4
SRR シェーピング重み（絶対）	25	0	0	0
SRR 共有重み	25	25	25	25

次の表は、QoS がイネーブルの場合のデフォルトの CoS 出力キューしきい値マップを示しています。

表 *67*：デフォルトの *CoS* 出力キューしきい値マップ

CoS 値	キュー ID-しきい値 ID
0、1	2 - 1
2、3	3 - 1
4	4 - 1
5	1 - 1
6、7	4 - 1

次の表は、QoS がイネーブルの場合のデフォルトの DSCP 出力キューしきい値マップを示しています。

表 *68*：デフォルトの *DSCP* 出力キューしきい値マップ

DSCP 値	キュー ID-しきい値 ID
0 ～ 15	2 - 1
16 ～ 31	3 - 1
32 ～ 39	4 - 1
40 ～ 47	1 - 1
48 ～ 63	4 - 1

次の表に、**mls qos srr-queue output queues 8** コマンドを使用して 8 出力キュー設定がイネーブルになる場合のデフォルトの出力キューの設定を示します。

表 *69*：*8* 出力キューのデフォルト設定

機能	キュー 1	キュー 2	キュー 3	キュー 4	キュー 5	キュー 6	キュー 7	キュー 8
バッファ割り当て	10	30	10	10	10	10	10	10
WTD ドロップしきい値 1	100	1600	100	100	100	100	100	100
WTD ドロップしきい値 2	100	2000	100	100	100	100	100	100
予約済みしきい値	100	100	100	100	100	100	100	100
最大しきい値	400	2400	400	400	400	400	400	400
SRR シェーピング重み	25	0	0	0	0	0	0	0
SRR 共有重み	25	25	25	25	25	25	25	25

次の表に、**mls qos srr-queue output queues 8** コマンドを使用して QoS がイネーブルで、8 出力キュー コンフィギュレーションがイネーブルの場合のデフォルトの CoS 出力キューしきい値マップを示します。

表 *70*：デフォルトの *CoS* 出力 *8* キューしきい値マップ

CoS	出力キュー	しきい値 ID	4 出力キュー マッピング
0	2	1	2
1	3	1	2
2	4	1	3
3	5	1	3
4	6	1	4

CoS	出力キュー	しきい値 ID	4 出力キュー マッピング
5	1	1	1
6	7	1	4
7	8	1	4

次の表に、**mls qos srr-queue output queues 8** コマンドを使用して QoS がイネーブルで、8 出力キュー コンフィギュレーションがイネーブルの場合のデフォルトの DSCP 出力キューしきい値マップを示します。

表 *71*：デフォルトの *DSCP* 出力 *8* キューしきい値マップ

DSCP	出力キュー	しきい値 ID	4 出力キュー マッピング
0 ～ 7	2	1	2
8 ～ 15	3	1	2
16 ～ 23	4	1	3
24 ～ 31	5	1	3
32 ～ 39	6	1	4
40 ～ 47	1	1	1
48 ～ 55	7	1	4
56 ～ 63	8	1	4

関連トピック

QoS のグローバルなイネーブル化，（764 ページ）

標準 QoS のデフォルト設定，（756 ページ）

マッピング テーブルのデフォルト設定

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌルマップです。

デフォルトのポリシング済み DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングする（マークダウンしない）空のマップです。

関連トピック

デフォルトの CoS/DSCP マップ，（762 ページ）
デフォルトの IP Precedence/DSCP マップ，（763 ページ）
デフォルトの DSCP/CoS マップ，（763 ページ）

DSCP マップ

デフォルトの CoS/DSCP マップ

CoS/DSCP マップを使用して、着信パケットの CoS 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングします。 次の表に、デフォルトの CoS/DSCP マップを示します。 これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 *72*：デフォルトの *CoS/DSCP* マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

関連トピック

マッピング テーブルのデフォルト設定，（761 ページ）
CoS/DSCP マップの設定，（799 ページ）
ポリシング済み DSCP マップの設定，（802 ページ）

デフォルトの IP Precedence/DSCP マップ

着信パケットの IP precedence 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングするには、IP precedence/DSCP マップを使用します。 次の表は、デフォルトの IP Precedence/DSCP マップを示しています。 これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 *73*：デフォルトの *IP Precedence/DSCP* マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

関連トピック

マッピング テーブルのデフォルト設定, （761 ページ）

IP precedence/DSCP マップの設定, （801 ページ）

ポリシング済み DSCP マップの設定, （802 ページ）

デフォルトの DSCP/CoS マップ

4 つの出力キューのうち 1 つを選択するために使用される CoS 値を生成するには、DSCP/CoS マップを使用します。 次の表に、デフォルトの DSCP/CoS マップを示します。 これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 *74*：デフォルトの *DSCP/CoS* マップ

DSCP 値	CoS 値
0 ～ 7	0
8 ～ 15	1

DSCP 値	CoS 値
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

関連トピック

マッピング テーブルのデフォルト設定，（761 ページ）
DSCP/CoS マップの設定，（804 ページ）
ポリシング済み DSCP マップの設定，（802 ページ）

QoS の設定方法

QoS のグローバルなイネーブル化

デフォルトでは、QoS はスイッチ上でディセーブルに設定されています。

QoS をイネーブルにするために次の手順が必要です。

手順の概要

1. **configure terminal**
2. **mls qos**
3. **end**
4. **show mls qos**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos** 例： `Switch(config)# mls qos`	QoS をグローバルにイネーブルにします。 QoS は、次の関連トピックのセクションで説明されているデフォルト設定で動作します。 （注） QoS をディセーブルにするには、**no mls qos** グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos** 例： `Switch# show mls qos`	QoS の設定を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

標準 QoS のデフォルト設定，（756 ページ）
出力キューのデフォルト設定，（758 ページ）
入力キューのデフォルト設定，（757 ページ）

ポートの信頼状態による分類の設定

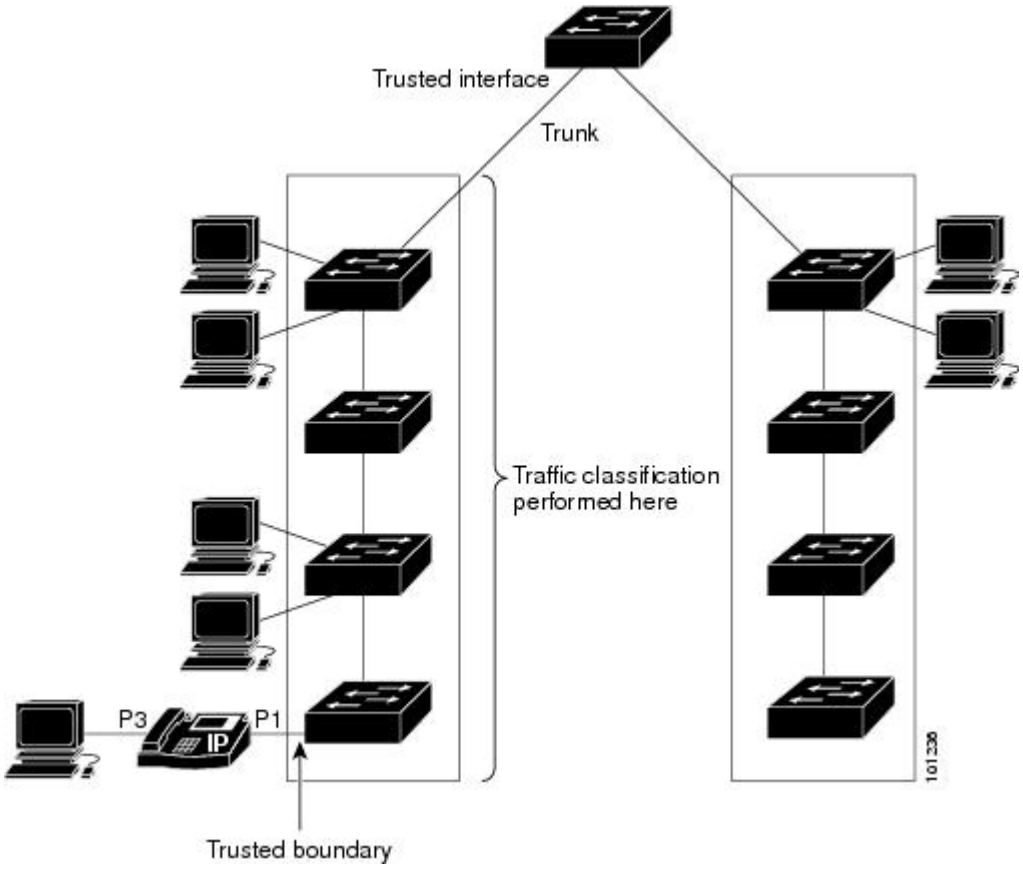
ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。

（注） ネットワークの設定によって、このモジュールのこれらのタスクの 1 つ以上または 37 ～ 47 ページのQoS ポリシーの設定の項のタスクの 1 つ以上を実行する必要があります。

QoS ドメイン内のポートの信頼状態の設定

QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。 パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチ ポートをいずれか 1 つの信頼状態に設定できます。

図 *67* : ***QoS*** ドメイン内のポートの信頼状態



手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **mls qos trust** [**cos** | **dscp** | **ip-precedence**]
4. **end**
5. **show mls qos interface**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/2`	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスは、物理ポートです。
ステップ 3	**mls qos trust** [**cos** | **dscp** | **ip-precedence**] 例： `Switch(config-if)# mls qos trust cos`	ポートの信頼状態を設定します。 デフォルトでは、ポートは trusted ではありません。 キーワードを指定しない場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos**：パケットの CoS 値を使用して入力パケットを分類します。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。 デフォルトのポート CoS 値は 0 です。 • **dscp**：パケットの DSCP 値を使用して入力パケットを分類します。 非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。 スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。 • **ip-precedence**：パケットの IP precedence 値を使用して入力パケットを分類します。 非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。 スイッチは、

	コマンドまたはアクション	目的
		内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。 untrusted ステートにポートを戻す場合は、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** 例： `Switch# show mls qos interface`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

インターフェイスの CoS 値の設定，（768 ページ）

CoS/DSCP マップの設定，（799 ページ）

インターフェイスの CoS 値の設定

QoS は、trusted ポートおよび untrusted ポートで受信したタグなしフレームに、**mls qos cos** インターフェイス コンフィギュレーション コマンドで指定された CoS 値を割り当てます。

ポートのデフォルト CoS 値を定義する場合、またはポート上のすべての着信パケットにデフォルト CoS 値を割り当てる場合には、特権 EXEC モードから次の手順を実行します。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **mls qos cos** {*default-cos* | **override**}
4. **end**
5. **show mls qos interface**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/1/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 3	**mls qos cos** {*default-cos*	**override**} 例： `Switch(config-if)# mls qos override`	ポートのデフォルトの CoS 値を設定します。 • *default-cos* には、ポートに割り当てるデフォルトの CoS 値を指定します。 パケットがタグなしの場合、デフォルトの CoS 値がパケットの CoS 値になります。 指定できる CoS 範囲は 0 ～ 7 です。デフォルトは 0 です。 • 着信パケットにすでに設定されている信頼状態を変更し、すべての着信パケットにデフォルトのポート CoS 値を適用する場合は、**override** キーワードを使用します。 デフォルトでは、CoS の上書きはディセーブルに設定されています。 特定のポートに届くすべての着信パケットに、他のポートからのパケットより高い、または低いプライオリティを与える場合には、**override** キーワードを使用します。 ポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されている場合でも、設定済みの信頼状態がこのコマンドによって上書き変更され、すべての着信 CoS 値にこのコマンドで設定されたデフォルトの CoS 値が割り当てられます。 着信パケットがタグ付きの場合、入力ポートで、ポートのデフォルト CoS を使用してパケットの CoS 値が変更されます。

	コマンドまたはアクション	目的
		（注） デフォルトの設定に戻す場合は、**no mls qos cos** {*default-cos* | **override**} インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** 例： `Switch# show mls qos interface`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

QoS ドメイン内のポートの信頼状態の設定, （766 ページ）

ポート セキュリティを確保するための信頼境界の設定

一般的なネットワークでは、スイッチ ポートに Cisco IP Phone を接続し、電話の背後からデータ パケットを生成するデバイスをカスケードします。 Cisco IP Phone では、音声パケット CoS レベルをハイ プライオリティ（CoS = 5）にマーキングし、データ パケットをロー プライオリティ（CoS = 0）にマーキングすることで、共有データ リンクを通して音声品質を保証しています。 電話からスイッチに送信されたトラフィックは通常 802.1Q ヘッダーを使用するタグでマーキングされています。 ヘッダーには VLAN 情報およびパケットのプライオリティになる CoS の 3 ビット フィールドが含まれています。

ほとんどの Cisco IP Phone 設定では、電話からスイッチに送信されるトラフィックは、音声トラフィックがネットワーク内の他のタイプのトラフィックに対して適切にプライオリティ付けがされていることを保証するように信頼されています。 **mls qos trust cos** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの CoS ラベルを信頼するように、電話が接続されているスイッチ ポートを設定します。 **mls qos trust dscp** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラ

フィックの DSCP ラベルを信頼するように、電話が接続されているルーテッド ポートを設定します。

信頼設定により、ユーザが電話をバイパスして PC を直接スイッチに接続する場合に、ハイプライオリティキューの誤使用を避けるのにも信頼境界機能を使用できます。信頼境界機能を使用しないと、（信頼性のある CoS 設定により）PC が生成した CoS ラベルがスイッチで信頼されてしまいます。 それに対して、信頼境界機能は CDP を使用してスイッチ ポートにある Cisco IP Phone（Cisco IP Phone 7910、7935、7940、7960 など）の存在を検出します。 電話が検出されない場合、信頼境界機能がハイプライオリティキューの誤使用を避けるためにスイッチポートの信頼設定を無効にします。 信頼境界機能は、PC および Cisco IP Phone がスイッチに接続されているハブに接続されている場合は機能しないことに注意してください。

Cisco IP Phone に接続した PC でハイ プライオリティのデータ キューを利用しないようにすることもできる場合があります。 **switchport priority extend cos** インターフェイス コンフィギュレーション コマンドを使用して、PC から受信するトラフィックのプライオリティを上書きするようにスイッチ CLI を介して電話を設定できます。

手順の概要

1. **configureterminal**
2. **cdp run**
3. **interface** *interface-id*
4. **cdp enable**
5. 次のいずれかを使用します。
   - **mls qos trust cos**
   - **mls qos trust dscp**
6. **mls qos trust device cisco-phone**
7. **end**
8. **show mls qos interface**
9. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**cdp run** 例： `Switch(config)# cdp run`	CDP をグローバルにイネーブルにします。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 2/1/1`	Cisco IP Phone に接続するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**cdp enable** 例： `Switch(config-if)# cdp enable`	ポート上で CDP をイネーブルにします。 デフォルトでは、CDP がイネーブルに設定されています。
ステップ 5	次のいずれかを使用します。 • **mls qos trust cos** • **mls qos trust dscp** 例： `Switch(config-if)# mls qos trust cos`	Cisco IP Phone から受信したトラフィックの CoS 値を信頼するようにスイッチ ポートを設定します。 または Cisco IP Phone から受信したトラフィックの DSCP 値を信頼するようにルーテッド ポートを設定します。 デフォルトでは、ポートは trusted ではありません。
ステップ 6	**mls qos trust device cisco-phone** 例： `Switch(config-if)# mls qos trust device cisco-phone`	Cisco IP Phone が信頼できるデバイスであることを指定します。 信頼境界機能と自動 QoS（(**auto qos voip** インターフェイス コンフィギュレーション コマンド）を同時にイネーブルにはできません。両者は相互に排他的です。 （注） 信頼境界機能をディセーブルにするには、**no mls qos trust device** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show mls qos interface** 例： `Switch# show mls qos interface`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

DSCP トランスペアレント モードのイネーブル化

スイッチは透過的な DSCP 機能をサポートします。 この機能は発信パケットの DSCP フィールドのみに作用します。 デフォルトでは、DSCP 透過性はディセーブルです。 スイッチでは着信パケットの DSCP フィールドが変更され、発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、DSCP/DSCP 変換マップを含めて Quality of Service（QoS）に基づきます。

no mls qos rewrite ip dscp コマンドを使用して DSCP 透過がイネーブルになっている場合、スイッチは着信パケットの DSCP フィールドは変更せず、送信パケットの DSCP フィールドも着信パケットのものと同じになります。

透過的な DSCP 設定にかかわらず、スイッチはパケット内部の DSCP 値を変更し、トラフィックのプライオリティを提示する CoS 値を生成します。 また、スイッチは内部 DSCP 値を使用して、出力キューおよびしきい値を選択します。

手順の概要

1. **configure terminal**
2. **mls qos**
3. **no mls qos rewrite ip dscp**
4. **end**
5. **show mls qos interface** [*interface-id*]
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos** 例： `Switch(config)# mls qos`	QoS をグローバルにイネーブルにします。
ステップ 3	**no mls qos rewrite ip dscp** 例： `Switch(config)# no mls qos rewrite ip dscp`	DSCP 透過性をイネーブルにします。 スイッチが IP パケットの DSCP フィールドを変更しないよう設定されます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** [*interface-id*] 例： `Switch# show mls qos interface gigabitethernet 2/1/1`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

DSCP 透過モード

透過的な DSCP 機能をディセーブルにして、信頼設定または ACL に基づいてスイッチに DSCP 値を変更させる設定にするには、**mls qos rewrite ip dscp** グローバル コンフィギュレーション コマンドを使用します。

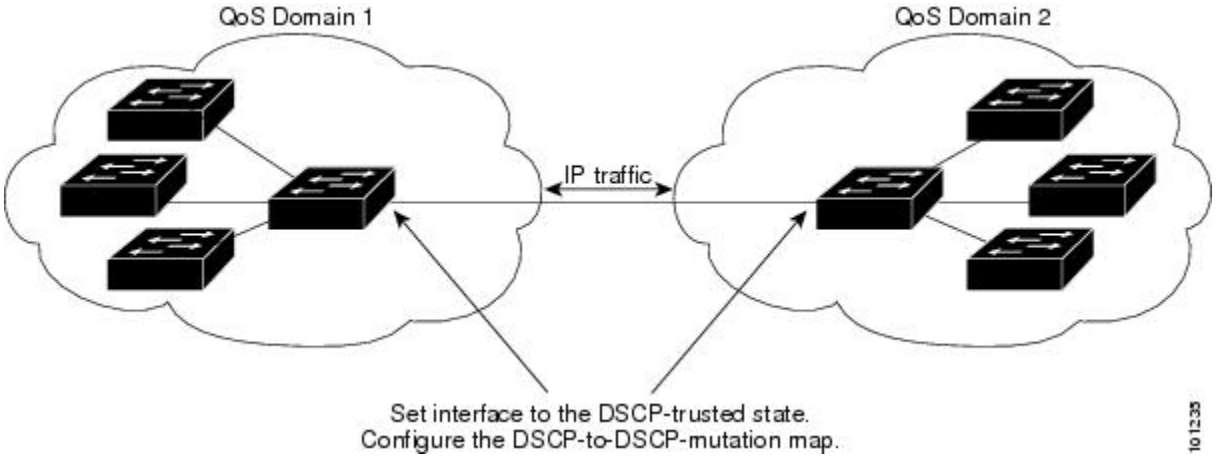
no mls qos グローバル コンフィギュレーション コマンドで QoS をディセーブルにした場合、CoS および DSCP 値は変更されません（デフォルトの QoS 設定）。

no mls qos rewrite ip dscp グローバル コンフィギュレーション コマンドを入力して DSCP 透過をイネーブルにしてから、**mls qos trust** [**cos** | **dscp**] インターフェイス コンフィギュレーション コマンドを入力した場合、DSCP 透過はイネーブルのままとなります。

別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定

2 つの異なる QoS ドメインを管理しているときに、その QoS ドメイン間の IP トラフィックに QoS 機能を実装する場合は、ドメインの境界に位置するスイッチ ポートを DSCP trusted ステートに設定できます。 受信ポートでは DSCP trusted 値をそのまま使用し、QoS の分類手順が省略されます。 2 つのドメインで異なる DSCP 値が使用されている場合は、他のドメイン内での定義に一致するように一連の DSCP 値を変換する DSCP/DSCP 変換マップを設定できます。

図 *68* : 別の *QoS* ドメインとのポート境界での *DSCP* 信頼ステート



ポート上に DSCP trusted ステートを設定して、DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。 両方の QoS ドメインに一貫した方法でマッピングするには、両方のドメイン内のポート上で次の手順を実行する必要があります。

手順の概要

1. **configureterminal**
2. **mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*
3. **interface** *interface-id*
4. **mls qos trust dscp**
5. **mls qos dscp-mutation** *dscp-mutation-name*
6. **end**
7. **show mls qos maps dscp-mutation**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp* 例： `Switch(config)# mls qos map dscp-mutation gigabitethernet1/0/2-mutation 10 11 12 13 to 30`	DSCP/DSCP 変換マップを変更します。 デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。 • *dscp-mutation-name* には、変換マップ名を入力します。 新しい名前を指定することにより、複数のマップを作成できます。 • *in-dscp* には、最大 8 つの DSCP 値をスペースで区切って入力します。 さらに、**to** キーワードを入力します。 • *out-dscp* には、1 つの DSCP 値を入力します。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**mls qos trust dscp** 例： `Switch(config-if)# mls qos trust dscp`	DSCP trusted ポートとして入力ポートを設定します。 デフォルトでは、ポートは trusted ではありません。 （注） ポートを trusted 以外のステートに戻すには、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name* 例： `Switch(config-if)# mls qos dscp-mutation gigabitethernet1/0/2-mutation`	指定された DSCP trusted 入力ポートにマップを適用します。 *dscp-mutation-name* には、ステップ 2 で作成した変換マップ名を指定します。 1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。 （注） デフォルトの DSCP/DSCP 変換マップ値に戻すには、**no mls qos map dscp-mutation** *dscp-mutation-name* グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos maps dscp-mutation** 例： `Switch# show mls qos maps dscp-mutation`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。 （注） ポートを trusted 以外のステートに戻すには、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの DSCP/DSCP 変換マップ値に戻すには、**no mls qos map dscp-mutation** *dscp-mutation-name* グローバル コンフィギュレーション コマンドを使用します。

関連トピック

例：DSCP 信頼状態へのポートの設定および DSCP/DSCP 変換マップの変更，（831 ページ）

QoS ポリシーの設定

QoS ポリシーを設定するには、次のタスクが必要です。

- トラフィックのクラスへの分類
- 各トラフィック クラスに適用するポリシーの設定
- ポートへのポリシーの付加

ここでは、トラフィックを分類、ポリシング、マーキングする方法について説明します。 ネットワーク設定に応じて、この項のモジュールの 1 つ以上を実行します。

関連トピック

ポリシングおよびマーキングの概要，（743 ページ）

分類の概要，（738 ページ）

ACL を使用したトラフィックの分類

IPv4 標準 ACLS、IPv4 拡張 ACL または IPv6 ACL を使用して IP トラフィックを分類できます。

非 IP トラフィックの分類はレイヤ 2 MAC ACL でできます。

IPv4 トラフィック用の *IP* 標準 *ACL* の作成

はじめる前に

この作業を実行する前に、QoS 設定のために使用するアクセス リストを決定します。

手順の概要

1. **configure terminal**
2. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
3. **end**
4. **show access-lists**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 1 permit 192.2.255.0 1.1.1.255`	IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、アクセス リスト番号を入力します。 有効範囲は 1 ～ 99 および 1300 ～ 1999 です。 • **permit** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。 **deny** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 • *source* には、パケットの送信元となるネットワークまたはホストを指定します。 **any** キーワードは 0.0.0.0 255.255.255.255 の省略形として使用できます。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメ

	コマンドまたはアクション	目的
		ントで一致が見つからなかったすべてのパケットに適用されることに注意してください。 （注） アクセス リストを削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** 例： `Switch# show access-lists`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

アクセス コントロール リスト，（741 ページ）
QoS ACL の注意事項，（732 ページ）
例：ACL によるトラフィックの分類，（831 ページ）

IPv4 トラフィック用の *IP* 拡張 *ACL* の作成

はじめる前に

この作業を実行する前に、QoS 設定のために使用するアクセス リストを決定します。

手順の概要

1. **configureterminal**
2. **access-list***access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*
3. **end**
4. **show access-lists**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list***access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* 例： `Switch(config)# access-list 100 permit ip any any dscp 32`	IP 拡張 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、アクセス リスト番号を入力します。 有効範囲は 100 ～ 199 および 2000 ～ 2699 です。 • **permit** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。 **deny** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 • *protocol* には、IP プロトコルの名前または番号を入力します。 疑問符（?）を使用すると、使用できるプロトコル キーワードのリストが表示されます。 • *source* には、パケットの送信元となるネットワークまたはホストを指定します。 ネットワークまたはホストを指定するには、ドット付き 10 進表記を使用するか、*source* 0.0.0.0 *source-wildcard* 255.255.255.255 の短縮形として **any** キーワードを使用するか、または *source* 0.0.0.0 を表す **host** キーワードを使用します。 • *source-wildcard* では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。 ワイルドカードを指定するには、ドット付き 10 進表記を使用するか、*source* 0.0.0.0 *source-wildcard* 255.255.255.255 の短縮形として **any** キーワードを使用するか、または *source* 0.0.0.0 を表す **host** キーワードを使用します。 • *destination* には、パケットの宛先となるネットワークまたはホストを指定します。 *destination* および *destination-wildcard* には、*source* および *source-wildcard* での説明と同じオプションを使用できます。 アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。 （注） アクセス リストを削除するには、**no access-list***access-list-number* グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** 例： `Switch# show access-lists`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

アクセス コントロール リスト，（741 ページ）

QoS ACL の注意事項，（732 ページ）

例：ACL によるトラフィックの分類，（831 ページ）

IPv6 トラフィック用の *IPv6 ACL* の作成

はじめる前に

この作業を実行する前に、QoS 設定のために使用するアクセス リストを決定します。

手順の概要

1. **configure terminal**
2. **ipv6 access-list** *access-list-name*
3. {**deny** | **permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]
4. **end**
5. **show ipv6 access-list**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 access-list** *access-list-name* 例： `Switch(config)# ipv6 access-list ipv6_Name_ACL`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。 アクセス リスト名にはスペースまたは引用符を含めることはできません。また、数字で開始することもできません。 （注） アクセス リストを削除するには、**no ipv6 access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	{**deny** | **permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] 例： `Switch(config-ipv6-acl)# permit ip host 10::1 host 11::2 host`	条件が一致した場合にパケットを拒否する場合は **deny**、許可する場合は **permit** を入力します。 次に、条件について説明します。 *protocol* には、インターネット プロトコルの名前または番号を入力します。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、**udp**、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • *source-ipv6-prefix/prefix-length* または *destination-ipv6-prefix/ prefix-length* は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、**any** を入力します。 • **host** *source-ipv6-address* または *destination-ipv6-address* には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （任意）*operator* には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。 オペランドには、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、**range**（包含範囲）があります。 *source-ipv6-prefix/prefix-length* 引数のあとの operator は、送信元ポートに一致する必要があります。 *destination-ipv6- prefix/prefix-length* 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）*port-number* は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。 TCP ポート名を使用できるのは、TCP の

	コマンドまたはアクション	目的
		フィルタリング時だけです。 UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）**dscp** *value* を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。 指定できる範囲は 0 ～ 63 です。 • （任意）**fragments** を入力して、先頭ではないフラグメントを確認します。 このキーワードが表示されるのは、プロトコルが IPv6 の場合だけです。 • （任意）**log** を指定すると、エントリと一致するパケットに関するログ メッセージがコンソールに送信されます。 **log-input** を指定すると、ログ エントリに入力インターフェイスが追加されます。 ロギングはルータ ACL でだけサポートされます。 • （任意）**routing** を入力して、IPv6 パケットのルーティングを指定します。 • （任意）**sequence** *value* を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。 指定できる範囲は 1 ～ 4294967295 です。 • （任意）**time-range** *name* を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 4	**end** 例： `Switch(config-ipv6-acl)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 access-list** 例： `Switch# show ipv6 access-list`	アクセス リストの設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

アクセス コントロール リスト, （741 ページ）

QoS ACL の注意事項, （732 ページ）

例：ACL によるトラフィックの分類, （831 ページ）

QoS ACL IPv6 の注意事項

非 *IP* トラフィック用のレイヤ *2 MAC ACL* の作成

はじめる前に

この作業を実行する前に、レイヤ 2 の MAC アクセス リストが QoS 設定に必要であることを決定します。

手順の概要

1. **configure terminal**
2. **mac access-list extended** *name*
3. {**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]
4. **end**
5. **show access-lists** [*access-list-number* | *access-list-name*]
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac access-list extended** *name* 例： `Switch(config)# mac access-list extended maclist1`	リストの名前を指定することによって、レイヤ 2 MAC ACL を作成します。 このコマンドを入力すると、拡張 MAC ACL コンフィギュレーション モードに切り替わります。 （注） アクセス リストを削除するには、**no mac access-list extended** *access-list-name* グローバル コンフィギュレーション コマンドを入力します。
ステップ 3	{**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	条件が一致した場合に許可または拒否するトラフィック タイプを指定します。必要な回数だけコマンドを入力します。 • *src-MAC-addr* には、パケットの送信元となるホストの MAC アドレスを指定します。 MAC アドレスを指定するには、16 進表

	コマンドまたはアクション	目的

	例：
	`Switch(config-ext-mac1) # permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0`
	`Switch(config-ext-mac1) # permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp`
		記（H.H.H）を使用するか、*source* 0.0.0、*source-wildcard* ffff.ffff.ffff の短縮形として **any** キーワードを使用するか、または *source* 0.0.0 を表す **host** キーワードを使用します。
		• *mask* では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。
		• *dst-MAC-addr* には、パケットの宛先となるホストの MAC アドレスを指定します。 MAC アドレスを指定するには、16 進表記（H.H.H）を使用するか、*source* 0.0.0、*source-wildcard* ffff.ffff.ffff の短縮形として **any** キーワードを使用するか、または *source* 0.0.0 を表す **host** キーワードを使用します。
		• （任意）*type mask* には、Ethernet II または SNAP でカプセル化されたパケットの Ethertype 番号を指定して、パケットのプロトコルを識別します。 *type* の範囲は 0 ～ 65535 です。通常は 16 進数で指定します。 *mask* では、一致をテストする前に Ethertype に適用される *don't care* ビットを入力します。
		アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

ステップ 4	**end** 例： `Switch(config-ext-mac1)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*access-list-number* | *access-list-name*] 例： `Switch# show access-lists`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

アクセス コントロール リスト, （741 ページ）

QoS ACL の注意事項, （732 ページ）

例：ACL によるトラフィックの分類, （831 ページ）

クラス マップによるトラフィックの分類

特定のトラフィック フロー（またはクラス）を他のすべてのトラフィックから分離して名前を付けるには、**class-map** グローバル コンフィギュレーション コマンドを使用します。 クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。 match ステートメントには、ACL、IP precedence 値、DSCP 値などの条件を指定できます。 一致条件は、クラス マップ コンフィギュレーション モードの中で match ステートメントを 1 つ入力することによって定義します。

（注） **class** ポリシー マップ コンフィギュレーション コマンドを使用することによって、ポリシー マップの作成時にクラス マップを作成することもできます。

手順の概要

1. **configureterminal**
2. 次のいずれかを使用します。
   - **access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
   - **access-list***access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*]
   - **ipv6 access-list***access-list-name* {**deny** | **permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host***destination-ipv6-address*} [*operator* [*port-number*]] [**dscp***value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence***value*] [**time-range***name*]
   - **mac access-list extended***name*{**permit** | **deny**} {**host***src-MAC-addr mask* | **any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match** {**access-group***acl-index-or-name* | **ip dscp***dscp-list* | **ip precedence***ip-precedence-list*}
5. **end**
6. **show class-map**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	次のいずれかを使用します。 • **access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] • **access-list***access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] • **ipv6 access-list***access-list-name* {**deny** | **permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [*operator* [*port-number*]] [**dscp***value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence***value*] [**time-range***name*] • **mac access-list extended***name*{**permit** | **deny**} {**host***src-MAC-addr mask* | **any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*] 例： `Switch(config)# access-list 103 permit ip any any dscp 10`	必要な回数だけコマンドを繰り返し、IP 標準または IP 拡張 ACL、IP トラフィック用の IPv6 ACL、または非 IP トラフィック用のレイヤ 2 MAC ACL を作成します。 アクセスリストを作成するときは、アクセスリストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name* 例： `Switch(config)# class-map class1`	クラスマップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）このクラスマップ配下のすべての一致ステートメントの論理 AND を実行するには**match-all** キーワードを使用します。この場合は、クラスマップ内のすべての一致条件と一致する必要があります。

	コマンドまたはアクション	目的
		• （任意）このクラスマップ配下のすべての一致ステートメントの論理 OR を実行するには、**match-any** キーワードを使用します。 この場合は、1 つまたは複数の一致条件と一致する必要があります。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 （注） 既存のクラス マップを削除するには、**no class-map** [**match-all** | **match-any**] *class-map-name* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**match** {**access-group***acl-index-or-name* | **ip dscp***dscp-list* | **ip precedence***ip-precedence-list*} 例： `Switch(config-cmap)# match ip dscp 10 11 12`	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件は定義されていません。 クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。 • **access-group***acl-index-or-name* には、ステップ 2 で作成した ACL の番号または名前を指定します。 • IPv6 トラフィックを **match access-group** コマンドでフィルタリングするには、ステップ 2 の手順で IPv6 ACL を作成します。 • **ip dscp***dscp-list* には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。 各値はスペースで区切ります。 指定できる範囲は 0 ～ 63 です。 • **ip precedence***ip-precedence-list* には、着信パケットと照合する IP precedence 値を 8 つまで入力します。 各値はスペースで区切ります。 指定できる範囲は 0 ～ 7 です。 （注） 一致条件を削除するには、**no match** {**access-group***acl-index-or-name* | **ip dscp** | **ip precedence**} クラス マップ コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Switch(config-cmap)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show class-map** 例： `Switch# show class-map`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング，（791 ページ）

階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング

例：クラス マップによるトラフィックの分類，（832 ページ）

クラス マップの使用と IPv6 トラフィックのフィルタリングによるトラフィックの分類

プライマリー致基準を IPv4 トラフィックに対してのみ適用するには、**match protocol** コマンドで **ip** キーワードを使用します。 プライマリー致基準を IPv6 トラフィックに対してのみ適用するには、**match protocol** コマンドで **ipv6** キーワードを使用します。

手順の概要

1. **configureterminal**
2. **class-map** {**match-all**} *class-map-name*
3. **match protocol** [*ip*|*ipv6*]
4. **match** {**ip dscp***dscp-list* | **ip precedence***ip-precedence-list*}
5. **end**
6. **show class-map**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** {**match-all**} *class-map-name* 例： `Switch(config)# class-map cm-1`	クラスマップを作成し、クラスマップコンフィギュレーションモードを開始します。 デフォルトでは、クラス マップは定義されていません。 **match protocol** コマンドを使用する場合、**match-all** キーワードのみがサポートされます。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 （注） 既存のクラス マップを削除するには、**no class-map** [**match-all** | **match-any**] *class-map-name* グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**match protocol** [*ip*|*ipv6*] 例： `Switch(config-cmap)# match protocol ip`	（任意）クラス マップを適用する IP プロトコルを指定します。 • IPv4 トラフィックを指定するには引数 *ip*、IPv6 トラフィックを指定するには *ipv6* をそれぞれ指定します。 • **match protocol** コマンドを使用する場合、**class-map** コマンドでは **match-all** キーワードのみがサポートされます。
ステップ 4	**match** {**ip dscp***dscp-list* | **ip precedence***ip-precedence-list*} 例： `Switch(config-cmap)# match ip dscp 10`	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件は定義されていません。 • **ip dscp***dscp-list* には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。 各値はスペースで区切ります。 指定できる範囲は 0 ～ 63 です。 • **ip precedence***ip-precedence-list* には、着信パケットと照合する IP precedence 値を 8 つまで入力します。 各値はスペースで区切ります。 指定できる範囲は 0 ～ 7 です。 （注） 一致条件を削除するには、no match {**access-group***acl-index-or-name* | **ip dscp** | **ip precedence**} クラス マップ コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config-cmap)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show class-map** 例： `Switch# show class-map`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：クラス マップによるトラフィックの分類, （832 ページ）

ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング

作用対象となるトラフィック クラスを指定するポリシー マップを、物理ポート上に設定できます。 トラフィック クラスの CoS 値、DSCP 値、または IP precedence 値を信頼するアクション、トラフィック クラスに特定の DSCP 値または IP precedence 値を設定するアクション、および一致する各トラフィック クラスにトラフィック帯域幅限度を指定するアクション（ポリサー）や、トラフィックが不適合な場合の対処法を指定するアクション（マーキング）などを指定できます。

ポリシー マップには、次の特性もあります。

- 1 つのポリシー マップに、それぞれ異なる一致条件とポリサーを指定した複数のクラス ステートメントを指定できます。
- ポリシー マップには、事前に定義されたデフォルトのトラフィック クラスを含めることができます。デフォルトのトラフィック クラスはマップの末尾に明示的に配置されます。
- 1 つのポートから受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。

物理ポートでポリシー マップを設定する場合には、次の注意事項に従ってください。

- 入力ポートごとに付加できるポリシー マップは、1 つだけです。

- **mls qos map ip-prec-dscp***dscp1...dscp8* グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにのみ影響を与えます。 ポリシー マップでは、 **set ip precedence***new-precedence* ポリシー マップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マップによる影響を受けません。 出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp new-dscp** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを入力または使用すると、スイッチは設定内で、このコマンドを **set dscp** に変更します。
- **set ip precedence** または **set precedence** ポリシーマップ クラス コンフィギュレーション コマンドを使用すると、パケット IP Precedence 値を変更できます。 スイッチ コンフィギュレーションではこの設定は set ip precedence として表示されます。
- ポリシーマップとポート信頼状態は、両方とも物理インターフェイス上で有効にすることができます。 ポリシー マップは、ポート信頼状態の前に適用されます。
- **class class-default** ポリシーマップ コンフィギュレーション コマンドを使用してデフォルトのトラフィック クラスを設定すると、未分類トラフィック（トラフィック クラスで指定された一致基準に一致しないトラフィック）はデフォルトのトラフィック クラス（class-default）として処理されます。

手順の概要

1. **configureterminal**
2. **class-map** [**match-all** | **match-any**] *class-map-name*
3. **policy-map***policy-map-name*
4. **class** [*class-map-name* | **class-default**]
5. **trust** [**cos** | **dscp** | **ip-precedence**]
6. **set** {**dscp***new-dscp* | **ip precedence***new-precedence*}
7. **police***rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]
8. **exit**
9. **exit**
10. **interface***interface-id*
11. **service-policy input***policy-map-name*
12. **end**
13. **show policy-map** [*policy-map-name* [**class***class-map-name*]]
14. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *class-map-name* 例： `Switch(config)# class-map ipclass1`	クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）このクラスマップ配下のすべての一致ステートメントの論理 AND を実行するには**match-all** キーワードを使用します。 この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • （任意）このクラスマップ配下のすべての一致ステートメントの論理 OR を実行するには、**match-any** キーワードを使用します。 この場合は、1 つまたは複数の一致条件と一致する必要があります。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。
ステップ 3	**policy-map***policy-map-name* 例： `Switch(config-cmap)# policy-map flowit`	ポリシーマップ名を入力することによってポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシーマップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。 ポリシングは実行されません。 （注） 既存のポリシー マップを削除するには、**no policy-map***policy-map-name* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**class** [*class-map-name* | **class-default**] 例： `Switch(config-pmap)# class ipclass1`	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップ クラス マップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **class-default** トラフィック クラスは定義済みで、どのポリシーにも追加できます。 このトラフィック クラスは、常にポリシー マップの最後に配置

	コマンドまたはアクション	目的
		されます。 暗黙の **match any** が **class-default** クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは **class-default** と一致します。 （注） 既存のクラス マップを削除するには、**no class***class-map-name* ポリシー マップ コンフィギュレーション コマンドを使用します。
ステップ 5	**trust** [**cos** | **dscp** | **ip-precedence**] 例： `Switch(config-pmap-c)# trust dscp`	CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼ステートを設定します。 このコマンドと **set** コマンドは、同じポリシー マップ内で相互に排他的になります。 **trust** コマンドを入力する場合は、ステップ 6 へ進んでください。 デフォルトでは、ポートは trusted ではありません。 キーワードを指定せずにコマンドを入力した場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos**：QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • **dscp**：QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。 タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。 いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • **ip-precedence**：QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。 タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非IPパケットの場合、QoSはデフォルトのポート CoS 値を使用して DSCP 値を抽出します。 いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 （注） untrusted ステートに戻すには、**no trust** ポリシーマップ コンフィギュレーション コマンドを使用します。
ステップ 6	**set** {**dscp***new-dscp* | **ip precedence***new-precedence*} 例： `Switch(config-pmap-c)# set dscp 45`	パケットに新しい値を設定することによって、IP トラフィックを分類します。 • **dscp***new-dscp* には、分類されたトラフィックに割り当てる新しいDSCP値を入力します。 指定できる範囲は 0 ～ 63 です。 • **ip precedence***new-precedence* には、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。 指定できる範囲は 0 ～ 7 です。

	コマンドまたはアクション	目的
		（注） 割り当てられた DSCP または IP precedence 値を削除するには、**no set** {**dscp***new-dscp* | **ip** precedence *new-precedence*} ポリシーマップ コンフィギュレーション コマンドを使用します。
ステップ 7	**police***rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] 例： `Switch(config-pmap-c)# police 100000 80000 drop`	分類したトラフィックにポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。 指定できる範囲は 8000 ～ 10000000000 です • *burst-byte* には、標準バースト サイズをバイト数で指定します。 指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。 （ポリシング済み DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。 （注） 既存のポリサーを削除するには、**no police***rate-bps burst-byte*[**exceed-action** {**drop** | **policed-dscp-transmit**}] ポリシーマップ コンフィギュレーション コマンドを使用します。
ステップ 8	**exit** 例： `Switch(config-pmap-c)# exit`	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 9	**exit** 例： `Switch(config-pmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 2/0/1`	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 11	**service-policy input***policy-map-name* 例： `Switch(config-if)#`	ポリシー マップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つだけです。 （注） ポリシー マップとポートの対応付けを削除するには、**no service-policy** *input policy-map-name* インターフェイス コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
	service-policy input flowit	
ステップ 12	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show policy-map** [*policy-map-name* [**class***class-map-name*]] 例： `Switch# show policy-map`	入力を確認します。
ステップ 14	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ポリシングおよびマーキングの概要，（743 ページ）

物理ポートのポリシング，（744 ページ）

クラス マップによるトラフィックの分類，（786 ページ）

物理ポートのポリシー マップ

例：ポリシー マップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング，（834 ページ）

物理ポートのポリシー マップの注意事項

集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング

集約ポリサーを使用すると、同じポリシーマップ内の複数のトラフィック クラスで共有されるポリサーを作成できます。ただし、集約ポリサーを複数の異なるポリシーマップまたはポートにわたって使用することはできません。

集約ポリサーは、物理ポートの非階層型ポリシー マップにだけ設定できます。

手順の概要

1. **configureterminal**
2. **mls qos aggregate-policer** *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**}
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **policy-map** *policy-map-name*
5. **class** [*class-map-name* | **class-default**]
6. **police aggregate** *aggregate-policer-name*
7. **exit**
8. **interface** *interface-id*
9. **service-policy input** *policy-map-name*
10. **end**
11. **show mls qos aggregate-policer** [*aggregate-policer-name*]
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos aggregate-policer** *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**} 例： `Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action policed-dscp-transmit`	同じポリシーマップ内の複数のトラフィック クラスに適用できるポリサー パラメータを定義します。 デフォルトでは、集約ポリサーは定義されていません。 • *aggregate-policer-name* には、集約ポリサーの名前を指定します。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。 指定できる範囲は 8000 ～ 10000000000 です • *burst-byte* には、標準バースト サイズをバイト数で指定します。 指定できる範囲は 8000 ～ 1000000 です。 • レートを超過した場合に実行するアクションを指定します。 パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。 （ポリシング済み DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。

	コマンドまたはアクション	目的
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name* 例： `Switch(config)# class-map ipclass1`	必要に応じて、トラフィックを分類するクラス マップを作成します。
ステップ 4	**policy-map** *policy-map-name* 例： `Switch(config-cmap)# policy-map aggflow1`	ポリシーマップ名を入力することによってポリシーマップを作成し、ポリシーマップコンフィギュレーションモードを開始します。
ステップ 5	**class** [*class-map-name* | **class-default**] 例： `Switch(config-cmap-p)# class ipclass1`	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 6	**police aggregate** *aggregate-policer-name* 例： `Switch(configure-cmap-p)# police aggregate transmit1`	同じポリシー マップ内の複数のクラスに集約ポリサーを適用します。 *aggregate-policer-name* には、ステップ 2 で指定した名前を入力します。 指定された集約ポリサーをポリシー マップから削除するには、**no police aggregate** *aggregate-policer-name* ポリシー マップ コンフィギュレーション コマンドを使用します。 集約ポリサーおよびそのパラメータを削除するには、**no mls qos aggregate-policer** *aggregate-policer-name* グローバル コンフィギュレーション コマンドを使用します。
ステップ 7	**exit** 例： `Switch(configure-cmap-p)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 2/0/1`	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。

	コマンドまたはアクション	目的
ステップ 9	**service-policy input** *policy-map-name* 例： `Switch(config-if)# service-policy input aggflow1`	ポリシー マップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 10	**end** 例： `Switch(configure-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show mls qos aggregate-policer** [*aggregate-policer-name*] 例： `Switch# show mls qos aggregate-policer transmit1`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ポリシングおよびマーキングの概要，（743 ページ）

例：集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング，（837 ページ）

DSCP マップの設定

関連トピック

マッピング テーブルの概要，（746 ページ）

CoS/DSCP マップの設定

CoS/DSCP マップを使用して、着信パケットの CoS 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングします。

CoS/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **mls qos map cos-dscp***dscp1...dscp8*
3. **end**
4. **show mls qos maps cos-dscp**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map cos-dscp***dscp1...dscp8* 例： `Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45`	CoS/DSCP マップを変更します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。 各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ～ 63 です。 （注） デフォルトのマップに戻すには、**no mls qos cos-dscp** グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps cos-dscp** 例： `Switch# show mls qos maps cos-dscp`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

デフォルトの CoS/DSCP マップ，（762 ページ）

QoS ドメイン内のポートの信頼状態の設定，（766 ページ）

例：DSCP マップの設定，（838 ページ）

IP precedence/DSCP マップの設定

着信パケットの IP precedence 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングするには、IP precedence/DSCP マップを使用します。

IP precedence/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **mls qos map ip-prec-dscp***dscp1...dscp8*
3. **end**
4. **show mls qos maps ip-prec-dscp**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map ip-prec-dscp***dscp1...dscp8* 例： `Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45`	IP precedence/DSCP マップを変更します。 *dscp1...dscp8* には、IP precedence 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。 各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ～ 63 です。 （注） デフォルトのマップに戻すには、**no mls qos ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps ip-prec-dscp** 例： `Switch# show mls qos maps ip-prec-dscp`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

デフォルトの IP Precedence/DSCP マップ, （763 ページ）

例：DSCP マップの設定, （838 ページ）

ポリシング済み DSCP マップの設定

ポリシングおよびマーキング アクションによって得られる新しい値に DSCP 値をマークダウンするには、ポリシング済み DSCP マップを使用します。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

ポリシング済み DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **mls qos map policed-dscp** *dscp-list* **to** *mark-down-dscp*
3. **end**
4. **show mls qos maps policed-dscp**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map policed-dscp** *dscp-list* **to** *mark-down-dscp* 例： `Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0`	ポリシング済み DSCP マップを変更します。 • *dscp-list* には、最大 8 つの DSCP 値をスペースで区切って入力します。 さらに、**to** キーワードを入力します。 • *mark-down-dscp* には、対応するポリシング設定（マークダウンされた）DSCP 値を入力します。 （注） デフォルトのマップに戻すには、**no mls qos policed-dscp** グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps policed-dscp** 例： `Switch(config)# show mls qos maps policed-dscp`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

デフォルトの CoS/DSCP マップ，（762 ページ）
デフォルトの IP Precedence/DSCP マップ，（763 ページ）
デフォルトの DSCP/CoS マップ，（763 ページ）

例：DSCP マップの設定，（838 ページ）

DSCP/CoS マップの設定

4 つの出力キューのうち 1 つを選択するために使用される CoS 値を生成するには、DSCP/CoS マップを使用します。

特権 EXEC モードで開始し、次の手順に従って DSCP/CoS マップを修正します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **mls qos map dscp-cos***dscp-list***to***cos*
3. **end**
4. **show mls qos maps dscp-to-cos**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-cos***dscp-list***to***cos* 例： `Switch# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0`	DSCP/CoS マップを変更します。 • *dscp-list* には、最大 8 つの DSCP 値をスペースで区切って入力します。 さらに、**to** キーワードを入力します。 • *cos* には、DSCP 値と対応する CoS 値を入力します。 DSCP の範囲は 0 ～ 63、CoS の範囲は 0 ～ 7 です。 （注） デフォルトのマップに戻すには、**no mls qos dscp-cos** グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**show mls qos maps dscp-to-cos** 例： `Switch# show mls qos maps dscp-to-cos`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

デフォルトの DSCP/CoS マップ，（763 ページ）

例：DSCP マップの設定，（838 ページ）

DSCP/DSCP 変換マップの設定

2 つの QoS ドメインで異なる DSCP 定義が使用されている場合は、一方のドメインの一連の DSCP 値を変換して、もう一方のドメインの定義に一致させる DSCP/DSCP 変換マップを使用します。DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポートに適用します（入力変換）。

入力変換により、パケットの DSCP 値が新しい DSCP 値で上書きされ、QoS はこの新しい値をパケットに適用します。 スイッチは、新しい DSCP 値とともにそのパケットをポートへ送出します。

1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。 デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*
3. **interface** *interface-id*
4. **mls qos trust dscp**
5. **mls qos dscp-mutation** *dscp-mutation-name*
6. **end**
7. **show mls qos maps dscp-mutation**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp* 例： `Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0`	DSCP/DSCP 変換マップを変更します。 • *dscp-mutation-name* には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 • *in-dscp* には、最大 8 つの DSCP 値をスペースで区切って入力します。 さらに、**to** キーワードを入力します。 • *out-dscp* には、1 つの DSCP 値を入力します。 DSCP の範囲は 0 ～ 63 です。 （注） デフォルトのマップに戻すには、**no mls qos dscp-mutation** *dscp-mutation-name* グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。

	コマンドまたはアクション	目的
ステップ 4	**mls qos trust dscp** 例： `Switch(config-if)# mls qos trust dscp`	DSCP trusted ポートとして入力ポートを設定します。 デフォルトでは、ポートは trusted ではありません。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name* 例： `Switch(config-if)# mls qos dscp-mutation mutation1`	指定された DSCP trusted 入力ポートにマップを適用します。 *dscp-mutation-name* には、ステップ 2 で指定した変換マップ名を入力します。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos maps dscp-mutation** 例： `Switch# show mls qos maps dscp-mutation`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

例：DSCP マップの設定, （838 ページ）

入力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さに応じて、次のモジュールの作業をすべて実行しなければならない場合があります。 次の特性を決定する必要があります。

- 各キューに（DSCP 値または CoS 値によって）割り当てるパケット
- 各キューに適用されるドロップしきい値、および各しきい値にマッピングされる CoS または DSCP 値

- 各キュー間に割り当てられる空きバッファ スペースの量
- 各キュー間に割り当てられる使用可能な帯域幅の量
- ハイ プライオリティを設定する必要があるトラフィック（音声など）の有無

関連トピック

プライオリティ キューイング，（751 ページ）

入力ポートのアクティビティ

入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットがドロップされるようにキューのしきい値を調整します。

DSCP または CoS 値を入力キューにマッピングして、WTD しきい値を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. 次のいずれかを使用します。
   - **mls qos srr-queue input dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8*
   - **mls qos srr-queue input cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*
3. **mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2*
4. **end**
5. **show mls qos maps**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	次のいずれかを使用します。 • **mls qos srr-queue input dscp-map queue** *queue-id*	DSCP または CoS 値を入力キューおよびしきい値 ID にマッピングします。

	コマンドまたはアクション	目的
	threshold *threshold-id dscp1...dscp8* • **mls qos srr-queue input cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8* 例： `Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26`	デフォルトでは、DSCP 値 0 ～ 39 および 48 ～ 63 はキュー 1 およびしきい値 1 にマッピングされます。 DSCP 値 40 ～ 47 はキュー 2 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 ～ 4、6、および 7 はキュー 1 およびしきい値 1 にマッピングされます。 CoS 値 5 はキュー 2 およびしきい値 1 にマッピングされます。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • *threshold-id* で指定できる範囲は 1 ～ 3 です。 しきい値 3 のドロップしきい値（%）は事前に定義されています。 パーセンテージはキューがいっぱいの状態に対して設定されます。 • *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。 指定できる範囲は 0 ～ 63 です。 • *cos1...cos8* には、各値をスペースで区切って、最大 8 の値を入力します。 指定できる範囲は 0 ～ 7 です。
ステップ 3	**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2* 例： `Switch(config)# mls qos srr-queue input threshold 1 50 70`	入力キューに 2 つの WTD しきい値の割合（しきい値 1 および 2 用）を割り当てます。 デフォルトでは、両方のしきい値が 100% に設定されています。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • *threshold-percentage1 threshold-percentage2* の範囲は、1 ～ 100 です。 各値はスペースで区切ります。 各しきい値は、キューに割り当てられたキュー記述子の総数に対する割合です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos maps** 例： `Switch# show mls qos maps`	入力を確認します。 DSCP 入力キューしきい値マップは、表形式で表示されます。 d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。 d1 および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1（02-01）のようになります。 CoS 入力キューしきい値マップでは、先頭行に CoS 値、2 番めの行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2（2-2）のようになります。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 デフォルトのCoS入力キューしきい値マップまたはデフォルトのDSCP入力キューしきい値マップに戻すには、**no mls qos srr-queue input cos-map**、または **no mls qos srr-queue input dscp-map** グローバル コンフィギュレーション コマンドを使用します。 デフォルトの WTD しきい値の割合に戻すには、**no mls qos srr-queue input threshold queue-id** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

入力キューでのキューイングおよびスケジューリング

WTD, （747 ページ）

入力キュー間のバッファ スペースの割り当て

2つのキュー間で入力バッファを分割する比率を定義します（スペース量を割り当てます）。バッファ割り当てと帯域幅割り当てにより、パケットがドロップされる前にバッファに格納できるデータ量が制御されます。

入力キュー間にバッファを割り当てるには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **mls qos srr-queue input buffers** *percentage1 percentage2*
3. **end**
4. 次のいずれかを使用します。
   - **show mls qos interface buffer**
   - **show mls qos input-queue**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input buffers** *percentage1 percentage2* 例： `Switch(config)# mls qos srr-queue input buffers 60 40`	入力キュー間のバッファを割り当てます。 デフォルトでは、バッファの 90% がキュー 1 に、残りの 10% がキュー 2 に割り当てられます。 *percentage1 percentage2* の範囲は 0 ～ 100 です。 各値はスペースで区切ります。 キューがバースト性のある着信トラフィックを処理できるようにバッファを割り当てる必要があります。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ステップ 4	次のいずれかを使用します。
	• **show mls qos interface buffer**
	• **show mls qos input-queue**
	
	例：
	`Switch# show mls qos interface buffer`
	または
	`Switch# show mls qos input-queue`
		入力を確認します。

ステップ 5	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。 デフォルトの設定に戻すには、**no mls qos srr-queue input buffers** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

入力キューでのキューイングおよびスケジューリング
例：入力キューの特性の設定，（840 ページ）

入力キュー間の帯域幅の割り当て

入力キュー間に割り当てられる使用可能な帯域幅の量を指定する必要があります。 重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。 帯域幅割り当てとバッファ割り当てにより、パケットがドロップされる前にバッファに格納できるデータ量を制御できます。 入力キューで SRR が動作するのは、共有モードの場合のみです。

入力キュー間に帯域幅を割り当てるには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **mls qos srr-queue input bandwidth** *weight1 weight2*
3. **end**
4. 次のいずれかを使用します。
   - **show mls qos interface queueing**
   - **show mls qos input-queue**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input bandwidth** *weight1 weight2* 例： `Switch(config)# mls qos srr-queue input bandwidth 25 75`	入力キューに共有ラウンド ロビン重みを割り当てます。 *weight1* および *weight2* のデフォルト設定は 4 です（帯域幅の 1/2 が 2 つのキューで等しく共有されます）。 *weight1* および *weight2* の場合、範囲は 1 ～ 100 です。 各値はスペースで区切ります。 SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重

	コマンドまたはアクション	目的
		みに従いプライオリティ キューを処理します。 次に、SRR は **mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ステップ 4	次のいずれかを使用します。
	• **show mls qos interface queueing**
	• **show mls qos input-queue**
	
	例：
	
	`Switch# show mls qos interface queueing`
	
	または
	
	`Switch# show mls qos input-queue`
		入力を確認します。

ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 デフォルトの設定に戻すには、**no mls qos srr-queue input bandwidth** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

入力キューでのキューイングおよびスケジューリング
例：入力キューの特性の設定，（840 ページ）
SRR のシェーピングおよび共有，（748 ページ）

入力プライオリティ キューの設定

プライオリティ キューは、優先して進める必要があるトラフィックに限り使用してください（遅延とジッタを最小限にとどめる必要のある音声トラフィックなど）。

プライオリティ キューは、オーバーサブスクライブ リングに激しいネットワーク トラフィックが発生している状況で（バックプレーンが伝達できるトラフィックよりも多くのトラフィックが発生し、キューがいっぱいになって、フレームがドロップされている場合）、遅延およびジッタを軽減するように帯域幅の一部が保証されています。

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューを処理します。 次に、SRR は **mls qos srr-queue input bandwidth** *weight1 weight2* グローバルコンフィギュレーションコマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

プライオリティ キューを設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight*
3. **end**
4. 次のいずれかを使用します。
   - **show mls qos interface queueing**
   - **show mls qos input-queue**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* 例： `Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10`	キューをプライオリティ キューとして割り当て、リングが輻輳している場合にスタックまたは内部リングの帯域幅を保証します。 デフォルトのプライオリティ キューはキュー2です。このキューには帯域幅の 10% が割り当てられています。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • **bandwidth** *weight* には、スタックまたは内部リングの帯域幅に対する割合を割り当てます。 指定できる範囲は 0 ～ 40 です。 値が大きい場合はリング全体に影響が及び、スイッ

	コマンドまたはアクション	目的
		チまたはスタックのパフォーマンスが低下することがあるため、保証できる帯域幅は制限されています。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	次のいずれかを使用します。 • **show mls qos interface queueing** • **show mls qos input-queue** 例： `Switch# show mls qos input-queue`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。 デフォルト設定に戻すには、**no mls qos srr-queue input priority-queue queue-id** グローバル コンフィギュレーション コマンドを使用します。 プライオリティ キューイングをディセーブルにするには、帯域幅の重みを 0 に設定します。たとえば、**mls qos srr-queue input priority-queue queue-id bandwidth 0** を入力します。

関連トピック

入力キューでのキューイングおよびスケジューリング

例：入力キューの特性の設定，（840 ページ）

入力キューでのキューイングおよびスケジューリング

出力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さに応じて、次のモジュールで示す作業をすべて実行しなければならない場合があります。 次の特性を決定する必要があります。

- DSCP 値または CoS 値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューセット（ポートごとの 4 つの出力キュー）に適用されるドロップしきい値の割合、およびトラフィック タイプに必要なメモリの確保量および最大メモリ

- キュー セットに割り当てる固定バッファ スペースの量
- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術（シェーピング、共有、または両方）

関連トピック

シェーピング モードまたは共有モード, （755 ページ）

設定時の注意事項

緊急キューがイネーブルにされているとき、またはSRRの重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー1に対してSRRのシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRRのシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して shaped モードは shared モードを無効にし、SRR はこのキューに shaped モードでサービスを提供します。
- 出力緊急キューがディセーブルで、SRRシェーピング重みが設定されていない場合、SRRはこのキューを共有モードで処理します。

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定

バッファの可用性の保証、WTDしきい値の設定、およびキューセットの最大割り当ての設定を行うには、**mls qos queue-set output***qset-id***threshold***queue-iddrop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* グローバル コンフィギュレーション コマンドを使用します。

各しきい値はキューに割り当てられたバッファの割合です。このパーセント値を指定するには、**mls qos queue-set output***qset-id***buffers***allocation1 ... allocation4* グローバル コンフィギュレーション コマンドを使用します。 キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。

（注） スイッチはデフォルトで 4 つの出力キューをサポートしますが、合計 8 つの出力キューをイネーブルにするオプションがあります。 8 つの出力キューをすべてイネーブルにするには、**mls qos srr-queue output queues 8** グローバル コンフィギュレーション コマンドを使用します。8 出力キューがイネーブルになると、8 つすべてのキューのしきい値、バッファ、帯域幅の共有重みおよび帯域幅シェーピング重みを設定できます。8出力キューの設定はスタンドアロンスイッチでのみサポートされます。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。 出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

キューセットのメモリ割り当てとドロップしきい値を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **mls qos srr-queue output queues 8**
3. **mls qos queue-set output***qset-id***buffers***allocation1 ... allocation8*
4. **mls qos queue-set output***qset-id***threshold***queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*
5. **interface***interface-id*
6. **queue-set***qset-id*
7. **end**
8. **show mls qos interface** [*interface-id*] **buffers**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue output queues 8** 例： `Switch(config)# mls qos srr-queue output queues 8`	（任意）スイッチはデフォルトで 4 つの出力キューをサポートしますが、合計 8 つの出力キューをイネーブルにすることができます。 4 つの追加出力キューをイネーブルにするには、オプションの **mls qos srr-queue output queues 8** コマンドを使用します。 8 つのキュー サポートがイネーブルになると、4 つの追加キューの設定に進むことができます。 追加のキューパラメータをサポートするように、既存の出力キュー設定コマンドが変更されます。 （注） 8 つのキューをイネーブルにするオプションは、スタンドアロンスイッチのみで使用できます。
ステップ 3	**mls qos queue-set output***qset-id***buffers***allocation1 ... allocation8*	バッファをキューセットに割り当てます。 デフォルトでは、すべての割り当て値は 4 つのキューに均等にマッピングされます（25、25、25、25）。 各キューがバッファ スペースの 1/4 を持ち

	コマンドまたはアクション	目的
	例： `Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20 10 10 10 10`	ます。8つの出力キューを設定すると、デフォルトで、合計バッファ スペースの 30 % がキュー 2 に割り当てられ、キュー 1、3、4、5、6、7、および 8 にそれぞれ 10 % が割り当てられます。 上記のステップ2で説明したように、8つの出力キューをイネーブルにした場合は次が適用されます。 • *qset-id* には、キューセットの ID を入力します。 指定できる範囲は 1 ～ 2 です。 各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。 • *allocation1 ... allocation8* には、キューセット内のキューごとに 1 つずつ、合計 8 つのパーセンテージを指定します。 *allocation1*、*allocation3*、および *allocation4* ~ *allocation8* の範囲は 0 ~ 99 です。 *allocation2* の範囲は 1 ～ 100 です（CPU バッファを含める）。 トラフィックの重要度に応じてバッファを割り当てます。たとえば、最高プライオリティのトラフィックを持つキューには多くの割合のバッファを与えます。 （注） デフォルトの設定に戻すには、**no mls qos queue-set output***qset-id***buffers** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**mls qos queue-set output***qset-id***threshold***queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* 例： `Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200`	WTD しきい値を設定し、バッファのアベイラビリティを保証し、キューセット（ポートごとに 4 つの出力キュー）の最大メモリ割り当てを設定します。 デフォルトでは、キュー 1、3、および 4 の WTD は 100% に設定されています。 キュー 2 の WTD は 200% に設定されています。 キュー 1、2、3、および 4 の専用は 50% に設定されています。 すべてのキューの最大しきい値はデフォルトで 400% に設定されています。 上記のステップ2で説明したように、8つの出力キューをイネーブルにした場合は次が適用されます。 • *qset-id* には、ステップ 2 で指定したキューセットの ID を入力します。 指定できる範囲は 1 ～ 2 です。 • *queue-id* には、コマンドの実行対象となるキュー セット内の特定のキューを入力します。 queue-id の範囲は、デフォルトでは 1 ~ 4、8 つのキューがイネーブルになっている場合は 1 ~ 8 です。 • *drop-threshold1 drop-threshold2* には、キューの割り当てメモリのパーセンテージとして表される 2 つの WTD しきい値を指定します。 指定できる範囲は 1 ～ 3200% です。

	コマンドまたはアクション	目的
		• *reserved-threshold* には、割り当てメモリのパーセンテージとして表されるキューに保証（確保）されるメモリ サイズを入力します。 指定できる範囲は 1 ～ 100% です。 • *maximum-threshold* を指定すると、いっぱいになったキューが確保量を超えるバッファを取得できるようになります。 この値は、共通プールが空でない場合に、パケットがドロップされるまでキューが使用できるメモリの最大値です。 指定できる範囲は 1 ～ 3200% です。 （注） デフォルトの WTD しきい値のパーセンテージに戻すには、**no mls qos queue-set output***qset-id***threshold** [*queue-id*] グローバル コンフィギュレーション コマンドを使用します。
ステップ 5	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**queue-set***qset-id* 例： `Switch(config-id)# queue-set 2`	キューセットにポートをマッピングします。 *qset-id* には、ステップ 2 で指定したキューセットの ID を入力します。 指定できる範囲は 1 ～ 2 です。 デフォルトは 1 です。
ステップ 7	**end** 例： `Switch(config-id)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show mls qos interface** [*interface-id*] **buffers** 例： `Switch# show mls qos interface buffers`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy-running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 デフォルトの設定に戻すには、the **no mls qos queue-set output** *qset-id***buffers** グローバル コンフィギュレーション コマンドを使用します。 デフォルトの WTD しきい値のパーセンテージに戻すには、**no mls qos queue-set output***qset-id***threshold**[*queue-id*] グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
	`startup-config`	

関連トピック

出力キューでのキューイングおよびスケジューリング
例：出力キューの特性の設定, （840 ページ）
WTD, （747 ページ）

出力キューおよびしきい値 ID への DSCP または CoS 値のマッピング

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットがドロップされるようにキューのしきい値を調整します。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。 デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびデフォルトの設定がご使用の QoS ソリューションを満たしていない場合だけです。

DSCP または CoS 値を出力キューおよび ID にマッピングするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. 次のいずれかを使用します。
   - **mls qos srr-queue output dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8*
   - **mls qos srr-queue output cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*
3. **end**
4. **show mls qos maps**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	次のいずれかを使用します。 • **mls qos srr-queue output dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8* • **mls qos srr-queue output cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8* 例： `Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11`	DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 15 はキュー 2 およびしきい値 1 に、 DSCP 値 16 ～ 31 はキュー 3 およびしきい値 1 に、 DSCP 値 32 ～ 39 および 48 ～ 63 はキュー 4 およびしきい値 1 に、 DSCP 値 40 ～ 47 はキュー 1 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 および 1 はキュー 2 およびしきい値 1 に、 CoS 値 2 および 3 はキュー 3 およびしきい値 1 に、 CoS 値 4、6、および 7 はキュー 4 およびしきい値 1 に、 CoS 値 5 はキュー 1 およびしきい値 1 にマッピングされます。 • *queue-id* で指定できる範囲は 1 ～ 4 です。 （注） **mls qos srr-queue output queues 8** グローバル コンフィギュレーション コマンドを使用して 8 つの出力キューをイネーブルにした場合、*queue-id* の範囲は 1 ～ 8 になります。 • *threshold-id* で指定できる範囲は 1 ～ 3 です。 しきい値 3 のドロップしきい値（%）は事前に定義されています。 パーセンテージはキューがいっぱいの状態に対して設定されます。 • *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。 指定できる範囲は 0 ～ 63 です。 • *cos1...cos8* には、各値をスペースで区切って、最大 8 の値を入力します。 指定できる範囲は 0 ～ 7 です。 （注） デフォルトの DSCP 出力キューしきい値マップまたはデフォルトの CoS 出力キューしきい値マップに戻すには、**no mls qos srr-queue output dscp-map** または **no mls qos srr-queue output cos-map** グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**show mls qos maps** 例： `Switch# show mls qos maps`	入力を確認します。 DSCP 出力キューしきい値マップは、表形式で表示されます。 d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。 d1 および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1（02-01）のようになります。 CoS 出力キューしきい値マップでは、先頭行に CoS 値、2 番めの行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2（2-2）のようになります。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 デフォルトの DSCP 出力キューしきい値マップまたはデフォルトの CoS 出力キューしきい値マップに戻すには、**no mls qos srr-queue output dscp-map** または **no mls qos srr-queue output cos-map** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

出力キューでのキューイングおよびスケジューリング
例：出力キューの特性の設定, （840 ページ）
WTD, （747 ページ）

出力キューでの SRR シェーピング重みの設定

各キューに割り当てられる使用可能な帯域幅の量を指定できます。 重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

出力キューにシェーピング重み、共有重み、またはその両方を設定できます。 バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。

ポートにマッピングされた 4 つの出力キューにシェーピング重みを割り当てて、帯域幅のシェーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **srr-queue bandwidth shape** *weight1 weight2 weight3 weight4*
4. **end**
5. **show mls qos interface** *interface-id* **queueing**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**srr-queue bandwidth shape** *weight1 weight2 weight3 weight4* 例： `Switch(config-if)# srr-queue bandwidth shape 8 0 0 0`	出力キューにSRR重みを割り当てます。 デフォルトでは、weight1は25、weight2、weight3、およびweight4は0に設定されています。 これらのキューは共有モードです。 *weight1 weight2 weight3 weight4* には、シェーピングされるポートの割合を制御する重みを入力します。 このキューのシェーピング帯域幅は、インバース比率（1/weight）によって制御されます。 各値はスペースで区切ります。 指定できる範囲は 0 ～ 65535 です。 重み 0 を設定した場合は、対応するキューが共有モードで動作します。 **srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。 シェーピングおよび共有の両方に対して同じキューセットのキューを設定した場合は、必ず番号が最も小さいキューにシェーピングを設定してください。 シェーピング モードは、共有モードを無効にします。 デフォルトの設定に戻すには、**no srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
		（注） **mls qos srr-queue output queues 8** グローバル コンフィギュレーション コマンドを使用して、8 個の出力キューを有効にした場合、合計 8 個のキューに SRR 重みを割り当てることができます。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id* **queueing** 例： `Switch# show mls qos interface interface-id queuing`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 デフォルトの設定に戻すには、**no srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドを使用します。

関連トピック

出力キューでのキューイングおよびスケジューリング
例：出力キューの特性の設定，（840 ページ）
SRR のシェーピングおよび共有，（748 ページ）

出力キューでの SRR 共有重みの設定

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。 このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。 たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有ができます。 共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。 出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

ポートにマッピングされた 4 つの出力キューに共有重みを割り当てて、帯域幅の共有をイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **srr-queue bandwidth share** *weight1 weight2 weight3 weight4*
4. **end**
5. **show mls qos interface** *interface-id* **queueing**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**srr-queue bandwidth share** *weight1 weight2 weight3 weight4* 例： `Switch(config-id)# srr-queue bandwidth share 1 2 3 4`	出力キューに SRR 重みを割り当てます。 デフォルトでは、4 つの重みがすべて 25 です（各キューに帯域幅の 1/4 が割り当てられています）。 *weight1 weight2 weight3 weight4* には、SRR スケジューラがパケットを送信する頻度の比率を制御する重みを入力します。 各値はスペースで区切ります。 指定できる範囲は 1 ～ 255 です。 デフォルトの設定に戻すには、**no srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
		（注） **mls qos srr-queue output queues 8** グローバル コンフィギュレーション コマンドを使用して、8 個の出力キューを有効にした場合、合計 8 個のキューに SRR 重みを割り当てることができます。
ステップ 4	**end** 例： `Switch(config-id)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id* **queueing** 例： `Switch# show mls qos interface interface_id queuing`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 デフォルトの設定に戻すには、**no srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドを使用します。

関連トピック

出力キューでのキューイングおよびスケジューリング
例：出力キューの特性の設定，（840 ページ）
SRR のシェーピングおよび共有，（748 ページ）

出力緊急キューの設定

出力緊急キューにパケットを入れることにより、特定のパケットのプライオリティを他のすべてのパケットより高く設定できます。 SRR は、このキューが空になるまで処理してから他のキューを処理します。

出力緊急キューをイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **mls qos**
3. **interface** *interface-id*
4. **priority-queue out**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos** 例： `Switch(config)# mls qos`	スイッチの QoS をイネーブルにします。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	出力ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**priority-queue out** 例： `Switch(config-if)# priority-queue out`	デフォルトでディセーブルに設定されている出力緊急キューをイネーブルにします。 このコマンドを設定すると、SRR に参加するキューは 1 つ少なくなるため、SRR 重みおよびキュー サイズの比率が影響を受けます。 つまり、**srr-queue bandwidth shape** または **srr-queue bandwidth share** コマンドの *weight1* が無視されます（比率計算に使用されません）。 （注） 出力緊急キューをディセーブルにするには、**no priority-queue out** インターフェイス コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 出力緊急キューをディセーブルにするには、**no priority-queue out** インターフェイス コンフィギュレーション コマンドを使用します。

関連トピック

出力キューでのキューイングおよびスケジューリング
例：出力キューの特性の設定，（840 ページ）

出力インターフェイスの帯域幅の制限

出力ポートの帯域幅は制限できます。 たとえば、カスタマーが高速リンクの一部しか費用を負担しない場合は、帯域幅をその量に制限できます。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。 出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

出力ポートの帯域幅を制限するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **srr-queue bandwidth limit** *weight1*
4. **end**
5. **show mls qos interface** [*interface-id*] **queueing**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	レートを制限するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**srr-queue bandwidth limit** *weight1* 例： `Switch(config-if)# srr-queue bandwidth limit 80`	ポートの上限となるポート速度の割合を指定します。 指定できる範囲は 10 ～ 90 です。 デフォルトでは、ポートのレートは制限されず、100% に設定されています。 （注） デフォルトの設定に戻すには、**no srr-queue bandwidth limit** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** [*interface-id*] **queueing** 例： `Switch# show mls qos interface interface_id queueing`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Switch# copy-running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 デフォルトの設定に戻すには、**no srr-queue bandwidth limit** インターフェイス コンフィギュレーション コマンドを使用します。

関連トピック

出力キューでのキューイングおよびスケジューリング
例：出力キューの特性の設定，（840 ページ）

標準 QoS のモニタリング

表 *75*：スイッチ上で標準 *QoS* をモニタリングするためのコマンド

コマンド	説明
show class-map [*class-map-name*]	トラフィックを分類するための一致基準を定義した QoS クラス マップを表示します。
show mls qos	グローバル QoS コンフィギュレーション情報を表示します。
show mls qos aggregate-policer [*aggregate-policer-name*]	集約ポリサーの設定を表示します。
show mls qos interface [*interface-id*] [**buffers** | **policers** | **queueing** | **statistics**]	バッファ割り当て、ポリサーが設定されているポート、キューイング方式、入出力統計情報など、ポート レベルの QoS 情報が表示されます。
show mls qos maps [**cos-dscp** | |**cos-output-q** | **dscp-cos** | |**dscp-mutation** *dscp-mutation-name* | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**]	QoS のマッピング情報を表示します。
show mls qos queue-set [*qset-id*]	出力キューの QoS 設定を表示します。

コマンド	説明
show policy-map [*policy-map-name* [**class** *class-map-name*]]	着信トラフィックの分類条件を定義した QoS ポリシー マップを表示します。 着信トラフィックの分類情報を表示する場合は、**show policy-map interface** 特権 EXEC コマンドを使用しないでください。 **control-plane** および **interface** キーワードはサポートされていません。表示される統計情報は無視してください。
show running-config | include rewrite	DSCP 透過性設定を表示します。

QoS の設定例

例：DSCP 信頼状態へのポートの設定および DSCP/DSCP 変換マップの変更

次に、ポートが DSCP を信頼する状態に設定し、着信した DSCP 値 10 ～ 13 が DSCP 値 30 にマッピングされるように DSCP/DSCP 変換マップ（*gi1/0/2-mutation*）を変更する例を示します。

```
Switch(config)# mls qos map dscp-mutation gigabitethernet1/0/2-mutation
10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gigabitethernet1/0/2-mutation
Switch(config-if)# end
```

関連トピック

別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定, （775 ページ）

例：ACL によるトラフィックの分類

次に、指定された 3 つのネットワーク上のホストだけにアクセスを許可する例を示します。 ネットワーク アドレスのホスト部分にワイルドカード ビットが適用されます。 アクセス リストのステートメントと一致しない送信元アドレスのホストはすべて拒否されます。

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
! (Note: all other access implicitly denied)
```

次に、任意の送信元から、DSCP 値が 32 に設定されている任意の宛先への IP トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IP トラフィック（precedence 値は 5）を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

次に、任意の送信元からアドレス 224.0.0.2 の宛先グループへの PIM トラフィック（DSCP 値は 32）を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 102 permit pim any 224.0.0.2 dscp 32
```

次に、任意の送信元から、DSCP 値が 32 に設定されている任意の宛先への IPv6 トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# ipv6 access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IPv6 トラフィック（precedence 値は 5）を許可する ACL を作成する例を示します。

```
Switch(config)# ipv6 access-list ipv6_Name_ACL permit ip host 10::1 host 10.1.1.2
precedence 5
```

次に、2 つの許可（permit）ステートメントを指定したレイヤ 2 の MAC ACL を作成する例を示します。 最初のステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。 2 番めのステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックのみが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)
```

関連トピック

IPv4 トラフィック用の IP 標準 ACL の作成, （778 ページ）

IPv4 トラフィック用の IP 拡張 ACL の作成, （779 ページ）

IPv6 トラフィック用の IPv6 ACL の作成, （781 ページ）

非 IP トラフィック用のレイヤ 2 MAC ACL の作成, （784 ページ）

例：クラス マップによるトラフィックの分類

次に、*class1* というクラス マップの設定例を示します。 *class1* にはアクセス リスト 103 という一致条件が 1 つ設定されています。 このクラス マップによって、任意のホストから任意の宛先へのトラフィック（DSCP 値は 10）が許可されます。

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# end
Switch#
```

次に、DSCP 値が 10、11、および 12 である着信トラフィックと照合する、*class2* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# end
Switch#
```

次に、IP precedence 値が 5、6、および 7 である着信トラフィックと照合する、*class3* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# end
Switch#
```

次に、IP DSCP および IPv6 と照合するクラス マップを設定する例を示します。

```
Switch(config)# Class-map cm-1
Switch(config-cmap)# match ip dscp 10
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# Class-map cm-2
Switch(config-cmap)# match ip dscp 20
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# Policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G1/0/1
Switch(config-if)# service-policy input pm1
```

次に、IPv4 トラフィックと IPv6 トラフィックの両方に適用するクラス マップを設定する例を示します。

```
Switch(config)# ip access-list 101 permit ip any any
Switch(config)# ipv6 access-list ipv6-any permit ip any any
Switch(config)# Class-map cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match access-group name ipv6-any
Switch(config-cmap)# exit
Switch(config)# Policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1
```

関連トピック

クラス マップによるトラフィックの分類, （786 ページ）

クラス マップの使用と IPv6 トラフィックのフィルタリングによるトラフィックの分類, （789 ページ）

例：ポリシーマップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング

次に、ポリシー マップを作成し、入力ポートに結合する例を示します。 この設定では、IP 標準 ACL でネットワーク 10.1.0.0 からのトラフィックを許可します。 この分類にトラフィックが一致した場合、着信パケットの DSCP 値が信頼されます。 一致したトラフィックが平均トラフィックレート（48000 bps）、および標準バーストサイズ（8000 バイト）を超過している場合は、（ポリシング済み DSCP マップに基づいて）DSCP はマークダウンされて、送信されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map flow1t
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input flow1t
```

次に、2 つの許可ステートメントを指定してレイヤ 2 MAC ACL を作成し、入力ポートに結合する例を示します。 最初の許可ステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。 2 番めの許可ステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックのみが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

次に、分類されていないトラフィックに適用されるデフォルト クラスを使用して、IPv4 と IPv6 の両方のトラフィックに適用されるクラス マップを作成する例を示します。

```
Switch(config)# ip access-list 101 permit ip any any
```

```
Switch(config)# ipv6 access-list ipv6-any permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match access-group name ipv6-any
Switch(config-cmap)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1
```

関連トピック

ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング，（791 ページ）

物理ポートのポリシー マップ

例：階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング

次に、階層型のポリシー マップの作成方法を示します。

```
Switch> enable
Switch#  configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access 101
Switch(config-cmap)# exit
Switch(config)# exit
Switch#
Switch#
```

次に、SVI に新しいマップを割り当てる例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input gigabitethernet3/0/1 - gigabitethernet3/0/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcmap
Switch(config-pmap)# class cm-interface-1
Switch(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan-plcmap
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
```

```
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c)# service-policy port-plcmap-2
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust dscp
Switch(config-pmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input vlan-plcmap
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

次の例では、子レベルのポリシー マップがクラス下に添付されるタイミング、そのクラスのアクションが指定される必要があるタイミングを示します。

```
Switch(config)# policy-map vlan-plcmap
Switch(config-pmap)# class cm-5
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy port-plcmap-1
```

次に、IP DSCP および IPv6 と照合するクラス マップを設定する例を示します。

```
Switch(config)# class-map cm-1
Switch(config-cmap)# match ip dscp 10
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match ip dscp 20
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G1/0/1
Switch(config-if)# service-policy input pm1
```

次に、デフォルト トラフィック クラスをポリシー マップに設定する例を示します。

```
Switch# configure terminal
Switch(config)# class-map cm-3
Switch(config-cmap)# match ip dscp 30
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# class-map cm-4
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# policy-map pm3
Switch(config-pmap)# class class-default
Switch(config-pmap)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c) set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust cos
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# exit
```

次に、class-default が最初に設定されていても、ポリシーマップ pm3 の最後にデフォルト トラフィック クラスが自動的に配置される例を示します。

```
Switch# show policy-map pm3
  Policy Map pm3
    Class cm-3
      set dscp 4
    Class cm-4
      trust cos
    Class class-default
      police 8000 80000 exceed-action drop
Switch#
```

関連トピック

階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング
SVI の階層型ポリシー マップに関する注意事項

例：集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング

次に、集約ポリサーを作成して、ポリシーマップ内の複数のクラスに結合する例を示します。 この設定では、IP ACL はネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィックを許可します。 ネットワーク 10.1.0.0 から着信するトラフィックの場合は、着信パケットの DSCP が信頼されます。 ホスト 11.3.1.1 から着信するトラフィックの場合、パケットの DSCP は 56 に変更されます。 ネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィック レートには、ポリシングが設定されます。 トラフィックが平均レート（48000 bps）、および標準バースト サイズ（8000 バイト）を超過している場合は、（ポリシング済み DSCP マップに基づいて）DSCP がマークダウンされて、送信されます。 ポリシー マップは入力ポートに結合されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action
policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit
```

関連トピック

集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング，（796 ページ）

例：DSCP マップの設定

次に、CoS/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp

Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

次に、IP precedence/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp

IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

次に、DSCP 50 ～ 57 を、マークダウンされる DSCP 値 0 にマッピングする例を示します。

```
Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp
Policed-dscp map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    00 00 00 00 00 00 00 00 58 59
      6 :    60 61 62 63
```

（注） このポリシング済み DSCP マップでは、マークダウンされる DSCP 値が表形式で示されています。 d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。 d1 と d2 の交点にある値が、マークダウンされる値です。 たとえば、元の DSCP 値が 53 の場合、マークダウンされる DSCP 値は 0 です。

次に、DSCP 値 0、8、16、24、32、40、48、および 50 を CoS 値 0 にマッピングして、マップを表示する例を示します。

```
Switch(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
Dscp-cos map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
```

```
 0 :    00 00 00 00 00 00 00 00 00 01
 1 :    01 01 01 01 01 01 00 02 02 02
 2 :    02 02 02 02 00 03 03 03 03 03
 3 :    03 03 00 04 04 04 04 04 04 04
 4 :    00 05 05 05 05 05 05 05 00 06
 5 :    00 06 06 06 06 06 07 07 07 07
 6 :    07 07 07 07
```

（注） 上記の DSCP/CoS マップでは、CoS 値が表形式で示されています。 d1 列は DSCP の最上位桁、d2 行は DSCP の最下位桁を示します。 d1 と d2 の交点にある値が CoS 値です。 たとえば、この DSCP/CoS マップでは、DSCP 値が 08 の場合、対応する CoS 値は 0 です。

次の例では、DSCP/DSCP 変換マップを定義する方法を示します。 明示的に設定されていないすべてのエントリは変更されません（空のマップで指定された値のままです）。

```
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
   mutation1:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    00 00 00 00 00 00 00 00 10 10
      1 :    10 10 10 10 14 15 16 17 18 19
      2 :    20 20 20 23 24 25 26 27 28 29
      3 :    30 30 30 30 30 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
```

（注） 上記の DSCP/DSCP 変換マップでは、変換される値が表形式で示されています。 d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。 d1 と d2 の交点の値が、変換される値です。 たとえば、DSCP 値が 12 の場合、対応する変換される値は 10 です。

関連トピック

CoS/DSCP マップの設定, （799 ページ）

IP precedence/DSCP マップの設定, （801 ページ）

ポリシング済み DSCP マップの設定, （802 ページ）

DSCP/CoS マップの設定, （804 ページ）

DSCP/DSCP 変換マップの設定, （805 ページ）

例：入力キューの特性の設定

次の例では、DSCP 値 0 ～ 6 を、入力キュー 1 とドロップしきい値 50% のしきい値 1 にマッピングする方法を示します。 DSCP 値 20 ～ 26 は、入力キュー 1 とドロップしきい値 70% のしきい値 2 にマッピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24
25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

この例では、50% の WTD しきい値が DSCP 値（0 ～ 6）に割り当てられており、70% の WTD しきい値が割り当てられた DSCP 値（20 ～ 26）よりも先にドロップされます。

次の例では、入力キュー 1 にバッファ スペースの 60% を、入力キュー 2 にバッファ スペースの 40% を割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

次に、キューに入力帯域幅を割り当てる例を示します。プライオリティキューイングはディセーブルです。割り当てられる共有帯域幅の比率は、キュー1が25/（25+75）、キュー2が75/（25+75）です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

次に、キューに入力帯域幅を割り当てる例を示します。 キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。 キュー 1 および 2 に割り当てられている帯域幅比率は 4/(4 + 4) です。 SRR は最初、設定された 10% の帯域幅をキュー 1（プライオリティ キュー）にサービスします。 その後、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

関連トピック

入力キュー間のバッファ スペースの割り当て，（810 ページ）

入力キューでのキューイングおよびスケジューリング

入力キュー間の帯域幅の割り当て，（812 ページ）

入力キューでのキューイングおよびスケジューリング

入力プライオリティ キューの設定，（813 ページ）

入力キューでのキューイングおよびスケジューリング

例：出力キューの特性の設定

次の例では、ポートをキューセット 2 にマッピングする方法を示します。 出力キュー 1 にはバッファ スペースの 40%、出力キュー 2、3、および 4 には 20% が割り当てられます。 キュー 2 のド

ロップしきい値は割り当てメモリの 40 および 60% に設定され、割り当てメモリの 100% が保証（確保）され、パケットがドロップされるまでこのキューが使用できる最大メモリが 200% に設定されます。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# queue-set 2
```

次に、DSCP 値 10 および 11 を出力キュー 1 およびしきい値 2 にマッピングする例を示します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11
```

次に、キュー 1 に帯域幅のシェーピングを設定する例を示します。 キュー 2、3、4 の重み比が 0 に設定されているので、これらのキューは共有モードで動作します。 キュー 1 の帯域幅の重みは 1/8（12.5%）です。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

次の例では、出力ポートで稼働する SRR スケジューラの重み比を設定する方法を示します。 4 つのキューが使用され、共有モードで各キューに割り当てられる帯域幅の比率は、キュー 1、2、3、および 4 に対して 1/(1 + 2 + 3 + 4)、2/(1 + 2 + 3 + 4)、3/(1 + 2 + 3 + 4)、および 4/(1 + 2 + 3 + 4) になります（それぞれ、10、20、30、および 40%）。 キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍であることを示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。 出力緊急キューは、設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
Switch(config-if)# end
```

次に、ポートの帯域幅を 80% に制限する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

このコマンドを 80% に設定すると、ポートは該当期間の 20% はアイドルになります。 回線レートは接続速度の 80%（800 Mbps）に低下します。 ただし、ハードウェアはライン レートを 6%単位で調整しているため、この値は厳密ではありません。

関連トピック

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定, （816 ページ）

出力キューでのキューイングおよびスケジューリング

出力キューおよびしきい値 ID への DSCP または CoS 値のマッピング, （820 ページ）

出力キューでのキューイングおよびスケジューリング
出力キューでの SRR シェーピング重みの設定, （822 ページ）

出力キューでのキューイングおよびスケジューリング
出力キューでの SRR 共有重みの設定, （824 ページ）

出力キューでのキューイングおよびスケジューリング
出力緊急キューの設定, （826 ページ）

出力キューでのキューイングおよびスケジューリング
出力インターフェイスの帯域幅の制限, （828 ページ）

出力キューでのキューイングおよびスケジューリング
出力キューでのキューイングおよびスケジューリング

次の作業

QoS 設定でこれらの自動機能を使用できるかどうかについては、自動 QoS のマニュアルを参照してください。

第 33 章

auto-QoS の設定

- 機能情報の確認，843 ページ
- 自動 QoS の前提条件，843 ページ
- 自動 QoS の設定に関する情報，844 ページ
- 自動 QoS の設定方法，850 ページ
- 自動 QoS のモニタリング，854 ページ
- 自動 QoS の設定例，855 ページ
- 自動 QoS の関連情報，865 ページ

機能情報の確認

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

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

自動 QoS の前提条件

標準 QoS または自動 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 使用するアプリケーションのタイプおよびネットワークのトラフィック パターン
- トラフィックの特性およびネットワークのニーズ。 バースト性の高いトラフィックかどうかの判別。 音声およびビデオ ストリーム用の帯域幅確保の必要性

- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

自動 QoS の設定に関する情報

自動 QoS の概要

自動 QoS 機能を使用して、QoS 機能の配置を容易にできます。 自動 QoS は、ネットワーク設計を確認し、スイッチがさまざまなトラフィック フローに優先度を指定できるようにQoS設定をイネーブルにします。 自動 QoS は、デフォルト（ディセーブル）の QoS 動作を使用せずに、出力キューを使用します。 スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供し、単一キューからパケットを送信します。

自動 QoS をイネーブルにすると、トラフィック タイプおよび入力パケット ラベルに基づいてトラフィックを自動的に分類します。 スイッチは分類した結果を使用して適切な出力キューを選択します。

自動 QoS コマンドを使用して、次のシスコ デバイスに接続しているポートを識別できます。

- Cisco IP Phone
- Cisco SoftPhone アプリケーションを実行しているデバイス
- Cisco TelePresence
- Cisco IP Camera
- Cisco Digital Media Player

また、auto-QoS コマンドを使用してアップリンクを介して信頼のおけるトラフィックを受信するポートを指定します。 自動 QoS は次の機能を実行します。

- 条件付きで信頼できるインターフェイスによる自動 QoS デバイスの有無の検出
- QoS 分類の設定
- 出力キューの設定

関連トピック

QoS の概要

自動 QoS 短縮機能の概要

自動 QoS コマンドを入力すると、CLI からコマンドを入力する場合と同様に、生成されたすべてのコマンドがスイッチにより表示されます。 自動 QoS 短縮機能を使用して、実行コンフィギュレーションから自動 QoS が生成したコマンドを非表示にできます。 これにより、実行コンフィギュレーションを容易に把握でき、またメモリをより効率的に使用できるようになります。

生成された自動 QoS 設定

デフォルトでは、自動QoSはすべてのポートでディセーブルです。 パケットは変更されません。つまり、パケットの CoS 値、DSCP 値、および IP precedence 値は変更されません。

インターフェイスの最初のポートで自動 QoS 機能をイネーブルにすると、次のようになります。

- 入力パケット ラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、入力キューと出力キューの設定が行われます。
- QoS は、グローバルにイネーブル（**mls qos** グローバル コンフィギュレーション コマンド）になり、他のグローバル コンフィギュレーション コマンドが自動的に生成されます （例：グローバルな自動 QoS 設定, （855 ページ） を参照）。
- スイッチで信頼境界の機能がイネーブルになり、サポートされているデバイスを検出するために Cisco Discovery Protocol（CDP）が使用されます。
- パケットがプロファイル内にあるかプロファイル外にあるかを判断するためにポリシングが使用され、パケット上のアクションが指定されます。

VOIP デバイスの詳細

以下のアクティビティは、これらの自動 QoS コマンドをポート上で実行する場合に発生します。

- **auto qos voip cisco-phone** コマンドを Cisco IP Phone に接続されたネットワーク エッジにあるポートに入力すると、スイッチは信頼境界機能をイネーブルにします。 パケットに24、26、または46というDSCP値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。 Cisco IP Phone が存在しない場合、入力分類はパケットの QoS ラベルを信用しないように設定されます。 ポリシングは、スイッチが信頼境界機能をイネーブルにする前に、ポリシーマップの分類に一致するトラフィックに適用されます。
- **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを、Cisco SoftPhone を稼働するデバイスに接続されたネットワークのエッジのポートに入力すると、スイッチはポリシングを使用して、パケットがプロファイル内にあるかプロファイル外にあるかを判断し、パケット上のアクションを指定します。 パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。
- ネットワーク内部に接続されたポート上で **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力すると、非ルーテッド ポートの場合は入力パケット内の CoS 値、ルーテッド ポートの場合は入力パケット内の DSCP 値が信頼されます（前提条件は、トラフィックがすでに他のエッジ デバイスによって分類されていることです）。

表 *76*：トラフィック タイプ、パケット ラベル、およびキュー

	VoIP データ トラフィック	VoIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP BPDU トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP の値	46	24、26	48	56	34	–	
CoS 値	5	3	6	7	3	–	
CoS から入力キューへのマッピング	4、5（キュー 2）					0、1、2、3、6、7（キュー 1）	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）			0（キュー 3）	2（キュー 3）	0、1（キュー 4）

スイッチは、次の表の設定値に従ってポートの入力キューを設定します。 次の表は、入力キューに対して生成された自動 QoS の設定を示しています。

表 *77*：入力キューに対する *Auto-QoS* の設定

入力キュー	キュー番号	CoS からキューへのマッピング	キューウェイト（帯域幅）	キュー（バッファ）サイズ
SRR 共有	1	0、1、2、3、6、7	70%	90%
優先度	2	4、5	30%	10%

スイッチは、次の表の設定値に従ってポートの出力キューを設定します。 次の表は、出力キューに対して生成された自動 QoS の設定を示しています。

表 *78*：出力キューに対する *auto-QoS* の設定

出力キュー	出力キュー	キュー番号	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネットポートのキュー（バッファ）サイズ
優先度	**1**	**4、5**	**最大 100%**	**25%**	**15%**
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

- **auto qos voip cisco-phone**、**auto qos voip cisco-softphone**、または **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを使用して自動 QoS をイネーブルにする場合、スイッチはトラフィック タイプおよび入力パケット ラベルに応じて自動的に QoS 設定を生成し、例：グローバルな自動 QoS 設定, （855 ページ） にリストされているコマンドをポートに適用します。

ビデオ、信頼、および分類用の拡張自動 QoS

自動 QoS は、ビデオをサポートするように拡張されました。 ここでは、Cisco TelePresence System と Cisco IP Camera からのトラフィックを分類して信頼する自動設定が生成されます。

自動 QoS 設定の移行

レガシー自動 QoS から拡張自動 QoS への自動 QoS 設定の移行は、次の場合に発生します。

- スイッチが 12.2(55)SE イメージで起動されます。QoS はディセーブルです。

  インターフェイス上のいずれかのビデオまたは音声の信頼設定によって、拡張自動QoS コマンドが自動的に生成されます。

- スイッチが QoS でイネーブルになっている場合（次のガイドラインが適用されます）。
  - 音声デバイスで条件付き信頼用にインターフェイスを設定すると、レガシー自動 QoS VoIP 設定だけが生成されます。
  - ビデオデバイスで条件付き信頼用にインターフェイスを設定すると、拡張自動QoS VoIP 設定が生成されます。

- 新しいインターフェイスの自動 QoS コマンドに基づいて分類または条件き信頼でインターフェイスを設定すると、拡張自動 QoS 設定が生成されます。

- **auto qos srnd4** グローバル コンフィギュレーション コマンドがイネーブルのときに、新しいデバイスを接続すると自動 QoS の移行が発生する場合。

（注） レガシー自動 QoS で以前に設定したインターフェイスが拡張自動 QoS に移行すると、新しいグローバル QoS コマンドに合わせて音声コマンドと設定が更新されます。

拡張自動 QoS からレガシー自動 QoS への自動 QoS 設定の移行が行われるのは、インターフェイスから既存の自動 QoS 設定をすべてディセーブルにした場合だけです。

自動 QoS 設定時の注意事項

自動 QoS を設定する前に、次の事項を確認してください。

- auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップやを変更しないでください。 ポリシー マップやを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやを変更します。 生成したポリシー マップではなくこの新しいポリシー マップを使用するには、生成したポリシーマップをインターフェイスから削除し、新しいポリシー マップをインターフェイスに適用します。
- auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。 必要に応じて QoS 設定を微調整できますが、自動 QoS が完了した後にのみ調整することを推奨します。
- 自動 QoS は、スタティック アクセス、ダイナミックアクセス、音声 VLAN アクセス、およびトランク ポートでイネーブルにできます。
- デフォルトでは、CDP 機能はすべてのポート上でイネーブルです。 自動 QoS が適切に動作するために、CDP をディセーブルにしないでください。

自動 QoS VoIP に関する考慮事項

自動 QoS VoIP を設定する前に、次の事項を確認してください。

- 自動 QoS は、非ルーテッド ポートおよびルーテッド ポートで Cisco IP Phone に VoIP のスイッチを設定します。 また、自動 QoS は Cisco SoftPhone アプリケーションを稼働するデバイスの VoIP 用にスイッチを設定します。

（注） Cisco SoftPhone を稼働するデバイスが非ルーテッド ポートまたはルーテッド ポートに接続されている場合、スイッチはポート単位で Cisco SoftPhone アプリケーション 1 つのみをサポートします。

- ルーテッド ポートで Cisco IP Phone の自動 QoS をイネーブルにすると、スタティック IP アドレスを IP Phone に割り当てます。
- このリリースは、Cisco IP SoftPhone Version 1.3(3) 以降のみをサポートします。
- 接続される装置は Cisco Call Manager バージョン 4 以降を使用する必要があります。

拡張された自動 QoS に関する考慮事項

自動 QoS は、ビデオをサポートするように拡張されました。 ここでは、Cisco TelePresence System と Cisco IP Camera からのトラフィックを分類して信頼する自動設定が生成されます。

拡張自動 QoS を設定する前に、次の事項を確認してください。

- **auto qos srnd4** グローバル コンフィギュレーション コマンドは、拡張自動 QoS 設定の結果として生成されます。

実行コンフィギュレーションでの自動 QoS の影響

自動 QoS がイネーブルになると、**auto qos** インターフェイス コンフィギュレーション コマンドおよび生成されたグローバル コンフィギュレーションが実行コンフィギュレーションに追加されます。

スイッチは、自動 QoS が生成したコマンドを、CLI から入力したように適用します。 既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。 これらのアクションが警告なしで発生する可能性があります。 生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。 上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。 生成コマンドが適用されなかった場合、以前の実行コンフィギュレーションが復元されます。

実行コンフィギュレーションに対する自動 QoS 短縮機能の影響

自動 QoS 短縮機能をイネーブルにした場合：

- CLI から入力された自動 QoS コマンドだけが実行コンフィギュレーションに表示されます。
- 生成されるグローバル コンフィギュレーションおよびインターフェイス コンフィギュレーションは表示されません。
- コンフィギュレーションを保存するときに、入力した自動QoSコマンドだけが保存されます（非表示のコンフィギュレーションは保存されません）。
- スイッチをリロードすると、保存された自動QoSコマンドがシステムにより検出、再実行され、AutoQoS SRND4.0 に準拠したコンフィギュレーション セットが生成されます。

（注） 自動 QoS 短縮機能がイネーブルである場合は、自動 QoS 生成コマンドを変更しないでください。これは、スイッチのリロード時にユーザ変更がオーバーライドされるためです。

自動 QoS グローバル短縮機能をイネーブルにした場合：

- 非表示の AQC 派生コマンドを表示するには、**show derived-config** コマンドを使用します。
- AQC コマンドはメモリに保存されません。 これらは、スイッチがリロードされるたびに再生成されます。
- 短縮機能がイネーブルである場合、自動QoSにより生成されたコマンドは変更しないでください。
- 自動 QoS でインターフェイスが設定されており、AQC をディセーブルにする必要がある場合は、最初に自動 QoS をインターフェイス レベルでディセーブルにする必要があります。

自動 QoS の設定方法

auto-QoS の設定

自動 QoS のイネーブル化

QoS パフォーマンスを最適化するには、ネットワーク内のすべてのデバイスで自動 QoS をイネーブルにします。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. 次のいずれかを使用します。
   - **auto qos voip**{**cisco-phone** | **cisco-softphone** | **trust**}
   - **auto qos video**{**cts** | **ip-camera** | **media-player**}
   - **auto qos classify** [**police**]
   - **auto qos trust** {**cos** | **dscp**}
4. **exit**
5. **interface** *interface-id*
6. **auto qos trust**
7. **end**
8. **show auto qos interface** *interface-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 3/0/1`	ビデオデバイスに接続されたポートか、またはネットワーク内部の別の信頼できるスイッチまたはルータに接続されたアップリンクポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **auto qos voip**{**cisco-phone** | **cisco-softphone** | **trust**} • **auto qos video**{**cts** | **ip-camera** | **media-player**} • **auto qos classify** [**police**] • **auto qos trust** {**cos** | **dscp**} 例： `Switch(config-if)# auto qos trust dscp`	VoIP 用の自動 QoS をイネーブルにします。 • **cisco-phone**：ポートが Cisco IP Phone に接続されている場合、着信パケットの QoS ラベルは電話が検出された場合のみ信頼されます。 • **cisco-softphone**：ポートが Cisco SoftPhone 機能を実行するデバイスに接続されています。 • **trust**：アップリンク ポートが信頼性のあるスイッチまたはルータに接続されていて、入力パケットの VoIP トラフィック分類が信頼されています。 ビデオ デバイス用の自動 QoS をイネーブルにします。 • **cts**：Cisco Telepresence System に接続されているポート。 • **ip-camera**：Cisco Video Surveillance カメラに接続されているポート。 • **media-player**：CDP 対応 Cisco Digital Media Player に接続されているポート。 着信パケットの QoS ラベルが信頼されるのは、システムが検知される場合に限ります。 分類用の自動 QoS をイネーブルにします。 • **police**：QoS ポリシー マップを定義し、それらをポートに適用してポリシングを設定します（ポートベースの QoS）。 信頼できるインターフェイス用の自動 QoS をイネーブルにします。 • **cos**：Class of Service（サービス クラス）。

	コマンドまたはアクション	目的
		• **dscp**：Differentiated Services Code Point（DiffServ コード ポイント） • <cr>：信頼インターフェイス。
ステップ 4	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 2/0/1`	信頼できるスイッチまたはルータに接続されていると識別されたスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**auto qos trust** 例： `Switch(config-if)# auto qos trust`	ポートで自動QoSをイネーブルにし、そのポートが信頼できるルータまたはスイッチに接続されるように指定します。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show auto qos interface** *interface-id* 例： `Switch# show auto qos interface gigabitethernet 2/0/1`	入力を確認します。 このコマンドは、自動QoSがイネーブルであるインターフェイス上の自動 QoS コマンドを表示します。 自動 QoS 設定およびユーザの変更を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

自動 QoS 短縮機能のイネーブル化

自動 QoS 短縮機能をイネーブルにするには、次のコマンドを入力します。

手順の概要

1. **configureterminal**
2. **auto qos global compact**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**auto qos global compact** 例： `Switch(config)# auto qos global compact`	自動QoS短縮機能がイネーブルになり、自動QoSのグローバルコンフィギュレーション（非表示）が生成されます。 その後、インターフェイス コンフィギュレーション モードで設定する自動QoSコマンドを入力できます。システムにより生成されるインターフェイス コマンドも非表示になります。 適用された自動QoS設定を表示するには、次の特権EXECコマンドを使用します。 • **show derived-config** • **show policy-map** • **show access-list** • **show class-map** • **show table-map** • **show auto-qos** • **show policy-map interface** • **show ip access-lists** これらのコマンドにはキーワード「**AutoQos-**」が付きます。

次の作業

自動 QoS 短縮機能をディセーブルにするには、対応する自動 QoS コマンドの **no** 形式を入力して自動 QoS インスタンスをすべてのインターフェイスから削除し、次に **no auto qos global compact** グローバル コンフィギュレーション コマンドを実行します。

自動 QoS に関するトラブルシューティング

自動 QoS のトラブルシューティングを行うには、**debug auto qos** 特権 EXEC コマンドを使用します。 詳細については、このリリースに対応するコマンド リファレンスにある **debug auto qos** コマンドを参照してください。

ポートで自動 QoS をディセーブルにするには、**auto qos** コマンドのインターフェイス コンフィギュレーション コマンドの **no** 形式（**no auto qos voip** など）を使用します。 このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。 auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

自動 QoS のモニタリング

表 *79*：自動 *QoS* のモニタリング用コマンド

コマンド	説明
show auto qos [**interface** [*interface-type*]]	最初の自動 QoS 設定を表示します。 **show auto qos** コマンド出力と **show running-config** コマンド出力を比較してユーザ定義の QoS 設定を比較できます。
show mls qos [**aggregate policer** | **interface** | **maps** | **queue-set** | **stack-port** | **stack-qset**]	自動 QoS によって影響されるかもしれない QoS 設定に関する情報を表示します。
show mls qos aggregate policer *policer_name*	自動 QoS によって影響される可能性がある QoS 集約ポリサー設定に関する情報を表示します。
show mls qos interface [*interface-type* | **buffers** | **policers** | **queueing** | **statistics**]	自動 QoS の影響を受ける可能性がある QoS インターフェイス設定に関する情報を表示します。
show mls qos maps [**cos-dscp** | **cos-output-q** | **dscp-cos** | **dscp-mutation** | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**]	自動 QoS によって影響されるかもしれない QoS マップ設定に関する情報を表示します。
show mls qos queue-set *queue-set ID*	自動 QoS によって影響されるかもしれない QoS キューセット設定に関する情報を表示します。
show mls qos stack-port buffers	自動 QoS によって影響されるかもしれない QoS スタック ポート バッファ設定に関する情報を表示します。

コマンド	説明
show mls qos stack-qset	自動 QoS によって影響されるかもしれない QoS スタック キューセット設定に関する情報を表示します。
show running-config	自動 QoS によって影響されるかもしれない QoS 設定に関する情報を表示します。 **show auto qos** コマンド出力と **show running-config** コマンド出力を比較してユーザ定義の QoS 設定を比較できます。

自動 QoS の設定例

例：グローバルな自動 QoS 設定

次の表は、自動 QoS および拡張自動 QoS に対してスイッチによって自動的に生成されたコマンドを説明しています。

表 *80*： 生成された自動 *QoS* 設定

説明	自動的に生成されるコマンド **{voip}**	自動的に生成される拡張コマンド **{Video|Trust|Classify}**
スイッチが自動的に標準 QoS をイネーブルにして Cos/DSCP マップ（着信パケットの CoS 値の DSCP 値へのマッピング）を設定します。	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp** **0 8 16 26 32 46 48 56**	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp** **0 8 16 24 32 46 48 56**
スイッチが、自動的に CoS 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 4 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 2 3** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 0** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 1**
スイッチが、自動的に DSCP 値を出力キューおよびしきい値 ID にマッピングします。		

説明	自動的に生成されるコマンド **{voip}**	自動的に生成される拡張コマンド **{Video|Trust|Classify}**
	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 2 24** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14**

説明	自動的に生成されるコマンド {voip}	自動的に生成される拡張コマンド {Video|Trust|Classify}
スイッチが自動的に出力キューのバッファサイズを設定します。ポートにマッピングされた出力キューの帯域幅と SRR モード（シェーピングまたは共有）を設定します。	Switch(config)# **mls qos queue-set output 1 threshold 1 138 138 92 138** Switch(config)# **mls qos queue-set output 1 threshold 2 138 138 92 400** Switch(config)# **mls qos queue-set output 1 threshold 3 36 77 100 318** Switch(config)# **mls qos queue-set output 1 threshold 4 20 50 67 400** Switch(config)# **mls qos queue-set output 2 threshold 1 149 149 100 149** Switch(config)# **mls qos queue-set output 2 threshold 2 118 118 100 235** Switch(config)# **mls qos queue-set output 2 threshold 3 41 68 100 272** Switch(config)# **mls qos queue-set output 2 threshold 4 42 72 100 242** Switch(config)# **mls qos queue-set output 1 buffers 10 10 26 54** Switch(config)# **mls qos queue-set output 2 buffers 16 6 17 61** Switch(config-if)# **priority-queue out** Switch(config-if)# **srr-queue bandwidth share 10 10 60 20**	Switch(config)# **mls qos queue-set output 1 threshold 2 100 100 50 200** Switch(config)# **mls qos queue-set output 1 threshold 2 125 125 100 400** Switch(config)# **mls qos queue-set output 1 threshold 3 100 100 100 400** Switch(config)# **mls qos queue-set output 1 threshold 4 60 150 50 200** Switch(config)# **mls qos queue-set output 1 buffers 15 25 40 20**

例：VoIP デバイス用に生成される自動 QoS 設定

次の表は、スイッチで VoIP デバイスの自動 QoS に対して自動的に生成されるコマンドについて説明しています。

表 *81*：*VoIP* デバイス用に生成される自動 *QoS* 設定

説明	自動的に生成されるコマンド（VoIP）
スイッチが自動的に標準 QoS をイネーブルにして Cos/DSCP マップ（着信パケットの CoS 値の DSCP 値へのマッピング）を設定します。	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 26 32 46 48 56**
スイッチが、自動的に CoS 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**
スイッチが、自動的に DSCP 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**
スイッチが自動的に出力キューのバッファサイズを設定します。ポートにマッピングされた出力キューの帯域幅と SRR モード（シェーピングまたは共有）を設定します。	

説明	自動的に生成されるコマンド（VoIP）
	SwitchSwitchconfig)# **mls qos queue-set output 1 threshold 1 138 138 92 138** Switch(config)# **mls qos queue-set output 1 threshold 2 138 138 92 400** Switch(config)# **mls qos queue-set output 1 threshold 3 36 77 100 318** Switch(config)# **mls qos queue-set output 1 threshold 4 20 50 67 400** Switch(config)# **mls qos queue-set output 2 threshold 1 149 149 100 149** Switch(config)# **mls qos queue-set output 2 threshold 2 118 118 100 235** Switch(config)# **mls qos queue-set output 2 threshold 3 41 68 100 272** Switch(config)# **mls qos queue-set output 2 threshold 4 42 72 100 242** Switch(config)# **mls qos queue-set output 1 buffers 10 10 26 54** Switch(config)# **mls qos queue-set output 2 buffers 16 6 17 61** Switch(config-if)# **priority-que out** Switch(config-if)# **srr-queue bandwidth share 10 10 60 20**

auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的に信頼境界機能をイネーブルにし、CDP を使用して Cisco IP Phone の有無を検出します（以下を参照）。

```
Switch(config-if)# mls qos trust device cisco-phone
```

auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します（以下を参照）。

```
Switch(config)# mls qos map policed-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Police-SoftPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ（別名 *AutoQoS-Police-SoftPhone*）を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します（以下を参照）。

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

例：VoIP デバイス用に生成される自動 QoS 設定

auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的に信頼境界機能をイネーブルにし、CDP を使用して Cisco IP Phone の有無を検出します。

```
Switch(config-if)# mls qos trust device cisco-phone
```

auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

```
Switch(config)# mls qos map policed-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Police-SoftPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ（別名 *AutoQoS-Police-SoftPhone*）を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

```
Switch(config-if)# mls qos trust device cisco-phone
```

auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

```
Switch(config)# mls qos map policed-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Police-CiscoPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ（別名 *AutoQoS-Police-SoftPhone*）を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

例：拡張されたビデオ、信頼、および分類デバイス用に自動 QoS で生成される設定

次の拡張自動 QoS コマンドを入力すると、スイッチは CoS/DSCP のマッピングを設定します（着信パケットの CoS 値を DSCP 値にマップします）。

- **auto qos video cts**
- **auto qos video ip-camera**
- **auto qos video media-player**
- **auto qos trust**
- **auto qos trust cos**
- **auto qos trust dscp**

次のコマンドは、上記の自動 QoS コマンドのいずれかを入力した後に開始されます。

```
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

（注） クラス マップとポリシー マップは設定されません。

auto qos classify コマンドを入力すると、スイッチが自動的にクラスマップおよびポリシーマップを作成します（以下を参照）。

```
Switch(config)# mls qos map policed-dscp 0 10 18 24 26 46 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICY
```

auto qos classify police コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します（以下を参照）。

```
Switch(config)# mls qos map policed-dscp 0 10 18 24 26 46 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# police 10000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
```

これは、**auto qos voip cisco-phone** コマンドの拡張コンフィギュレーションです。

```
Switch(config)# mls qos map policed-dscp 0 10 18 24 26 46 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
```

これは、**auto qos voip cisco-softphone** コマンドの拡張コンフィギュレーションです。

```
Switch(config)# mls qos map policed-dscp 0 10 18 24 26 46 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

```
Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER

Switch(config)# policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)#class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)#set dscp af41
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# police 10000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY
```

auto qos global compact

次に、**auto qos global compact** コマンドの例を示します。

```
Switch# configure terminal
Switch(config)# auto qos global compact
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# auto qos voip cisco-phone

Switch# show auto-qos

GigabitEthernet1/2
auto qos voip cisco-phone

Switch# show running-config interface GigabitEthernet 1/0/2

interface GigabitEthernet1/0/2
auto qos voip cisco-phone
end
```

自動 QoS の関連情報

自動 QoS 設定で特定の QoS の変更をする必要がある場合は、QoS のマニュアルを確認してください。

第 VII 部

ルーティング

- IP ユニキャスト ルーティングの設定，869 ページ
- フォールバック ブリッジングの設定，1047 ページ

第 34 章

IP ユニキャスト ルーティングの設定

- 機能情報の確認，870 ページ
- IP ユニキャスト ルーティングの設定に関する情報，870 ページ
- IP ルーティングに関する情報，870 ページ
- IP ルーティングの設定方法，871 ページ
- IP アドレッシングの設定方法，872 ページ
- IP アドレスのモニタリングおよびメンテナンス，898 ページ
- IP ユニキャスト ルーティングの設定方法，899 ページ
- RIP 情報，900 ページ
- RIP の設定方法，901 ページ
- OSPF に関する情報，910 ページ
- OSPF のモニタリング，926 ページ
- EIGRP に関する情報，927 ページ
- EIGRP の設定方法，929 ページ
- EIGRP のモニタリングおよびメンテナンス，939 ページ
- BGP に関する情報，940 ページ
- BGP の設定方法，941 ページ
- BGP のモニタリングおよびメンテナンス，974 ページ
- ISO CLNS ルーティングに関する情報，976 ページ
- ISO CLNS ルーティングの設定方法，977 ページ
- ISO IGRP と IS-IS のモニタリングおよびメンテナンス，990 ページ
- Multi-VRF CE に関する情報，993 ページ

- Multi-VRF CE の設定方法，996 ページ
- ユニキャスト リバース パス転送の設定，1018 ページ
- プロトコル独立機能，1019 ページ
- IP ネットワークのモニタリングおよびメンテナンス，1045 ページ

機能情報の確認

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

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

IP ユニキャスト ルーティングの設定に関する情報

このモジュールでは、スイッチで IP Version 4（IPv4）ユニキャスト ルーティングを設定する方法について説明します。

スタティック ルーティング、Routing Information Protocol（RIP）などの基本的なルーティング機能は、で使用できます。 Catalyst 3560-CX スイッチの IP Base フィーチャ セットおよび IP Services フィーチャセット。 Catalyst 2960-CX スイッチではスタティック ルーティングのみをサポートします。

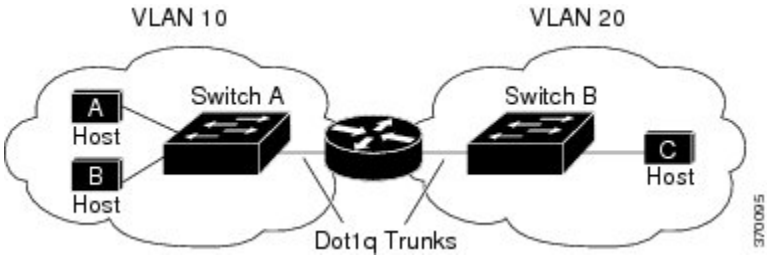
（注） IPv4 トラフィックに加えて、IP バージョン 6（IPv6）ユニキャストルーティングをイネーブルにし、IPv6 トラフィックを転送するようにインターフェイスを設定できます。

IP ルーティングに関する情報

一部のネットワーク環境で、VLAN（仮想 LAN）は各ネットワークまたはサブネットワークに関連付けられています。 IP ネットワークで、各サブネットワークは 1 つの VLAN に対応しています。 VLAN を設定すると、ブロードキャスト ドメインのサイズを制御し、ローカル トラフィックをローカル内にとどめることができます。 ただし、異なる VLAN 内のネットワーク デバイスが相互に通信するには、VLAN 間でトラフィックをルーティング（VLAN 間ルーティング）するレイヤ 3 デバイス（ルータ）が必要です。 VLAN 間ルーティングでは、適切な宛先 VLAN にトラフィックをルーティングするため、1 つまたは複数のルータを設定します。

次の図に基本的なルーティング トポロジを示します。 スイッチ A は VLAN 10 内、スイッチ B は VLAN 20 内にあります。 ルータには各 VLAN のインターフェイスが備わっています。

図 *69* : ルーティング トポロジの例



VLAN 10 内のホスト A が VLAN 10 内のホスト B と通信する場合、ホスト A はホスト B 宛にアドレス指定されたパケットを送信します。 スイッチ A はパケットをルータに送信せず、ホスト B に直接転送します。

ホスト A から VLAN 20 内のホスト C にパケットを送信する場合、スイッチ A はパケットをルータに転送し、ルータは VLAN 10 インターフェイスでトラフィックを受信します。 ルータはルーティング テーブルを調べて正しい発信インターフェイスを判別し、VLAN 20 インターフェイスを経由してパケットをスイッチ B に送信します。スイッチ B はパケットを受信し、ホスト C に転送します。

ルーティング タイプ

ルータおよびレイヤ 3 スイッチは、次の方法でパケットをルーティングできます。

- デフォルト ルーティング
- 事前にプログラミングされているトラフィックのスタティック ルートの使用
- ルーティング プロトコルによるルートの動的な計算

スイッチでは、スタティック ルートとデフォルト ルートはサポートされますが、ルーティング プロトコルはサポートされていません。

IP ルーティングの設定方法

スイッチ上で、IP ルーティングはデフォルトでディセーブルとなっているため、ルーティングを行う前に、IP ルーティングをイネーブルにする必要があります。 IP ルーティングに関する設定情報については、『*Cisco IOS IP Configuration Guide*』を参照してください。

次の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。

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

- スイッチ仮想インターフェイス（SVI）：**interface vlan***vlan_id* グローバル コンフィギュレーション コマンドによって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
- レイヤ 3 モードの Etherchannel ポート チャネル：**interface port-channel***port-channel-number* グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャネル グループにバインドして作成されたポートチャネル論理インターフェイスです。 詳細については、『Layer 2 Configuration Guide』の「Configuring Layer 3 EtherChannels」の章を参照してください。

（注） スイッチは、ユニキャスト ルーテッド トラフィックのトンネル インターフェイスをサポートしません。

ルーティングが発生するすべてのレイヤ 3 インターフェイスに、IP アドレスを割り当てる必要があります。

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

ルーティングを設定するための主な手順は次のとおりです。

- VLAN インターフェイスをサポートするには、スイッチまたはスイッチ スタックで VLAN を作成および設定し、レイヤ 2 インターフェイスに VLAN メンバーシップを割り当てます。詳細については、『VLAN Configuration Guide』の「Configuring VLANs」の章を参照してください。
- レイヤ 3 インターフェイスを設定します。
- スイッチ上で IP ルーティングをイネーブルに設定します。
- レイヤ 3 インターフェイスに IP アドレスを割り当てます。
- 選択したルーティング プロトコルをスイッチ上でイネーブルにします。
- ルーティング プロトコル パラメータを設定します（任意）。

関連トピック

ネットワーク インターフェイスへの IP アドレスの割り当て，（874 ページ）

IP アドレッシングの設定方法

IP ルーティングを設定するには、レイヤ 3 ネットワーク インターフェイスに IP アドレスを割り当ててインターフェイスをイネーブルにし、IP を使用するインターフェイスを経由してホストとの通信を許可する必要があります。 次の項では、さまざまなIPアドレス指定機能の設定方法につ

いて説明します。 IP アドレスをインターフェイスに割り当てる手順は必須ですが、その他の手順は任意です。

- アドレス指定のデフォルト設定
- ネットワーク インターフェイスへの IP アドレスの割り当て
- アドレス解決方法の設定
- IP ルーティングがディセーブルの場合のルーティング支援機能
- ブロードキャスト パケットの処理方法の設定
- IP アドレスのモニタリングおよびメンテナンス

IP アドレス指定のデフォルト設定

表 *82*：アドレス指定のデフォルト設定

機能	デフォルト設定
IP アドレス	未定義
ARP	ARP キャッシュに永続的なエントリはありません カプセル化：標準イーサネット形式の ARP 14400 秒（4 時間）
IP ブロードキャスト アドレス	255.255.255.255（すべて 1）
IP クラスレス ルーティング	イネーブル
IP デフォルト ゲートウェイ	ディセーブル
IP ダイレクト ブロードキャスト	ディセーブル（すべての IP ダイレクト ブロードキャストがドロップされます）
IP ドメイン	ドメイン リスト：ドメイン名は未定義 ドメイン検索：イネーブル ドメイン名：イネーブル

機能	デフォルト設定
IP 転送プロトコル	ヘルパー アドレスが定義されているか、またはユーザ データグラム プロトコル（UDP）フラッディングが設定されている場合、デフォルト ポートでは UDP 転送がイネーブルとなります ローカル ブロードキャスト：ディセーブル スパニングツリー プロトコル（STP）：ディセーブル ターボフラッディング：ディセーブル
IP ヘルパー アドレス	ディセーブル
IP ホスト	ディセーブル
ICMP Router Discovery Protocol（IRDP）	ディセーブル イネーブルの場合のデフォルト： • ブロードキャスト IRDP アドバタイズメント • アドバタイズメント間の最大インターバル：600 秒 • アドバタイズ間の最小インターバル：最大インターバルの 0.75 倍 • プリファレンス：0
IP プロキシ ARP	イネーブル
IP ルーティング	ディセーブル
IP サブネットゼロ	ディセーブル

ネットワーク インターフェイスへの IP アドレスの割り当て

IP アドレスは IP パケットの送信先を特定します。 一部の IP アドレスは特殊な目的のために予約されていて、ホスト、サブネット、またはネットワーク アドレスには使用できません。 RFC 1166 の『Internet Numbers』には IP アドレスに関する公式の説明が記載されています。

インターフェイスには、1 つのプライマリ IP アドレスを設定できます。 マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。 マスクを使用してネットワークをサブネット化する場合、そのマスクをサブネットマスクと呼びます。 割り当てられているネットワーク番号については、インターネット サービス プロバイダーにお問い合わせください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 5	**ip address***ip-address subnet-mask* 例： `Switch(config-if)# ip address 10.1.5.1 255.255.255.0`	IP アドレスおよび IP サブネット マスクを設定します。
ステップ 6	**no shutdown** 例： `Switch(config-if)# no shutdown`	物理インターフェイスをイネーブルにします。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip route** 例： `Switch# show ip route`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 9	**show ip interface** [*interface-id*] 例： `Switch# show ip interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IP ルーティングの設定方法, （871 ページ）

サブネット ゼロの使用

サブネット アドレスがゼロであるサブネットを作成しないでください。同じアドレスを持つネットワークおよびサブネットがある場合に問題が発生することがあります。 たとえば、ネットワーク 131.108.0.0 のサブネットが 255.255.255.0 の場合、サブネット ゼロは 131.108.0.0 と記述され、ネットワーク アドレスと同じとなってしまいます。

すべてが 1 のサブネット（131.108.255.0）は使用可能です。また、IP アドレス用にサブネット スペース全体が必要な場合は、サブネット ゼロの使用をイネーブルにできます（ただし推奨できません）。

デフォルトに戻して、サブネット ゼロの使用をディセーブルにするには、**no ip subnet-zero** グローバル コンフィギュレーション コマンドを使用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip subnet-zero** 例： `Switch(config)# ip subnet-zero`	インターフェイス アドレスおよびルーティングのアップデート時にサブネット ゼロの使用をイネーブルにします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

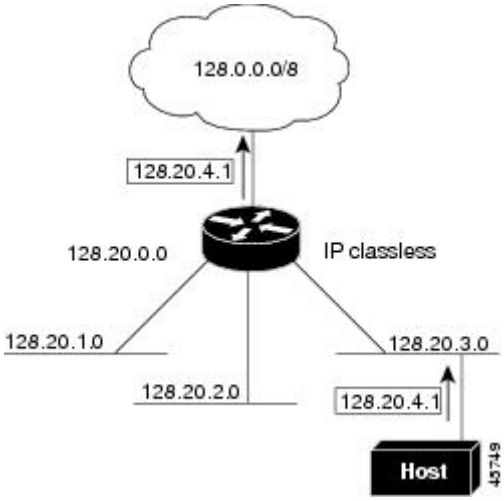
クラスレス ルーティング

ルーティングを行うように設定されたスイッチで、クラスレス ルーティング動作はデフォルトでイネーブルとなっています。 クラスレス ルーティングがイネーブルの場合、デフォルト ルートがないネットワークのサブネット宛てパケットをルータが受信すると、ルータは最適なスーパーネットルートにパケットを転送します。 スーパーネットは、単一の大規模アドレス空間をシミュ

レートするために使用されるクラスCアドレス空間の連続ブロックで構成されています。スーパーネットは、クラス B アドレス空間の急速な枯渇を回避するために設計されました。

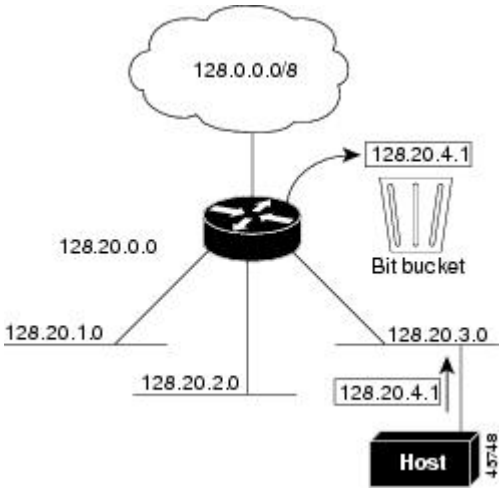
図では、クラスレス ルーティングがイネーブルとなっています。 ホストがパケットを 128.20.4.1 に送信すると、ルータはパケットを廃棄せずに、最適なスーパーネットルートに転送します。 クラスレスルーティングがディセーブルの場合、デフォルトルートがないネットワークのサブネット宛てパケットを受信したルータは、パケットを廃棄します。

図 *70*：*IP* クラスレス ルーティングがイネーブルの場合



図では、ネットワーク 128.20.0.0 のルータはサブネット 128.20.1.0、128.20.2.0、128.20.3.0 に接続されています。 ホストがパケットを 128.20.4.1 に送信した場合、ネットワークのデフォルト ルートが存在しないため、ルータはパケットを廃棄します。

図 *71*：*IP* クラスレス ルーティングがディセーブルの場合



スイッチが認識されないサブネット宛てのパケットを最適なスーパーネット ルートに転送しないようにするには、クラスレス ルーティング動作をディセーブルにします。

クラスレス ルーティングのディセーブル化

スイッチが認識されないサブネット宛てのパケットを最適なスーパーネット ルートに転送しないようにするには、クラスレス ルーティング動作をディセーブルにします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ip classless** 例： `Switch(config)#no ip classless`	クラスレスルーティング動作をディセーブルにします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

アドレス解決方法の設定

アドレス解決を設定するために必要な作業は次のとおりです。

アドレス解決

インターフェイス固有の IP 処理方法を制御するには、アドレス解決を行います。 IP を使用するデバイスには、ローカル セグメントまたは LAN 上のデバイスを一意に定義するローカル アドレス（MAC アドレス）と、デバイスが属するネットワークを特定するネットワーク アドレスがあります。

（注） スイッチスタックでは、スタックの単一のMACアドレスおよびIPアドレスを使用して、ネットワーク通信を行います。

ローカルアドレス（MAC アドレス）は、パケット ヘッダーのデータ リンク層（レイヤ 2）セクションに格納されて、データ リンク（レイヤ 2）デバイスによって読み取られるため、データ リンク アドレスと呼ばれます。 ソフトウェアがイーサネット上のデバイスと通信するには、デバイスの MAC アドレスを学習する必要があります。 IP アドレスから MAC アドレスを学習するプロセスを、アドレス解決と呼びます。 MAC アドレスから IP アドレスを学習するプロセスを、逆アドレス解決と呼びます。

スイッチでは、次の形式のアドレス解決を行うことができます。

- ARP：IP アドレスを MAC アドレスと関連付けるために使用されます。 ARP は IP アドレスを入力と解釈し、対応する MAC アドレスを学習します。次に、IP アドレス/MAC アドレス アソシエーションを ARP キャッシュにストアし、すぐに取り出せるようにします。 その後、IP データグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。 イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化、および ARP 要求や応答については、サブネットワーク アクセス プロトコル（SNAP）で規定されています。
- プロキシ ARP：ルーティング テーブルを持たないホストで、他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにします。 スイッチ（ルータ）が送信元と異なるインターフェイス上のホストに宛てた ARP 要求を受信した場合、そのルータに他のインターフェイスを経由してそのホストに至るすべてのルートが格納されていれば、ルータは自身のローカル データ リンク アドレスを示すプロキシ ARP パケットを生成します。 ARP 要求を送信したホストはルータにパケットを送信し、ルータはパケットを目的のホストに転送します。

スイッチでは、ARP と同様の機能（ローカル MAC アドレスでなく IP アドレスを要求する点を除く）を持つ Reverse Address Resolution Protocol（RARP）を使用することもできます。 RARP を使用するには、ルータ インターフェイスと同じネットワーク セグメント上に RARP サーバを設置する必要があります。 サーバを識別するには、**ip rarp-server***address* インターフェイス コンフィギュレーション コマンドを使用します。

RARP の詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』を参照してください。

スタティック ARP キャッシュの定義

ARP および他のアドレス解決プロトコルを使用すると、IP アドレスと MAC アドレス間をダイナミックにマッピングできます。 ほとんどのホストではダイナミックアドレス解決がサポートされているため、通常の場合、スタティック ARP キャッシュエントリを指定する必要はありません。スタティック ARP キャッシュエントリを定義する必要がある場合は、グローバルにそれを定義できます。グローバルに定義すると、IP アドレスを MAC アドレスに変換するためにスイッチが使用するARP キャッシュに永続的なエントリをインストールします。 また、指定された IP アドレスに属しているかのように、スイッチが ARP 要求に応答するように指定することもできます。ARP エントリを永続的なエントリにしない場合は、ARP エントリのタイムアウト期間を指定できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**arp***ip-address hardware-address type* 例： `Switch(config)# ip 10.1.5.1 c2f3.220a.12f4 arpa`	ARP キャッシュ内で IP アドレスを MAC（ハードウェア）アドレスに関連付け、次に示すカプセル化タイプのいずれかを指定します。 • **arpa**：ARP カプセル化（イーサネット インターフェイス用） • **snap**：SNAP カプセル化（トークン リングおよび FDDI インターフェイス用） • **sap**：HP の ARP タイプ

	コマンドまたはアクション	目的
ステップ 4	**arp***ip-address hardware-address type* [**alias**] 例： `Switch(config)# ip 10.1.5.3 d7f3.220d.12f5 arpa alias`	（任意）指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定します。
ステップ 5	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 6	**arp***timeout seconds* 例： `Switch(config-if)# arp 20000`	（任意）ARP キャッシュ エントリがキャッシュに保持される期間を設定します。 デフォルト値は 14400 秒（4 時間）です。 指定できる範囲は 0 ～ 2147483 秒です。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** [*interface-id*] 例： `Switch# show interfaces gigabitethernet 1/0/1`	すべてのインターフェイスまたは特定のインターフェイスで使用される ARP のタイプおよびタイムアウト値を確認します。
ステップ 9	**show arp** 例： `Switch# show arp`	ARP キャッシュの内容を表示します。
ステップ 10	**show ip arp** 例： `Switch# show ip arp`	ARP キャッシュの内容を表示します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ARP のカプセル化の設定

IP インターフェイスでは、イーサネット ARP カプセル化（**arpa** キーワードで表される）がデフォルトでイネーブルに設定されています。 ネットワークの必要性に応じて、カプセル化方法を SNAP に変更できます。

カプセル化タイプをディセーブルにするには、**no arp arpa** または **no arp snap** インターフェイス コンフィギュレーション コマンドを使用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/2`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**arp** {**arpa** | **snap**} 例： `Switch(config-if)# arp arpa`	ARP カプセル化方法を指定します。 • **arpa**：Address Resolution Protocol • **snap**：Subnetwork Address Protocol
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*] 例： `Switch# show interfaces`	すべてのインターフェイスまたは指定されたインターフェイスの ARP カプセル化設定を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

プロキシ ARP のイネーブル化

デフォルトでは、プロキシARPがスイッチで使用されます。ホストが他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにするためです。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/2`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip proxy-arp** 例： `Switch(config-if)# ip proxy-arp`	インターフェイス上でプロキシ ARP をイネーブルにします。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show ip interface** [*interface-id*] 例： `Switch# show ip interface gigabitethernet 1/0/2`	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ルーティングがディセーブルの場合のルーティング支援機能

次のメカニズムを使用することで、スイッチは IP ルーティングがイネーブルでない場合、別のネットワークへのルートを学習できます。

- プロキシ ARP
- デフォルト ゲートウェイ
- ICMP Router Discovery Protocol（IRDP）

プロキシ ARP

プロキシ ARP は、他のルートを学習する場合の最も一般的な方法です。プロキシ ARP を使用すると、ルーティング情報を持たないイーサネット ホストと、他のネットワークまたはサブネット上のホストとの通信が可能になります。 このホストでは、すべてのホストが同じローカルイーサネット上にあり、ARP を使用して MAC アドレスを学習すると想定されています。 スイッチが送信元と異なるネットワーク上にあるホストに宛てた ARP 要求を受信した場合、スイッチはそのホストへの最適なルートがあるかどうかを調べます。 最適なルートがある場合、スイッチはスイッチ自身のイーサネット MAC アドレスが格納された ARP 応答パケットを送信します。要求の送信元ホストはパケットをスイッチに送信し、スイッチは目的のホストにパケットを転送します。 プロキシ ARP は、すべてのネットワークをローカルな場合と同様に処理し、IP アドレスごとに ARP 処理を実行します。

プロキシ ARP

プロキシ ARP は、デフォルトでイネーブルに設定されています。 ディセーブル化されたプロキシ ARP をイネーブルにするには、「プロキシ ARP のイネーブル化」の項を参照してください。 プロキシ ARP は、他のルータでサポートされているかぎり有効です。

デフォルト ゲートウェイ

ルートを特定するもう 1 つの方法は、デフォルト ルータ、つまりデフォルト ゲートウェイを定義する方法です。 ローカルでないすべてのパケットはこのルータに送信されます。このルータは適切なルーティングを行う、または IP 制御メッセージ プロトコル（ICMP）リダイレクト メッセージを返信するという方法で、ホストが使用するローカルルータを定義します。 スイッチはリダイレクトメッセージをキャッシュに格納し、各パケットをできるだけ効率的に転送します。 この方法には、デフォルト ルータがダウンした場合、または使用できなくなった場合に、検出が不可能となる制限があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip default-gateway***ip-address* 例： `Switch(config)# ip default gateway 10.1.5.1`	デフォルト ゲートウェイ（ルータ）を設定します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip redirects** 例： `Switch# show ip redirects`	設定を確認するため、デフォルト ゲートウェイ ルータのアドレスを表示します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ICMP Router Discovery Protocol

ルータ ディスカバリを使用すると、スイッチはICMP Router Discovery Protocol（IRDP）を使用し、他のネットワークへのルートを動的に学習します。 ホストは IRDP を使用し、ルータを特定します。 クライアントとして動作しているスイッチは、ルータ ディスカバリ パケットを生成します。 ホストとして動作しているスイッチは、ルータ ディスカバリ パケットを受信します。 スイッチはRouting Information Protocol（RIP）ルーティングのアップデートを受信し、この情報を使用してルータの場所を推測することもできます。 実際のところ、ルーティングデバイスによって送信されたルーティング テーブルは、スイッチにストアされません。どのシステムがデータを送信しているのかが記録されるだけです。 IRDP を使用する利点は、プライオリティと、パケットが受信されなくなってからデバイスがダウンしていると見なされるまでの期間の両方をルータごとに指定できることです。

検出された各デバイスは、デフォルトルータの候補となります。現在のデフォルトルータがダウンしたと宣言された場合、または再送信が多すぎて TCP 接続がタイムアウトになりつつある場合、プライオリティが上位のルータが検出されると、最も高いプライオリティを持つ新しいルータが選択されます。

ICMP Router Discovery Protocol（IRDP）

インターフェイスでIRDPルーティングを行う場合は、インターフェイスでIRDP処理をイネーブルにしてください。 IRDP処理をイネーブルにすると、デフォルトのパラメータが適用されます。

これらのパラメータを変更することもできます。 **maxadvertinterval** 値を変更すると、**holdtime** 値および **minadvertinterval** 値も変更されます。最初に **maxadvertinterval** 値を変更し、次に **holdtime** 値または **minadvertinterval** 値のいずれかを手動で変更することが重要です。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip irdp** 例： `Switch(config-if)# ip irdp`	インターフェイスで IRDP 処理をイネーブルにします。
ステップ 5	**ip irdp multicast** 例： `Switch(config-if)# ip irdp multicast`	（任意）IP ブロードキャストの代わりとして、マルチキャスト アドレス（224.0.0.1）に IRDP アドバタイズを送信します。 （注） このコマンドを使用すると、IRDP パケットをマルチキャストとして送信するサンマイクロシステムズ社の Solaris との互換性を維持できます。 実装機能の中には、これらのマルチキャストを受信できないものも多くあります。このコマンドを使用する前に、エンドホストがこの機能に対応していることを確認してください。
ステップ 6	**ip irdp holdtime***seconds* 例： `Switch(config-if)# ip irdp holdtime 1000`	（任意）アドバタイズが有効である IRDP 期間を設定します。デフォルト値は **maxadvertinterval** 値の 3 倍です。**maxadvertinterval** 値よりも大きな値（9000 秒以下）を指定する必要があります。 **maxadvertinterval** 値を変更すると、この値も変更されます。
ステップ 7	**ip irdp maxadvertinterval***seconds* 例： `Switch(config-if)# ip irdp maxadvertinterval 650`	（任意）アドバタイズメントの IRDP 最大間隔を設定します。デフォルトは 600 秒です。
ステップ 8	**ip irdp minadvertinterval***seconds* 例： `Switch(config-if)# ip irdp minadvertinterval 500`	（任意）アドバタイズ間の IRDP の最小インターバルを設定します。 デフォルト値は **maxadvertinterval** 値の 0.75 倍です。**maxadvertinterval** を変更すると、この値も新しいデフォルト値（**maxadvertinterval** の 0.75 倍）に変更されます。
ステップ 9	**ip irdp preference***number* 例： `Switch(config-if)# ip irdp preference 2`	（任意）デバイスの IRDP プリファレンス レベルを設定します。 指定できる範囲は -231 ～ 231 です。 デフォルトは 0 です。 大きな値を設定すると、ルータのプリファレンス レベルも高くなります。

	コマンドまたはアクション	目的
ステップ 10	**ip irdp address***address* [*number*] 例： `Switch(config-if)# ip irdp address 10.1.10.10`	（任意）プロキシ アドバタイズを行うための IRDP アドレスとプリファレンスを設定します。
ステップ 11	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show ip irdp** 例： `Switch# show ip irdp`	IRDP 値を表示し、設定を確認します。
ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ブロードキャスト パケットの処理方法の設定

これらの方式をイネーブルにするには、次に示す作業を実行します。

- ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化
- UDP ブロードキャスト パケットおよびプロトコルの転送
- IP ブロードキャスト アドレスの確立
- IP ブロードキャストのフラッディング

ブロードキャスト パケットの処理

IP インターフェイス アドレスを設定したあとで、ルーティングをイネーブルにしたり、1 つまたは複数のルーティングプロトコルを設定したり、ネットワークブロードキャストへのスイッチの応答方法を設定したりできます。 ブロードキャストは、物理ネットワーク上のすべてのホスト宛てのデータ パケットです。 スイッチでは、2 種類のブロードキャストがサポートされています。

- ダイレクト ブロードキャスト パケット：特定のネットワークまたは一連のネットワークに送信されます。 ダイレクト ブロードキャスト アドレスには、ネットワークまたはサブネット フィールドが含まれます。
- フラッディング ブロードキャスト パケット：すべてのネットワークに送信されます。

（注） **storm-control** インターフェイス コンフィギュレーション コマンドを使用して、トラフィック抑制レベルを設定し、レイヤ 2 インターフェイスでブロードキャスト、ユニキャスト、マルチキャスト トラフィックを制限することもできます。

ルータはローカル ケーブルまでの範囲を制限して、ブロードキャスト ストームを防ぎます。 ブリッジ（インテリジェントなブリッジを含む）はレイヤ 2 デバイスであるため、ブロードキャストはすべてのネットワーク セグメントに転送され、ブロードキャスト ストームを伝播します。 ブロードキャスト ストーム問題を解決する最善の方法は、ネットワーク上で単一のブロードキャスト アドレス方式を使用することです。 最新の IP 実装機能ではほとんどの場合、アドレスをブロードキャストアドレスとして使用するように設定できます。スイッチをはじめ、多数の実装機能では、ブロードキャスト メッセージを転送するためのアドレス方式が複数サポートされています。

ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化

デフォルトでは、IP ダイレクト ブロードキャストがドロップされるため、転送されることはありません。 IP ダイレクト ブロードキャストがドロップされると、ルータが DoS 攻撃（サービス拒絶攻撃）にさらされる危険が少なくなります。

ブロードキャストが物理（MAC レイヤ）ブロードキャストになるインターフェイスでは、IP ダイレクト ブロードキャストの転送をイネーブルにできます。 **ip forward-protocol** グローバル コンフィギュレーション コマンドを使用し、設定されたプロトコルだけを転送できます。

転送するブロードキャストを制御するアクセス リストを指定できます。 アクセス リストを指定すると、アクセス リストで許可されている IP パケットだけが、ダイレクト ブロードキャストから物理ブロードキャストに変換できるようになります。 アクセス リストの詳細については、『Security Configuration Guide』の「Information about Network Security with ACLs」の項を参照してください。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/2`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ip directed-broadcast** [*access-list-number*] 例： `Switch(config-if)# ip directed-broadcast 103`	インターフェイス上で、ダイレクトブロードキャストから物理ブロードキャストへの変換をイネーブルにします。 転送するブロードキャストを制御するアクセス リストを指定できます。 アクセス リストを指定すると、アクセス リストで許可されている IP パケットだけが変換可能になります。
ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**} 例： `Switch(config)# ip forward-protocol nd`	ブロードキャスト パケットを転送するとき、ルータによって転送されるプロトコルおよびポートを指定します。 • **udp**：UDP データグラムを転送します。 port：（任意）転送される UDP サービスを制御する宛先ポートです。 • **nd**：ND データグラムを転送します。 • **sdns**：SDNS データグラムを転送します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip interface** [*interface-id*] 例： `Switch# show ip interface`	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。

	コマンドまたはアクション	目的
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

UDP ブロードキャスト パケットおよびプロトコル

ユーザ データグラム プロトコル（UDP）は IP のホスト間レイヤ プロトコルで、TCP と同様です。 UDP はオーバーヘッドが少ない、コネクションレスのセッションを 2 つのエンド システム間に提供しますが、受信されたデータグラムの確認応答は行いません。 場合に応じてネットワーク ホストは UDP ブロードキャストを使用し、アドレス、コンフィギュレーション、名前に関する情報を検索します。 このようなホストが、サーバを含まないネットワークセグメント上にある場合、通常 UDP ブロードキャストは転送されません。 この状況を改善するには、特定のクラスのブロードキャストをヘルパー アドレスに転送するように、ルータのインターフェイスを設定します。 インターフェイスごとに、複数のヘルパー アドレスを使用できます。

UDP 宛先ポートを指定し、転送される UDP サービスを制御できます。 複数の UDP プロトコルを指定することもできます。 旧式のディスクレス Sun ワークステーションおよびネットワーク セキュリティ プロトコル SDNS で使用される Network Disk（ND）プロトコルも指定できます。

ヘルパー アドレスがインターフェイスに定義されている場合、デフォルトでは UDP と ND の両方の転送がイネーブルになっています。 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』の **ip forward-protocol** インターフェイス コンフィギュレーション コマンドの説明には、UDP ポートを指定しない場合にデフォルトで転送されるポートがリストされています。

UDP ブロードキャスト パケットおよびプロトコルの転送

UDP ブロードキャストの転送を設定するときに UDP ポートを指定しないと、ルータは BOOTP フォワーディング エージェントとして動作するように設定されます。 BOOTP パケットは Dynamic Host Configuration Protocol（DHCP）情報を伝達します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip helper-address***address* 例： `Switch(config-if)# ip helper address 10.1.10.1`	転送をイネーブルにし、BOOTP などの UDP ブロードキャスト パケットを転送するための宛先アドレスを指定します。
ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**} 例： `Switch(config)# ip forward-protocol sdns`	ブロードキャスト パケットを転送するときに、ルータによって転送されるプロトコルを指定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip interface** [*interface-id*] 例： `Switch# show ip interface gigabitethernet 1/0/1`	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。

	コマンドまたはアクション	目的
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ブロードキャスト アドレスの確立

最も一般的な（デフォルトの）IP ブロードキャスト アドレスは、すべて 1 で構成されているアドレス（255.255.255.255）です。 ただし、任意の形式の IP ブロードキャスト アドレスを生成するようにスイッチを設定することもできます。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**ip broadcast-address***ip-address* 例： `Switch(config-if)# ip broadcast-address 128.1.255.255`	デフォルト値と異なるブロードキャスト アドレス（128.1.255.255 など）を入力します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip interface** [*interface-id*] 例： `Switch# show ip interface`	指定されたインターフェイスまたはすべてのインターフェイスのブロードキャストアドレスを確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP ブロードキャストのフラッディング

IP ブロードキャストをインターネットワーク全体に、制御可能な方法でフラッディングできるようにするには、ブリッジング STP で作成されたデータベースを使用します。 この機能を使用すると、ループを回避することもできます。 この機能を使用できるようにするには、フラッディングが行われるインターフェイスごとにブリッジングを設定する必要があります。 ブリッジングが設定されていないインターフェイス上でも、ブロードキャストを受信できます。 ただし、ブリッジングが設定されていないインターフェイスでは、受信したブロードキャストが転送されません。 また、異なるインターフェイスで受信されたブロードキャストを送信する場合、このインターフェイスは使用されません。

IP ヘルパーアドレスのメカニズムを使用して単一のネットワークアドレスに転送されるパケットを、フラッディングできます。 各ネットワーク セグメントには、パケットのコピーが 1 つだけ送信されます。

フラッディングを行う場合、パケットは次の条件を満たす必要があります （これらの条件は、IP ヘルパー アドレスを使用してパケットを転送するときの条件と同じです）。

- パケットは MAC レベルのブロードキャストでなければなりません。
- パケットは IP レベルのブロードキャストでなければなりません。

- パケットは Trivial File Transfer Protocol（TFTP）、ドメイン ネーム システム（DNS）、Time、NetBIOS、ND、または BOOTP パケット、または **ip forward-protocol udp** グローバル コンフィギュレーション コマンドで指定された UDP でなければなりません。
- パケットの存続可能時間（TTL）値は 2 以上でなければなりません。

フラッディングされた UDP データグラムには、出力インターフェイスで **ip broadcast-address** インターフェイス コンフィギュレーション コマンドによって指定された宛先アドレスが表示されます。宛先アドレスを、任意のアドレスに設定できます。このため、データグラムがネットワーク内に伝播されるにつれ、宛先アドレスが変更されることもあります。送信元アドレスは変更されません。TTL 値が減ります。

フラッディングされた UDP データグラムがインターフェイスから送信されると（場合によっては宛先アドレスが変更される）、データグラムは通常の IP 出力ルーチンに渡されます。このため、出力インターフェイスにアクセス リストがある場合、データグラムはその影響を受けます。

スイッチでは、パケットの大部分がハードウェアで転送され、スイッチの CPU を経由しません。CPU に送信されるパケットの場合は、ターボフラッディングを使用し、スパニングツリーベースの UDP フラッディングを約 4 ～ 5 倍高速化します。この機能は、ARP カプセル化用に設定されたイーサネット インターフェイスでサポートされています。

IP ブロードキャストのフラッディング

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip forward-protocol spanning-tree** 例： `Switch(config)# ip forward-protocol spanning-tree`	ブリッジング スパニングツリーデータベースを使用し、UDP データグラムをフラッディングします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。
ステップ 7	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 8	**ip forward-protocol turbo-flood** 例： `Switch(config)# ip forward-protocol turbo-flood`	スパニングツリー データベースを使用し、UDP データグラムのフラッディングを高速化します。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

IP アドレスのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容が無効になっている場合、または無効である可能性がある場合は、**clear** 特権 EXEC コマンドを使用し、すべての内容を削除できます。次の表に、内容をクリアするために使用するコマンドを示します。

表 *83* : キャッシュ、テーブル、データベースをクリアするコマンド

clear arp-cache	IP ARP キャッシュおよび高速スイッチング キャッシュをクリアします。
clear host {*name* | *****}	ホスト名およびアドレス キャッシュから 1 つまたはすべてのエントリを削除します。
clear ip route {**network** [*mask*] | *****}	IP ルーティング テーブルから 1 つまたは複数のルートを削除します。

IP ルーティング テーブル、キャッシュ、データベースの内容、ノードへの到達可能性、ネットワーク内のパケットのルーティングパスなど、特定の統計情報を表示できます。 次の表に、IP統計情報を表示するために使用する特権 EXEC コマンドを示します。

表 *84* : キャッシュ、テーブル、データベースを表示するコマンド

show arp	ARP テーブル内のエントリを表示します。
show hosts	デフォルトのドメイン名、検索サービスの方式、サーバ ホスト名、およびキャッシュに格納されているホスト名とアドレスのリストを表示します。
show ip aliases	TCP ポートにマッピングされた IP アドレスを表示します（エイリアス）。
show ip arp	IP ARP キャッシュを表示します。
show ip interface[*interface-id*]	インターフェイスの IP ステータスを表示します。
show ip irdp	IRDP 値を表示します。
show ip masks*address*	ネットワーク アドレスに対して使用されるマスクおよび各マスクを使用するサブネット番号を表示します。

show ip redirects	デフォルト ゲートウェイのアドレスを表示します。
show ip route [*address* [*mask*]] | [*protocol*]	ルーティング テーブルの現在の状態を表示します。
show ip route summary	サマリー形式でルーティング テーブルの現在のステータスを表示します。

IP ユニキャスト ルーティングの設定方法

IP ユニキャスト ルーティングのイネーブル化

デフォルトで、スイッチはレイヤ 2 スイッチング モード、IP ルーティングはディセーブルとなっています。 スイッチのレイヤ 3 機能を使用するには、IP ルーティングをイネーブルにする必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip routing** 例： `Switch(config)# ip routing`	IP ルーティングをイネーブルにします。
ステップ 4	**router***ip_routing_protocol* 例： `Switch(config)# router rip`	IP ルーティング プロトコルを指定します。 このステップでは、他のコマンドを実行することもできます。たとえば、**network**（RIP）ルータ コンフィギュレーション コマンドを使用し、ルーティングするネットワークを指定できます。 具体的なプロトコルの詳細については、この章の後半および『*Cisco IOS IP Configuration Guide*』を参照してください。

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

IP ユニキャスト ルーティングのイネーブル化の例

次に、Switch上で IP ルーティングをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing

Switch(config-router)# end
```

RIP 情報

RIP は、小規模な同種ネットワーク間で使用するために作成された Interior Gateway Protocol（IGP）です。 RIP は、ブロードキャスト ユーザ データグラム プロトコル（UDP）データ パケットを使用してルーティング情報を交換するディスタンスベクトル ルーティング プロトコルです。 このプロトコルは RFC 1058 に文書化されています。 RIP の詳細については、『*IP Routing Fundamentals*』（Cisco Press 刊）を参照してください。

（注） RIP は でサポートされています。

スイッチは RIP を使用し、30 秒ごとにルーティング情報アップデート（アドバタイズメント）を送信します。 180 秒以上を経過しても別のルータからアップデートがルータに届かない場合、該

当するルータから送られたルートは使用不能としてマークされます。 240 秒後もまだ更新がない場合、ルータは更新のないルータのルーティング テーブル エントリをすべて削除します。

RIP では、各ルートの値を評価するためにホップ カウントが使用されます。 ホップ カウントは、ルート内で経由されるルータ数です。 直接接続されているネットワークのホップ カウントは 0 です。ホップ カウントが 16 のネットワークに到達できません。 このように範囲（0 ～ 15）が狭いため、RIP は大規模ネットワークには適していません。

ルータにデフォルトのネットワーク パスが設定されている場合、RIP はルータを疑似ネットワーク 0.0.0.0 にリンクするルートをアドバタイズします。 0.0.0.0 ネットワークは存在しません。RIP はデフォルトのルーティング機能を実行するためのネットワークとして、このネットワークを処理します。 デフォルト ネットワークが RIP によって学習された場合、またはルータにラスト リゾート ゲートウェイがあり、RIP がデフォルトのメトリックによって設定されている場合、スイッチはデフォルト ネットワークをアドバタイズします。 RIP は指定されたネットワーク内のインターフェイスにアップデートを送信します。 インターフェイスのネットワークを指定しなければ、RIP のアップデート中にアドバタイズされません。

RIP の設定方法

RIP のデフォルト設定

表 *85* : *RIP* のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル
デフォルト情報送信元	ディセーブル
デフォルト メトリック	自動メトリック変換（組み込み）
IP RIP 認証キーチェーン	認証なし 認証モード：クリア テキスト
IP RIP の起動	ディセーブル
IP スプリット ホライズン	メディアにより異なる
ネイバー	未定義
ネットワーク	指定なし
オフセット リスト	ディセーブル

機能	デフォルト設定
出力遅延	0 ミリ秒
タイマー基準	• 更新：30 秒 • 無効：180 秒 • ホールドダウン：180 秒 • フラッシュ：240 秒
アップデート送信元の検証	イネーブル
Version	RIP バージョン 1 およびバージョン 2 パケットを受信し、バージョン 1 パケットを送信します。

基本的な RIP パラメータの設定

RIP を設定するには、ネットワークに対して RIP ルーティングをイネーブルにします。他のパラメータを設定することもできます。 スイッチでは、ネットワーク番号を設定するまで RIP コンフィギュレーション コマンドは無視されます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip routing** 例： `Switch(config)# ip routing`	IP ルーティングをイネーブルにします。 （IP ルーティングがディセーブルになっている場合だけ、必須です）。

	コマンドまたはアクション	目的
ステップ 4	**router rip** 例： `Switch(config)# router rip`	RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 5	**network***network number* 例： `Switch(config)# network 12`	ネットワークを RIP ルーティング プロセスと関連付けます。 複数の **network** コマンドを指定できます。 RIP ルーティング アップデートの送受信は、これらのネットワークのインターフェイスを経由する場合だけ可能です。 （注） RIP コマンドを有効にするには、ネットワーク番号を設定する必要があります。
ステップ 6	**neighbor***ip-address* 例： `Switch(config)# neighbor 10.2.5.1`	（任意）ルーティング情報を交換する隣接ルータを定義します。 このステップを使用すると、RIP（通常はブロードキャスト プロトコル）からのルーティング アップデートが非ブロードキャスト ネットワークに到達するようになります。
ステップ 7	**offset-list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*] 例： `Switch(config)# offset-list 103 in 10`	（任意）オフセット リストをルーティング メトリックに適用し、RIP によって取得したルートへの着信および発信メトリックを増加します。 アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。
ステップ 8	**timers basic***update invalid holddown flush* 例： `Switch(config)# timers basic 45 360 400 300`	（任意）ルーティング プロトコル タイマーを調整します。 すべてのタイマーの有効範囲は 0 ～ 4294967295 秒です。 • *update*：ルーティング アップデートの送信間隔。 デフォルトは 30 秒です。 • *invalid*：ルートが無効と宣言されるまでの時間。 デフォルト値は 180 秒です。 • *holddown*：ルートがルーティング テーブルから削除されるまでの時間。 デフォルト値は 180 秒です。 • *flush*：ルーティング アップデートが延期される時間。 デフォルトは 240 秒です。
ステップ 9	**version** {**1** | **2**} 例： `Switch(config)# version 2`	（任意）RIP バージョン 1 または RIP バージョン 2 のパケットだけを送受信するようにスイッチを設定します。 デフォルトの場合、スイッチではバージョン 1 および 2 を受信しますが、バージョン 1 だけを送信します。 インターフェイス コマンド **ip rip** {**send** | **receive**} **version 1** | **2** | **1 2**} を使用し、インターフェイスでの送受信に使用するバージョンを制御することもできます。

	コマンドまたはアクション	目的
ステップ 10	**no auto summary** 例： `Switch(config)# no auto summary`	（任意）自動要約をディセーブルにします。 デフォルトでは、クラスフル ネットワーク境界を通過するときにサブプレフィックスがサマライズされます。 サマライズをディセーブルにし（RIP バージョン 2 だけ）、クラスフル ネットワーク境界にサブネットおよびホスト ルーティング情報をアドバタイズします。
ステップ 11	**no validate-update-source** 例： `Switch(config)# no validdate-update-source`	（任意）着信 RIP ルーティング アップデートの送信元 IP アドレスの検証をディセーブルにします。 デフォルトでは、スイッチが着信 RIP ルーティング アップデートの送信元 IP アドレスを検証します。 送信元アドレスが無効な場合は、アップデートが廃棄されます。 通常の環境で使用する場合は、この機能をディセーブルにしないでください。 ただし、ネットワークに接続されていないルータがあり、そのルータのアップデートを受信する場合は、このコマンドを使用できます。
ステップ 12	**output-delay***delay* 例： `Switch(config)# output-delay 8`	（任意）送信する RIP アップデートにパケット間遅延を追加します。 デフォルトでは、複数のパケットからなる RIP アップデートのパケットに、パケット間遅延が追加されません。 パケットを低速なデバイスに送信する場合は、8 ～ 50 ミリ秒のパケット間遅延を追加できます。
ステップ 13	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show ip protocols** 例： `Switch# show ip protocols`	入力を確認します。
ステップ 15	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

RIP 認証の設定

RIP Version 1 は認証をサポートしていません。 RIP バージョン 2 のパケットを送受信する場合は、インターフェイスで RIP 認証をイネーブルにできます。 インターフェイスで使用できる一連のキーは、キー チェーンによって指定されます。 キー チェーンが設定されていないと、デフォルトの場合でも認証は実行されません。

RIP 認証がイネーブルであるインターフェイスでは、プレーン テキストと MD5 という 2 つの認証モードがスイッチでサポートされます。 デフォルトはプレーン テキストです。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ip rip authentication key-chain***name-of-chain* 例： `Switch(config-if)# ip rip authentication key-chain trees`	RIP 認証をイネーブルにします。
ステップ 5	**ip rip authentication mode** {**text** | **md5**} 例： `Switch(config-if)# ip rip authentication mode md5`	プレーン テキスト認証（デフォルト）または MD5 ダイジェスト認証を使用するように、インターフェイスを設定します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

サマリー アドレスおよびスプリット ホライズン

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティングループの発生を抑えるために、スプリット ホライズン メカニズムが使用されます。 スプリット ホライズンは、ルートに関する情報の発信元であるインターフェイス上の、ルータによって、その情報がアドバタイズされないようにします。この機能を使用すると、通常の場合は複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。

サマリー アドレスおよびスプリット ホライズンの設定

（注） ルートを適切にアドバタイズするため、アプリケーションがスプリット ホライズンをディセーブルにする必要がある場合を除き、通常はこの機能をディセーブルにしないでください。

ダイヤルアップ クライアント用のネットワーク アクセス サーバで、サマライズされたローカル IP アドレス プールをアドバタイズするように、RIP が動作しているインターフェイスを設定する場合は、**ip summary-address rip** インターフェイス コンフィギュレーション コマンドを使用します。

（注） スプリット ホライズンがイネーブルの場合、自動サマリーとインターフェイス IP サマリー アドレスはともにアドバタイズされません。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip address***ip-address subnet-mask* 例： `Switch(config-if)# ip address 10.1.1.10 255.255.255.0`	IP アドレスおよび IP サブネットを設定します。
ステップ 5	**ip summary-address rip ip address***ip-network mask* 例： `Switch(config-if)# ip summary-address rip ip address 10.1.1.30 255.255.255.0`	サマライズする IP アドレスおよび IP ネットワーク マスクを設定します。
ステップ 6	**no ip split horizon** 例： `Switch(config-if)# no ip split horizon`	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show ip interface***interface-id* 例： `Switch# show ip interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

スプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティングループの発生を抑えるために、スプリット ホライズン メカニズムが使用されます。 スプリット ホライズンは、ルートに関する情報の発信元であるインターフェイス上の、ルータによって、その情報がアドバタイズされないようにします。この機能を使用すると、複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。

（注） ルートを適切にアドバタイズするために、アプリケーションがスプリット ホライズンをディセーブルにする必要がある場合を除き、通常この機能をディセーブルにしないでください。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイスコンフィギュレーションモードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ip address***ip-address subnet-mask* 例： `Switch(config-if)# ip address 10.1.1.10 255.255.255.0`	IP アドレスおよび IP サブネットを設定します。
ステップ 5	**no ip split-horizon** 例： `Switch(config-if)# no ip split-horizon`	インターフェイスでスプリットホライズンをディセーブルにします。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip interface***interface-id* 例： `Switch# show ip interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

サマリー アドレスおよびスプリット ホライズンの設定例

次の例では、主要ネットは 10.0.0.0 です。 自動サマリー アドレス 10.0.0.0 はサマリー アドレス 10.2.0.0 によって上書きされるため、10.2.0.0 はインターフェイス ギガビット イーサネット ポート 2 からアドバタイズされますが、10.0.0.0 はアドバタイズされません。 次の例では、インターフェイスがまだレイヤ 2 モード（デフォルト）の場合、**no switchport** インターフェイス コンフィギュレーション コマンドを入力してから、**ip address** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

（注） スプリット ホライズンがイネーブルである場合、（**ip summary-address rip** ルータ コンフィギュレーション コマンドによって設定される）自動サマリーとインターフェイス サマリー アドレスはともにアドバタイズされません。

```
Switch(config)# router rip
Switch(config-router)# interface gigabitethernet1/0/2
Switch(config-if)# ip address 10.1.5.1 255.255.255.0
Switch(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Switch(config-if)# no ip split-horizon
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# neighbor 2.2.2.2 peer-group mygroup
Switch(config-router)# end
```

OSPF に関する情報

OSPF は IP ネットワーク専用の IGP で、IP サブネット化、および外部から取得したルーティング情報のタグ付けをサポートしています。 OSPF を使用するとパケット認証も可能になり、パケットを送受信するときに IP マルチキャストが使用されます。 シスコの実装では、RFC1253 の OSPF 管理情報ベース（MIB）がサポートされています。

シスコの実装は、次の主要機能を含む OSPF バージョン 2 仕様に準拠します。

- スタブ エリアの定義がサポートされています。
- 任意の IP ルーティング プロトコルによって取得されたルートは、別の IP ルーティング プロトコルに再配信されます。 つまり、ドメイン内レベルで、OSPF は EIGRP および RIP によって取得したルートを取り込むことができます。 OSPF ルートを RIP に伝達することもできます。
- エリア内の隣接ルータ間でのプレーン テキスト認証および MD5 認証がサポートされています。
- 設定可能なルーティング インターフェイス パラメータには、インターフェイス出力コスト、再送信インターバル、インターフェイス送信遅延、ルータ プライオリティ、ルータのデッド インターバルと hello インターバル、認証キーなどがあります。
- 仮想リンクがサポートされています。
- RFC 1587 に基づく Not-So-Stubby-Area（NSSA）がサポートされています。

通常、OSPF を使用するには、多くの内部ルータ、複数のエリアに接続された Area Border Router（ABR; エリア境界ルータ）、および自律システム境界ルータ（ASBR）間で調整する必要があります。 最小設定では、すべてのデフォルト パラメータ値、エリアに割り当てられたインターフェイスが使用され、認証は行われません。 環境をカスタマイズする場合は、すべてのルータの設定を調整する必要があります。

OSPF の設定方法

OSPF のデフォルト設定

表 *86*：*OSPF* のデフォルト設定

機能	デフォルト設定
インターフェイス パラメータ	コスト：デフォルト コストは未定義 再送信インターバル：5 秒 送信遅延：1 秒 プライオリティ：1 hello インターバル：10 秒 デッド インターバル：hello インターバルの 4 倍 認証なし パスワードの指定なし MD5 認証はディセーブル
エリア	認証タイプ：0（認証なし） デフォルト コスト：1 範囲：ディセーブル スタブ：スタブ エリアは未定義 NSSA：NSSA エリアは未定義
自動コスト	100 Mb/s
デフォルト情報送信元	ディセーブル イネーブルの場合、デフォルトのメトリック設定は 10 で、外部ルート タイプのデフォルトはタイプ 2 です。
デフォルト メトリック	各ルーティング プロトコルに適切な、組み込みの自動メトリック変換
距離 OSPF	dist1（エリア内のすべてのルート）：110 dist2（エリア間のすべてのルート）：110 dist3（他のルーティング ドメインからのルート）：110。
OSPF データベース フィルタ	ディセーブル すべての発信 LSA がインターフェイスにフラッディングされます。
IP OSPF 名検索	ディセーブル

機能	デフォルト設定
隣接関係変更ログ	イネーブル
Neighbor	指定なし
ネイバー データベース フィルタ	ディセーブル すべての発信 LSA はネイバーにフラッディングされます。
ネットワーク エリア	ディセーブル
ノンストップ フォワーディング（NSF）認識	イネーブル レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
NSF 対応	ディセーブル （注） スイッチ スタックは OSPF NSF 対応ルーティングを IPv4 に対してサポートします。
ルータ ID	OSPF ルーティング プロセスは未定義
サマリー アドレス	ディセーブル
タイマー LSA グループのペーシング	240 秒
タイマー Shortest Path First（SPF）	spf 遅延：5 秒、spf ホールドタイム：10 秒
仮想リンク	エリア ID またはルータ ID は未定義 hello インターバル：10 秒 再送信インターバル：5 秒 送信遅延：1 秒 デッド インターバル：40 秒 認証キー：キーは未定義 メッセージ ダイジェスト キー（MD5）：キーは未定義

ルーテッド アクセスの *OSPF*

Cisco IOS Release 12.2(55)SE で、IP Base イメージは OSPF for Routed Access をサポートしています。 ルート制限のない複数の OSPFv2 および OSPFv3 インスタンスが必要な場合は、IP サービス イメージが必要です。 また、マルチ VRF CE 機能をイネーブルにするためにも、IP サービス イメージが必要です。

OSPF for Routed Access は、特にレイヤ 3 のルーティング機能をワイヤリング クローゼットに拡張するために作成されました。

（注） OSPF for Routed Access は、動的に学習された合わせて 200 のルートを持つ OSPFv2 インスタンスと OSPFv3 インスタンスをそれぞれ 1 つだけサポートします。 IP ベース イメージは、ルーテッド アクセス用に OSPF を提供します。
ただし、これらの制限はこのリリースでは適用されません。

構内環境内の標準的なトポロジ（ハブおよびスポーク）では、すべての非ローカル トラフィックをディストリビューション レイヤに転送するディストリビューション スイッチ（ハブ）にワイヤリング クローゼット（スポーク）が接続されているため、ワイヤリング クローゼット スイッチで完全なルーティング スイッチ テーブルを保持する必要はありません。 OSPF for Routed Access をワイヤリング クローゼットで使用する場合、エリア間ルートおよび外部ルートに到達するためのデフォルト ルートがディストリビューション スイッチによってワイヤリング クローゼット スイッチに送信される、ベスト プラクティスの設計（OSPF スタブまたは完全スタブ エリア構成）を使用する必要があります。

詳細については、『High Availability Campus Network Design—Routed Access Layer using EIGRP or OSPF』を参照してください。

OSPF NSF

スイッチまたはスイッチ スタックは 2 つのレベルのノンストップ フォワーディング（NSF）をサポートしています。

- OSPF NSF 認識, （913 ページ）
- OSPF NSF 対応, （913 ページ）

OSPF NSF 認識

IP サービス フィーチャ セットは、OSPF NSF 認識を IPv4 に対してサポートしています。 隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータに障害（クラッシュ）が発生してプライマリ ルート プロセッサ（RP）がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能をディセーブルにできません。

OSPF NSF 対応

IP サービス フィーチャ セットでは、前のリリースでサポートされていた OSPFv2 NSF Cisco フォーマットに加えて、OSPFv2 NSF IETF フォーマットもサポートされます。 この機能の詳細については、『*NSF—OSPF (RFC 3623 OSPF Graceful Restart)*』を参照してください。

IP サービス フィーチャ セットは、OSPF NSF 対応ルーティングも IPv4 に対してサポートし、スタック マスター変更後のコンバージェンスの向上と、トラフィック損失の低減を実現します。 OSPF NSF 対応スタックでスタック マスターの変更が生じた場合、新しいスタック マスターは自身のリンクステート データベースを OSPF ネイバーと再同期化するために、次の 2 つの処理をする必要があります。

- ネイバー関係をリセットせずにネットワーク上の使用可能な OSPF ネイバーを解放します。
- ネットワークのリンクステート データベースの内容を再取得します。

スタック マスターの変更後、新しいマスターは隣接する NSF 認識デバイスに OSPF NSF 信号を送信します。 デバイスはこの信号を、スタックとのネイバー関係をリセットしない指示として認識します。 NSF 対応スタック マスターは、ネットワーク上の他のルータから信号を受け取ると、自身のネイバー リストの再構築を開始します。

NSF 対応スタック マスターはネイバー関係を再確立すると、自身のデータベースを NSF 認識ネイバーと再同期化し、OSPF ネイバー間でルーティング情報を交換します。 新しいスタック マスターはこのルーティング情報を使用して、新しい情報を基に古いルートの削除、ルーティング情報ベース（RIB）の更新、転送情報ベース（FIB）のアップデートを行います。 これで OSPF プロトコルは完全に収束します。

（注） OSPF NSF では、すべてのネイバー ネットワーク デバイスが NSF 認識である必要があります。ネットワーク セグメント上に非 NSF 認識ネイバーが検出された場合、NSF 対応ルータはそのセグメントに対する NSF 機能をディセーブルにします。 すべてのデバイスが NSF 認識または NSF 対応デバイスとなっているその他のネットワーク セグメントでは、NSF 対応機能が継続して提供されます。

OSPF NSF ルーティングをイネーブルにするには、**nsf** OSPF ルーティング コンフィギュレーション コマンドを使用します。 OSPF NSF ルーティングがイネーブルになっていることを確認するには、**show ip ospf** 特権 EXEC コマンドを使用します。

詳細については、次の URL の『*Cisco Nonstop Forwarding*』を参照してください。 http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-nonstp_fwdg.html

基本的な OSPF パラメータの設定

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、そのルーティング プロセスに関連付けられる IP アドレスの範囲を指定し、その範囲に関連付けられるエリア ID を割り当てます。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**router ospf** process-id 例： `Switch(config)# router ospf 15`	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 プロセス ID はローカルに割り当てられ、内部で使用される識別パラメータで、任意の正の整数を指定できます。 各 OSPF ルーティング プロセスには一意の値があります。 （注） OSPF for Routed Access は、OSPFv2 インスタンスと OSPFv3 インスタンスをそれぞれ 1 つずつと、最大 200 のダイナミックに学習されるルートをサポートします。
ステップ 3	**network** address wildcard-mask **area** area-id 例： `Switch(config)# network 10.1.1.1 255.240.0.0 area 20`	OSPF が動作するインターフェイス、およびそのインターフェイスのエリア ID を定義します。 単一のコマンドにワイルドカードマスクを指定し、特定の OSPF エリアに関連付けるインターフェイスを 1 つまたは複数定義できます。 エリア ID には 10 進数または IP アドレスを指定できます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols** 例： `Switch# show ip protocols`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

例：基本的な OSPF パラメータの設定

次に、OSPF ルーティング プロセスを設定し、プロセス番号 109 を割り当てる例を示します。

```
Switch(config)# router ospf 109
Switch(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

OSPF インターフェイスの設定

ip ospf インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイス固有の OSPF パラメータを変更できます。 これらのパラメータを変更する必要はありませんが、一部のインターフェイス パラメータ（hello インターバル、デッド インターバル、認証キーなど）については、接続されたネットワーク内のすべてのルータで統一性を維持する必要があります。 これらのパラメータを変更した場合は、ネットワーク内のすべてのルータの値も同様に変更してください。

（注） **ip ospf** インターフェイス コンフィギュレーション コマンドはすべてオプションです。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** interface-id 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip ospf** cost 例： `Switch(config-if)# ip ospf 8`	（任意）インターフェイスでパケットを送信するコストを明示的に指定します。
ステップ 4	**ip ospf retransmit-interval** seconds 例： `Switch(config-if)# ip ospf transmit-interval 10`	（任意）LSA 送信間隔を秒数で指定します。 指定できる範囲は 1 ～ 65535 秒です。 デフォルト値は 5 秒です。
ステップ 5	**ip ospf transmit-delay** seconds 例： `Switch(config-if)# ip ospf transmit-delay 2`	（任意）リンク ステートアップデート パケットを送信するまでの予測待機時間を秒数で設定します。 指定できる範囲は 1 ～ 65535 秒です。 デフォルト値は 1 秒です。

	コマンドまたはアクション	目的
ステップ 6	**ip ospf priority** number 例： `Switch(config-if)# ip ospf priority 5`	（任意）ネットワークに対して、OSPF で指定されたルータを検索するときに役立つプライオリティを設定します。 有効な範囲は 0 ～ 255 です。 デフォルトは 1 です。
ステップ 7	**ip ospf hello-interval** seconds 例： `Switch(config-if)# ip ospf hello-interval 12`	（任意）OSPF インターフェイスで hello パケットの送信間隔を秒数で設定します。 ネットワークのすべてのノードで同じ値を指定する必要があります。 指定できる範囲は 1 ～ 65535 秒です。 デフォルトは 10 秒です。
ステップ 8	**ip ospf dead-interval** seconds 例： `Switch(config-if)# ip ospf dead-interval 8`	（任意）最後のデバイスで hello パケットが確認されてから、OSPF ルータがダウンしていることがネイバーによって宣言されるまでの時間を秒数で設定します。 ネットワークのすべてのノードで同じ値を指定する必要があります。 指定できる範囲は 1 ～ 65535 秒です。 デフォルト値は hello インターバルの 4 倍です。
ステップ 9	**ip ospf authentication-key** key 例： `Switch(config-if)# ip ospf authentication-key password`	（任意）隣接 OSPF ルータで使用されるパスワードを割り当てます。 パスワードには、キーボードから入力した任意の文字列（最大 8 バイト長）を指定できます。 同じネットワーク上のすべての隣接ルータには、OSPF 情報を交換するため、同じパスワードを設定する必要があります。
ステップ 10	**ip ospf message digest-key** keyid **md5** key 例： `Switch(config-if)# ip ospf message digest-key 16 md5 your1pass`	（任意）MDS 認証をイネーブルにします。 • *keyid*：1 ～ 255 の ID。 • *key*：最大 16 バイトの英数字パスワード
ステップ 11	**ip ospf database-filter all out** 例： `Switch(config-if)# ip ospf database-filter all out`	（任意）インターフェイスへの OSPF LSA パケットのフラッディングを阻止します。 デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。
ステップ 12	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 13	**show ip ospf interface** [*interface-name*] 例： `Switch# show ip ospf interface`	OSPF に関連するインターフェイス情報を表示します。
ステップ 14	**show ip ospf neighbor detail** 例： `Switch# show ip ospf neighbor detail`	ネイバー スイッチの NSF 認証ステータスを表示します。 出力には、次のいずれかが表示されます。 • *Options is 0x52* *LLS Options is 0x1 (LR)* これらの行の両方が表示される場合、ネイバー スイッチが NSF 認識です。 • *Options is 0x42*：ネイバー スイッチが NSF 認識でないことを示します。
ステップ 15	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

その他の OSPF パラメータの設定, （922 ページ）

OSPF エリア パラメータ

複数の OSPF エリア パラメータを設定することもできます。 設定できるパラメータには、エリア、スタブ エリア、および NSSA への無許可アクセスをパスワードによって阻止する認証用パラメータがあります。 スタブ エリアは、外部ルートの情報が送信されないエリアです。 が、代わりに、自律システム（AS）外の宛先に対するデフォルトの外部ルートが、ABR によって生成されます。 NSSA ではコアからそのエリアへ向かう LSA の一部がフラッディングされませんが、再配信することによって、エリア内の AS 外部ルートをインポートできます。

経路集約は、アドバタイズされたアドレスを、他のエリアでアドバタイズされる単一のサマリー ルートに統合することです。 ネットワーク番号が連続する場合は、**area range** ルータ コンフィギュレーション コマンドを使用し、範囲内のすべてのネットワークを対象とするサマリー ルートをアドバタイズするように ABR を設定できます。

OSPF エリア パラメータの設定

はじめる前に

（注） OSPF **area** ルータ コンフィギュレーション コマンドはすべて任意です。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** process-id 例： `Switch(config)# router ospf 109`	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**area***area-id***authentication** 例： `Switch(config-router)# area 1 authentication`	（任意）特定のエリアへの無許可アクセスに対して、パスワードベースの保護を可能にします。 ID には 10 進数または IP アドレスのいずれかを指定できます。
ステップ 4	**area***area-id***authentication message-digest** 例： `Switch(config-router)# area 1 authentication message-digest`	（任意）エリアに関して MD5 認証をイネーブルにします。
ステップ 5	**area***area-id***stub** [**no-summary**] 例： `Switch(config-router)# area 1 stub`	（任意）エリアをスタブ エリアとして定義します。 **no-summary** キーワードを指定すると、ABR はサマリー リンク アドバタイズメントをスタブエリアに送信できなくなります。
ステップ 6	**area***area-id***nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**] 例： `Switch(config-router)# area 1 nssa default-information-originate`	（任意）エリアを NSSA として定義します。 同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。 次のキーワードのいずれかを選択します。 • **no-redistribution**：ルータが NSSA ABR の場合、**redistribute** コマンドを使用して、ルートを NSSA でなく通常のエリアにインポートする場合に選択します。

	コマンドまたはアクション	目的
		• **default-information-originate**：タイプ 7 LSA を NSSA にインポートするようにする場合に、ABR で選択します。 • **no-redistribution**：サマリー LSA を NSSA に送信しない場合に選択します。
ステップ 7	**area***area-id***range***address mask* 例： `Switch(config-router)# area 1 range 255.240.0.0`	（任意）単一のルートをアドバタイズするアドレス範囲を指定します。 このコマンドは、ABR に対してだけ使用します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip ospf**[*process-id*] 例： `Switch# show ip ospf`	設定を確認するため、一般的な OSPF ルーティング プロセスまたは特定のプロセス ID に関する情報を表示します。
ステップ 10	**show ip ospf** [*process-id* [*area-id*]] **database** 例： `Switch# show ip osfp database`	特定のルータの OSPF データベースに関連する情報のリストを表示します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

その他の OSPF パラメータ

ルータ コンフィギュレーション モードで、その他の OSPF パラメータを設定することもできます。

- ルート集約：他のプロトコルからルートを再配信すると、 各ルートは外部 LSA 内で個別にアドバタイズされます。 OSPF リンク ステート データベースのサイズを小さくするには、**summary-address** ルータ コンフィギュレーション コマンドを使用し、指定されたネットワー

ク アドレスおよびマスクに含まれる、再配信されたすべてのルートを単一のルータにアドバタイズします。

- 仮想リンク：OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。 バックボーンが不連続である場合に仮想リンクを確立するには、2 つの ABR を仮想リンクのエンドポイントとして設定します。 設定情報には、他の仮想エンドポイント（他の ABR）の ID、および 2 つのルータに共通する非バックボーン リンク（通過エリア）などがあります。 仮想リンクをスタブ エリアから設定できません。
- デフォルト ルート：OSPF ルーティング ドメイン内へのルート再配信を設定すると、ルータは自動的に自律システム境界ルータ（ASBR）になります。 ASBR を設定し、強制的に OSPF ルーティング ドメインにデフォルト ルートを生成できます。
- すべての OSPF **show** 特権 EXEC コマンドで使用されるドメイン ネーム サーバ（DNS）名を使用すると、ルータ ID やネイバー ID を指定して表示する場合に比べ、ルータを簡単に特定できます。
- デフォルト メトリック：OSPF は、インターフェイスの帯域幅に従ってインターフェイスの OSPF メトリックを計算します。 メトリックは、帯域幅で分割された *ref-bw* として計算されます。ここでの *ref* のデフォルト値は 10 で、帯域幅（*bw*）は **bandwidth** インターフェイス コンフィギュレーション コマンドによって指定されます。 大きな帯域幅を持つ複数のリンクの場合は、大きな数値を指定し、これらのリンクのコストを区別できます。
- アドミニストレーティブ ディスタンスは、ルーティング情報送信元の信頼性を表す数値です。0 ～ 255 の整数を指定でき、値が大きいほど信頼性は低下します。 アドミニストレーティブ ディスタンスが 255 の場合はルーティング情報の送信元をまったく信頼できないため、無視する必要があります。 OSPF では、エリア内のルート（エリア内）、別のエリアへのルート（エリア間）、および再配信によって学習した別のルーティング ドメインからのルート（外部）の 3 つの異なるアドミニストレーティブ ディスタンスが使用されます。 どのアドミニストレーティブ ディスタンスの値でも変更できます。
- 受動インターフェイス：イーサネット上の 2 つのデバイス間のインターフェイスは 1 つのネットワーク セグメントしか表しません。このため、OSPF が送信側インターフェイスに hello パケットを送信しないようにするには、送信側デバイスを受動インターフェイスに設定する必要があります。 両方のデバイスは受信側インターフェイス宛ての hello パケットを使用することで、相互の識別を可能にします。
- ルート計算タイマー：OSPF がトポロジ変更を受信してから SPF 計算を開始するまでの遅延時間、および 2 つの SPF 計算の間のホールド タイムを設定できます。
- ネイバー変更ログ：OSPF ネイバー ステートが変更されたときに Syslog メッセージを送信するようにルータを設定し、ルータの変更を詳細に表示できます。

関連トピック

ルート マップの概要, （1027 ページ）
ルート マップの設定方法
ルート配信の制御方法, （1032 ページ）

その他の OSPF パラメータの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf***process-id* 例： `Switch(config)# router ospf 10`	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**summary-address***address mask* 例： `Switch(config)# summary-address 10.1.1.1 255.255.255.0`	（任意）1 つのサマリールートだけがアドバタイズされるように、再配信されたルートのアドレスおよびIP サブネット マスクを指定します。
ステップ 4	**area***area-id***virtual-link***router-id* [**hello-interval***seconds*] [**retransmit-interval***seconds*] [**trans**] [[**authentication-key***key*] | **message-digest-key***keyid***md5***key*]] 例： `Switch(config)# area 2 virtual-link 192.168.255.1 hello-interval 5`	（任意）仮想リンクを確立し、パラメータを設定します。
ステップ 5	**default-information originate** [**always**] [**metric***metric-value*] [**metric-type***type-value*] [**route-map***map-name*] 例： `Switch(config)# default-information originate metric 100 metric-type 1`	（任意）強制的に OSPF ルーティング ドメインにデフォルト ルートを生成するように ASBR を設定します。 パラメータはすべて任意です。
ステップ 6	**ip ospf name-lookup** 例： `Switch(config)# ip ospf name-lookup`	（任意）DNS 名検索を設定します。 デフォルトではディセーブルになっています。

	コマンドまたはアクション	目的
ステップ 7	**ip auto-cost reference-bandwidth***ref-bw* 例： `Switch(config)# ip auto-cost reference-bandwidth 5`	（任意）単一のルートをアドバタイズするアドレス範囲を指定します。 このコマンドは、ABR に対してだけ使用します。
ステップ 8	**distance ospf** {[**inter-area***dist1*] [**inter-area***dist2*] [**external***dist3*]} 例： `Switch(config)# distance ospf inter-area 150`	（任意）OSPF の距離の値を変更します。 各タイプのルートのデフォルト距離は 110 です。 指定できる範囲は 1 ～ 255 です。
ステップ 9	**passive-interface***type number* 例： `Switch(config)# passive-interface gigabitethernet 1/0/6`	（任意）指定されたインターフェイス経由の hello パケットの送信を抑制します。
ステップ 10	**timers throttle spf***spf-delay spf-holdtime spf-wait* 例： `Switch(config)# timers throttle spf 200 100 100`	（任意）ルート計算タイマーを設定します。 • *spf-delay*：SPF 計算の変更を受信する間の遅延。 指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-holdtime*：最初と 2 番目の SPF 計算の間の遅延。 指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-wait*：SPF 計算の最大待機時間（ミリ秒）。 指定できる範囲は 1 ～ 600000 ミリ秒です。
ステップ 11	**ospf log-adj-changes** 例： `Switch(config)# ospf log-adj-changes`	（任意）ネイバー ステートが変更されたとき、syslog メッセージを送信します。
ステップ 12	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show ip ospf** [*process-id* [*area-id*]] **database** 例： `Switch# show ip ospf database`	特定のルータの OSPF データベースに関連する情報のリストを表示します。

	コマンドまたはアクション	目的
ステップ 14	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

OSPF インターフェイスの設定，（916 ページ）
OSPF のモニタリング，（926 ページ）

LSA グループ ペーシング

OSPF LSA グループ ペーシング機能を使用すると、OSPF LSA をグループ化し、リフレッシュ、チェックサム、エージング機能の同期を取って、ルータをより効率的に使用できるようになります。デフォルトでこの機能はイネーブルとなっています。デフォルトのペーシング インターバルは 4 分間です。通常は、このパラメータを変更する必要はありません。 最適なグループ ペーシング インターバルは、ルータがリフレッシュ、チェックサム、エージングを行う LSA 数に反比例します。 たとえば、データベース内に約 10000 個の LSA が格納されている場合は、ペーシング インターバルを短くすると便利です。 小さなデータベース（40 ～ 100 LSA）を使用する場合は、ペーシング インターバルを長くし、10 ～ 20 分に設定してください。

LSA グループ ペーシングの変更

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf***process-id* 例： `Switch(config)# router ospf 25`	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**timers lsa-group-pacing***seconds* 例： `Switch(config-router)# timers lsa-group-pacing 15`	LSA の グループ ペーシングを変更します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ループバック インターフェイス

OSPF は、インターフェイスに設定されている最大の IP アドレスをルータ ID として使用します。このインターフェイスがダウンした場合、または削除された場合、OSPF プロセスは新しいルータ ID を再計算し、すべてのルーティング情報をそのルータのインターフェイスから再送信します。ループバック インターフェイスが IP アドレスによって設定されている場合、他のインターフェイスにより大きな IP アドレスがある場合でも、OSPF はこの IP アドレスをルータ ID として使用します。 ループバック インターフェイスに障害は発生しないため、安定性は増大します。 OSPF は他のインターフェイスよりもループバック インターフェイスを自動的に優先し、すべてのループバック インターフェイスの中で最大の IP アドレスを選択します。

ループバック インターフェイスの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface loopback 0** 例： `Switch(config)# interface loopback 0`	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip address** address mask 例： `Switch(config-if)# ip address 10.1.1.5 255.255.240.0`	このインターフェイスに IP アドレスを割り当てます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip interface** 例： `Switch# show ip interface`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF のモニタリング

IP ルーティング テーブルの内容、キャッシュの内容、およびデータベースの内容など、特定の統計情報を表示できます。

表 *87* : ***IP OSPF*** 統計情報の表示コマンド

show ip ospf [*process-id*]	OSPF ルーティングプロセスに関する一般情報を表示します。
show ip ospf [*process-id*] **database** [**router**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**router**] [**self-originate**] **show ip ospf** [*process-id*] **database** [**router**] [**adv-router** [*ip-address*]] **show ip ospf** [*process-id*] **database** [**network**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**asbr-summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**external**] [*link-state-id*] **show ip ospf** [*process-id area-id*] **database** [**database-summary**]	OSPF データベースに関連する情報のリストを表示します。
show ip ospf border-routes	内部の OSPF ルーティング ABR および ASBR テーブル エントリを表示します。
show ip ospf interface[*interface-name*]	OSPF に関連するインターフェイス情報を表示します。
show ip ospf neighbor[*interface-name*] [*neighbor-id*] **detail**	OSPF インターフェイス ネイバー情報を表示します。
show ip ospf virtual-links	OSPF に関連する仮想リンク情報を表示します。

関連トピック

その他の OSPF パラメータの設定, （922 ページ）

EIGRP に関する情報

EIGRP は IGRP のシスコ独自の拡張バージョンです。 EIGRP は IGRP と同じディスタンス ベクトル アルゴリズムおよび距離情報を使用しますが、EIGRP では収束性および動作効率が大幅に改善されています。

コンバージェンス テクノロジーには、拡散更新アルゴリズム（DUAL）と呼ばれるアルゴリズムが採用されています。DUAL を使用すると、ルート計算の各段階でループが発生しなくなり、トポロジの変更に関連するすべてのデバイスを同時に同期できます。 トポロジ変更の影響を受けないルータは、再計算に含まれません。

IP EIGRP を導入すると、ネットワークの幅が広がります。 RIP の場合、ネットワークの最大幅は 15 ホップです。 EIGRP メトリックは数千ホップをサポートするほど大きいため、ネットワークを拡張するときに問題となるのは、トランスポート レイヤのホップ カウンタだけです。 IP パケットが 15 台のルータを経由し、宛先方向のネクスト ホップが EIGRP によって取得されている場合だけ、EIGRP は転送制御フィールドの値を増やします。 RIP ルートを宛先へのネクスト ホップとして使用する場合、転送制御フィールドでは、通常どおり値が増加します。

EIGRP の機能

EIGRP には次の機能があります。

- 高速コンバージェンス
- 差分更新：宛先のステートが変更された場合、ルーティングテーブルの内容全体を送信する代わりに差分更新を行い、EIGRP パケットに必要な帯域幅を最小化します。
- 低い CPU 使用率：完全更新パケットを受信ごとに処理する必要がないため、CPU 使用率が低下します。
- プロトコルに依存しないネイバー探索メカニズム：このメカニズムを使用し隣接ルータに関する情報を取得します。
- 可変長サブネット マスク（VLSM）
- 任意のルート集約
- 大規模ネットワークへの対応

EIGRP コンポーネント

EIGRP には次に示す 4 つの基本コンポーネントがあります。

- ネイバー探索および回復：直接接続されたネットワーク上の他のルータに関する情報を動的に取得するために、ルータで使用されるプロセスです。 また、ネイバーが到達不能または動作不能になっていることを検出するためにも使用されます。 ネイバー探索および回復は、サイズの小さな hello パケットを定期的に送信することにより、わずかなオーバーヘッドで実現されます。 hello パケットが受信されているかぎり、Cisco ISO ソフトウェアは、ネイバーが有効に機能していると学習します。 このように判別された場合、隣接ルータはルーティング情報を交換できます。
- Reliable Transport Protocol：EIGRP パケットをすべてのネイバーに確実に、順序どおりに配信します。 マルチキャスト パケットとユニキャスト パケットが混在した伝送もサポートされます。 EIGRP パケットには確実に送信する必要があるものと、そうでないものがあります。 効率化のため、信頼性は必要時にのみ提供されます。 たとえば、マルチキャスト機能があるマルチアクセス ネットワーク（イーサネットなど）では、すべてのネイバーにそれぞれ hello パケットを確実に送信する必要はありません。 そのため、EIGRP は、1 つのマルチキャスト hello を送信し、パケットに確認応答が必要ないという通知をそのパケットに含めます。 他のタイプのパケット（アップデートなど）の場合は、確認応答（ACK パケット）を要求します。 信頼性の高い伝送であれば、ペンディング中の未確認応答パケットがある場合、マルチ

キャスト パケットを迅速に送信できます。 このため、リンク速度が変化する場合でも、コンバージェンス時間を短く保つことができます。

- DUAL有限状態マシンには、すべてのルート計算の決定プロセスが組み込まれており、すべてのネイバーによってアドバタイズされたすべてのルートが追跡されます。 DUALは距離情報（メトリックともいう）を使用して、効率的な、ループのないパスを選択し、 さらにDUALは適切な後継ルータに基づいて、ルーティング テーブルに挿入するルートを選択します。 後継ルータは、宛先への最小コスト パス（ルーティング ループに関連しないことが保証されている）を持つ、パケット転送に使用される隣接ルータです。 適切な後継ルータが存在しなくても、宛先にアドバタイズするネイバーが存在する場合は再計算が行われ、 この結果、新しい後継ルータが決定されます。 ルートの再計算に要する時間によって、コンバージェンス時間が変わります。 再計算はプロセッサに負荷がかかるため、必要でない場合は、再計算しないようにしてください。 トポロジが変更されると、DUAL はフィジブル サクセサの有無を調べます。 適切なフィジブル サクセサが存在する場合は、それらを探して使用し、不要な再計算を回避します。
- プロトコル依存モジュールは、ネットワーク層プロトコル固有のタスクを実行します。 たとえば、IP EIGRP モジュールは、IP でカプセル化された EIGRP パケットを送受信します。 また、EIGRPパケットを解析したり、DUALに受信した新しい情報を通知したりします。 EIGRP は DUAL にルーティング決定を行うように要求しますが、結果は IP ルーティング テーブルに格納されます。 EIGRP は、他の IP ルーティング プロトコルによって取得したルートの再配信も行います。

（注） EIGRP をイネーブルにするには、スイッチまたはスタック マスター上で IP サービス フィーチャ セットが稼働している必要があります。

EIGRP の設定方法

EIGRPルーティング プロセスを作成するには、EIGRPをイネーブルにし、ネットワークを関連付ける必要があります。 EIGRPは指定されたネットワーク内のインターフェイスにアップデートを送信します。 インターフェイス ネットワークを指定しないと、どの EIGRP アップデートでもアドバタイズされません。

（注） ネットワーク上にIGRP用に設定されているルータがあり、この設定をEIGRPに変更する場合は、IGRPとEIGRPの両方が設定された移行ルータを指定する必要があります。 この場合は、この次の項に記載されているステップ 1 ～ 3 を実行し、さらに「スプリット ホライゾンの設定」も参照してください。 ルートを自動的に再配信するには、同じAS番号を使用する必要があります。

EIGRP のデフォルト設定

表 *88* : *EIGRP* のデフォルト設定

機能	デフォルト設定
自動サマリー	ディセーブル
デフォルト情報	再配信中は外部ルートが許可され、EIGRP プロセス間でデフォルト情報が渡されます。
デフォルト メトリック	デフォルト メトリックなしで再配信できるのは、接続されたルートおよびインターフェイスのスタティック ルートだけです。 デフォルト メトリックは次のとおりです。 • 帯域幅：0 以上の kb/s • 遅延（10 マイクロ秒）：0 または 39.1 ナノ秒の倍数である任意の正の数値 • 信頼性：0 ～ 255 の任意の数値（255 の場合は信頼性が 100%） • 負荷：0 ～ 255 の数値で表される有効帯域幅（255 の場合は 100% の負荷） • MTU：バイトで表されたルートの MTU サイズ （0 または任意の正の整数）
ディスタンス	内部距離：90 外部距離：170
EIGRP の隣接関係変更ログ	ディセーブル 隣接関係の変更はロギングされません。
IP 認証キーチェーン	認証なし
IP 認証モード	認証なし
IP 帯域幅比率	50%
IP hello 間隔	低速非ブロードキャスト マルチアクセス（NBMA）ネットワークの場合：60 秒、それ以外のネットワークの場合：5 秒
IP ホールドタイム	低速 NBMA ネットワークの場合：180 秒、それ以外のネットワークの場合：15 秒

機能	デフォルト設定
IP スプリットホライズン	イネーブル
IP サマリー アドレス	サマリー集約アドレスは未定義
メトリック重み	tos：0、k1 および k3：1、k2、k4、および k5：0
ネットワーク	指定なし
ノンストップ フォワーディング（NSF）認識	IP サービス フィーチャ セットを実行するスイッチ上で IPv4 対してイネーブルになっています。 レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
NSF 対応	ディセーブル （注） スイッチは EIGRP NSF 対応ルーティングを IPv4 に対してサポートします。
オフセットリスト	ディセーブル
ルータ EIGRP	ディセーブル
メトリック設定	ルート マップにはメトリック設定なし
トラフィック共有	メトリックの比率に応じて配分
Variance	1（等コスト ロード バランシング）

EIGRP NSF

スイッチスタックは、次の 2 つのレベルの EIGRP ノンストップ フォワーディングをサポートします。

- EIGRP NSF 認識
- EIGRP NSF 対応

EIGRP NSF 認識

IP サービス フィーチャ セットは、EIGRP NSF 認識を IPv4 に対してサポートしています。 隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能をディセーブルにできません。 この機能の詳細については、『*Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*』の「EIGRP Nonstop Forwarding (NSF) Awareness」を参照してください。

EIGRP NSF 対応

IP サービス フィーチャ セットでは、EIGRP Cisco NSF ルーティングがサポートされています。それにより、コンバージェンスの時間が短くなり、スタック マスター変更後のトラフィック損失がなくなります。 この NSF 機能の詳細については、『*High Availability Configuration Guide, Cisco IOS XE Release 3S*』の「Configuring Nonstop Forwarding」を参照してください。

IP サービス フィーチャ セットは、EIGRP NSF 対応ルーティングも IPv4 に対してサポートし、スタック マスター変更後のコンバージェンスの向上と、トラフィック損失の低減を実現します。 EIGRP NSF 対応のスタック マスターが再起動したとき、または新しいスタック マスターが起動して NSF が再起動したとき、このスイッチにはネイバーが存在せず、トポロジテーブルは空の状態です。 スイッチは、スイッチ スタックに対するトラフィックを中断することなく、インターフェイスの起動、ネイバーの再取得、およびトポロジテーブルとルーティングテーブルの再構築を行う必要があります。 EIGRP ピア ルータは新しいスタック マスターから学習したルートを維持し、NSF の再起動処理の間トラフィックの転送を継続します。

ネイバーによる隣接リセットを防ぐために、新しいスタック マスターは EIGRP パケット ヘッダーの新しい Restart（RS）ビットを使用して再起動を示します。 これを受信したネイバーは、ピア リスト内のスタックと同期を取り、スタックとの隣接関係を維持します。 続いてネイバーは、RS ビットがセットされているスタック マスターにトポロジ テーブルを送信して、自身が NSF 認識デバイスであることおよび新しいスタック マスターを補助していることを示します。

スタックのピア ネイバーの少なくとも 1 つが NFS 認識デバイスであれば、スタック マスターはアップデート情報を受信してデータベースを再構築します。 各 NSF 認識ネイバーは、最後のアップデート パケットに End of Table（EOT）マーカーを付けて送信して、テーブル情報の最後であることを示します。 スタック マスターは、EOT マーカーを受信したときにコンバージェンスを認識し、続いてアップデートの送信を始めます。 スタック マスターがネイバーからすべての EOT マーカーを受信した場合、または NSF コンバージ タイマーが期限切れになった場合、EIGRP は RIB にコンバージェンスを通知し、すべての NSF 認識ピアにトポロジテーブルをフラッディングします。

基本的な EIGRP パラメータの設定

はじめる前に

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**router eigrp** autonomous-system 例： `Switch(config)# router eigrp 10`	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 AS 番号によって他の EIGRP ルータへのルートを特定し、ルーティング情報をタグ付けします。
ステップ 3	**nsf** 例： `Switch(config)# nsf`	（任意）EIGRP NSF をイネーブルにします。 スタック マスターおよびそのすべてのピア上でこのコマンドを入力します。
ステップ 4	**network** network-number 例： `Switch(config)# network 192.168.0.0`	ネットワークを EIGRP ルーティング プロセスに関連付けます。 EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。
ステップ 5	**eigrp log-neighbor-changes** 例： `Switch(config)# eigrp log-neighbor-changes`	（任意）EIGRP 隣接関係変更のロギングをイネーブルにし、ルーティング システムの安定性をモニタします。
ステップ 6	**metric weights***tos k1 k2 k3 k4 k5* 例： `Switch(config)# metric weights 0 2 0 2 0 0`	（任意）EIGRP メトリックを調整します。 デフォルト値はほとんどのネットワークで適切に動作するよう入念に設定されていますが、調整することも可能です。 **注意** メトリックを設定する作業は複雑です。熟練したネットワーク設計者の指導がない場合は、行わないでください。
ステップ 7	**offset-list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*] 例： `Switch(config)# offset-list 21 out 10`	（任意）オフセット リストをルーティング メトリックに適用し、EIGRP によって取得したルートへの着信および発信メトリックを増加します。 アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。
ステップ 8	**auto-summary** 例： `Switch(config)# auto-summary`	（任意）ネットワーク レベル ルートへのサブネット ルートの自動サマライズをイネーブルにします。
ステップ 9	**ip summary-address eigrp***autonomous-system-number address mask*	（任意）サマリー集約を設定します。

	コマンドまたはアクション	目的
	例： `Switch(config)# ip summary-address eigrp 1 192.168.0.0 255.255.0.0`	
ステップ 10	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show ip protocols** 例： `Switch# show ip protocols`	入力を確認します。 NSF 認識の場合、出力に次のように表示されます。 *** IP Routing is NSF aware *** EIGRP NSF enabled
ステップ 12	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

EIGRP インターフェイスの設定

インターフェイスごとに、他の EIGRP パラメータを任意で設定できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 3	**ip bandwidth-percent eigrp***percent* 例： `Switch(config-if)# ip bandwidth-percent eigrp 60`	（任意）インターフェイスで EIGRP が使用できる帯域幅の割合を設定します。 デフォルト値は 50% です。
ステップ 4	**ip summary-address eigrp***autonomous-system-number address mask* 例： `Switch(config-if)# ip summary-address eigrp 109 192.161.0.0 255.255.0.0`	（任意）指定されたインターフェイスのサマリー集約アドレスを設定します（auto-summary がイネーブルの場合は、通常設定する必要はありません）。
ステップ 5	**ip hello-interval eigrp***autonomous-system-number seconds* 例： `Switch(config-if)# ip hello-interval eigrp 109 10`	（任意）EIGRP ルーティング プロセスの hello タイム インターバルを変更します。 指定できる範囲は 1 ～ 65535 秒です。 低速 NBMA ネットワークの場合のデフォルト値は 60 秒、その他のすべてのネットワークでは 5 秒です。
ステップ 6	**ip hold-time eigrp***autonomous-system-number seconds* 例： `Switch(config-if)# ip hold-time eigrp 109 40`	（任意）EIGRP ルーティング プロセスのホールド タイム インターバルを変更します。 指定できる範囲は 1 ～ 65535 秒です。 低速 NBMA ネットワークの場合のデフォルト値は 180 秒、その他のすべてのネットワークでは 15 秒です。 **注意** ホールド タイムを調整する前に、シスコのテクニカルサポートにお問い合わせください。
ステップ 7	**no ip split-horizon eigrp***autonomous-system-number* 例： `Switch(config-if)# no ip split-horizon eigrp 109`	（任意）スプリット ホライズンをディセーブルにし、ルート情報が情報元インターフェイスからルータによってアドバタイズされるようにします。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip eigrp interface** 例： `Switch# show ip eigrp interface`	EIGRP がアクティブであるインターフェイス、およびそれらのインターフェイスに関連する EIGRP の情報を表示します。

	コマンドまたはアクション	目的
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

EIGRP ルート認証の設定

EIGRP ルート認証を行うと、EIGRP ルーティング プロトコルからのルーティング アップデートに関する MD5 認証が可能になり、承認されていない送信元から無許可または問題のあるルーティング メッセージを受け取ることがなくなります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** interface-id 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**ip authentication mode eigrp***autonomous-system***md5** 例： `Switch(config-if)# ip authentication mode eigrp 104 md5`	IP EIGRP パケットの MD5 認証をイネーブルにします。
ステップ 4	**ip authentication key-chain eigrp** *autonomous-system key-chain* 例： `Switch(config-if)# ip authentication key-chain eigrp 105 chain1`	IP EIGRP パケットの認証をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバルコンフィギュレーションモードに戻ります。
ステップ 6	**key chain** *name-of-chain* 例： `Switch(config)# key chain chain1`	キーチェーンを識別し、キーチェーンコンフィギュレーション モードを開始します。 ステップ 4 で設定した名前を指定します。
ステップ 7	**key***number* 例： `Switch(config-keychain)# key 1`	キーチェーン コンフィギュレーション モードで、キー番号を識別します。
ステップ 8	**key-string***text* 例： `Switch(config-keychain-key)# key-string key1`	キーチェーン コンフィギュレーション モードで、キーストリングを識別します。
ステップ 9	**accept-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*} 例： `Switch(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200`	（任意）キーを受信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。 デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。 デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 10	**send-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*} 例： `Switch(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600`	（任意）キーを送信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。 デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。 デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 11	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 12	**show key chain** 例： `Switch# show key chain`	認証キーの情報を表示します。
ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

EIGRP スタブ ルーティング

EIGRP スタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を低減させます。

（注） フィーチャ セットに含まれる EIGRP スタブ ルーティング機能では、ルーティング テーブルからの接続ルートまたはサマリー ルートをネットワーク内のほかのスイッチにアドバタイズすることだけを行います。 スイッチはアクセス レイヤで EIGRP スタブ ルーティングを使用することにより、ほかのタイプのルーティング アドバタイズメントの必要性を排除しています。

EIGRP スタブ ルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、EIGRP スタブ ルーティングを設定しているスイッチ経由です。 スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

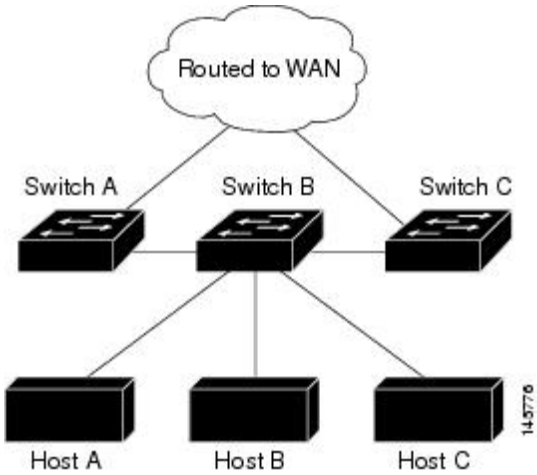
EIGRP スタブ ルーティングを使用しているときは、EIGRP を使用してスイッチだけをスタブとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。 指定したルートだけがスイッチから伝播されます。 スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブ ルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブ ルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。 スタブ ルータは、ディストリビューション ルータを使用して適切なアップデートをすべてのピアに送信します。

次の図では、スイッチ B は EIGRP スタブ ルータとして設定されています。 スイッチ A および C は残りの WAN に接続されています。 スイッチ B は、接続ルート、スタティック ルート、再配信

ルート、およびサマリー ルートをスイッチ A と C にアドバタイズします。スイッチ B はスイッチ A から学習したルートをアドバタイズしません（逆の場合も同様です）。

図 *72*：*EIGRP* スタブ ルータ設定



EIGRP スタブ ルーティングの詳細については、『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols*』の「Configuring EIGRP Stub Routing」の項を参照してください。

EIGRP のモニタリングおよびメンテナンス

ネイバー テーブルからネイバーを削除できます。 さらに、各種 EIGRP ルーティング統計情報を表示することもできます。 下の図に、ネイバーを削除し、統計情報を表示する特権 EXEC コマンドを示します。 表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

表 *89*：*IP EIGRP* の *clear* および *show* コマンド

clear ip eigrp neighbors [*if-address* | *interface*]	ネイバーテーブルからネイバーを削除します。
show ip eigrp interface [*interface*] [*as number*]	EIGRP に設定されているインターフェイスに関する情報を表示します。
show ip eigrp neighbors [*type-number*]	EIGRP によって検出されたネイバーを表示します。
show ip eigrp topology [*autonomous-system-number*] | [[*ip-address*] *mask*]]	指定されたプロセスの EIGRP トポロジ テーブルを表示します。
show ip eigrp traffic [*autonomous-system-number*]	すべてまたは指定された EIGRP プロセスの送受信パケット数を表示します。

BGP に関する情報

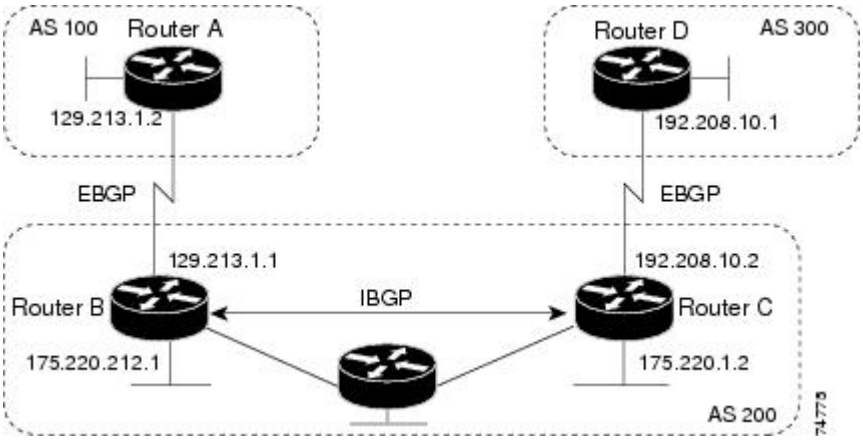
ボーダー ゲートウェイ プロトコル（BGP）は、Exterior Gateway Protocol です。自律システム間で、ループの発生しないルーティング情報交換を保証するドメイン間ルーティング システムを設定するために使用されます。 自律システムは、同じ管理下で動作して RIP や OSPF などの Interior Gateway Protocol（IGP）を境界内で実行し、Exterior Gateway Protocol（EGP）を使用して相互接続されるルータで構成されます。 BGP バージョン 4 は、インターネット内でドメイン間ルーティングを行うための標準 EGP です。 このプロトコルは、RFC 1163、1267、および 1771 で定義されています。 BGP の詳細については、『*Internet Routing Architectures*』（Cisco Press 刊）、および『*Cisco IP and IP Routing Configuration Guide*』の「Configuring BGP」を参照してください。

BGP コマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』の「IP Routing Protocols」を参照してください。

BGP ネットワーク トポロジ

同じ自律システム（AS）に属し、BGP アップデートを交換するルータは内部BGP（IBGP）を実行し、異なる自律システムに属し、BGP アップデートを交換するルータは外部 BGP（EBGP）を実行します。 大部分のコンフィギュレーション コマンドは、EBGP と IBGP で同じですが、 ルーティング アップデートが自律システム間で交換されるか（EBGP）、または AS 内で交換されるか（IBGP）という点で異なります。 下の図に、EBGP と IBGP の両方を実行しているネットワークを示します。

図 *73*：*EBGP*、*IBGP*、および複数の自律システム



外部 AS と情報を交換する前に、BGP は AS 内のルータ間で内部 BGP ピアリングを定義し、IGRP や OSPF など AS 内で稼働する IGP に BGP ルーティング情報を再配信して、AS 内のネットワークに到達することを確認します。

BGP ルーティング プロセスを実行するルータは、通常 BGP スピーカーと呼ばれます。 BGP はトランスポート プロトコルとして伝送制御プロトコル（TCP）を使用します（特にポート 179）。

ルーティング情報を交換するため相互に TCP 接続された 2 つの BGP スピーカーを、ピアまたはネイバーと呼びます。 上の図では、ルータ A と B が BGP ピアで、ルータ B と C、ルータ C と D も同様です。ルーティング情報は、宛先ネットワークへの完全パスを示す一連の AS 番号です。BGP はこの情報を使用し、ループのない自律システム マップを作成します。

このネットワークの特徴は次のとおりです。

- ルータ A および B では EBGP が、ルータ B および C では IBGP が稼働しています。 EBGP ピアは直接接続されていますが、IBGP ピアは直接接続されていないことに注意してください。 IGP が稼働し、2 つのネイバーが相互に到達するかぎり、IBGP ピアを直接接続する必要はありません。
- AS 内のすべての BGP スピーカーは、相互にピア関係を確立する必要があります。 つまり、AS 内の BGP スピーカーは、論理的な完全メッシュ型に接続する必要があります。 BGP4 は、論理的な完全メッシュに関する要求を軽減する 2 つの技術（連合およびルート リフレクタ）を提供します。
- AS 200 は AS 100 および AS 300 の中継 AS です。つまり、AS 200 は AS 100 と AS 300 間でパケットを転送するために使用されます。

BGP ピアは完全な BGP ルーティング テーブルを最初に交換し、差分更新だけを送信します。 BGP ピアはキープアライブ メッセージ（接続が有効であることを確認）、および通知メッセージ（エラーまたは特殊条件に応答）を交換することもできます。

BGP の場合、各ルートはネットワーク番号、情報が通過した自律システムのリスト（自律システム パス）、および他のパス属性リストで構成されます。 BGP システムの主な機能は、AS パスのリストに関する情報など、ネットワークの到達可能性情報を他の BGP システムと交換することです。 この情報は、AS が接続されているかどうかを判別したり、ルーティング ループをプルーニングしたり、AS レベル ポリシー判断を行うために使用できます。

Cisco IOS が稼働しているルータまたはスイッチが IBGP ルートを選択または使用するのは、ネクストホップ ルータで使用可能なルートがあり、IGP から同期信号を受信している（IGP 同期がディセーブルの場合は除く）場合です。 複数のルートが使用可能な場合、BGP は属性値に基づいてパスを選択します。 BGP 属性については、「BGP 判断属性の設定」の項を参照してください。

BGP バージョン 4 ではクラスレス ドメイン間ルーティング（CIDR）がサポートされているため、集約ルートを作成してスーパーネットを構築し、ルーティング テーブルのサイズを削減できます。 CIDR は、BGP 内部のネットワーク クラスの概念をエミュレートし、IP プレフィックスのアドバタイズをサポートします。

BGP の設定方法

BGP のデフォルト設定

下の表に、BGP のデフォルト設定を示します。 すべての特性の詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』の特定のコマンドを参照してください。

表 *90*：*BGP* のデフォルト設定

機能	デフォルト設定
集約アドレス	ディセーブル：未定義
AS パス アクセス リスト	未定義
自動サマリー	ディセーブル
最適パス	• ルータはルートを選択する場合に *as-path* を考慮し、外部 BGP ピアからの類似ルートは比較しません。 • ルータ ID の比較：ディセーブル
BGP コミュニティ リスト	• 番号：未定義。 コミュニティ番号を示す特定の値を許可すると、許可されていないその他すべてのコミュニティ番号は、暗黙の拒否にデフォルト設定されます。 • フォーマット：シスコデフォルト フォーマット（32 ビット番号）
BGP 連合 ID/ピア	• ID：未設定 • ピア：識別なし
BGP 高速外部フォールオーバー	イネーブル
BGP ローカル初期設定	100。 指定できる範囲は 0～4294967295 です（大きな値を推奨）。
BGP ネットワーク	指定なし。バックドア ルートのアドバタイズなし
BGP ルート ダンプニング	デフォルトでは、ディセーブルです。 イネーブルの場合は、次のようになります。 • 半減期は 15 分 • 再使用は 750（10 秒増分） • 抑制は 2000（10 秒増分） • 最大抑制時間は半減期の 4 倍（60 分）

機能	デフォルト設定
BGP ルータ ID	ループバック インターフェイスに IP アドレスが設定されている場合は、ループバック インターフェイスの IP アドレス、またはルータの物理インターフェイスに対して設定された最大の IP アドレス
デフォルトの情報送信元（プロトコルまたはネットワーク再配信）	ディセーブル
デフォルト メトリック	自動メトリック変換（組み込み）
ディスタンス	• 外部ルート アドミニストレーティブ ディスタンス：20（有効値は 1 ～ 255） • 内部ルート アドミニストレーティブ ディスタンス：200（有効値は 1 ～ 255） • ローカル ルート アドミニストレーティブ ディスタンス：200（有効値は 1 ～ 255）
ディストリビュート リスト	• 入力（アップデート中に受信されたネットワークをフィルタリング）：ディセーブル • 出力（アップデート中のネットワークのアドバタイズを抑制）：ディセーブル
内部ルート再配信	ディセーブル
IP プレフィックス リスト	未定義
Multi Exit Discriminator（MED）	• 常に比較：ディセーブル。 異なる自律システム内のネイバーからのパスに対して、MED を比較しません。 • 最適パスの比較：ディセーブル • 最悪パスである MED の除外：ディセーブル • 決定的な MED 比較：ディセーブル

機能	デフォルト設定
Neighbor	• アドバタイズメントインターバル：外部ピアの場合は30秒、内部ピアの場合は 5 秒 • ロギング変更：イネーブル • 条件付きアドバタイズ：ディセーブル • デフォルト送信元：ネイバーに送信されるデフォルト ルートはなし • 説明：なし • ディストリビュート リスト：未定義 • 外部 BGP マルチホップ：直接接続されたネイバーだけを許可 • フィルタ リスト：使用しない • 受信したプレフィックスの最大数：制限なし • ネクストホップ（BGP ネイバーのネクストホップとなるルータ）：ディセーブル • パスワード：ディセーブル • ピア グループ：定義なし、割り当てメンバーなし • プレフィックス リスト：指定なし • リモート AS（ネイバー BGP テーブルへのエントリ追加）：ピア定義なし • プライベート AS 番号の削除：ディセーブル • ルート マップ：ピアへの適用なし • コミュニティ属性送信：ネイバーへの送信なし。 • シャットダウンまたはソフト再設定：ディセーブル • タイマー：60 秒、ホールドタイム：180 秒 • アップデート送信元：最適ローカル アドレス • バージョン：BGP バージョン 4 • 重み：BGP ピアによって学習されたルート：0、ローカルルータから取得されたルート：32768
NSF[7] 認識	ディセーブル状態の[8]。 イネーブル状態の場合、レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。

機能	デフォルト設定
ルート リフレクタ	未設定
同期化（BGP および IGP）	ディセーブル
テーブルマップ アップデート	ディセーブル
タイマー	キープアライブ：60 秒、ホールドタイム：180 秒

7 Nonstop Forwarding

8 NSF 認識は、グレースフル リスタートをイネーブルにすることにより、IP サービス フィーチャ セットを実行するスイッチ上で IPv4 に対してイネーブルにできます

NSF 認識

BGP NSF 認識は、IP サービス フィーチャ セットで IPv4 に対してサポートされます。 BGP ルーティングでこの機能をイネーブルにするには、グレースフル リスタートをイネーブルにする必要があります。 隣接ルータが NSF 対応で、この機能がイネーブルである場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能の詳細については、『*Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*』の「BGP Nonstop Forwarding (NSF) Awareness」を参照してください。

BGP ルーティングに関する情報

BGP ルーティングをイネーブルにするには、BGP ルーティング プロセスを確立し、ローカル ネットワークを定義します。 BGP はネイバーとの関係を完全に認識する必要があるため、BGP ネイバーも指定する必要があります。

BGP は、内部および外部の 2 種類のネイバーをサポートします。 内部ネイバーは同じ AS 内に、外部ネイバーは異なる AS 内にあります。 通常の場合、外部ネイバーは相互に隣接し、1 つのサブネットを共有しますが、内部ネイバーは同じ AS 内の任意の場所に存在します。

スイッチではプライベート AS 番号を使用できます。プライベート AS 番号は通常サービス プロバイダーによって割り当てられ、ルートが外部ネイバーにアドバタイズされないシステムに設定されます。 プライベート AS 番号の範囲は 64512 ～ 65535 です。 AS パスからプライベート AS 番号を削除するように外部ネイバーを設定するには、**neighbor remove-private-as** ルータ コンフィギュレーション コマンドを使用します。 この結果、外部ネイバーにアップデートを渡すとき、AS パス内にプライベート AS 番号が含まれている場合は、これらの番号が削除されます。

AS が別の AS からさらに別の AS にトラフィックを渡す場合は、アドバタイズ対象のルートに矛盾が存在しないことが重要です。 BGP がルートをアドバタイズしてから、ネットワーク内のすべてのルータが IGP を通してルートを学習した場合、AS は一部のルータがルーティングできなかっ

たトラフィックを受信することがあります。 このような事態を避けるため、BGP は IGP が AS に情報を伝播し、BGP が IGP と同期化されるまで、待機する必要があります。 同期化は、デフォルトでイネーブルに設定されています。 AS が特定の AS から別の AS にトラフィックを渡さない場合、または自律システム内のすべてのルータで BGP が稼働している場合は、同期化をディセーブルにし、IGP 内で伝送されるルート数を少なくして、BGP がより短時間で収束するようにします。

BGP ルーティングのイネーブル化

はじめる前に

（注） BGP をイネーブルにするには、スイッチまたはスタック マスター上で IP サービス フィーチャ セットが稼働している必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： `Switch(config)# ip routing`	IP ルーティングをイネーブルにします。
ステップ 3	**router bgp***autonomous-system* 例： `Switch(config)# router bgp 45000`	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。 指定できる AS 番号は 1～65535 です。64512～65535 は、プライベート AS 番号専用です。
ステップ 4	**network***network-number* [**mask***network-mask*] [**route-map***route-map-name*] 例： `Switch(config)# network 10.108.0.0`	この AS に対してローカルとなるようにネットワークを設定し、BGP テーブルにネットワークを格納します。

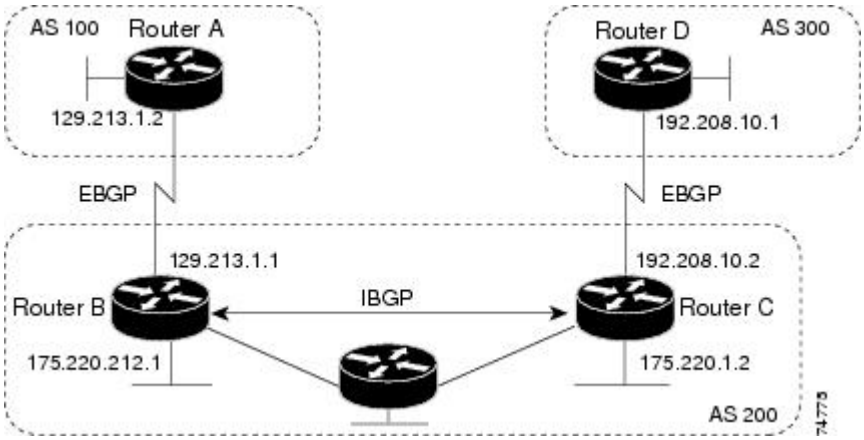
	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***number* 例： `Switch(config)# neighbor 10.108.1.2 remote-as 65200`	BGP ネイバー テーブルに設定を追加し、IP アドレスによって識別されるネイバーが、指定された AS に属することを示します。 EBGP の場合、通常ネイバーは直接接続されており、IP アドレスは接続のもう一方の端におけるインターフェイスのアドレスです。 IBGP の場合、IP アドレスにはルータ インターフェイス内の任意のアドレスを指定できます。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remove-private-as** 例： `Switch(config)# neighbor 172.16.2.33 remove-private-as`	（任意）発信ルーティング アップデート内の AS パスからプライベート AS 番号を削除します。
ステップ 7	**synchronization** 例： `Switch(config)# synchronization`	（任意）BGP と IGP の同期化をイネーブルにします。
ステップ 8	**auto-summary** 例： `Switch(config)# auto-summary`	（任意）自動ネットワーク サマライズをイネーブルにします。 IGP から BGP にサブネットが再配信された場合、ネットワーク ルートだけが BGP テーブルに挿入されます。
ステップ 9	**bgp graceful-restart** 例： `Switch(config)# bgp graceful-start`	（任意）NSF 認識をスイッチでイネーブルにします。 NSF 認識はデフォルトではディセーブルです。
ステップ 10	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show ip bgp network***network-number* 例： `Switch# show ip bgp network 10.108.0.0`	設定を確認します。

	コマンドまたはアクション	目的
ステップ 12	**show ip bgp neighbor** 例： `Switch# show ip bgp neighbor`	NSF 認識（グレースフル リスタート）がネイバーでイネーブルにされていることを確認します。 スイッチおよびネイバーで NSF 認識がイネーブルである場合は、次のメッセージが表示されます。 グレースフル リスタート機能: アドバタイズおよび受信される スイッチで NSF 認識がイネーブルであり、ネイバーでディセーブルである場合は、次のメッセージが表示されます。 グレースフル リスタート機能: アドバタイズされる
ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

例：ルータでの BGP の設定

次に、下の図のルータでの BGP の設定例を示します。

図 *74*：*EBGP*、*IBGP*、および複数の自律システム



ルータ A：

```
Switch(config)# router bgp 100
Switch(config-router)# neighbor 129.213.1.1 remote-as 200
```

ルータ B：

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 129.213.1.2 remote-as 100
Switch(config-router)# neighbor 175.220.1.2 remote-as 200
```

ルータ C：

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 175.220.212.1 remote-as 200
Switch(config-router)# neighbor 192.208.10.1 remote-as 300
```

ルータ D：

```
Switch(config)# router bgp 300
Switch(config-router)# neighbor 192.208.10.2 remote-as 200
```

BGP ピアが稼働していることを確認するには、show ip bgp neighbors 特権 EXEC コマンドを使用します。 次に、ルータ A にこのコマンドを実行した場合の出力例を示します。

```
Switch# show ip bgp neighbors

BGP neighbor is 129.213.1.1, remote AS 200, external link
 BGP version 4, remote router ID 175.220.212.1
 BGP state = established, table version = 3, up for 0:10:59
 Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
 Minimum time between advertisement runs is 30 seconds
 Received 2828 messages, 0 notifications, 0 in queue
 Sent 2826 messages, 0 notifications, 0 in queue
 Connections established 11; dropped 10
```

state = established 以外の情報が出力された場合、ピアは稼働していません。 リモート ルータ ID は、ルータ（または最大のループバック インターフェイス）上の最大の IP アドレスです。 テーブルが新規情報でアップデートされるたびに、テーブルのバージョン番号は増加します。 継続的にテーブルバージョン番号が増加している場合は、ルートがフラッピングし、ルーティングアップデートが絶えず発生しています。

外部プロトコルの場合、**network** ルータ コンフィギュレーション コマンドから IP ネットワークへの参照によって制御されるのは、アドバタイズされるネットワークだけです。 これは、**network** コマンドを使用してアップデートの送信先を指定する IGP（EIGRP など）と対照的です。

BGP 設定の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Routing Protocols」を参照してください。 特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

ルーティング ポリシーの変更

ピアのルーティング ポリシーには、インバウンドまたはアウトバウンド ルーティング テーブル アップデートに影響する可能性があるすべての設定が含まれます。 BGP ネイバーとして定義された 2 台のルータは、BGP 接続を形成し、ルーティング情報を交換します。 このあとで BGP フィルタ、重量、距離、バージョン、またはタイマーを変更する場合、または同様の設定変更を行う場合は、BGP セッションをリセットし、設定の変更を有効にする必要があります。

リセットには、ハード リセットとソフト リセットの 2 種類があります。 Cisco IOS Release 12.1 以降では、事前に設定を行わなくても、ソフト リセットを使用できます。 事前設定なしにソフト リセットを使用するには、両方の BGP ピアでソフト ルート リフレッシュ機能がサポートされていなければなりません。この機能は、ピアによって TCP セッションが確立されたときに送信される OPEN メッセージに格納されてアドバタイズされます。 ソフト リセットを使用すると、BGP

ルータ間でルート リフレッシュ要求およびルーティング情報を動的に交換したり、それぞれのアウトバウンド ルーティング テーブルをあとで再アドバタイズできます。

- ソフト リセットによってネイバーからインバウンド アップデートが生成された場合、このリセットはダイナミック インバウンド ソフト リセットといいます。
- ソフトリセットによってネイバーに一連のアップデートが送信された場合、このリセットはアウトバウンド ソフト リセットといいます。

ソフト インバウンド リセットが発生すると、新規インバウンド ポリシーが有効になります。 ソフトアウトバウンドリセットが発生すると、BGPセッションがリセットされずに、新規ローカルアウトバウンド ポリシーが有効になります。 アウトバウンド ポリシーのリセット中に新しい一連のアップデートが送信されると、新規インバウンド ポリシーも有効になる場合があります。

下の表に、ハード リセットとソフト リセットの利点および欠点を示します。

表 *91*：ハード リセットとソフト リセットの利点および欠点

リセット タイプ	利点	欠点
ハード リセット	メモリ オーバーヘッドが発生しません。	ネイバーから提供されたBGP、IP、およびFIBテーブルのプレフィックスが失われます。 推奨しません。
発信ソフト リセット	ルーティングテーブルアップデートが設定、保管されません。	インバウンド ルーティング テーブル アップデートがリセットされません。
ダイナミック インバウンドソフトリセット	BGP セッションおよびキャッシュがクリアされません。 ルーティングテーブルアップデートを保管する必要がなく、メモリ オーバーヘッドが発生しません。	両方の BGP ルータでルート リフレッシュ機能をサポートする必要があります（Cisco IOS Release 12.1 以降）。

ルーティング ポリシー変更の管理

BGP ピアがルート リフレッシュ機能をサポートするかどうかを学習して、BGP セッションをリセットするには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ip bgp neighbors** 例： `Switch# show ip bgp neighbors`	ネイバーがルート リフレッシュ機能をサポートするかどうかを表示します。 サポートされている場合は、ルータに関する次のメッセージが表示されます。 *Received route refresh capability from peer*
ステップ 2	**clear ip bgp** {***** | *address* | *peer-group-name*} 例： `Switch# clear ip bgp *`	指定された接続上でルーティング テーブルをリセットします。 • すべての接続をリセットする場合は、アスタリスク（*）を入力します。 • 特定の接続をリセットする場合は、IP アドレスを入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 3	**clear ip bgp** {***** | *address* | *peer-group-name*} **soft out** 例： `Switch# clear ip bgp * soft out`	（任意）指定された接続上でインバウンドルーティングテーブルをリセットするには、アウトバウンドソフトリセットを実行します。このコマンドは、ルート リフレッシュがサポートされている場合に使用してください。 • すべての接続をリセットする場合は、アスタリスク（*）を入力します。 • 特定の接続をリセットする場合は、IP アドレスを入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 4	**show ip bgp** 例： `Switch# show ip bgp`	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 5	**show ip bgp neighbors** 例： `Switch# show ip bgp neighbors`	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。

BGP 判断属性

BGP スピーカーが複数の自律システムから受信したアップデートが、同じ宛先に対して異なるパスを示している場合、BGP スピーカーはその宛先に到達する最適パスを 1 つ選択する必要があり

ます。 選択されたパスは BGP ルーティング テーブルに格納され、ネイバーに伝播されます。 この判断は、アップデートに格納されている属性値、および BGP で設定可能な他の要因に基づいて行われます。

BGP ピアはネイバー AS からプレフィックスに対する 2 つの EBGP パスを学習するとき、最適パスを選択して IP ルーティング テーブルに挿入します。 BGP マルチパス サポートがイネーブルで、同じネイバー自律システムから複数の EBGP パスを学習する場合、単一の最適パスの代わりに、複数のパスが IP ルーティング テーブルに格納されます。 そのあと、パケット スイッチング中に、複数のパス間でパケット単位または宛先単位のロード バランシングが実行されます。 maximum-paths**maximum-paths** ルータ コンフィギュレーション コマンドは、許可されるパス数を制御します。

これらの要因により、BGP が最適パスを選択するために属性を評価する順序が決まります。

1. パスで指定されているネクストホップが到達不能な場合、このアップデートは削除されます。 BGP ネクスト ホップ属性（ソフトウェアによって自動判別される）は、宛先に到達するために使用されるネクストホップの IP アドレスです。 EBGP の場合、通常このアドレスは **neighbor remote-as router** ルータ コンフィギュレーション コマンドで指定されたネイバーの IP アドレスです。 ネクストホップの処理をディセーブルにするには、ルート マップまたは **neighbor next-hop-self** ルータ コンフィギュレーション コマンドを使用します。
2. 最大の重みのパスを推奨します（シスコ独自のパラメータ）。 ウェイト属性はルータにローカルであるため、ルーティング アップデートで伝播されません。 デフォルトでは、ルータ送信元のパスに関するウェイト属性は 32768 で、それ以外のパスのウェイト属性は 0 です。 最大の重みのルートを推奨します。 重みを設定するには、アクセス リスト、ルート マップ、または **neighbor weight** ルータ コンフィギュレーション コマンドを使用します。
3. ローカルプリファレンス値が最大のルートを推奨します。 ローカルプリファレンスはルーティング アップデートに含まれ、同じ AS 内のルータ間で交換されます。 ローカル初期設定属性のデフォルト値は 100 です。 ローカルプリファレンスを設定するには、**bgp default local-preference** ルータ コンフィギュレーション コマンドまたはルート マップを使用します。
4. ローカル ルータ上で稼働する BGP から送信されたルートを推奨します。
5. AS パスが最短のルートを推奨します。
6. 送信元タイプが最小のルートを推奨します。 内部ルートまたは IGP は、EGP によって学習されたルートよりも小さく、EGP で学習されたルートは、未知の送信元のルートまたは別の方法で学習されたルートよりも小さくなります。
7. 想定されるすべてのルートについてネイバー AS が同じである場合は、MED メトリック属性が最小のルートを推奨します。 MED を設定するには、ルート マップまたは **default-metric** ルータ コンフィギュレーション コマンドを使用します。 IBGP ピアに送信されるアップデートには、MED が含まれます。
8. 内部（IBGP）パスより、外部（EBGP）パスを推奨します。
9. 最も近い IGP ネイバー（最小の IGP メトリック）を通って到達できるルートを推奨します。 ルータは、AS 内の最短の内部パス（BGP のネクストホップへの最短パス）を使用し、宛先に到達するためです。

10 次の条件にすべて該当する場合は、このパスのルートを IP ルーティング テーブルに挿入してください。

最適ルートと目的のルートがともに外部ルートである

最適ルートと目的のルートの両方が、同じネイバー自律システムからのルートである

maximum-paths がイネーブルである

11 マルチパスがイネーブルでない場合は、BGP ルータ ID の IP アドレスが最小であるルートを推奨します。 通常、ルータ ID はルータ上の最大の IP アドレスまたはループバック（仮想）アドレスですが、実装に依存することがあります。

BGP 判断属性の設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： `Switch(config)# router bgp 4500`	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp best-path as-path ignore** 例： `Switch(config-router)# bgp bestpath as-path ignore`	（任意）ルート選択中に AS パス長を無視するようにルータを設定します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self** 例： `Switch(config-router)# neighbor 10.108.1.1 next-hop-self`	（任意）ネクストホップ アドレスの代わりに使用される特定の IP アドレスを入力し、ネイバーへの BGP アップデートに関するネクストホップの処理をディセーブルにします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **weight***weight* 例： `Switch(config-router)# neighbor 172.16.12.1 weight 50`	（任意）ネイバー接続に重みを割り当てます。 指定できる値は 0 ～ 65535 です。最大の重みのルートを推奨します。 別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ローカル ルータから送信されたルートのデフォルトの重みは 32768 です。

	コマンドまたはアクション	目的
ステップ 6	**default-metric***number* 例： `Switch(config-router)# default-metric 300`	（任意）推奨パスを外部ネイバーに設定するように MED メトリックを設定します。 MED を持たないすべてのルータも、この値に設定されます。 指定できる範囲は 1 ～ 4294967295 です。 最小値を推奨します。
ステップ 7	**bgp bestpath med missing-as-worst** 例： `Switch(config-router)# bgp bestpath med missing-as-worst`	（任意）MED がない場合は無限の値が指定されていると見なし、MED 値を持たないパスが最も望ましくないパスになるように、スイッチを設定します。
ステップ 8	**bgp always-compare med** 例： `Switch(config-router)# bgp always-compare-med`	（任意）異なる AS 内のネイバーからのパスに対して、MED を比較するようにスイッチを設定します。 デフォルトでは、MED は同じ AS 内のパス間でだけ比較されます。
ステップ 9	**bgp bestpath med confed** 例： `Switch(config-router)# bgp bestpath med confed`	（任意）連合内の異なるサブ AS によってアドバタイズされたパスから特定のパスを選択する場合に、MED を考慮するようにスイッチを設定します。
ステップ 10	**bgp deterministic med** 例： `Switch(config-router)# bgp deterministic med`	（任意）同じ AS 内の異なるピアによってアドバタイズされたルートから選択する場合に、MED 変数を考慮するようにスイッチを設定します。
ステップ 11	**bgp default local-preference***value* 例： `Switch(config-router)# bgp default local-preference 200`	（任意）デフォルトのローカルプリファレンス値を変更します。 指定できる範囲は 0 ～ 4294967295 で、デフォルト値は 100 です。 最大のローカル プリファレンス値を推奨します。
ステップ 12	**maximum-paths***number* 例： `Switch(config-router)# maximum-paths 8`	（任意）IP ルーティングテーブルに追加するパスの数を設定します。 デフォルトでは、最適パスだけがルーティングテーブルに追加されます。 指定できる範囲は 1 ～ 16 です。 複数の値を指定すると、パス間のロードバランシングが可能になります。 スイッチ ソフトウェア では最大 32 の等コスト ルートが許可されていますが、スイッチ ハードウェアはルートあたり 17 パス以上は使用しません。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show ip bgp** 例： `Switch# show ip bgp`	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 15	**show ip bgp neighbors** 例： `Switch# show ip bgp neighbors`	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 16	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルート マップ

BGP 内でルート マップを使用すると、ルーティング情報を制御、変更したり、ルーティング ドメイン間でルートを再配信する条件を定義できます。 ルート マップの詳細については、「Using Route Maps to Redistribute Routing Information」の項を参照してください。 各ルート マップには、ルート マップを識別する名前（マップ タグ）およびオプションのシーケンス番号が付いています。

ルート マップによる BGP フィルタリングの設定

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Switch(config)# route-map set-peer-address permit 10`	ルート マップを作成し、ルート マップ コンフィギュレーション モードを開始します。
ステップ 3	**set ip next-hop***ip-address* [*...ip-address*] [**peer-address**] 例： `Switch(config)# set ip next-hop 10.1.1.3`	（任意）ネクストホップ処理をディセーブルにするようにルート マップを設定します。 • インバウンド ルート マップの場合は、一致するルートのネクスト ホップをネイバー ピア アドレスに設定し、サードパーティのネクスト ホップを上書きします。 • BGP ピアのアウトバウンド ルート マップの場合は、ネクスト ホップをローカル ルータのピア アドレスに設定して、ネクストホップ計算をディセーブルにします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show route-map** [*map-name*] 例： `Switch# show route-map`	設定を確認するため、設定されたすべてのルートマップ、または指定されたルート マップだけを表示します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

BGP フィルタリング

BGP アドバタイズメントをフィルタリングするには、**as-path access-list** グローバル コンフィギュレーション コマンドや **neighbor filter-list** ルータ コンフィギュレーション コマンドなどの AS パス フィルタを使用します。 **neighbor distribute-list** ルータ コンフィギュレーション コマンドとアクセス リストを併用することもできます。 distribute-list フィルタはネットワーク番号に適用され

ます。 **distribute-list** コマンドの詳細については、「ルーティング アップデートのアドバタイズおよび処理の制御」の項を参照してください。

ネイバー単位でルート マップを使用すると、アップデートをフィルタリングしたり、さまざまな属性を変更したりできます。 ルート マップは、インバウンド アップデートまたはアウトバウンド アップデートのいずれかに適用できます。 ルート マップを渡すルートだけが、アップデート内で送信または許可されます。 着信および発信の両方のアップデートで、AS パス、コミュニティ、およびネットワーク番号に基づくマッチングがサポートされています。 AS パスのマッチングには **match as-path access-list** ルート マップ コマンド、コミュニティに基づくマッチングには **match community-list** ルート マップ コマンド、ネットワークに基づくマッチングには **ip access-list** グローバル コンフィギュレーション コマンドが必要です。

ネイバーによる BGP フィルタリングの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： `Switch(config)# router bgp 109`	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** {*ip-address* | *peer-group name*} **distribute-list** {**access-list-number** | *name*} {**in** | **out**} 例： `Switch(config-router)# neighbor 172.16.4.1 distribute-list 39 in`	（任意）アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。 （注） **neighbor prefix-list** ルータ コンフィギュレーション コマンドを使用して、アップデートをフィルタリングすることもできますが、両方のコマンドを使用して同じ BGP ピアを設定することはできません。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **route-map***map-tag*{**in** | **out**} 例： `Switch(config-router)# neighbor 172.16.70.24 route-map internal-map in`	（任意）ルート マップを適用し、着信または発信ルートをフィルタリングします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors** 例： `Switch# show ip bgp neighbors`	設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

アクセス リストおよびネイバーによる BGP フィルタリングの設定

BGP 自律システム パスに基づいて着信および発信の両方のアップデートにアクセス リスト フィルタを指定して、フィルタリングすることもできます。 各フィルタは、正規表現を使用するアクセス リストです。 （正規表現の作成方法については、『*Cisco IOS Dial Technologies Command Reference, Release 12.4*』の付録「Regular Expressions」を参照してください。） この方法を使用するには、自律システムパスのアクセスリストを定義し、特定のネイバーとの間のアップデートに適用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**ip as-path access-list***access-list-number* {**permit** | **deny**} *as-regular-expressions* 例： `Switch(config)# ip as-path access-list 1 deny _65535_`	BGP-relatedアクセス リストを定義します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp***autonomous-system* 例： `Switch(config)# router bgp 110`	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **filter-list** {*access-list-number* | *name*} {**in** | **out** | **weight***weight*} 例： `Switch(config-router)# neighbor 172.16.1.1 filter-list 1 out`	アクセス リストに基づいて、BGP フィルタを確立します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors** [**paths***regular-expression*] 例： `Switch# show ip bgp neighbors`	設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP フィルタリングのプレフィックス リスト

neighbor distribute-list ルータ コンフィギュレーション コマンドを含む多数の BGP ルート フィルタリング コマンドでは、アクセス リストの代わりにプレフィックス リストを使用できます。 プレフィックス リストを使用すると、大規模リストのロードおよび検索パフォーマンスが改善し、差分更新がサポートされ、コマンドライン インターフェイス（CLI）設定が簡素化され、柔軟性が増すなどの利点が生じます。

プレフィックスリストによるフィルタリングでは、アクセスリストの照合の場合と同様に、プレフィックスリストに記載されたプレフィックスとルートのプレフィックスが照合されます。 一致すると、一致したルートが使用されます。 プレフィックスが許可されるか、または拒否されるかは、次に示すルールに基づいて決定されます。

- 空のプレフィックス リストはすべてのプレフィックスを許可します。

- 特定のプレフィックスがプレフィックス リストのどのエントリとも一致しなかった場合、実質的に拒否されたものと見なされます。
- 指定されたプレフィックスと一致するエントリがプレフィックス リスト内に複数存在する場合は、シーケンス番号が最小であるプレフィックス リスト エントリが識別されます。

デフォルトでは、シーケンス番号は自動生成され、5 ずつ増分します。 シーケンス番号の自動生成をディセーブルにした場合は、エントリごとにシーケンス番号を指定する必要があります。シーケンス番号を指定する場合の増分値に制限はありません。 増分値が 1 の場合は、このリストに追加エントリを挿入できません。増分値が大きい場合は、値がなくなることがあります。

BGP フィルタリング用のプレフィックス リストの設定

コンフィギュレーション エントリを削除する場合は、シーケンス番号を指定する必要はありません。 **show** コマンドの出力には、シーケンス番号が含まれます。

コマンド内でプレフィックス リストを使用する場合は、あらかじめプレフィックス リストを設定しておく必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip prefix-list***list-name* [**seq***seq-value*] **deny** | **permit***network/len* [**ge***ge-value*] [**le***le-value*] 例： `Switch(config)# ip prefix-list BLUE permit 172.16.1.0/24`	一致条件に合わせてアクセスを拒否（**deny**）または許可（**permit**）するプレフィックス リストを作成します。シーケンス 番号を指定することもできます。 少なくとも 1 つの **permit** コマンドまたは **deny** コマンドを入力する必要があります。 • *network/len* は、ネットワーク番号およびネットワーク マスクの長さ（ビット単位）です。 • （任意）**ge** および **le** の値は、照合するプレフィックス長の範囲を指定します。指定された *ge-value* および *le-value* は、次の条件を満たす必要があります。 *len* < *ge-value* < *le-value*< 32

	コマンドまたはアクション	目的
ステップ 3	**ip prefix-list***list-name***seq***seq-value***deny* | **permit***network/len* [**ge***ge-value*] [**le***le-value*] 例： `Switch(config)# ip prefix-list BLUE seq 10 permit 172.24.1.0/24`	（任意）プレフィックス リストにエントリを追加し、そのエントリにシーケンス番号を割り当てます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip prefix list** [**detail** | **summary**] *name* [*network/len*] [**seq***seq-num*] [**longer**] [**first-match**] 例： `Switch# show ip prefix list summary test`	プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示して、設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP コミュニティ フィルタリング

BGP コミュニティ フィルタリングは、COMMUNITIES 属性の値に基づいてルーティング情報の配信を制御する BGP の方法の 1 つです。 この属性によって、宛先はコミュニティにグループ化され、コミュニティに基づいてルーティング判断が適用されます。 この方法を使用すると、ルーティング情報の配信制御を目的とする BGP スピーカーの設定が簡単になります。

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。 各宛先は複数のコミュニティに属します。 AS 管理者は、宛先が属するコミュニティを定義できます。 デフォルトでは、すべての宛先が一般的なインターネットコミュニティに属します。 コミュニティは、過渡的でグローバルなオプションの属性である、COMMUNITIES 属性（1 ～ 4294967200 の数値）によって識別されます。 事前に定義された既知のコミュニティの一部を、次に示します。

- **internet**：このルートをインターネット コミュニティにアドバタイズします。 すべてのルータが所属します。
- **no-export**：EBGP ピアにこのルートをアドバタイズしません。

- **no-advertise**：どのピア（内部または外部）にもこのルートをアドバタイズしません。
- **local-as**：ローカルな AS 外部のピアにこのルートをアドバタイズしません。

コミュニティに基づき、他のネイバーに許可、送信、配信するルーティング情報を制御できます。BGP スピーカーは、ルートを学習、アドバタイズ、または再配信するときに、ルートのコミュニティを設定、追加、または変更します。ルートを集約すると、作成された集約内のCOMMUNITIES属性に、すべての初期ルートの全コミュニティが含まれます。

コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。 さらに、アクセス リストの場合と同様、一連のコミュニティ リストを作成することもできます。 ステートメントは一致が見つかるまでチェックされ、 1 つのステートメントが満たされると、テストは終了します。

コミュニティに基づいて COMMUNITIES 属性および match 句を設定するには、「ルート マップによるルーティング情報の再配信」に記載されている **match community-list** および **set community** ルート マップ コンフィギュレーション コマンドを参照してください。

BGP コミュニティ フィルタリングの設定

デフォルトでは、COMMUNITIES 属性はネイバーに送信されません。 COMMUNITIES 属性が特定の IP アドレスのネイバーに送信されるように指定するには、**neighbor send-community** ルータ コンフィギュレーション コマンドを使用します。

手順の概要

1. **configureterminal**
2. **ip community-list***community-list-number* {**permit** | **deny**} *community-number*
3. **router bgp***autonomous-system*
4. **neighbor** {*ip-address* | *peer-group name*} **send-community**
5. **set comm-list***list-num***delete**
6. **exit**
7. **ip bgp-community new-format**
8. **end**
9. **show ip bgp community**
10. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ip community-list***community-list-number* {**permit** | **deny**} *community-number* 例： `Switch(config)# ip community-list 1 permit 50000:10`	コミュニティ リストを作成し、番号を割り当てます。 • *community-list-number* は 1 ～ 99 の整数です。この値は、コミュニティの1つ以上の許可または拒否グループを識別します。 • *community-number* は、**set community** ルートマップ コンフィギュレーション コマンドで設定される番号です。
ステップ 3	**router bgp***autonomous-system* 例： `Switch(config)# router bgp 108`	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group name*} **send-community** 例： `Switch(config-router)# neighbor 172.16.70.23 send-community`	この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 5	**set comm-list***list-num***delete** 例： `Switch(config-router)# set comm-list 500 delete`	（任意）ルートマップで指定された標準または拡張コミュニティ リストと一致する着信または発信アップデートのコミュニティ属性から、コミュニティを削除します。
ステップ 6	**exit** 例： `Switch(config-router)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip bgp-community new-format** 例： `Switch(config)# ip bgp-community new format`	（任意）AA:NN の形式で、BGP コミュニティを表示、解析します。 BGP コミュニティは、2 つの部分からなる 2 バイト長形式で表示されます。 シスコのデフォルトのコミュニティ形式は、NNAA です。 BGP に関する最新の RFC では、コミュニティは AA:NN の形式をとります。最初の部分は AS 番号で、その次の部分は 2 バイトの数値です。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**show ip bgp community** 例： `Switch# show ip bgp community`	設定を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP ネイバーおよびピア グループ

通常、BGP ネイバーの多くは同じアップデート ポリシー（同じアウトバウンド ルート マップ、配信リスト、フィルタ リスト、アップデート送信元など）を使用して設定されます。 アップデート ポリシーが同じネイバーをピア グループにまとめると設定が簡単になり、アップデートの効率が高まります。 多数のピアを設定した場合は、この方法を推奨します。

BGP ピア グループを設定するには、ピア グループを作成し、そこにオプションを割り当てて、ピア グループ メンバーとしてネイバーを追加します。 ピア グループを設定するには、**neighbor** ルータ コンフィギュレーション コマンドを使用します。 デフォルトでは、ピア グループ メンバーは remote-as（設定されている場合）、version、update-source、out-route-map、out-filter-list、out-dist-list、minimum-advertisement-interval、next-hop-self など、ピア グループの設定オプションをすべて継承します。 すべてのピア グループ メンバーは、ピア グループに対する変更を継承します。 また、アウトバウンド アップデートに影響しないオプションを無効にするように、メンバーを設定することもできます。

BGP ネイバーおよびピア グループの設定

各ネイバーに設定オプションを割り当てるには、ネイバーの IP アドレスを使用し、次に示すルータ コンフィギュレーション コマンドのいずれかを指定します。 ピア グループにオプションを割り当てるには、ピア グループ名を使用し、いずれかのコマンドを指定します。 **neighbor shutdown** ルータ コンフィギュレーション コマンドを使用すると、すべての設定情報を削除せずに、BGP ピアまたはピア グループをディセーブルにできます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system*	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor***peer-group-name***peer-group**	BGP ピア グループを作成します。
ステップ 4	**neighbor***ip-address***peer-group***peer-group-name*	BGP ネイバーをピア グループのメンバにします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***number*	BGP ネイバーを指定します。 **remote-as***number* を使用してピア グループが設定されていない場合は、このコマンドを使用し、EBGP ネイバーを含むピア グループを作成します。 指定できる範囲は 1 ～ 65535 です。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **description***text*	（任意）ネイバーに説明を関連付けます。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map***map-name*]	（任意）BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **update-source***interface*	（任意）内部 BGP セッションに、TCP 接続に関するすべての操作インターフェイスの使用を許可します。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop**	（任意）ネイバーがセグメントに直接接続されていない場合でも、BGPセッションを使用可能にします。 マルチホップ ピア アドレスへの唯一のルートがデフォルト ルート（0.0.0.0）の場合、マルチホップ セッションは確立されません。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **local-as***number*	（任意）ローカル AS として使用する AS 番号を指定します。 指定できる範囲は 1 ～ 65535 です。
ステップ 12	**neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval***seconds*	（任意）BGPルーティング アップデートを送信する最小インターバルを設定します。
ステップ 13	**neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix***maximum* [*threshold*]	（任意）ネイバーから受信できるプレフィックス数を制御します。 指定できる範囲は1～4294967295 です。

	コマンドまたはアクション	目的
		threshold（任意）は、警告メッセージが生成される基準となる最大値（パーセンテージ）です。デフォルトは 75% です。
ステップ 14	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	（任意）ネイバー宛ての BGP アップデートに関して、ネクストホップでの処理をディセーブルにします。
ステップ 15	neighbor {*ip-address* | *peer-group-name*} password *string*	（任意）TCP 接続での MD5 認証を BGP ピアに設定します。 両方の BGP ピアに同じパスワードを設定する必要があります。そうしないと、BGP ピア間に接続が作成されません。
ステップ 16	**neighbor** {*ip-address* | *peer-group-name*} **route-map***map-name* {**in** | **out**}	（任意）着信または発信ルートにルートマップを適用します。
ステップ 17	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 18	**neighbor** {*ip-address* | *peer-group-name*} **timers***keepalive holdtime*	（任意）ネイバーまたはピアグループ用のタイマーを設定します。 • *keepalive* インターバルは、キープアライブ メッセージがピアに送信される間隔です。 指定できる範囲は 1 ～ 4294967295 秒です。デフォルト値は 60 秒です。 • *holdtime* は、キープアライブメッセージを受信しなかった場合、ピアが非アクティブと宣言されるまでのインターバルです。 指定できる範囲は 1 ～ 4294967295 秒です。デフォルト値は 180 秒です。
ステップ 19	**neighbor** {*ip-address* | *peer-group-name*} **weight***weight*	（任意）ネイバーからのすべてのルートに関する重みを指定します。
ステップ 20	**neighbor** {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *name*} {**in** | **out**}	（任意）アクセスリストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。
ステップ 21	**neighbor** {*ip-address* | *peer-group-name*} **filter-list***access-list-number* {**in** | **out** | **weight***weight*}	（任意）BGP フィルタを確立します。
ステップ 22	**neighbor** {*ip-address* | *peer-group-name*} **version***value*	（任意）ネイバーと通信するときに使用する BGP バージョンを指定します。

	コマンドまたはアクション	目的
ステップ 23	**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**	（任意）受信したアップデートのストアを開始するようにソフトウェアを設定します。
ステップ 24	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 25	**show ip bgp neighbors**	設定を確認します。
ステップ 26	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

集約ルート

クラスレス ドメイン間ルーティング（CIDR）を使用すると、集約ルート（またはスーパーネット）を作成して、ルーティングテーブルのサイズを最小化できます。 BGP 内に集約ルートを設定するには、集約ルートを BGP に再配信するか、または BGP ルーティング テーブル内に集約エントリを作成します。 BGP テーブル内に特定のエントリがさらに 1 つまたは複数存在する場合は、BGP テーブルに集約アドレスが追加されます。

ルーティング テーブルでの集約アドレスの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： `Switch(config)# router bgp 106`	BGP ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aggregate-address***address mask* 例： `Switch(config-router)# aggregate-address 10.0.0.0 255.0.0.0`	BGP ルーティングテーブル内に集約エントリを作成します。 集約ルートは AS からのルートとしてアドバタイズされます。情報が失われた可能性があることを示すため、アトミック集約属性が設定されます。
ステップ 4	**aggregate-address***address mask***as-set** 例： `Switch(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set`	（任意）AS 設定パス情報を生成します。 このコマンドは、この前のコマンドと同じルールに従う集約エントリを作成します。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET です。 多くのパスを集約するときは、このキーワードを使用しないでください。このルートは絶えず取り消され、アップデートされます。
ステップ 5	**aggregate-address***address-mask***summary-only** 例： `Switch(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only`	（任意）サマリーアドレスだけをアドバタイズします。
ステップ 6	**aggregate-address***address mask***suppress-map***map-name* 例： `Switch(config-router)# aggregate-address 10.0.0.0 255.0.0.0 suppress-map map1`	（任意）選択された、より具体的なルートを抑制します。
ステップ 7	**aggregate-address***address mask***advertise-map***map-name* 例： `Switch(config-router)# aggregate-address 10.0.0.0 255.0.0.0 advertise-map map2`	（任意）ルートマップによって指定された設定に基づいて集約を生成します。
ステップ 8	**aggregate-address***address mask***attribute-map***map-name* 例： `Switch(config-router)# aggregate-address 10.0.0.0 255.0.0.0 attribute-map map3`	（任意）ルートマップで指定された属性を持つ集約を生成します。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show ip bgp neighbors** [**advertised-routes**] 例： `Switch# show ip bgp neighbors`	設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング ドメイン コンフェデレーション

IBGP メッシュを削減する方法の 1 つは、自律システムを複数のサブ自律システムに分割して、単一の自律システムとして認識される単一の連合にグループ化することです。 各自律システムは内部で完全にメッシュ化されていて、同じコンフェデレーション内の他の自律システムとの間には数本の接続があります。 異なる自律システム内にあるピアでは EBGP セッションが使用されますが、ルーティング情報は IBGP ピアと同様な方法で交換されます。 具体的には、ネクスト ホップ、MED、およびローカル プリファレンス情報は維持されます。 すべての自律システムで単一の IGP を使用できます。

ルーティング ドメイン連合の設定

自律システムのグループの自律システム番号として機能する連合 ID を指定する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： `Switch(config)# router bgp 100`	BGP ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**bgp confederation identifier***autonomous-system* 例： `Switch(config)# bgp confederation identifier 50007`	BGP 連合 ID を設定します。
ステップ 4	**bgp confederation peers***autonomous-system* [*autonomous-system*...] 例： `Switch(config)# bgp confederation peers 51000 51001 51002`	連合に属する AS、および特殊な EBGP ピアとして処理する AS を指定します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbor** 例： `Switch# show ip bgp neighbor`	設定を確認します。
ステップ 7	**show ip bgp network** 例： `Switch# show ip bgp network`	設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP ルート リフレクタ

BGP では、すべての IBGP スピーカーを完全メッシュ構造にする必要があります。 外部ネイバーからルートを受信したルータは、そのルートをすべての内部ネイバーにアドバタイズする必要があります。 ルーティング情報のループを防ぐには、すべての IBGP スピーカーを接続する必要があります。 内部ネイバーは、内部ネイバーから学習されたルートを他の内部ネイバーに送信しません。

ルート リフレクタを使用すると、学習されたルートをネイバーに渡す場合に他の方法が使用されるため、すべての IBGP スピーカーを完全メッシュ構造にする必要はありません。 IBGP ピアをルート リフレクタに設定すると、その IBGP ピアは IBGP によって学習されたルートを一連の IBGP ネイバーに送信するようになります。 ルート リフレクタの内部ピアには、クライアント ピアと非クライアント ピア（AS 内の他のすべてのルータ）の 2 つのグループがあります。 ルート リフレクタは、これらの 2 つのグループ間でルートを反映させます。 ルート リフレクタおよびクライアント ピアは、クラスタを形成します。 非クライアント ピアは相互に完全メッシュ構造にする必要がありますが、クライアント ピアはその必要はありません。 クラスタ内のクライアントは、そのクラスタ外の IBGP スピーカーと通信しません。

アドバタイズされたルートを受信したルート リフレクタは、ネイバーに応じて、次のいずれかのアクションを実行します。

- 外部 BGP スピーカーからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズします。
- 非クライアント ピアからのルートをすべてのクライアントにアドバタイズします。
- クライアントからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズします。 したがって、クライアントを完全メッシュ構造にする必要はありません。

通常、クライアントのクラスタにはルート リフレクタが 1 つあり、クラスタはルート リフレクタのルータ ID で識別されます。 冗長性を高めて、シングル ポイントでの障害を回避するには、クラスタに複数のルート リフレクタを設定する必要があります。 このように設定した場合は、ルート リフレクタが同じクラスタ内のルート リフレクタからのアップデートを認識できるように、クラスタ内のすべてのルート リフレクタに同じクラスタ ID（4 バイト）を設定する必要があります。 クラスタを処理するすべてのルート リフレクタは完全メッシュ構造にし、一連の同一なクライアント ピアおよび非クライアント ピアを設定する必要があります。

BGP ルート リフレクタの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： `Switch(config)# router bgp 101`	BGP ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**neighbor** {*ip-address* | *peer-group-name*} **route-reflector-client** 例： `Switch(config-router)# neighbor 172.16.70.24 route-reflector-client`	ローカル ルータを BGP ルート リフレクタとして、指定されたネイバーをクライアントとして、それぞれ設定します。
ステップ 4	**bgp cluster-id***cluster-id* 例： `Switch(config-router)# bgp cluster-id 10.0.1.2`	（任意）クラスタに複数のルート リフレクタが存在する場合、クラスタ ID を設定します。
ステップ 5	**no bgp client-to-client reflection** 例： `Switch(config-router)# no bgp client-to-client reflection`	（任意）クライアント間のルート反映をディセーブルにします。 デフォルトでは、ルート リフレクタ クライアントからのルートは、他のクライアントに反映されます。 ただし、クライアントが完全メッシュ構造の場合、ルート リフレクタはルートをクライアントに反映させる必要がありません。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp** 例： `Switch# show ip bgp`	設定を確認します。 送信元 ID およびクラスタリスト属性を表示します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルート ダンプニング

ルート フラップ ダンプニングは、インターネットワーク内でフラッピング ルートの伝播を最小化するための BGP 機能です。 ルートの状態が使用可能、使用不可能、使用可能、使用不可能という具合に、繰り返し変化する場合、ルートはフラッピングと見なされます。 ルート ダンプニングがイネーブルの場合は、フラッピングしているルートにペナルティ値が割り当てられます。 ルー

トの累積ペナルティが、設定された制限値に到達すると、ルートが稼働している場合であっても、BGPはルートのアドバタイズメントを抑制します。 再使用限度は、ペナルティと比較される設定可能な値です。 ペナルティが再使用限度より小さくなると、起動中の抑制されたルートのアドバタイズメントが再開されます。

IBGP によって取得されたルートには、ダンプニングが適用されません。 このポリシーにより、IBGP ピアのペナルティが AS 外部のルートよりも大きくなることはありません。

ルート ダンプニングの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system* 例： `Switch(config)# router bgp 100`	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp dampening** 例： `Switch(config-router)# bgp dampening`	BGPルート ダンプニングをイネーブルにします。
ステップ 4	**bgp dampening***half-life reuse suppress max-suppress* [**route-map***map*] 例： `Switch(config-router)# bgp dampening 30 1500 10000 120`	（任意）ルート ダンプニング係数のデフォルト値を変更します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp flap-statistics** [{**regexp***regexp*} | {**filter-list***list*} | {*address mask* [**longer-prefix**]}] 例： `Switch# show ip bgp flap-statistics`	（任意）フラッピングしているすべてのパスのフラップを監視します。 ルートの抑制が終了し、安定状態になると、統計情報が削除されます。

	コマンドまたはアクション	目的
ステップ 7	**show ip bgp dampened-paths** 例： `Switch# show pi bgp dampened-paths`	（任意）抑制されるまでの時間を含めて、ダンプニングされたルートを表示します。
ステップ 8	**clear ip bgp flap-statistics** [{**regexp***regexp*} | {**filter-list***list*} | {*address mask* [**longer-prefix**]} 例： `Switch# clear ip bgp flap-statistics`	（任意）BGP フラップ統計情報を消去して、ルートがダンプニングされる可能性を小さくします。
ステップ 9	**clear ip bgp dampening** 例： `Switch# clear ip bgp dampening`	（任意）ルート ダンプニング情報を消去して、ルートの抑制を解除します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP の追加情報

BGP 設定の詳しい説明については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Routing Protocols」にある「BGPの設定」を参照してください。 特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

BGP のモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。 この作業は、特定の構造の内容が無効になる場合、または無効である疑いがある場合に必要となります。

BGP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。 さらに、リソースの利用率を取得したり、ネットワーク問題を解決するための情報を使用することもできます。 さらに、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のルーティング パスを検出することもできます。

下の図に、BGP を消去および表示するために使用する特権 EXEC コマンドを示します。 表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』を参照してください。

表 *92*： ***IP BGP*** の ***clear*** および ***show*** コマンド

clear ip bgp*address*	特定の BGP 接続をリセットします。
clear ip bgp *	すべての BGP 接続をリセットします。
clear ip bgp peer-group*tag*	BGP ピア グループのすべてのメンバを削除します。
show ip bgp*prefix*	プレフィックスがアドバタイズされるピア グループ、またはピア グループに含まれないピアを表示します。 ネクストホップやローカルプレフィックスなどのプレフィックス属性も表示されます。
show ip bgp cidr-only	サブネットおよびスーパーネット ネットワーク マスクを含むすべての BGP ルートを表示します。
show ip bgp community [*community-number*] [**exact**]	指定されたコミュニティに属するルートを表示します。
show ip bgp community-list*community-list-number* [**exact-match**]	コミュニティ リストで許可されたルートを表示します。
show ip bgp filter-list*access-list-number*	指定された AS パス アクセス リストによって照合されたルートを表示します。
show ip bgp inconsistent-as	送信元の AS と矛盾するルートを表示します。
show ip bgp regexp*regular-expression*	コマンドラインに入力された特定の正規表現と一致する AS パスを持つルートを表示します。
show ip bgp	BGP ルーティング テーブルの内容を表示します。
show ip bgp neighbors [*address*]	各ネイバーとの BGP 接続および TCP 接続に関する詳細情報を表示します。
show ip bgp neighbors [*address*] [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths***regular-expression* | **received-routes** | **routes**]	特定の BGP ネイバーから取得されたルートを表示します。
show ip bgp paths	データベース内のすべての BGP パスを表示します。
show ip bgp peer-group [*tag*] [**summary**]	BGP ピア グループに関する情報を表示します。
show ip bgp summary	BGP 接続すべての状況を表示します。

bgp log-neighbor changes コマンドは、デフォルトでイネーブルです。 そのため、BGP ネイバーのリセット、起動、またはダウン時に生成されるメッセージをログに記録できます。

ISO CLNS ルーティングに関する情報

コネクションレス型ルーティング

国際標準化機構（ISO）コネクションレス型ネットワーク サービス（CLNS）プロトコルとは、オープン システムインターコネクション（OSI）モデルのネットワーク層の標準の 1 つです。 ISO ネットワーク アーキテクチャ内のアドレスは、ネットワーク サービスアクセスポイント（NSAP）アドレスおよび Network Entity Titles（NETs）と呼ばれます。 OSI ネットワークの各ノードには、1 つ以上の NETs が含まれます。 さらに、各ノードには、多数の NSAP アドレスが含まれます。

スイッチ上で、**clns routing** グローバル コンフィギュレーション コマンドを使用してコネクションレス型ルーティングをイネーブルにすると、スイッチはルーティング関連の機能を果たさず、転送の決定だけを行います。 ダイナミック ルーティングには、ルーティング プロトコルもイネーブルにする必要があります。 スイッチは、Intermediate System-to-Intermediate System（IS-IS）ダイナミック ルーティング プロトコルをサポートします。このプロトコルは、ISO CLNS ネットワーク用の OSI ルーティング プロトコルに基づいています。

動的にルーティングを行う場合は、IS-IS を使用します。 このルーティング プロトコルは、エリアの概念をサポートします。 1 つのエリア内部では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。 エリア間では、ルータは適切なエリアに到達する方法を認識しています。 IS-IS は、ステーション ルーティング（1 つのエリア内）およびエリア ルーティング（エリア間）という 2 つのレベルのルーティングをサポートします。

ISO IGRP と IS-IS NSAP アドレス方式の主な違いは、エリア アドレスの定義にあります。 両方ともレベル 1 ルーティング（1 つのエリア内）にはシステム ID を使用します。 ただし、エリア ルーティングに関してアドレスが指定される方法が異なります。 ISO IGRP NSAP アドレスには、ドメイン、エリア、およびシステム ID という 3 つの異なるフィールドが含まれます。 IS-IS アドレスには、単一の連続的エリア フィールド（ドメイン フィールドおよびエリア フィールドから成る）とシステム ID という 2 つのフィールドが含まれます。

（注） ISO CLNS の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Configuration Guide, Release 12.4*』を参照してください。 この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.4*』を参照するか、IOS コマンド リファレンス マスター インデックスを使用するか、オンライン検索を行ってください。

ISO CLNS ルーティングの設定方法

IS-IS ダイナミック ルーティング

IS-IS は、ISO ダイナミック ルーティング プロトコルの 1 つです（ISO 105890 で説明されている）。 その他のルーティング プロトコルとは異なり、IS-IS をイネーブルするには、IS-IS ルーティング プロセスを作成し、それをネットワークではなく特定のインターフェイスに割り当てる必要があります。 マルチエリア IS-IS コンフィギュレーション構文を使用することで、レイヤ 3 スイッチまたはルータごとに複数の IS-IS ルーティング プロトコルを指定できます。 その後、IS-IS ルーティング プロセスのインスタンスごとにパラメータを設定します。

小規模の IS-IS ネットワークは、ネットワーク内にすべてのルータが含まれる単一のエリアとして構築されます。 ネットワークの規模が大きくなるに従って、このネットワークは、すべてのエリアに属する、接続されたすべてのレベル 2 ルータのセットから構成されるバックボーン エリア内に再編成され、その後、このネットワークはローカル エリアに接続されます。 ローカル エリア内部では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。 エリア間では、ルータはバックボーンへの到達方法を認識しており、バックボーン ルータは他のエリアに到達する方法を認識しています。

ルータは、ローカル エリア内でルーティングを実行するために、レベル 1 の隣接関係を確立します（ステーション ルーティング）。 ルータは、レベル 1 のエリア間でルーティングを実行するために、レベル 2 の隣接関係を確立します（エリア ルーティング）。

1 つの Cisco ルータは、最大 29 エリアのルーティングに参加でき、バックボーンでレベル 2 ルーティングを実行できます。 一般に、ルーティング プロセスごとに 1 つのエリアに対応します。 デフォルトでは、ルーティング プロセスの最初のインスタンスが、レベル 1 および レベル 2 両方のルーティングを実行するように設定されます。 追加のルーティングインスタンスを設定できます。このインスタンスは、自動的にレベル 1 エリアとして扱われます。 IS-IS ルーティング プロセスの各インスタンスごとに個別にパラメータを設定する必要があります。

IS-IS マルチエリア ルーティングでは、シスコの各装置に対して最大 29 個の レベル 1 エリアを定義できますが、レベル 2 ルーティングを実行するプロセスは 1 つだけ設定できます。 レベル 2 ルーティングが任意のプロセス上に設定されている場合、追加のプロセスは、すべて自動的にレベル 1 に設定されます。 同時に、このプロセスがレベル 1 ルーティングを実行するように設定することもできます。 ルータ インスタンスにレベル 2 ルーティングが必要でない場合は、**is-type** グローバル コンフィギュレーション コマンドを使用してレベル 2 の機能を削除します。 別のルータ インスタンスをレベル 2 ルータとして設定する場合にも **is-type** コマンドを使用します。

（注） IS-IS の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Routing Protocols」を参照してください。 ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS IP Command Reference, Release 12.4*』を参照してください。

IS-IS のデフォルト設定

表 *93* : *IS-IS* のデフォルト設定

機能	デフォルト設定
リンクステート PDU（LSP）エラーを無視	イネーブル
IS-IS タイプ	従来型の IS-IS：ルータは、レベル 1（ステーション）とレベル 2（エリア） 両方のルータとして機能します。 マルチエリア IS-IS：IS-IS ルーティング プロセスの最初のインスタンスが レベル 1-2 ルータです。 残りのインスタンスは、レベル 1 ルータです。
デフォルト情報送信元	ディセーブル
IS-IS 隣接関係のステート変更を記録	ディセーブル
LSP 生成スロットリング タイマー	連続で生成した 2 つの間の最大インターバル：5 秒 初期 LSP 生成遅延：50 ミリ秒 1 番目と 2 番目の LSP 生成間のホールド タイム：5000 ミリ秒
LSP 最大ライフ タイム（リフレッシュなし）	LSP パケットが削除されるまで 1200 秒（20 分）
LSP リフレッシュ インターバル	LSP リフレッシュを 900 秒（15 分）ごとに送信
最大 LSP パケット サイズ	1497 バイト
NSF 認識	イネーブル レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
部分ルート計算（PRC）スロットリング タイマー	最大 PRC 待機インターバル：5 秒 トポロジの変更後の初期 PRC 計算遅延：2000 ミリ秒 1 番目と 2 番目の PRC 計算間のホールド タイム：5000 ミリ秒
パーティション回避	ディセーブル

機能	デフォルト設定
パスワード	エリアまたはドメインのパスワードが定義されておらず、認証はディセーブルになっています。
過負荷ビットの設定	ディセーブル イネーブルの際に引数が入力されない場合、過負荷ビットがただちに設定され、**no set-overload-bit** コマンドが入力されるまで設定されたままになります。
Shortest Path First（SPF）スロットリング タイマー	連続した SFP 間の最大インターバル：10 秒 トポロジの変更後の初期 SFP 計算：5500 ミリ秒 1 番目と 2 番目の SFP 計算間のホールド タイム：5500 ミリ秒
サマリー アドレス	ディセーブル

NSF 認識

統合型 IS-IS NSF 認識機能は IPv4G でサポートされています。 この機能により、NSF を認識する顧客宅内装置（CPE）ルータが、NFS 対応ルータによるパケットのノンストップ転送を実現します。 ローカルルータでは、必ずしもNSFを実行している必要はありませんが、このルータがNSFを認識していると、スイッチオーバープロセス時にルーティングデータベースの整合性と精度、および隣接 NSF 対応ルータ上のリンクステート データベースが保持されます。

この機能は、自動的にイネーブルにされ、設定は必要ありません。 この機能の詳細については、『*Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

IS-IS ルーティングのイネーブル化

IS-IS をイネーブルにするには、各ルーティング プロセスに名前と NET を指定します。 その後、インターフェイス上で IS-IS ルーティングをイネーブルにし、ルーティング プロセスの各インスタンスに対してエリアを指定します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**clns routing** 例： `Switch(config)# clns routing`	スイッチ上で ISO コネクションレス型ルーティングをイネーブルに設定します。
ステップ 3	**router isis** [*area tag*] 例： `Switch(config)# router isis tag1`	指定したルーティング プロセスに対して IS-IS ルーティングをイネーブルにし、IS-IS ルーティング コンフィギュレーション モードを開始します。 （任意）*area tag* 引数を使用して、IS-IS ルータが割り当てられているエリアを特定します。 複数の IS-IS エリアを設定する場合は、値を入力する必要があります。 最初に設定された IS-IS インスタンスは、デフォルトでレベル 1-2 です。 後のインスタンスは、自動的にレベル 1 になります。 **is-type** グローバル コンフィギュレーション コマンドを使用してルーティングのレベルを変更できます。
ステップ 4	**net** network-entity-title 例： `Switch(config-router)# net 47.0004.004d.0001.0001.0c11.1111.00`	ルーティング プロセスに NET を設定します。 マルチエリア IS-IS を設定する場合、各ルーティング プロセスに NET を指定します。 NET およびアドレスの名前を指定できます。
ステップ 5	**is-type** {**level-1** | **level-1-2** | **level-2-only**} 例： `Switch(config-router)# is-type level-2-only`	（任意）レベル 1（ステーション）ルータ、マルチエリア ルーティング用のレベル 2（エリア）ルータ、または両方（デフォルト）として機能するようにルータを設定します。 • **level-1**：ステーション ルータとしてだけ機能します。 • **level-1-2**：ステーション ルータおよびエリア ルータの両方として機能します。 • **level 2**：エリア ルータだけとして機能します。
ステップ 6	**exit** 例： `Switch(config-router)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	IS-IS をルーティングするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスがまだレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力し、インターフェイスをレイヤ 3 モードにします。

	コマンドまたはアクション	目的
ステップ 8	**ip router isis** [*area tag*] 例： `Switch(config-if)# ip router isis tag1`	インターフェイス上の ISO CLNS に対して IS-IS ルーティングプロセスを設定し、ルーティングプロセスにエリアデジグネータを接続します。
ステップ 9	**clns router isis** [*area tag*] 例： `Switch(config-if)# clns router isis tag1`	インターフェイス上で ISO CLNS をイネーブルにします。
ステップ 10	**ip address***ip-address-mask* 例： `Switch(config-if)# ip address 10.0.0.5 255.255.255.0`	インターフェイスの IP アドレスを定義します。 インターフェイスのいずれかで IS-IS ルーティングが設定されている場合は、IS-IS がイネーブルになっているエリアに含まれるすべてのインターフェイスで IP アドレスが必要です。
ステップ 11	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show isis** [*area tag*] **database detail** 例： `Switch# show isis database detail`	入力を確認します。
ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

例：IS-IS ルーティングの設定

次に、従来型の IS-IS を IP ルーティング プロトコルとして実行するために 3 つのルータを設定する方法を示します。 従来型の IS-IS では、すべてのルータはレベル 1 およびレベル 2 のルータとして機能します（デフォルト）。

ルータ A：

```
Switch(config)# clns routing
Switch(config)# router isis
```

```
Switch(config-router)# net 49.0001.0000.0000.000a.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

ルータ B：

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000b.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

ルータ C：

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000c.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

IS-IS グローバル パラメータ

設定可能ないくつかのオプションの IS-IS グローバル パラメータを次に示します。

- ルート マップによって制御されるデフォルト ルートを設定することで、デフォルト ルートを IS-IS ルーティング ドメイン内に強制的に設定できます。 ルート マップで設定可能な、その他のフィルタリング オプションも指定できます。
- 内部チェックサム エラーとともに受信された IS-IS LSP を無視したり、破損した LSP を消去するようにルータを設定できます。これにより、LSP の発信側は、LSP を再生成します。
- エリアおよびドメインにパスワードを割り当てられます。
- サマリー アドレスを使用して、ルーティング テーブル内に表示される集約アドレスを作成できます（経路集約）。他のルーティング プロトコルから学習したルートも集約できます。サマリーをアドバタイズするのに使用されるメトリックは、すべての個別ルートにおける最小のメトリックです。
- 過負荷ビットを設定できます。
- LSP リフレッシュ インターバルおよび LSP がリフレッシュなしでルータ データベース内にとどまることができる最大時間を設定できます。

- LSP 生成に対するスロットリング タイマー、最短パス優先計算、および部分ルート計算を設定できます。
- IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、スイッチがログ メッセージを生成するように設定できます。
- ネットワーク内のリンクが、1500 バイト未満の最大伝送単位（MTU）サイズの場合、それでもルーティングが行われるように LSP MTU の値を低くできます。
- パーティション回避ルータ コンフィギュレーション コマンドは、レベル 1-2 境界ルータ、隣接レベル 1 ルータ、およびエンド ホスト間で完全な接続が失われた場合に、エリアがパーティション化されるのを防ぎます。

IS-IS グローバル パラメータの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clns routing** 例： `Switch(config)# clns routing`	スイッチ上で ISO コネクションレス型ルーティングをイネーブルに設定します。
ステップ 3	**router isis** 例： `Switch(config)# router isis`	IS-IS ルーティング プロトコルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**default-information originate** [**route-map***map-name*] 例： `Switch(config-router)# default-information originate route-map map1`	（任意）デフォルト ルートを IS-IS ルーティング ドメインに強制的に設定します。 **route-map***map-name* を入力すると、ルートマップが条件に一致している場合にルーティング プロセスによってデフォルト ルートが生成されます。
ステップ 5	**ignore-lsp-errors** 例： `Switch(config-router)# ignore-lsp-errors`	（任意）LSP を消去する代わりに、内部チェックサムにエラーがある LSP を無視するようにルータを設定します。 このコマンドは、デフォルトでイネーブルになっています（破損した LSP はドロップされます）。 破損した LSP を消去するには、**no**

	コマンドまたはアクション	目的
		ignore-lsp-errors ルータ コンフィギュレーション コマンドを入力します。
ステップ 6	**area-password***password* 例： `Switch(config-router)# area-password 1password`	（任意）レベル 1（ステーション ルータ レベル）LSP に挿入されるエリア認証パスワードを設定します。
ステップ 7	**domain-password***password* 例： `Switch(config-router)# domain-password 2password`	（任意）レベル 2（エリア ルータ レベル）LSP に挿入されるルーティング ドメイン認証パスワードを設定します。
ステップ 8	**summary-address***address mask* [**level-1** | **level-1-2** | **level-2**] 例： `Switch(config-router)# summary-address 10.1.0.0 255.255.0.0 level-2`	（任意）所定のレベルのアドレスのサマリーを作成します。
ステップ 9	**set-overload-bit** [**on-startup** {*seconds* | **wait-for-bgp**}] 例： `Switch(config-router)# set-overload-bit on-startup wait-for-bgp`	（任意）ルータに問題がある場合に、他のルータが最短パス優先（SPF）計算でこのルータを無視するように過負荷ビット（hippity ビット）を設定します。 • （任意）**on-startup**：起動時だけ過負荷ビットを設定します。 **on-startup** が指定されない場合、過負荷ビットが即座に設定され、**no set-overload-bit** コマンドを入力するまで設定されたままになります。 **on-startup** が指定された場合、秒数または **wait-for-bgp** を入力する必要があります。 • *seconds*：**on-startup** キーワードが設定されている場合、システム起動時に過負荷ビットが設定されて、この秒数の間設定されたままになります。 指定できる範囲は 5 ～ 86400 秒です。 • **wait-for-bgp**：**on-startup** キーワードが設定されている場合、システム起動時に過負荷ビットが設定されて、BGP が収束するまで設定されたままになります。 BGP が収束されたことが IS-IS に通知されない場合、IS-IS は 10 分後に過負荷ビットをオフにします。

	コマンドまたはアクション	目的
ステップ 10	**lsp-refresh-interval***seconds* 例： `Switch(config-router)# lsp-refresh-interval 1080`	（任意）LSP リフレッシュ インターバル（秒）を設定します。範囲は 1 ～ 65535 秒です。 デフォルトでは、LSP リフレッシュを 900 秒（15 分）ごとに送信します。
ステップ 11	**max-lsp-lifetime***seconds* 例： `Switch(config-router)# max-lsp-lifetime 1000`	（任意）LSPパケットがリフレッシュされずにルータデータベース内に存続する最大時間を設定します。 範囲は 1 ～ 65535 秒です。 デフォルト値は 1200 秒（20 分）です。 指定されたタイムインターバルのあと、LSP パケットは削除されます。
ステップ 12	**lsp-gen-interval**[**level-1** | **level-2**] *lsp-max-wait*[*lsp-initial-wait lsp-second-wait*] 例： `Switch(config-router)# lsp-gen-interval level-2 2 50 100`	（任意）IS-IS 生成スロットリング タイマーを設定します。 • *lsp-max-wait*：2 つの連続する LSP 生成間の最大インターバル（秒）。 指定できる範囲は 1 ～ 120 秒です。デフォルト値は 5 秒です。 • *lsp-initial-wait*：最初の LSP 生成遅延（ミリ秒）。 指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。 • *lsp-second-wait*：最初と 2 番目の LSP 生成間（ミリ秒）のホールド タイム。 指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
ステップ 13	**spf-interval**[**level-1** | **level-2**] *spf-max-wait*[*spf-initial-wait spf-second-wait*] 例： `Switch(config-router)# spf-interval level-2 5 10 20`	（任意）IS-IS SPF スロットリング タイマーを設定します。 • *spf-max-wait*：連続する SFP 間（秒）の最大インターバル。指定できる範囲は 1 ～ 120 で、デフォルトは 10 です。 • *spf-initial-wait*：トポロジ変更後の最初の SFP 計算（ミリ秒）。 指定できる値の範囲は 1 ～ 10000 です。デフォルトは 5500 です。 • *spf-second-wait*：最初と 2 番目の SFP 計算間（ミリ秒）のホールド タイム。 指定できる値の範囲は 1 ～ 10000 です。デフォルトは 5500 です。
ステップ 14	**prc-interval***prc-max-wait*[*prc-initial-wait prc-second-wait*] 例： `Switch(config-router)# prc-interval 5 10 20`	（任意）IS-IS PRC スロットリング タイマーを設定します。 • *prc-max-wait*：2 つの連続する PRC 計算間の最大インターバル（秒）。 指定できる範囲は 1 ～ 120 秒です。デフォルト値は 5 秒です。 • *prc-initial-wait*：トポロジ変更後の最初の PRC 計算遅延（ミリ秒）。 指定できる範囲は 1 ～ 10,000 ミリ秒です。デフォルト値は 2000 ミリ秒です。

	コマンドまたはアクション	目的
		• *prc-second-wait*：最初と 2 番目の PRC 計算間（ミリ秒）のホールド タイム。 指定できる範囲は 1 ～ 10,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
ステップ 15	**log-adjacency-changes** [**all**] 例： `Switch(config-router)# log-adjacency-changes all`	（任意）IS-IS 隣接ステート変更をログするようルータを設定します。 End System-to-Intermediate System PDU およびリンクステートパケット（LSP）など、IS-IS Hello に関連しないイベントにより生成されたすべての変更をログに含めるには、**all** を入力します。
ステップ 16	**lsp-mtu***size* 例： `Switch(config-router)# lsp mtu 1560`	（任意）最大 LSP パケット サイズ（バイト）を指定します。 指定できる範囲は 128 ～ 4352 バイトです。デフォルト値は 1497 バイトです。 （注） ネットワーク内の任意のリンクで MTU サイズが縮小された場合、ネットワーク内のすべてのルータで LSP MTU サイズを変更する必要があります。
ステップ 17	**partition avoidance** 例： `Switch(config-router)# partition avoidance`	（任意）境界ルータ、すべての隣接レベル 1 ルータ、およびエンド ホスト間で、フル接続が切断された場合、IS-IS レベル 1-2 境界ルータがレベル 1 エリア プレフィックスをレベル 2 バックボーンにアドバタイズしないようにします。
ステップ 18	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 19	**show clns** 例： `Switch# show clns`	入力を確認します。
ステップ 20	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

IS-IS インターフェイス パラメータ

任意で、特定のインターフェイス固有のIS-ISパラメータを、付加されている他のルータとは別に設定できます。ただし、一部の値（乗数およびタイムインターバルなど）をデフォルトから変更する場合、複数のルータおよびインターフェイス上でもこれを変更する必要があります。 ほとんどのインターフェイス パラメータは、レベル 1、レベル 2、またはその両方で設定できます。

次に、設定可能なインターフェイス レベル パラメータの一部を示します。

- インターフェイスのデフォルト メトリック：Quality of Service（QoS）ルーティングが実行されない場合に、IS-IS メトリックの値として使用され、割り当てられます。
- hello インターバル（インターフェイスから送信される hello パケットの間隔）またはデフォルトの hello パケット乗数：インターフェイス上で使用されて、IS-IS hello パケットで送信されるホールド タイムを決定します。 ホールド タイムは、ネイバーがダウンしていると宣言するまでに、別の hello パケットを待機する時間を決定します。 これにより、障害リンクまたはネイバーが検出される速さも決定し、ルートを再計算できるようになります。 hello パケットが頻繁に失われ、IS-IS 隣接に無用な障害が発生する場合は、hello 乗数を変更してください。 hello 乗数を大きくし、それに対応して hello インターバルを小さくすると、リンク障害を検出するのに必要な時間を増やすことなく、helloプロトコルの信頼性を高めることができます。
- その他のタイム インターバル：
  - Complete Sequence Number PDU（CSNP）インターバル。 CSNP は、指定ルータにより送信され、データベースの同期を維持します。
  - 再送信インターバル。 これは、ポイントツーポイント リンクの IS-IS LSP の再送信間隔です。
  - IS-IS LSP 再送信スロットル インターバル。 これは、IS-IS LSP がポイントツーポイント リンクで再送信される最大レート（パケット間のミリ秒数）です。このインターバルは、同じ LSP が連続する再送信間隔である再送信インターバルとは異なります。
- 指定ルータの選択プライオリティ：マルチアクセス ネットワークで必要な隣接数を削減し、その代わりに、ルーティング プロトコル トラフィックの量およびトポロジ データベースのサイズを削減できます。
- インターフェイス回線タイプ：指定されたインターフェイス上のネイバーに必要な隣接タイプです。
- インターフェイスのパスワード認証

IS-IS インターフェイス パラメータの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスがまだレイヤ3インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力し、インターフェイスをレイヤ 3 モードにします。
ステップ 3	**isis metric***default-metric* [**level-1** | **level-2**] 例： `Switch(config-if)# isis metric 15`	（任意）指定したインターフェイスにメトリック（またはコスト）を設定します。 範囲は0～63です。 デフォルトは10です。 レベルが入力されない場合は、レベル1およびレベル2ルータの両方にデフォルト値が適用されます。
ステップ 4	**isis hello-interval** {*seconds* | **minimal**} [**level-1** | **level-2**] 例： `Switch(config-if)# isis hello-interval minimal`	（任意）スイッチがhelloパケットを送信する間隔を指定します。 デフォルトでは、helloインターバル *seconds* の 3 倍の値が、送信される hello パケットの *holdtime* としてアドバタイズされます。 helloインターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。 • **minimal**：ホールドタイムが1秒になるように、システムがhello乗数に基づいてhelloインターバルを計算するようにします。 • *seconds*：範囲は 1 ～ 65535 秒です。 デフォルトは 10 秒です。
ステップ 5	**isis hello-multiplier***multiplier* [**level-1** | **level-2**] 例： `Switch(config-if)# isis hello-multiplier 5`	（任意）ルータが隣接装置のダウンを宣言するまでに、ネイバーが損失するIS-IShelloパケット数を指定します。 指定できる範囲は 3 ～ 1000 です。 デフォルトは 3 です。 hello 乗数を小さくすると、高速コンバージェンスとなりますが、ルーティングが不安定になる場合があります。

	コマンドまたはアクション	目的
ステップ 6	**isis csnp-interval***seconds* [**level-1** | **level-2**] 例： `Switch(config-if)# isis csnp-interval 15`	（任意）インターフェイスに IS-IS CSNP を設定します。 範囲は 0 ～ 65535 です。 デフォルトは 10 秒です。
ステップ 7	**isis retransmit-interval***seconds* 例： `Switch(config-if)# isis retransmit-interval 7`	（任意）ポイントツーポイント リンクの IS-IS LSP の再送信間隔（秒）を設定します。 指定する値は、ネットワーク上の任意の 2 つのルータ間の予測ラウンドトリップ遅延よりも大きい整数である必要があります。 範囲は 0 ～ 65535 です。 デフォルトは 5 秒です。
ステップ 8	**isis retransmit-throttle-interval***milliseconds* 例： `Switch(config-if)# isis retransmit-throttle-interval 4000`	（任意）IS-IS LSP 再送信スロットルインターバルを設定します。これは、IS-IS LSP がポイントツーポイント リンク上で再送信される最大レート（パケット間のミリ秒数）です。 範囲は 0 ～ 65535 です。 デフォルト値は、**isis lsp-interval** コマンドにより決定します。
ステップ 9	**isis priority***value* [**level-1** | **level-2**] 例： `Switch(config-if)# isis priority 50`	（任意）指定ルータ選択で使用するプライオリティを設定します。 指定できる範囲は 0 ～ 127 です。 デフォルトは 64 です。
ステップ 10	**isis circuit-type** {**level-1** | **level-1-2** | **level-2-only**} 例： `Switch(config-if)# isis circuit-type level-1-2`	（任意）指定されたインターフェイス上のネイバーで必要な隣接タイプを設定します（インターフェイスの回線タイプを指定します）。 • **level-1**：このノードとネイバーの両方に共通のエリア アドレスが少なくとも 1 つある場合、レベル 1 隣接関係が確立されます。 • **level-1-2**：ネイバーもレベル 1 およびレベル 2 の両方として設定されていて、少なくとも 1 つの共通のエリアがある場合、レベル 1 およびレベル 2 隣接関係が確立されます。 共通のエリアがない場合は、レベル 2 隣接関係が確立されます。これはデフォルト設定です。 これはデフォルトです。 • **level 2**：レベル 2 隣接関係が確立されます。 ネイバー ルータがレベル 1 ルータである場合、隣接関係は確立されません。

	コマンドまたはアクション	目的
ステップ 11	**isis password***password* [**level-1** | **level-2**] 例： `Switch(config-if)# isis password secret`	（任意）インターフェイスの認証パスワードを設定します。 デフォルトでは、認証はディセーブルに設定されています。 レベル 1 またはレベル 2 を指定すると、それぞれレベル 1 またはレベル 2 ルーティング用のパスワードだけがイネーブルになります。 レベルを指定しない場合、デフォルトはレベル 1 およびレベル 2 です。
ステップ 12	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show clns interface***interface-id* 例： `Switch# show clns interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 14	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ISO IGRP と IS-IS のモニタリングおよびメンテナンス

CLNS キャッシュのすべての内容または特定のネイバーまたはルートの情報を削除できます。 ルーティング テーブル、キャッシュ、およびデータベースの内容など、特定の CLNS または IS-IS の統計情報を表示できます。 また、特定のインターフェイス、フィルタ、またはネイバーに関する情報も表示できます。

次の表に、ISO CLNS および IS-IS ルーティングを消去および表示するために使用する特権 EXEC コマンドを示します。 出力フィールドの詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference,* 』を参照するか、Cisco IOS コマンド リファレンス マスター インデックスを使用するか、オンライン検索を行ってください。

表 *94*：*ISO CLNS* と *IS-IS* の *clear* および *show* コマンド

コマンド	目的
clear clns cache	CLNS ルーティング キャッシュをクリアおよび再初期化します。
clear clns es-neighbors	隣接データベースから End System（ES）ネイバー情報を削除します。
clear clns is-neighbors	隣接データベースから Intermediate System（IS）ネイバー情報を削除します。
clear clns neighbors	隣接データベースから CLNS ネイバー情報を削除します。
clear clns route	動的に派生した CLNS ルーティング情報を削除します。
show clns	CLNS ネットワークに関する情報を表示します。
show clns cache	CLNS ルーティング キャッシュ内のエントリを表示します。
show clns es-neighbors	ES ネイバー エントリ（関連のあるエリアなど）を表示します。
show clns filter-expr	フィルタ式を表示します。
show clns filter-set	フィルタ セットを表示します。
show clns interface [*interface-id*]	各インターフェイスの CLNS 固有の情報または ES-IS 情報を表示します。

コマンド	目的
show clns neighbor	IS-IS ネイバーに関する情報を表示します。
show clns protocol	このルータの IS-IS または ISO IGRP ルーティング プロセスごとにプロトコル固有の情報を表示します。
show clns route	このルータが CLNS パケットをルーティングする方法を把握している宛先をすべて表示します。
show clns traffic	このルータで確認された CLNS パケットに関する情報を表示します。
show ip route isis	ISIS IP ルーティング テーブルの現在のステートを表示します。
show isis database	IS-IS リンクステート データベースを表示します。
show isis routes	IS-IS レベル 1 ルーティング テーブルを表示します。
show isis spf-log	IS-IS の Shortest Path First（SPF）計算の履歴を表示します。
show isis topology	すべてのエリアで接続済みルータのリストを表示します。
show route-map	設定されたすべてのルートマップ、または指定した1つのルート マップだけを表示します。
trace clns*destination*	ネットワークのパケットが指定された宛先までに経由するパスを検出します。

コマンド	目的
which-route {*nsap-address* | *clns-name*}	指定された CLNS の宛先が見つかったルーティングテーブルを表示します。

Multi-VRF CE に関する情報

バーチャル プライベート ネットワーク（VPN）は、ISP バックボーン ネットワーク上でお客様にセキュアな帯域幅共有を提供します。 VPN は、共通ルーティング テーブルを共有するサイトの集合です。 カスタマー サイトは、1 つまたは複数のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーは、VRF テーブルと呼ばれる VPN ルーティング テーブルと各インターフェイスを関連付けます。

スイッチ上で IP サービスまたは拡張 IP サービス フィーチャ セットが稼働している場合、スイッチはカスタマー エッジ（CE）デバイスの複数の VRF ルーティング/転送（Multi-VRF）インスタンスをサポートします（Multi-VRF CE）。 サービス プロバイダーは、Multi-VRF CE により、重複する IP アドレスで複数の VPN をサポートできます。

（注） スイッチでは、VPN のサポートのためにマルチプロトコル ラベル スイッチング（MPLS）が使用されません。

Multi-VRF CE の概要

Multi-VRF CE は、サービス プロバイダーが複数の VPN をサポートし、VPN 間で IP アドレスを重複して使用できるようにする機能です。 Multi-VRF CE は入力インターフェイスを使用して、さまざまな VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスと各 VRF を関連付けて仮想パケット転送テーブルを形成します。 VRF 内のインターフェイスは、イーサネット ポートのように物理的なもの、または VLAN SVI のように論理的なものにもできますが、複数の VRF に属すことはできません。

（注） Multi-VRF CE インターフェイスは、レイヤ 3 インターフェイスである必要があります。

Multi-VRF CE には、次のデバイスが含まれます。

- お客様は、CE デバイスにより、1 つまたは複数のプロバイダー エッジ（PE）ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。 CE デバイスは、サイトのローカル ルートをルータにアドバタイズし、リモート VPN ルートをそこから学習します。 スイッチを CE に設定することができます。

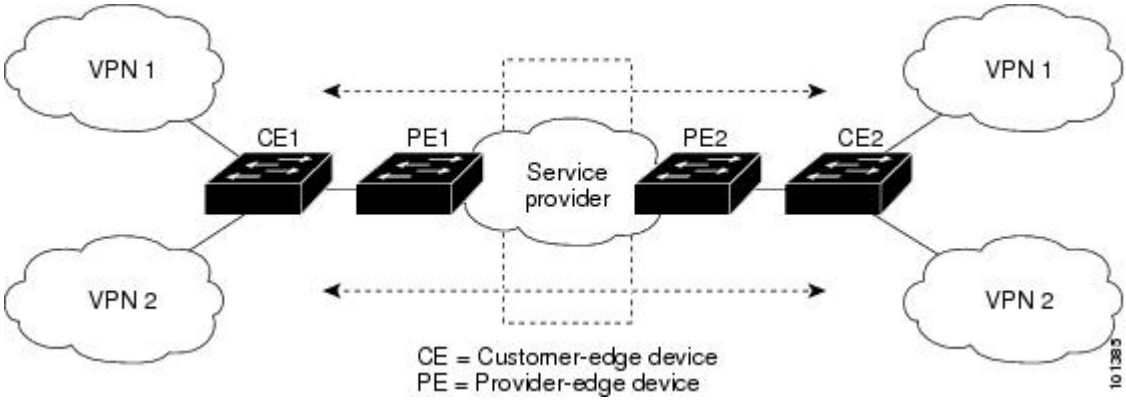
- PE ルータは、スタティック ルーティング、または BGP、RIPv2、OSPF、EIGRP などのルーティング プロトコルを使用して、CEデバイスとルーティング情報を交換します。 PEは、直接接続している VPN に対する VPN ルートのみを保守する必要があります。そのため、すべてのサービス プロバイダー VPN ルートを PE が保守する必要はありません。 各 PE ルータは、直接接続しているサイトごとに VRF を維持します。 すべてのサイトが同じ VPN に存在する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。 各 VPN は、指定された VRF にマッピングされます。 PE ルータは、ローカル VPN ルートを CE から学習したあとで、IBGP を使用して別の PE ルータと VPN ルーティング情報を交換します。
- CE デバイスに接続していないサービス プロバイダー ネットワークのルータは、プロバイダー ルータやコア ルータになります。

Multi-VRF CE では、複数のお客様が 1 つの CE を共有でき、CE と PE の間で 1 つの物理リンクだけが使用されます。 共有 CE は、お客様ごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、お客様ごとにパケットをスイッチングまたはルーティングします。 Multi-VRF CE は、制限付きの PE 機能を CE デバイスに拡張して、別々の VRF テーブルを維持し、VPN のプライバシーおよびセキュリティをブランチ オフィスに拡張します。

ネットワーク トポロジ

次の図に、スイッチを複数の仮想 CE として使用した構成例を示します。 このシナリオは、中小企業など、VPN サービスの帯域幅要件の低いお客様に適しています。 この場合、スイッチにはマルチ VRF CE のサポートが必要です。 Multi-VRF CE はレイヤ 3 機能なので、VRF のそれぞれのインターフェイスはレイヤ 3 インターフェイスである必要があります。

図 *75*：複数の仮想 *CE* として機能するスイッチ



CE スイッチは、レイヤ 3 インターフェイスを VRF に追加するコマンドを受信すると、Multi-VRF CE 関連のデータ構造で VLAN ID と Policy Label（PL）の間に適切なマッピングを設定し、VLAN ID と PL を VLAN データベースに追加します。

Multi-VRF CE を設定すると、レイヤ 3 フォワーディング テーブルは、次の 2 つのセクションに概念的に分割されます。

- Multi-VRF CE ルーティング セクションには、さまざまな VPN からのルートが含まれます。
- グローバル ルーティング セクションには、インターネットなど、VPN 以外のネットワークへのルートが含まれます。

さまざまな VRF の VLAN ID はさまざまな PL にマッピングされ、処理中に VRF を区別するために使用されます。 レイヤ 3 設定機能では、学習した新しい VPN ルートごとに、入力ポートの VLAN ID を使用して PL を取得し、Multi-VRF CE ルーティング セクションに PL および新しいルートを挿入します。 ルーテッド ポートからパケットを受信した場合は、ポート内部 VLAN ID 番号が使用されます。SVI からパケットを受信した場合は、VLAN 番号が使用されます。

パケット転送処理

Multi-VRF CE 対応ネットワークのパケット転送処理は次のとおりです。

- スイッチは、VPN からパケットを受信すると、入力 PL 番号に基づいてルーティング テーブルを検索します。 ルートが見つかると、スイッチはパケットを PE に転送します。
- 入力 PE は、CE からパケットを受信すると、VRF 検索を実行します。 ルートが見つかると、ルータは対応する MPLS ラベルをパケットに追加し、MPLS ネットワークに送信します。
- 出力 PE は、ネットワークからパケットを受信すると、ラベルを除去してそのラベルを使用し、正しい VPN ルーティング テーブルを識別します。 次に、通常のルート検索を実行します。 ルートが見つかると、パケットを正しい隣接デバイスに転送します。
- CE は、出力 PE からパケットを受信すると、入力 PL を使用して正しい VPN ルーティング テーブルを検索します。 ルートが見つかると、パケットを VPN 内で転送します。

ネットワーク コンポーネント

VRF を設定するには、VRF テーブルを作成し、VRF に関連するレイヤ 3 インターフェイスを指定します。 次に、VPN、および CE と PE 間でルーティング プロトコルを設定します。 プロバイダーのバックボーンで VPN ルーティング情報を配信する場合は、BGP が優先ルーティング プロトコルです。 Multi-VRF CE ネットワークには、次の 3 つの主要コンポーネントがあります。

- VPN ルート ターゲット コミュニティ：VPN コミュニティのその他すべてのメンバのリスト。 VPN コミュニティ メンバーごとに VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング：VPN コミュニティのすべてのメンバーに VRF 到達可能性情報を伝播します。 VPN コミュニティのすべての PE ルータで BGP ピアリングを設定する必要があります。
- VPN 転送：VPN サービス プロバイダー ネットワークを介し、全 VPN コミュニティ メンバー間で、全トラフィックを伝送します。

VRF 認識サービス

IP サービスはグローバル インターフェイスに設定可能で、グローバル ルーティング インスタンスで稼働します。 IP サービスは複数のルーティング インスタンス上で稼働するように拡張されま

す。これが、VRF 認識です。 システム内の任意の設定済み VRF であればいずれも、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームに依存しないモジュールに実装されます。 VRF とは、Cisco IOS 内の複数のルーティング インスタンスを意味します。 各プラットフォームには、サポートする VRF 数に関して独自の制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに ping を実行できます。
- ARP エントリは、個別の VRF で学習されます。 ユーザは、特定の VRF の ARP エントリを表示できます。

Multi-VRF CE の設定方法

Multi-VRF CE のデフォルト設定

表 *95* : ***VRF*** のデフォルト設定

機能	デフォルト設定
VRF	ディセーブル。 VRF は定義されていません。
マップ	インポート マップ、エクスポート マップ、ルート マップは定義されていません。
VRF 最大ルート数	ファスト イーサネット スイッチ：8000 ギガビット イーサネット スイッチ：12000
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブルです。

Multi-VRF CE の設定時の注意事項

（注） Multi-VRF CE を使用するには、スイッチで IP サービスまたは拡張 IP サービス フィーチャ セットをイネーブルにする必要があります。

- Multi-VRF CE を含むスイッチは複数のお客様によって共有され、各お客様には独自のルーティング テーブルがあります。
- お客様は別々の VRF テーブルを使用するので、同じ IP アドレスを再利用できます。 別々の VPN では IP アドレスの重複が許可されます。
- Multi-VRF CE では、複数のお客様が、PE と CE の間で同じ物理リンクを共有できます。 複数の VLAN を持つトランク ポートでは、パケットがお客様間で分離されます。 それぞれのお客様には独自の VLAN があります。
- Multi-VRF CE ではサポートされない MPLS-VRF 機能があります。 ラベル交換、LDP 隣接関係、ラベル付きパケットはサポートされません。
- PE ルータの場合、Multi-VRF CE の使用と複数の CE の使用に違いはありません。 図 41-6 では、複数の仮想レイヤ 3 インターフェイスが Multi-VRF CE デバイスに接続されています。
- スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合わせを使用して、VRF を設定できます。 SVI は、アクセス ポートまたはトランク ポートで接続できます。
- お客様は、別のお客様と重複しないかぎり、複数の VLAN を使用できます。 お客様の VLAN は、スイッチに保存されている適切なルーティング テーブルの識別に使用される特定のルーティング テーブル ID にマッピングされます。
- スイッチは、1 つのグローバル ネットワークおよび最大 26 の VRF をサポートします。
- CE と PE の間では、ほとんどのルーティング プロトコル（BGP、OSPF、RIP、およびスタティック ルーティング）を使用できます。 ただし、次の理由から External BGP（EBGP）を使用することを推奨します。
  - BGP では、複数の CE とのやり取りに複数のアルゴリズムを必要としません。
  - BGP は、さまざまな管理者によって稼働するシステム間でルーティング情報を渡すように設計されています。
  - BGP では、ルートの属性を CE に簡単に渡すことができます。
- Multi-VRF CE は、パケットのスイッチング レートに影響しません。
- VPN マルチキャストはサポートされません。
- プライベート VLAN で VRF をイネーブルにできます（逆も同様です）。
- インターフェイスでポリシーベース ルーティング（PBR）がイネーブルになっている場合は、VRF をイネーブルにできません（逆も同様です）。
- インターフェイスで Web Cache Communication Protocol（WCCP）がイネーブルになっている場合は、VRF をイネーブルにできません（逆も同様です）。

VRF の設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： `Switch(config)# ip routing`	IP ルーティングをイネーブルにします。
ステップ 3	**ip vrf***vrf-name* 例： `Switch(config)# ip vrf vpn1`	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd***route-distinguisher* 例： `Switch(config-vrf)# rd 100:2`	ルート識別子を指定して VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `Switch(config-vrf)# route-target both 100:2`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。 AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。 *route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同一にする必要があります。
ステップ 6	**import map***route-map* 例： `Switch(config-vrf)# import map importmap1`	（任意）VRF にルート マップを対応付けます。

	コマンドまたはアクション	目的
ステップ 7	**interface***interface-id* 例： `Switch(config-vrf)# interface gigabitethernet 1/0/1`	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。インターフェイスにはルーテッドポートまたは SVI を設定できます。
ステップ 8	**ip vrf forwarding***vrf-name* 例： `Switch(config-if)# ip vrf forwarding vpn1`	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： `Switch# show ip vrf interfaces vpn1`	設定を確認します。 設定した VRF に関する情報を表示します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

VRF 認識サービスの設定

次のサービスは、VRF 認識です。

- ARP
- ping
- 簡易ネットワーク管理プロトコル（SNMP）
- ユニキャスト RPF（uRPF）
- Syslog
- traceroute
- FTP および TFTP

（注） このスイッチでは、ユニキャスト RPF（uRPF）およびネットワーク タイム プロトコル（NTP）に対して VRF 認識のサービスはサポートされません。

ARP 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ip arp vrf***vrf-name* 例： `Switch# show ip arp vrf vpn1`	指定された VRF 内の ARP テーブルを表示します。

ping 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ping vrf***vrf-name***ip-host** 例： `Switch# ping vrf vpn1 ip-host`	指定された VRF 内の ARP テーブルを表示します。

SNMP 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server trap authentication vrf** 例： `Switch(config)# snmp-server trap authentication vrf`	VRF で、パケットに対して SNMP トラップをイネーブルにします。
ステップ 3	**snmp-server engineID remote***host***vrf***vpn-instance engine-id string* 例： `Switch(config)# snmp-server engineID remote 172.16.20.3 vrf vpn1 80000009030000B064EFE100`	スイッチ上で、リモート SNMP エンジンの名前を設定します。
ステップ 4	**snmp-server host***host***vrf***vpn-instance***traps***community* 例： `Switch(config)# snmp-server host 172.16.20.3 vrf vpn1 traps comaccess`	SNMP トラップ動作の受信側、および SNMP トラップの送信に使用される VRF テーブルを指定します。
ステップ 5	**snmp-server host***host***vrf***vpn-instance***informs***community* 例： `Switch(config)# snmp-server host 172.16.20.3 vrf vpn1 informs comaccess`	SNMP 通知動作の受信先を指定し、SNMP 通知の送信に使用される VRF テーブルを指定します。
ステップ 6	**snmp-server user***user group***remote***host***vrf***vpn-instance security model* 例： `Switch(config)# snmp-server user abcd remote 172.16.20.3 vrf vpn1 priv v2c 3des secure3des`	SNMP アクセス用に、VRF 上にあるリモートホストの SNMP グループにユーザを追加します。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

HSRP 用 VRF 認識サービスの設定

VRF の HSRP サポートにより、HSRP 仮想 IP アドレスが、確実に適切な IP ルーティング テーブルに追加されます。

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	**ip vrf forwarding***vrf-name* 例： `Switch(config-if)# ip vrf forwarding vpn1`	インターフェイス上で VRF を設定します。
ステップ 5	**ip address***ip-address* 例： `Switch(config-if)# ip address 10.1.5.1`	インターフェイスの IP アドレスを入力します。
ステップ 6	**standby 1 ip***ip-address* 例： `Switch(config-if)#standby 1 ip 10.1.1.254`	HSRP をイネーブルにして、仮想 IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

uRPF 用 VRF 認識サービスの設定

uRPF は、VRF に割り当てられたインターフェイス上で設定でき、送信元検索が VRF テーブルで実行されます。

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

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

ステップ 2	**interface** *interface-id*
	
	例：
	`Switch(config)#`
	`interface gigabitethernet 1/0/1`
		インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。

ステップ 3	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	**ip vrf forwarding***vrf-name* 例： `Switch(config-if)# ip vrf forwarding vpn2`	インターフェイス上で VRF を設定します。

	コマンドまたはアクション	目的
ステップ 5	**ip address***ip-address* 例： `Switch(config-if)# ip address 10.1.5.1`	インターフェイスの IP アドレスを入力します。
ステップ 6	**ip verify unicast reverse-path** 例： `Switch(config-if)# ip verify unicast reverse-path`	インターフェイス上で uRPF をイネーブルにします。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

VRF 認識 RADIUS の設定

VRF 認識 RADIUS を設定するには、まず RADIUS サーバ上で AAA をイネーブルにする必要があります。『Per VRF AAA Feature Guide』で説明されているとおり、スイッチで **ip vrf forwarding** *vrf-name* サーバグループ コンフィギュレーション コマンドと **ip radius source-interface** グローバル コンフィギュレーション コマンドがサポートされます。

syslog 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**logging on** 例： `Switch(config)# logging on`	ストレージルータイベントメッセージのロギングを、イネーブルまたは一時的にディセーブルにします。
ステップ 3	**logging host***ip-address***vrf***vrf-name* 例： `Switch(config)# logging host 10.10.1.0 vrf vpn1`	ロギング メッセージが送信される Syslog サーバのホスト アドレスを指定します。
ステップ 4	**logging buffered***logging buffered size***debugging** 例： `Switch(config)# logging buffered critical 6000 debugging`	メッセージを内部バッファにロギングします。
ステップ 5	**logging trap debugging** 例： `Switch(config)# logging trap debugging`	Syslog サーバに送信されるロギング メッセージを制限します。
ステップ 6	**logging facility***facility* 例： `Switch(config)# logging facility user`	ロギング ファシリティにシステム ロギング メッセージを送信します。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

traceroute 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『Cisco IOS Switching Services Command Reference, Release 12.4』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**traceroute vrf***vrf-name ipaddress* 例： `Switch(config)# traceroute vrf vpn2 10.10.1.1`	宛先アドレスを取得する VPN VRF の名前を指定します。

FTP および TFTP 用 VRF 認識サービスの設定

FTP および TFTP を VRF 認識とするには、いくつかの FTP/TFTP CLI を設定する必要があります。たとえば、インターフェイスに付加される VRF テーブルを使用する場合、E1/0 であれば、ip tftp source-interface E1/0 コマンドまたは ip ftp source-interface E1/0 コマンドを設定して、特定のルーティング テーブルを使用するように TFTP または FTP サーバに通知する必要があります。 この例では、VRF テーブルが宛先 IP アドレスを検索するのに使用されます。 これらの変更には下位互換性があり、既存の動作には影響を及ぼしません。 つまり、VRF がそのインターフェイスに設定されていない場合でも、送信元インターフェイス CLI を使用して、特定のインターフェイスにパケットを送信できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip ftp source-interface***interface-type interface-number* 例： `Switch(config)# ip ftp source-interface gigabitethernet 1/0/2`	FTP 接続の発信元 IP アドレスを指定します。
ステップ 3	**end** 例： `Switch(config)#end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**configure terminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 5	**ip tftp source-interface***interface-type interface-number* 例： `Switch(config)# ip tftp source-interface gigabitethernet 1/0/2`	TFTP 接続用の送信元 IP アドレスを指定します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**end** 例： `Switch(config)#end`	特権 EXEC モードに戻ります。

マルチキャスト VRF の設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS IP Multicast Command Reference*』を参照してください。

Multi-VRF CE 内でのマルチキャスト設定の詳細については、『*IP Routing: Protocol-Independent Configuration Guide, Cisco IOS Release 15S*』を参照してください。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**ip routing** 例： `Switch(config)# ip routing`	IP ルーティング モードをイネーブルにします
ステップ 3	**ip vrf***vrf-name* 例： `Switch(config)# ip vrf vpn1`	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd***route-distinguisher* 例： `Switch(config-vrf)# rd 100:2`	ルート識別子を指定して VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `Switch(config-vrf)# route-target import 100:2`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。 AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。 *route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同一にする必要があります。
ステップ 6	**import map***route-map* 例： `Switch(config-vrf)# import map importmap1`	（任意）VRF にルート マップを対応付けます。
ステップ 7	**ip multicast-routing vrf***vrf-name***distributed** 例： `Switch(config-vrf)# ip multicast-routing vrf vpn1 distributed`	（任意）VRF テーブルでグローバル マルチキャスト ルーティングをイネーブルにします。
ステップ 8	**interface***interface-id* 例： `Switch(config-vrf)# interface gigabitethernet 1/0/2`	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスはルーテッド ポートまたは SVI に設定できます。
ステップ 9	**ip vrf forwarding***vrf-name* 例： `Switch(config-if)# ip vrf forwarding vpn1`	VRF をレイヤ 3 インターフェイスに対応付けます。

	コマンドまたはアクション	目的
ステップ 10	**ip address***ip-address***mask** 例： `Switch(config-if)# ip address 10.1.5.1 255.255.255.0`	レイヤ3インターフェイスのIPアドレスを設定します。
ステップ 11	**ip pim sparse-dense mode** 例： `Switch(config-if)# ip pim sparse-dense mode`	VRF に関連付けられているレイヤ 3 インターフェイス上で、PIM をイネーブルにします。
ステップ 12	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： `Switch# show ip vrf detail vpn1`	設定を確認します。 設定した VRF に関する情報を表示します。
ステップ 14	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされている任意のルーティング プロトコル（RIP、OSPF、EIGRP、BGP）、またはスタティック ルーティングで設定できます。 ここで説明する設定はOSPFのものですが、その他のプロトコルでも手順は同じです。

（注） VRF インスタンス内で EIGRP ルーティング プロセスが実行されるように設定するには、**autonomous-system***autonomous-system-number* アドレス ファミリ コンフィギュレーション モード コマンドを入力して、自律システム番号を設定する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf***process-id***vrf***vrf-name* 例： `Switch(config)# router ospf 1 vrf vpn1`	OSPF ルーティングをイネーブルにして VPN 転送テーブルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**log-adjacency-changes** 例： `Switch(config-router)# log-adjacency-changes`	（任意）隣接ステートの変更を記録します。 これは、デフォルトの状態です。
ステップ 4	**redistribute bgp***autonomous-system-number***subnets** 例： `Switch(config-router)# redistribute bgp 10 subnets`	BGP ネットワークから OSPF ネットワークに情報を再配布するようにスイッチを設定します。
ステップ 5	**network***network-number***area***area-id* 例： `Switch(config-router)# network 1 area 2`	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**end** 例： `Switch(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip ospf***process-id* 例： `Switch# show ip ospf 1`	OSPF ネットワークの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP PE/CE ルーティング セッションの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp***autonomous-system-number* 例： `Switch(config)# router bgp 2`	その他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**network***network-number***mask***network-mask* 例： `Switch(config-router)# network 5 mask 255.255.255.0`	BGP を使用してアナウンスするネットワークおよびマスクを指定します。
ステップ 4	**redistribute ospf***process-id***match internal** 例： `Switch(config-router)# redistribute ospf 1 match internal`	OSPF 内部ルートを再配布するようにスイッチを設定します。
ステップ 5	**network***network-number***area***area-id* 例： `Switch(config-router)# network 5 area 2`	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**address-family ipv4 vrf***vrf-name* 例： `Switch(config-router)# address-family ipv4 vrf vpn1`	PE/CE ルーティング セッションの BGP パラメータを定義し、VRF アドレス ファミリ モードを開始します。
ステップ 7	**neighbor***address***remote-as***as-number* 例： `Switch(config-router)# neighbor 10.1.1.2 remote-as 2`	PE と CE ルータの間の BGP セッションを定義します。

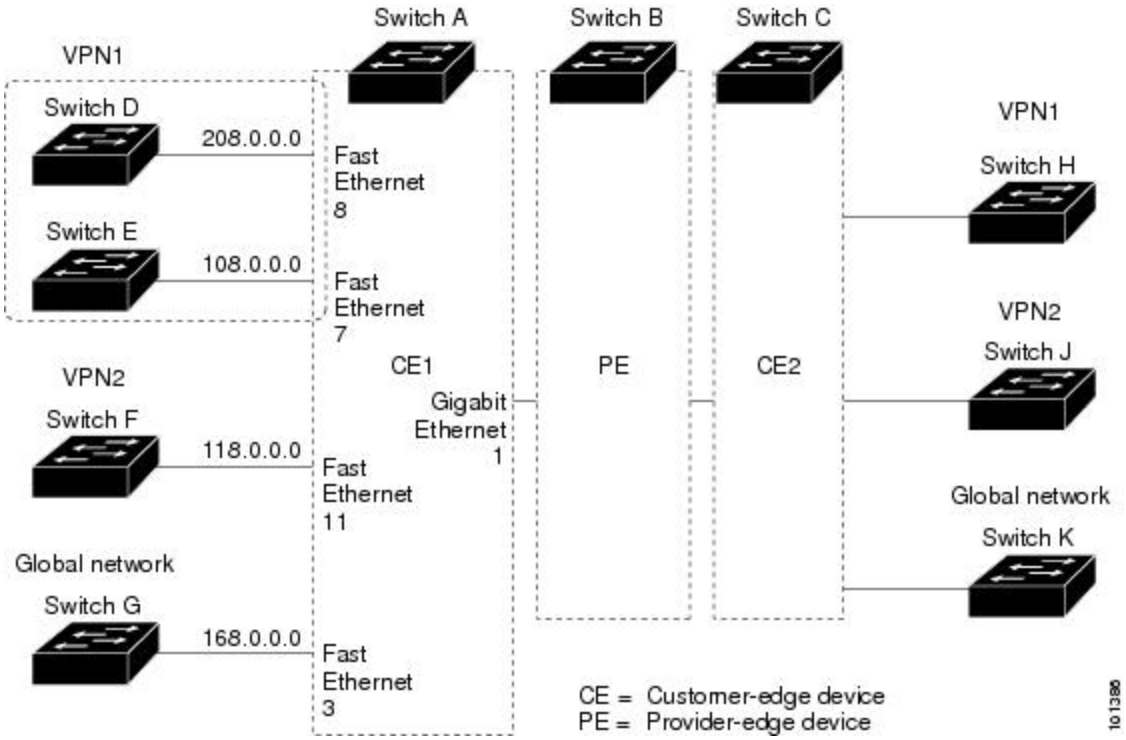
	コマンドまたはアクション	目的
ステップ 8	**neighbor***address***activate** 例： `Switch(config-router)# neighbor 10.2.1.1 activate`	IPv4 アドレス ファミリのアドバタイズメントをアクティブ化します。
ステップ 9	**end** 例： `Switch(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip bgp** [**ipv4**] [**neighbors**] 例： `Switch# show ip bgp ipv4 neighbors`	BGP 設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Multi-VRF CE の設定例

VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。 CE/PE 接続には BGP が使用されます。 図のあとに続く出力は、スイッチを CE スイッチ A として設定する例、およびカスタマー スイッチ D と F の VRF 設定を示しています。CE スイッチ C とその他のカスタマー スイッチを設定するコマンドは含まれていませんが、内容は同様です。 この例には、PE

ルータとして動作する Catalyst 6000 スイッチまたは Catalyst 6500 スイッチのスイッチ A へのトラフィックを設定するコマンドも含まれています。

図 *76*：*Multi-VRF CE* の設定例



スイッチ A では、ルーティングをイネーブルにして VRF を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

スイッチ A のループバックおよび物理インターフェイスを設定します。ギガビット イーサネット ポート 1 は PE へのトランク接続です。 ギガビット イーサネット ポート 8 と 11 は VPN に接続されます。

```
Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
```

```
Switch(config-if)# exit

Switch(config)# interface gigabitethernet1/0/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
```

スイッチ A で使用する VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。 VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。 VLAN 118 と 208 は、それぞれスイッチ F とスイッチ D を含む VPN に使用されます。

```
Switch(config)# interface vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface vlan208
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit
```

VPN1 と VPN2 で OSPF ルーティングを設定します。

```
Switch(config)# router ospf 1 vrf vl1
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf vl2
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
```

CE/PE ルーティングに BGP を設定します。

```
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf vl2
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit
Switch(config-router)# address-family ipv4 vrf vl1
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

スイッチ D は VPN 1 に属します。 次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface gigabitethernet1/0/2
```

```
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

スイッチ F は VPN 2 に属します。 次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

このコマンドをスイッチ B（PE ルータ）で使用すると、CE デバイス、スイッチ A に対する接続だけが設定されます。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit
Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/1/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/1/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
```

```
Router(config-router)# address-family ipv4 vrf vl
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end
```

Multi-VRF CE のモニタリング

表 *96*：***Multi-VRF CE*** 情報を表示するコマンド

show ip protocols vrf *vrf-name*	VRF に対応付けられたルーティング プロトコル情報を表示します。
show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**] [**supernets-only**]	VRF に対応付けられた IP ルーティング テーブル情報を表示します。
show ip vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]	定義された VRF インスタンスに関する情報を表示します。

表示される情報の詳細については、『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

ユニキャスト リバース パス転送の設定

uRPF 機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造（スプーフィングされた）送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。 たとえば、Smurf や Tribal Flood Network（TFN）など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタすることを攻撃者が阻止できるようにします。パブリック アクセスを提供するインターネット サービス プロバイダー（ISP）の場合、uRPF が IP ルーティング テーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、そのような攻撃をそらします。 この処理により、ISP のネットワーク、その顧客、および残りのインターネットが保護されます。

（注）

- uRPF は、 でサポートされます。

IP uRPF 設定の詳細については、『*Cisco IOS Security Configuration Guide*』の「*Other Security Features*」の章を参照してください。

プロトコル独立機能

この項では、IP ルーティング プロトコルに依存しない機能について説明します。これらの機能は、 フィーチャ セットが稼働するスイッチ上で使用できます。 この章の IP ルーティング プロトコル独立コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』の「IP Routing Protocol-Independent Commands」の章を参照してください。

分散型シスコ エクスプレス フォワーディング

シスコ エクスプレス フォワーディングに関する情報

シスコエクスプレスフォワーディング（CEF）は、ネットワーク パフォーマンスを最適化するために使用されるレイヤ 3 IP スイッチング技術です。 CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。 高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に割り当てることができます。 スイッチ スタックでは、ハードウェアによって distributed CEF（dCEF）が使用されます。 動的なネットワークでは、ルーティングの変更によって、高速スイッチング キャッシュ エントリが頻繁に無効になります。高速スイッチング キャッシュエントリが無効になると、トラフィックがルートキャッシュによって高速スイッチングされずに、ルーティングテーブルによってプロセス スイッチングされることがあります。 CEF および dCEF は転送情報ベース（FIB）検索テーブルを使用して、宛先ベースの IP パケット スイッチングを実行します。

CEF および dCEF での 2 つの主要なコンポーネントは、分散 FIB と分散隣接テーブルです。

- FIB はルーティング テーブルや情報ベースと同様、IP ルーティング テーブルに転送情報のミラー イメージが保持されます。 ネットワーク内でルーティングまたはトポロジが変更されると、IP ルーティング テーブルがアップデートされ、これらの変更が FIB に反映されます。 FIB には、IP ルーティング テーブル内の情報に基づいて、ネクストホップのアドレス情報が保持されます。 FIB にはルーティング テーブル内の既知のルートがすべて格納されているため、CEF はルート キャッシュをメンテナンスする必要がなく、トラフィックのスイッチングがより効率化され、トラフィック パターンの影響も受けません。
- リンク層上でネットワーク内のノードが 1 ホップで相互に到達可能な場合、これらのノードは隣接関係にあると見なされます。 CEF は隣接テーブルを使用し、レイヤ 2 アドレッシング情報を付加します。 隣接テーブルには、すべての FIB エントリに対する、レイヤ 2 のネクストホップのアドレスが保持されます。

スイッチまたはスイッチスタックは、ギガビット速度の回線レート IP トラフィックを達成するため特定用途向け集積回路（ASIC）を使用しているので、CEF または dCEF 転送はソフトウェア転送パス（CPU により転送されるトラフィック）にだけ適用されます。

シスコ エクスプレス フォワーディングの設定方法

デフォルトで、CEF または dCEF はグローバルにイネーブルに設定されています。 何らかの理由でこれがディセーブルになった場合は、**ip cef** または **ip cef distributed** グローバル コンフィギュレーション コマンドを使用し、再度イネーブルに設定できます。

デフォルト設定では、すべてのレイヤ 3 インターフェイスで CEF または dCEF がイネーブルです。 **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドを入力すると、ソフトウェアが転送するトラフィックに対して CEF がディセーブルになります。 このコマンドは、ハードウェア転送パスには影響しません。 CEF をディセーブルにして **debug ip packet detail** 特権 EXEC コマンドを使用すると、ソフトウェア転送トラフィックをデバッグするのに便利です。 ソフトウェア転送パス用のインターフェイスで CEF をイネーブルにするには、**ip route-cache cef** インターフェイス コンフィギュレーション コマンドを使用します。

注意 CLI には、インターフェイス上で CEF をディセーブルにする **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドが表示されますが、デバッグ以外の目的でインターフェイス上で CEF または dCEF をディセーブルにしないようにしてください。

ディセーブルである CEF または dCEF をグローバルにイネーブルにしたり、ソフトウェア転送トラフィックのインターフェイス上でイネーブルにするには、次の手順を実行します。

手順の概要

1. **configureterminal**
2. **ip cef**
3. **ip cef distributed**
4. **interface***interface-id*
5. **ip route-cache cef**
6. **end**
7. **show ip cef**
8. **show cef linecard** [**detail**]
9. **show cef linecard** [*slot-number*] [**detail**]
10. **show cef interface** [*interface-id*]
11. **show adjacency**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip cef** 例： `Switch(config)# ip cef`	非スタッキング スイッチで CEF の動作をイネーブルにします。 ステップ 4 に進みます。
ステップ 3	**ip cef distributed** 例： `Switch(config)# ip cef distributed`	アクティブ スイッチで CEF の動作をイネーブルにします。
ステップ 4	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 5	**ip route-cache cef** 例： `Switch(config-if)# ip route-cache cef`	ソフトウェア転送トラフィック用のインターフェイスで CEF をイネーブルにします。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip cef** 例： `Switch# show ip cef`	すべてのインターフェイスの CEF ステータスを表示します。
ステップ 8	**show cef linecard [detail]** 例： `Switch# show cef linecard detail`	（任意）非スタッキング スイッチの CEF 関連インターフェイス情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	**show cef linecard** [*slot-number*] [**detail**] 例： `Switch# show cef linecard 5 detail`	（任意）スタック内のすべてのスイッチ、または指定されたスイッチに対して、スイッチのCEF関連インターフェイス情報をスタック メンバ別に表示します。 （任意）*slot-number* には、スタック メンバーのスイッチ番号を入力します。
ステップ 10	**show cef interface** [*interface-id*] 例： `Switch# show cef interface gigabitethernet 1/0/1`	すべてのインターフェイスまたは指定されたインターフェイスの詳細な CEF 情報を表示します。
ステップ 11	**show adjacency** 例： `Switch# show adjacency`	CEF の隣接テーブル情報を表示します。
ステップ 12	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

等コスト ルーティング パスの個数

等コスト ルーティング パスに関する情報

同じネットワークへ向かう同じメトリックのルートが複数ルータに格納されている場合、これらのルートは等価コストを保有していると見なされます。ルーティングテーブルに複数の等コストルートが含まれる場合は、これらをパラレルパスと呼ぶこともあります。ネットワークへの等コストパスがルータに複数格納されている場合、ルータはこれらを同時に使用できます。パラレルパスを使用すると、パスに障害が発生した場合に冗長性を確保できます。また、使用可能なパスにパケットの負荷を分散し、使用可能な帯域幅を有効利用することもできます。等コストルートは、スタック内の各スイッチでサポートされます。

等コスト ルートはルータによって自動的に取得、設定されますが、ルーティング テーブルの IP ルーティング プロトコルでサポートされるパラレル パスの最大数は制御可能です。 スイッチ ソフトウェア では最大 32 の等コスト ルーティングが許可されていますが、スイッチ ハードウェアはルートあたり 17 パス以上は使用しません。

等コスト ルーティング パスの設定方法

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**rip** | **ospf** | **eigrp**} 例： `Switch(config)# router eigrp`	ルータ コンフィギュレーションモードを開始します。
ステップ 3	**maximum-paths** *maximum* 例： `Switch(config-router)# maximum-paths 2`	プロトコル ルーティング テーブルのパラレル パスの最大数を設定します。 指定できる範囲は 1 ～ 16 です。ほとんどの IP ルーティング プロトコルでデフォルトは 4 ですが、BGP の場合だけ 1 です。
ステップ 4	**end** 例： `Switch(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols** 例： `Switch# show ip protocols`	*Maximum path* フィールドの設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スタティック ユニキャスト ルート

スタティック ユニキャスト ルートに関する情報

スタティックユニキャストルートは、特定のパスを通過して送信元と宛先間でパケットを送受信するユーザ定義のルートです。 ルータが特定の宛先へのルートを構築できない場合、スタティッ

ク ルートは重要で、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

ユーザによって削除されるまで、スタティック ルートはスイッチに保持されます。 ただし、アドミニストレーティブ ディスタンスの値を割り当て、スタティック ルートをダイナミック ルーティング情報で上書きできます。 各ダイナミック ルーティング プロトコルには、デフォルトのアドミニストレーティブ ディスタンスが設定されています（表 10 を参照）。 ダイナミック ルーティング プロトコルの情報でスタティック ルートを上書きする場合は、スタティック ルートのアドミニストレーティブ ディスタンスがダイナミック プロトコルのアドミニストレーティブ ディスタンスよりも大きな値になるように設定します。

表 *97*：ダイナミック ルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルト距離
接続されているインターフェイス	0
スタティック ルート	1
EIGRP サマリー ルート	5
内部 EIGRP	90
IGRP	100
OSPF	110
不明（Unknown）	225

インターフェイスを指し示すスタティック ルートは、RIP、IGRP、およびその他のダイナミック ルーティング プロトコルを通してアドバタイズされます。**redistribute** スタティック ルータ コンフィギュレーション コマンドが、これらのルーティング プロトコルに対して指定されているかどうかは関係ありません。 これらのスタティック ルートがアドバタイズされるのは、インターフェイスを指し示すスタティック ルートが接続された結果、静的な性質を失ったとルーティング テーブルで見なされるためです。 ただし、network コマンドで定義されたネットワーク以外のインターフェイスに対してスタティック ルートを定義する場合は、ダイナミック ルーティング プロトコルに **redistribute** スタティック コマンドを指定しない限り、ルートはアドバタイズされません。

インターフェイスがダウンすると、ダウンしたインターフェイスを経由するすべてのスタティック ルートが IP ルーティング テーブルから削除されます。 転送ルータのアドレスとして指定されたアドレスへ向かう有効なネクスト ホップがスタティック ルート内に見つからない場合は、IP ルーティング テーブルからそのスタティック ルートも削除されます。

スタティック ユニキャスト ルートの設定

スタティック ユニキャスト ルートは、特定のパスを通過して送信元と宛先間でパケットを送受信するユーザ定義のルートです。 ルータが特定の宛先へのルートを構築できない場合、スタティッ

ク ルートは重要で、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

スタティック ルートを設定するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip routeprefix mask** {*address* | *interface*} [*distance*] 例： `Switch(config)# ip route prefix mask gigabitethernet 1/0/4`	スタティック ルートを確立します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip route** 例： `Switch# show ip route`	設定を確認するため、ルーティング テーブルの現在の状態を表示します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

スタティック ルートを削除するには、**no ip route***prefix mask*{*address*|*interface*} グローバル コンフィギュレーション コマンドを使用します。 ユーザによって削除されるまで、スタティック ルートはスイッチに保持されます。

デフォルトのルートおよびネットワーク

デフォルトのルートおよびネットワークに関する情報

ルータは、他のすべてのネットワークへのルートを学習できません。 完全なルーティング機能を実現するには、一部のルータをスマート ルータとして使用し、それ以外のルータのデフォルト ルートをスマート ルータ宛てに指定します （スマート ルータにはインターネットワーク全体のルーティング テーブルに関する情報が格納されます）。 これらのデフォルト ルートは動的に学習できますが、ルータごとに設定することもできます。 ほとんどのダイナミックな内部ルーティングプロトコルには、スマートルータを使用してデフォルト情報を動的に生成し、他のルータに転送するメカニズムがあります。

指定されたデフォルト ネットワークに直接接続されたインターフェイスがルータに存在する場合は、そのデバイス上で動作するダイナミック ルーティング プロトコルによってデフォルト ルートが生成されます。 RIP の場合は、疑似ネットワーク 0.0.0.0 がアドバタイズされます。

ネットワークのデフォルトを生成しているルータには、そのルータ自身のデフォルト ルートも指定する必要があります。 ルータが自身のデフォルト ルートを生成する方法の 1 つは、適切なデバイスを経由してネットワーク 0.0.0.0 に至るスタティック ルートを指定することです。

ダイナミックルーティングプロトコルによってデフォルト情報を送信するときは、特に設定する必要はありません。 ルーティング テーブルは定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。 IGRP ネットワークでは、システムのデフォルト ネットワークの候補が複数存在する場合もあります。 Cisco ルータでは、デフォルト ルートまたは最終ゲートウェイを設定するため、アドミニストレーティブ ディスタンスおよびメトリック情報を使用します。

ダイナミックなデフォルト情報がシステムに送信されない場合は、**ip default-network** グローバル コンフィギュレーション コマンドを使用し、デフォルト ルートの候補を指定します。 このネットワークが任意の送信元のルーティングテーブルに格納されている場合は、デフォルトルートの候補としてフラグ付けされます。 ルータにデフォルトネットワークのインターフェイスが存在しなくても、そこへのパスが格納されている場合、そのネットワークは 1 つの候補と見なされ、最適なデフォルト パスへのゲートウェイが最終ゲートウェイになります。

デフォルトのルートおよびネットワークの設定方法

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip default-network***network number* 例： `Switch(config)# ip default-network 1`	デフォルト ネットワークを指定します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ip route** 例： `Switch# show ip route`	最終ゲートウェイで選択されたデフォルト ルートを表示します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング情報を再配信するためのルート マップ

ルート マップの概要

スイッチでは複数のルーティングプロトコルを同時に実行し、ルーティングプロトコル間で情報を再配信できます。ルーティングプロトコル間での情報の再配信は、サポートされているすべての IP ベース ルーティング プロトコルに適用されます。

2 つのドメイン間で拡張パケット フィルタまたはルート マップを定義することにより、ルーティング ドメイン間でルートの再配信を条件付きで制御することもできます。 **match** および **set** ルート マップ コンフィギュレーション コマンドは、ルート マップの条件部を定義します。 **match** コマンドは、条件が一致する必要があることを指定しています。**set** コマンドは、ルーティングアップデートが match コマンドで定義した条件を満たす場合に行われる処理を指定します。 再配信は

プロトコルに依存しない機能ですが、**match** および **set** ルート マップ コンフィギュレーション コマンドの一部は特定のプロトコル固有のものです。

route-map コマンドのあとに、**match** コマンドおよび **set** コマンドをそれぞれ 1 つまたは複数指定します。 **match** コマンドを指定しない場合は、すべて一致すると見なされます。 **set** コマンドを指定しない場合、一致以外の処理はすべて実行されません。 このため、少なくとも 1 つの **match** または **set** コマンドを指定する必要があります。

（注） **set** ルート マップ コンフィギュレーション コマンドを使用しないルート マップは、CPU に送信されるので、CPU の使用率が高くなります。

ルートマップ ステートメントは、**permit** または **deny** として識別することもできます。 ステートメントが拒否としてマークされている場合、一致基準を満たすパケットは通常の転送チャネルを通じて送り返されます（宛先ベースルーティング）。ステートメントが許可としてマークされている場合は、一致基準を満たすパケットに set コマンドが適用されます。 一致基準を満たさないパケットは、通常のルーティング チャネルを通じて転送されます。

関連トピック

ポリシーベース ルーティングの概要, （1034 ページ）
その他の OSPF パラメータ, （920 ページ）

ルート マップの設定方法

次に示すステップ 3 ～ 14 はそれぞれ任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

（注） キーワードは、ルート配信を制御する手順で定義されているものと同じです。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map***map-tag* [**permit** | **deny**] [*sequence number*] 例： `Switch(config)# route-map rip-to-ospf permit 4`	再配信を制御するために使用するルートマップを定義し、ルート マップ コンフィギュレーション モードを開始します。 *map-tag*：ルート マップ用のわかりやすい名前を指定します。 **redistribute** ルータ コンフィギュレーション コマン

	コマンドまたはアクション	目的
		ドはこの名前を使用して、このルート マップを参照します。 複数のルート マップで同じマップ タグ名を共有できます。 （任意）**permit** が指定され、このルート マップの一致条件が満たされている場合は、set アクションの制御に従ってルートが再配信されます。 **deny** が指定されている場合、ルートは再配信されません。 *sequence number*（任意）：同じ名前によってすでに設定されているルート マップのリスト内で、新しいルート マップの位置を指定する番号です。
ステップ 3	**match as-path***path-list-number* 例： `Switch(config-route-map)#match as-path 10`	BGP AS パス アクセス リストと照合します。
ステップ 4	**match community-list***community-list-number* [**exact**] 例： `Switch(config-route-map)# match community-list 150`	BGP コミュニティ リストのマッチングを行います。
ステップ 5	**match ip address** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*] 例： `Switch(config-route-map)# match ip address 5 80`	名前または番号を指定し、標準アクセス リストと照合します。 1 ～ 199 の整数を指定できます。
ステップ 6	**match metric** metric-value 例： `Switch(config-route-map)# match metric 2000`	指定されたルート メトリックと一致させます。 *metric-value* には、0 ～ 4294967295 の値が指定された、EIGRP のメトリックを指定できます。
ステップ 7	**match ip next-hop** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*] 例： `Switch(config-route-map)# match ip next-hop 8 45`	指定されたアクセス リスト（番号 1 ～ 199）のいずれかで送信される、ネクストホップのルータ アドレスと一致させます。

	コマンドまたはアクション	目的
ステップ 8	**match tag** *tag value* [*...tag-value*] 例： `Switch(config-route-map)# match tag 3500`	1 つまたは複数のルート タグ値からなるリスト内の指定されたタグ値と一致させます。 0 ～ 4294967295 の整数を指定できます。
ステップ 9	**match interface***type number* [*...type-number*] 例： `Switch(config-route-map)# match interface gigabitethernet 1/0/1`	指定されたインターフェイスの 1 つから、指定されたネクスト ホップへのルートと一致させます。
ステップ 10	**match ip route-source**{*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*] 例： `Switch(config-route-map)# match ip route-source 10 30`	アドバタイズされた指定のアクセス リストによって指定したアドレスに一致します。
ステップ 11	**match route-type** {**local** | **internal** | **external** [**type-1** | **type-2**]} 例： `Switch(config-route-map)# match route-type local`	指定された **route-type** と一致させます。 • **local**：ローカルに生成された BGP ルート。 • **internal**：OSPF エリア内およびエリア間ルート、または EIGRP 内部ルート。 • **external**：OSPF 外部ルート（タイプ 1 またはタイプ 2）または EIGRP 外部ルート。
ステップ 12	**set dampening***halflife reuse suppress max-suppress-time* 例： `Switch(config-route-map)# set dampening 30 1500 10000 120`	BGP ルート ダンプニング係数を設定します。
ステップ 13	**set local-preference***value* 例： `Switch(config-route-map)# set local-preference 100`	ローカル BGP パスに値を割り当てます。
ステップ 14	**set origin** {**igp** | **egp***as* | **incomplete**} 例： `Switch(config-route-map)#set origin igp`	BGP 送信元コードを設定します。

	コマンドまたはアクション	目的
ステップ 15	**set as-path** {**tag** | **prepend***as-path-string*} 例： `Switch(config-route-map)# set as-path tag`	BGP の自律システム パスを変更します。
ステップ 16	**set level** {**level-1** | **level-2** | **level-1-2** | **stub-area** | **backbone**} 例： `Switch(config-route-map)# set level level-1-2`	ルーティング ドメインの指定エリアにアドバタイズされるルートのレベルを設定します。 **stub-area** および **backbone** は、OSPF NSSA およびバックボーン エリアです。
ステップ 17	**set metric** *metric value* 例： `Switch(config-route-map)# set metric 100`	再配布されるルートを指定するためのメトリック値を設定します（EIGRP のみ）。 *metric value* は -294967295 ～ 294967295 の整数です。
ステップ 18	**set metric***bandwidth delay reliability loading mtu* 例： `Switch(config-route-map)# set metric 10000 10 255 1 1500`	再配布されるルートを指定するためのメトリック値を設定します（EIGRP のみ）。 • *bandwidth*：0 ～ 4294967295 の範囲のルートのメトリック値またはIGRP帯域幅（キロビット/秒単位）。 • *delay*：0 ～ 4294967295 の範囲のルート遅延（10 マイクロ秒単位）。 • *reliability*：0 ～ 255 の数値で表されるパケット伝送の成功可能性。255 は信頼性が 100% であること、0 は信頼性がないことを意味します。 • *loading*：0 ～ 255 の数値で表されるルートの有効帯域幅（255 は 100% の負荷）。 • *mtu*：ルートの MTU の最小サイズ（バイト単位）。範囲は 0 ～ 4294967295 です。
ステップ 19	**set metric-type** {**type-1** | **type-2**} 例： `Switch(config-route-map)# set metric-type type-2`	再配信されるルートに OSPF 外部メトリック タイプを設定します。

	コマンドまたはアクション	目的
ステップ 20	**set metric-type internal** 例： `Switch(config-route-map)# set metric-type internal`	ネクスト ホップの IGP メトリックと一致するように、EBGP ネイバーにアドバタイズされるプレフィックスの Multi-Exit 識別子（MED）値を設定します。
ステップ 21	**set weight***number* 例： `Switch(config-route-map)# set weight 100`	ルーティング テーブルの BGP 重みを設定します。 指定できる値は 1 ～ 65535 です。
ステップ 22	**end** 例： `Switch(config-route-map)# end`	特権 EXEC モードに戻ります。
ステップ 23	**show route-map** 例： `Switch# show route-map`	設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ 24	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルート配信の制御方法

次に示すステップ 3 ～ 14 はそれぞれ任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

（注） キーワードは、再配信用にルート マップを設定する手順で定義されているものと同じです。

ルーティング プロトコルのメトリックを、必ずしも別のルーティング プロトコルのメトリックに変換する必要はありません。 たとえば、RIP メトリックはホップ カウントで、IGRP メトリックは 5 つの特性の組み合わせです。 このような場合は、メトリックを独自に設定し、再配信されたルートに割り当てます。 ルーティング情報を制御せずにさまざまなルーティング プロトコル間で交換するとルーティング ループが発生し、ネットワーク動作が著しく低下することがあります。

メトリック変換の代わりに使用されるデフォルトの再配信メトリックが定義されていない場合は、ルーティング プロトコル間で自動的にメトリック変換が発生することがあります。

- RIP はスタティック ルートを自動的に再配信できます。 スタティック ルートにはメトリック 1（直接接続）が割り当てられます。
- デフォルト モードになっている場合、どのプロトコルも他のルーティング プロトコルを再配信できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**rip** | **ospf** | **eigrp**} 例： `Switch(config)# router eigrp 10`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**redistribute***protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric***metric-value*] [**metric-type***type-value*] [**match internal** | **external***type-value*] [**tag***tag-value*] [**route-map***map-tag*] [**weight***weight*] [**subnets**] 例： `Switch(config-router)# redistribute eigrp 1`	ルーティングプロトコル間でルートを再配信します。route-map を指定しないと、すべてのルートが再配信されます。 キーワード **route-map** に *map-tag* を指定しないと、ルートは配信されません。
ステップ 4	**default-metric***number* 例： `Switch(config-router)# default-metric 1024`	現在のルーティング プロトコルが、再配信されたすべてのルートに対して同じメトリック値を使用するように設定します（RIP、OSPF）。
ステップ 5	**default-metric** bandwidth delay reliability loading mtu 例： `Switch(config-router)# default-metric 1000 100 250 100 1500`	EIGRP ルーティング プロトコルが、EIGRP 以外で再配信されたすべてのルートに対して同じメトリック値を使用するように設定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Switch(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show route-map** 例： `Switch# show route-map`	設定を確認するため、設定されたすべてのルートマップ、または指定されたルート マップだけを表示します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ポリシーベース ルーティングの概要，（1034 ページ）
その他の OSPF パラメータ，（920 ページ）

Policy-Based Routing：ポリシーベース ルーティング

ポリシーベース ルーティングの概要

PBR を使用すると、トラフィック フローに定義済みポリシーを設定できます。 PBR を使用してルーティングをより細かく制御するには、ルーティング プロトコルから取得したルートの信頼度を小さくします。 PBR は、次の基準に基づいて、パスを許可または拒否するルーティング ポリシーを設定したり、実装したりできます。

- 特定のエンド システムの ID
- アプリケーション
- プロトコル

PBR を使用すると、等価アクセスや送信元依存ルーティング、インタラクティブ対バッチ トラフィックに基づくルーティング、専用リンクに基づくルーティングを実現できます。 たとえば、在庫記録を本社に送信する場合は高帯域で高コストのリンクを短時間使用し、電子メールなど日常的に使用するアプリケーション データは低帯域で低コストのリンクで送信できます。

PBR がイネーブルの場合は、アクセスコントロールリスト（ACL）を使用してトラフィックを分類し、各トラフィックがそれぞれ異なるパスを経由するようにします。 PBR は着信パケットに適

用されます。 PBR がイネーブルのインターフェイスで受信されたすべてのパケットは、ルートマップを通過します。 ルート マップで定義された基準に基づいて、パケットは適切なネクストホップに転送（ルーティング）されます。

- 許可とマークされているルート マップ文は次のように処理されます。
  - match コマンドは長さまたは複数の ACL で照合できます。 ルート マップ文には複数の match コマンドを含めることができます。 論理関数またはアルゴリズム関数は、許可または拒否の決定がされるまで、すべての match コマンドで実行されます。
    次に例を示します。

    match length A B

    match ip address acl1 acl2

    match ip address acl3

  パケットは、match length A B または acl1 または acl2 または acl3 により許可される場合に許可されます。

  - 決定が許可の場合は、set コマンドで指定されたアクションがパケットで適用されます。
  - 下された決定が拒否の場合は、PBR アクション（set コマンドで指定された）が適用されません。 代わりに、処理ロジックが、シーケンス内の次のルート マップ文（シーケンス番号が次に高い文）に移動します。 次の文が存在しない場合は、PBR 処理が終了し、パケットがデフォルトの IP ルーティング テーブルを使用してルーティングされます。

- PBR では、拒否としてマークされているルートマップ ステートメントはサポートされません。

標準 IP ACL を使用すると、アプリケーション、プロトコル タイプ、またはエンド ステーションに基づいて一致基準を指定するように、送信元アドレスまたは拡張IP ACLの一致基準を指定できます。 一致が見つかるまで、ルート マップにこのプロセスが行われます。 一致が見つからない場合、通常の宛先ベース ルーティングが行われます。 match ステートメント リストの末尾には、暗黙の拒否ステートメントがあります。

match 句が満たされた場合は、set 句を使用して、パス内のネクスト ホップ ルータを識別する IP アドレスを指定できます。

PBR コマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』を参照してください。

関連トピック

ルート マップの概要, （1027 ページ）
ルート マップの設定方法
ルート配信の制御方法, （1032 ページ）

PBR の設定方法

- PBR を使用するには、スイッチまたはスタック マスター上で フィーチャ セットをイネーブルにしておく必要があります。
- マルチキャスト トラフィックには、ポリシーによるルーティングが行われません。 PBR が適用されるのはユニキャスト トラフィックだけです。
- ルーテッド ポートまたは SVI 上で、PBR をイネーブルにできます。
- スイッチは一致長に基づき PBR をサポートします。
- レイヤ 3 モードの EtherChannel ポート チャネルにはポリシー ルート マップを適用できますが、EtherChannel のメンバーである物理インターフェイスには適用できません。 適用しようとすると、コマンドが拒否されます。 ポリシー ルートマップが適用されている物理インターフェイスは、EtherChannel のメンバーになることができません。
- スイッチまたはスイッチ スタックには最大 128 個の IP ポリシー ルート マップを定義できます。
- スイッチまたはスイッチ スタックには、PBR 用として最大 512 個のアクセス コントロール エントリ（ACE）を定義できます。
- ルート マップに一致基準を設定する場合は、次の注意事項に従ってください。
  - ローカル アドレス宛てのパケットを許可する ACL と照合させないでください。 PBR がこれらのパケットを転送するため、ping または Telnet の失敗やルート プロトコルのフラッピングを発生させる可能性があります。
- VRF と PBR は、スイッチ インターフェイス上で相互に排他的です。 PBR がインターフェイスでイネーブルになっているときは、VRF をイネーブルにはできません。 その反対の場合も同じで、VRF がインターフェイスでイネーブルになっているときは、PBR をイネーブルにできません。
- PBR で使用されるハードウェア エントリ数は、ルート マップ自体、使用される ACL、ACL およびルート マップ エントリの順序によって異なります。
- TOS、DSCP、および IP Precedence に基づく PBR はサポートされません。
- set interface、set default next-hop、および set default interface はサポートされません。
- set アクションのないポリシー マップはサポートされます。 一致パケットは通常どおりにルーティングされます。
- match 句のないポリシー マップはサポートされます。 set アクションはすべてのパケットに適用されます。

デフォルトでは、PBR はスイッチ上でディセーブルです。 PBR をイネーブルにするには、一致基準および結果アクションを指定するルートマップを作成する必要があります。 次に、特定のインターフェイスでそのルート マップ用の PBR をイネーブルにします。 指定したインターフェイスに着信したパケットのうち、match 句と一致したものはすべて PBR の対象になります。

スイッチで生成されたパケットまたはローカルパケットは、通常どおりにポリシールーティングされません。 スイッチ上でローカルPBRをグローバルにイネーブルにすると、そのスイッチから送信されたすべてのパケットがローカル PBR の影響を受けます。 ローカル PBR は、デフォルトでディセーブルに設定されています。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map***map-tag* [**permit**] [*sequence number*] 例： `Switch(config)# route-map pbr-map permit`	パケットの出力場所を制御するために使用するルート マップを定義し、ルートマップ コンフィギュレーションモードを開始します。 • *map-tag*：ルート マップ用のわかりやすい名前を指定します。 **ip policy route-map** インターフェイス コンフィギュレーション コマンドはこの名前を使用して、このルートマップを参照します。 同じ map-tag がある複数の route-map 文は、1 つの route-map を定義します。 • （任意）**permit** が指定され、このルートマップの一致条件が満たされている場合は、set アクションの制御に従ってルートがポリシー ルーティングされます。 • *sequence number*（任意）：特定のルートマップで route-map ステートメントの位置を示す番号です。
ステップ 3	**match ip address** {*access-list-number* | *access-list-name*} [*access-list-number* |...*access-list-name*] 例： `Switch(config-route-map)# match ip address 110 140`	1 つまたは複数の標準または拡張アクセス リストで許可されている送信元および宛先 IP アドレスを照合します。 ACL は、複数の送信元および宛先 IP アドレス以外でも照合できます。 **match** コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。
ステップ 4	**match length min max** 例： `Switch(config-route-map)# match length 64 1500`	パケット長と照合します。
ステップ 5	**set ip next-hop***ip-address* [...*ip-address*] 例： `Switch(config-route-map)# set ip next-hop 10.1.6.2`	基準と一致するパケットの動作を指定します。 パケットのルーティング先となるネクストホップを設定します（ネクストホップは隣接している必要があります）。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Switch(config-route-map)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 8	**ip policy route-map***map-tag* 例： `Switch(config-if)# ip policy route-map pbr-map`	レイヤ 3 インターフェイス上で PBR をイネーブルにし、使用するルート マップを識別します。 1 つのインターフェイスに設定できるルート マップは、1 つだけです。 ただし、異なるシーケンス番号を持つ複数のルート マップ エントリを設定できます。これらのエントリは、最初の一致が見つかるまで、シーケンス番号順に評価されます。 一致が見つからない場合、パケットは通常どおりにルーティングされます。
ステップ 9	**ip route-cache policy** 例： `Switch(config-if)# ip route-cache policy`	（任意）PBR の高速スイッチングをイネーブルにします。 PBR の高速スイッチングをイネーブルにするには、まず PBR をイネーブルにする必要があります。
ステップ 10	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**ip local policy route-map***map-tag* 例： `Switch(config)# ip local policy route-map local-pbr`	（任意）ローカル PBR をイネーブルにして、スイッチから送信されるパケットに PBR を実行します。 ローカル PBR は、スイッチによって生成されるパケットに適用されます。着信パケットには適用されません。
ステップ 12	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show route-map** [*map-name*] 例： `Switch# show route-map`	（任意）設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ 14	**show ip policy** 例： `Switch# show ip policy`	（任意）インターフェイスに付加されたポリシー ルート マップを表示します。

	コマンドまたはアクション	目的
ステップ 15	**show ip local policy** 例： `Switch# show ip local policy`	（任意）ローカル PBR がイネーブルであるかどうか、およびイネーブルである場合は使用されているルート マップを表示します。

ルーティング情報のフィルタリング

ルーティング プロトコル情報をフィルタリングする場合は、以下の作業を実行します。

（注） OSPF プロセス間でルートが再配信される場合、OSPF メトリックは保持されません。

受動インターフェイスの設定

ローカル ネットワーク上の他のルータが動的にルートを取得しないようにするには、**passive-interface** ルータ コンフィギュレーション コマンドを使用し、ルーティング アップデート メッセージがルータ インターフェイスから送信されないようにします。 OSPF プロトコルでこのコマンドを使用すると、パッシブに指定したインターフェイス アドレスが OSPF ドメインのスタブ ネットワークとして表示されます。 OSPF ルーティング情報は、指定されたルータ インターフェイスから送受信されません。

多数のインターフェイスが存在するネットワークで、インターフェイスを手動でパッシブに設定する作業を回避するには、**passive-interface default** ルータ コンフィギュレーション コマンドを使用し、すべてのインターフェイスをデフォルトでパッシブになるように設定します。このあとで、隣接関係が必要なインターフェイスを手動で設定します。

パッシブとしてイネーブルにしたインターフェイスを確認するには、**show ip ospf interface** などのネットワーク モニタリング用特権 EXEC コマンドを使用します。アクティブとしてイネーブルにしたインターフェイスを確認するには、**show ip interface** 特権 EXEC コマンドを使用します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**router** {**rip** | **ospf** | **eigrp**} 例： `Switch(config)# router ospf`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**passive-interface***interface-id* 例： `Switch(config-router)# passive-interface gigabitethernet 1/0/1`	指定されたレイヤ 3 インターフェイス経由のルーティング アップデートの送信を抑制します。
ステップ 4	**passive-interface default** 例： `Switch(config-router)# passive-interface default`	（任意）すべてのインターフェイスを、デフォルトでパッシブとなるように設定します。
ステップ 5	**no passive-interface***interface type* 例： `Switch(config-router)# no passive-interface gigabitethernet1/0/3 gigabitethernet 1/0/5`	（任意）隣接関係を送信する必要があるインターフェイスだけをアクティブにします。
ステップ 6	**network***network-address* 例： `Switch(config-router)# network 10.1.1.1`	（任意）ルーティング プロセス用のネットワークリストを指定します。 *network-address* は IP アドレスです。
ステップ 7	**end** 例： `Switch(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング アップデートのアドバタイズおよび処理の制御

アクセス コントロール リストと **distribute-list** ルータ コンフィギュレーション コマンドを組み合わせて使用すると、ルーティング アップデート中にルートのアドバタイズを抑制し、他のルータ

が 1 つまたは複数のルートを取得しないようにできます。 この機能を OSPF で使用した場合は外部ルートにだけ適用されるため、インターフェイス名を指定できません。

distribute-list ルータ コンフィギュレーション コマンドを使用し、着信したアップデートのリストのうち特定のルートを処理しないようにすることもできます。 （OSPF にこの機能は適用されません）。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**rip** | **eigrp**} 例： `Switch(config)# router eigrp 10`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**distribute-list** {*access-list-number* | *access-list-name*} **out** [*interface-name* | *routing process* | *autonomous-system-number*] 例： `Switch(config-router)# distribute 120 out gigabitethernet 1/0/7`	アクセス リスト内のアクションに応じて、ルーティング アップデート内のルートのアドバタイズを許可または拒否します。
ステップ 4	**distribute-list** {*access-list-number* | *access-list-name*} **in** [*type-number*] 例： `Switch(config-router)# distribute-list 125 in`	アップデートにリストされたルートの処理を抑制します。
ステップ 5	**end** 例： `Switch(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング情報の送信元のフィルタリング

一部のルーティング情報が他の情報よりも正確な場合があるため、フィルタリングを使用して、さまざまな送信元から送られる情報にプライオリティを設定できます。「アドミニストレーティブ ディスタンス」は、ルータやルータのグループなど、ルーティング情報の送信元の信頼性を示す数値です。大規模ネットワークでは、他のルーティングプロトコルよりも信頼できるルーティング プロトコルが存在する場合があります。アドミニストレーティブ ディスタンスの値を指定すると、ルータはルーティング情報の送信元をインテリジェントに区別できるようになります。常にルーティングプロトコルのアドミニストレーティブディスタンスが最短（値が最小）であるルートが選択されます。

各ネットワークには独自の要件があるため、アドミニストレーティブ ディスタンスを割り当てる一般的な注意事項はありません。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router** {**rip** | **ospf** | **eigrp**} 例： `Switch(config)# router eigrp 10`	ルータ コンフィギュレーション モードを開始します。
ステップ 3	**distance***weight*{*ip-address* {*ip-address mask*}} [*ip access list*] 例： `Switch(config-router)# distance 50 10.1.5.1`	アドミニストレーティブ ディスタンスを定義します。 *weight*：アドミニストレーティブディスタンスは10～255の整数です。単独で使用した場合、*weight*はデフォルトのアドミニストレーティブディスタンスを指定します。ルーティング情報の送信元に他の指定がない場合に使用されます。アドミニストレーティブディスタンスが255のルートはルーティング テーブルに格納されません。 （任意）*ip access list*：着信ルーティング アップデートに適用される IP 標準または IP 拡張アクセス リストです。
ステップ 4	**end** 例： `Switch(config-router)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show ip protocols** 例： `Switch# show ip protocols`	指定されたルーティングプロセス用のデフォルトのアドミニストレーティブ ディスタンスを表示します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

認証キーの管理

キー管理を使用すると、ルーティングプロトコルで使用される認証キーを制御できます。 一部のプロトコルでは、キー管理を使用できません。 認証キーはEIGRPおよびRIPバージョン2で使用できます。

前提条件

認証キーを管理する前に、認証をイネーブルにする必要があります。 プロトコルに対して認証をイネーブルにする方法については、該当するプロトコルについての説明を参照してください。 認証キーを管理するには、キー チェーンを定義してそのキー チェーンに属するキーを識別し、各キーの有効期間を指定します。 各キーには、ローカルにストアされる独自のキーID（**key** *number* キー チェーン コンフィギュレーション コマンドで指定）があります。 キーID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよびMessage Digest 5（MD5）認証キーが一意に識別されます。

認証キーの設定方法

有効期間が指定された複数のキーを設定できます。 存在する有効なキーの数にかかわらず、送信される認証パケットは1つだけです。 最小の番号から順にキー番号が調べられ、最初に見つかった有効なキーが使用されます。 キー変更中は、有効期間が重なっても問題ありません。 これらの有効期間は、ルータに通知する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**key chain***name-of-chain* 例： `Switch(config)# key chain key10`	キー チェーンを識別し、キーチェーン コンフィギュレーション モードを開始します。
ステップ 3	**key***number* 例： `Switch(config-keychain)# key 2000`	キー番号を識別します。 指定できる範囲は0～2147483647です。
ステップ 4	**key-string***text* 例： `Switch(config-keychain)# Room 20, 10th floor`	キー ストリングを確認します。 ストリングには 1 ～ 80 文字の大文字および小文字の英数字を指定できますが、最初の文字に数字を指定できません。
ステップ 5	**accept-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*} 例： `Switch(config-keychain)# accept-lifetime 12:30:00 Jan 25 1009 infinite`	（任意）キーを受信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。 デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。 デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 6	**send-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*} 例： `Switch(config-keychain)# accept-lifetime 23:30:00 Jan 25 1019 infinite`	（任意）キーを送信できる期間を指定します。 *start-time* および *end-time* 構文には、*hh:mm:ss Month date year* または *hh:mm:ss date Month year* のいずれかを使用できます。 デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。 デフォルトの *end-time* および **duration** は **infinite** です。
ステップ 7	**end** 例： `Switch(config-keychain)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show key chain** 例： `Switch# show key chain`	認証キーの情報を表示します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

IP ネットワークのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。 特定の統計情報を表示することもできます。

表 *98*：*IP* ルートの削除またはルート ステータスの表示を行うコマンド

show ip route [*address* [*mask*] [**longer-prefixes**]]	ルーティング テーブルの現在の状態を表示します。
show ip route summary	サマリー形式でルーティングテーブルの現在のステータスを表示します。
show platform ip unicast	プラットフォームに依存する IP ユニキャストの情報を表示します。

第 35 章

フォールバック ブリッジングの設定

- 機能情報の確認，1047 ページ
- フォールバック ブリッジングの制約事項，1047 ページ
- フォールバック ブリッジングに関する情報，1048 ページ
- フォールバック ブリッジングの設定方法，1050 ページ
- フォールバック ブリッジングのデフォルト設定，1063 ページ

機能情報の確認

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

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

フォールバック ブリッジングの制約事項

- スイッチには、最大 32 個のブリッジ グループを設定できます。
- 1 つのインターフェイス（SVI またはルーテッド ポート）が所属できるブリッジ グループは 1 つだけです。
- スイッチに接続されている個別のブリッジドネットワーク（トポロジの上で区別されるネットワーク）ごとに、1 つのブリッジ グループを使用してください。
- フォールバック ブリッジングをプライベート VLAN が設定されたスイッチに設定しないでください。

- IP（バージョン4とバージョン6）、アドレス解決プロトコル（ARP）、逆ARP（RARP）、LOOPBACK、フレームリレーARP、共有STPパケットを除くすべてのプロトコルは、フォールバック ブリッジングされます。

（注） フォールバック ブリッジングをサポートするのは、Cisco Catalyst 3560-CX スイッチのみです。

フォールバック ブリッジング CCP は IP Services ライセンスを実行している Catalyst スイッチでのみサポートされます。

関連トピック

VLAN ブリッジ スパニング ツリーのプライオリティの変更, （1052 ページ）

インターフェイスのプライオリティの変更, （1054 ページ）

パス コストの割り当て, （1055 ページ）

hello BPDU 間のインターバルの調整, （1057 ページ）

転送遅延時間の変更, （1059 ページ）

最大アイドル時間の変更, （1060 ページ）

フォールバック ブリッジングに関する情報

フォールバック ブリッジングの概要

フォールバック ブリッジングを使用すると、スイッチは複数の VLAN またはルーテッド ポート（特に1つのブリッジ ドメイン内で複数のVLANに接続されているVLANまたはルーテッド ポート）をまとめてブリッジングできます。フォールバックブリッジングを行うと、スイッチでルーティングおよび転送されないトラフィックや、DECnetなどのルーティングできないプロトコルに属するトラフィックが転送されます。VLANブリッジ ドメインは、スイッチ仮想インターフェイス（SVI）によって表されます。 （VLAN が関連付けられていない）一連の SVI およびルーテッド ポートは、ブリッジ グループを形成するように設定（グループ化）できます。SVIはスイッチポートのVLANを、ブリッジ グループを形成するように設定（グループ化）できるルーティング ポート（VLAN が関連付けられていない）へのインターフェイスの 1 つとして表します。 SVI はスイッチ ポートの VLAN を、システム内のルーティング機能またはブリッジング機能へのインターフェイスの 1 つとして表します。 1 つの VLAN に関連付けることができる SVI は 1 つだけです。VLAN 間のルーティング、VLAN 間でルーティングできないプロトコルのフォールバック ブリッジング、またはスイッチと IP ホストの接続を実現する場合にだけ、VLAN に SVI を設定してください。ルーテッドポートはルータ上のポートと同様に機能する物理ポートですが、ルータには接続されていません。 ルーテッド ポートは特定の VLAN と関連付けられておらず、VLAN サブインターフェイスをサポートしていませんが、通常のルーテッド ポートのように動作します。

ブリッジ グループは、スイッチ上のネットワーク インターフェイスの内部構造です。 ブリッジ グループが定義されているスイッチの外側にあるブリッジ グループ内では、スイッチングされるトラフィックを識別する目的でのブリッジ グループの使用はできません。 同じスイッチ上のブ

リッジグループは、異なるブリッジとして機能します。つまり、スイッチ上の異なるブリッジグループ間で、ブリッジドトラフィックおよびブリッジプロトコルデータユニット（BPDU）は交換されません。

フォールバックブリッジングを使用しても、ブリッジングされているVLANのスパニングツリーは縮小できません。 各 VLAN には、独自のスパニングツリー インスタンスと、ループを防止するためにブリッジ グループの一番上で動作する個別のスパニングツリー（別名 VLAN ブリッジ スパニングツリー）があります。

ブリッジ グループが作成されると、スイッチは VLAN ブリッジ スパニングツリー インスタンスを作成します。 スイッチはブリッジ グループを実行し、ブリッジ グループ内の SVI およびルーテッド ポートをスパニングツリー ポートとして処理します。

ネットワーク インターフェイスをブリッジ グループに格納する理由は、次のとおりです。

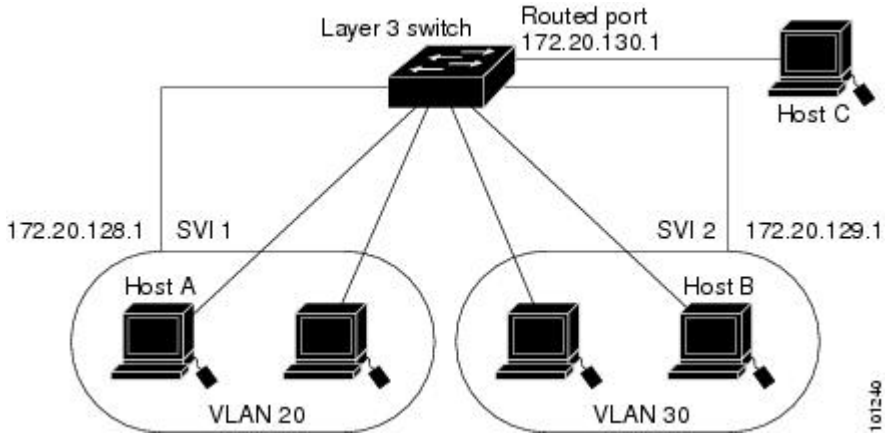
- ブリッジ グループを構成するネットワーク インターフェイス間でルーティングされない全トラフィックをブリッジングするため。 宛先アドレスがブリッジ テーブルに格納されているパケットは、ブリッジ グループ内の単一のインターフェイス上で転送されます。 宛先アドレスがブリッジ テーブル内に格納されていないパケットは、ブリッジ グループ内のすべての転送インターフェイス上でフラッディングされます。 ブリッジ グループで送信元 MAC アドレスが学習されるのは、このアドレスがVLAN上で学習された場合だけです（この逆は成り立ちません）。 スタック メンバで学習されたアドレスは、スタック内のすべてのスイッチで学習されます。
- 接続されている LAN 上で BPDU を受信（場合によっては送信）することにより、スパニングツリー アルゴリズムに参加するため。 設定されたブリッジ グループごとに、個別のスパニングツリー プロセスが動作します。 各ブリッジ グループは個別のスパニングツリー インスタンスに参加します。 ブリッジ グループは、メンバー インターフェイスだけが受信するBPDUに基づいて、スパニングツリーインスタンスを確立します。 VLANがブリッジグループに属していないポートに着信したブリッジ STP BPDU は、VLAN のすべての転送ポートでフラッディングされます。

例：フォールバック ブリッジング ネットワーク

次の図に、フォールバック ブリッジング ネットワークの例を示します。 このスイッチには、SVI として 2 つのポートが設定されています。これらの SVI は異なる IP アドレスを持ち、2 つの異なる VLAN に接続されています。 さらに、もう 1 つのポートが独自の IP アドレスを持つルーテッド ポートとして設定されています。 これらの 3 つのポートがすべて同じブリッジ グループに割り当てられている場合は、これらのポートが異なるネットワークや異なる VLAN にあっても、スイッチに接続されているエンド ステーション間で非 IP プロトコル フレームを転送できます。

フォールバック ブリッジングを機能させるために IP アドレスをルーテッド ポートや SVI に割り当てる必要はありません。

図 *77*：フォールバック ブリッジング ネットワークの例



フォールバック ブリッジングの設定方法

ブリッジ グループの作成

一連の SVI またはルーテッド ポートにフォールバック ブリッジングを設定する場合は、これらのインターフェイスをブリッジ グループに割り当てる必要があります。 同じグループ内のすべてのインターフェイスは、同じブリッジ ドメインに属します。 各 SVI またはルーテッド ポートは、1 つのブリッジ グループだけに割り当てることができます。

（注） 保護ポート機能とフォールバック ブリッジングとの併用はできません。 フォールバック ブリッジングがイネーブルである場合、ある保護ポートから、別の VLAN 内にある同じスイッチ上の別の保護ポートにパケットが転送される可能性があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **bridge***bridge-group***priority***number*
4. **interface***interface -id*
5. **bridge-group***bridge-group*
6. **show running-config**
7. **copy running-config startup-config**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bridge***bridge-group***priority***number* 例： `Switch(config)# bridge 10 protocol vlan-bridge`	ブリッジ グループ番号を割り当て、ブリッジ グループで実行する VLAN ブリッジ スパニングツリー プロトコルを指定します。 **ibm** および **dec** キーワードはサポートされていません。 bridge-group には、ブリッジ グループ番号を指定します。 指定できる範囲は 1 ～ 255 です。 最大 32 個のブリッジ グループを作成できます。 フレームは同じグループ内のインターフェイス間でだけブリッジングされます。
ステップ 4	**interface***interface -id* 例： `Switch(config)# interface gigabitethernet3/0/1`	ブリッジ グループを割り当てるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：no switchport インターフェイス コンフィギュレーション コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。 • SVI：**interface vlan***vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 （注） ルーテッド ポートや SVI に IP アドレスを割り当てることができますが、これは必須ではありません。
ステップ 5	**bridge-group***bridge-group* 例： `Switch(config)# bridge-group 10`	ブリッジ グループ番号を割り当て、ブリッジ グループで実行する VLAN ブリッジ スパニングツリー プロトコルを指定します。 **ibm** および **dec** キーワードはサポートされていません。 bridge-group には、ブリッジ グループ番号を指定します。 指定できる範囲は 1 ～ 255 です。 最大 32 個のブリッジ グループを作成できます。 フレームは同じグループ内のインターフェイス間でだけブリッジングされます。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 8	**end**	特権 EXEC モードに戻ります。

スパニングツリー パラメータの調整

特定のスパニングツリー パラメータのデフォルト値が不適切な場合は、このパラメータを調整する必要があります。 スパニングツリー全体に影響するパラメータを設定する場合は、さまざまなタイプの bridge グローバル コンフィギュレーション コマンドを使用します。 インターフェイス固有のパラメータを設定する場合は、さまざまなタイプの bridge-group インターフェイス コンフィギュレーション コマンドを使用します。

（注） スパニングツリーパラメータの調整は、スイッチおよびSTPの機能に精通しているネットワーク管理者だけが行ってください。 計画が不十分なまま調整を行うと、パフォーマンスの低下を招くことがあります。 スイッチングに関する資料としては、IEEE 802.1D 仕様が適しています。

VLAN ブリッジ スパニング ツリーのプライオリティの変更

ルート スイッチの候補として別のスイッチと同等のレベルにあるスイッチには、VLAN ブリッジ スパニングツリーのプライオリティをグローバルに設定できます。 このスイッチがルート スイッチとして選択される可能性を設定することもできます。 スイッチのプライオリティを変更するには、次の手順を実行します。 この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **bridge***bridge-group***priority***number*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**bridge***bridge-group***priority***number* 例： `Switch(config)# bridge 10 priority 100`	Switchの VLAN ブリッジスパニングツリープライオリティを変更します。 • bridge-group には、ブリッジグループ番号を指定します。 指定できる範囲は 1 ～ 255 です。 • number には、0 ～ 65535 の数字を入力します。 デフォルトは 32768 です。 この値が低いほど、Switchがルートとして選択される可能性が高くなります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config`	（任意）コンフィギュレーションファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

関連トピック

フォールバック ブリッジングの制約事項, （1047 ページ）

フォールバック ブリッジングのデフォルト設定, （1063 ページ）

インターフェイスのプライオリティの変更

ポートのプライオリティを変更できます。 2 つのスイッチがルート スイッチの候補として同等のレベルにある場合は、レベルに差が付くようにポート プライオリティを設定します。 インターフェイスのプライオリティ値が低いスイッチが選択されます。 インターフェイスのプライオリティを変更するには、次の手順を実行します。 この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **bridge-group***bridge-group***priority***number*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
	例： `Switch(config)# interface gigabitethernet2/0/1`	
ステップ 4	**bridge-group***bridge-group***priority***number* 例： `Switch(config)# bridge-group 10 priority 20`	スイッチの VLAN ブリッジ スパニングツリー プライオリティを変更します。 • bridge-group には、ブリッジ グループ番号を指定します。 指定できる範囲は 1 ～ 255 です。 • number には、0 ～ 255 の値を入力します（増分値は 4）。 この値が低いほど、スイッチのポートがルートとして選択される可能性が高くなります。 デフォルト値は 128 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

フォールバック ブリッジングの制約事項, （1047 ページ）

フォールバック ブリッジングのデフォルト設定, （1063 ページ）

パス コストの割り当て

各ポートにはパス コストが割り当てられています。 規定では、パス コストは 1000/（接続された LAN のデータ速度）の値を Mbps 単位で表したものです。 パス コストを割り当てるには、次の手順を実行します。 この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **bridge-group***bridge-group***path cost***cost*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	
ステップ 4	**bridge-group***bridge-group***path cost***cost* 例： `Switch(config)# bridge-group 10 path-cost 20`	ポートのパス コストを割り当てます。 • bridge-group には、ブリッジ グループ番号を指定します。 指定できる範囲は 1 ～ 255 です。 • cost には、0 ～ 65535 の数字を入力します。 値が大きいほど、コストは大きくなります。 • 10 Mb/s の場合、デフォルトのパス コストは 100 です。 • 100 Mb/s の場合、デフォルトのパス コストは 19 です。 • 1000 Mb/s の場合、デフォルトのパス コストは 4 です。

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

関連トピック

フォールバック ブリッジングの制約事項, （1047 ページ）

フォールバック ブリッジングのデフォルト設定, （1063 ページ）

BPDU 間隔の調整

hello BPDU 間のインターバルの調整

スパニングツリーの各スイッチには、個々の設定に関係なく、ルートスイッチの hello BPDU インターバル、転送遅延時間、および最大アイドル時間パラメータが採用されています。

hello BPDU 間のインターバルを調整するには、次の手順を実行します。 この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **bridge***bridge-group***hello-time***seconds*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bridge***bridge-group***hello-time***seconds* 例： `Switch(config)# bridge 10 hello-time 5`	hello BPDU 間のインターバルを指定します。 • bridge-group には、ブリッジ グループ番号を指定します。 指定できる範囲は 1 ～ 255 です。 • seconds には、1 ～ 10 の数字を入力します。 デフォルトは 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

フォールバック ブリッジングの制約事項, （1047 ページ）

フォールバック ブリッジングのデフォルト設定, （1063 ページ）

転送遅延時間の変更

転送遅延時間は、ポートでスイッチングがアクティブになってから実際に転送を開始するまでの時間です。この間にトポロジ変更情報の受信が行われます。

転送遅延時間を変更するには、次の手順を実行します。 この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **bridge***bridge-group***forward-time***seconds*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bridge***bridge-group***forward-time***seconds* 例： `Switch(config)# bridge 10 forward-time 10`	転送時間の間隔を指定します。 • bridge-group には、ブリッジ グループ番号を指定します。 指定できる範囲は 1 ～ 255 です。 • seconds には、4 ～ 200 の数字を入力します。 デフォルトは 20 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。

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

関連トピック

フォールバック ブリッジングの制約事項，（1047 ページ）

フォールバック ブリッジングのデフォルト設定，（1063 ページ）

最大アイドル時間の変更

指定時間内にルートスイッチからBPDUが受信されない場合は、スイッチはスパニングツリートポロジを再計算します。

最大アイドル時間（最大エージングタイム）を変更するには、次の手順を実行します。この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **bridge***bridge-group***max-age***seconds*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bridge***bridge-group***max-age***seconds* 例： `Switch(config)# bridge 10 max-age 30`	ルート スイッチから BPDU をヒアリングするためにスイッチが待機する時間を指定します。 • bridge-group には、ブリッジ グループ番号を指定します。 指定できる範囲は 1 ～ 255 です。 • seconds には、6 ～ 200 の数字を入力します。 デフォルトは 30 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

フォールバック ブリッジングの制約事項, （1047 ページ）

フォールバック ブリッジングのデフォルト設定, （1063 ページ）

インターフェイスでのスパニング ツリーのディセーブル化

2 つの任意のスイッチング サブネットワーク間にループのないパスが存在する場合は、一方のスイッチング サブネットワークで生成された BPDU の影響が他方のサブネットワーク内のデバイスに及ばないようにできます（ただし、ネットワーク全体に及ぶスイッチングは可能です）。 たとえば、スイッチング LAN サブネットワークが WAN によって分離されている場合は、BPDU の WAN リンク間移動を禁止できます。

ポート上でスパニングツリーをディセーブルにするには、次の手順を実行します。この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **bridge-group***bridge-group***priority***spanning-disabled*
5. **show running-config**
6. **copy running-config startup-config**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	
ステップ 4	**bridge-group***bridge-group***priority***spanning-disabled* 例： `Switch(config)# bridge group 10 spanning-disabled`	ポート上でスパニングツリーをディセーブルにします。 bridge-group には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

フォールバック ブリッジングのモニタリングおよびメンテナンス

表 *99*：フォールバック ブリッジングのモニタリングおよびメンテナンスのコマンド

コマンド	目的
clear bridge*bridge-group*	学習したエントリを転送データベースから削除します。
show bridge*[bridge-group]* **group**	ブリッジ グループの詳細を表示します。
show bridge*[bridge-group] interface-id\mac -address***verbose**	ブリッジ グループ内で学習した MAC アドレスを表示します。

フォールバック ブリッジングのデフォルト設定

表 *100*：フォールバック ブリッジングのデフォルト設定

機能	デフォルト設定
ブリッジ グループ	未定義であるか、またはポートに割り当てられていません。 VLAN ブリッジ STP は定義されていません。
動的に学習されたステーションに対するスイッチからのフレーム転送	イネーブル
スイッチ プライオリティ	32768
ポート プライオリティ	128

機能	デフォルト設定
ポート パス コスト	• 10 Mb/s：100 • 100 Mb/s：19 • 1000 Mb/s：4
hello BPDU インターバル	2 秒
転送遅延時間	20 秒
最大アイドル時間	30 秒

関連トピック

VLAN ブリッジ スパニング ツリーのプライオリティの変更, （1052 ページ）
インターフェイスのプライオリティの変更, （1054 ページ）
パス コストの割り当て, （1055 ページ）
hello BPDU 間のインターバルの調整, （1057 ページ）
転送遅延時間の変更, （1059 ページ）
最大アイドル時間の変更, （1060 ページ）

第 VIII 部

マルチキャスト ルーティング

- IP マルチキャスト ルーティング テクノロジーの概要，1067 ページ
- IGMP の設定，1075 ページ
- CGMP の設定，1099 ページ
- PIM の設定，1105 ページ
- HSRP 認識 PIM の設定，1171 ページ
- VRRP 認識 PIM の設定，1179 ページ
- 基本的な IP マルチキャスト ルーティングの設定，1185 ページ
- SSM の設定，1199 ページ
- IGMP スヌーピングおよびマルチキャスト VLAN レジストレーションの設定，1227 ページ
- MSDP の設定，1283 ページ

第 36 章

IP マルチキャスト ルーティング テクノロジーの概要

- 機能情報の確認，1067 ページ
- IP マルチキャスト テクノロジーに関する情報，1067 ページ

機能情報の確認

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

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

IP マルチキャスト テクノロジーに関する情報

情報配信における IP マルチキャストの役割

IP マルチキャストは、単一の情報ストリームを何千もの潜在的な企業および家庭に同時に配信することによってトラフィックを削減する帯域幅節約テクノロジーです。 マルチキャストを利用するアプリケーションには、ビデオ会議、企業コミュニケーション、通信教育、およびソフトウェア、株価情報、ニュースの配信などが含まれます。

IP マルチキャスト ルーティングにより、ホスト（ソース）は、IP マルチキャスト グループ アドレスと呼ばれる特別な形式の IP アドレスを使用して、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。 ソースのホストは、マルチキャスト グループ アド

レスをパケットの宛先 IP アドレス フィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、受信した IP マルチキャスト パケットを、マルチキャスト グループのメンバにつながるすべてのインターフェイスから転送します。 どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。 ただし、グループのメンバだけがメッセージを受信します。

IP マルチキャスト ルーティング プロトコル

ソフトウェアでは、IP マルチキャスト ルーティングを実装するため、次のプロトコルがサポートされています。

- IGMP を LNA 上のホストとその LAN上のルータ間で使用して、ホストがメンバになっているマルチキャスト グループを追跡します。
- プロトコル独立マルチキャスト（PIM）は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにルータ間で使用されます。

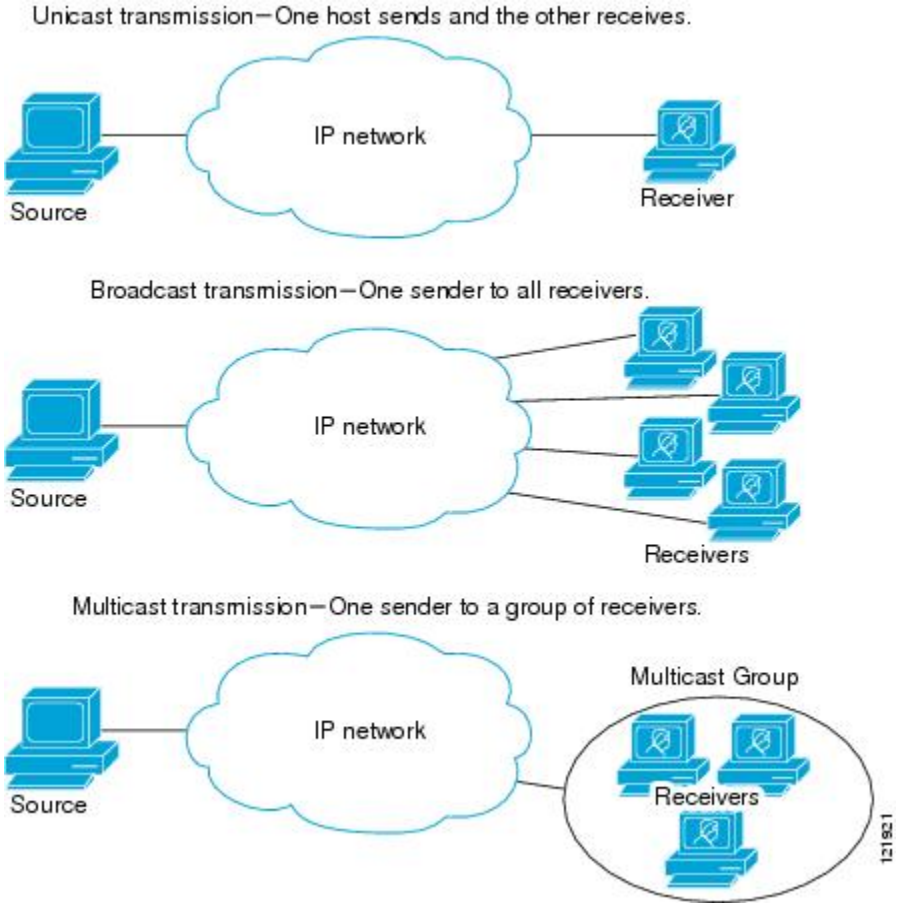
次の図に、これらのプロトコルが IP マルチキャスト環境内のどの部分で動作するかを示します。

マルチキャスト グループ伝送方式

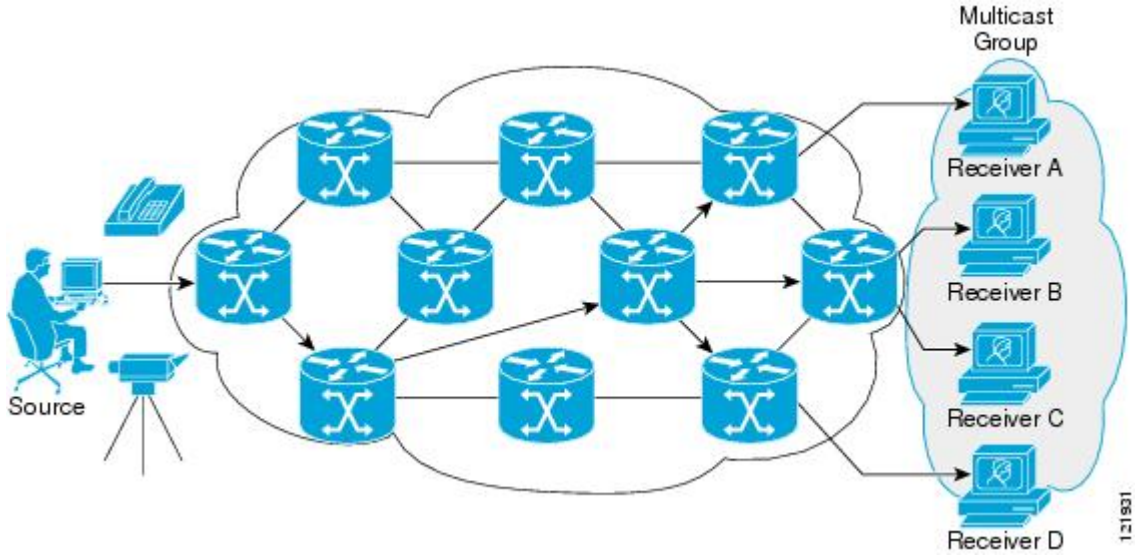
IP 通信は、最初の図に示すように、トラフィックの送信者として機能するホストと、レシーバとして機能するホストで構成されます。 送信者はソースと呼ばれます。 従来の IP 通信は、単一のホスト ソースがパケットを別の単一ホスト（ユニキャスト伝送）またはすべてのホスト（ブロードキャスト伝送）に送信することによって行われます。 IP マルチキャストは第三の方式を提供するものであり、ホストはすべてのホストのサブセットにパケットを送信できます（マルチキャスト伝送）。受信側のホストのこのサブセットをマルチキャスト グループと呼びます。 マルチキャスト グループに属するホストは、グループ メンバと呼ばれます。

マルチキャストは、このグループの概念に基づいています。 マルチキャスト グループは、特定のデータ ストリームを受信するためにグループに加入する任意の数のレシーバです。 このマルチキャスト グループには、物理的境界または地理的境界はありません。ホストは、インターネット上または任意のプライベート ネットワーク上のどこにでも配置できます。 ソースから特定のグループに対するデータを受信する必要があるホストはそのグループに加入する必要があります。 グループに加入するには、ホスト レシーバで Internet Group Management Protocol（IGMP）を使用します。

マルチキャスト環境では、どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。 ただし、そのグループに送信されたパケットはグループのメンバだけが受信できます。 IP ユニキャスト パケットと同様、マルチキャスト パケットは、ベストエフォート型の信頼性を使用してグループに配信されます。



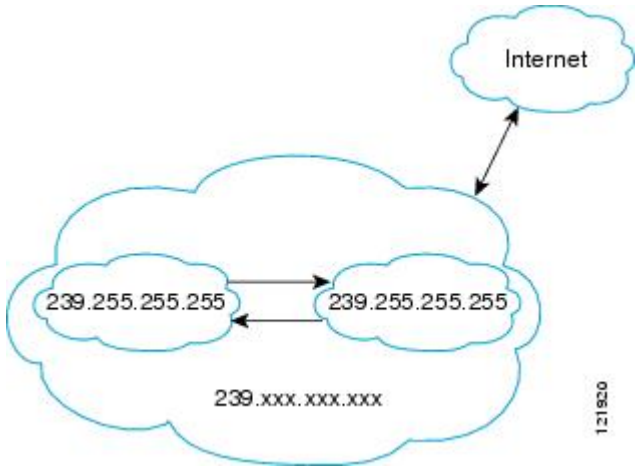
次の図では、レシーバ（指定したマルチキャスト グループ）がソースからのビデオ データ ストリームを受信する必要があります。 これらのレシーバは、ネットワーク内のルータに IGMP ホスト レポートを送信することによってその意思を示します。 この場合、ルータがソースからレシーバへのデータの配信を担います。 ルータは、Protocol Independent Multicast（PIM）を使用して、マルチキャスト配信ツリーを動的に作成します。 その後、ソースとレシーバ間のパスにあるネットワーク セグメントにのみ、ビデオ データ ストリームが配信されます。



IP マルチキャスト境界

図に示すように、アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界を定義します。 スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

図 *78* : 境界でのアドレス スコーピング



マルチキャスト グループ アドレッシングのインターフェイスに管理スコープの境界を設定するには、**ipmulticastboundary** コマンドと *access-list* 引数を使用します。 影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。 境界が設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。 境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

Internet Assigned Numbers Authority（IANA）は、マルチキャスト アドレス範囲 239.0.0.0 ～ 239.255.255.255 を管理スコープ アドレスとして指定しています。 この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。 これらは、グローバルに一意ではなくローカルとみなされます。

filter-autorp キーワードを設定して、管理用スコープの境界で Auto-RP 検出と通知メッセージを検査し、フィルタできます。 境界のアクセス コントロール リスト（ACL）に拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。 Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。 許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。 インターフェイスに着信するすべてのマルチキャスト トラフィックをブロックし、インターフェースから送信されるマルチキャスト トラフィックを許可するには、**{ ip | ipv6 } multicast boundary block sources** を使用します。

IP マルチキャスト グループ アドレッシング

マルチキャスト グループは、マルチキャスト グループ アドレスによって識別されます。 マルチキャスト パケットは、そのマルチキャスト グループ アドレスに配信されます。 単一のホストを独自に識別するユニキャストアドレスとは異なり、マルチキャスト IP アドレスは特定のホストを識別しません。 マルチキャストアドレスに送信されるデータを受信するには、アドレスが識別するグループにホストが参加する必要があります。 データは、マルチキャスト アドレスに送信され、そのグループに送信されたトラフィックを受信する意思を示してグループに加入しているすべてのホストによって受信されます。 マルチキャスト グループ アドレスは、送信元でグループに割り当てられます。 マルチキャスト グループ アドレスを割り当てるネットワーク管理者は、Internet Assigned Numbers Authority（IANA）で予約されるマルチキャスト アドレスの範囲にアドレスが準拠していることを確認する必要があります。

IP クラス D アドレス

IP マルチキャスト アドレスは、IANA によって IPv4 クラス D アドレス空間に割り当てられました。 クラス D アドレスの上位 4 ビットは 1110 です。 したがって、ホスト グループ アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 であると考えられます。 マルチキャスト アドレスは送信元（送信者）でマルチキャスト グループの受信先として選択されます。

（注） クラス D アドレスの範囲は、IP マルチキャスト トラフィックのグループ アドレスまたは宛先アドレスにだけ使用されます。 マルチキャストデータグラムの送信元アドレスは常にユニキャスト送信元アドレスになります。

IP マルチキャスト アドレスのスコーピング

さまざまなアドレス範囲の予測可能な動作を提供したり、より小規模なドメイン内でアドレスを再利用したりできるよう、マルチキャストアドレスの範囲はさらに分割されます。 表に、マルチキャスト アドレスの範囲を要約します。 それに続いて、各範囲について簡単に説明します。

表 *101*：マルチキャスト アドレス範囲の割り当て

名前	範囲	説明
予約済みリンクローカル アドレス	224.0.0.0 ～ 224.0.0.255	ローカル ネットワーク セグメントのネットワーク プロトコルで使用するために予約されています。
グローバル スコープ アドレス	224.0.1.0 ～ 238.255.255.255	組織間およびインターネット上でマルチキャストデータを送信するために予約されています。
Source Specific Multicast	232.0.0.0 ～ 232.255.255.255	明示的にグループに参加している受信者だけにデータを転送する SSM データグラム配信モデル用に予約されています。
GLOP アドレス	233.0.0.0 ～ 233.255.255.255	割り当て済みの自律システム（AS）ドメイン番号をすでに持つ組織によって静的に定義されるアドレス用に予約されています。
限定スコープ アドレス	239.0.0.0 ～ 239.255.255.255	管理スコープ アドレスまたはプライベート マルチキャスト ドメインで使用するための限定スコープアドレスとして予約されています。

予約済みリンクローカル アドレス

IANA では、ローカル ネットワーク セグメントのネットワーク プロトコルで使用するために 224.0.0.0 ～ 224.0.0.255 の範囲を予約しています。 この範囲のアドレスを持つパケットはスコープ内ローカルであり、IP ルータによって転送されません。 通常、リンク ローカル宛先アドレスを持つパケットは存続可能時間（TTL）値 1 を使用して送信されるため、ルータによって転送されません。

この範囲内の予約済みリンクローカルアドレスは、それぞれに予約されたネットワーク プロトコル機能を提供します。 ネットワーク プロトコルは、これらのアドレスをルータの自動検出および重要なルーティング情報の伝達用に使用します。 たとえば、Open Shortest Path First（OSPF）は、IP アドレスの 224.0.0.5 と 224.0.0.6 を使用してリンクステート情報を交換します。

IANA では、ネットワーク プロトコルやネットワーク アプリケーションに対する単一マルチキャスト アドレス要求を 224.0.1.xxx のアドレス範囲外に割り当てています。 マルチキャスト ルータはこれらのマルチキャスト アドレスを転送します。

グローバル スコープ アドレス

224.0.1.0 ～ 238.255.255.255 の範囲のアドレスは、グローバル スコープ アドレスと呼ばれます。これらのアドレスは、組織間およびインターネット上でのマルチキャスト データの送信に使用します。 これらのアドレスの一部はマルチキャスト アプリケーションで使用するよう IANA によって予約されています。 たとえば、IPアドレス 224.0.1.1 は、Network Time Protocol（NTP）用に予約されています。

Source Specific Multicast アドレス

232.0.0.0/8 のアドレス範囲は、Source Specific Multicast（SSM）用に予約されています。 Cisco IOS ソフトウェアでは、**ippimssm** コマンドを使用して任意の IP マルチキャスト アドレス用の SSM も設定できます。 SSM は、1 対多通信での効率的なデータ配信メカニズムを可能にする Protocol Independent Multicast（PIM）の拡張版です。 SSM については、IP マルチキャスト配信モード, （1074 ページ）の項を参照してください。

GLOP アドレス

GLOP アドレッシングでは（233/8 の RFC 2770、GLOP アドレッシングで提案されているように）、AS 番号をすでに予約している組織による静的に定義されたアドレス用に 233.0.0.0/8 の範囲を予約することを提案しています。 これは、GLOP アドレッシングと呼ばれます。 ドメインの AS 番号は 233.0.0.0/8 アドレス範囲の 2 番目と 3 番目のオクテットに組み込まれます。 たとえば、AS 62010 は 16 進数形式で F23A と表されます。 この 2 つのオクテット F2 および 3A を分割すると、結果は 10 進数でそれぞれ 242 および 58 となります。 これらの値は、AS 62010 に使用するようにグローバルに予約される 233.242.58.0/24 のサブネットとなります。

限定スコープ アドレス

239.0.0.0 ～ 239.255.255.255 の範囲は、管理スコープ アドレス、またはプライベート マルチキャスト ドメインで使用する限定スコープ アドレスとして予約されています。 これらのアドレスは、ローカル グループまたは組織に使用するように制限されています。 会社、大学および他の組織は、限定スコープ アドレスを使用すると、ドメイン外に転送されないローカル マルチキャスト アプリケーションを使用できます。 通常、ルータは、このアドレス範囲のマルチキャスト トラフィックが自律システム（AS）またはユーザ定義のドメイン外にフローしないようにするフィルタを使用して設定されます。 AS またはドメイン内では、ローカル マルチキャスト境界を定義できるように、限定スコープ アドレス範囲を細分化することもできます。

（注） ネットワーク管理者はこの範囲内のマルチキャスト アドレスを使用できます。これによって、インターネット内の他の場所と競合することはありません。

レイヤ 2 マルチキャスト アドレス

従来、LAN セグメントのネットワーク インターフェイス カード（NIC）が受信できるのは、Burned-In MAC Address またはブロードキャスト MAC アドレスに指定されたパケットだけでした。IP マルチキャストでは、複数のホストが共通の宛先 MAC アドレスを使用した単一のデータ スト

リームを受信する必要があります。 複数のホストが同じパケットを受信する場合、複数のマルチキャスト グループを区別できるように、何らかの方法を考案する必要があります。 そのための 1 つの方法は、IP マルチキャスト クラス D アドレスを MAC アドレスに直接マッピングすることです。 この方法を使用すると、NIC は多くの異なる MAC アドレスを宛先とするパケットを受信できます。

Cisco グループ管理プロトコル（CGMP）は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたルータ上で使用されます。 IP マルチキャスト データパケットと IGMP レポート メッセージ（いずれも MAC レベルで同じグループ アドレスにアドレス指定されます）を区別できない Catalyst スイッチの場合、CGMP が必要になります。

IP マルチキャスト配信モード

IP マルチキャスト配信のモードは、送信元ホストではなく、受信側ホストのみによって異なります。 送信元ホストは、パケットの IP 送信元アドレスとしての固有の IP アドレスと、パケットの IP 宛先アドレスとしてのグループ アドレスを使用して、IP マルチキャスト パケットを送信します。

Source Specific Multicast

Source Specific Multicast（SSM）は、ブロードキャスト アプリケーションとしても知られる 1 対多アプリケーションをサポートする最善のデータグラム配信モデルです。 SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャストのコア ネットワーク テクノロジーです。

SSM 配信モードの場合、IP マルチキャスト レシーバ ホストは IGMP バージョン3（IGMPv3）を使用してチャネル（S, G）を登録する必要があります。 このチャネルに登録することによって、ソース ホストがグループ G に送信した IP マルチキャスト トラフィックの受信をレシーバ ホストが要求していることを示します。ネットワークは、ソース ホスト S からグループ G に送信された IP マルチキャスト パケットを、チャネル (S, G) に登録したネットワーク内のすべてのホストに配信します。

SSM では、ネットワーク内でグループ アドレスを割り当てる必要はありません。各ソース ホスト内で割り当てるだけです。 同じソースホストで実行している各アプリケーションはそれぞれ異なる SSM グループを使用する必要があります。 異なるソース ホストで実行しているアプリケーションは、SSM グループアドレスを再利用できます。ネットワークに大量のトラフィックを発生させることはありません。

第 37 章

IGMP の設定

- 機能情報の確認，1075 ページ
- IGMP の前提条件，1075 ページ
- IGMP 設定の制約事項，1076 ページ
- IGMP に関する情報，1076 ページ
- IGMP の設定方法，1083 ページ
- IGMP のモニタリング，1096 ページ
- IGMP の設定例，1097 ページ

機能情報の確認

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

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

IGMP の前提条件

- このモジュールの作業を実行する前に、『IP Multicast Routing Technology Overview』モジュールで説明している概念をよく理解しておく必要があります。
- このモジュールの作業では、IP マルチキャストがイネーブルに設定され、「Configuring Multicast Routing」モジュールで説明されている作業を使用して、Protocol Independent Multicast（PIM）インターフェイスが設定されていることを前提とします。

関連トピック

グループのメンバとしてのスイッチの設定, （1083 ページ）
IGMP の加入処理, （1081 ページ）
IGMP の脱退処理, （1082 ページ）

IGMP 設定の制約事項

次に、IGMP を設定する際の制約事項を示します。

- スイッチは、IGMP バージョン 1、2、および 3 をサポートします。

（注） IGMP バージョン 3 の場合、IGMP バージョン 3 BISS（基本的な IGMPv3 スヌーピング サポート）のみがサポートされます。

- IGMP バージョン 3 では新しいメンバーシップ レポート メッセージを使用しますが、これらは以前の IGMP スヌーピング スイッチが正しく認識しない可能性があります。
- IGMPv3 は、ISM および SSM と同時に動作可能です。 ISM では、exclude と include の両方のモードのレポートを適用できます。 SSM では、ラストホップ ルータは include モードのレポートだけを受け入れます。 exclude モードのレポートは無視されます。

関連トピック

IGMP バージョン 3, （1078 ページ）

IGMP に関する情報

Internet Group Management Protocol の役割

IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。 インターフェイスで PIM をイネーブルにすると、IGMP もイネーブルになります。 IGMP は、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャスト トラフィックのフローを自動的に制御および制限する手段を提供します。

- クエリアは、クエリー メッセージを送信して、特定のマルチキャスト グループのメンバであるネットワーク デバイスを検出するネットワーク デバイス（ルータなど）です。
- ホストは、クエリアにホスト メンバーシップを通知するためのレポート メッセージ（クエリー メッセージに応答するメッセージ）を送信するレシーバで、ルータも含まれます。 ホストでは、IGMP メッセージを使用して、マルチキャスト グループに加入し、マルチキャスト グループを脱退します。

ホストは、そのローカル マルチキャスト デバイスに IGMP メッセージを送信することで、グループ メンバーシップを識別します。 IGMP では、デバイスは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

IGMP マルチキャスト アドレス

IP マルチキャスト トラフィックには、グループ アドレス（クラス D IP アドレス）が使用されます。 クラス D アドレスの上位 4 ビットは 1110 です。 したがって、ホスト グループ アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 であると考えられます。

224.0.0.0 ～ 224.0.0.255 のマルチキャスト アドレスは、ルーティング プロトコルおよびその他のネットワーク制御トラフィックが使用するために予約されています。 アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは IP マルチキャスト グループ アドレスを使用して次のように送信されます。

- IGMP 汎用クエリーは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリーは、クエリー対象デバイスのグループ IP アドレスを宛先とします。
- IGMP グループ メンバーシップ レポートは、レポート対象デバイスのグループ IP アドレスを宛先とします。
- IGMPv2 グループ脱退メッセージは、アドレス 224.0.0.2（サブネット上のすべてのデバイス）を宛先とします。
- IGMPv3 メンバーシップ レポートはアドレス 224.0.0.22 を宛先とします。すべての IGMPv3 対応マルチキャスト デバイスはこのアドレスをリッスンする必要があります。

IGMP のバージョン

スイッチは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしています。 これらのバージョンは、スイッチ上で相互運用できます。 たとえば、IGMP スヌーピングがイネーブルになっており、クエリーのバージョンが IGMPv2 で、スイッチがホストから IGMPv3 レポートを受信している場合、スイッチは IGMPv3 レポートをマルチキャスト ルータに転送できます。

IGMPv3 スイッチは、Source Specific Multicast（SSM）機能を実行しているデバイスとメッセージの送受信を行うことができます。

関連トピック

IGMP バージョンの変更, （1088 ページ）

IGMP スヌーピングの制約事項, （1228 ページ）

IGMPv1

IGMP Version 1（IGMPv1）にはクエリー応答モデルが使用されているため、マルチキャスト ルータおよびマルチレイヤ スイッチは、ローカル サブネット上のどのマルチキャスト グループがアクティブであるか（マルチキャスト グループに関係するホストが 1 台または複数存在するか）を判別できます。 IGMPv1 では別のプロセスを使用して、ホストをマルチキャスト グループに加入および脱退させることができます。 詳細については、RFC 1112 を参照してください。

IGMPv2

IGMPv2 は IGMP 機能の拡張版です。IGMP 脱退処理などの機能を提供して、脱退遅延を短縮し、グループ固有のクエリー数を削減し、明示的な最大クエリー応答時間を短縮します。 また、この作業を実行するために、マルチキャスト プロトコルに依存することなく IGMP クエリアを選択する機能もルータに追加されます。 詳細については、RFC 2236 を参照してください。

（注） IGMP バージョン 2 はスイッチのデフォルト バージョンです。

IGMP バージョン 3

スイッチは IGMP バージョン 3 をサポートしています。

IGMPv3 スイッチは、Basic IGMPv3 Snooping Support（BISS）をサポートしています。BISS は、IGMPv1 および IGMPv2 スイッチでのスヌーピング機能と、IGMPv3 メンバーシップ レポート メッセージをサポートしています。 ネットワークに IGMPv3 ホストがある場合、BISS によりマルチキャスト トラフィックのフラッディングは抑制されます。 トラフィックは、IGMPv2 または IGMPv1 ホストの IGMP スヌーピング機能の場合とほぼ同じポート セットに抑制されます。

IGMPv3 スイッチは、Source Specific Multicast（SSM）機能を実行しているデバイスとメッセージの送受信を行うことができます。

関連トピック

IGMP 設定の制約事項, （1076 ページ）

IGMPv3 ホスト シグナリング

IGMPv3 では、ホストはマルチキャスト グループのラストホップ ルータにメンバーシップ シグナルを送信します。 ホストは、グループ メンバーシップ シグナルの送信に、送信元に関するフィルタリング機能を使用できます。 ホストは、いくつかの特定の送信元を除くすべての送信元からグループへのトラフィックを受信する（exclude モード）というシグナルか、または、いくつかの特定の送信元からグループへのトラフィックだけを受信する（include モード）というシグナルを送信できます。

IGMPv3 は、インターネット標準マルチキャスト（ISM）でも、Source Specific Multicast（SSM）でも動作できます。 ISM では、exclude と include の両方のモードのレポートを適用できます。

SSM では、ラストホップ ルータは include モードのレポートだけを受け入れます。 exclude モードのレポートは無視されます。

IGMP のバージョンの違い

Internet Engineering Task Force（IETF）の Request for Comments（RFC）ドキュメントで定義されているように、IGMP には 3 種類のバージョンがあります。 IGMPv2 は IGMPv1 の強化版で、ホストがマルチキャスト グループからの脱退を通知する機能が追加されていいます。IGMPv3 は IGMPv2 の強化版で、あるソース IP アドレスのセットから送信されたマルチキャストだけをリッスンする機能が追加されています。

表 *102*：*IGMP* のバージョン

IGMP のバージョン	説明
IGMPv1	どのマルチキャスト グループがアクティブであるかをマルチキャスト デバイスが判断できる基本的なクエリー応答メカニズムと、ホストがマルチキャスト グループに加入および脱退できるようにするためのその他のプロセスを提供します。 RFC 1112 で、IP マルチキャスト用の IGMPv1 ホスト拡張が定義されています。
IGMPv2	IGMP の拡張で、IGMP の脱退処理、グループ固有のクエリーおよび明示的な最大応答時間フィールドなどの機能が可能になっています。 また、IGMPv2 ではこの作業を実行するために、マルチキャスト プロトコルに依存することなく IGMP クエリアを選択する機能もデバイスに追加されます。 IGMPv2 は RFC 2236 で定義されています。

（注） デフォルトでは、インターフェイスで PIM をイネーブルにすると、そのデバイスで IGMPv2 がイネーブルになります。 IGMPv2 は、可能な限り IGMPv1 と下位互換性を保つよう設計されました。 この下位互換性を実現するために、RFC 2236 は特別な相互運用性ルールを定義しています。 ネットワークにレガシー IGMPv1 ホストが含まれている場合は、これらの運用性ルールをよく知っておく必要があります。 IGMPv1 と IGMPv2 の相互運用性の詳細については、RFC 2236『Internet Group Management Protocol, Version 2』を参照してください。

IGMPv1 を実行するデバイス

IGMPv1 デバイスは、「全ホスト」へのマルチキャスト アドレスである 224.0.0.1 に IGMP クエリーを送信して、アクティブ マルチキャスト レシーバが存在するマルチキャスト グループを求めます。 マルチキャスト レシーバも、デバイスに IGMP レポートを送信して、特定のマルチキャストストリームの受信を待機していることを通知できます。 ホストは非同期に、またはデバイス

によって送信される IGMP クエリーに対応して、レポートを送信できます。 同じマルチキャスト グループに複数のマルチキャスト レシーバが存在する場合、これらのホストの 1 つのみで、IGMP レポート メッセージが送信されます。他のホストでは、レポート メッセージが抑制されます。

IGMPv1 では、IGMP クエリア選択はありません。 セグメント内に複数のデバイスがある場合、すべてのデバイスが定期的に IGMP クエリーを送信します。 IGMPv1 には、ホストがグループから脱退できる特別なメカニズムはありません。 ホストで、特定のグループに対するマルチキャスト パケットを受信する必要がなくなった場合は、デバイスから送信される IGMP クエリー パケットに対する応答を行わないだけです。 デバイスはクエリー パケットを送信し続けます。 デバイスが 3 回 IGMP クエリーの応答を受信しないと、グループはタイムアウトし、デバイスはグループのセグメントへのマルチキャストパケットの送信を停止します。 ホストがタイムアウト期間後にマルチキャスト パケットを受信する場合、そのホストは新しい IGMP join をデバイスに送信するだけです。これにより、デバイスはマルチキャスト パケットの転送を再開します。

LAN 上に複数のデバイスが存在する場合は、指定ルータ（DR）を選択して、接続されているホストに対するマルチキャスト トラフィックの重複を回避する必要があります。 PIM デバイスは DR を選択する選定プロセスに従います。 最も大きい IP アドレスを持つ PIM デバイスが DR になります。

DR は、次のタスクを担当します。

- PIM 登録メッセージ、PIM 加入メッセージ、および PIM プルーニング メッセージをランデブー ポイント（RP）に送信し、ホスト グループ メンバーシップに関する情報を通知する。
- IGMP ホスト クエリー メッセージを送信する。
- IGMP オーバーヘッドをホストおよびネットワークでできるだけ低く維持するために、ホスト クエリー メッセージをデフォルトで 60 秒ごとに送信する。

IGMPv2 を実行するデバイス

IGMPv2 では、IGMPv1 のクエリー メッセージング機能が改善されました。

IGMPv2 のクエリーおよびメンバーシップ レポート メッセージは、次の 2 つの例外を除き、IGMPv1 メッセージと同じです。

- IGMPv2 クエリー メッセージは、一般クエリー（IGMPv1 クエリーと同じ）とグループ固有クエリーの 2 つのカテゴリに分かれる。
- IGMPv1 メンバーシップ レポートと IGMPv2 メンバーシップ レポートの IGMP タイプ コードが異なる。

IGMPv2 では、次の機能に対するサポートを追加することにより、IGMP の機能の強化も行われました。

- クエリア選択プロセス：IGMPv2 デバイスが、プロセスを実行するマルチキャスト ルーティング プロトコルに依存せずに、IGMP クエリアを選択できる機能を提供します。
- [Maximum Response Time] フィールド：IGMP クエリアを使用して最大クエリー応答時間を指定できる、クエリー メッセージの新しいフィールド。 このフィールドで、応答のバースト性を制御し、脱退遅延を調整するクエリー応答プロセスの調整ができます。

- グループ固有クエリー メッセージ：すべてのグループではなく特定の 1 つのグループでクエリー操作を実行する目的で、IGMP クエリアを使用することができます。
- グループ脱退メッセージ：グループから脱退することをネットワーク上のデバイスに通知する手段をホストに提供します。

DR と IGMP クエリアが通常同じデバイスである IGMPv1 とは異なり、IGMPv2 では 2 つの機能は分離されます。 DR と IGMP クエリアは異なる基準で選択され、同じサブネット上の異なるデバイスである場合があります。 DR はサブネットで IP アドレスが最大のデバイスで、IGMP クエリアは最小の IP アドレスを持つデバイスです。

次のように、クエリー メッセージは IGMP クエリアの選択に使用されます。

1. 各 IGMPv2 デバイスは起動時に、そのインターフェイス アドレスを一般クエリー メッセージのソース IP アドレス フィールドに使用して、当該メッセージを全システムのグループ アドレス 224.0.0.1 にマルチキャスト送信します。
2. IGMPv2 デバイスが一般クエリー メッセージを受信すると、デバイスは自分のインターフェイス アドレスとメッセージのソース IP アドレスを比較します。 サブネット上の最下位 IP アドレスが使用されているデバイスにより、IGMP クエリアが選択されます。
3. すべてのデバイス（クエリアは除く）でクエリー タイマーが開始されます。IGMP クエリアから一般クエリー メッセージを受信するたびに、タイマーはリセットされます。 クエリー タイマーが切れると、IGMP クエリアがダウンしたと見なされ、新しい IGMP クエリアを選択するために選択プロセスが再度実行されます。

デフォルトでは、タイマーはクエリー インターバルの 2 倍です。

IGMP の加入および脱退処理

IGMP の加入処理

ホストがマルチキャスト グループに加入するとき、ホストは、加入するマルチキャスト グループに 1 つ以上の送信要求されていないメンバーシップ レポートを送信します。 IGMP 加入処理は、IGMPv1 ホストと IGMPv2 ホストで同じです。

IGMPv3 では、ホストの加入処理は次のように処理されます。

- ホストがグループに加入する場合は、空の EXCLUDE リストを使用して、224.0.0.22 に IGMPv3 メンバーシップ レポートを送信します。
- ホストが特定のチャネルに加入する場合は、特定のソース アドレスを含む INCLUDE リストを使用して、224.0.0.22 に IGMPv3 メンバーシップ レポートを送信します。
- ホストが特定のソースを除くグループに加入する場合は、これらのソースを EXCLUDE リストで除外して、224.0.0.22 に IGMPv3 メンバーシップ レポートを送信します。

（注） LAN 上にある一部の IGMPv3 ホストでソースが除外され、その他のホストで同じソースが含まれている場合、デバイスは LAN 上でそのソースのトラフィックを送信します（つまり、この場合、包含が除外より優先されます）。

関連トピック

グループのメンバとしてのスイッチの設定, （1083 ページ）
IGMP の前提条件, （1075 ページ）
例：マルチキャスト グループのメンバとしてのスイッチの設定, （1097 ページ）

IGMP の脱退処理

ホストがグループから脱退するために使用する方法は、動作中の IGMP のバージョンによって異なります。

IGMPv1 の脱退処理

IGMPv1 には、ホストがあるグループからのマルチキャスト トラフィックを受信しないことをそのサブネットのデバイスに通知するグループ脱退メッセージはありません。 ホストでは、マルチキャスト グループに対するトラフィックの処理が停止するだけで、そのグループに対する IGMP メンバーシップ レポートを使用した IGMP クエリーへの応答が終了します。 その結果、IGMPv1 デバイスがサブネットの特定のマルチキャスト グループにアクティブなレシーバがなくなったことを認識する唯一の方法は、デバイスがメンバーシップ レポートを受信しなくなったときになります。 このプロセスを容易にするために、IGMPv1 デバイスは、サブネットの IGMP グループとカウント ダウン タイマーを関連付けます。 サブネットのグループがメンバーシップ レポートを受信すると、タイマーがリセットされます。 IGMPv1 デバイスでは、このタイム アウト間隔は通常クエリー間隔の 3 倍（3 分）です。 このタイムアウト間隔は、すべてのホストがマルチキャスト グループから脱退した後最大 3 分間、デバイスがサブネットにマルチキャスト トラフィックを転送し続ける可能性があることを意味します。

IGMPv2 の脱退処理

IGMPv2 には、特定のグループのマルチキャスト トラフィックの受信を停止することをホストが提示する手段を提供するグループ脱退メッセージが組み込まれています。 IGMPv2 ホストがマルチキャスト グループから脱退するとき、そのホストがそのグループのメンバーシップ レポートでクエリーに応答する最後のホストである場合、デバイス全体のマルチキャスト グループ（224.0.0.2）にグループ脱退メッセージを送信します。

IGMPv3 の脱退処理

IGMPv3 は、IGMPv3 メンバーシップ レポートにソース、グループ、またはチャネルを含めるか除外することによって、ホストが特定のグループ、ソース、またはチャネルからのトラフィックの受信を停止できる機能を導入することで、脱退処理を拡張しています。

関連トピック

グループのメンバとしてのスイッチの設定, （1083 ページ）
IGMP の前提条件, （1075 ページ）
例：マルチキャスト グループのメンバとしてのスイッチの設定, （1097 ページ）

IGMP のデフォルト設定

次の表に、スイッチの IGMP のデフォルト設定を示します。

表 *103*：*IGMP* のデフォルト設定

機能	デフォルト設定
マルチキャスト グループのメンバとしてのマルチレイヤ スイッチ	グループ メンバーシップは未定義
マルチキャスト グループへのアクセス	インターフェイスのすべてのグループを許可
IGMP のバージョン	すべてのインターフェイスでバージョン 2
IGMP ホストクエリー メッセージ インターバル	すべてのインターフェイスで 60 秒
IGMP クエリー タイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒
静的に接続されたメンバとしてのマルチレイヤ スイッチ	ディセーブル

IGMP の設定方法

グループのメンバとしてのスイッチの設定

スイッチをマルチキャスト グループのメンバとして設定し、マルチキャストがネットワークに到達可能かどうかを検出できます。 管理しているすべてのマルチキャスト対応ルータおよびマルチレイヤスイッチがマルチキャストグループのメンバである場合、グループにpingを送信すると、これらのすべてのデバイスが応答します。 デバイスは、所属グループにアドレス指定されたICMPエコー要求パケットに応答します。 もう 1 つの例は、ソフトウェア付属のマルチキャスト トレースルート ツールです。

⚠

注意 この手順を実行すると、グループ アドレス用のデータ トラフィックがすべて CPU に送られるため、CPU のパフォーマンスが低下する場合があります。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp join-group***group-address*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにする インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip igmp join-group***group-address* 例： `Switch(config-if)# ip igmp join-group 225.2.2.2`	スイッチをマルチキャスト グループに参加するように設定します。 デフォルトで、グループのメンバーシップは定義されていません。 *group-address* には、マルチキャスト IP アドレスをドット付き 10 進表記で指定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Switch# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP の加入処理，（1081 ページ）
IGMP の脱退処理，（1082 ページ）
IGMP の前提条件，（1075 ページ）
例：マルチキャスト グループのメンバとしてのスイッチの設定，（1097 ページ）

IP マルチキャスト グループへのアクセスの制御

スイッチは IGMP ホストクエリー メッセージを送信し、接続されたローカル ネットワーク上のメンバーが属しているマルチキャスト グループを判別します。次に、スイッチは、マルチキャスト グループにアドレス指定されたすべてのパケットをこれらのグループ メンバーに転送します。インターフェイスごとにフィルタを適用し、インターフェイスで処理されるサブネット上のホストが加入可能なマルチキャスト グループを制限できます。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp access-group***access-list-number*
5. **exit**
6. **access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
7. **end**
8. **show ip igmp interface** [*interface-id*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface GigabitEthernet 1/0/12`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip igmp access-group***access-list-number* 例： `Switch(config-if)# ip igmp access-group 10`	インターフェイスで処理されるサブネット上のホストが加入できるマルチキャスト グループを指定します。 デフォルトでは、インターフェイスのすべてのグループが許可されています。 *access-list-number* には、IP 標準アドレス アクセス リスト番号を指定します。 指定できる範囲は 1 ～ 199 です。 （注） インターフェイスでグループをディセーブルにするには、**no ip igmp access-group** インターフェイス コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 10 permit`	標準アクセス リストを作成します。 • *access-list-number* には、ステップ 3 で作成したアクセス リストを指定します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、サブネット上のホストが加入できるマルチキャスト グループを指定します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 7	**end** 例： `Switch(config-igmp-profile)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip igmp interface** [*interface-id*] 例： `Switch# show ip igmp interface`	入力を確認します。

関連トピック

例：IP マルチキャスト グループへのアクセスの制御, （1097 ページ）

IGMP バージョンの変更

スイッチでは、IGMP クエリー タイムアウトや最大クエリー応答時間などの機能を使用できる IGMP バージョン 2 がデフォルトで使用されます。

サブネット上のすべてのシステムで、同じバージョンをサポートする必要があります。 スイッチは自動的にバージョン 1 のシステムを検出せず、バージョン 1 へのスイッチングも行いません。 バージョン 2 のルータまたはスイッチは、常に IGMPv1 ホストと正しく連動しているため、バージョン 1 とバージョン 2 のホストはサブネット上で混在できます。

使用しているホストでバージョン 2 がサポートされていない場合は、スイッチをバージョン 1 に設定してください。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp version** {**1**| **2** | **3** }
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**ip igmp version** {**1**| **2** | **3** } 例： `Switch(config-if)# ip igmp version 2`	スイッチで使用する IGMP バージョンを指定します。 （注） バージョン 1 に変更すると、 **ip igmp query-interval** または **ip igmp query-max-response-time** インターフェイス コンフィギュレーション コマンドを設定できません。 デフォルトの設定に戻すには、**no ip igmp version** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Switch# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP のバージョン，（1077 ページ）

IGMP ホストクエリー メッセージ インターバルの変更

スイッチは、IGMP ホストクエリー メッセージを定期的に送信し、接続されたネットワーク上にあるマルチキャスト グループを検出します。 これらのメッセージは、TTL が 1 の全ホスト マルチキャスト グループ（224.0.0.1）に送信されます。 スイッチはホストクエリー メッセージを送信し、ネットワーク上に存在するメンバーシップに関する情報をリフレッシュします。 クエリーをいくつか実行したあとで、マルチキャスト グループのメンバーであるローカルホストが存在しないことをソフトウェアが検出した場合、そのグループのリモート送信元からローカル ネットワークへのマルチキャストパケット転送が停止され、プルーニング メッセージが送信元のアップストリーム方向へ送信されます。

スイッチは LAN（サブネット）用の PIM DR を選択します。 DR は、LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。 SM の場合、DR は PIM 登録メッセージおよび PIM Join メッセージも RP ルータに向けて送信します。 IGMPv2 では、DR は IP アドレスが最大である、ルータまたはマルチレイヤ スイッチです。 IGMPv1 では、DR は LAN 上で動作するマルチキャスト ルーティング プロトコルに従って選択されます。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp query-interval***seconds*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにする インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip igmp query-interval***seconds* 例： `Switch(config-if)# ip igmp query-interval 75`	DR が IGMP ホストクエリー メッセージを送信する頻度を設定します。 デフォルトでは、DR は IGMP ホストクエリー メッセージを 60 秒ごとに送信し、ホストおよびネットワークでの IGMP オーバーヘッドを抑制します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Switch# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMPv2 の IGMP クエリー タイムアウトの変更

IGMPv2 を使用している場合、スイッチがインターフェイスのクエリアとして引き継ぐまでの時間を指定できます。 デフォルトでは、スイッチは **ip igmp query-interval** インターフェイス コンフィギュレーション コマンドによって制御されるクエリー インターバルの 2 倍の時間だけ待機します。 この時間を経過しても、スイッチがクエリーを受信しない場合は、スイッチがクエリアになります。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp querier-timeout***seconds*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにする インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip igmp querier-timeout***seconds* 例： `Switch(config-if)# ip igmp querier-timeout 120`	IGMP クエリー タイムアウトを指定します。 デフォルトは 60 秒です（クエリー インターバルの 2 倍）。 指定できる範囲は 60 ～ 300 です。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Switch# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMPv2 の最大クエリー応答時間の変更

IGMPv2 を使用している場合は、IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更できます。 スイッチは最大クエリー応答時間を使用し、LAN 上に直接接続されたグループ メンバが存在しないことを短時間で検出します。 値を小さくすると、スイッチによるグループのプルーニング速度が向上します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp query-max-response-time***seconds*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにする インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip igmp query-max-response-time***seconds* 例： `Switch(config-if)# ip igmp query-max-response-time 15`	IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更します。 デフォルトは 10 秒です。 指定できる範囲は 1 ～ 25 秒です。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Switch# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

静的に接続されたメンバとしてのスイッチの設定

ネットワーク セグメント上にグループ メンバが存在しなかったり、ホストで IGMP を使用してグループ メンバーシップを報告できないことがあります。 しかし、そのネットワーク セグメントに対して、マルチキャスト トラフィックの送信が必要な場合もあります。 マルチキャスト トラフィックをネットワーク セグメントに送り込むには、次のコマンドを使用します。

- **ip igmp join-group**：スイッチはマルチキャスト パケットの転送だけでなく、マルチキャスト パケットを受信します。 マルチキャスト パケットを受信すると、スイッチは高速スイッチングを実行できません。
- **ip igmp static-group**：スイッチは、パケットを転送するだけで、パケット自体は受信しません。 この方法を使用すると、高速スイッチングが可能です。 発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャスト ルート エントリに「L」（ローカル）フラグが付かないことからも明らかなように、スイッチ自体はメンバではありません。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp static-group***group-address*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip igmp static-group***group-address* 例： `Switch(config-if)# ip igmp static-group 239.100.100.101`	スイッチを静的に接続されたグループのメンバとして設定します。 デフォルトでは、この機能はディセーブルになっています。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Switch# show ip igmp interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

（注） このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。 さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

次の表に示す特権 EXEC コマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 *104*：システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
show ip igmp groups [*type-number* | *detail*]	スイッチに直接接続され、IGMP によって取得されたマルチキャスト グループを表示します。
show ip igmp interface [*type number*]	インターフェイスのマルチキャスト関連情報を表示します。
show ip igmp profile [*profile_number*]	IGMP プロファイル情報を表示します。
show ip igmp ssm-mapping [*hostname/IP address*]	IGMP SSM マッピング情報を表示します。

コマンド	目的
show ip igmp static-group {**class-map** [**interface** [*type*]]	スタティック グループ情報を表示します。
show ip igmp vrf	選択した VPN ルーティング/転送インスタンスを名前別に表示します。

IGMP の設定例

例：マルチキャスト グループのメンバとしてのスイッチの設定

次に、マルチキャスト グループ 255.2.2.2 へのスイッチの加入を許可する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp join-group 255.2.2.2
Switch(config-if)#
```

関連トピック

グループのメンバとしてのスイッチの設定, （1083 ページ）
IGMP の加入処理, （1081 ページ）
IGMP の脱退処理, （1082 ページ）

例：IP マルチキャスト グループへのアクセスの制御

次に、ポートに接続されたホストが、グループ 255.2.2.2 にだけ加入できるように設定する例を示します。

```
Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp access-group 1
```

関連トピック

IP マルチキャスト グループへのアクセスの制御, （1085 ページ）

第 38 章

CGMP の設定

- 機能情報の確認，1099 ページ
- CGMP の設定の前提条件，1099 ページ
- CGMP の制約事項，1100 ページ
- CGMP に関する情報，1100 ページ
- CGMP サーバ サポートのイネーブル化，1100 ページ
- CGMP のモニタリング，1102 ページ

機能情報の確認

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

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

CGMP の設定の前提条件

CGMP を設定する際の前提条件は次のとおりです。

- 複数のシスコ CGMP 対応デバイスがスイッチド ネットワークに接続されていて、**ip cgmp proxy** コマンドを使用する必要がある場合は、すべてのデバイスを同じ CGMP オプションを使用して設定し、他社製のルータよりも IGMP クエリアになる優先順位を上げてください。
- CGMP を使用するには、3560-CX スイッチで IP Services フィーチャ セットがイネーブルになっている必要があります。

CGMP の制約事項

次に、CGMP の制約事項を示します。

- CGMP と HSRPv1 は両立できません。 CGMP 脱退処理と HSRPv1 を同時にイネーブルにできません。 ただし、CGMP と HSRPv2 は同時にイネーブルにできます。

CGMP に関する情報

Cisco Group Management Protocol、または CGMP サーバ サポートはスイッチで提供されます。クライアント側機能は提供されません。 スイッチは、IGMP スヌーピングをサポートしない、CGMP クライアント機能が組み込まれているデバイス用の CGMP サーバとして機能します。

CGMP はレイヤ 2 Catalyst スイッチに接続された Cisco ルータおよびマルチレイヤ スイッチで使用され、IGMP で実行される作業と同様の作業を実行します。 CGMP を使用すると、レイヤ 2 グループ メンバーシップ情報を CGMP サーバからスイッチに通信できます。 これにより、スイッチはすべてのスイッチインターフェイスにマルチキャスト トラフィックをフラッディングしないで、マルチキャスト メンバーが存在するインターフェイスを取得できるようになります。 （IGMP スヌーピングは、マルチキャスト パケットのフラッディングを抑制するためのもう 1 つの方法です）。

CGMP が必要となるのは、レイヤ 2 スイッチで IP マルチキャスト データ パケットと IGMP レポート メッセージを区別できないためです。これらはともに MAC レベルで、同じグループ アドレスにアドレス指定されます。

CGMP サーバ サポートのイネーブル化

複数のシスコ CGMP 対応デバイスがスイッチド ネットワークに接続されていて、**ip cgmp proxy** コマンドを設定する場合は、すべてのデバイスを同じ CGMP オプションを使用して設定し、他社製のルータよりも IGMP クエリアになる優先順位を上げてください。 スイッチ インターフェイスで CGMP サーバをイネーブルにするには、次の手順を実行します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip cgmp** [**proxy** | **router-only**]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	レイヤ 2 Catalyst スイッチに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip cgmp** [**proxy** | **router-only**] 例： `Switch(config-if)# ip cgmp proxy`	インターフェイスで CGMP をイネーブルにします。 デフォルトでは、CGMP はすべてのインターフェイス上でディセーブルです。 CGMP をイネーブルにすると、CGMP Join メッセージが送信されます。レイヤ 2 Catalyst スイッチに接続されたレイヤ 3 インターフェイスでだけ、CGMP をイネーブルにします。 （任意）**proxy** キーワードを入力すると、CGMP プロキシ機能がイネーブルになります。 プロキシ ルータは、CGMP 非対応ルータの MAC アドレス、およびグループ アドレス 0000.0000.0000 が格納された CGMP Join メッセージを送信し、CGMP 非対応ルータが存在することをアドバタイズします。 （注） CGMP プロキシを実行するには、スイッチを IGMP クエリアに設定する必要があります。 **ip cgmp proxy** コマンドを設定する場合は、ネットワークで動作中の IGMP のバージョンに応じて、IP アドレスが最大または最小のスイッチが IGMP クエリアになるように IP アドレスを手動で操作する必要があります。 IGMP バージョン 2 クエリアは、インターフェイスの最小の IP アドレスに基づいて選択されます。 IGMP バージョン 1 クエリアは、インターフェイスで使用されるマルチキャスト ルーティング プロトコルに基づいて選択されます。 （注） インターフェイス上で CGMP をディセーブルにするには、**no ip cgmp** インターフェイス コンフィギュレーション コマンドを使用します。

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

次の作業

レイヤ 2 Catalyst スイッチ CGMP クライアントの設定を確認します。 詳細については、製品に付属のマニュアルを参照してください。

CGMP のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

（注） このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。 さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

次の表に示す特権 EXEC コマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 *105*：システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
ping [*group-name* | *group-address*]	マルチキャスト グループ アドレスにインターネット制御メッセージ プロトコル（ICMP）エコー要求を送信します。
show ip igmp groups [*group-name* | *group-address* | *type number*]	スイッチに直接接続されており、IGMP を介して学習したマルチキャスト グループを表示します。
show ip igmp interface [*type number*]	インターフェイスのマルチキャスト関連情報を表示します。
show ip mcache [*group* [*source*]]	IP 高速スイッチング キャッシュの内容を表示します。
show ip mpacket [*source-address* | *name*] [*group-address* | *name*] [**detail**]	循環キャッシュヘッダーバッファの内容を表示します。
show ip mroute [*group-name* | *group-address*] [*source*] [**summary**] [**count**] [**active** *kbps*]	IP マルチキャスト ルーティング テーブルの内容を表示します。
show ip pim interface [*type number*] [**count**] [**detail**]	PIM に対して設定されたインターフェイスに関する情報を表示します。 このコマンドは、すべてのソフトウェアイメージで使用できます。
show ip pim neighbor [*type number*]	スイッチによって検出された PIM ネイバーのリストを示します。 このコマンドは、すべてのソフトウェアイメージで使用できます。
show ip pim rp [*group-name* | *group-address*]	スパース モードのマルチキャスト グループに関連付けられた RP ルータを表示します。 このコマンドは、すべてのソフトウェア イメージで使用できます。
show ip rpf {*source-address* | *name*}	スイッチの RPF の実行方法（ユニキャスト ルーティング テーブル、DVMRP ルーティング テーブル、またはスタティック マルチキャスト ルーティングのいずれか）を表示します。
show ip sap [*group* | *session-name* | **detail**]	Session Announcement Protocol（SAP）バージョン 2 キャッシュを表示します。

第 39 章

PIM の設定

- 機能情報の確認，1105 ページ
- PIM の前提条件，1105 ページ
- PIM に関する制約事項，1106 ページ
- PIM に関する情報，1109 ページ
- PIM の設定方法，1125 ページ
- PIM のモニタリングとトラブルシューティング，1165 ページ
- PIM の設定例，1167 ページ

機能情報の確認

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

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

PIM の前提条件

- PIM 設定プロセスを開始する前に、使用する PIM モードを決定します。 この決定は、ネットワーク上でサポートするアプリケーションに基づきます。 次の注意事項に従ってください。
  - 一般に、本質的に 1 対多または多対多アプリケーションでは PIM-SM を正常に使用できます。

- 1 対多アプリケーションで最適なパフォーマンスを得るには、SSM が適しています。ただし、IGMP バージョン 3 サポートが必要です。

- PIM スタブ ルーティングを設定する前に、次の条件を満たしていることを確認します。
  - スタブ ルータと中央のルータの両方に IP マルチキャスト ルーティングが設定されている必要があります。 さらに、スタブ ルータのアップリンク インターフェイスに PIM モード（デンス モード、スパース モード、または スパース - デンス モード）が設定されている必要があります。
  - また、スイッチに Enhanced Interior Gateway Routing Protocol（EIGRP）スタブ ルーティングのが設定されている必要があります。
  - PIM スタブ ルータは、ディストリビューション ルータ間の伝送トラフィックのルーティングは行いません。 ユニキャスト（EIGRP）スタブ ルーティングではこの動作が強制されます。 PIM スタブ ルータの動作を支援するためにユニキャスト スタブ ルーティングを設定する必要があります。

PIM に関する制約事項

PIMv1 および PIMv2 の相互運用性

スイッチ上でのマルチキャスト ルーティングの設定ミスを回避するには、ここに記載する情報を確認してください。

シスコの PIMv2 実装を使用すると、バージョン 1 とバージョン 2 間での相互運用性および変換が可能となります。ただし、若干の問題が発生する場合もあります。

PIMv2 に差分的にアップグレードできます。 PIM バージョン 1 および 2 を、1 つのネットワーク内の異なるルータおよびマルチレイヤ スイッチに設定できます。 内部的には、共有メディア ネットワーク上のすべてのルータおよびマルチレイヤ スイッチで同じ PIM バージョンを実行する必要があります。 したがって、PIMv2 デバイスが PIMv1 デバイスを検出した場合は、バージョン 1 デバイスがシャットダウンするかアップグレードされるまで、バージョン 2 デバイスはバージョン 1 にダウングレードされます。

PIMv2 は BSR を使用して各グループ プレフィックスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータおよびマルチレイヤ スイッチにアナウンスします。 自動 RP 機能を組み合わせることにより、PIMv2 BSR と同じ作業を PIMv1 で実行できます。 ただし、自動 RP は PIMv1 から独立している、スタンドアロンのシスコ独自のプロトコルで、 PIMv2 は IETF 標準の追跡プロトコルです。

（注） したがって、PIMv2 の使用を推奨します。 BSR 機能は、Cisco ルータおよびマルチレイヤ スイッチ上の Auto-RP と相互運用します。

PIMv2 デバイスを PIMv1 デバイスと相互運用させる場合は、自動 RP を事前に導入しておく必要があります。 自動 RP マッピング エージェントでもある PIMv2 BSR は、自動 RP で選択された RP を自動的にアドバタイズします。 つまり、自動 RP によって、グループ内のルータまたはマルチレイヤ スイッチごとに 1 つの RP が設定されます。 ドメイン内のルータおよびスイッチの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

PIMv1 と PIMv2 が混在する領域内の DM グループは、特殊な設定を行わなくても自動的に相互運用します。

PIMv1 の自動 RP 機能は PIMv2 RP 機能と相互運用するため、PIMv1 と PIMv2 が混在する領域内に SM グループを設定できます。 すべての PIMv2 デバイスで PIMv1 を使用できますが、RP を PIMv2 にアップグレードすることを推奨します。 PIMv2 への移行を簡単に行うには、以下を推奨します。

- 領域全体で Auto-RP を使用します。
- 領域全体でスパース - デンス モードを設定します。

自動 RP がまだ PIMv1 領域に設定されていない場合は、自動 RP を設定してください。

関連トピック

PIM のバージョン, （1112 ページ）

PIM スタブ ルーティングの設定に関する制約事項

- IP Services イメージには完全なマルチキャスト ルーティングが含まれています。
- 直接接続されたマルチキャスト（IGMP）レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。 アクセス ドメインでは、PIM プロトコルはサポートされません。
- PIM スタブ ルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、PIM スタブ ルーティングを設定しているスイッチ経由です。
- 冗長 PIM スタブ ルータ トポロジーはサポートされません。 PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけがサポートされます。

関連トピック

PIM スタブ ルーティングのイネーブル化, （1125 ページ）
PIM スタブ ルーティング, （1113 ページ）

Auto-RP および BSR の設定に関する制約事項

Auto-RP および BSR を設定する場合は、ネットワーク設定と次の制約事項を考慮してください。

Auto-RP の制約事項

次に、Auto-RP の設定に関する制約事項を示します（ネットワーク設定で使用する場合）。

- PIM をスパース モードまたはデンス モードに設定し、Auto-RP を設定しない場合は、RP を手動で設定する必要があります。
- ルーテッドインターフェイスがSMに設定されていると、すべてのデバイスが自動RPグループの手動 RP アドレスによって設定されている場合も、自動 RP を使用できます。
- ルーテッド インターフェイスが SM で設定され、**ip pim autorp listener** グローバル コンフィギュレーション コマンドを入力する場合、すべてのデバイスが Auto-RP グループの手動 RP アドレスを使用して設定されていなくても、Auto-RP は引き続き使用できます。

BSR 設定の制約事項

次に、BSR の設定に関する制約事項を示します（ネットワーク設定で使用する場合）。

- 候補 BSR を自動 RP 用の RP マッピング エージェントとして設定します。
- グループ プレフィックスが自動 RP によってアドバタイズされた場合は、異なる RP セットによって処理されたこれらのグループ プレフィックスのサブ範囲が、PIMv2 BSR メカニズムによってアドバタイズされないようにする必要があります。 PIMv1 および PIMv2 ドメインが混在する環境では、バックアップ RP で同じグループ プレフィックスが処理されるように設定します。 このようにすると、RP マッピング データベースの最長一致検索によって、PIMv2 DR はこれらの PIMv1 DR から異なる RP を選択できなくなります。

Auto-RP および BSR の注意事項と制限事項

次に、Auto-RP および BSR の設定に関する制約事項を示します（ネットワーク設定で使用する場合）。

- 使用しているネットワークがすべて Cisco ルータおよびマルチレイヤ スイッチである場合は、Auto-RP または BSR のいずれかを使用できます。
- ネットワークに他社製のルータがある場合は、BSR を使用する必要があります。
- Cisco PIMv1 および PIMv2 ルータとマルチレイヤ スイッチ、および他社製のルータがある場合は、自動 RP と BSR の両方を使用する必要があります。 ネットワークに他のベンダー製のルータが含まれる場合には、シスコの PIMv2 デバイス上に自動 RP マッピング エージェントと BSR を設定します。 BSR と他社製の PIMv2 デバイス間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。

（注） PIMv2 は 2 つの方法で使用できます。 1 つはバージョン 2 をネットワーク内で排他的に使用する方法、もう 1 つは PIM バージョンの混在環境を採用してバージョン 2 に移行する方法です。

- ブートストラップ メッセージはホップ単位で送信されるため、PIMv1デバイスの場合、これらのメッセージはネットワーク内の一部のルータおよびマルチレイヤスイッチに到達しません。 このため、ネットワーク内に PIMv1 デバイスがあり、Cisco ルータおよびマルチレイヤスイッチだけが存在する場合は、Auto-RP を使用してください。

- ネットワーク内に他社製のルータが存在する場合は、Cisco PIMv2 ルータまたはマルチレイヤ スイッチに Auto-RP マッピング エージェントおよび BSR を設定します。 BSR と他社製の PIMv2 ルータ間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。
- シスコ PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、Auto-RP と BSR の両方が必要です。 シスコ PIMv2 デバイスを、自動 RP マッピング エージェントと BSR の両方に設定してください。

関連トピック

新規インターネットワークでの Auto-RP の設定, （1130 ページ）

Auto-RP, （1115 ページ）

候補 BSR の設定, （1148 ページ）

ブートストラップ ルータ, （1117 ページ）

PIM に関する情報

Protocol Independent Multicast

PIM（Protocol Independent Multicast）プロトコルは、受信側が開始したメンバーシップの現在の IP マルチキャスト サービス モードを維持します。 PIM は、特定のユニキャスト ルーティング プロトコルに依存しません。つまり、IP ルーティング プロトコルに依存せず、ユニキャスト ルーティング テーブルへの入力に使用されるユニキャスト ルーティング プロトコル（Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Border Gateway Protocol（BGP）、およびスタティック ルート）のいずれも利用できます。 PIM は、ユニキャスト ルーティング情報を使用してマルチキャスト転送機能を実行します。

PIM はマルチキャスト ルーティング テーブルと呼ばれていますが、実際には完全に独立したマルチキャスト ルーティング テーブルを作成する代わりに、ユニキャスト ルーティング テーブルを使用して リバース パス フォワーディング（RPF）チェック機能を実行します。 他のルーティング プロトコルとは異なり、PIM はルータ間のルーティング アップデートを送受信しません。

PIM は、デンス モードまたはスパース モードで動作します。 ルータは、スパース グループとデンス グループの両方を同時に処理できます。 これらのモードは、ルータによるマルチキャスト ルーティング テーブルの書き込み方法と、ルータが直接接続された LAN から受信したマルチキャスト パケットの転送方法を決定します。

PIM は 3560 CX スイッチでのみサポートされます。

PIM 転送（インターフェイス）モードについては、次の項を参照してください。

PIM デンス モード（PIM-DM）

PIM デンス モード（PIM-DM）は、プッシュ モデルを使用してマルチキャスト トラフィックをネットワークの隅々にまでフラッディングします。 このプッシュ モデルは、データを要求するレ

シーバを使用せずにデータをレシーバに配信するための方式です。 この方式は、ネットワークのあらゆるサブネットにアクティブなレシーバが存在する特定の配置には効率的です。

デンスモードでは、ルータは、他のすべてのルータが特定のグループのマルチキャストパケットの転送を求めていると想定します。 あるルータがマルチキャストパケットを受信した場合、直接接続されたメンバまたはPIMネイバーが存在しないときは、ソースにプルーニング メッセージが返送されます。 後続のマルチキャストパケットは、このプルーニング済みのブランチのこのルータにはフラッディングされません。 PIMは、ソース ベースのマルチキャスト配信ツリーを構築します。

PIM-DM は最初に、ネットワーク全体にマルチキャスト トラフィックをフラッディングします。 ダウンストリーム ネイバーを持たないルータは、不要なトラフィックをプルーニングします。 このプロセスは 3 分ごとに繰り返されます。

ルータは、フラッディングとプルーニングのメカニズムを介してデータ ストリームを受信することでステート情報を累積します。 これらのデータ ストリームには送信元およびグループの情報が含まれているため、ダウンストリーム ルータがマルチキャスト転送テーブルを構築できます。 PIM-DM ではソース ツリー、つまり（S, G）エントリしかサポートしていないため、共有配信ツリーの構築に使用できません。

（注） デンス モードはほとんど使用されておらず、また、その使用もお勧めしません。 このため、関連モジュールの設定作業では指定されません。

PIM スパース モード（PIM-SM）

PIM スパース モード（PIM-SM）は、プル モデルを使用してマルチキャスト トラフィックを配信します。 明示的にデータを要求したアクティブなレシーバを含むネットワーク セグメントだけがトラフィックを受信します。

デンスモードのインターフェイスと異なり、スパースモードのインターフェイスは、ダウンストリームのルータから定期的に加入メッセージを受信する場合またはインターフェイスに直接接続のメンバがある場合のみマルチキャスト ルーティング テーブルに追加されます。 LAN から転送する場合、グループが認識しているRPがあれば、SM動作が行われます。 その場合、パケットはカプセル化され、その RP に送信されます。 認識している RP がなければ、パケットは DM 方式でフラッディングされます。 特定のソースからのマルチキャスト トラフィックが十分である場合、レシーバのファースト ホップ ルータは、ソース ベースのマルチキャスト配信ツリーを構築するために加入メッセージをソースに向けて送信できます。

PIM-SM は、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。 PIM-SM は少なくとも最初は共有ツリーを使用するので、ランデブー ポイント（RP）を使用する必要があります。 RP は管理上メットワークで設定されている必要があります。 詳細については、ランデブー ポイント，（1114 ページ）を参照してください。

スパース モードでは、ルータは、トラフィックに対する明示的な要求がない限り、他のルータはグループのマルチキャストパケットを転送しないと見なします。 ホストがマルチキャスト グループに加入すると、直接接続されたルータは RP に PIM 加入メッセージを送信します。 RP はマルチキャスト グループを追跡します。 マルチキャスト パケットを送信するホストは、そのホスト

のファーストホップルータによってRPに登録されます。 その後、RPは、ソースに加入メッセージを送信します。 この時点で、パケットが共有配信ツリー上で転送されます。 特定のソースからのマルチキャスト トラフィックが十分である場合、ホストのファースト ホップ ルータは、ソース ベースのマルチキャスト配信ツリーを構築するために加入メッセージをソースに向けて送信できます。

送信元が RP に登録され、データは共有ツリーを下ってレシーバに転送されます。 エッジ ルータは、RP を介してソースから共有ツリーでデータ パケットを受信するときに、そのソースについて学習します。 次に、エッジ ルータは、そのソースに向けて PIM（S, G）加入メッセージを送信します。 リバース パスに沿った各ルータは、RP アドレスのユニキャスト ルーティング メトリックをソース アドレスのメトリックと比較します。 送信元アドレスのメトリックの方が良い場合は、ソースに向けて PIM（S, G）加入メッセージを転送します。 RP のメトリックと同じ、または RP のメトリックの方が良い場合は、RP と同じ方向に PIM（S, G）加入メッセージが送信されます。 この場合、共有ツリーとソース ツリーは一致すると見なされます。

共有ツリーがソースとレシーバの間の最適なパスでない場合、ルータは動的にソース ツリーを作成し、共有ツリーの下方向へのトラフィック フローを停止します。 この動作は、ソフトウェアのデフォルトの動作です。 ネットワーク管理者は、**ip pim spt-threshold infinity** コマンドを使用して、トラフィックを強制的に共有ツリー上で保持することができます。

PIM-SM は、WAN リンク付きのネットワークを含む、任意のサイズのネットワークに合わせて拡大または縮小します。 明示的な加入メカニズムによって、不要なトラフィックが WAN リンクでフラッディングするのを防ぎます。

関連トピック

既存のスパース モード クラウドへの Auto-RP の追加, （1134 ページ）

単一スタティック RP でのスパース モードの設定, （1138 ページ）

スパース-デンス モード

インターフェイス上でスパースモードまたはデンスモードを設定すると、そのインターフェイス全体にスパース性またはデンス性が適用されます。 ただし、環境によっては、単一リージョン内の一部のグループについてはPIMをスパース モードで実行し、残りのグループについてはデンスモードで実行しなければならない場合があります。

デンス モードだけ、またはスパース モードだけをイネーブルにする代わりに、スパース - デンスモードをイネーブルにできます。 この場合、グループがデンスモードであればインターフェイスはデンスモードとして処理され、グループがスパースモードであればインターフェイスはスパース モードとして処理されます。 インターフェイスがスパース - デンス モードである場合にグループをスパース グループとして処理するには、RP が必要です。

スパース - デンス モードを設定すると、ルータがメンバになっているグループにスパース性またはデンス性の概念が適用されます。

スパース - デンス モードのもう 1 つの利点は、Auto-RP 情報をデンス モードで配信しながら、ユーザ グループのマルチキャスト グループをスパース モード方式で使用できることです。 したがって、リーフ ルータ上にデフォルト RP を設定する必要はありません。

インターフェイスがデンス モードで処理される場合、次のいずれかの条件が満たされると、そのインターフェイスはマルチキャスト ルーティング テーブルの発信インターフェイス リストに追加されます。

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する。
- PIM ネイバーが存在し、グループがプルーニングされていない。

インターフェイスがスパース モードで処理される場合、次のいずれかの条件が満たされると、そのインターフェイスはマルチキャスト ルーティング テーブルの発信インターフェイス リストに追加されます。

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する。
- インターフェイス上の PIM ネイバーが明示的な加入メッセージを受信した。

PIM のバージョン

PIMv2 は、PIMv1 と比べて次の点が改善されています。

- マルチキャスト グループごとに、複数のバックアップ ランデブー ポイント（RP）を持つアクティブな RP が 1 つ存在します。 この単一の RP で、PIMv1 内の同じグループにアクティブな RP が複数ある場合と同様の処理を行います。
- ブートストラップ ルータ（BSP）は耐障害性のある、自動化された RP ディスカバリ メカニズム、および配信機能を提供します。これらの機能により、ルータおよびマルチレイヤ スイッチはグループ/RP マッピングを動的に取得できます。
- スパースモード（SM）およびデンスモード（DM）は、インターフェイスではなく、グループに関するプロパティです。

（注） SM または DM のいずれか一方だけでなく、SM-DM（スパース/デンス モード）を使用してください。

- PIM の Join メッセージおよびプルーニング メッセージを使用すると、複数のアドレス ファミリを柔軟に符号化できます。
- 現在以降の機能オプションを符号化するため、クエリーパケットではなく、より柔軟な hello パケット形式が使用されています。
- RP に送信される登録メッセージが、境界ルータによって送信されるか、あるいは指定ルータによって送信されるかを指定します。
- PIM パケットは IGMP パケット内に格納されず、独立したパケットとして処理されます。

関連トピック

PIMv1 および PIMv2 の相互運用性, （1106 ページ）

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング, （1166 ページ）

PIM スタブ ルーティング

PIM スタブ ルーティング機能は、すべてのスイッチ ソフトウェア イメージで使用でき、エンドユーザの近くにルーテッド トラフィックを移動することでリソースの使用状況を低減させます。

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。 サポート対象の PIM インターフェイスは、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類です。 PIM パッシブ モードに設定されているルーテッド インターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過させたり転送したりするのは IGMP トラフィックだけです。

PIM スタブ ルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、PIM スタブ ルーティングを設定しているスイッチ経由です。 PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセス ドメイン、または他のレイヤ 2 デバイスに接続されているインターフェイスに接続されます。 直接接続されたマルチキャスト（IGMP）レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。 PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

PIM スタブ ルーティングを使用しているときは、IP マルチキャスト ルーティングを使用し、スイッチだけを PIM スタブ ルータとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。 スイッチは分散ルータ間の伝送トラフィックをルーティングしません。 スイッチのルーテッドアップリンク ポートも設定する必要があります。 SVI の場合は、スイッチのアップリンク ポートを使用できません。 SVI アップリンク ポートの PIM が必要な場合は、IP Services フィーチャ セットにアップグレードする必要があります。

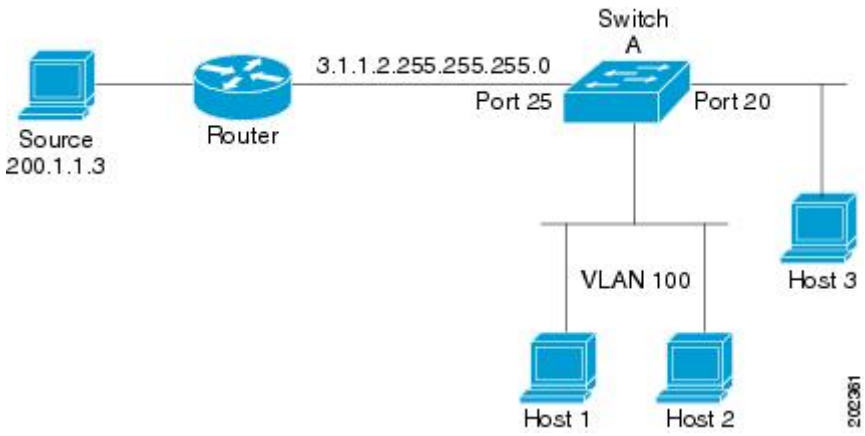
（注） また、PIM スタブ ルーティングをスイッチに設定するときは、EIGRP スタブ ルーティングも設定する必要があります。

冗長 PIM スタブ ルータ トポロジーはサポートされません。 単一のアクセス ドメインにマルチキャスト トラフィックを転送している複数の PIM ルータがある場合、冗長トポロジーが存在します。 PIM メッセージはブロックされ、PIM 資産および指定ルータ検出メカニズムは、PIM 受動インターフェイスでサポートされません。 PIM スタブ機能では、非冗長アクセスルータ トポロジーだけがサポートされます。 非冗長トポロジーを使用することで、PIM 受動インターフェイスはそのアクセス ドメインで唯一のインターフェイスおよび指定ルータであると想定します。

次の図では、スイッチ A ルーテッド アップリンク ポート 25 がルータに接続され、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。 この設定

により、直接接続されたホストはマルチキャスト発信元 200.1.1.3 からトラフィックを受信できます。

図 *79*：*PIM* スタブ ルータ設定



関連トピック

PIM スタブ ルーティングのイネーブル化, （1125 ページ）
例：PIM スタブ ルーティングのイネーブル化, （1167 ページ）
例：PIM スタブ ルーティングの確認, （1167 ページ）
PIM スタブ ルーティングの設定に関する制約事項, （1107 ページ）

IGMP ヘルパー

PIM スタブ ルーティングはルーティングされたトラフィックをエンドユーザの近くに移動させ、ネットワーク トラフィックを軽減します。 スタブ ルータ（スイッチ）に IGMP ヘルパー機能を設定する方法でもトラフィックを軽減できます。

ip igmp helper-address*ip-address*インターフェイス コンフィギュレーション コマンドを使用してスタブ ルータ（スイッチ）を設定すると、スイッチによるネクストホップインターフェイスへのレポート送信をイネーブルにできます。 ダウンストリーム ルータに直接接続されていないホストはアップストリーム ネットワークの送信元マルチキャスト グループに加入できます。 この機能が設定されていると、マルチキャスト ストリームへの加入を求めるホストからの IGMP パケットはアップストリームのネクストホップ デバイスに転送されます。 アップストリームのセントラル ルータは、ヘルパー IGMP レポートまたは leave を受信すると、そのグループの発信インターフェイス リストからインターフェイスの追加または削除を行います。

ランデブー ポイント

ランデブー ポイント（RP）は、デバイスが PIM（Protocol Independent Multicast）スパース モード（SM）で動作している場合にデバイスが実行するロールです。 RP が必要になるのは、PIM SM を実行しているネットワークだけです。 PIM-SM モデルでは、マルチキャスト データを明示的に要求したアクティブなレシーバを含むネットワーク セグメントだけにトラフィックが転送されま

す。 マルチキャスト データの配信方法は、PIM デンス モード（PIM DM）とは対照的です。 PIM DM では、マルチキャスト トラフィックが最初にネットワークのすべてのセグメントにフラッディングされます。 ダウンストリーム ネイバーを持たないルータ、または直接レシーバに接続されているルータは、不要なトラフィックをプルーニングします。

RP は、マルチキャスト データのソースとレシーバの接点として機能します。 PIM SIM ネットワークでは、ソースが RP にトラフィックを送信する必要があります。 このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。 デフォルトでは、レシーバのファースト ホップ デバイスがソースを認識すると、ソースに Join メッセージを直接送信し、ソースからレシーバへのソース ベースの配信ツリーを作成します。 ソースとレシーバ間の最短パス内に RP が配置されていない限り、このソース ツリーに RP は含まれません。

ほとんどの場合、ネットワークにおける RP の配置は複雑な判断を必要としません。 デフォルトでは、RP が必要になるのは、ソースおよびレシーバとの新しいセッションを開始する場合だけです。 その結果、RP では、トラフィックのフローまたは処理によるオーバーヘッドはほとんど発生しません。 PIM バージョン 2 で実行される処理は PIM バージョン 1 よりも少なくなっています。これは、ソースを定期的に RP に登録するだけでステートを作成できるためです。

関連トピック

ランデブー ポイントの設定, （1126 ページ）

Auto-RP

PIM-SM の最初のバージョンでは、すべてのリーフ ルータ（ソースまたはレシーバに直接接続されたルータ）は、RP の IP アドレスを使用して手動で設定する必要がありました。 このような設定は、スタティック RP 設定とも呼ばれます。 スタティック RP の設定は、小規模のネットワークでは比較的容易ですが、大規模で複雑なネットワークでは困難を伴う可能性があります。

PIM-SM バージョン 1 の導入に続き、シスコは、Auto-RP 機能を備えた PIM-SM のバージョンを実装しました。 Auto-RP は、PIM ネットワークにおけるグループから RP へのマッピングの配信を自動化します。 Auto-RP には、次の利点があります。

- さまざまなグループにサービスを提供するために、ネットワーク内で複数の RP を設定することが比較的容易です。
- Auto-RP では、複数の RP 間で負荷を分散し、グループに加入するホストの場所に従って RP を配置できます。
- Auto-RP により、接続の問題の原因となる、矛盾した手動 RP 設定を回避できます。

複数の RP を使用して、異なるグループ範囲にサービスを提供したり、互いにバックアップとしての役割を果たしたりできます。 Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。 その場合、RP マッピング エージェントは、グループから RP への一貫したマッピングを他のすべてのルータに送信します。 これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。

（注） PIM をスパース モードまたはデンス モードに設定し、Auto-RP を設定しない場合は、RP を静的に設定する必要があります。

（注） ルータ インターフェイスがスパース モードに設定されている場合、Auto-RP グループに対してすべてのルータが 1 つのスタティック アドレスで設定されているときは、引き続き Auto-RP グループを使用できます。

Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。 その後、RP マッピング エージェントは、デンス モード フラッディングにより、グループから RP への一貫したマッピングを他のすべてのルータに送信するようになります。 これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。 インターネット割り当て番号局（IANA）は、224.0.1.39 と 224.0.1.40 という 2 つのグループ アドレスを Auto-RP 用に割り当てています。 Auto-RP の利点の 1 つは、指定した RP に対するすべての変更は、RP であるルータ上で設定するだけで、リーフ ルータ上で設定する必要がないことです。 Auto-RP のもう 1 つの利点は、ドメイン内で RP アドレスのスコープを設定する機能を提供することです。 スコーピングを設定するには、Auto-RP アドバタイズメントに許容されている存続可能時間（TTL）値を定義します。

RP の各設定方式には、それぞれの長所、短所、および複雑度のレベルがあります。 従来の IP マルチキャスト ネットワーク シナリオにおいては、Auto-RP を使用して RP を設定することを推奨します。Auto-RP は、設定が容易で、十分にテストされており、安定しているためです。 代わりの方法として、スタティック RP、Auto-RP、およびブートストラップ ルータを使用して RP を設定することもできます。

関連トピック

新規インターネットワークでの Auto-RP の設定, （1130 ページ）

例：Auto-RP の設定, （1168 ページ）

Auto-RP および BSR の設定に関する制約事項, （1107 ページ）

Auto-RP のスパース - デンス モード

Auto-RP の前提条件として、**ip pim sparse-dense-mode** インターフェイス コンフィギュレーション コマンドを使用してすべてのインターフェイスをスパース-デンス モードで設定する必要があります。 スパース - デンス モードで設定されたインターフェイスは、マルチキャスト グループの動作モードに応じてスパース モードまたはデンス モードで処理されます。 マルチキャスト グループ内に既知の RP が存在する場合、インターフェイスはスパース モードで処理されます。 グループ内に既知の RP が存在しない場合、デフォルトでは、インターフェイスはデンス モードで処理され、このインターフェイス上にデータがフラッディングされます （デンス モード フォールバックを回避することもできます。「Configuring Basic IP Multicast」モジュールを参照してください）。

Auto-RP を正常に実装し、224.0.1.39 および 224.0.1.40 以外のグループがデンス モードで動作することを回避するには、「シンク RP」（「ラスト リゾート RP」とも呼ばれます）を設定すること

を推奨します。 シンク RP は、ネットワーク内に実際に存在するかどうかわからない静的に設定された RP です。 デフォルトでは、Auto-RP メッセージはスタティック RP 設定よりも優先されるため、シンク RP の設定は Auto-RP の動作と干渉しません。 未知のソースや予期しないソースをアクティブにできるため、ネットワーク内の可能なすべてのマルチキャスト グループにシンク RP を設定することを推奨します。 ソースの登録を制限するように設定された RP がない場合は、グループがデンス モードに戻り、データがフラッディングされる可能性があります。

ブートストラップ ルータ

PIM-SM バージョン 2 では、Auto-RP に続いてブートストラップ ルータ（BSP）と呼ばれるもう 1 つの RP 選択モデルが導入されました。 BSR は、RP 機能およびグループの RP 情報のリレーに候補ルータを使用するという点において Auto-RP と同様に動作します。 RP 情報は、PIM メッセージ内で伝送される BSR メッセージを通じて配信されます。 PIM メッセージは、PIM ルータから PIM ルータへ移動するリンクローカル マルチキャスト メッセージです。 この RP 情報を配布するシングル ホップ方式により、BSR では TTL スコーピングを使用できません。 BSR は、デンス モード動作に戻るリスクを冒さず、ドメイン内でスコーピング機能を提供しないこと以外は、RP と同様に実行します。

関連トピック

候補 BSR の設定, （1148 ページ）

例：候補 BSR の設定, （1169 ページ）

Auto-RP および BSR の設定に関する制約事項, （1107 ページ）

PIM ドメイン境界

IP マルチキャストの普及に伴い、PIMv2 ドメインと別の PIMv2 ドメインが境界を挟んで隣接する場合が増えています。 2 つのドメインは同じ RP、BSR、候補 RP、候補 BSR のセットを共有していないことが多いため、PIMv2 BSR メッセージがドメインの内外に流れないようにする必要があります。 メッセージのドメイン境界通過を許可すると、通常の BSR 選択メカニズムに悪影響が及んだり、境界に位置するすべてのドメインで単一の BSR が選択されたり、候補 RP アドバタイズメントが混在し、間違ったドメイン内で RP が選択されたりします。

関連トピック

PIM ドメイン境界の定義, （1144 ページ）

マルチキャスト転送

マルチキャスト トラフィックの転送は、マルチキャスト対応ルータによって行われます。 このようなルータは、すべてのレシーバにトラフィックを配信するために、IP マルチキャストがネットワーク上でたどるパスを制御する配信ツリーを作成します。

マルチキャスト トラフィックは、すべてのソースをグループ内のすべてのレシーバに接続する配信ツリー上で、ソースからマルチキャスト グループに流れます。 このツリーは、すべてのソースで共有できます（共有ツリー）。または、各ソースに個別の配信ツリーを作成することもできます（ソース ツリー）。 共有ツリーは一方向または双方向です。

ソース ツリーと共有ツリーの構造を説明する前に、マルチキャスト ルーティング テーブルで使用する表記について触れておきます。 これらの表記には次のものが含まれます。

- (S, G) = (マルチキャスト グループ G のユニキャスト ソース, マルチキャスト グループ G)
- (*, G) = (マルチキャスト グループ G のすべてのソース, マルチキャスト グループ G)

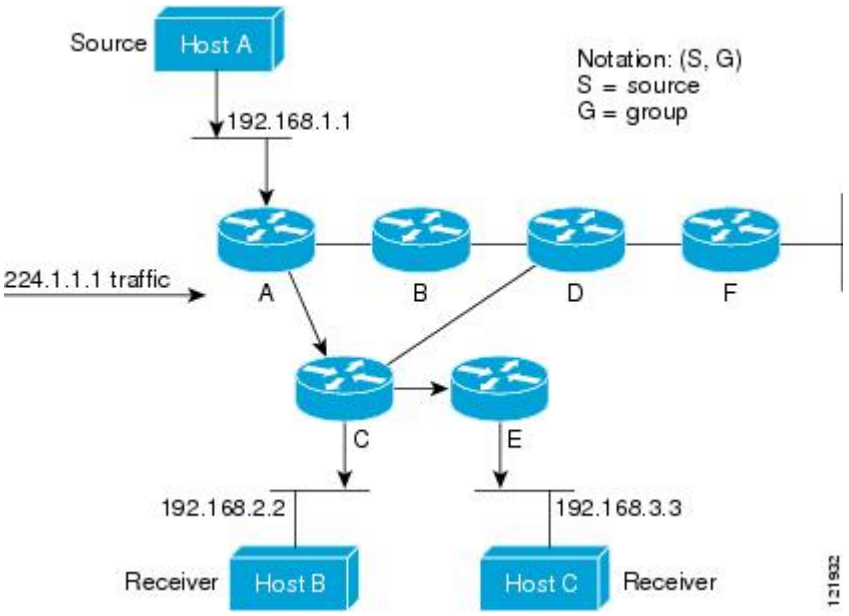
(S, G) という表記（「S カンマ G」と読みます）は、最短パス ツリーの列挙です。S はソースの IP アドレス、G はマルチキャスト グループ アドレスを表します。

共有ツリーは (*, G) で表されます。ソース ツリーは (S, G) で表され、常にソースでルーティングされます。

マルチキャスト配信のソース ツリー

マルチキャスト配信ツリーの最も単純な形式は、ソース ツリーです。 ソース ツリーは、ソース ホストをルートとし、ネットワークを介してレシーバに接続するスパニングツリーを形成するブランチを持ちます。 このツリーはネットワーク上での最短パスを使用するため、最短パスツリー（SPT）とも呼ばれます。

次の図に、ソース（ホスト A）をルートとし、2 つのレシーバ（ホスト B およびホスト C）に接続するグループ 224.1.1.1 の SPT の例を示します。



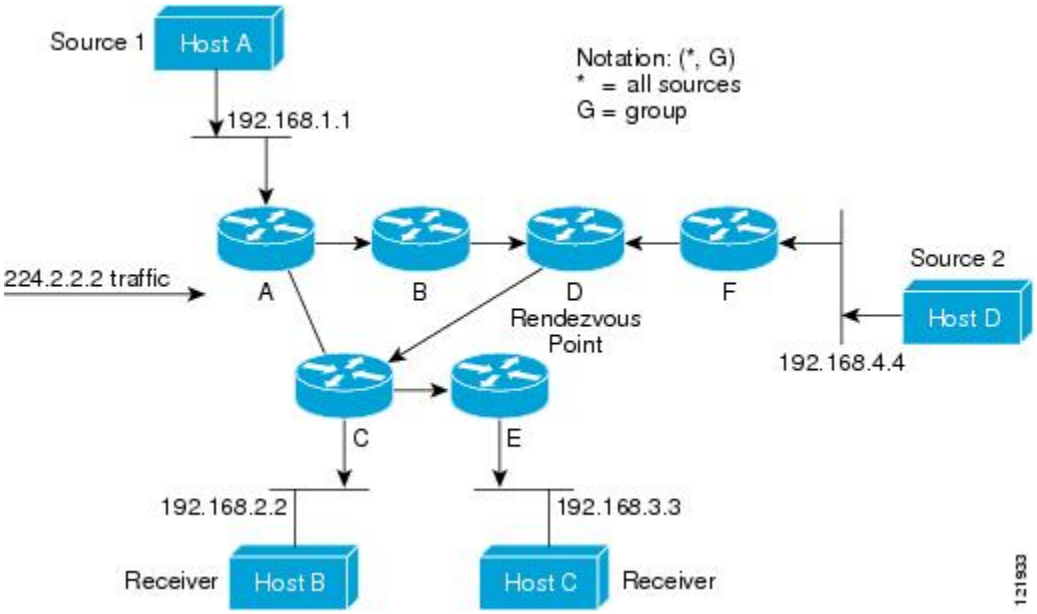
標準表記を使用すると、図の例の SPT は（192.168.1.1, 224.1.1.1）となります。

(S, G) という表記は、各グループに送信する個々のソースに個別の SPT が存在することを意味します。

マルチキャスト配信の共有ツリー

ソースをルートとするソース ツリーとは異なり、共有ツリーはネットワーク内の選択されたポイントに配置された単一の共通ルートを使用します。 この共有されたルートは、ランデブーポイント（RP）と呼ばれます。

マルチキャスト配信の共有ツリー に、ルータ D にルートが配置されたグループ 224.2.2.2 の共有ツリーを示します。この共有ツリーは単方向です。 ソース トラフィックは、ソース ツリー上の RP に向けて送信されます。 このトラフィックは、次に RP から共有ツリーを下方向に転送され、すべてのレシーバに到達します（レシーバがソースと RP の間に配置されていない場合は、直接サービスが提供されます）。



この例では、ソース（ホスト A およびホスト D）からのマルチキャスト トラフィックがルート（ルータ D）に移動した後に共有ツリーから 2 つのレシーバ（ホスト B およびホスト C）へと到達します。マルチキャスト グループ内のすべての送信元が一般的な共有ツリーを使用するため、(*, G) というワイルドカード表記（「アスタリスク、カンマ、G」と読みます）でそのツリーを表します。 この場合、* はすべてのソースを意味し、G はマルチキャスト グループを表します。 したがって、マルチキャスト配信の共有ツリー の共有ツリーは (*, 224.2.2.2) と表記します。

ソースツリーと共有ツリーは、どちらもループフリーです。 ツリーが分岐する場所でのみ、メッセージが複製されます。 マルチキャストグループのメンバは常に加入または脱退する可能性があるため、配信ツリーを動的に更新する必要があります。 特定のブランチに存在するすべてのアクティブ レシーバが特定のマルチキャスト グループに対してトラフィックを要求しなくなると、ルータは配信ツリーからそのブランチをプルーニングし、そのブランチから下方向へのトラフィック転送を停止します。 そのブランチの特定のレシーバがアクティブになり、マルチキャスト トラフィックを要求すると、ルータは配信ツリーを動的に変更し、トラフィック転送を再開します。

ソース ツリーの利点

ソースツリーには、ソースとレシーバの間に最適なパスを作成するという利点があります。 この利点により、マルチキャスト トラフィックの転送におけるネットワーク遅延を最小限に抑えることができます。 ただし、この最適化は代償を伴います。 ルータがソースごとにパス情報を維持する必要があるのです。 何千ものソース、何千ものグループが存在するネットワークでは、このオーバーヘッドがすぐにルータ上でのリソースの問題につながる可能性があります。 ネットワーク設計者は、マルチキャストルーティングテーブルのサイズによるメモリ消費について考慮する必要があります。

共有ツリーの利点

共有ツリーには、各ルータにおいて要求されるステートの量が最小限に抑えられるという利点があります。 この利点により、共有ツリーだけが許容されるネットワークの全体的なメモリ要件が緩和されます。 共有ツリーの欠点は、特定の状況でソースとレシーバの間のパスが最適パスではなくなり、パケット配信に遅延を生じる可能性があることです。 たとえば、上の図のホスト A（ソース 1）とホスト 2（レシーバ）間の最短パスはルータ A とルータ B です。共有ツリーのルートとしてルータ D を使用するため、トラフィックはルータ A、B、D、そして次に C を通過する必要があります。ネットワーク設計者は、共有ツリー専用環境を実装する際にランデブー ポイント（RP）の配置を慎重に考慮する必要があります。

ユニキャスト ルーティングでは、トラフィックは、ネットワーク上でソースから宛先ホストまでの単一パスに沿ってルーティングされます。 ユニキャスト ルータは、ソース アドレスを考慮せず、宛先アドレスおよびその宛先へのトラフィックの転送方法だけを考慮します。 ルータは、ルーティング テーブル全体をスキャンして宛先アドレスを取得し、適正なインターフェイスから宛先の方向へユニキャスト パケットのコピーを転送します。

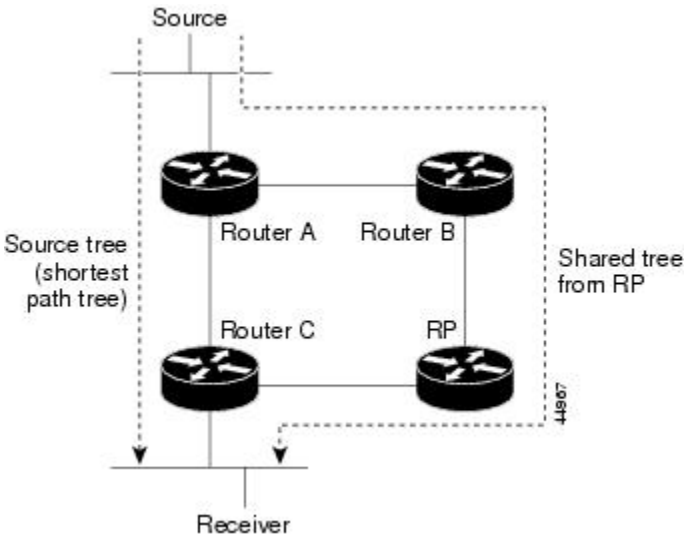
マルチキャスト転送では、ソースは、マルチキャスト グループ アドレスによって表される任意のホスト グループにトラフィックを送信します。 マルチキャスト ルータは、どの方向が（ソースへ向かう）アップストリーム方向で、どの方向（1 方向または複数の方向）が（レシーバへ向かう）ダウンストリーム方向であるかを決定する必要があります。 複数のダウンストリーム パスがある場合、ルータはパケットを複製し、それを適切なダウンストリーム パス（最善のユニキャスト ルート メトリック）で下方向に転送します。これらのパスがすべてであるとは限りません。レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャスト トラフィック転送は、Reverse Path Forwarding（RPF）と呼ばれます。 RPF については、次の項を参照してください。

PIM 共有ツリーおよびソース ツリー

デフォルトでは、グループのメンバーで受信されるデータは、RP でルーティングされた単一のデータ配信ツリーを経由して、送信側からグループに送られます。

次の図に、このタイプの共有配信ツリーを示します。 送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。

図 *80* : 共有ツリーおよびソース ツリー（最短パスツリー）



データ レートによって保証されている場合は、送信元でルーティングされるデータ配信ツリーを、共有ツリーのリーフルータ（ダウンストリーム接続がないルータ）で使用できます。 このタイプの配信ツリーは、SPT またはソース ツリーと呼ばれます。 デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、ソース ツリーにスイッチします。

共有ツリーからソース ツリーへの移動プロセスは、次のとおりです。

1. レシーバがグループに加入します。 リーフ ルータ C は Join メッセージを RP に向けて送信します。
2. RP はルータ C とのリンクを発信インターフェイス リストに格納します。
3. 送信元がデータを送信します。 ルータ A はデータをカプセル化して登録メッセージに格納し、RP に送信します。
4. RP はデータをルータ C に向けて共有ツリーの下方向に転送し、送信元に向けて Join メッセージを送信します。 この時点で、データはルータ C に 2 回着信する可能性があります（カプセル化されたデータ、およびネイティブ状態のデータ）。
5. データがネイティブ状態（カプセル化されていない状態）で着信すると、RP は登録停止メッセージをルータ A に送信します。
6. デフォルトでは、最初のデータ パケット受信時に、ルータ C が Join メッセージを送信元に送信するよう要求します。
7. ルータ C が（S, G）でデータを受信すると、ルータ C は共有ツリーの上位方向にある送信元に prune メッセージを送信します。
8. RP が（S, G）の発信インターフェイスからルータ C へのリンクを削除します。 RP は送信元に向けてプルーニング メッセージを送信します。

送信元および RP に join および prune メッセージが送信されます。 これらのメッセージはホップ単位で送信され、送信元または RP へのパス上にある各 PIM デバイスで処理されます。 register および register-stop メッセージは、ホップバイホップで送信されません。 これらのメッセージは、送信元に直接接続されている指定ルータによって送信され、グループの RP によって受信されます。

グループへ送信する複数の送信元で、共有ツリーが使用されます。 共有ツリー上に存在するように、PIM デバイスを設定できます。

最初のデータ パケットがラスト ホップ ルータに着信すると、共有ツリーからソース ツリーへと変更されます。 この変更は、**ip pim spt-threshold** グローバル コンフィギュレーション コマンドを使用して設定したしきい値によって異なります。

SPT には共有ツリーよりも多くのメモリが必要ですが、遅延が短縮されます。 SPT の使用を延期することもできます。 リーフ ルータを SPT にすぐ移動せず、トラフィックがしきい値に最初に到達したあとで移動するように指定できます。

PIM リーフ ルータが、指定グループの SPT に加入する時期を設定できます。 送信元の送信速度が指定速度（キロビット/秒）以上の場合、マルチレイヤ スイッチは PIM Join メッセージを送信元に向けて送信し、ソース ツリー（SPT）を構築します。 送信元からのトラフィック速度がしきい値を下回ると、リーフルータは共有ツリーに再び切り替わり、プルーニング メッセージを送信元に送信します。

SPT しきい値を適用するグループを指定するには、グループ リスト（標準アクセス リスト）を使用します。 値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。

関連トピック

PIM 最短パス ツリーの使用の延期, （1152 ページ）

リバース パス フォワーディング

ユニキャスト ルーティングでは、トラフィックは、ネットワーク上でソースから宛先ホストまでの単一パスに沿ってルーティングされます。 ユニキャスト ルータは、ソース アドレスを考慮せず、宛先アドレスおよびその宛先へのトラフィックの転送方法だけを考慮します。 ルータは、ルーティング テーブル全体をスキャンして宛先ネットワークを取得し、適正なインターフェイスから宛先の方向へユニキャスト パケットのコピーを転送します。

マルチキャスト転送では、ソースは、マルチキャスト グループ アドレスによって表される任意のホスト グループにトラフィックを送信します。 マルチキャスト ルータは、どの方向が（ソースへ向かう）アップストリーム方向で、どの方向（1 方向または複数の方向）が（レシーバへ向かう）ダウンストリーム方向であるかを決定する必要があります。 複数のダウンストリーム パスがある場合、ルータはパケットを複製し、それを適切なダウンストリーム パス（最善のユニキャスト ルート メトリック）で下方向に転送します。 これらのパスがすべてであるとは限りません。 レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャスト トラフィック転送は、Reverse Path Forwarding（RPF）と呼ばれます。 RPF は、マルチキャスト データグラムの転送に使用されるアルゴリズムです。

Protocol Independent Multicast（PIM）は、ユニキャスト ルーティング情報を使用して、レシーバからソースへ向かうリバース パスに沿って配信ツリーを作成します。 その後、マルチキャスト ルータは、その配信ツリーに沿ってソースからレシーバにパケットを転送します。 RPF は、マルチキャスト転送における重要な概念です。 RPF により、ルータは、配信ツリーの下方向へ正しくマルチキャスト トラフィックを転送できます。 RPF は、既存のユニキャスト ルーティング テーブルを使用して、アップストリーム ネイバーとダウンストリーム ネイバーを決定します。 ルータは、アップストリームインターフェイスで受信した場合にのみ、マルチキャストパケットを転送します。 この RPF チェックにより、配信ツリーがループフリーであることを保証できます。

RPF チェック

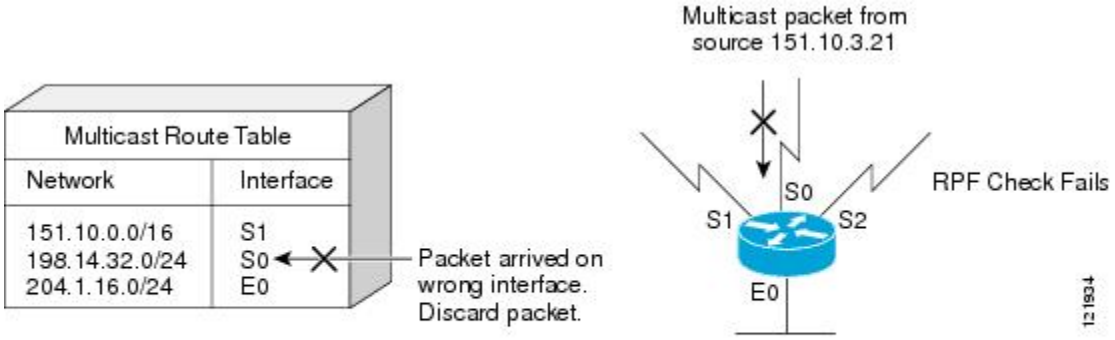
マルチキャスト パケットがルータに到達すると、ルータはそのパケットに対して RPF チェックを実行します。 RPF チェックが成功すると、パケットが転送されます。 そうでない場合、パケットはドロップされます。

ソース ツリーを下方向へ流れるトラフィックに対する RPF チェック手順は次のとおりです。

1. ルータは、ユニキャスト ルーティング テーブルでソース アドレスを検索して、ソースへのリバース パス上にあるインターフェイスにパケットが到達したかどうかを判定します。
2. ソースに戻すインターフェイスにパケットが到達した場合、RPF チェックは成功し、マルチキャスト ルーティング テーブル エントリの発信インターフェイス リストに示されているインターフェイスからパケットが転送されます。
3. ステップ 2 で RPF チェックに失敗した場合は、パケットがドロップされます。

図に、RPF チェックの失敗例を示します。

図 *81*：*RPF* チェックの失敗

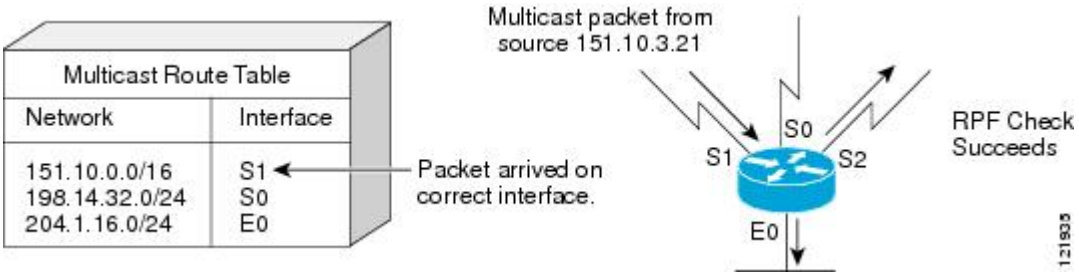


図に示すように、ソース 151.10.3.21 からのマルチキャスト パケットはシリアル インターフェイス 0（S0）上で受信されています。 ユニキャスト ルート テーブルのチェック結果は、このルータが 151.10.3.21 にユニキャスト データを転送するために使用するインターフェイスは S1 であるこ

とを示しています。 パケットはインターフェイス S0 に到達しているため、このパケットは廃棄されます。

図に RPF チェックの成功例を示します。

図 *82*：*RPF* チェックの成功



この例では、マルチキャスト パケットはインターフェイス S1 に到達しています。 ルータはユニキャストルーティングテーブルを参照し、S1 が適正なインターフェイスであることを知ります。RPF チェックが成功し、パケットが転送されます。

PIM ルーティングのデフォルト設定

次の表に、スイッチの PIM ルーティングのデフォルト設定を示します。

表 *106*：マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル
PIM マルチキャスト境界	なし。
候補 BSR	ディセーブル
候補 RP	ディセーブル
SPT しきい値レート	0 kb/s

機能	デフォルト設定
PIM ルータ クエリー メッセージ インターバル	30 秒

PIM の設定方法

PIM スタブ ルーティングのイネーブル化

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip pim passive**
5. **end**
6. **show ip pim interface**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**ip pim passive** 例： `Switch(config-if)# ip pim passive`	インターフェイスに PIM スタブ機能を設定します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip pim interface** 例： `Switch# show ip pim interface`	（任意）各インターフェイスで有効になっている PIM スタブを表示します。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

PIM スタブ ルーティング，（1113 ページ）
例：PIM スタブ ルーティングのイネーブル化，（1167 ページ）
例：PIM スタブ ルーティングの確認，（1167 ページ）
PIM スタブ ルーティングの設定に関する制約事項，（1107 ページ）

ランデブー ポイントの設定

インターフェイスがスパース - デンス モードで、グループをスパース グループとして扱う場合には、ランデブー ポイント（RP）を設定する必要があります。 次の方法を使用できます。

- RP をマルチキャスト グループに手動で割り当てる

- PIMv1 から独立した、以下を含むスタンドアロンとしてのシスコ独自のプロトコル
  - 新規インターネットワークでの自動 RP の設定
  - 既存のスパースモード クラウドへの自動 RP の追加
  - 問題のある RP への Join メッセージの送信禁止
  - 着信 RP アナウンスメント メッセージのフィルタリング
- Internet Engineering Task Force（IETF）の標準追跡プロトコルの使用（PIMv2 BSR の設定を含む）

（注） 動作中の PIM バージョン、およびネットワーク内のルータ タイプに応じて、自動 RP、BSR、またはこれらを組み合わせて使用できます。 ネットワーク内の異なるバージョンの PIM を利用する方法については、PIMv1 および PIMv2 の相互運用性,（1106 ページ）を参照してください。

関連トピック

ランデブー ポイント,（1114 ページ）

マルチキャスト グループへの RP の手動割り当て

ダイナミック メカニズム（自動 RP や BSR など）を使用してグループのランデブー ポイント（RP）を取得する場合、RP を手動で割り当てる必要はありません。

マルチキャスト トラフィックの送信側は、送信元の先頭ホップ ルータ（指定ルータ）から受信して RP に転送される登録メッセージを通し、自身の存在をアナウンスします。 マルチキャスト パケットの受信側は RP を使用し、マルチキャスト グループに加入します。この場合は、明示的な Join メッセージが使用されます。

（注） RP はマルチキャスト グループのメンバーではなく、マルチキャスト送信元およびグループ メンバーの合流地点として機能します。

アクセス リストで定義される複数のグループに、単一の RP を設定できます。 グループに RP が設定されていない場合、マルチレイヤスイッチはデンスとしてグループに応答し、デンスモードの PIM 技術を使用します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip pim rp-address***ip-address* [*access-list-number*] [**override**]
4. **access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim rp-address***ip-address* [*access-list-number*] [**override**] 例： `Switch(config)# ip pim rp-address 10.1.1.1 20 override`	PIM RP のアドレスを設定します。 デフォルトで、PIM RP アドレスは設定されていません。 すべてのルータおよびマルチレイヤ スイッチ（RP を含む）で、RP の IP アドレスを設定する必要があります。 （注） グループに RP が設定されていない場合、スイッチは PIM DM 技術を使用し、グループをデンスとして処理します。 1 台の PIM デバイスを、複数のグループの RP にできます。 1 つの PIM ドメイン内で一度に使用できる RP アドレスは、1 つだけです。 アクセス リスト条件により、デバイスがどのグループの RP であるかを指定します。 • *ip-address* には、RP のユニキャスト アドレスをドット付き 10 進表記で入力します。 • （任意）*access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。 アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • （任意）**override** キーワードを指定すると、このコマンドによって設定された RP と、自動 RP または BSR で取得された RP との

	コマンドまたはアクション	目的
		間に矛盾が生じた場合に、このコマンドによって設定された RP が優先されます。
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 25 permit 10.5.0.1 255.224.0.0`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、RP が使用されるマルチキャスト グループのアドレスを入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：マルチキャスト グループへの RP の手動割り当て，（1168 ページ）

新規インターネットワークでの Auto-RP の設定

新規インターネットワーク内に自動 RP を設定している場合は、すべてのインターフェイスが SM-DM に設定されるため、デフォルトの RP は不要です。

（注） PIM ルータをローカル グループの RP として設定する場合は、次の手順のステップ 3 を省略します。

手順の概要

1. **enable**
2. **show running-config**
3. **configureterminal**
4. **ip pim send-rp-announce***interface-id***scope***ttl***group-list***access-list-number***interval***seconds*
5. **access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
6. **ip pim send-rp-discovery scope***ttl*
7. **end**
8. **show running-config**
9. **show ip pim rp mapping**
10. **show ip pim rp**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**show running-config** 例： `Switch# show running-config`	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内にあることを確認します。 RP は、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって設定済みです。

	コマンドまたはアクション	目的
		（注） SM-DM 環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。 この RP は、グローバル グループ（224.x.x.x やその他のグローバル グループなど）に対して使用されます。 この RP で処理されるグループ アドレス範囲は再設定しないでください。 自動 RP によって動的に検出された RP は、静的に設定された RP よりも優先されます。 ローカル グループ用に 2 番めの RP を使用することもできます。
ステップ 3	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**ip pim send-rp-announce***interface-id***scope***ttl***group-list***access-list-number***interval***seconds* 例： `Switch(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120`	別の PIM デバイスをローカル グループの候補 RP として設定します。 • *interface-id* には、RP アドレスを識別するインターフェイス タイプおよび番号を入力します。 有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • **scope***ttl* には、ホップの TTL 値を指定します。 RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達するように、十分な大きさのホップ数を入力します。 デフォルト設定はありません。 指定できる範囲は 1 ～ 255 です。 • **group-list***access-list-number* を指定する場合は、1 ～ 99 の

	コマンドまたはアクション	目的
		IP 標準アクセス リスト番号を入力します。 アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • **interval***seconds* には、アナウンスメント メッセージを送信する頻度を指定します。 デフォルトは 60 秒です。 指定できる範囲は 1 ～ 16383 です。
ステップ 5	**access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 10 permit 10.10.0.0`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 （注） アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

	コマンドまたはアクション	目的
ステップ 6	**ip pim send-rp-discovery scope***ttl* 例： `Switch(config)# ip pim send-rp-discovery scope 50`	接続が中断される可能性がないスイッチを検索し、RP マッピングエージェントの役割を割り当てます。 **scope***ttl* には、ホップの TTL 値を指定し、RP ディスカバリ パケットを制限します。 ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリメッセージを受信します。 これらのメッセージは他のデバイスに対し、矛盾（グループ/RP 範囲の重なりなど）を回避するために使用されるグループ/RP マッピングを通知します。 デフォルト設定はありません。 指定できる範囲は 1 ～ 255 です。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**show ip pim rp mapping** 例： `Switch# show ip pim rp mapping`	関連するマルチキャストルーティングエントリとともに保管されているアクティブな RP を表示します。
ステップ 10	**show ip pim rp** 例： `Switch# show ip pim rp`	ルーティングテーブルに保管されている情報を表示します。

	コマンドまたはアクション	目的
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

Auto-RP, （1115 ページ）
例：Auto-RP の設定, （1168 ページ）
Auto-RP および BSR の設定に関する制約事項, （1107 ページ）

既存のスパース モード クラウドへの Auto-RP の追加

ここでは、最初に自動 RP を既存の SM クラウドに導入し、既存のマルチキャスト インフラストラクチャができるだけ破壊されないようにする方法について説明します。

この手順は任意です。

手順の概要

1. **enable**
2. **show running-config**
3. **configureterminal**
4. **ip pim send-rp-announce***interface-id***scope***ttl***group-list***access-list-number***interval***seconds*
5. **access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
6. **ip pim send-rp-discovery scope***ttl*
7. **end**
8. **show running-config**
9. **show ip pim rp mapping**
10. **show ip pim rp**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**show running-config** 例： `Switch# show running-config`	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内にあることを確認します。 RP は、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって設定済みです。 （注） SM-DM 環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。 この RP は、グローバル グループ（224.x.x.x やその他のグローバル グループなど）に対して使用されます。 この RP で処理されるグループ アドレス範囲は再設定しないでください。 自動 RP によって動的に検出された RP は、静的に設定された RP よりも優先されます。 ローカル グループ用に 2 番めの RP を使用することもできます。
ステップ 3	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**ip pim send-rp-announce***interface-id***scope***ttl***group-list***access-list-number***interval***seconds* 例： `Switch(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120`	別の PIM デバイスをローカル グループの候補 RP として設定します。 • *interface-id* には、RP アドレスを識別するインターフェイス タイプおよび番号を入力します。 有効なインターフェイス

	コマンドまたはアクション	目的
		は、物理ポート、ポートチャネル、VLAN などです。 • **scope***ttl* には、ホップの TTL 値を指定します。 RP アナウンスメッセージがネットワーク内のすべてのマッピングエージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。 指定できる範囲は 1 ～ 255 です。 • **group-list***access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセスリスト番号を入力します。 アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • **interval***seconds* には、アナウンスメントメッセージを送信する頻度を指定します。 デフォルトは 60 秒です。 指定できる範囲は 1 ～ 16383 です。
ステップ 5	**access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 10 permit 224.0.0.0 15.255.255.255`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 3 で指定したアクセスリスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。

	コマンドまたはアクション	目的
		• *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 6	**ip pim send-rp-discovery scope***ttl* 例： `Switch(config)# ip pim send-rp-discovery scope 50`	接続が中断される可能性がないスイッチを検索し、RP マッピング エージェントの役割を割り当てます。 **scope***ttl* には、ホップの TTL 値を指定し、RP ディスカバリ パケットを制限します。 ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリ メッセージを受信します。 これらのメッセージは他のデバイスに対し、矛盾（グループ/RP 範囲の重なりなど）を回避するために使用されるグループ/RP マッピングを通知します。 デフォルト設定はありません。 指定できる範囲は 1 ～ 255 です。 （注） RP マッピング エージェントとして設定されたスイッチを削除するには、**no ip pim send-rp-discovery** グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。

ステップ 9	**show ip pim rp mapping**
	
	例：
	`Switch#`
	`show ip pim rp mapping`
		関連するマルチキャスト ルーティング エントリとともに保管されているアクティブな RP を表示します。

ステップ 10	**show ip pim rp** 例： `Switch# show ip pim rp`	ルーティング テーブルに保管されている情報を表示します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

PIM スパース モード（PIM-SM），（1110 ページ）

単一スタティック RP でのスパース モードの設定

ランデブー ポイント（RP）は Protocol Independent Multicast Sparse Mode（PIM-SM）を実行しているネットワークで必要です。 PIM-SM でトラフィックは、明示的にマルチキャスト データを要求したアクティブなレシーバを持つネットワーク セグメントにのみ転送されます。

ここでは、単一のスタティック RP を使用したスパース モードの設定方法について説明します。

はじめる前に

単一のスタティック RP を使用してスパース モードを設定するときに必要なすべてのアクセス リストは、設定作業を開始する前に設定しておく必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipmulticast-routing** [**distributed**]
4. **interface***typenumber*
5. **ippimsparse-mode**
6. IP マルチキャストを使用するすべてのインターフェイスでステップ 1 ～ 5 を繰り返します。
7. **exit**
8. **ippimrp-address***rp-address* [*access-list*] [**override**]
9. **end**
10. **showippimrp** [**mapping**] [*rp-address*]
11. **showipigmpgroups** [*group-name* | *group-address*|*interface-typeinterface-number*] [**detail**]
12. **showipmroute**
13. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ipmulticast-routing** [**distributed**] 例： `Switch(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。 • **distributed** キーワードを使用して、マルチキャスト分散スイッチングをイネーブルにします。
ステップ 4	**interface***typenumber* 例： `Switch(config)# interface gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 5	**ippimsparse-mode** 例： `Switch(config-if)# ip pim sparse-mode`	インターフェイスに対して PIM をイネーブルにします。スパース モードを使用する必要があります。
ステップ 6	IP マルチキャストを使用するすべてのインターフェイスでステップ 1 ～ 5 を繰り返します。	--
ステップ 7	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**ippimrp-address***rp-address* [*access-list*] [**override**] 例： `Switch(config)# ip pim rp-address 192.168.0.0`	特定のグループの PIM RP のアドレスを設定します。 • マルチキャスト グループを RP に静的にマッピングされるよう定義する標準アクセス リストに名前を付けたり、番号を指定するために、オプションの *access-list* 引数が使用されます。 （注） アクセス リストが定義されていない場合、RP がすべてのマルチキャスト グループ 224/4 にマッピングされます。 • ダイナミックとスタティックのグループと RP のマッピングが共に使用され、RP アドレスが競合している場合、スタティックのグループと RP のマッピングに設定された RP アドレスが優先されるよう指定するには、オプションの **override** キーワードを使用します。 （注） **override** キーワードが指定されておらず、RP アドレスが競合している場合、ダイナミックのグループと RP のマッピングがスタティックのグループと RP のマッピングに優先されます。
ステップ 9	**end** 例： `Switch(config)# end`	現在のコンフィギュレーション セッションを終了して、EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**showippimrp** [**mapping**] [*rp-address*] 例： `Switch# show ip pim rp mapping`	（任意）ネットワークで既知の RP を表示し、ルータが各 RP について学習する方法を示します。
ステップ 11	**showipigmpgroups** [*group-name* | *group-address*|*interface-typeinterface-number*] [**detail**] 例： `Switch# show ip igmp groups`	（任意）ルータに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。 • レシーバ情報が結果の画面に表示されるには、レシーバがこのコマンドが発行された時点でネットワーク上でアクティブである必要があります。
ステップ 12	**showipmroute** 例： `Switch# show ip mroute`	（任意）IP mroute テーブルの内容を表示します。
ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

PIM スパース モード（PIM-SM），（1110 ページ）

問題のある RP への Join メッセージの送信禁止

ip pim accept-rp コマンドがネットワーク全体に設定されているかどうかを判別するには、**show running-config** 特権 EXEC コマンドを使用します。 **ip pim accept-rp** コマンドが設定されていないデバイスがある場合は、後でこの問題を解決できます。ルータまたはマルチレイヤスイッチが **ip pim accept-rp** コマンドによってすでに設定されている場合は、このコマンドを再入力し、新規にアドバタイズされる RP を許可する必要があります。

自動 RP によってアドバタイズされるすべての RP を許可し、他のすべての RP をデフォルトで拒否するには、**ip pim accept-rp auto-rp** グローバル コンフィギュレーション コマンドを使用します。

この手順は任意です。

関連トピック

例：問題のある RP への Join メッセージの送信禁止，（1169 ページ）

着信 RP アナウンスメント メッセージのフィルタリング

マッピングエージェントにコンフィギュレーションコマンドを追加すると、故意に不正設定されたルータが候補 RP として動作し問題を引き起こさないようにできます。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip pim rp-announce-filter rp-list***access-list-number***group-list***access-list-number*
4. **access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim rp-announce-filter rp-list***access-list-number***group-list***access-list-number* 例： `Switch(config)# ip pim rp-announce-filter rp-list 10 group-list 14`	着信 RP アナウンスメント メッセージをフィルタリングします。 ネットワーク内のマッピングエージェントごとに、このコマンドを入力します。このコマンドを使用しないと、すべての着信 RP アナウンスメント メッセージがデフォルトで許可されます。 **rp-list***access-list-number* には、候補 RP アドレスのアクセスリストを設定します。アクセスリストが許可されている場合は、**group-list***access-list-number* 変数で指定された

	コマンドまたはアクション	目的
		グループ範囲に対してアクセス リストを使用できます。この変数を省略すると、すべてのマルチキャスト グループにフィルタが適用されます。 複数のマッピング エージェントを使用する場合は、グループ/RP マッピング情報に矛盾が生じないようにするため、すべてのマッピングエージェント間でフィルタを統一する必要があります。
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 10 permit 10.8.1.0 255.255.224.0`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • どのルータおよびマルチレイヤスイッチからの候補 RP アナウンスメント（rp-list アクセス コントロール リスト（ACL））がマッピング エージェントによって許可されるかを指定するアクセスリストを作成します。 • 許可または拒否するマルチキャスト グループの範囲を指定するアクセスリスト（グループリスト ACL）を作成します。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

例：着信 RP アナウンスメント メッセージのフィルタリング，（1169 ページ）

PIMv2 BSR の設定

PIMv2 BSR を設定するプロセスには、次のオプションの作業が含まれることがあります。

- PIM ドメイン境界の定義
- IP マルチキャスト境界の定義
- 候補 BSR の設定
- 候補 RP の設定

PIM ドメイン境界の定義

PIM ドメイン境界を設定するには、次の手順を実行します。 この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip pim bsr-border**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip pim bsr-border** 例： `Switch(config-if)# ip pim bsr-border`	PIM ドメイン用の PIM ブートストラップ メッセージ境界を定義します。 境界に位置する他の PIM ドメインに接続されているインターフェイスごとに、このコマンドを入力します。 このコマンドを実行すると、スイッチは、このインターフェイス上で PIMv2 BSR メッセージを送受信しないように指示されます。 （注） PIM 境界を削除するには、**no ip pim bsr-border** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

PIM ドメイン境界，（1117 ページ）

IP マルチキャスト境界の定義

自動 RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。 自動 RP 情報を伝達する 224.0.1.39 および 224.0.1.40 宛てのパケットを拒否するアクセスリストを作成します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **access-list***access-list-number***deny***source* [*source-wildcard*]
4. **interface***interface-id*
5. **ip multicast boundary***access-list-number*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list***access-list-number***deny***source* [*source-wildcard*] 例： `Switch(config)#` **`access-list 12 deny 224.0.1.39`** **`access-list 12 deny 224.0.1.40`**	標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • *source* には、自動 RP 情報を伝達するマルチキャスト アドレス 224.0.1.39 および 224.0.1.40 を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 4	**interface***interface-id* 例： `Switch(config)#` **`interface gigabitethernet 1/0/1`**	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip multicast boundary***access-list-number* 例： `Switch(config-if)#` **`ip multicast boundary 12`**	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 6	**end** 例： `Switch(config)#` **`end`**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch#` **`show running-config`**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義, （1168 ページ）

候補 BSR の設定

候補 BSR を、1 つまたは複数設定できます。 候補 BSR として機能するデバイスは、他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip pim bsr-candidate***interface-id hash-mask-length* [*priority*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip pim bsr-candidate***interface-id hash-mask-length* [*priority*] 例： `Switch(config)# ip pim bsr-candidate gigabitethernet 1/0/3 28 100`	候補 BSR となるようにスイッチを設定します。 • *interface-id* には、スイッチを候補 BSR に設定するときに BSR アドレスの取得元となるスイッチ上のインターフェイスを入力します。 このインターフェイスは PIM を使用してイネーブルにする必要があります。 有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • *hash-mask-length* には、ハッシュ機能を呼び出す前にグループ アドレスとの AND 条件となるマスク長（最大 32 ビット）を指定します。 ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。 たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。 • （任意）*priority* を指定する場合は、0 ～ 255 の番号を入力します。 プライオリティが大きな BSR が優先されます。 このプライオリティ値が同じである場合は、大きな IP アドレスを持つデバイスが BSR として選択されます。 デフォルトは 0 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ブートストラップ ルータ, （1117 ページ）
例：候補 BSR の設定, （1169 ページ）
Auto-RP および BSR の設定に関する制約事項, （1107 ページ）

候補 RP の設定

候補 RP を、1 つまたは複数設定できます。 BSR と同様、RP は他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。 RP は IP マルチキャスト アドレス空間全体、またはその一部を処理します。 候補 RP は候補 RP アドバタイズを BSR に送信します。

この手順は任意です。

はじめる前に

RP となるデバイスを決定するときは、次の可能性を考慮してください。

- 自動 RP だけが使用されている Cisco ルータおよびマルチレイヤ スイッチで構成されるネットワークでは、すべてのデバイスを RP として設定できます。
- シスコの PIMv2 ルータおよびマルチレイヤ スイッチと、他のベンダーのルータだけで構成されるネットワークでは、すべてのデバイスを RP として使用できます。
- シスコの PIMv1 ルータ、PIMv2 ルータ、および他のベンダーのルータで構成されるネットワークでは、シスコ PIMv2 ルータおよびマルチレイヤ スイッチを RP として設定できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip pim rp-candidate***interface-id* [**group-list***access-list-number*]
4. **access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip pim rp-candidate***interface-id* [**group-list***access-list-number*] 例： `Switch(config)# ip pim rp-candidate gigabitethernet 1/0/5 group-list 10`	候補 RP となるようにスイッチを設定します。 • *interface-id* には、対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスを指定します。有効なインターフェイスは、物理ポート、ポートチャネル、VLAN などです。 • （任意）**group-list***access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。 group-list を指定しない場合は、スイッチがすべてのグループの候補 RP となります。
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 10 permit 239.0.0.0 0.255.255.255`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

例：候補 RP の設定, （1170 ページ）

PIM 最短パス ツリーの使用の延期

マルチキャスト ルーティングが送信元ツリーから最短パスツリーに切り替わる前に到達する必要があるトラフィック レートしきい値を設定するには、次の手順を実行します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
4. **ip pim spt-threshold** {*kbps* | **infinity**} [**group-list***access-list-number*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 16 permit 225.0.0.0 0.255.255.255`	標準アクセス リストを作成します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、しきい値が適用されるマルチキャスト グループを指定します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 4	**ip pim spt-threshold** {*kbps* | **infinity**} [**group-list***access-list-number*] 例： `Switch(config)# ip pim spt-threshold infinity group-list 16`	最短パスツリー（SPT）に移行するまでに到達する必要があるしきい値を指定します。 • *kbps* を指定する場合は、トラフィック レートをキロビット/秒で指定します。 デフォルト値は 0 キロビット/秒です。 （注） 有効範囲は 0 ～ 4294967 ですが、スイッチ ハードウェアの制限により、0キロビット/秒以外は無効です。 • **infinity** を指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。 • （任意）**group-list***access-list-number* には、ステップ 2 で作成したアクセス リストを指定します。 値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。

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

関連トピック

PIM 共有ツリーおよびソース ツリー, （1120 ページ）

PIM ルータクエリー メッセージ間隔の変更

PIM ルータおよびマルチレイヤ スイッチでは、各 LAN セグメント（サブネット）の指定ルータ（DR）になるデバイスを検出するため、PIM ルータクエリー メッセージが送信されます。 DR は、直接接続された LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。

PIM DM 動作では、IGMPv1 が使用中の場合だけ、DR は意味を持ちます。 IGMPv1 には IGMP クエリア選択プロセスがないため、選択された DR は IGMP クエリアとして機能します。 PIM-SM 動作では、マルチキャスト送信元に直接接続されたデバイスが DR になります。 DR は PIM 登録メッセージを送信し、送信元からのマルチキャスト トラフィックを共有ツリーの下方向へ転送する必要があることを RP に通知します。 この場合、DR は最大の IP アドレスを持つデバイスです。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip pim query-interval***seconds*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip pim query-interval***seconds* 例： `Switch(config-if)# ip pim query-interval 45`	スイッチが PIM ルータクエリー メッセージを送信する頻度を設定します。 デフォルトは 30 秒です。 指定できる範囲は 1 ～ 65535 です。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Switch# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM の動作の確認

PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト動作の確認

PIM-SM ネットワークまたはPIM-SSM ネットワークでのIPマルチキャスト動作を確認するには、次の作業を実行します。 これらの作業は、ソースとレシーバが想定どおりに動作しない場合に障害のあるホップを検出するのに役立ちます。

（注） パケットが想定された宛先に到達しない場合は、IP マルチキャストのファスト スイッチングをディセーブルにすることを検討してください。ディセーブルにすると、ルータがプロセス スイッチング モードになります。 IP マルチキャストのファスト スイッチングをディセーブルにした後、パケットが正しい宛先に到達するようになった場合、問題は IP マルチキャストのファスト スイッチングに関連している可能性があります。

ファースト ホップ ルータでの *IP* マルチキャストの確認

ファースト ホップ ルータでの IP マルチキャスト動作を確認するには、ファースト ホップ ルータに次のコマンドを入力します。

手順の概要

1. **enable**
2. **showipmroute** [*group-address*]
3. **showipmrouteactive**[*kb/s*]

手順の詳細

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

ステップ 2	**showipmroute** [*group-address*]
	
	例：
	`Switch# show ip mroute 239.1.2.3`
	`(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF`
	`  Incoming interface: Serial1/0, RPF nbr 172.31.200.2`
	`  Outgoing interface list: Null`
	
	`(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT`
	`  Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0`
	`  Outgoing interface list:`
	`  Serial1/0, Forward/Sparse-Dense, 00:18:10/00:03:19`
		ファーストホップルータの mroute に F フラグが設定されていることを確認します。

ステップ 3	**showipmrouteactive**[*kb/s*]
	
	例：
	`Switch# show ip mroute active`
	`Active IP Multicast Sources - sending >= 4 kbps`
	
	`Group: 239.1.2.3, (?)`
	`  Source: 10.0.0.1 (?)`
	`  Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)`
		グループに送信しているアクティブなマルチキャスト送信元に関する情報を表示します。 このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。
		
		（注） デフォルトでは、**showipmroute** コマンドと **active** キーワードによる出力では、4 kb/s 以上のレートでグループにトラフィックを送信するアクティブな送信元の情報が表示されます。 より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。 この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

SPT 上のルータでの *IP* マルチキャストの確認

PIM-SM または PIM-SSM ネットワーク内の SPT 上のルータでの IP マルチキャスト動作を確認するには、SPT 上のルータに次のコマンドを入力します。

手順の概要

1. **enable**
2. **showipmroute** [*group-address*]
3. **showipmrouteactive**

手順の詳細

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

ステップ 2	**showipmroute** [*group-address*]
	
	例：
	`Switch# show ip mroute 239.1.2.3`
	`(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S`
	`  Incoming interface: Null, RPF nbr 0.0.0.0`
	`  Outgoing interface list:`
	`  GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:17:56/00:03:02`
	
	`(10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T`
	`  Incoming interface: Serial1/0, RPF nbr 172.31.200.1`
	`  Outgoing interface list:`
	`  GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:15:34/00:03:02`
		特定のグループの送信元に対する RPF ネイバーを確認します。

ステップ 3	**showipmrouteactive**
	
	例：
	`Switch# show ip mroute active`
	`Active IP Multicast Sources - sending >= 4 kbps`
		グループに送信しているアクティブなマルチキャスト送信元に関する情報を表示します。 このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。

	コマンドまたはアクション	目的

	`Group: 239.1.2.3, (?)`
	`  Source: 10.0.0.1 (?)`
	`  Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)`
		（注） デフォルトでは、**showipmroute** コマンドと **active** キーワードによる出力では、4 kb/s 以上のレートでグループにトラフィックを送信するアクティブな送信元の情報が表示されます。 より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。 この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

ラスト ホップ ルータでの *IP* マルチキャスト動作の確認

ラスト ホップ ルータでの IP マルチキャスト動作を確認するには、ラスト ホップ ルータで次のコマンドを入力します。

手順の概要

1. **enable**
2. **showipigmpgroups**
3. **showippimrpmapping**
4. **showipmroute**
5. **showipinterface** [*typenumber*]
6. **showippiminterfacecount**
7. **showipmroutecount**
8. **showipmrouteactive**[*kb/s*]

手順の詳細

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

	コマンドまたはアクション	目的

ステップ 2	**showipigmpgroups**
	
	例：
	`Switch# show ip igmp groups`
	`IGMP Connected Group Membership`
	`Group Address  Interface  Uptime  Expires  Last Reporter`
	`239.1.2.3  GigabitEthernet1/0/0  00:05:14  00:02:14  10.1.0.6`
	`224.0.1.39  GigabitEthernet0/0/0  00:09:11  00:02:08  172.31.100.1`
		ラスト ホップ ルータの IGMP メンバーシップを確認します。 この情報によって、ラスト ホップ ルータに直接接続され、IGMP を介して認識されるレシーバが使用されているマルチキャスト グループが確認されます。

ステップ 3	**showippimrpmapping**
	
	例：
	`Switch# show ip pim rp mapping`
	`PIM Group-to-RP Mappings`
	
	`Group(s) 224.0.0.0/4`
	`  RP 172.16.0.1 (?), v2v1`
	`  Info source: 172.16.0.1 (?), elected via Auto-RP`
	
	`  Uptime: 00:09:11, expires: 00:02:47`
		グループと RP 間のマッピングがラスト ホップ ルータで正しく生成されていることを確認します。
		
		（注） PIM/SSM ネットワークでラスト ホップ ルータを確認する場合は、この手順を無視してください。 PIM-SSM ではランデブー ポイント（RP）が使用されないため、**showippimrpmapping** コマンドは PIM/SSM ネットワーク内のルータでは動作しません。 さらに、正しく設定されている場合は、PIM/SSM グループは **showippimrpmapping** コマンドの出力には表示されません。

ステップ 4	**showipmroute**
	
	例：
	`Switch# show ip mroute`
	`(*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC`
	`  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1`
	`  Outgoing interface list:`
	`  GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:10/00:03:04`
	
	`(10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T`
	
	`  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1`
	`  Outgoing interface list:`
	`  GigabitEthernet1/0, Forward/Sparse-Dense, 00:02:49/00:03:04`
	
	`(*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC`
	`  Incoming interface: Null, RPF nbr 0.0.0.0`
	`  Outgoing interface list:`
	`  GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:15/00:00:00`
	`  GigabitEthernet0/0, Forward/Sparse-Dense, 00:10:05/00:00:00`
	
	`(172.16.0.1, 224.0.1.39), 00:02:00/00:01:33, flags: PTX`
		mroute テーブルがラスト ホップ ルータに正しく入力されていることを確認します。

	コマンドまたはアクション	目的
	Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1	
ステップ 5	**showipinterface** [*typenumber*] 例： Switch# **show ip interface GigabitEthernet 0/0/0** GigabitEthernet0/0 is up, line protocol is up Internet address is 172.31.100.2/24 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1500 bytes Helper address is not set Directed broadcast forwarding is disabled Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13 224.0.0.5 224.0.0.6 Outgoing access list is not set Inbound access list is not set Proxy ARP is enabled Local Proxy ARP is disabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachables are always sent ICMP mask replies are never sent IP fast switching is enabled IP fast switching on the same interface is disabled IP Flow switching is disabled IP CEF switching is disabled IP Fast switching turbo vector IP multicast fast switching is enabled IP multicast distributed fast switching is disabled IP route-cache flags are Fast Router Discovery is disabled IP output packet accounting is disabled IP access violation accounting is disabled TCP/IP header compression is disabled RTP/IP header compression is disabled Policy routing is disabled Network address translation is disabled WCCP Redirect outbound is disabled WCCP Redirect inbound is disabled WCCP Redirect exclude is disabled BGP Policy Mapping is disabled	マルチキャスト高速スイッチングがイネーブルになっており、ラストホップルータの発信インターフェイスでのパフォーマンスが最適化されていることを確認します。 （注） **noipmroute-cache** インターフェイス コマンドを使用すると IP マルチキャスト高速スイッチングがディセーブルになります。 IP マルチキャスト高速スイッチングがディセーブルになると、プロセススイッチドパスを介してパケットが転送されます。
ステップ 6	**showippiminterfacecount** 例： Switch# **show ip pim interface count** State: * - Fast Switched, D - Distributed Fast Switched H - Hardware Switching Enabled Address Interface FS Mpackets In/Out 172.31.100.2 GigabitEthernet0/0/0 * 4122/0 10.1.0.1 GigabitEthernet1/0/0 * 0/3193	マルチキャストトラフィックがラストホップルータに転送されることを確認します。

	コマンドまたはアクション	目的

ステップ 7	**showipmroutecount**
	
	例：
	`Switch# show ip mroute count`
	`IP Multicast Statistics`
	`6 routes using 4008 bytes of memory`
	`3 groups, 1.00 average sources per group`
	`Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second`
	`Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)`
	
	`Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165`
	`RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0`
	`Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0`
	
	`Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120`
	`Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99`
	
	`Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10`
	`Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0`
		マルチキャスト トラフィックがラスト ホップ ルータに転送されることを確認します。

ステップ 8	**showipmrouteactive**[*kb/s*]
	
	例：
	`Switch# show ip mroute active`
	`Active IP Multicast Sources - sending >= 4 kbps`
	
	`Group: 239.1.2.3, (?)`
	`Source: 10.0.0.1 (?)`
	`Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg)`
		ラスト ホップ ルータ上のグループにトラフィックを送信しているアクティブなマルチキャスト ソースに関する情報を表示します。 このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。
		
		（注） デフォルトでは、**showipmroute** コマンドと **active** キーワードによる出力では、4 kb/s以上のレートでグループにトラフィックを送信するアクティブなソースの情報が表示されます。 より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。 この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

PIM 対応ルータを使用した IP マルチキャストの到達可能性のテスト

管理しているすべての PIM 対応ルータおよびアクセス サーバが、マルチキャスト グループのメンバで、すべてのルータが応答する原因となる ping が送信されます。これは、効果的な管理およびデバッグのツールです。

PIM 対応ルータを使用して IP マルチキャストの到達可能性をテストするには、次の作業を実行します。

マルチキャスト *ping* に応答するルータの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **ipigmpjoin-group***group-address*
5. マルチキャスト ネットワークに加入しているルータ上のインターフェイスで、ステップ 3 とステップ 4 を繰り返します。
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Switch(config)# interface gigabitethernet 1/0/0`	インターフェイス コンフィギュレーション モードを開始します。 *type* 引数および *number* 引数には、ホストに直接接続されているインターフェイス、またはホストに対応しているインターフェイスを指定します。
ステップ 4	**ipigmpjoin-group***group-address* 例： `Switch(config-if)# ip igmp join-group 225.2.2.2`	（任意）指定したグループに加入するようにルータ上のインターフェイスを設定します。

	コマンドまたはアクション	目的
		この作業の目的として、マルチキャスト ネットワークに加入しているルータ上のすべてのインターフェイス上で、*group-address* 引数に同じグループ アドレスを設定します。 （注） この方法では、ルータは、マルチキャストパケットの転送に加えて、マルチキャストパケットを受信します。 マルチキャスト パケットを受信することにより、ルータの高速スイッチングは行われません。
ステップ 5	マルチキャスト ネットワークに加入しているルータ上のインターフェイスで、ステップ 3 とステップ 4 を繰り返します。	--
ステップ 6	**end** 例： `Switch(config-if)# end`	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。

マルチキャスト *ping* に応答するように設定されたルータへの *ping*

マルチキャスト ping に応答するように設定されているルータに対して ping テストを開始するには、ルータで次のこのタスクは、ネットワーク内の IP マルチキャストの到達可能性のテストに使用します。

手順の概要

1. **enable**
2. **ping***group-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**ping***group-address* 例： `Switch# ping 225.2.2.2`	IP マルチキャスト グループ アドレスを ping します。 正常な応答は、グループ アドレスが機能していることを示します。

PIM のモニタリングとトラブルシューティング

PIM 情報のモニタリング

PIM 設定をモニタするには、次の表に記載された特権 EXEC コマンドを使用します。

表 *107* : *PIM* モニタリング コマンド

コマンド	目的
show ip pim interface	Protocol Independent Multicast（PIM）のために設定されているインターフェイスに関する情報を表示します。
show ip pim neighbor	PIM ネイバー情報を表示します。
show ip pim rp[*group-name* | *group-address*]	スパース モードのマルチキャスト グループに関連付けられた RP ルータを表示します。 このコマンドは、すべてのソフトウェアイメージで使用できます。

RP マッピングおよび BSR 情報のモニタリング

次の表に示す特権 EXEC モードを使用して、グループ/RP マッピングの一貫性を確認します。

表 *108* : ***RP*** マッピングのモニタリング コマンド

コマンド	目的
show ip pim rp [*hostname* or *IP address* | **mapping** [*hostname* or *IP address* | **elected** | **in-use**] | **metric** [*hostname* or *IP address*]]	使用可能なすべてのRPマッピングおよびメトリックを表示します。 これにより、（BSR または Auto-RP メカニズムを通じて）スイッチがどのようにRPを学習するかがわかります。 • （任意）*hostname* を指定する場合は、RP を表示するグループの IP 名を指定します。 • （任意）*IP address* を指定する場合は、RP を表示するグループの IP アドレスを指定します。 • （任意）シスコデバイスによって認識されている（設定されている、または Auto-RP によって取得されている）すべてのグループ/RP マッピングを表示するには、**mapping** キーワードを使用します。 • （任意）**metric** キーワードを使用して、RP RPF メトリックを表示します。
show ip pim rp-hash*group*	指定したグループに選択されているRPを表示します。 つまり、PIMv2 ルータまたはマルチレイヤ スイッチ上で、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。 *group* には、RP 情報を表示するグループ アドレスを入力します。

BSR の情報をモニタするには、次の表に示す特権 EXEC コマンドを使用します。

表 *109* : ***VTP*** モニタリング コマンド

コマンド	目的
show ip pim bsr	選択された BSR に関する情報を表示します。

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング

PIMv1 および PIMv2 間の相互運用性に関する問題をデバッグするには、次の点を順にチェックします。

1 **show ip pim rp-hash** 特権 EXEC コマンドを使用して RP マッピングを確認し、すべてのシステムが同じグループの同じ RP に同意していることを確認します。

2 DR と RP の各バージョン間の相互運用性を確認し、 RP が DR と適切に相互作用していることを確認します（この場合は、登録停止に応答し、カプセル化が解除されたデータパケットをレジスタから転送します）。

関連トピック

PIM のバージョン, （1112 ページ）

PIM の設定例

例：PIM スタブ ルーティングのイネーブル化

次の例では、IP マルチキャスト ルーティングがイネーブルになっており、スイッチ A の PIM アップリンク ポート 25 はルーテッド アップリンク ポートとして設定されています（**spare-dense-mode** がイネーブル）。 VLAN 100 インターフェイスとギガビット イーサネット ポート 20 で PIM スタブ ルーティングがイネーブルに設定されています。

```
Switch(config)# ip multicast-routing distributed
Switch(config)# interface GigabitEthernet3/0/25
Switch(config-if)# no switchport
Switch(config-if)# ip address 3.1.1.2 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet3/0/20
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet3/0/20
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# end
```

関連トピック

PIM スタブ ルーティングのイネーブル化, （1125 ページ）

PIM スタブ ルーティング, （1113 ページ）

例：PIM スタブ ルーティングの確認

各インターフェイスの PIM スタブがイネーブルになっていることを確認するには、**show ip pim interface** 特権 EXEC コマンドを使用します。

```
Switch# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet3/0/25 v2/SD 1 30 1 3.1.1.2
```

```
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet3/0/20 v2/P 0 30 1 10.1.1.1
```

関連トピック

PIM スタブ ルーティングのイネーブル化, （1125 ページ）

PIM スタブ ルーティング, （1113 ページ）

例：マルチキャスト グループへの RP の手動割り当て

次に、マルチキャスト グループ 225.2.2.2 の場合だけ、RP のアドレスを 147.106.6.22 に設定する例を示します。

```
Switch(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Switch(config)# ip pim rp-address 147.106.6.22 1
```

関連トピック

マルチキャスト グループへの RP の手動割り当て, （1127 ページ）

例：Auto-RP の設定

次に、最大ホップ数が 31 であるすべての PIM 対応インターフェイスから RP アナウンスメントを送信する例を示します。 ポート 1 の IP アドレスが RP です。 アクセス リスト 5 には、このスイッチが RP として機能するグループが記述されています。

```
Switch(config)# ip pim send-rp-announce gigabitethernet1/0/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

関連トピック

新規インターネットワークでの Auto-RP の設定, （1130 ページ）

Auto-RP, （1115 ページ）

例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義

次に、Auto-RP 情報を拒否する IP マルチキャスト境界の設定例の一部を示します。

```
Switch(config)# access-list 1 deny 224.0.1.39
Switch(config)# access-list 1 deny 224.0.1.40
Switch(config)# access-list 1 permit all
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip multicast boundary 1
```

関連トピック

IP マルチキャスト境界の定義, （1146 ページ）

例：着信 RP アナウンスメント メッセージのフィルタリング

次に、候補 RP アナウンスメントが不正な候補 RP から許可されないようにするために使用される自動 RP マッピング エージェントの設定例を示します。

```
Switch(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Switch(config)# access-list 10 permit host 172.16.5.1
Switch(config)# access-list 10 permit host 172.16.2.1
Switch(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Switch(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

マッピング エージェントは 2 つのデバイス（172.16.5.1 および 172.16.2.1）からの候補 RP アナウンスだけを許可します。 マッピング エージェントは 2 つのデバイスからの候補 RP アナウンスメントのうち、グループ範囲が 224.0.0.0 ～ 239.255.255.255 であるマルチキャスト グループ宛てのアナウンスメントだけを許可します。 マッピングエージェントは、ネットワーク内の他のデバイスからの候補RPアナウンスメントを許可しません。 さらに、候補RPアナウンスメントが239.0.0.0 ～239.255.255.255の範囲のグループに宛てたものである場合、マッピングエージェントは172.16.5.1または 172.16.2.1 からの候補 RP アナウンスメントを許可しません。 この範囲は、管理の有効範囲付きアドレス範囲です。

関連トピック

着信 RP アナウンスメント メッセージのフィルタリング, （1142 ページ）

例：問題のある RP への Join メッセージの送信禁止

すべてのインターフェイスがSMの場合はデフォルト設定のRPを使用し、既知のグループ224.0.1.39および 224.0.1.40 をサポートします。 自動 RP はこれら 2 つの既知のグループを使用し、RP マッピング情報を収集、配信します。 **ip pim accept-rp auto-rp** コマンドが設定されている場合は、RP を許可する別の **ip pim accept-rp** コマンドを次のように設定してください。

```
Switch(config)# ip pim accept-rp 172.10.20.1 1
Switch(config)# access-list 1 permit 224.0.1.39
Switch(config)# access-list 1 permit 224.0.1.40
```

関連トピック

問題のある RP への Join メッセージの送信禁止, （1141 ページ）

例：候補 BSR の設定

次に、候補 BSR の設定例を示します。この例では、アドバタイズ済み BSR アドレスとしてポートの IP アドレス 172.21.24.18 を、hash-mask-length として 30 ビットを使用します。プライオリティは 10 です。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip address 172.21.24.18 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# ip pim bsr-candidate gigabitethernet1/0/2 30 10
```

関連トピック

候補 BSR の設定, （1148 ページ）

ブートストラップ ルータ, （1117 ページ）

例：候補 RP の設定

次に、スイッチが自身を候補 RP として PIM ドメイン内の BSR にアドバタイズするよう設定する例を示します。 標準アクセス リスト番号 4 により、ポートで識別されるアドレスを持つ RP に対応するグループ プレフィックスが指定されます。 この RP は、プレフィックスが 239 であるグループを処理します。

```
Switch(config)# ip pim rp-candidate gigabitethernet1/0/2 group-list 4
Switch(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

関連トピック

候補 RP の設定, （1150 ページ）

第 40 章

HSRP 認識 PIM の設定

- HSRP 認識 PIM, 1171 ページ

HSRP 認識 PIM

このモジュールでは、ホットスタンバイルータプロトコル（HSRP）のアクティブルータ（AR）経由で転送するマルチキャスト トラフィックをイネーブルにし、PIM（Protocol Independent Multicast）を許可して HSRP の冗長性を活用し、潜在的なトラフィックの重複を回避し、フェールオーバーをイネーブルにできるように HSRP 認識 PIM 機能を設定する方法について説明します。

機能情報の確認

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

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

HSRP 認識 PIM の制約事項

- HSRP IPv6 はサポートされません。
- ステートフル フェールオーバーはサポートされません。 PIM ステートレス フェールオーバー時は、HSRP グループの仮想 IP アドレスがスタンバイ ルータに転送されますが、mrouting ステート情報は転送されません。 PIM はステート変更イベントをリッスンして応答し、フェールオーバー時に mroute ステートを作成します。

- 各インターフェイスの PIM がトラッキングできる HSRP グループの最大数は 16 です。
- PIM DR の冗長性プライオリティは、同じ RSRP グループがイネーブルになるか、または HSRP アクティブが DR の選択で成功しないデバイスの PIM DR プライオリティの設定値またはデフォルト値（1）よりも大きくする必要があります。

HSRP 認識 PIM に関する情報

HSRP

Hot Standby Router Protocol（HSRP）はフォールトトレラント デフォルト ゲートウェイを確立するためのシスコ独自の冗長プロトコルです。

このプロトコルは、プライマリ ゲートウェイがアクセスできなくなった場合にデフォルト ゲートウェイのフェールオーバーを実現できるようにネットワーク デバイス間にフレームワークを確立します。 複数のデバイスは、IP アドレスと MAC（レイヤ 2）アドレスを共有することで単一の仮想ルータとして機能できます。 仮想ルータ グループのメンバは常にステータス メッセージを交換し、あるデバイスが予定されたまたは予定外の理由によって稼働しなくなった場合に、別のデバイスがルーティング処理を請け負うことができます。 ホストは、一貫した IP および MAC アドレスに IP パケットを送信しつづけ、ルーティングを実行するデバイスは透過的に切り替えられます。

HSRP は、ホストが Router Discovery Protocol をサポートしておらず、選択されたデバイスのリロードや電源故障時に新しいデバイスに切り替えることができない場合に有効です。 また、既存の TCP セッションはフェールオーバーが発生しても存続するため、このプロトコルでは IP トラフィックをルーティングするためにネクスト ホップを動的に選択するホストの回復をさらに透過的に実行できます。

HSRP をネットワーク セグメントに設定すると、HSRP が動作するデバイスのグループ間で仮想 MAC アドレスと IP アドレスを共有できるようになります。 この HSRP グループのアドレスが仮想 IP アドレスと呼ばれます。 このようなデバイスの 1 つが、アクティブ ルータ（AR）としてプロトコルによって選択されます。 AR は、グループの MAC アドレス宛のパケットを受信してルーティングします。

HSRP では、プライオリティ メカニズムを使用して、デフォルトの AR にする HSRP 設定済みデバイスを決定します。 デバイスを AR として設定するには、他のすべての HSRP 設定済みデバイスのプライオリティよりも高いプライオリティをそのデバイスに割り当てます。 デフォルトのプライオリティは 100 です。 したがって、100 よりも高いプライオリティを持つデバイスを 1 つだけ設定した場合、そのデバイスがデフォルトの AR になります。

HSRP を実行しているデバイスは、User Datagram Protocol（UDP）ベースのマルチキャスト hello メッセージを送信および受信して、デバイスの障害を検出したり、アクティブ デバイスとスタンバイ デバイスを割り当てたりします。 AR が設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイ デバイスが AR になります。 このようにパケット転送機能が別のデバイスに移行しても、ネットワークのいずれのホストにもまったく影響はありません。

複数のホット スタンバイ グループをインターフェイスに設定できるので、冗長デバイスおよびロード シェアリングを余すところなく活用できるようになっています。

HSRP は IP ルートをアドバタイズせず、また、ルーティング テーブルに影響しないため、ルーティング プロトコルではありません。

HSRP には、デバイスの 1 つ以上のインターフェイスに障害が発生した場合にフェールオーバーをトリガーする機能があります。 これは、ヘッドエンドに戻す 1 つのシリアル リンクをそれぞれ持つデュアル ブランチ デバイスに役立つ場合があります。 プライマリ デバイスのシリアル リンクがダウンした場合、バックアップ デバイスがプライマリ機能を引き継ぎ、ヘッドエンドへの接続を保持します。

HSRP 認識 PIM

PIM（Protocol Independent Multicast）には固有の冗長性機能がなく、その動作は Hot Standby Router Protocol（HSRP）グループ ステートに依存しません。 その結果、IP マルチキャスト トラフィックは、HSRP によって選択されたものと同じデバイスによって必ずしも転送されるとは限りません。 HSRP 認識 PIM 機能は、イネーブルになっている仮想ルーティング グループの冗長ネットワークで一貫した IP マルチキャスト転送を実現します。

HSRP 認識 PIM は HSRPアクティブ ルータ（AR）経由でのマルチキャスト トラフィックを転送することができるため、デバイスの HSRP ステートによっては、PIM は HSRP 冗長性を活用し、潜在的なトラフィックの重複を回避し、フェールオーバーをイネーブルにすることができます。 PIM 代表ルータ（DR）は HSRP AR と同じゲートウェイで実行し、mroute ステートを維持します。

マルチアクセス セグメントで（LAN など）では、PIM DR 選択は冗長構成に対応していないため、選択した DR および HSRP AR が同じルータでない場合があります。 PIM DR が RP または FHR に常に PIM Join/Prune メッセージを送信するようにするために、（HSRP グループが 1 つだけの場合は）HSRP AR が PIM DR になります。 PIM はグループ ステートに基づく DR プライオリティの調整を担います。 フェールオーバーが発生すると、HSRP グループによって選択された新しい AR 上にマルチキャスト ステートが作成され、その AR が HSRP 仮想 IP アドレスにアドレス指定されたすべてのトラフィックをルーティングし、転送する役割を引き受けます。

HSRP 認識 PIM をイネーブルにすると、PIM はデバイスが HSRP Active になった時点で PIM Hello 追加メッセージを各アクティブ HSRP グループの送信元アドレスとして HSRP 仮想 アドレスを使用して送信します。 PIM Hello は、フェールオーバーに対応するための他のルータをトリガーするため、新しい GenID を伝送します。 ダウンストリーム デバイスでこの PIM Hello を受信すると、仮想アドレスを PIM ネイバー リストに追加します。 PIM Hello で伝送された新しい GenID はダウンストリームのルータをトリガーし、PIM Join メッセージを仮想アドレスに再送信します。 アップストリーム ルータは、HSRP グループ ステートに基づいて PIM Join/Prunes（J/P）を処理します。

J/P の宛先が HSRP グループの仮想アドレスに一致し、宛先のデバイスが HSRP がアクティブ ステートである場合は、新しい AR が PIM DR として機能しているため、この AR が PIM Join を処理します。 これにより、すべての PIM Join/Prune が HSRP グループの仮想アドレスに到達するため、ダウンストリーム ルータ側での変更とコンフィギュレーションが最小限に抑えられます。

IP ルーティング サービスが既存の仮想ルーティング プロトコルを使用して、基本的なステートレス フェールオーバー サービスを PIM などのクライアントアプリケーションに提供します。 ローカルの HSRP グループ ステートの変更とスタンバイ ルータが担うタスクは対象のクライアント アプリケーションに通知されます。 クライアント アプリケーションが IRS の最上部に構築され、ステートフルまたはステートレスのフェールオーバーを構築することがあります。 HSRP クライ

アントとして PIM は HSRP からのステート変更通知をリッスンし、HSRP ステートに基づいて PIM DR のプライオリティを自動的に調整します。 PIM クライアントも、新しい AR に mroute ステートを作成するためにフェールオーバーの時点でアップストリーム デバイスとダウンストリーム デバイス間の通信をトリガーします。

HSRP 認識 PIM の設定方法

インターフェイスでの HSRP グループの設定

はじめる前に

- デバイス上に IP マルチキャストがすでに設定されている必要があります。
- デバイス上に PIM がすでに設定されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***type number* [*name-tag*]
4. **ip address***ip-address mask*
5. **standby** [*group-number*] **ip** [*ip-address* [*secondary*]]
6. **standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*
7. **standby** [*group-number*] **priority***priority*
8. **standby** [*group-number*] **name***group-name*
9. **end**
10. **show standby** [*type number* [*group*]] [**all** | **brief**]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface***type number* [*name-tag*] 例： `Device(config)# interface ethernet 0/0`	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address***ip-address mask* 例： `Device(config-if)# ip address 10.0.0.2 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 5	**standby** [*group-number*] **ip** [*ip-address* [*secondary*]] 例： `Device(config-if)# standby 1 ip 192.0.2.99`	HSRP をアクティブ化して HSRP グループを定義します。
ステップ 6	**standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime* 例： `Device(config-if)# standby 1 timers 5 15`	（任意）hello パケット間隔、および HSRP のアクティブ ルータまたはスタンバイ ルータのダウンを他のデバイスが宣言するまでの時間を設定します。
ステップ 7	**standby** [*group-number*] **priority***priority* 例： `Device(config-if)# standby 1 priority 120`	（任意）HSRP のアクティブ ルータおよびスタンバイ ルータを選択しやすいように使用する HSRP プライオリティを割り当てます。
ステップ 8	**standby** [*group-number*] **name***group-name* 例： `Device(config-if)# standby 1 name HSRP1`	（任意）HSRP グループの名前を定義します。 （注） HSRP 認識 PIM に使用する HSRP グループを設定する際は、**standby ip name** コマンドを常に設定することを推奨します。
ステップ 9	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show standby** [*type number* [*group*]] [**all** | **brief**] 例： `Device# show standby`	設定を確認するための HSRP グループ情報が表示されます。

PIM 冗長性の設定

はじめる前に

HSRP グループはインターフェイス上で設定済みになっている必要があります。「インターフェイスでの HSRP グループの設定」を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***type number* [*name-tag*]
4. **ip address***ip-address mask*
5. **ip pim redundancy***group***dr-priority***priority*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***type number* [*name-tag*] 例： `Device(config)# interface ethernet 0/0`	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address***ip-address mask* 例： `Device(config-if)# ip address 10.0.0.2 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 5	**ip pim redundancy***group***dr-priority***priority* 例： `Device(config-if)# ip pim redundancy HSRP1 dr-priority 60`	PIM 冗長性をイネーブルにし、冗長性プライオリティ値をアクティブな PIM 指定ルータ（DR）に割り当てます。 • HSRP グループ名では大文字と小文字が区別されるため、*group* 引数の値は **standby ip name** コマンドを使用して設定したグループ名と一致している必要があります。

	コマンドまたはアクション	目的
		• PIM DR の冗長性プライオリティは、同じ HSRP グループがイネーブルになっているデバイスの PIM DR プライオリティに設定されている値またはデフォルト値（1）よりも大きくする必要があります。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

HSRP 認識 PIM の設定例

例：インターフェイスでの HSRP グループの設定

```
interface ethernet 0/0
 ip address 10.0.0.2 255.255.255.0
 standby 1 ip 192.0.2.99
 standby 1 timers 5 15
 standby 1 priority 120
 standby 1 name HSRP1
 !
!
```

例：PIM 冗長性の設定

```
interface ethernet 0/0
 ip address 10.0.0.2 255.255.255.0
 ip pim redundancy HSRP1 dr-priority 60
 !
!
```

第 41 章

VRRP 認識 PIM の設定

- VRRP 認識 PIM, 1179 ページ

VRRP 認識 PIM

仮想ルータ冗長プロトコル（VRRP）によって、静的なデフォルトのルーティング環境に固有の単一障害点が除外されます。 VRRP は、1 つ以上の仮想ルータに対する責任を LAN 上の VRRP ルータに動的に割り当てて、マルチアクセスリンク上の複数のルータで同じ仮想IPアドレスを利用できるようにする選定プロトコルです。

VRRP 認識 PIMは、VRRP と相互運用する PIM（Protocol Independent Multicast）の冗長性メカニズムです。 このメカニズムでは、PIM が VRRP ステートを追跡し、仮想ルーティング グループがイネーブルになっている冗長ネットワークでのフェールオーバー時にマルチキャスト トラフィックを保持できます。

ここでは、ネットワークの VRRP 認識 PIM の設定方法を説明します。

機能情報の確認

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

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

VRRP 認識 PIM の制約事項

- PIM スパース モード（SM）とSource Specific Multicast（SSM）モードがサポートされています。 双方向（BiDir）PIM はサポートされません。

- Hot Standby Router Protocol（HSRP）での PIMの相互運用性はサポートされません。
- PIM は、インターフェイスごとに Virtual Router Redundancy Protocol（VRRP）または HSRP のいずれか 1 つの仮想グループのみをサポートします。
- VRRP 認識 PIMは中継ネットワークではサポートされません。 PIM の冗長性対応インターフェイスは、ダウン ストリームからネットワークに参加する PIM をサポートしません。

VRRP 認識 PIM に関する情報

VRRP 認識 PIM の概要

Virtual Router Redundancy Protocol（VRRP）は、フォールトトレラント デフォルト ゲートウェイを確立するための冗長プロトコルです。 このプロトコルは、プライマリ ゲートウェイがアクセスできなくなった場合にデフォルト ゲートウェイのフェールオーバーを実現できるようにネットワーク デバイス間にフレームワークを確立します。

PIM（Protocol Independent Multicast）には固有の冗長性機能がないため、その動作は VRRP グループの状態に依存しません。 したがって、IP マルチキャストのトラフィックは、VRRP によって選択されたものと同じデバイスによって転送されるとは限りません。 VRRP 認識 PIM 機能は、イネーブルの状態の仮想ルーティング グループの冗長ネットワークで一貫した IP マルチキャスト転送を実行します。

マルチアクセス セグメント（LAN など）では、PIM 代表ルータ（DR）選択が冗長設定を認識しないため、選択された DR および VRRP のマスター ルータは同じルータでない場合があります。 PIM DR が常に PIM Join/Prume メッセージを RP または FHR に送信できるようにするため、VRRP MR が PIM DR になります（VRRP グループが 1 つだけの場合）。 PIM はグループ ステートに基づく DR プライオリティの調整を担います。 フェールオーバーが発生すると、マルチキャスト ステートが VRRP グループによって選択された新しい MR に作成され、その MR が VRRP 仮想 IP アドレスにアドレス指定されたすべてのトラフィックのルーティングと転送を担います。 こうすることによって、PIM DR は VRRP MR と同じゲートウェイで実行され、mroute ステートが保持されます。 これにより、マルチキャスト トラフィックが VRRP MR を通じて転送され、PIM が VRRP の冗長性を利用してトラフィックが重複する可能性をなくし、デバイスの VRRP 状態に応じてフェールオーバーを有効にします。

仮想ルータ冗長性サービス（FRRS）はクライアントにパブリック API を提供して VRRP との通信を行います。 VRRP 認識 PIM は、IPv4 と IPv6 の両方で BRRPv3（ユニファイド VRRP）をサポートする VRRS の機能です。

VRRS クライアントとしての PIM は VRRS クライアント API を使用して一般的な First Hop Redundancy Protocol（FHRP）状態と設定情報を取得し、マルチキャスト冗長性機能を提供します。

PIM は、VRRS クライアントとして次の処理を実行します。

- 状態の変更をリッスンし、VRRS サーバ（VRRP）からの通知を更新します。
- VRRP の状態に基づいて PIM DR の優先度を調整します。

- VRRP がフェールオーバーすると、PIM は トラッキング対象の VRRS から状態変更通知を受け取り、VRRP MRからトラフィックが転送されるようにします。

VRRP 認識 PIM の設定方法

VRRP 認識 PIM の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **fhrp version vrrp** *version*
4. **interface** *type number*
5. **ip address***address*
6. **vrrp***group id***address-familyipv4**
7. **vrrsleader** *group name*
8. **vrrp** *group id* **ip** *ip address*
9. **exit**
10. **interface** *type number*
11. **ip pim redundancy***group name***vrrpdr-priority***priority-value*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**fhrp version vrrp** *version* 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `Device(config)# interface Ethernet0/0`	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address***address* 例： `Device(config-if)# ip address 192.0.2.2`	VRRP グループのプライマリ アドレスまたはセカンダリ アドレスを指定します。
ステップ 6	**vrrp***group id***address-familyipv4** 例： `Device(config-if)# vrrp 1 address-family ipv4`	VRRP グループを作成し、VRRP コンフィギュレーション モードを開始します。
ステップ 7	**vrrsleader** *group name* 例： `Device(config-if-vrrp)# vrrs leader VRRP1`	指定されたネイバーとのコミュニティおよび（または）拡張コミュニティの交換をイネーブルにします。
ステップ 8	**vrrp** *group id* **ip** *ip address* 例： `Device(config-if-vrrp)# vrrp 1 ip 10.1.6.1`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 9	**exit** 例： `Device(config-if-vrrp)# exit`	VRRP コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface Ethernet0/0`	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**ip pim redundancy***group name***vrrpdr-priority***priority-value* 例： `Device(config-if)# ip pim redundancy VRRP1 vrrp dr-priority 90`	ルータが指定ルータ（DR）として選択されるプライオリティを設定します。 • 冗長性の dr-priority 値は、VRRP 認識 PIM 機能でイネーブルにされたすべてのルータの値と同じにする必要があります。
ステップ 12	**end** 例： `Device(config-if)# end`	インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

VRRP 認識 PIM の設定例

例：VRRP 認識 PIM

```
conf terminal
 fhrp version vrrp v3
interface Ethernet0/0
 ip  address 192.0.2.2
 vrrp 1 address-family ipv4

 vrrp 1 ip 10.1.6.1

 vrrs leader VRRP1
interface Ethernet0/0
 ip pim redundancy VRRP1 vrrp  dr-priority 90
 !
```

第 42 章

基本的な IP マルチキャスト ルーティングの設定

- 機能情報の確認，1185 ページ
- 基本的な IP マルチキャスト ルーティングの前提条件，1185 ページ
- 基本的な IP マルチキャスト ルーティングの制約事項，1186 ページ
- 基本的な IP マルチキャスト ルーティングに関する情報，1186 ページ
- 基本的な IP マルチキャスト ルーティングの設定方法，1188 ページ
- 基本的な IP マルチキャスト ルーティングのモニタリングおよびメンテナンス，1196 ページ

機能情報の確認

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

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

基本的な IP マルチキャスト ルーティングの前提条件

次に、基本的な IP マルチキャスト ルーティングを設定するための前提条件を示します。

-
- IP マルチキャスト ルーティングを実行するには、PIM バージョンおよび PIM モードを設定する必要があります。 スイッチはモード設定に従って、マルチキャスト ルーティング テー

ブルを読み込み、直接接続されたLANから受信したマルチキャストパケットを転送します。インターフェイスはPIMデンス モード、スパース モード、またはSM-DMスパース - デンス モードのいずれかに設定できます。

- インターフェイスでPIMをイネーブルにすると、同じインターフェイス上でIGMP処理もイネーブルになります （IPマルチキャスティングに加入するには、マルチキャスト ホスト、ルータ、およびマルチレイヤ デバイスでIGMPが動作している必要があります）。

  複数のインターフェイスでPIMをイネーブルにした場合に、そのほとんどのインターフェイスが発信インターフェイス リストに含まれておらず、IGMPスヌーピングがディセーブルになっている場合は、レプリケーションが増加することにより、発信インターフェイスが回線レートを維持できないこともあります。

関連トピック

基本的な IP マルチキャスト ルーティングの設定, （1188 ページ）

基本的な IP マルチキャスト ルーティングに関する情報, （1186 ページ）

基本的な IP マルチキャスト ルーティングの制約事項

次に、IP マルチキャスト ルーティングの制約事項を示します。

- マルチキャスト ルーティングは Catalyst 3560-CX スイッチでのみサポートされます。

基本的な IP マルチキャスト ルーティングに関する情報

IP マルチキャストは、ネットワーク リソース（特に、音声やビデオなどの帯域幅集約型サービス）を効率的に使用する方法です。 IP マルチキャスト ルーティングにより、ホスト（ソース）は、IP マルチキャスト グループ アドレスと呼ばれる特別な形式の IP アドレスを使用して、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。

送信側ホストは、マルチキャスト グループ アドレスをパケットの IP 宛先アドレス フィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、マルチキャスト グループのメンバーに接続されたすべてのインターフェイスから着信した IP マルチキャストパケットを転送します。 どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。 ただし、グループのメンバだけがメッセージを受信します。

関連トピック

基本的な IP マルチキャスト ルーティングの設定, （1188 ページ）

IP マルチキャスト ルーティングのデフォルト設定, （1187 ページ）

基本的な IP マルチキャスト ルーティングの前提条件, （1185 ページ）

IP マルチキャスト ルーティングのデフォルト設定

次の表に、IP マルチキャスト ルーティングのデフォルト設定を示します。

表 *110* : *IP* マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル
PIM マルチキャスト境界	なし。
候補 BSR	ディセーブル
候補 RP	ディセーブル
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

関連トピック

基本的な IP マルチキャスト ルーティングの設定, （1188 ページ）

基本的な IP マルチキャスト ルーティングに関する情報, （1186 ページ）

sdr リスナー サポート

MBONE は、相互接続された、IP マルチキャスト トラフィックの転送が可能なインターネット ルータおよびホストの小さなサブセットです。 その他のマルチメディア コンテンツも、通常は MBONE を通してブロードキャストされます。 マルチメディア セッションに加入する前に、このセッションで使用されているマルチメディア グループ アドレス、ポート、セッションがアクティブになる時期、およびワークステーションで必要となるアプリケーションの種類（音声、ビデオなど）を把握する必要があります。 この情報は、MBONE Session Directory バージョン 2（sdr）ツールによって提供されます。 このフリーウェア アプリケーションは WWW 上の複数のサイト（http://www.video.ja.net/mice/index.html など）からダウンロードできます。

SDR は、Session Announcement Protocol（SAP）マルチキャスト パケット用の Well-known マルチキャスト グループ アドレスおよびポートを、SAP クライアントから傍受するマルチキャスト アプリケーションです（SAP クライアントは、会議セッションをアナウンスします）。 これらの SAP パケットには、セッションの説明、セッションがアクティブな期間、IP マルチキャスト グループアドレス、メディア形式、担当者、およびアドバタイズされたマルチメディアセッションに関するその他の情報が格納されます。 SAP パケットの情報は、[SDR Session Announcement] ウィンドウに表示されます。

基本的な IP マルチキャスト ルーティングの設定方法

基本的な IP マルチキャスト ルーティングの設定

デフォルトでは、マルチキャスト ルーティングはディセーブルとなっており、モードは設定されていません。

この手順は必須です。

はじめる前に

PIM バージョンと PIM モードを設定する必要があります。 スイッチはモード設定に従って、マルチキャスト ルーティング テーブルを読み込み、直接接続された LAN から受信したマルチキャスト パケットを転送します。

マルチキャスト ルーティング テーブルへのパケット読み込みでは、DM インターフェイスは常にテーブルに追加されます。 SM インターフェイスがテーブルに追加されるのは、ダウンストリーム デバイスから定期的な Join メッセージを受信した場合、またはインターフェイスに直接接続されたメンバーが存在する場合に限ります。 LAN から転送する場合、グループが認識している RP があれば、SM 動作が行われます。 その場合、パケットはカプセル化され、その RP に送信されます。 認識している RP がなければ、パケットは DM 方式でフラッディングされます。 特定の送信元からのマルチキャスト トラフィックが十分であれば、レシーバの先頭ホップルータからその送信元に Join メッセージが送信され、送信元を基点とする配信ツリーが構築されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ 3 インターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッド ポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 また、インターフェイスの IP PIM スパース □ デンスモードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 設定例については、次を参照してください。 例：ルーテッド ポートとしてのインターフェイス設定 • SVI：**interface vlan***vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。 設定例については、次を参照してください。 例：SVI としてのインターフェイスの設定 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**} 例： `Switch(config-if)# ip pim`	インターフェイスで PIM モードをイネーブルにします。 デフォルトで、モードは設定されていません。 キーワードの意味は次のとおりです。 • **dense-mode**：デンス モードの動作をイネーブルにします。

	コマンドまたはアクション	目的
	`sparse-dense-mode`	• **sparse-mode**：スパース モードの動作をイネーブルにします。 SM を設定する場合は、RP も設定する必要があります。 • **sparse-dense-mode**：グループが属するモードでインターフェイスが処理されるようにします。 DM-SM 設定を推奨します。 （注） インターフェイスで PIM をディセーブルにするには、**no ip pim** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

基本的な IP マルチキャスト ルーティングに関する情報, （1186 ページ）
IP マルチキャスト ルーティングのデフォルト設定, （1187 ページ）
基本的な IP マルチキャスト ルーティングの前提条件, （1185 ページ）

オプションの IP マルチキャスト ルーティングの設定

IP マルチキャスト境界の定義

自動 RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。 自動 RP 情報を伝達する 224.0.1.39 および 224.0.1.40 宛てのパケットを拒否するアクセス リストを作成します。

この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **access-list***access-list-number***deny***source* [*source-wildcard*]
4. **interface***interface-id*
5. **ip multicast boundary***access-list-number*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

ステップ 3	**access-list***access-list-number***deny***source* [*source-wildcard*]
	
	例：
	`Switch(config)#`
	`access-list 12 deny 224.0.1.39`
	`access-list 12 deny 224.0.1.40`
		標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。
		• *access-list-number* の範囲は 1 ～ 99 です。
		• **deny** キーワードは、条件が一致した場合にアクセスを拒否します。
		• *source* には、自動 RP 情報を伝達するマルチキャスト アドレス 224.0.1.39 および 224.0.1.40 を入力します。
		• （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。
		
		アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。

	コマンドまたはアクション	目的
ステップ 4	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip multicast boundary***access-list-number* 例： `Switch(config-if)# ip multicast boundary 12`	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義, （1168 ページ）

マルチキャスト VRF の設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチコマンドリファレンスおよび『*Cisco IOS IP Multicast Command Reference*』を参照してください。

Multi-VRF CE 内でのマルチキャスト設定の詳細については、『*IP Routing: Protocol-Independent Configuration Guide, Cisco IOS Release 15S*』を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： `Switch(config)# ip routing`	IP ルーティング モードをイネーブルにします
ステップ 3	**ip vrf***vrf-name* 例： `Switch(config)# ip vrf vpn1`	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd***route-distinguisher* 例： `Switch(config-vrf)# rd 100:2`	ルート識別子を指定して VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `Switch(config-vrf)# route-target import 100:2`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。 AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。 *route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同一にする必要があります。
ステップ 6	**import map***route-map* 例： `Switch(config-vrf)# import map importmap1`	（任意）VRF にルート マップを対応付けます。
ステップ 7	**ip multicast-routing vrf***vrf-name***distributed** 例： `Switch(config-vrf)# ip multicast-routing vrf vpn1 distributed`	（任意）VRF テーブルでグローバル マルチキャスト ルーティングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 8	**interface***interface-id* 例： `Switch(config-vrf)# interface gigabitethernet 1/0/2`	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスはルーテッド ポートまたは SVI に設定できます。
ステップ 9	**ip vrf forwarding***vrf-name* 例： `Switch(config-if)# ip vrf forwarding vpn1`	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 10	**ip address***ip-address***mask** 例： `Switch(config-if)# ip address 10.1.5.1 255.255.255.0`	レイヤ 3 インターフェイスの IP アドレスを設定します。
ステップ 11	**ip pim sparse-dense mode** 例： `Switch(config-if)# ip pim sparse-dense mode`	VRF に関連付けられているレイヤ 3 インターフェイス上で、PIM をイネーブルにします。
ステップ 12	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： `Switch# show ip vrf detail vpn1`	設定を確認します。 設定した VRF に関する情報を表示します。
ステップ 14	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SAP リスナーを使用したマルチキャスト マルチメディア セッションのアドバタイジング

マルチキャストメディア会議やその他のマルチキャストセッションを支援したり、参加予定者に関連セッションの設定情報を通知したりするためにSession Description Protocol と Session Anouncement Protocol、およびアプリケーションを使用する場合は、SAP リスナー サポートをイネーブルにします。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipsapcache-timeout***minutes*
4. **interface***typenumber*
5. **ipsaplisten**
6. **end**
7. **clearipsap** [*group-address* | **“** *session-name* **”**]
8. **showipsap** [*group-address* | **“** *session-name* **”**| **detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipsapcache-timeout***minutes* 例： `Router(config)# ip sap cache-timeout 600`	（任意）SAP キャッシュ エントリがキャッシュ内でアクティブである期間を制限します。 • デフォルトでは、SAP キャッシュ エントリはネットワークから受信された 24 時間後に削除されます。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface ethernet 1`	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 5	**ipsaplisten** 例： `Router(config-if)# ip sap listen`	セッションディレクトリ アナウンスメントをリッスンするソフトウェアをイネーブルにします。
ステップ 6	**end** 例： `Router(config-if)# end`	セッションを終了し、EXEC モードに戻ります。
ステップ 7	**clearipsap** [*group-address* | **“** *session-name* **”**] 例： `Router# clear ip sap "Sample Session"`	SAP キャッシュ エントリまたは SAP キャッシュ全体を削除します。
ステップ 8	**showipsap** [*group-address* | **“** *session-name* **”**| **detail**] 例： `Router# show ip sap 224.2.197.250 detail`	（任意）SAP キャッシュを表示します。

基本的な IP マルチキャスト ルーティングのモニタリングおよびメンテナンス

キャッシュ、テーブル、およびデータベースのクリア

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。 特定のキャッシュ、テーブル、またはデータベースの内容が無効である場合、または無効である可能性がある場合は、これらをクリアする必要があります。

次の表に示す特権 EXEC コマンドのいずれかを使用すると、IP マルチキャストのキャッシュ、テーブル、データベースをクリアできます。

表 *111* : キャッシュ、テーブル、およびデータベースをクリアするコマンド

コマンド	目的
clear ip igmp group {**group** [*hostname* | *IP address*] | **vrf***name***group** [*hostname* | *IP address*] }	IGMP キャッシュのエントリを削除します。
clear ip mroute { ***** | [*hostname* | *IP address*] | **vrf***name***group** [*hostname* | *IP address*] }	IP マルチキャスト ルーティング テーブルからエントリを削除します。
clear ip sap [*group-address* | **"***session-name***"**]	Session Directory Protocol バージョン 2 キャッシュ（sdr キャッシュ）エントリを削除します。

システムおよびネットワーク統計情報の表示

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

（注） このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。 さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

次の表に示す特権 EXEC コマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 *112* : システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
ping [*group-name* | *group-address*]	マルチキャスト グループ アドレスにインターネット制御メッセージ プロトコル（ICMP）エコー要求を送信します。
show ip igmp groups [*group-name*|*group-address*|*type-number*]	スイッチに直接接続され、IGMP によって取得されたマルチキャスト グループを表示します。
show ip igmp interface [*type number*]	インターフェイスのマルチキャスト関連情報を表示します。
show ip mroute [*group-name* | *group-address*] [*source*] [**count** | **interface** | **proxy** | **pruned** | **summary** | **verbose**]	IP マルチキャスト ルーティング テーブルの内容を表示します。

コマンド	目的
show ip pim interface [*type number*] [**count** | **detail** | **df** | **stats**]	PIM に対して設定されたインターフェイスに関する情報を表示します。 このコマンドは、すべてのソフトウェア イメージで使用できます。
show ip pim neighbor [*type number*]	スイッチによって検出された PIM ネイバーのリストを示します。 このコマンドは、すべてのソフトウェア イメージで使用できます。
show ip pim rp [*group-name* | *group-address*]	スパース モードのマルチキャスト グループに関連付けられた RP ルータを表示します。 このコマンドは、すべてのソフトウェア イメージで使用できます。
show ip rpf {*source-address* | *name*}	スイッチのリバース パス転送（RPF）の実行方法（ユニキャスト ルーティング テーブル、DVMRP ルーティング テーブル、またはスタティック マルチキャスト ルーティングのいずれかから）を表示します。 コマンド パラメータは次のとおりです。 • *Host name* または *IP address*：IP 名またはグループ アドレス。 • **Select**：グループ ベースの VRF 選択情報。 • **vrf**：VPN ルーティング/転送インスタンスを選択します。
show ip sap [*group* | **"***session-name***"** | **detail**]	Session Announcement Protocol（SAP）バージョン 2 キャッシュを表示します。 コマンド パラメータは次のとおりです。 • *A.B.C.D*：IP グループ アドレス。 • *WORD*：セッション名（二重引用符で囲む）。 • **detail**：セッションの詳細。

第 43 章

SSM の設定

- 機能情報の確認，1199 ページ
- SSM の設定の前提条件，1199 ページ
- SSM 設定の制約事項，1200 ページ
- SSM および SSM マッピングに関する情報，1201 ページ
- SSM および SSM マッピングの設定方法，1209 ページ
- SSM および SSM マッピングのモニタリング，1219 ページ
- SSM および SSM マッピングの設定例，1220 ページ

機能情報の確認

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

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

SSM の設定の前提条件

次に、Source-Specific Multicast （SSM）および SSM マッピングを設定するための前提条件を示します。

- SSM および SSM マッピングを使用するには、3560-CX スイッチの IP Services フィーチャセットをイネーブルにする必要があります。

- SSM マッピングを設定する前に、次の作業を実行する必要があります。
  - IP マルチキャスト ルーティングをイネーブルにします。
  - PIM スパース モードをイネーブルにします。
  - SSM を設定します。
- スタティック SSM マッピングを設定する場合は、事前にアクセス コントロール リスト（ACL）を設定して、送信元アドレスにマッピングされるグループ範囲を定義する必要があります。
- SSM マッピングを設定し、DNS ルックアップで使用できるようにするには、稼動中の DNS サーバにレコードを追加する必要があります。 稼働中の DNS サーバがない場合は、DNS サーバをインストールする必要があります。

（注） 実行中の DNS サーバにレコードを追加するには、*Cisco Network Registrar* などの製品を使用できます。

SSM 設定の制約事項

次に、SSM を設定する際の制約事項を示します。

- IGMPv3 で SSM を使用するには、Cisco IOS ルータ、アプリケーションが稼働しているホスト、そしてアプリケーション自体が SSM をサポートしている必要があります。
- SSM にまだ対応していないネットワーク内の既存のアプリケーションは、（S, G）チャネルの加入登録をサポートするように変更していない限り、SSM 範囲内では機能しません。 そのため、既存のアプリケーションが指定の SSM 範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題が発生することがあります。
- IGMP スヌーピング：IGMPv3 で使用される新しいメンバーシップ レポート メッセージは、旧型の IGMP スヌーピング スイッチでは正しく認識されない場合があります。
- SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。 Cisco Group Management Protocol（CGMP）、IGMP スヌーピング、または Router-Port Group Management Protocol（RGMP）でサポートされるのはグループ固有のフィルタリングだけであり、（S, G）チャネル固有のフィルタリングはサポートされていません。 同じスイッチド ネットワーク内の異なるレシーバーが異なる（S, G）チャネルを要求し、これらのチャネルが同じグループを共有している場合、レシーバーは上記のような既存メカニズムの利点を活用できません。 どちらのレシーバーも、すべての（S, G）チャネル トラフィックを受信し、不要なトラフィックを入力から除外します。 SSM は、独立した多くのアプリケーションに SSM 範囲のグループ アドレスを再利用できるので、このような状況では、スイッチド ネットワークのトラフィック フィルタリング機能が低下する可能性があります。 そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM 範囲内の 1 つのアドレスがさまざまなアプリケーションに再利用される可能性を小

さくすることが重要です。 たとえば、TV チャネル セットを提供するアプリケーション サービスで、SSM を使用する場合は、各 TV（S, G）チャネルに異なるグループを使用する必要があります。 このようにすれば、同じアプリケーション サービス内の異なるチャネルに複数のレシーバが接続されていても、レイヤ 2 デバイスを含むネットワークでトラフィック エイリアシングが発生しなくなります。

- PIM-SSM では、ラストホップ ルータは、そのインターフェイス上に適切な（S,G）加入登録があると、定期的に（S, G）Join メッセージを送信し続けます。 このため、レシーバが（S, G）加入を送信する限り、ソースが長時間（または二度と）トラフィックを送信しなくてもレシーバからソースへの最短パス ツリー（SPT）状態が維持されます。

  送信元がトラフィックを送信し、レシーバーがグループに加入している場合にだけ（S, G）ステートが維持される PIM-SM では、これとは対照的な状況が発生します。 PIM-SM では、送信元がトラフィックの送信を 3 分以上停止すると、（S, G）ステートは削除され、その送信元からのパケットが RPT を通じて再度到達した場合のみに再確立されます。 PI-SSM では、送信元がアクティブであることをレシーバに通知するメカニズムがないので、レシーバが（S, G）チャネルの受信を要求している限り、（S, G）ステートを維持する必要があります。

次に、SSM マッピングを設定する際の制約事項を示します。

- SSM マッピング機能は、完全な SSM の利点を共有しません。 SSM マッピングでは、ホストからグループ G の加入が取得され、1 つまたは複数のソースに関連付けられているアプリケーションでこのグループを指定できるため、グループ G ごとにこのようなアプリケーション 1 つのみをサポートできます。それにもかかわらず、完全な SSM アプリケーションは、SSM マッピングにも使用される同じグループを共有することができます。
- 完全な SSM への移行ソリューションとして SSM マッピングだけを使用する場合は、ラストホップ ルータの IGMPv3 をイネーブルにする際に十分に注意してください。

SSM および SSM マッピングに関する情報

SSM コンポーネント

SSM は、1 対多のアプリケーション（ブロードキャスト アプリケーション）に最適なデータグラム配信モデルです。

SSM は、オーディオおよびビデオ ブロードキャスト アプリケーション環境を対象とした IP マルチキャスト ソリューションのシスコによって実装されたコア ネットワーキング テクノロジーで、RFC 3569 に説明されています。 次のコンポーネントを組み合わせることで、SSM の実装がサポートされます。

- Protocol Independent Multicast Source-Specific Mode（PIM-SSM）
- インターネット グループ管理プロトコル バージョン 3（IGMPv3）

Protocol Independent Multicast（PIM）SSM（PIM-SSM）は、SSM の実装をサポートするルーティングプロトコルで、PIM スパースモード（PIM-SM）から派生しました。 IGMP は、ホストがルータにマルチキャストグループメンバーシップを伝えるために使用するインターネット技術特別調査委員会（IETF）標準トラック プロトコルです。 IGMP バージョン 3 は、SSM に必要なソースフィルタリングをサポートします。 SSM を IGMPv3 と共に実行するには、SSM が IOS ルータ、アプリケーションが実行されるホスト、およびアプリケーション自体でサポートされる必要があります。

関連トピック

SSM の設定, （1209 ページ）

IGMPv3 を使用した SSM の例, （1220 ページ）

Internet Standard Multicast と SSM の違い

インターネットと多くの企業イントラネットの標準IPマルチキャストインフラストラクチャは、PIM-SM プロトコルと Multicast Source Discovery Protocol（MSDP）に基づいています。 これらのプロトコルは信頼でき、広範で、効率的であることが証明されています。 しかし、インターネット標準マルチキャスト（ISM）サービス モデルの複雑さと機能性の制限があります。 たとえば、ISM では、ネットワークは、実際にマルチキャスト トラフィックを送信しているホストについての情報を維持する必要があります。 SSM では、この情報は IGMPv3 によって最後のホップ デバイスにリレーされた発信元アドレスを介して受信することで提供されます。 SSM は、ISM に関連付けられた問題への対応を強化し、ネットワーク内で ISM 用に開発されたプロトコルと共存することを目的としています。 一般に、SSM は SSM を使用するアプリケーションに IP マルチキャスト サービスを提供します。

ISM サービスは RFC 1112 で定義されています。 このサービスは、任意のソースからマルチキャスト ホスト グループと呼ばれるレシーバのグループへの IP データグラムの配信によって構成されています。 マルチキャスト ホスト グループのデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス S と IP 宛先アドレスとしてのマルチキャスト グループ アドレス G のデータグラムで構成されます。 システムはホスト グループのメンバになることによってこのトラフィックを受信します。 ホスト グループのメンバーシップには IGMP バージョン 1、2、または 3 によるホスト グループのシグナリングが必要です。

SSM では、データグラムは（S, G）チャネルに基づいて配信されます。 1 つの (S, G) チャネルのトラフィックは、IP 宛先アドレスとして IP ユニキャスト ソース アドレス S とマルチキャスト グループ アドレス G を持つデータグラムで構成されています。 システムは、（S, G）チャネルのメンバになることによって、このトラフィックを受信します。 SSM と ISM のどちらでも、ソースになるためにシグナリングは必要ありません。 ただし、SSM では、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために（S, G）への加入または脱退を行う必要があります。 つまり、レシーバは加入した（S, G）チャネルからだけトラフィックを受信できます。 一方、ISM では、レシーバは受信するトラフィックの送信元の IP アドレスを知る必要はありません。 提案されているチャネル加入シグナリングの標準的な方法では、IGMP INCLUDE モード メンバーシップ レポートを使用します。これは、IGMP バージョン 3 でのみサポートされています。

IP マルチキャスト グループ アドレス範囲の設定済みのサブセットに SSM 配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。 インターネット割り当て番号局（IANA）

は、SSM アプリケーションおよびプロトコル用に 232.0.0.0 ～ 232.255.255.255 のアドレス範囲を確保しています。 ソフトウェアでは、224.0.0.0 ～ 239.255.255.255 の IP マルチキャスト アドレス範囲の任意のサブセットの SSM 設定を許可します。 SSM 範囲が定義されると、アプリケーションが明示的な (S, G) チャネル加入登録を使用するように変更されているか、URL Rendezvous Directory（URD）によって SSM に対応していない限り、SSM 範囲内でアドレスを使用しようとする場合に既存の IP マルチキャスト レシーバ アプリケーションはトラフィックを受信しません。

SSM の動作

確立されているネットワークは、IP マルチキャスト サービスが PIM SM に基づいているので、SSM サービスをサポートできます。 ドメイン間の PIM-SM に必要なプロトコルがすべて揃っていないネットワークでも、SSM を単独で導入できます。 つまり、SSM は RP を必要としないため、Auto-RP、MSDP、またはブートストラップ ルータ（BSR）などの RP メカニズムの必要がありません。

SSM がすでに PIM-SM 用に設定済みのネットワークで配備されている場合、ラスト ホップ ルータのみを SSM をサポートするソフトウェア イメージにアップグレードする必要があります。 レシーバに直接接続されていないルータを SSM をサポートするソフトウェア イメージにアップグレードする必要はありません。 一般的に、これらのラスト ホップではないルータは、SSM 範囲で PIM-SM のみを実行する必要があります。 これらは、MSDP シグナリング、登録、または PIM-SM 共有ツリー動作が SSM 範囲内で発生することを抑制するために、追加のアクセス コントロール設定を必要とする場合もあります。

SSM モードの動作は、**ip pim ssm** グローバル コンフィギュレーション コマンドを使用して SSM 範囲を設定することによってイネーブルできます。 この設定による影響は次のとおりです。

- SSM 範囲内のグループの場合、(S, G) チャネル加入は IGMPv3 INCLUDE モード メンバーシップ レポートによって受け入れられます。
- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、PIM (S, G) 加入およびプルーニング メッセージのみがルータによって生成されます。 ランデブー ポイント ツリー（RPT）動作に関連した着信メッセージは無視されるか、拒否され、着信 PIM 登録メッセージは登録停止メッセージによってただちに応答されます。 ラストホップ ルータ以外のルータでは、PIM-SSM は PIM-SM と下位互換性を保ちます。 したがって、ラストホップ ルータ以外のルータは SSM グループに PIM-SM を使用できます（SSM をサポートしていない場合など）。
- SSM 範囲内のグループの場合、SSM 範囲内の MSDP Source-Active（SA）メッセージは受け入れ、生成、または転送されません。

IGMPv3 ホスト シグナリング

IGMPv3 は、ホストがマルチキャスト グループのラスト ホップ ルータにメンバーシップを伝える IETF 標準トラック プロトコルの第 3 バージョンです。 IGMPv3 は、グループ メンバーシップを伝える能力をホストに与えます。これによってソースに関するフィルタリングが可能になります。ホストは、特定のソースを除いて、グループに送信するすべてのソースからトラフィックを受信

したい（EXCLUDE と呼ばれるモード）、またはグループに送信する特定のソースからのみトラフィックを受信したい（INCLUDE と呼ばれるモード）と伝えることができます。

IGMPv3 は、ISM および SSM と同時に動作可能です。 ISM では、EXCLUDE モードと INCLUDE モードの両方のレポートがラストホップルータによって受け入れられます。 SSM では、INCLUDE モード レポートのみがラスト ホップ ルータによって受け入れられます。

の利点

IP マルチキャスト アドレス管理が不要

ISM サービスで、トラフィック ディストリビューションは使用する IP マルチキャスト グループ アドレスにのみ基づくため、アプリケーションは一意の IP マルチキャスト グループ アドレスを取得する必要があります。 異なるソースとレシーバを持つ 2 つのアプリケーションが同じ IP マルチキャスト グループ アドレスを使用すると、両方のアプリケーションのレシーバが両方のアプリケーションのソースからトラフィックを受信します。 適切にプログラムしている場合、レシーバは不要なトラフィックをフィルタできますが、この状態は一般的に許容できないレベルの不要なトラフィックを生み出します。

アプリケーションへの一意の IP マルチキャスト グループ アドレスの割り当ては問題となります。最も短期のアプリケーションはセッション記述プロトコル（SDP）やセッション通知プロトコル（SAP）のようなメカニズムを使用して、ランダムアドレスを取得します。これは、インターネット内のアプリケーションの増加によってうまく機能しないソリューションです。 長期アプリケーションの現在のベストソリューションは、RFC 2770 に説明されていますが、このソリューションは各自律システムが 255 の使用可能な IP マルチキャスト アドレスのみに限定される制限の影響を受けます。

SSM で、他のソースからのトラフィックとは関係なく、各ソースからのトラフィックはネットワーク内のルータ間で転送されます。 このため、異なるソースが SSM 範囲のマルチキャスト グループ アドレスを再利用できます。

望ましくないソースからの DoS 攻撃を防ぐ

SSM で、個別の各ソースからのマルチキャスト トラフィックは、（IGMPv3、IGMP v3lite または URD メンバーシップによって）レシーバから要求された場合にのみネットワーク中に転送されます。 これに対し、ISM はマルチキャスト グループに送信するアクティブなソースからそのマルチキャスト グループを要求するすべてのレシーバにトラフィックを転送します。 インターネット ブロードキャストアプリケーションで、トラフィックを同じマルチキャストグループにただ送信するだけで、望ましくないソースが実際のインターネットブロードキャスト ソースを簡単に妨害できるため、この ISM の動作は非常に望ましくありません。 この状況は、レシーバ側で不要なトラフィックによって帯域幅を消耗させるため、インターネット ブロードキャストの無停止の受信を妨害します。 SSM では、トラフィックをマルチキャスト グループにただ送信するだけでは、このような種類の DoS 攻撃は行えません。

導入と管理が容易

ネットワークがマルチキャスト グループに送信しているアクティブ ソースについての情報を維持する必要がないため、SSM は簡単にインストールし、ネットワークでプロビジョニングできます。 この要件は、（IGMPv1、IGMPv2、または IGMPv3 を使用する）ISM でのみ存在します。

ISM サービスの現在の標準ソリューションは PIM-SM と MSDP です。 PIM-SM（Auto-RP または BSR の必要性を含む）および MSDP での Rendezvous Point（RP）管理は、ネットワークがアクティブ ソースについて学習するためにのみ必要です。 この管理は SSM では必要ありません。このため、SSM は ISM よりインストールや管理が簡単で、配備での動作面の拡張も ISM より簡単です。SSM のインストールが簡単であるその他の要素は、既存の PIM-SM ネットワークを活用でき、ラスト ホップ ルータをアップグレードするだけで IGMPv3、IGMP v3lite、または URD をサポートできる点です。

インターネット ブロードキャスト アプリケーションに最適

上記の 3 つの利点により、次の理由で SSM はインターネット ブロードキャスト スタイルのアプリケーションに理想的です。

- 一意の IP マルチキャスト アドレスなしで SSM によって、インターネット ブロードキャスト サービスを提供できるため、コンテンツ プロバイダーはサービスを簡単に提供できます（コンテンツ プロバイダーにとって、IP マルチキャスト アドレス割り当てはこれまで深刻な問題でした）。
- インターネットブロードキャストサービスは多数のレシーバに公開されることにより、DoS 攻撃の最も一般的な対象となるため、このような攻撃の阻止はインターネットブロードキャスト サービスの重要な要素です。
- SSM はインストールや動作が簡単なため、特に、コンテンツを複数の独立した PIM ドメイン間で転送する必要のある場合（SSM のために PIM ドメイン間で MSDP を管理する必要がないため）、ネットワーク オペレータにとって理想的です。

SSM マッピングの概要

管理上または技術上の理由によりエンド システム上で SSM をサポートすることができない、または望ましくない場合、SSM マッピングは SSM 移行をサポートします。 SSM を使用して IGMPv3 をサポートしていないレガシー STB に対して、ライブ ストリーミング ビデオを提供することは、SSM マッピングの一般的な応用例です。

典型的な STB 配置では、各 TV チャネルは独立した 1 つの IP マルチキャスト グループを使用し、その TV チャネルの送信を行うアクティブなサーバは 1 つです。 1 つのサーバから複数の TV チャネルへの送信は可能ですが、各チャネルのグループはそれぞれ異なります。 このようなネットワーク環境で、ルータが特定のグループ G の IGMPv1 または IGMPv2 のメンバーシップ レポートを受信した場合、レポートの宛先は暗黙的に、そのマルチキャスト グループに関連付けられている TV チャネルの well-known TV サーバになります。

SSM マッピングは、グループに送信しているソースをラスト ホップ ルータで検出する手段を提供します。 SSM マッピングが設定されている場合、特定のグループ G の IGMPv1 または IGMPv2

のメンバーシップ レポートを受信したルータは、レポートを、このグループに関連付けられている既知のソースの 1 つ以上の (S, G) チャネル メンバーシップに変換します。

（注）

ルータはグループ G の IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、SSM マッピングを使用して、グループ G の 1 つ以上のソース IP アドレスを決定します。その後、SSM マッピングは IGMPv3 レポートの INCLUDE (G, [S1, G], [S2, G]...[Sn, G]) に従ってメンバーシップ レポートを変換し、IGMPv3 レポートを受信したときと同様に続行します。 ルータ は、IGMPv1 または IGMPv2 メンバーシップ レポートを受信し続ける限り、さらに、グループの SSM マッピングが変更されない限り、PIM Join を（S1, G）から（Sn, G）までに送信し、これらのグループに加入し続けます。 このため、SSM マッピングにより、IGMPv3 が未サポートであるレガシー STB への映像配信や、IGMPv3 ホスト スタックを利用しないアプリケーションに SSM を活用できます。

SSM マッピング機能を使用すると、ラスト ホップ ルータはスタティックに設定されたルータ上のテーブルまたは DNS サーバへの問い合わせを通じて、ソース アドレスを決定できます。 スタティックに設定されたテーブルが変更された場合や、DNS マッピングが変更された場合、ルータは、現在のソースを加入したグループに関連付けたままにします。

スタティック SSM マッピング

SSM スタティック マッピングを使用して、スタティック マップを使用してグループに送信するソースを決定するようにラスト ホップ ルータを設定できます。 スタティック SSM マッピングを使用するには、グループ範囲を定義するアクセス リスト（ACL）を設定する必要があります。 これらの ACL によって許可されたグループを **ipigmpstaticssm-map** グローバル コンフィギュレーション コマンドを使用してソースにマッピングできます。

DNS が必要ない小規模なネットワークで、または一時的に不正確になった DNS マッピングをローカルに上書きするために、スタティック SSM マッピングを設定できます。 設定されたスタティック SSM マッピングは、DNS マッピングよりも優先されます。

関連トピック

スタティック SSM マッピングの設定, （1211 ページ）

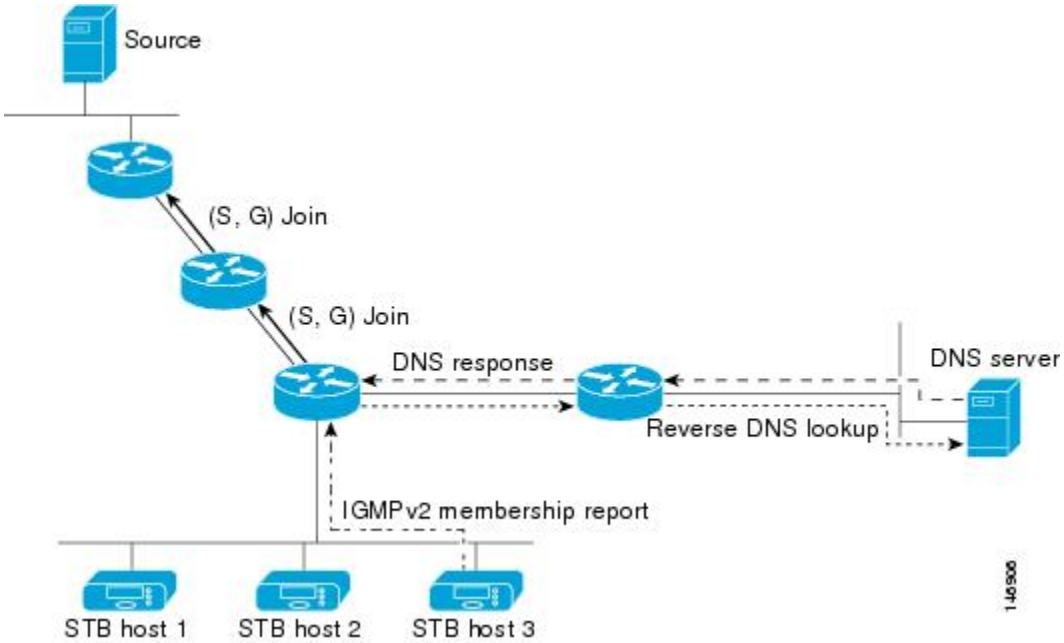
SSM マッピングの設定と動作の確認, （1217 ページ）

DNS ベースの SSM マッピング

DNS ベースの SSM マッピングを使用して、逆 DNS ルックアップを実行してグループを送信するソースを決定するようにラスト ホップ ルータを設定できます（次の図を参照）。 DNS ベースの SSM マッピングが設定されると、ルータはグループ アドレス G を含むドメイン名を構築し、DNS への逆ルックアップを実行します。 ルータにより、この構築されたドメイン名に戻される IP アドレス リソース レコード（IP ARR）がルックアップされ、戻された IP アドレスが、このグループに関連付けられるソース アドレスとして使用されます。 SSM マッピングでサポートできる送信

元の数は、グループごとに最大 20 です。 ルータは各グループに設定されているすべてのソースに加入します。

図 *83*：*DNS* ベースの *SSM* マッピング



ラスト ホップ ルータが 1 つのグループの複数のソースに加入できるようにする SSM マッピング メカニズムを使用すると、TV ブロードキャストのソース冗長性を提供できます。 このコンテキストでは、同じ TV チャネルで 2 つのビデオ ソースに加入するために、SSM マッピングを使用しているラスト ホップ ルータによって、冗長性が提供されます。 ただし、ラスト ホップ ルータでのビデオ トラフィックの重複を防ぐため、ビデオ ソースは、サーバ側のスイッチオーバー メカニズム（1 つのビデオ ソースがアクティブになる間、残りのバックアップ ビデオ ソースがパッシブになる）を使用する必要があります。 パッシブの送信元は待機状態になり、アクティブな送信元の障害が検出された場合に、その TV チャネルにビデオ トラフィックを送信します。 このため、サーバ側のスイッチオーバー メカニズムによって、1 台のサーバだけが TV チャネルにビデオ トラフィックを実際に送信するようになります。

G1、G2、G3、G4 を含むグループ G について 1 つ以上のソース アドレスをルックアップするには、次の DNS リソース レコード（RR）を DNS サーバで設定する必要があります。

G4.G3.G2.G1 [*multicast-domain*] [*timeout*]	IN A *source-address-1*
	IN A*source-address-2*
	IN A*source-address-n*

multicast-domain 引数は、設定可能な DNS プレフィックスです。 デフォルト DNS プレフィックスは、in-addr.arpa です。 インストールがインターネットから切り離されている場合、またはマッピ

ングするグループ名が自分の所有するグローバル スコープのグループ アドレス（SSM 用に設定する RFC 2770 タイプのアドレス）である場合にだけ、デフォルトのプレフィックスを使用します。

timeout 引数は、SSM マッピングを実行しているルータが DNS ルックアップをキャッシュする時間を設定します。 この引数はオプションで、エントリが設定されているゾーンのタイムアウトのデフォルトです。 タイムアウトは、ルータがこのグループについて DNS サーバに問い合わせるまで、現在のマッピングを保持する期間を示します。 タイムアウトは DNS RR エントリのキャッシュ時間から導出され、DNS サーバでグループ/ソースごとに設定できます。 ルータによって生成される DNS クエリー数を最小にする場合は、この時間に大きな値を設定します。 新しいソース アドレスですべてのルータを早く更新する場合は、この時間に小さな値を設定します。

（注） DNS RR の設定に関する詳細については、DNS サーバのマニュアルを参照してください。

ソフトウェアで DNS ベースの SSM マッピングを設定するには、いくつかのグローバル コマンドを設定する必要がありますが、チャネルごとに特定の設定をする必要はありません。 追加チャネルが追加された場合も、SSM マッピングの設定は変更しません。 DNS ベースの SSM マッピングが設定されるときに、1 つまたは複数の DNS サーバによって、マッピングが全体的に処理されます。 DNS ベースの SSM マッピングで、設定および冗長性管理に使用されるすべての DNS テクニックを必要なエントリに適用できます。

関連トピック

DNS ベースの SSM マッピングの設定, （1213 ページ）
SSM マッピングを使用したスタティック トラフィック転送の設定, （1215 ページ）

SSM マッピングの利点

- SSM マッピング機能は、IGMPv3 に基づく純粋な SSM ソリューションと同じくらいに、ネットワーク導入および管理を簡単にします。 SSM マッピングをイネーブルにするために、いくつかの追加設定が必要です。
- SSM の利点である DoS 攻撃の禁止は、SSM マッピングの設定時に適用されます。 SSM マッピングを設定した場合、まだ DoS 攻撃に対して脆弱な唯一のネットワーク セグメントが、ラスト ホップ ルータに接続された LAN のレシーバになります。 これらのレシーバはまだ IGMPv1 および IGMPv2 を使用しているため、同じ LAN 上の不要なソースからの攻撃に対して脆弱です。 ただし、SSM マッピングは、ネットワーク上のあらゆる不要なソースからのマルチキャスト トラフィックからこれらのレシーバ（およびそれらに繋がるネットワーク パス）を保護します。
- SSM マッピングを使用したネットワーク内でのアドレスの割り当てには、調整が必要ですが、ネットワークからのコンテンツが他のネットワークに転送される場合でも、外部認証局からの割り当ては必要ではありません。

SSM および SSM マッピングの設定方法

SSM の設定

SSM を設定するには、次の手順を実行します。

この手順は任意です。

はじめる前に

Source Specific Multicast（SSM）範囲の定義にアクセス リストを使用する場合、**ip pim ssm** コマンドでアクセス リストを参照する前にアクセス リストを設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip pim ssm** [**default** | **range***access-list*]
4. **interface***type number*
5. **ip pim** {**sparse-mode** | **sparse-dense-mode**}
6. **ip igmp version 3**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim ssm** [**default**	**range***access-list*] 例： `Switch(config)# ip pim ssm range 20`	IP マルチキャスト アドレスの SSM 範囲を定義します。

	コマンドまたはアクション	目的
ステップ 4	**interface***type number* 例： `Switch(config)# interface gigabitethernet 1/0/1`	IGMPv3 をイネーブルに設定可能なホストに接続されているインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip pim {sparse-mode | sparse-dense-mode}** 例： `Switch(config-if)# ip pim sparse-dense-mode`	インターフェイスに対して PIM をイネーブルにします。 スパース モードまたはスパース — デンス モードのどちらかを使用する必要があります。
ステップ 6	**ip igmp version 3** 例： `Switch(config-if)# ip igmp version 3`	このインターフェイス上で IGMPv3 をイネーブルにします。 デフォルトでは、IGMP のバージョン 2 が設定されます。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

SSM コンポーネント，（1201 ページ）
IGMPv3 を使用した SSM の例，（1220 ページ）

SSM マッピングの設定

スタティック SSM マッピングの設定

スタティック SSM マッピングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipigmpssm-mapenable**
4. **noipigmpssm-mapquerydns**
5. **ipigmpssm-mapstatic***access-listsource-address*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ipigmpssm-mapenable** 例： `Switch(config)# ip igmp ssm-map enable`	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。 （注） このコマンドでは、デフォルトで、DNS ベースの SSM マッピングがイネーブルにされます。
ステップ 4	**noipigmpssm-mapquerydns** 例： `Switch(config)# no ip igmp ssm-map query dns`	（任意）DNS ベースの SSM マッピングをディセーブルにします。 （注） スタティック SSM マッピングだけを使用する場合は、DNS ベースの SSM マッピングをディセーブルにします。デフォルトでは、**ipigmpssm-map** コマンドによって DNS ベースの SSM マッピングがイネーブルになります。

	コマンドまたはアクション	目的
ステップ 5	**ipigmpssm-mapstatic***access-listsource-address* 例： `Switch(config)# ip igmp ssm-map static 11 172.16.8.11`	スタティック SSM マッピングを設定します。 • *access-list* 引数に入力した ACL によって、*source-address* 引数に入力したソース IP アドレスにマッピングされるグループが決まります。 （注） 追加のスタティック SSM マッピングを設定することもできます。 SSM マッピングを追加設定した場合、ルータが SSM 範囲のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、スイッチは、設定されている各 **ipigmpssm-mapstatic** コマンドに基づいて、そのグループに関連付けられている送信元アドレスを決定します。 スイッチは各グループに最大 20 の送信元を関連付けます。 必要な場合は、ステップを繰り返して、追加のスタティック SSM マッピングを設定します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

スタティック SSM マッピング，（1206 ページ）

DNS ベースの SSM マッピングの設定

DNS ルックアップを実行してグループに送信を実行しているソースの IP アドレスを認識するよう、ラスト ホップ ルータを設定する場合は、この作業を実行します。

はじめる前に

- このタスクを実行する前に、IPマルチキャストルーティングをイネーブルにし、PIM スパース モードをイネーブルにし、SSM を設定します。
- SSM マッピングを設定し、DNS ルックアップで使用できるようにするためには、実行中の DNS サーバにレコードを追加できるようになる必要があります。 稼働中の DNS サーバがない場合は、DNS サーバをインストールする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipigmpssm-mapenable**
4. **ipigmpssm-mapquerydns**
5. **ipdomainmulticast***domain-prefix*
6. **ipname-server***server-address1* [*server-address2...server-address6*]
7. 必要に応じて、ステップステップ 6, （1214 ページ）を繰り返し、追加の DNS サーバを設定して冗長構成にします。
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ipigmpssm-mapenable** 例： `Switch(config)# ip igmp ssm-map enable`	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。
ステップ 4	**ipigmpssm-mapquerydns** 例： `Switch(config)# ip igmp ssm-map query dns`	（任意）DNS ベースの SSM マッピングをイネーブルにします。 • デフォルトでは、**ipigmpssm-map** コマンドによって DNS ベースの SSM マッピングがイネーブルになります。 実行コンフィギュレーションに保存されるのは、このコマンドを **no** 形式で使用した場合だけです。 （注） DNS ベースの SSM マッピングがディセーブルの場合、このコマンドを使用して DNS ベースの SSM マッピングを再度イネーブルにします。
ステップ 5	**ipdomainmulticast***domain-prefix* 例： `Switch(config)# ip domain multicast ssm-map.cisco.com`	（任意）が DNS ベースの SSM マッピングに使用するドメイン プレフィックスを変更します。 • デフォルトでは、ip-addr.arpa ドメイン プレフィックスが使用されます。
ステップ 6	**ipname-server***server-address1* [*server-address2...server-address6*] 例： `Switch(config)# ip name-server 10.48.81.21`	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。
ステップ 7	必要に応じて、ステップステップ 6, （1214 ページ）を繰り返し、追加の DNS サーバを設定して冗長構成にします。	--
ステップ 8	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

DNS ベースの SSM マッピング，（1206 ページ）

SSM マッピングを使用したスタティック トラフィック転送の設定

ラスト ホップ ルータ上の SSM マッピングでスタティック トラフィック転送を設定する場合は、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp static-group***group-address***source ssm-map**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	SSM マッピングを使用してマルチキャスト グループにスタティックにトラフィックを転送するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 （注） SSM マッピングを使用したトラフィックのスタティック転送は、DNS ベースの SSM マッピングとスタティックに設定された SSM マッピングのいずれかで機能します。
ステップ 4	**ip igmp static-group***group-address***source ssm-map** 例： `Switch(config-if)# ip igmp static-group 239.1.2.1 source ssm-map`	そのインターフェイスから（S, G）チャネルへのスタティック転送用の SSM マッピングを設定します。 このコマンドは、特定グループに SSM トラフィックをスタティックに転送する場合に使用します。 チャネルの送信元アドレスを決定するには DNS ベースの SSM マッピングを使用します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

DNS ベースの SSM マッピング，（1206 ページ）

SSM マッピングの設定と動作の確認

SSM マッピングの設定と動作を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **showipigmpssm-mapping**
3. **showipigmpssm-mapping***group-address*
4. **showipigmpgroups** [*group-name* | *group-address* | *interface-typeinterface-number*] [**detail**]
5. **showhost**
6. **debugipigmp***group-address*

手順の詳細

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

ステップ 2	**showipigmpssm-mapping**
	
	例：
	
	`Switch# show ip igmp ssm-mapping`
	`SSM Mapping  : Enabled`
	`DNS Lookup  : Enabled`
	`Mcast domain : ssm-map.cisco.com`
	`Name servers : 10.0.0.3`
	`10.0.0.4`
		（任意）SSM マッピングの設定に関する情報を表示します。

ステップ 3	**showipigmpssm-mapping***group-address*
	
	例：
	
	`Switch# show ip igmp ssm-mapping 232.1.1.4`
	`Group address: 232.1.1.4`
	`Database  : DNS`
	`DNS name  : 4.1.1.232.ssm-map.cisco.com`
	`Expire time  : 860000`
	`Source list  : 172.16.8.5`
	`: 172.16.8.6`
		（任意）SSM マッピングが特定のグループに使用するソースを表示します。
		
		次に、設定済みの DNS ベースの SSM マッピングに関する情報の例を示します。 ルータはソース 172.16.8.5 および 172.16.8.6 にグループ 232.1.1.4 をマッピングする DNS ベースのマッピングを使用しています。 このエントリのタイムアウトは、860000 ミリ秒（860 秒）です。

ステップ 4	**showipigmpgroups** [*group-name* | *group-address* | *interface-typeinterface-number*] [**detail**] 例： `Switch# show ip igmp group 232.1.1.4 detail`	（任意）ルータに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。 この例の「M」フラグは、SSM マッピングが設定されることを示します。

	コマンドまたはアクション	目的

	`Interface: GigabitEthernet2/0/0`
	`Group: 232.1.1.4 SSM`
	`Uptime: 00:03:20`
	`Group mode: INCLUDE`
	`Last reporter: 0.0.0.0`
	`CSR Grp Exp: 00:02:59`
	`Group source list: (C - Cisco Src Report, U - URD, R - Remote, S - Static, M - SSM Mapping)`
	`Source Address Uptime v3 Exp CSR Exp Fwd Flags`
	`172.16.8.3 00:03:20 stopped 00:02:59 Yes CM`
	`172.16.8.4 00:03:20 stopped 00:02:59 Yes CM`
	`172.16.8.5 00:03:20 stopped 00:02:59 Yes CM`
	`172.16.8.6 00:03:20 stopped 00:02:59 Yes CM`	

ステップ 5	**showhost**
	
	例：
	`Switch# show host`
	`Default domain is cisco.com`
	`Name/address lookup uses domain service`
	`Name servers are 10.48.81.21`
	`Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate`
	`temp - temporary, perm - permanent`
	`NA - Not Applicable None - Not defined`
	`Host Port Flags Age Type Address(es)`
	`10.0.0.0.ssm-map.cisco.c None (temp, OK) 0 IP 172.16.8.5`
	`172.16.8.6`
	`172.16.8.3`
		（任意）デフォルト ドメイン名、名前のルックアップ サービスのスタイル、ネーム サーバ ホストのリスト、および、ホスト名とアドレスのキャッシュにあるリストを表示します。

ステップ 6	**debugipigmp***group-address*
	
	例：
	`Switch# debug ip igmp`
	`IGMP(0): Convert IGMPv2 report (*,232.1.2.3) to IGMPv3 with 2 source(s) using STATIC.`
	`Switch# debug ip igmp`
	`IGMP(0): Convert IGMPv2 report (*,232.1.2.3) to IGMPv3 with 2 source(s) using DNS.`
	`Switch# debug ip igmp`
	`IGMP(0): DNS source lookup failed for (*, 232.1.2.3), IGMPv2 report failed`
		（任意）受信および送信した IGMP パケットとホスト関連イベントを表示します。
		
		最初の例の出力は、ルータによってグループ G の IGMPv2 加入が IGMPv3 加入に変換されていることを示しています。
		
		2 番目の例の出力は、DNS ルックアップが成功したことを示しています。
		
		3 番目の例の出力は、DNS ベースの SSM マッピングがイネーブルで、DNS ルックアップが失敗したことを示しています。

関連トピック

スタティック SSM マッピング，（1206 ページ）

SSM および SSM マッピングのモニタリング

SSM のモニタリング

SSM をモニタするには、必要に応じて特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Switch#` **show ip igmp groups detail**	IGMPv3 で（S,G）チャネル加入を表示します。
`Switch#` **show ip mroute**	マルチキャスト グループが SSM サービスをサポートしているかどうか、または送信元固有のホスト レポートが受信されたかどうかを表示します。

SSM マッピングのモニタリング

SSM マッピングをモニタするには、次の表の特権 EXEC コマンドを使用します。

表 ***113*** : ***SSM*** マッピングをモニタするコマンド

コマンド	目的
Switch# **show ip igmp ssm-mapping**	SSM マッピングについての情報を表示します。
Switch#**show ip igmp ssm-mapping***group-address*	SSMマッピングが特定のグループに使用する送信元を表示します。
Switch#**show ip igmp groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]	ルータに直接接続されているレシーバとIGMPによって学習されたレシーバを持つマルチキャスト グループを表示します。
Switch#**show host**	デフォルトのドメイン名、名前ルックアップサービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。

コマンド	目的
Switch#**debug ip igmp***group-address*	送受信された IGMP パケットと IGMP ホスト関連イベントを表示します。

SSM および SSM マッピングの設定例

IGMPv3 を使用した SSM の例

次に、SSM 用に（IGMPv3 を実行する）デバイスを設定する例を示します。

```
ip multicast-routing
!
interface GigabitEthernet3/1/0
 ip address 172.21.200.203 255.255.255.0
 description backbone interface
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-mode
 description ethernet connected to hosts
 ip igmp version 3
!
ip pim ssm default
```

関連トピック

SSM の設定, （1209 ページ）

SSM コンポーネント, （1201 ページ）

SSM フィルタリングの例

次に、SSM ルーティングをサポートしないソフトウェア リリースを実行しているレガシー RP ルータでフィルタリングを設定する例を示します。 このフィルタリングは SSM 範囲で不要な PIM-SM および MSDP トラフィックをすべて抑制します。 このフィルタリングがなくても SSM は動作しますが、レガシーのファースト ホップ ルータとラスト ホップ ルータがネットワークに存在する場合、追加の RPT トラフィックがある場合があります。

```
ip access-list extended  no-ssm-range
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM range
  permit ip any any
! Deny registering in SSM range
ip pim accept-register list no-ssm-range
ip access-list extended msdp-nono-list
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM Range
  ! .
  ! .
  ! .
  ! See ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt for other SA
  ! messages that typically need to be filtered.
  permit ip any any
! Filter generated SA messages in SSM range. This configuration is only needed if there
! are directly connected sources to this router. The “ip pim accept-register” command
```

```
! filters remote sources.
ip msdp redistribute list msdp-nono-list
! Filter received SA messages in SSM range. "Filtered on receipt" means messages are
! neither processed or forwarded. Needs to be configured for each MSDP peer.
ip msdp sa-filter in msdp-peer1 list msdp-nono-list
! .
! .
! .
ip msdp sa-filter in msdp-peerN list msdp-nono-list
```

SSM マッピングの例

次に、SSMマッピング用にルータを設定する設定例を示します。 この例では、機能間の互換性を示すために、他の IGMP および SSM 設定オプションの範囲も示します。 例で使用されている機能のすべてを理解していない場合、この設定例をモデルとして使用しないでください。

（注） グローバル SSM 範囲 232.0.0.0/8 のアドレス割り当てはランダムです。 この設定例の一部またはすべてをコピーする場合、この例で示されているように、232.1.1.x ではなくランダム アドレス範囲を選択してください。 ランダムなアドレス範囲を使用することで、SSM マッピングの使用時に他の SSM の内容をインポートしたときに、アドレスの衝突が発生する可能性を最小限に抑え、競合を防ぐことができます。

```
!
no ip domain lookup
ip domain multicast ssm.map.cisco.com
ip name-server 10.48.81.21
!
!
ip multicast-routing distributed
ip igmp ssm-map enable
ip igmp ssm-map static 10 172.16.8.10
ip igmp ssm-map static 11 172.16.8.11
!
!
.
.
.
!
interface GigabitEthernet0/0/0
 description Sample IGMP Interface Configuration for SSM-Mapping Example
 ip address 10.20.1.2 255.0.0.0
 ip pim sparse-mode
 ip igmp last-member-query-interval 100
 ip igmp static-group 232.1.2.1 source ssm-map
 ip igmp version 3
 ip igmp explicit-tracking
 ip igmp limit 2
 ip igmp v3lite
 ip urd
!
.
.
.
!
ip pim ssm default
!
access-list 10 permit 232.1.2.10
access-list 11 permit 232.1.2.0 0.0.0.255
!
```

次の表で、SSM マッピング設定例に示されている重要なコマンドについて説明します。

表 *114* : *SSM* マッピングの設定例で使用されているコマンドの説明

コマンド	説明
noipdomainlookup	IP DNS に基づいたホスト名からのアドレス変換をディセーブルにします。 （注） **noipdomain-list** コマンドは、IP DNS ベースのホスト名/アドレス間変換をディセーブルにすることにより、SSM マッピングの設定に矛盾が生じないことを示すためにのみ、設定に表示されます。 このコマンドがイネーブルの場合、Cisco IOS XE ソフトウェアは、ホスト名として未知の文字列の解決を試みます。
ipdomainmulticastssm-map.cisco.com	SSM マッピングのドメイン プレフィックスとして ssm-map.cisco.com を指定します。
ipname-server10.48.81.21	SSM マッピングおよび DNS が利用されるソフトウェアの他のすべてのサービスで使用される DNS サーバの IP アドレスとして、10.48.81.21 を指定します。
ipmulticast-routing	IP マルチキャスト ルーティングをイネーブルにします。
ipigmpssm-mapenable	SSM マッピングをイネーブルにします。
ipigmpssm-mapstatic10172.16.8.10	ソース アドレス 172.16.8.10 を使用するよう、ACL 10 によって許可されるグループを設定します。 • この例では、ACL 10 によって、232.1.2.10 を除く 232.1.2.0/25 範囲ですべてのグループが許可されます。
ipigmpssm-mapstatic11172.16.8.11	ソース アドレス 172.16.8.11 を使用するよう、ACL 11 によって許可されるグループを設定します。 • この例では、ACL 11 によって、グループ 232.1.2.10 が許可されます。
ippimsparse-mode	PIM スパース モードをイネーブルにします。

コマンド	説明
ipigmplast-member-query-interval100	IGMPv2 ホストの脱退遅延を減らします。 （注） このコマンドは、SSM マッピングの設定には必要ではありません。ただし、SSM マッピングに依存している IGMPv2 ホストでは、このコマンドは効果的です。
ipigmpstatic-group232.1.2.1sourcessm-map	グループ 232.1.2.1 に関連付けられているソースを特定するために使用されるよう、SSMマッピングを設定します。 その結果得られる (S, G) チャネルは、静的に転送されます。
ipigmpversion3	このインターフェイス上で IGMPv3 をイネーブルにします。 （注） このコマンドは、IGMPv3 が SSM マッピングと同時に設定できることを示すためにのみ、設定で使用されますが、必須ではありません。
ipigmpexplicit-tracking	マルチキャスト チャネルから脱退する IGMPv3 ホストの脱退遅延を最小限に抑えます。 （注） このコマンドは、SSM マッピングの設定には必要ではありません。
ipigmplimit2	1 つのインターフェイス当たりのベースで、IGMP メンバーシップ状態から生じる IGMP 状態の数を制限します。 （注） このコマンドは、SSM マッピングの設定には必要ではありません。
ipigmpv3lite	このインターフェイスで IGMP v3lite メンバーシップ レポートの受け入れと処理をイネーブルにします。 （注） このコマンドは、IGMP v3lite が SSM マッピングと同時に設定できることを示すためにのみ、設定で使用されますが、必須ではありません。

コマンド	説明
ipurd	インターフェイスで確保された URD ポート 465 に送信された TCP パケットの代行受信と URD チャネル加入レポートの処理をイネーブルにします。 （注） このコマンドは、URD が SSM マッピングと同時に設定できることを示すためにのみ、設定で使用されますが、必須ではありません。
ippimssmdefault	SSM サービスを設定します。 • **default** キーワードは SSM 範囲のアクセスリストを 232/8 と定義します。
access-list10permit232.1.2.10 **access-list11permit232.1.2.00.0.0.255**	スタティック SSM マッピングに使用されるよう、ACL を設定します。 （注） これらは、この設定例で **ipigmpssm-mapstatic** コマンドによって参照される ACL です。

DNS サーバの設定例

DNS ベースの SSM マッピングを設定するには、DNS サーバ ゾーンを作成するか、または既存のゾーンにレコードを追加する必要があります。 DNS ベースの SSM マッピングを使用しているルータで、SSM マッピング以外の目的で DNS も使用している場合、通常設定の DNS サーバを使用する必要があります。 そのルータで使用されている DNS 実装が DNS ベースの SSM マッピングだけの場合は、ルート ゾーンが空であるか、またはそれ自身を指すような疑似 DNS セットアップが可能です。

次に、ゾーンを作成し、Network Registrar を使用してゾーン データをインポートする例を示します。

```
Router> zone 1.1.232.ssm-map.cisco.com. create primary file=named.ssm-map
100 Ok
Router> dns reload
100 Ok
```

次に、BIND 8 の named.conf ファイルからゾーン ファイルをインポートする例を示します。

```
Router> ::import named.conf /etc/named.conf
Router> dns reload
100 Ok:
```

（注） ネットワーク レジストラ バージョン 8.0 およびそれ以降では、インポート BIND 8 形式の定義がサポートされます。

第 44 章

IGMP スヌーピングおよびマルチキャスト VLAN レジストレーションの設定

- 機能情報の確認，1227 ページ
- IGMP スヌーピングおよび MVR の設定の前提条件，1227 ページ
- IGMP スヌーピングおよび MVR の設定の制約事項，1228 ページ
- IGMP スヌーピングおよび MVR に関する情報，1230 ページ
- IGMP スヌーピングおよび MVR の設定方法，1241 ページ
- IGMP スヌーピングおよび MVR のモニタリング，1275 ページ
- IGMP スヌーピングおよび MVR の設定例，1278 ページ

機能情報の確認

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

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

IGMP スヌーピングおよび MVR の設定の前提条件

IGMP スヌーピングの前提条件

IGMP スヌーピング クエリアを設定するときには、次の注意事項を順守します。

- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。 IGMP スヌーピング クエリアは、イネーブルの場合この IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。 グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN スイッチ仮想インターフェイス（SVI）IP アドレス（存在する場合）の使用を試みます。 SVI IP アドレスが存在しない場合、スイッチはスイッチ上で設定された利用可能な最初の IP アドレスを使用します。 利用可能な最初の IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。 IGMP スヌーピング クエリアはスイッチ上で利用可能な IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
- IGMP スヌーピング クエリアは IGMP バージョン 1 および 2 をサポートします。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアはネットワークにマルチキャスト ルータの存在を検出すると、非クエリア ステートになります。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアは操作上、次の状況でディセーブル ステートになります。
  - IGMP スヌーピングが VLAN でディセーブルの場合
  - PIM が、VLAN に対応する SVI でイネーブルの場合

関連トピック

IGMP スヌーピング クエリアの設定, （1257 ページ）

IGMP スヌーピング, （1230 ページ）

MVR の前提条件

マルチキャスト VLAN レジストレーション（MVR）の前提条件は次のとおりです。

- MVR を使用するには、スイッチが LAN Base イメージを実行している必要があります。

IGMP スヌーピングおよび MVR の設定の制約事項

IGMP スヌーピングの制約事項

次に、IGMP スヌーピングの制約事項を示します。

- スイッチは同種スタックおよび混合スタック構成をサポートします。 混合スタック構成は、Catalyst 2960-S スイッチだけでサポートされます。 同種スタックは 8 つまで、混合スタックは4つまでのスタック メンバを持つことができます。 スイッチ スタック内のすべてのスイッチが LAN Base イメージを実行している必要があります。

- IGMP フィルタリングまたはマルチキャスト VLAN レジストレーション（MVR）が実行されているスイッチは、IGMPv3 Join および Leave メッセージをサポートしません。
- IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。 この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。
- IGMP の脱退時間の設定は、IGMP バージョン 2 が稼働しているホストでのみサポートされます。 IGMP バージョン 2 はスイッチのデフォルト バージョンです。

  ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。 ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間を前後することがあります。
- IGMP スロットリング アクションの制約事項は、レイヤ 2 ポートにだけ適用されます。 **ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドは論理 EtherChannel インターフェイスで使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

  グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups action** {**deny**| **replace**} コマンドを入力しても効果はありません。

  インターフェイスによりマルチキャストエントリが転送テーブルに追加されてから、スロットリングアクションを設定し、グループの最大数の制限を設定すると、転送テーブルのエントリは、スロットリング アクションに応じて期限切れになるか削除されます。

関連トピック

IGMP のバージョン, （1077 ページ）

IGMP プロファイルの設定, （1267 ページ）

IGMP プロファイルの適用, （1269 ページ）

IGMP グループの最大数の設定, （1271 ページ）

IGMP スロットリング アクションの設定, （1272 ページ）

IGMP フィルタリングおよびスロットリング, （1240 ページ）

MVR の制約事項

次に、MVR の制約事項を示します。

- MVR に参加するのは、レイヤ 2 ポートだけです。 ポートを MVR 受信ポートとして設定する必要があります。
- 各スイッチまたはスイッチ スタックでサポートされる MVR マルチキャスト VLAN は 1 つのみです。

- 受信ポートはアクセス ポートでなければなりません。トランク ポートにはできません。 スイッチのレシーバ ポートは異なる VLAN に属していてもかまいませんが、マルチキャスト VLAN に属することはできません。
- スイッチ上で設定可能なマルチキャスト エントリ（MVR グループ アドレス）の最大数（つまり、受信可能な TV チャネルの最大数）は、256 です。
- 送信元 VLAN で受信され、レシーバ ポートから脱退する MVR マルチキャスト データは、スイッチで存続可能時間（TTL）が 1 だけ少なくなります。
- スイッチ上の MVR は、MAC マルチキャスト アドレスではなく IP マルチキャスト アドレスを使用するので、スイッチ上でエイリアス IP マルチキャスト アドレスを使用できます。 ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス（224.0.0.xxx 範囲内）を設定する必要はありません。
- プライベート VLAN ポートに MVR を設定しないでください。
- スイッチ上でマルチキャスト ルーティングがイネーブルの場合、MVR はサポートされません。 MVR がイネーブルの場合に、マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにすると、MVR がディセーブルになり、警告メッセージが表示されます。 マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの場合に、MVR をイネーブルにしようとすると、MVR をイネーブルにする操作が取り消され、エラー メッセージが表示されます。
- MVR 受信ポートで受信した MVR データは、MVR 送信元ポートに転送されません。
- MVR は IGMPv3 メッセージをサポートしていません。
- スイッチは同種スタックおよび混合スタック構成をサポートします。 混合スタック構成は、Catalyst 2960-S スイッチだけでサポートされます。 同種スタックは 8 つまで、混合スタックは4つまでのスタック メンバを持つことができます。 スイッチ スタック内のすべてのスイッチが LAN Base イメージを実行している必要があります。

IGMP スヌーピングおよび MVR に関する情報

IGMP スヌーピング

レイヤ2スイッチはIGMPスヌーピングを使用して、レイヤ2インターフェイスを動的に設定し、マルチキャスト トラフィックが IP マルチキャスト デバイスと対応付けられたインターフェイスにのみ転送されるようにすることによって、マルチキャスト トラフィックのフラッディングを制限できます。 名称が示すとおり、IGMP スヌーピングの場合は、LAN スイッチでホストとルータ間の IGMP 伝送をスヌーピングし、マルチキャスト グループとメンバ ポートを追跡する必要があります。 特定のマルチキャスト グループについて、スイッチがホストから IGMP レポートを受信すると、そのスイッチはホストのポート番号を転送テーブル エントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブル エントリからホスト ポートを削除します。 マルチキャスト クライアントから IGMP メンバーシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。

（注） IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。

マルチキャスト ルータは、すべての VLANに一般的なクエリーを定期的に送信します。 このマルチキャスト トラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加されます。 スイッチは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ごとに 1 つずつエントリを作成します。

スイッチは、MAC アドレスに基づくグループではなく、IP マルチキャスト グループに基づくブリッジングをサポートしています。 マルチキャスト MAC アドレスに基づくグループの場合、設定されている IP アドレスを設定済みの MAC アドレス（エイリアス）または予約済みのマルチキャスト MAC アドレス（224.0.0.xxx の範囲内）に変換すると、コマンドがエラーになります。 スイッチでは IP マルチキャスト グループを使用するので、アドレス エイリアスの問題は発生しません。

IGMP スヌーピングによって、IP マルチキャスト グループは動的に学習されます。 ただし、**ip igmp snooping vlan***vlan-id* **static***ip_address* **interface***interface-id* グローバル コンフィギュレーション コマンドを使用すると、マルチキャスト グループを静的に設定できます。 グループ メンバーシップをマルチキャスト グループ アドレスに静的に指定すると、その設定値は IGMP スヌーピングによる自動操作より優先されます。 マルチキャスト グループ メンバーシップのリストは、ユーザが定義した設定値および IGMP スヌーピングによって学習された設定値の両方で構成できます。

マルチキャスト トラフィックはルーティングする必要がないのでマルチキャスト インターフェイスを使用せずに、サブネットの IGMP スヌーピングをサポートするよう IGMP スヌーピング クエリーを設定できます。

ポート スパニングツリー、ポート グループ、または VLAN ID が変更された場合、VLAN 上のこのポートから IGMP スヌーピングで学習されたマルチキャスト グループは削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

関連トピック

IGMP スヌーピング クエリアの設定, （1257 ページ）

IGMP スヌーピングの前提条件, （1227 ページ）

例：IGMP スヌーピング クエリアの送信元アドレスの設定, （1279 ページ）

例：IGMP スヌーピング クエリアの最大応答時間の設定, （1279 ページ）

例：IGMP スヌーピング クエリア タイムアウトの設定, （1279 ページ）

例：IGMP スヌーピング クエリア機能の設定, （1280 ページ）

IGMP のバージョン

スイッチは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしています。 これらのバージョンは、スイッチ上で相互運用できます。 たとえば、IGMP スヌーピングがイネーブルになっており、クエリーのバージョンが IGMPv2 で、スイッチがホストから IGMPv3 レポートを受信している場合、スイッチは IGMPv3 レポートをマルチキャスト ルータに転送できます。

IGMPv3 スイッチは、Source Specific Multicast（SSM）機能を実行しているデバイスとメッセージの送受信を行うことができます。

関連トピック

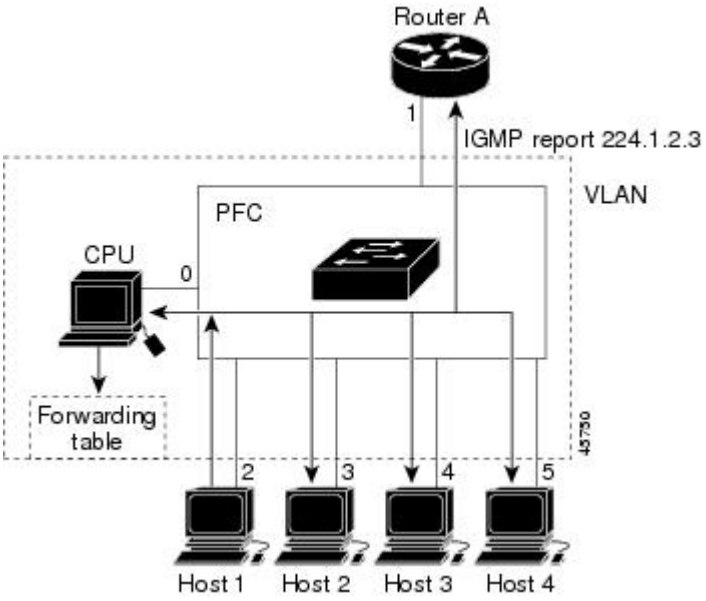
IGMP バージョンの変更, （1088 ページ）

IGMP スヌーピングの制約事項, （1228 ページ）

マルチキャスト グループへの加入

スイッチに接続したホストが IP マルチキャスト グループに加入し、なおかつそのホストが IGMP バージョン 2 クライアントの場合、ホストは加入する IP マルチキャスト グループを指定した非送信請求 IGMP Join メッセージを送信します。 別の方法として、ルータから一般クエリーを受信したスイッチは、そのクエリーを VLAN 内のすべてのポートに転送します。 IGMP バージョン 1 またはバージョン 2 のホストがマルチキャスト グループに加入する場合、ホストはスイッチに Join メッセージを送信することによって応答します。 スイッチの CPU は、そのグループのマルチキャスト転送テーブルエントリがまだ存在していないのであれば、エントリを作成します。 CPU はさらに、Join メッセージを受信したインターフェイスを転送テーブル エントリに追加します。 そのインターフェイスと対応付けられたホストが、そのマルチキャスト グループ用のマルチキャスト トラフィックを受信します。

図 *84*： 最初の *IGMP Join* メッセージ



ルータ A がスイッチに一般クエリーを送信し、スイッチがそのクエリーを同じ VLAN のすべてのメンバであるポート 2 ～ 5 に転送します。 ホスト 1 はマルチキャスト グループ 224.1.2.3 に加入するために、グループに IGMP メンバーシップ レポート（IGMP Join メッセージ）をマルチキャストします。 スイッチの CPU は IGMP レポートの情報を使用して、転送テーブルのエントリを設定します。転送テーブルにはホスト 1 およびルータに接続しているポート番号が含まれます。

表 *115* : *IGMP* スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1、2

スイッチのハードウェアは、IGMP 情報パケットをマルチキャスト グループの他のパケットと区別できます。 テーブルの情報は、224.1.2.3 マルチキャスト IP アドレス宛ての、IGMP パケットではないフレームを、ルータおよびグループに加入したホストに対して送信するように、スイッチング エンジンに指示します。

別のホスト（たとえば、ホスト4）が、同じグループ用に非送信請求IGMP Join メッセージを送信する場合、CPU がそのメッセージを受け取り、ホスト 4 のポート番号を転送テーブルに追加します。 転送テーブルはCPU宛てだけにIGMP メッセージを送るので、メッセージはスイッチの他のポートへフラッディングされません。 認識されているマルチキャスト トラフィックは、CPU宛てではなくグループ宛てに転送されます。

図 *85* : *2* 番目のホストのマルチキャスト グループへの加入

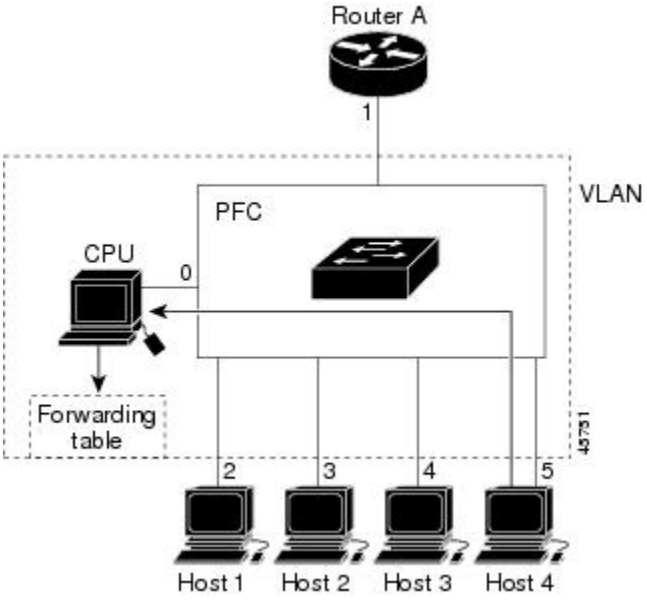


表 *116* : 更新された *IGMP* スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2, 5

関連トピック

グループに加入するホストの静的な設定, （1248 ページ）

例：グループに加入するホストの静的な設定，（1278 ページ）

マルチキャスト グループからの脱退

ルータは定期的にマルチキャスト一般クエリーを送信し、スイッチはそれらのクエリーを VLAN 内のすべてのポート経由で転送します。 関心のあるホストがクエリーに応答します。 VLAN 内の少なくとも 1 つのホストがマルチキャスト トラフィックを受信するようなら、ルータは、その VLAN へのマルチキャスト トラフィックの転送を続行します。 スイッチは、その IGMP スヌーピングによって維持された IP マルチキャスト グループの転送テーブルで指定されたホストに対してだけ、マルチキャスト グループ トラフィックを転送します。

ホストがマルチキャスト グループから脱退する場合、何も通知せずに脱退することも、Leave メッセージを送信することもできます。 ホストから Leave メッセージを受信したスイッチは、グループ固有のクエリーを送信して、そのインターフェイスに接続された他のデバイスが所定のマルチキャスト グループのトラフィックに関与しているかどうかを学習します。 スイッチはさらに、転送テーブルでその MAC グループの情報を更新し、そのグループのマルチキャスト トラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。 ルータが VLAN からレポートを受信しなかった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

即時脱退

スイッチは IGMP スヌーピングの即時脱退を使用して、先にスイッチからインターフェイスにグループ固有のクエリーを送信しなくても、Leave メッセージを送信するインターフェイスを転送テーブルから削除できるようにします。 VLAN インターフェイスは、最初の Leave メッセージで指定されたマルチキャスト グループのマルチキャスト ツリーからプルーニングされます。 即時脱退によって、複数のマルチキャスト グループが同時に使用されている場合でも、スイッチド ネットワークのすべてのホストに最適な帯域幅管理が保証されます。

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。 IGMP バージョン 2 はスイッチのデフォルト バージョンです。

（注） 即時脱退機能を使用するのは、各ポートに接続されているホストが 1 つだけの VLAN に限定してください。 ポートに複数のホストが接続されている VLAN 上で即時脱退をイネーブルにすると、一部のホストが誤ってドロップされる可能性があります。

関連トピック

IGMP 即時脱退のイネーブル化，（1249 ページ）

例：IGMP 即時脱退のイネーブル化，（1279 ページ）

IGMP 設定可能 Leave タイマー

特定のマルチキャスト グループへの参加がまだ必要かどうかを確認するために、グループ固有のクエリーを送信した後のスイッチの待機時間を設定できます。 IGMP 脱退応答時間は、100 ～ 32767 ミリ秒の間で設定できます。

関連トピック

IGMP 脱退タイマーの設定, （1251 ページ）

IGMP レポート抑制

（注） IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。 この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

スイッチは、IGMP レポート抑制を使用して、1 つのマルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけマルチキャスト デバイスに転送します。 IGMP ルータ抑制がイネーブル（デフォルト）である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャスト ルータに送信します。 スイッチは、グループの残りの IGMP レポートをマルチキャスト ルータに送信しません。 この機能により、マルチキャスト デバイスにレポートが重複して送信されることを防ぎます。

マルチキャスト ルータ クエリーに IGMPv1 および IGMPv2 レポートに対する要求だけが含まれている場合、スイッチは最初の IGMPv1 レポートまたは IGMPv2 レポートだけを、グループのすべてのホストからすべてのマルチキャスト ルータに送信します。

マルチキャスト ルータ クエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送します。

IGMP レポート抑制をディセーブルにすると、すべての IGMP レポートはマルチキャスト ルータに転送されます。

関連トピック

IGMP レポート抑制のディセーブル化, （1260 ページ）

IGMP スヌーピングのデフォルト設定

次の表に、スイッチの IGMP スヌーピングのデフォルト設定を示します。

表 *117* : *IGMP* スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位でイネーブル

機能	デフォルト設定
マルチキャスト ルータ	未設定
IGMP スヌーピング即時脱退	ディセーブル
スタティック グループ	未設定
TCN[9]フラッド クエリ カウント	2
TCN クエリー送信要求	ディセーブル
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	イネーブル

9 (1) TCN = トポロジ変更通知

関連トピック

スイッチでの IGMP スヌーピングのイネーブル化またはディセーブル化, （1241 ページ）

VLANインターフェイスでのIGMPスヌーピングのイネーブル化またはディセーブル化, （1243 ページ）

マルチキャスト VLAN レジストレーション

マルチキャスト VLAN レジストレーション（MVR）は、イーサネット リング ベースのサービス プロバイダーネットワーク上でマルチキャスト トラフィックの広範囲展開を使用するアプリケーション（サービス プロバイダー ネットワーク上の複数の TV チャネルのブロードキャストなど）用に設計されています。 MVR によってポート上の加入者は、ネットワークワイドなマルチキャスト VLAN 上のマルチキャスト ストリームに加入し、脱退できます。 また、ネットワーク上で 1 つのマルチキャスト VLAN を共有しながら、加入者が別の VLAN に接続できます。 MVR によって、マルチキャスト VLAN でマルチキャスト ストリームを連続送信する能力が得られますが、ストリームと加入者の VLAN は、帯域幅およびセキュリティ上の理由で分離されます。

ここでは、MVR について説明します。

MVR と IGMP

（注） スイッチ上で、MVR は IGMP スヌーピングと共存できます。

MVR では、加入者ポートが IGMP Join および Leave メッセージを送信することによって、マルチキャスト ストリームへの加入および脱退（Join および Leave）を行うことが前提です。 これらのメッセージは、イーサネットで接続され、IGMP バージョン 2 に準拠しているホストから発信で

きます。 MVR は IGMP スヌーピングの基本メソッドで動作しますが、この 2 つの機能はそれぞれ単独で動作します。 それぞれ他方の機能の動作に影響を与えずに、イネーブルまたはディセーブルにできます。 ただし、IGMP スヌーピングと MVR が両方ともイネーブルの場合、MVR は MVR 環境で設定されたマルチキャスト グループが送信した Join および Leave メッセージだけに反応します。 他のマルチキャスト グループから送信された Join および Leave メッセージはすべて、IGMP スヌーピングが管理します。

スイッチの CPU は、MVR IP マルチキャストストリームとそれに対応するスイッチ転送テーブル内の IP マルチキャスト グループを識別し、IGMP メッセージを代行受信し、転送テーブルを変更して、マルチキャスト ストリームの受信側としての加入者を追加または削除します。受信側が送信元と異なる VLAN 上に存在している場合でも同じです。 この転送動作により、異なる VLAN の間でトラフィックを選択して伝送できます。

動作モード

スイッチの MVR 動作は、互換モードまたはダイナミック モードに設定できます。

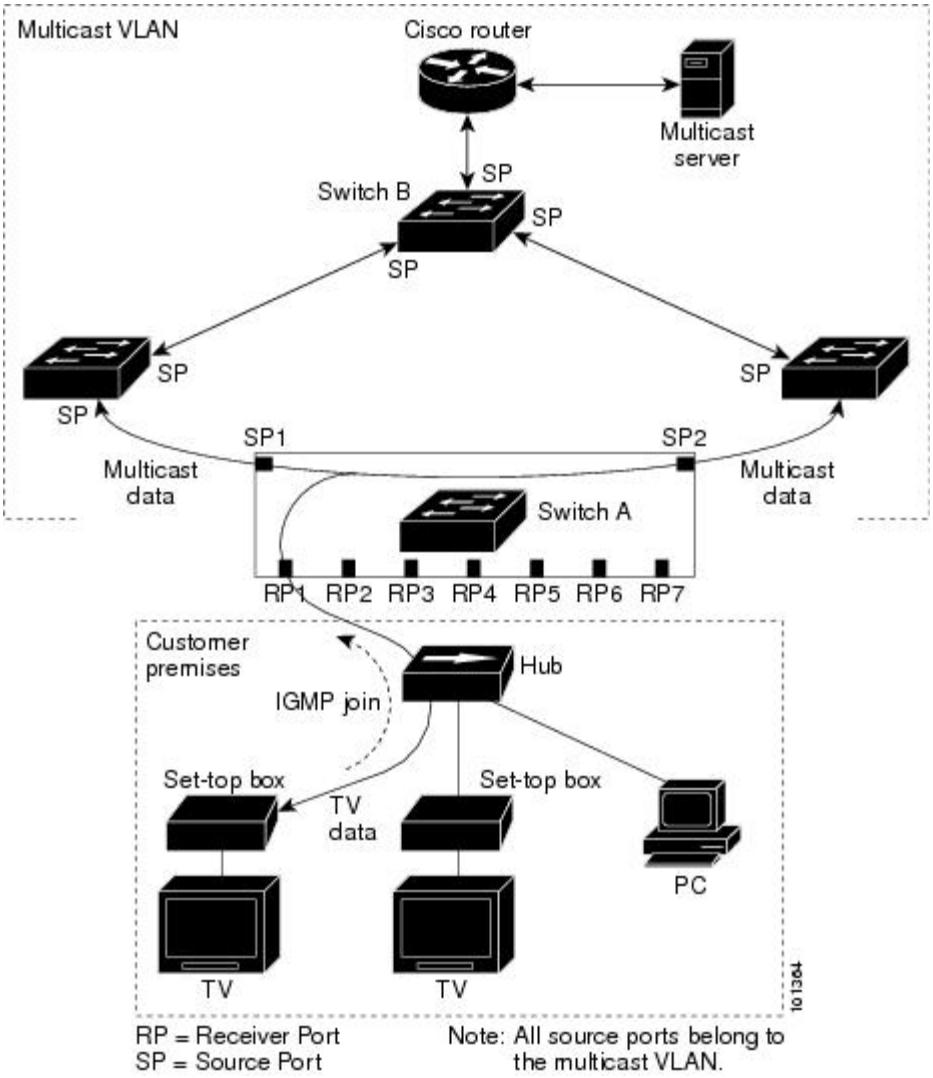
- 互換モードの場合、MVR ホストが受信したマルチキャスト データはすべての MVR データ ポートに転送されます。MVR データ ポートの MVR ホスト メンバーシップは無関係です。マルチキャストデータは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入しているレシーバ ポートだけに転送されます。 MVR ホストから受信した IGMP レポートが、スイッチに設定された MVR データ ポートから転送されることはありません。
- ダイナミック モードの場合、スイッチ上の MVR ホストが受信したマルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入している MVR データおよびクライアント ポートから転送されます。それ以外のポートからは転送されません。 MVR ホストから受信した IGMP レポートも、ホストのすべての MVR データ ポートから転送されます。 したがって、互換モードでスイッチを稼働させた場合と異なり、MVR データ ポート リンクで不要な帯域幅を使用しなくてすみます。

マルチキャスト TV アプリケーションでの MVR

マルチキャスト TV アプリケーションでは、PC またはセットトップ ボックスを装備したテレビでマルチキャスト ストリームを受信できます。 1 つの加入者ポートに複数のセットトップ ボックスまたは PC を接続できます。加入者ポートは、MVR レシーバ ポートとして設定されたスイッチ ポートです。

次に、設定例を示します。

図 *86*：マルチキャスト *VLAN* レジストレーションの例



この設定例では、Dynamic Host Configuration Protocol（DHCP）によって、セットトップ ボックスまたは PC に IP アドレスが割り当てられます。 加入者がチャネルを選択すると、適切なマルチキャストに加入するために、セットトップ ボックスまたは PC からスイッチ A に IGMP レポートが送信されます。 IGMP レポートが、設定されている IP マルチキャスト グループ アドレスの 1 つと一致すると、スイッチの CPU がハードウェア アドレス テーブルを変更して、指定のマルチキャスト ストリームをマルチキャスト VLAN から受信したときの転送先として、レシーバ ポートと VLAN を追加します。 マルチキャスト VLAN との間でマルチキャスト データを送受信するアップリンク ポートを、MVR 送信元ポートと呼びます。

加入者がチャネルを切り替えた場合、またはテレビのスイッチを切った場合には、セットトップ ボックスからマルチキャスト ストリームに対する IGMP Leave メッセージが送信されます。 スイッチの CPU は、受信ポートの VLAN を介して MAC ベースの一般クエリーを送信します。 VLAN

に、このグループに加入している別のセットトップボックスがある場合、そのセットトップボックスはクエリーに指定された最大応答時間内に応答しなければなりません。 応答を受信しなかった場合、CPU はこのグループの転送先としての受信ポートを除外します。

即時脱退機能を使用しない場合、レシーバ ポートの加入者から IGMP Leave メッセージを受信したスイッチは、そのポートに IGMP クエリーを送信し、IGMP グループ メンバーシップ レポートを待ちます。 設定された時間内にレポートを受信しなかった場合は、受信ポートがマルチキャスト グループ メンバーシップから削除されます。 即時脱退機能がイネーブルの場合、IGMP Leave を受信したレシーバ ポートから IGMP クエリーが送信されません。 Leave メッセージの受信後ただちに、受信ポートがマルチキャストグループメンバーシップから削除されるので、脱退遅延時間が短縮されます。 即時脱退機能をイネーブルにするのは、接続されているレシーバデバイスが 1 つだけのレシーバ ポートに限定してください。

MVR を使用すると、各 VLAN の加入者に対してテレビ チャネルのマルチキャスト トラフィックを重複して送信する必要がなくなります。 すべてのチャネル用のマルチキャスト トラフィックは、マルチキャスト VLAN 上でのみ、VLAN トランクに 1 回だけ送信されます。 IGMP Leave および Join メッセージは、加入者ポートが割り当てられている VLAN で送信されます。 これらのメッセージは、レイヤ 3 デバイス上のマルチキャスト VLAN のマルチキャスト トラフィック ストリームに対し、動的に登録します。 アクセス レイヤ スイッチ（スイッチ A）は、マルチキャスト VLAN から別の VLAN 内の加入者ポートにトラフィックが転送されるよう転送動作を変更し、2 つの VLAN 間で選択的にトラフィックが送信されるようにします。

IGMP レポートは、マルチキャスト データと同じ IP マルチキャスト グループ アドレスに送信されます。 スイッチ A の CPU は、レシーバ ポートから送られたすべての IGMP Join および Leave メッセージを取り込み、MVR モードに基づいて、送信元（アップリンク）ポートのマルチキャスト VLAN に転送しなければなりません。

MVR のデフォルト設定

表 *118* : *MVR* のデフォルト設定

機能	デフォルト設定
MVR	グローバルおよびインターフェイス単位でディセーブル
マルチキャスト アドレス	未設定
クエリーの応答時間	0.5 秒
マルチキャスト VLAN	VLAN 1
モード	互換
インターフェイスのデフォルト（ポート単位）	受信ポートでも送信元ポートでもない

機能	デフォルト設定
即時脱退	すべてのポートでディセーブル

IGMP フィルタリングおよびスロットリング

都市部や集合住宅（MDU）などの環境では、スイッチ ポート上のユーザが属する一連のマルチキャスト グループを制御する必要があります。 この機能を使用することにより、IP/TV などのマルチキャスト サービスの配信を、特定タイプの契約またはサービス計画に基づいて制御できます。 また、マルチキャスト グループの数を、スイッチ ポート上でユーザが所属できる数に制限することもできます。

IGMP フィルタリング機能を使用すると、IP マルチキャスト プロファイルを設定し、それらを各スイッチ ポートに関連付けて、ポート単位でマルチキャスト加入をフィルタリングできます。 IGMP プロファイルにはマルチキャスト グループを 1 つまたは複数格納して、グループへのアクセスを許可するか拒否するかを指定できます。 マルチキャストグループへのアクセスを拒否する IGMP プロファイルがスイッチ ポートに適用されると、IP マルチキャスト トラフィックのストリームを要求する IGMP Join レポートが廃棄され、ポートはそのグループからの IP マルチキャスト トラフィックを受信できなくなります。 マルチキャスト グループへのアクセスがフィルタリング アクションで許可されている場合は、ポートからの IGMP レポートが転送されて、通常の処理が行われます。 レイヤ 2 インターフェイスが加入できる IGMP グループの最大数も設定できます。

IGMP フィルタリングで制御されるのは、グループ固有のクエリーおよびメンバーシップ レポート（Join および Leave レポートを含む）だけです。 一般 IGMP クエリーは制御されません。 IGMP フィルタリングは、IP マルチキャスト トラフィックの転送を指示する機能とは無関係です。 フィルタリング機能は、マルチキャスト トラフィックの転送に CGMP が使用されているか、または MVR が使用されているかに関係なく、同じように動作します。

IGMP フィルタリングが適用されるのは、IP マルチキャスト グループ アドレスを動的に学習する場合だけです。静的な設定には適用されません。

IGMP スロットリング機能を使用すると、レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定できます。 IGMP グループの最大数が設定され、IGMP スヌーピング転送テーブルに最大数のエントリが登録されていて、インターフェイスで IGMP Join レポートを受信する場合、インターフェイスを設定することにより、IGMP レポートを廃棄するか、あるいは受信した IGMP レポートでランダムに選択されたマルチキャスト エントリを上書きします。

（注） IGMP フィルタリングが実行されているスイッチは、IGMPv3 Join および Leave メッセージをサポートしていません。

関連トピック

IGMP プロファイルの設定, （1267 ページ）

IGMP プロファイルの適用, （1269 ページ）

IGMP グループの最大数の設定, （1271 ページ）
IGMP スロットリング アクションの設定, （1272 ページ）
IGMP スヌーピングの制約事項, （1228 ページ）

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

次の表に、スイッチの IGMP フィルタリングおよびスロットリングのデフォルト設定を示します。

表 *119*：*IGMP* フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用なし
IGMP グループの最大数	最大数の設定なし （注） 転送テーブルに登録されているグループが最大数に達していると、デフォルトの IGMP スロットリング アクションは IGMP レポートを拒否します。
IGMP プロファイル	未定義
IGMP プロファイル アクション	範囲で示されたアドレスを拒否

IGMP スヌーピングおよび MVR の設定方法

スイッチでの IGMP スヌーピングのイネーブル化またはディセーブル化

IGMP スヌーピングがグローバルにイネーブルまたはディセーブルに設定されている場合は、既存のすべての VLAN インターフェイスでもイネーブルまたはディセーブルになります。 デフォルトでは IGMP スヌーピングはすべての VLAN でイネーブルになっていますが、VLAN 単位でイネーブルまたはディセーブルにすることができます。

グローバル IGMP スヌーピングは、VLAN IGMP スヌーピングより優先されます。 グローバル スヌーピングがディセーブルの場合、VLAN スヌーピングをイネーブルに設定することはできません。 グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

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

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping**
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping** 例： `Switch(config)# ip igmp snooping`	既存のすべての VLAN インターフェイスでグローバルに IGMP スヌーピングを有効にします。 （注） すべての VLAN インターフェイス上で IGMP スヌーピングをグローバルにディセーブルにするには、**no ip igmp snooping** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP スヌーピングのデフォルト設定, （1235 ページ）

VLAN インターフェイスでの IGMP スヌーピングのイネーブル化またはディセーブル化

VLAN インターフェイス上で IGMP スヌーピングを有効にするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping vlan***vlan-id*
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan***vlan-id* 例： `Switch(config)# ip igmp snooping vlan 7`	VLAN インターフェイス上で IGMP スヌーピングをイネーブルにします。 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 VLAN スヌーピングをイネーブルにするには、IGMP スヌーピングをグローバルにイネーブルに設定しておく必要があります。 （注） 特定の VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、**no ip igmp snooping vlan***vlan-id* グローバル コンフィギュレーション コマンドを、指定した VLAN 番号に対して使用します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP スヌーピングのデフォルト設定，（1235 ページ）

スヌーピング方法の設定

マルチキャスト対応のルータ ポートは、レイヤ 2 マルチキャスト エントリごとに転送テーブルに追加されます。 スイッチは、次のいずれかの方法でポートを学習します。

- IGMP クエリー、Protocol-Independent Multicast（PIM）パケット、およびディスタンスベクトル マルチキャスト ルーティング プロトコル（DVMRP）パケットのスヌーピング
- 他のルータからの Cisco Group Management Protocol（CGMP）パケットのリスニング
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによるマルチキャスト ルータ ポートへの静的な接続

IGMP クエリーおよび PIM パケットと DVMRP パケットのスヌーピング、または CGMP self-join パケットまたは proxy-join パケットのいずれかの待ち受けを行うように、スイッチを設定できます。 デフォルトでは、スイッチはすべての VLAN 上の PIM パケットと DVMRP パケットをスヌーピングします。 CGMP パケットだけでマルチキャスト ルータ ポートを学習するには、**ip igmp snooping vlan vlan-id mrouter learn cgmp** グローバル コンフィギュレーション コマンドを使用します。 このコマンドを入力すると、ルータは CGMP self-join パケットおよび CGMP proxy-join パケットだけを待ち受け、その他の CGMP パケットは待ち受けません。 PIM-DVMRP パケットだけでマルチキャスト ルータ ポートを学習するには、 **ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp** グローバル コンフィギュレーション コマンドを使用します。

学習方法として CGMP を使用する場合で、なおかつ VLAN に CGMP プロキシ対応のマルチキャスト ルータがない場合は、**ip cgmp router-only** コマンドを入力し、ルータに動的にアクセスする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping vlan***vlan-id***mrouterlearn** {**cgmp** | **pim-dvmrp** }
4. **end**
5. **show ip igmp snooping**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ip igmp snooping vlan***vlan-id***mrouterlearn** {**cgmp** | **pim-dvmrp** } 例： `Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp`	マルチキャスト ルータの学習方式を指定します。 • **cgmp**—Listens for CGMP packets. この方法は、制御トラフィックを減らす場合に有用です。 • **pim-dvmrp**：IGMP クエリーおよび PIM/DVMRP パケットをスヌーピングします。 これはデフォルトです。 （注） デフォルトの学習方式に戻すには、**no ip igmp snooping vlan***vlan-id***mrouter learn cgmp** グローバルコンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show ip igmp snooping** 例： `Switch# show ip igmp snooping`	設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

マルチキャスト ルータ ポートの設定

スイッチにマルチキャスト ルータ ポートを追加する（マルチキャスト ルータへのスタティック接続をイネーブルにする）には、次の手順を実行します。

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

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping vlan***vlan-id***mrouter interface***interface-id*
4. **end**
5. **show ip igmp snooping mrouter** [**vlan***vlan-id*]
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan***vlan-id***mrouter interface***interface-id* 例： `Switch(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet1/0/1`	マルチキャスト ルータの VLAN ID およびマルチキャスト ルータに対するインターフェイスを指定します。 • 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポートチャネルを指定できます。ポートチャネル範囲は 1 ～ 128 です。 （注） VLANからマルチキャストルータ ポートを削除するには、**no ip igmp snooping vlan***vlan-id***mrouter interface***interface-id* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping mrouter** [**vlan***vlan-id*] 例： `Switch# show ip igmp snooping mrouter vlan 5`	VLANインターフェイス上でIGMPスヌーピングがイネーブルになっていることを確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：マルチキャスト ルータへの静的な接続のイネーブル化，（1278 ページ）

グループに加入するホストの静的な設定

ホストまたはレイヤ 2 ポートは通常、マルチキャスト グループに動的に加入しますが、インターフェイス上にホストを静的に設定することもできます。

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

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping vlan***vlan-id***static***ip_address***interface***interface-id*
4. **end**
5. **show ip igmp snooping groups**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan***vlan-id***static***ip_address***interface***interface-id* 例： `Switch(config)# ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1`	マルチキャスト グループのメンバとしてレイヤ2ポートを静的に設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。 指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。 • *ip-address* は、グループの IP アドレスです。 • *interface-id* は、メンバ ポートです。 物理インターフェイスまたはポート チャネル（1 ～ 128）に設定できます。

	コマンドまたはアクション	目的
		（注） マルチキャスト グループからレイヤ 2 ポートを削除するには、**no ip igmp snooping vlan***vlan-id***static***mac-address***interface***interface-id* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping groups** 例： `Switch# show ip igmp snooping groups`	メンバ ポートおよび IP アドレスを確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

マルチキャスト グループへの加入，（1232 ページ）

例：グループに加入するホストの静的な設定，（1278 ページ）

IGMP 即時脱退のイネーブル化

IGMP 即時脱退をイネーブルに設定すると、スイッチはポート上で IGMP バージョン 2 の Leave メッセージを検出した場合、ただちにそのポートを削除します。 即時脱退機能は、VLAN の各ポートにレシーバが 1 つ存在する場合にだけ使用してください。

（注） 即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。 IGMP バージョン 2 はスイッチのデフォルト バージョンです。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping vlan***vlan-id***immediate-leave**
4. **end**
5. **show ip igmp snooping vlan***vlan-id*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan***vlan-id***immediate-leave** 例： `Switch(config)# ip igmp snooping vlan 21 immediate-leave`	VLAN インターフェイス上で、IGMP 即時脱退をイネーブルにします。 （注） VLAN 上で IGMP 即時脱退をディセーブルにするには、**no ip igmp snooping vlan***vlan-id***immediate-leave** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping vlan***vlan-id* 例： `Switch# show ip igmp snooping vlan 21`	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。

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

関連トピック

即時脱退，（1234 ページ）

例：IGMP 即時脱退のイネーブル化，（1279 ページ）

IGMP 脱退タイマーの設定

脱退時間はグローバルまたは VLAN 単位で設定できます。 IGMP 脱退タイマーの設定をイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping last-member-query-interval***time*
4. **ip igmp snooping vlan***vlan-id***last-member-query-interval***time*
5. **end**
6. **show ip igmp snooping**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip igmp snooping last-member-query-interval***time* 例： `Switch(config)# ip igmp snooping last-member-query-interval 1000`	IGMP 脱退タイマーをグローバルに設定します。 指定できる範囲は 100 ～ 32767 ミリ秒です。 デフォルトの脱退時間は 1000 ミリ秒です。 （注） IGMP 脱退タイマーをグローバルにリセットしてデフォルト設定に戻すには、**no ip igmp snooping last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**ip igmp snooping vlan***vlan-id***last-member-query-interval***time* 例： `Switch(config)# ip igmp snooping vlan 210 last-member-query-interval 1000`	（任意）VLAN インターフェイス上で IGMP 脱退時間を設定します。 有効値は 100 ～ 32767 ミリ秒です。 （注） VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。 （注） 特定の VLAN から IGMP 脱退タイマーの設定を削除するには、**no ip igmp snooping vlan***vlan-id***last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping** 例： `Switch# show ip igmp snooping`	（任意）設定された IGMP 脱退時間を表示します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP 設定可能 Leave タイマー, （1235 ページ）

TCN 関連コマンドの設定

TCN イベント後のマルチキャスト フラッディング時間の制御

トポロジ変更通知（TCN）イベント後にフラッディングするマルチキャスト データのトラフィックに対し、一般クエリー数を設定できます。 TCN フラッド クエリ カウントを 1 に設定した場合は、1 つの一般クエリーを受信した後にフラッディングが停止します。 カウントを 7 に設定した場合、一般クエリーを 7 つ受信するまでフラッディングが続きます。 グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

クライアント ロケーションが変更され、ブロックされていた後に現在は転送中の受信者が同じポートに存在する場合や、ポートが脱退メッセージを送信せずにダウンした場合などにTCNイベントが発生します。

TCN フラッド クエリー カウントを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping tcn flood query count***count*
4. **end**
5. **show ip igmp snooping**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping tcn flood query count***count* 例： `Switch(config)# ip igmp snooping tcn`	マルチキャスト トラフィックがフラッディングする IGMP の一般クエリー数を指定します。 指定できる範囲は 1 ～ 10 です。 デフォルトのフラッディング クエリー カウントは 2 です。

	コマンドまたはアクション	目的
	`flood query count 3`	（注） デフォルトのフラッディング クエリー カウントに戻すには、**no ip igmp snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping** 例： `Switch# show ip igmp snooping`	TCN の設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

フラッディング モードからの回復

トポロジの変更が発生した場合、スパニングツリーのルートは特別な IGMP Leave メッセージ（グローバル Leave メッセージ）をグループ マルチキャスト アドレス 0.0.0.0. に送信します。 ただし、スパニングツリーのルートであるかどうかにかかわらず、グローバルな Leave メッセージを送信するようにスイッチを設定できます。 ルータはこの特別な Leave メッセージを受信した場合、即座に一般クエリーを送信して、TCN 中のフラッディング モードからできるだけ早く回復するようにします。 スイッチがスパニングツリーのルートであれば、このコンフィギュレーションに関係なく、Leave メッセージが常に送信されます。

Leave メッセージを送信できるようにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping tcn query solicit**
4. **end**
5. **show ip igmp snooping**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping tcn query solicit** 例： `Switch(config)# ip igmp snooping tcn query solicit`	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ（グローバル脱退）を送信します。 デフォルトでは、クエリー送信要求はディセーブルに設定されています。 （注） デフォルトのクエリー送信要求に戻すには、**no ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping** 例： `Switch# show ip igmp snooping`	TCN の設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

TCN イベント中のマルチキャスト フラッディングのディセーブル化

スイッチは TCN を受信すると、一般クエリーを 2 つ受信するまで、すべてのポートに対してマルチキャスト トラフィックをフラッディングします。 異なるマルチキャスト グループのホストに

接続しているポートが複数ある場合、リンク範囲を超えてスイッチによるフラッディングが行われ、パケット損失が発生する可能性があります。 TCN フラッディングを制御するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **no ip igmp snooping tcn flood**
5. **end**
6. **show ip igmp snooping**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no ip igmp snooping tcn flood** 例： `Switch(config-if)# no ip igmp snooping tcn flood`	スパニングツリーの TCN イベント中に発生するマルチキャスト トラフィックのフラッディングをディセーブルにします。 デフォルトでは、インターフェイス上のマルチキャスト フラッディングはイネーブルです。 （注） インターフェイス上でマルチキャスト フラッディングを再度イネーブルにするには、**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping** 例： `Switch# show ip igmp snooping`	TCN の設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP スヌーピング クエリアの設定

特定の VLAN で IGMP スヌーピング クエリア機能をイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping querier**
4. **ip igmp snooping querier address***ip_address*
5. **ip igmp snooping querier query-interval***interval-count*
6. **ip igmp snooping querier tcn query** [**count***count* | **interval***interval*]
7. **ip igmp snooping querier timer expiry***timeout*
8. **ip igmp snooping querier version***version*
9. **end**
10. **show ip igmp snooping vlan***vlan-id*
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping querier** 例： `Switch(config)# ip igmp snooping querier`	IGMP スヌーピング クエリアをイネーブルにします。
ステップ 4	**ip igmp snooping querier address***ip_address* 例： `Switch(config)# ip igmp snooping querier address 172.16.24.1`	（任意）IGMP スヌーピング クエリアの IP アドレスを指定します。 IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。 （注） IGMP スヌーピング クエリアはスイッチ上で IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
ステップ 5	**ip igmp snooping querier query-interval***interval-count* 例： `Switch(config)# ip igmp snooping querier query-interval 30`	（任意）IGMP クエリアの間隔を設定します。 指定できる範囲は 1 ～ 18000 秒です。
ステップ 6	**ip igmp snooping querier tcn query** [**count***count* | **interval***interval*] 例： `Switch(config)# ip igmp snooping querier tcn query interval 20`	（任意）トポロジ変更通知（TCN）クエリーの間隔を設定します。 指定できる count の範囲は 1 ～ 10 です。 指定できる interval の範囲は 1 ～ 255 秒です。

	コマンドまたはアクション	目的
ステップ 7	**ip igmp snooping querier timer expiry***timeout* 例： `Switch(config)# ip igmp snooping querier timer expiry 180`	（任意）IGMP クエリアが期限切れになる時間を設定します。 指定できる範囲は 60 ～ 300 秒です。
ステップ 8	**ip igmp snooping querier version***version* 例： `Switch(config)# ip igmp snooping querier version 2`	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。 選択できる番号は 1 または 2 です。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip igmp snooping vlan***vlan-id* 例： `Switch# show ip igmp snooping vlan 30`	（任意）VLAN インターフェイス上で IGMP スヌーピング クエリアがイネーブルになっていることを確認します。 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP スヌーピング，（1230 ページ）
IGMP スヌーピングの前提条件，（1227 ページ）
例：IGMP スヌーピング クエリアの送信元アドレスの設定，（1279 ページ）
例：IGMP スヌーピング クエリアの最大応答時間の設定，（1279 ページ）
例：IGMP スヌーピング クエリア タイムアウトの設定，（1279 ページ）
例：IGMP スヌーピング クエリア機能の設定，（1280 ページ）

IGMP レポート抑制のディセーブル化

IGMP レポート抑制をディセーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **no ip igmp snooping report-suppression**
4. **end**
5. **show ip igmp snooping**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ip igmp snooping report-suppression** 例： `Switch(config)# no ip igmp snooping report-suppression`	IGMP レポート抑制をディセーブルにします。 IGMP レポート抑制がディセーブルの場合、すべての IGMP レポートがマルチキャスト ルータに転送されます。 IGMP レポート抑制はデフォルトでイネーブルです。 IGMP レポート抑制がイネーブルの場合、スイッチはマルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけ転送します。 （注） IGMP レポート抑制を再びイネーブルにするには、**ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show ip igmp snooping** 例： `Switch# show ip igmp snooping`	IGMP レポート抑制がディセーブルになっていることを確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP レポート抑制，（1235 ページ）

MVR グローバル パラメータの設定

デフォルト値を使用する場合は、オプションの MVR パラメータを設定する必要はありません。デフォルトのパラメータを変更する場合には（MVR VLAN 以外）、最初に MVR をイネーブルにする必要があります。

（注） ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **mvr**
4. **mvr group***ip-address* [*count*]
5. **mvrquerytime***value*
6. **mvrvlan***vlan-id*
7. **mvr mode** {**dynamic** | **compatible**}
8. **end**
9. 次のいずれかを使用します。
   - **show mvr**
   - **show mvr members**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mvr** 例： `Switch (config)# mvr`	スイッチ上で MVR をイネーブルにします。
ステップ 4	**mvr group***ip-address* [*count*] 例： `Switch(config)# mvr group 228.1.23.4`	スイッチ上で IP マルチキャスト アドレスを設定するか、または *count* パラメータを使用して（*count* の範囲は 1 ～ 256 で、デフォルトは 1）連続する MVR グループ アドレスを設定します。 このアドレスに送信されるすべてのマルチキャスト データは、スイッチ上の送信元ポートおよびこのマルチキャスト アドレス上のデータを受信するよう選択されたすべての受信ポートに送信されます。 マルチキャスト アドレスとテレビ チャネルは 1 対 1 の対応です。

	コマンドまたはアクション	目的
		（注） スイッチをデフォルトの設定に戻すには、**no mvr** [**mode** | **group***ip-address* | **querytime** | **vlan**] グローバル コンフィギュレーション コマンドを使用します。
ステップ 5	**mvrquerytime***value* 例： `Switch(config)# mvr querytime 10`	（任意）マルチキャスト グループ メンバーシップからポートを削除する前に、受信ポート上で IGMP レポート メンバーシップを待機する最大時間を定義します。 この値は 10 分の 1 秒単位で設定します。 範囲は 1 ～ 100、デフォルトは 10 分の 5 秒、つまり 0.5 秒です。
ステップ 6	**mvrvlan***vlan-id* 例： `Switch(config)# mvr vlan 22`	（任意）マルチキャスト データを受信する VLAN を指定します。すべての送信元ポートはこの VLAN に属する必要があります。VLAN の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 デフォルトは VLAN 1 です。
ステップ 7	**mvr mode** {**dynamic** | **compatible**} 例： `Switch(config)# mvr mode dynamic`	（任意）次の MVR の動作モードを指定します。 • **dynamic**：送信元ポートでダイナミック MVR メンバーシップを使用できます。 • **compatible**：Catalyst 3500 XL および Catalyst 2900 XL スイッチとの互換性が得られます。送信元ポートでのダイナミック IGMP Join はサポートされません。 デフォルトは **compatible** モードです。 （注） スイッチをデフォルトの設定に戻すには、**no mvr** [**mode** | **group***ip-address* | **querytime** | **vlan**] グローバル コンフィギュレーション コマンドを使用します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。 • **show mvr** • **show mvr members** 例： `Switch# show mvr` OR	設定を確認します。

	コマンドまたはアクション	目的
	`Switch# show mvr members`	
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MVR インターフェイスの設定

レイヤ 2 MVR インターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **mvr**
4. **interface***interface-id*
5. **mvr type** {**source** | **receiver**}
6. **mvr vlan***vlan-id***group** [*ip-address*]
7. **mvr immediate**
8. **end**
9. 次のいずれかを使用します。
   - **show mvr**
   - **show mvr interface**
   - **show mvr members**
10. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mvr** 例： `Switch (config)# mvr`	スイッチ上で MVR をイネーブルにします。
ステップ 4	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	設定するレイヤ2ポートを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 5	**mvr type** {**source** | **receiver**} 例： `Switch(config-if)# mvr type receiver`	MVR ポートを次のいずれかに設定します。 • **source**：マルチキャスト データを送受信するアップリンク ポートを送信元ポートとして設定します。 加入者が送信元ポートに直接接続することはできません。 スイッチ上の送信元ポートはいずれも、1 つのマルチキャスト VLAN に属する必要があります。 • **receiver**：ポートが加入者ポートで、マルチキャスト データの受信だけを行う場合には、ポートを受信ポートとして設定します。 受信ポートは、スタティックな設定、または IGMP Leave および Join メッセージによってマルチキャスト グループのメンバーになるまでは、データを受信しません。 受信ポートをマルチキャスト VLAN に所属させることはできません。 デフォルトでは、非 MVR ポートとして設定されます。 非 MVR ポートに MVR 特性を設定しようとしても、エラーになります。 （注） インターフェイスをデフォルトの設定に戻すには、**no mvr**[**type** | **immediate** | **vlan***vlan-id* | **group**] インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 6	**mvr vlan***vlan-id***group** [*ip-address*] 例： `Switch(config-if)# mvr vlan 22 group`	（任意）マルチキャスト VLAN および IP マルチキャスト アドレスに送信されたマルチキャスト トラフィックを受信するポートを静的に設定します。 グループ メンバとして静的に設定されたポートは、静的に削除されない限り、グループ メンバのままです。

	コマンドまたはアクション	目的
	228.1.23.4	（注） 互換モードでは、このコマンドが適用されるのはレシーバ ポートだけです。 ダイナミック モードでは、レシーバ ポートおよび送信元ポートに適用されます。 レシーバ ポートは、IGMP Join および Leave メッセージを使用することによって、マルチキャスト グループに動的に加入することもできます。
ステップ 7	**mvr immediate** 例： `Switch(config-if)# mvr immediate`	（任意）ポート上で MVR の即時脱退機能をイネーブルにします。 （注） このコマンドが適用されるのは、受信ポートだけです。また、イネーブルにするのは、単一の受信デバイスが接続されている受信ポートに限定してください。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ステップ 9	次のいずれかを使用します。
	• **show mvr**
	• **show mvr interface**
	• **show mvr members**
	
	例：
	`Switch# show mvr interface`
	`Port  Type  Status  Immediate Leave`
	`----  ----  -------  ----------`
	`Gi1/0/2 RECEIVER  ACTIVE/DOWN  ENABLED`
		設定を確認します。

ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP プロファイルの設定

IGMP プロファイルを作成するには、次の手順を実行します。

このタスクはオプションです。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp profile***profile number*
4. **permit** | **deny**
5. **range***ip multicast address*
6. **end**
7. **show ip igmp profile***profile number*
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp profile***profile number* 例： `Switch(config)# ip igmp profile 3`	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。 指定できるプロファイル番号の範囲は 1 ～ 4294967295 です。 IGMP プロファイル コンフィギュレーションモードでは、次のコマンドを使用することでプロファイルを作成できます。 • **deny**：一致するアドレスを拒否します。デフォルトで設定されています。 • **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
		• **no**：コマンドを否定するか、または設定をデフォルトに戻します。 • **permit**：一致するアドレスを許可します。 • **range**：プロファイルの IP アドレスの範囲を指定します。 単一の IP アドレス、または開始アドレスと終了アドレスで指定された IP アドレス範囲を入力できます。 デフォルトでは、スイッチには IGMP プロファイルが設定されていません。 （注） プロファイルを削除するには、**no ip igmp profile***profile number* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**permit** | **deny** 例： `Switch(config-igmp-profile)# permit`	（任意）IP マルチキャスト アドレスへのアクセスを許可または拒否するアクションを設定します。 アクションを設定しないと、プロファイルのデフォルト設定はアクセス拒否になります。
ステップ 5	**range***ip multicast address* 例： `Switch(config-igmp-profile)# range 229.9.9.0`	アクセスを制御する IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を入力します。 範囲を入力する場合は、IP マルチキャスト アドレスの下限値、スペースを 1 つ、IP マルチキャスト アドレスの上限値を入力します。 **range** コマンドを複数回入力すると、複数のアドレスまたはアドレス範囲を入力できます。 （注） IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を削除するには、**no range** *ip multicast address* IGMP プロファイル コンフィギュレーション コマンドを使用します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip igmp profile***profile number* 例： `Switch# show ip igmp profile 3`	プロファイルの設定を確認します。

	コマンドまたはアクション	目的
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP フィルタリングおよびスロットリング, （1240 ページ）

IGMP スヌーピングの制約事項, （1228 ページ）

IGMP プロファイルの適用

IGMP プロファイルで定義されているとおりにアクセスを制御するには、プロファイルを該当するインターフェイスに適用する必要があります。 IGMP プロファイルを適用できるのは、レイヤ 2 アクセス ポートだけです。ルーテッド ポートや SVI には適用できません。 EtherChannel ポートグループに所属するポートに、プロファイルを適用することはできません。 1 つのプロファイルを複数のインターフェイスに適用できますが、1 つのインターフェイスに適用できるプロファイルは 1 つだけです。

スイッチ ポートに IGMP プロファイルを適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp filter***profile number*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスは、EtherChannel ポート グループに所属していないレイヤ 2 ポートでなければなりません。
ステップ 4	**ip igmp filter***profile number* 例： `Switch(config-if)# ip igmp filter 321`	インターフェイスに指定された IGMP プロファイルを適用します。 指定できる範囲は 1 ～ 4294967295 です。 （注） インターフェイスからプロファイルを削除するには、**no ip igmp filter***profile number* インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

IGMP フィルタリングおよびスロットリング, （1240 ページ）
IGMP スヌーピングの制約事項, （1228 ページ）

IGMP グループの最大数の設定

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定するには、次の手順を実行します。

はじめる前に

この制限が適用されるのはレイヤ 2 ポートだけです。ルーテッド ポートや SVI には IGMP グループの最大数を設定できません。 このコマンドは、論理 EtherChannel インターフェイスでも使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp max-groups***number*
5. **end**
6. **show running-config interface***interface-id*
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。

	コマンドまたはアクション	目的
	`gigabitethernet1/0/2`	
ステップ 4	**ip igmp max-groups***number* 例： `Switch(config-if)# ip igmp max-groups 20`	インターフェイスが加入できる IGMP グループの最大数を設定します。 指定できる範囲は 0 ～ 4294967294 です。 デフォルトでは最大数は設定されません。 （注） グループの最大数に関する制限を削除し、デフォルト設定（制限なし）に戻すには、**no ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface***interface-id* 例： `Switch# show running-config interface gigabitethernet1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP フィルタリングおよびスロットリング, （1240 ページ）

IGMP スヌーピングの制約事項, （1228 ページ）

IGMP スロットリング アクションの設定

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定した後、受信した IGMP レポートの新しいグループで、既存のグループを上書きするようにインターフェイスを設定できます。

転送テーブルに最大数のエントリが登録されているときにスロットリング アクションを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip igmp max-groups action** {**deny** | **replace**}
5. **end**
6. **show running-config interface***interface-id*
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。 トランク ポートをインターフェイスにすることはできません。
ステップ 4	**ip igmp max-groups action** {**deny** | **replace**} 例： `Switch(config-if)# ip igmp max-groups action replace`	インターフェイスが IGMP レポートを受信したときに、転送テーブルに最大数のエントリが登録されている場合は、次のいずれかのアクションをインターフェイスに指定します。 • **deny**：レポートを廃棄します。 このスロットリング アクションを設定すると、すでに転送テーブルに登録されていたエントリは、削除されることはありませんが期限切れになります。 エントリが期限切れになり、最大数のエントリが転送テーブルに登録されていると、スイッチは、インターフェイスで受信した次の IGMP レポートを廃棄します。 • **replace**：既存のグループを、IGMP レポートを受信した新しいグループで上書きします。 このスロットリング アクションを設定すると、すでに転送テーブルに登録されていたエントリは削除されます。 転送テーブルのエントリが最大数まで達したら、スイッ

	コマンドまたはアクション	目的
		チはランダムに選択したエントリを受信した IGMP レポートで上書きします。 スイッチが転送テーブルのエントリを削除しないようにするには、インターフェイスにより転送テーブルにエントリが追加される前に、IGMP スロットリング アクションを設定します。 （注） レポートの廃棄というデフォルトのアクションに戻すには、**no ip igmp max-groups action** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface***interface-id* 例： `Switch# show running-config interface gigabitethernet1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IGMP フィルタリングおよびスロットリング, （1240 ページ）

IGMP スヌーピングの制約事項, （1228 ページ）

IGMP スヌーピングおよび MVR のモニタリング

IGMP スヌーピング情報のモニタリング

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

表 *120*：*IGMP* スヌーピング情報を表示するためのコマンド

コマンド	目的
show ip igmp snooping [**vlan***vlan-id* [detail]]	スイッチ上のすべての VLAN または特定の VLAN のスヌーピング設定情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan***vlan-id* を入力します。 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ip igmp snooping groups [**count** |**dynamic** [**count**] | **user** [**count**]]	スイッチまたは特定のパラメータに関して、マルチキャスト テーブル情報を表示します。 • **count**：実際のエントリではなく、特定のコマンドオプションのエントリの総数を表示します。 • **dynamic**：IGMP スヌーピングによって学習されたエントリを表示します。 • **user**：ユーザによって設定されたマルチキャストエントリだけを表示します。

コマンド	目的
show ip igmp snooping groups vlan*vlan-id* [*ip_address*| **count** | **dynamic** [**count**] | **user**[**count**]]	マルチキャスト VLAN またはその VLAN の特定のパラメータについて、マルチキャスト テーブル情報を表示します。 • *vlan-id*：VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • **count**：実際のエントリではなく、特定のコマンドオプションのエントリの総数を表示します。 • **dynamic**：IGMP スヌーピングによって学習されたエントリを表示します。 • *ip_address*：指定したグループ IP アドレスのマルチキャスト グループの特性を表示します。 • **user**：ユーザによって設定されたマルチキャストエントリだけを表示します。
show ip igmp snooping mrouter[**vlan***vlan-id*]	ダイナミックに学習され、手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。 （注） IGMP スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先インターフェイスを自動的に学習します。 これらのインターフェイスは動的に学習されます。 （任意）特定の VLAN に関する情報を表示するには、**vlan***vlan-id* を入力します。
show ip igmp snooping querier[**vlan***vlan-id*] **detail**	IP アドレスおよび VLAN で受信した最新の IGMP クエリー メッセージの受信ポートに関する情報、VLAN の IGMP スヌーピング クエリアの設定および動作ステートに関する情報を表示します。

MVR のモニタリング

スイッチまたは指定されたインターフェイスの MVR をモニタするには、次の MVR 情報を表示します。

表 *121*：*MVR* 情報を表示するためのコマンド

コマンド	目的
show mvr	スイッチの MVR ステータスおよび値を表示します。これは、MVR のイネーブルまたはディセーブルの判別、マルチキャスト VLAN、マルチキャスト グループの最大数（256）および現在の数（0 ～ 256）、クエリーの応答時間、および MVR モードです。
show mvrinterface [*interface-id*] [**members** [**vlan***vlan-id*]]	すべての MVR インターフェイスおよびその MVR 設定を表示します。 特定のインターフェイスを指定すると、次の情報が表示されます。 • Type：Receiver または Source • Status：次のいずれか ◦ ACTIVE は、ポートが VLAN に含まれていることを意味します。 ◦ UP/DOWN は、ポートが転送中または転送中ではないことを示します。 ◦ INACTIVE は、ポートが VLAN に含まれていないことを意味します。 • Immediate Leave：Enabled または Disabled **members** キーワードを入力すると、そのポート上のすべてのマルチキャスト グループ メンバが表示されます。VLAN ID を入力した場合は、VLAN 上のすべてのマルチキャスト グループ メンバが表示されます。 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show mvr members [*ip-address*]	すべての IP マルチキャスト グループまたは指定した IP マルチキャスト グループ IP アドレスに含まれているレシーバ ポートおよび送信元ポートがすべて表示されます。

IGMP フィルタリングおよび IGMP スロットリングの設定のモニタリング

IGMP プロファイルの特性を表示したり、スイッチ上のすべてのインターフェイスまたは指定されたインターフェイスの IGMP プロファイルや最大グループ設定を表示したりできます。 また、スイッチ上のすべてのインターフェイスまたは指定したインターフェイスに関する IGMP スロットリング設定を表示することもできます。

表 *122*：*IGMP* フィルタリングおよび *IGMP* スロットリング設定を表示するためのコマンド

コマンド	目的
show ip igmp profile [*profile number*]	特定の IGMP プロファイルまたはスイッチ上で定義されているすべての IGMP プロファイルを表示します。
show running-config[**interface***interface-id*]	インターフェイスが所属できる IGMP グループの最大数（設定されている場合）や、インターフェイスに適用される IGMP プロファイルを含む、特定のインターフェイスまたはスイッチ上のすべてのインターフェイスの設定を表示します。

IGMP スヌーピングおよび MVR の設定例

例：CGMP パケットを使用した IGMP スヌーピングの設定

次に、CGMP パケットを学習方式として使用するように IGMP スヌーピングを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
```

例：マルチキャスト ルータへの静的な接続のイネーブル化

次に、マルチキャスト ルータへの静的な接続をイネーブルにする例を示します。

```
Switch configure terminal
Switch ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Switch end
```

関連トピック

マルチキャスト ルータ ポートの設定，（1246 ページ）

例：グループに加入するホストの静的な設定

次に、ポート上のホストを静的に設定する例を示します。

```
Switch#  configure terminal
Switch#  ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/0/1
Switch#  end
```

関連トピック

グループに加入するホストの静的な設定，（1248 ページ）

マルチキャスト グループへの加入, （1232 ページ）

例：IGMP 即時脱退のイネーブル化

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

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end
```

関連トピック

IGMP 即時脱退のイネーブル化, （1249 ページ）

即時脱退 , （1234 ページ）

例：IGMP スヌーピング クエリアの送信元アドレスの設定

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end
```

関連トピック

IGMP スヌーピング クエリアの設定, （1257 ページ）

IGMP スヌーピング, （1230 ページ）

例：IGMP スヌーピング クエリアの最大応答時間の設定

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end
```

関連トピック

IGMP スヌーピング クエリアの設定, （1257 ページ）

IGMP スヌーピング, （1230 ページ）

例：IGMP スヌーピング クエリア タイムアウトの設定

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end
```

関連トピック

IGMP スヌーピング クエリアの設定, （1257 ページ）

IGMP スヌーピング, （1230 ページ）

例：IGMP スヌーピング クエリア機能の設定

次に、IGMP スヌーピング クエリア機能をバージョン 2 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end
```

関連トピック

IGMP スヌーピング クエリアの設定, （1257 ページ）

IGMP スヌーピング, （1230 ページ）

例：IGMP プロファイルの設定

次に、単一の IP マルチキャスト アドレスへのアクセスを許可する IGMP プロファイル 4 を作成して、設定を確認する例を示します。アクションが拒否（デフォルト）である場合は、**show ip igmp profile** の出力には表示されません。

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

例：IGMP プロファイルの適用

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

例：IGMP グループの最大数の設定

次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

例：MVR グローバル パラメータの設定

次に、MVR をイネーブルにして、MVR グループ アドレスを設定し、クエリー タイムを 1 秒（10 分の 10 秒）に設定し、MVR マルチキャスト VLAN を VLAN 22 として指定し、MVR モードをダイナミックに設定する例を示します。

```
Switch(config)# mvr
Switch(config)# mvr group 228.1.23.4
Switch(config)# mvr querytime 10
Switch(config)# mvr vlan 22
Switch(config)# mvr mode dynamic
```

```
Switch(config)# end
```

例：MVR インターフェイスの設定

次に、ポートをレシーバ ポートとして設定し、マルチキャスト グループ アドレスに送信されたマルチキャスト トラフィックを受信するようにポートを静的に設定し、ポートに即時脱退機能を設定し、結果を確認する例を示します。

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr type receiver
Switch(config-if)# mvr vlan 22 group 228.1.23.4
Switch(config-if)# mvr immediate
Switch(config)# end
Switch# show mvr interface

Port Type Status Immediate Leave
---- ---- ------- ---------------
Gi1/0/2 RECEIVER ACTIVE/DOWN ENABLED
```

第 45 章

MSDP の設定

- 機能情報の確認，1283 ページ
- MSDP の前提条件，1283 ページ
- Multicast Source Discovery Protocol に関する情報，1284 ページ
- MSDP の設定方法，1293 ページ
- MSDP のモニタリングおよびメンテナンス，1315 ページ
- MSDP の設定例，1318 ページ

機能情報の確認

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

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

MSDP の前提条件

MSDP を使用するには、Catalyst 3560-CX スイッチで IP サービス フィーチャ セットをイネーブルにする必要があります。

Multicast Source Discovery Protocol に関する情報

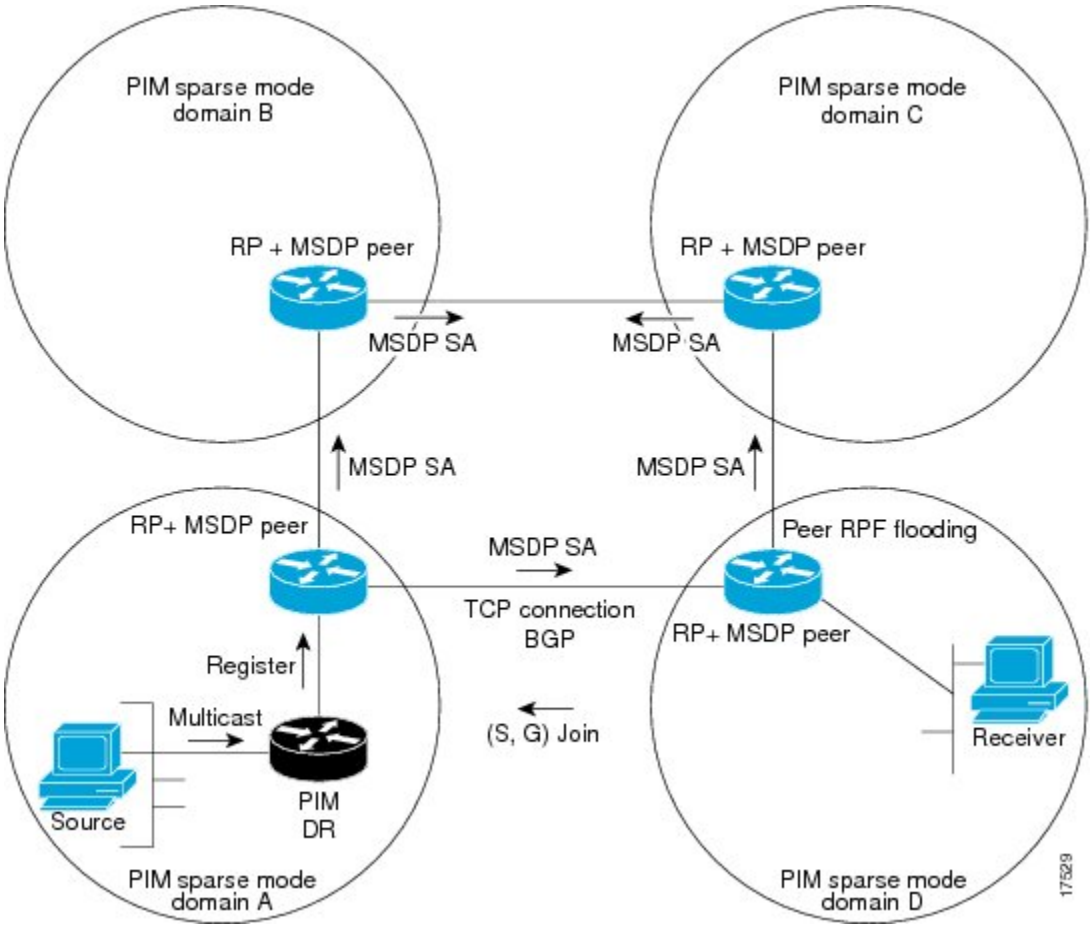
MSDP は複数の PIM-SM ドメインを接続するメカニズムです。 MSDP は、他の PIM ドメイン内のマルチキャスト送信元を検出することを目的としています。 MSDP の主な利点は、（一般的な共有ツリーではなく）ドメイン間ソース ツリーを PIM-SM ドメインで使用できるようにし、複数の PIM-SM ドメインを相互接続する複雑性を軽減することです。 MSDP がネットワークで設定されている場合、RP は他のドメイン内の RP と送信元情報を交換します。 RP は、レシーバがいるグループに送信するソースのドメイン間ソース ツリーに参加できます。 RP は、そのドメイン内の共有ツリーのルートであり、アクティブ レシーバが存在するドメイン内のすべてのポイントへのブランチがあるため、これを行うことができます。 PIM-SM ドメイン外の新しい送信元を（共有ツリーの送信元からのマルチキャスト パケットの到着によって）ラスト ホップ デバイスが認識すると、その送信元に加入要求を送信してドメイン間ソース ツリーに参加できます。

（注） RP に特定グループの共有ツリーがないか、発信インターフェイス リストがヌルの共有ツリーがある場合は、別のドメインの発信元に加入要求を送信しません。

MSDP がイネーブルになっている場合、PIM-SM ドメインの RP は、他のドメインの MSDP 対応デバイスとの MSDP ピアリング関係を維持します。 このピアリング関係は TCP 接続を通じて発生します。交換されるのは主にマルチキャスト グループを送信する送信元のリストです。 MSDP はピアリング接続に TCP（ポート 639）を使用します。 BGP と同様に、ポイントツーポイント TCP ピアリングを使用する場合は、各ピアを明示的に設定する必要があります。 さらに、RP 間の TCP 接続は基本的なルーティング システムによって実現されます。 受信側の RP では、送信元リストを使用して送信元のパスが確立されます。マルチキャスト ソースがレシーバがいるドメインの対象である場合、マルチキャスト データは PIM-SM で提供される通常のソース ツリー構築メカニズムを使用して配信されます。 MSDP は、グループを送信する送信元のアナウンスにも使用されます。 これらのアナウンスは、ドメインの RP で発信する必要があります。

図に、2 つの MSDP ピア間の MSDP の動作を示します。 PIM では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP が使用されます。

図 *87* : *RP* ピア間で動作する *MSDP*



MSDP が実装されている場合、次のイベント シーケンスが発生します。

1 図に示すように、PIM 指定デバイス（DR）が送信元を RP に登録すると、その RP が Source-Active（SA）メッセージをすべての MSDP ピアに送信します。

（注） DR は、（ソースがアクティブになると）カプセル化されたデータをソースごとに 1 回だけ RP に送信します。 ソースがタイムアウトした場合、ソースが再度アクティブになるとこのプロセスが実行されます。 これは、発信元 RP に登録されているすべての発信元を含んでいる定期的な SA メッセージの場合とは異なります。 これらの SA メッセージは MSDP 制御パケットであるため、アクティブな送信元からのカプセル化されたデータを含んでいません。

1 SA メッセージでは、ソース アドレス、ソースの送信先グループ、および RP のアドレスまたは発信者 ID が識別されます（設定されている場合）。

2. SA メッセージを受信する各 MSDP ピアは、発信者からのダウンストリームのすべてのピアに SA メッセージをフラッディングします。 場合によっては（図の PIM-SM ドメイン B および C 内の RP の場合など）、RP は複数の MSDP ピアからの SA メッセージのコピーを受信することがあります。 ループが作成されないように、RP は BGP ネクスト ホップ データベースに問い合わせて、SA メッセージの発信者へのネクスト ホップを識別します。 MBGP とユニキャスト BGP の両方が設定されている場合、MBGP が最初に確認されてからユニキャスト BGP が確認されます。 そのネクストホップ ネイバーが発信元の RPF ピアです。 RPF ピアへのインターフェイス以外のインターフェイスにある発信元から受信した SA メッセージはドロップされます。 そのため、SA メッセージ フラッディング プロセスはピア RPF フラッディングと呼ばれます。 ピア RPF フラッディング メカニズムにより、BGP または MBGP は MSDP とともに実行する必要があります。

1. SA メッセージを受信した RP は、グループの (*, G) 送信インターフェイス リストにインターフェイスが存在するかどうかを確認することによって、そのドメイン内にアドバタイズされたグループのメンバが存在するかどうかを確認します。 グループ メンバが存在しない場合、RP は何も実行しません。 グループ メンバが存在する場合、RP は（S, G）加入要求を送信元に送信します。 その結果、ドメイン間ソース ツリーのブランチが自律システムの RP との境界に構築されます。 マルチキャスト パケットは、RP に着信すると、その共有ツリーを経由して RP のドメイン内のグループ メンバに転送されます。 メンバの DR は、標準的な PIM-SM 手順を使用してソースへのランデブー ポイント ツリー（RPT）に加入することもできます。

2. 発信元 RP は、送信元がグループにパケットを送信し続ける限り、60 秒ごとに（S, G）ステートに関する SA メッセージを定期的に送信し続けます。 RP は SA メッセージを受信すると、SA メッセージをキャッシュします。 たとえば、発信元 RP 10.5.4.3 から (172.16.5.4, 228.1.2.3) に対する SA メッセージを受信したとします。 RP は mroute テーブルを確認し、グループ 228.1.2.3 にアクティブなメンバが存在しないことを検出すると、SA メッセージを 10.5.4.3 のダウンストリームにあるピアに渡します。 次に、ドメイン内のホストが加入要求をグループ 228.1.2.3 の RP に送信した場合、その RP はホストへのインターフェイスを (*, 224.1.2.3) エントリの発信インターフェイス リストに追加します。 RP は SA メッセージをキャッシュするため、デバイスは (172.16.5.4, 228.1.2.3) のエントリを持ち、ホストが加入を要求するとすぐにソース ツリーに加入できます。

（注） 現行のすべてのサポート対象のソフトウェア リリースでは、MSDP SA メッセージのキャッシュは必須であり、手動でイネーブルまたはディセーブルにすることはできません。 デフォルトでは、MSDP ピアが設定されると、**ipmulticastcache-sa-state** コマンドが自動的に実行コンフィギュレーションに追加されます。

MSDP の利点

MSDP には次の利点があります。

- 共有されたマルチキャスト配信ツリーが分割され、共有ツリーがドメインに対してローカルになるように設定できます。 ローカルメンバーはローカルツリーに加入します。共有ツリーへの Join メッセージはドメインから脱退する必要はありません。
- PIM SM ドメインは独自の RP だけを信頼するため、他のドメインの RP に対する信頼度が低下します。 このため、送信元の情報がドメイン外部に漏れないようにでき、セキュリティが高まります。
- レシーバーだけが配置されているドメインは、グループ メンバーシップをグローバルにアドバタイズしなくても、データを受信できます。
- グローバルな送信元マルチキャスト ルーティング テーブル ステートが不要になり、メモリが削減されます。

デフォルト MSDP ピア

スタブ自律システムには、冗長性を実現するために複数の RP との MSDP ピアリングが必要な場合もあります。 たとえば、RPF チェック メカニズムがないため、SA メッセージは複数のデフォルト ピアから受け入れられません。 その代わりに、SA メッセージは 1 つのピアからだけ受け入れられます。 そのピアに障害が発生した場合、SA メッセージは別のピアから受け入れられます。 もちろん、デフォルトのピアが両方とも同じ SA メッセージを送信することがこの基本的な前提となっています。

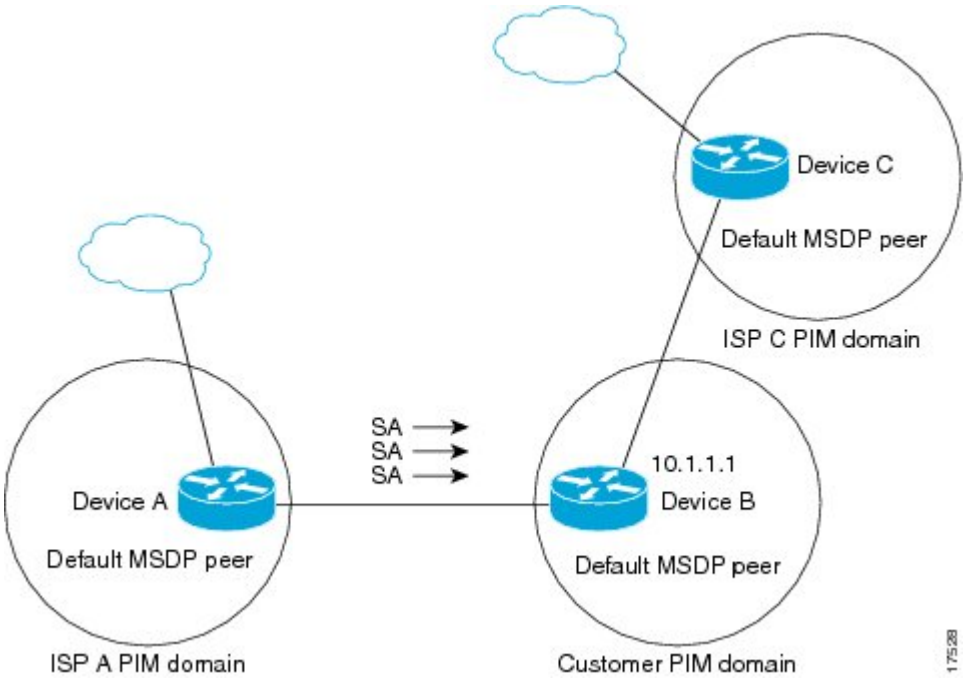
下の図に、デフォルトの MSDP ピアが使用されるシナリオを示します。 この図では、デバイス B を所有するカスタマーが 2 つのインターネット サービス プロバイダー（ISP）を介してインターネットに接続されています。一方の ISP はデバイス A を所有し、もう一方の ISP はデバイス C を所有しています。どちらもそれらの間で BGP も MBGP も実行していません。 カスタマーが ISP ドメインまたは他のドメイン内のソースについて学習するために、デバイス B はデバイス A をデフォルト MSDP ピアとして識別します。 デバイス B はデバイス A とデバイス C の両方に SA メッセージをアドバタイズしますが、デバイス A だけまたはデバイス C だけから SA メッセージを受け入れます。 デバイス A が設定内の最初のデフォルト ピアである場合、デバイス A が稼働していれば デバイス A が使用されます。 デバイス A が稼働していない場合に限り、デバイス B がデバイス C からの SA メッセージを受け入れます。

ISP は、プレフィックス リストを使用して、カスタマーのデバイスから受け入れるプレフィックスを定義する場合もあります。 カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

カスタマーは 2 つの ISP を使用しています。 カスタマーはこの 2 つの ISP をデフォルト ピアとして定義します。 設定内で最初のデフォルト ピアとして特定されているピアが稼働している限り、

このピアがデフォルト ピアになり、カスタマーはそのピアから受信するすべての SA メッセージを受け入れます。

図 *88*：デフォルト *MSDP* ピアのシナリオ



デバイス B はデバイス A およびデバイス C に SA をアドバタイズしますが、デバイス A またはデバイス C だけを使用して SA メッセージを受け入れます。 デバイス A が設定内の最初のデバイスである場合、デバイス A が稼働していればデバイス A が使用されます。 デバイス A が稼働していない場合に限り、デバイス B がデバイス C から SA メッセージを受け入れます。これは、プレフィックス リストを使用しない動作です。

プレフィックス リストを指定すると、リスト内のプレフィックスに対してだけピアはデフォルト ピアになります。 プレフィックスリストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。 プレフィックス リストがない場合も、複数のデフォルト ピアを設定できますが、アクティブなデフォルト ピアになるのは最初のピアだけです（このピアにデバイスが接続されていて、ピアがアクティブの場合に限ります）。 最初に設定されたピアがダウンするか、このピアとの接続がダウンした場合、2 番目に設定されたピアがアクティブなデフォルト ピアになります。以下同様です。

MSDP メッシュ グループ

MSDP メッシュ グループは、MSDP によってフル メッシュ型に相互接続された MSDP スピーカーのグループです。 つまり、グループの各 MSDP ピアには、グループ内の他のすべての MSDP ピアとの MSDP ピアリング関係（MSDP 接続）が必要です。 MSDP メッシュ グループが MSDP ピアのグループ間に設定されている場合、SA メッセージのフラッディングが削減されます。 グループ内の MSDP ピアがグループ内の別の MSDP ピアから SA メッセージを受信すると、この SA メッ

セージはグループ内のその他のすべての MSDP ピアに送信されたとみなされるためです。 その結果、受信側の MSDP ピアがグループ内の他の MSDP ピアに SA メッセージをフラッディングする必要はありません。

MSDP メッシュ グループの利点

- SA フラッディングの最適化：グループ内に複数のピアがある場合、SA フラッディングを最適化するために MSDP メッシュ グループは特に有用です。
- インターネットを通過する SA トラフィック量の削減：MSDP メッシュ グループを使用すると、SA メッセージは他のメッシュ グループ ピアにフラッディングされません。
- 着信 SA メッセージの RPF チェックの省略：MSDP メッシュ グループが設定されていると、メッシュ グループ ピアからの SA メッセージは常に受け入れられます。

SA 発信フィルタ

デフォルトでは、MSDP を実行するように設定されている RP は、それが RP であるすべてのローカル ソースの SA メッセージを発信します。 そのため、RP に登録されているローカル ソースは SA メッセージでアドバタイズされますが、これが望ましくない場合もあります。 たとえば、PIM-SM ドメイン内のソースがプライベート アドレス（たとえば、ネットワーク 10.0.0.0/8）を使用している場合、SA 発信フィルタを設定してこれらのアドレスがインターネット上の他の MSDP ピアにアドバタイズされないようにする必要があります。

SA メッセージでアドバタイズされるソースを制御するには、RP に SA 発信フィルタを設定します。 SA 発信フィルタを作成すると、SA メッセージでアドバタイズされるソースを次のように制御できます。

- デバイスが SA メッセージでローカル ソースをアドバタイズしないように RP を設定できます。 この場合もデバイスは通常の方法で他の MSDP ピアからの SA メッセージを転送します。ローカル ソースの SA メッセージは発信しません。
- 拡張アクセス リストで定義されている（S, G）ペアと一致する、特定のグループに送信するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。 その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- AS パス アクセス リストで定義されている AS パスと一致する、特定のグループに送信するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。 その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- ルート マップで定義されている基準と一致するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。 その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- 拡張アクセス リスト、AS パス アクセス リスト、およびルート マップ（またはそれらのその組み合わせ）を含む SA 発信フィルタを設定します。 この場合、ローカル ソースが SA メッセージでアドバタイズされる前に、すべての条件を満たしている必要があります。

MSDP での発信フィルタ リストの使用

デフォルトでは、MSDP 対応デバイスは、受信したすべての SA メッセージをその MSDP ピアすべてに転送します。 ただし、発信フィルタ リストを作成することで、SA メッセージが MSDP ピアに転送されないようにできます。 発信フィルタ リストは、ローカルに発信されたか別の MSDP ピアから受信したかに関係なくすべての SA メッセージに適用されますが、SA 発信フィルタはローカルに発信された SA メッセージだけに適用されます。 ローカル デバイスから発信される MSDP SA メッセージのフィルタをイネーブルにする方法の詳細については、ローカル ソースの RP によって発信された SA メッセージの制御を参照してください。

発信フィルタ リストを作成すると、デバイスがピアへ転送する SA メッセージを次のように制御できます。

- 指定した MSDP ピアへ転送したすべての発信 SAメッセージをフィルタリングするには、MSDP ピアへの SA メッセージの転送を停止するようにデバイスを設定します。
- 指定した MSDP ピアへ転送した発信 SA メッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアに基づいてフィルタリングするには、拡張アクセス リストで許可されている（S, G）ペアに一致する MSDP ピアへの SA メッセージだけを転送するようにデバイスを設定します。 その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- 指定した MSDP へ転送した発信 SA メッセージのサブセットをルート マップに定義された一致基準に基づいてフィルタリングするには、ルート マップに定義された基準に一致する SA メッセージだけを転送するようにデバイスを設定します。 その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- 指定したピアからの発信 SA メッセージのサブセットを SA メッセージに含まれているアナウンス側 RP アドレスに基づいてフィルタリングするには、SA メッセージが1 つ以上の MSDP ピアに送信されていても、それらの発信元に基づいて発信 SA メッセージをフィルタリングするようにデバイスを設定します。 その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- 拡張アクセス リスト、ルート マップ、および RP アクセス リストまたは RP ルート マップのいずれかを含む発信フィルタ リストを設定できます。 この場合、MSDP ピアで発信 SA メッセージを転送するにはすべての条件を満たしている必要があります。

注意 SA メッセージの任意のフィルタリングを実行すると、ダウンストリーム MSDP ピアで正当なアクティブソースの SA メッセージを受信できなくなることがあります。 そのため、このタイプのフィルタを使用する場合は注意が必要です。 通常、発信フィルタ リストは、プライベート アドレスを使用するソースなど、望ましくないソースを拒否するためだけに使用します。

MSDP での着信フィルタ リストの使用

デフォルトでは、MSDP 対応デバイスは MSDP ピアからそのデバイスに送信されたすべての SA メッセージを受信します。 ただし、着信フィルタ リストを作成することによって、MSDP ピアからデバイスが受信する送信元情報を制御できます。

着信フィルタ リストを作成すると、デバイスがピアから受信する着信 SA メッセージを次のように制御できます。

- 指定した MSDP ピアからのすべての着信 SAメッセージをフィルタリングするには、指定した MSDP ピアから送信されたすべての SAメッセージを無視するようにデバイスを設定します。
- 指定したピアからの着信SAメッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアに基づいてフィルタリングするには、拡張アクセス リストに定義された（S, G）ペアに一致する MSDP ピアからの SA メッセージだけを受信するようにデバイスを設定します。 MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 指定したピアからの着信 SA 要求メッセージのサブセットをルート マップに定義された一致基準に基づいてフィルタリングするには、ルート マップに指定された基準に一致する SA メッセージだけを受信するようにデバイスを設定します。 MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 指定したピアからの着信SAメッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアと、ルート マップに定義された基準の両方に基づいてフィルタリングするには、拡張アクセス リストに定義された（S, G）ペアと、ルート マップに定義された基準の両方に一致する着信 SA メッセージだけを受信するようにデバイスを設定します。 MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 指定したピアからの着信 SA メッセージのサブセットを SA メッセージに含まれているアナウンス側 RP アドレスに基づいてフィルタリングするには、SA メッセージがすでに1 つ以上の MSDP ピア全体に送信されている可能性がある場合でも、それらの発信元に基づいて着信 SA メッセージをフィルタリングするようにデバイスを設定します。
- 拡張アクセス リスト、ルート マップ、および RP アクセス リストまたは RP ルート マップのいずれかを含む着信フィルタ リストを設定できます。 この場合、MSDP ピアで着信 SA メッセージを受信するにはすべての条件を満たしている必要があります。

注意 SA メッセージの任意のフィルタリングを実行すると、ダウンストリーム MSDP ピアで正当なアクティブソースの SA メッセージを受信できなくなることがあります。 そのため、このタイプのフィルタを使用する場合は注意が必要です。 通常、着信フィルタ リストは、プライベートアドレスを使用するソースなど、望ましくないソースを拒否するためだけに使用されます。

MSDP の TTL しきい値

存続可能時間（TTL）値を使用して、ドロップされる前にパケットが取得できるホップの数を制限できます。 特定の MSDP ピアに送信された、データがカプセル化された SA メッセージの TTL を指定するには、**ip multicast ttl-threshold** コマンドを使用します。 デフォルトでは、パケットの TTL 値が 0（標準 TTL 動作）より大きい場合は、SA メッセージのマルチキャスト データ パケットは MSDP ピアに送信されます。

一般に、TTL しきい値の問題は、SA メッセージ内でソースの初期マルチキャスト パケットがカプセル化されることによって発生することがあります。 マルチキャストパケットはユニキャスト SA メッセージ内部でカプセル化されるため（TTL は 255）、SA メッセージが MSDP ピアに送信されるときに TTL は減少しません。 さらに、マルチキャスト トラフィックおよびユニキャスト トラフィックは MSDP ピア、したがってリモート PIM-SM ドメインへのまったく異なるパスに従うため、SA メッセージが通過するホップの総数は、通常のマルチキャスト パケットとは大きく異なります。 その結果、カプセル化されたパケットはTTL しきい値に違反することになります。 この問題を解決するには、**ip multicast ttl-threshold** コマンドを使用して、特定の MSDP ピアに送信された SA メッセージにカプセル化されているマルチキャスト パケットに関連付けられた TTL しきい値を設定します。 **ip msdp ttl-threshold** コマンドを使用すると、IP ヘッダーの TTL が *ttl-value* 引数に指定されている TTL 値未満であるマルチキャスト パケットが、ピアに送信される SA メッセージにカプセル化されないようにすることができます。

MSDP メッセージ タイプ

MSDP メッセージには 4 つの基本タイプがあり、それぞれが固有の Type、Length、および Value（TLV）データ フォーマットでエンコードされています。

SA メッセージ

SA メッセージを使用して、ドメイン内のアクティブなソースをアドバタイズします。 また、これらの SA メッセージには送信元によって送信された最初のマルチキャスト データ パケットが含まれていることがあります。

SA メッセージには、発信元 RP の IPアドレスと、アドバタイズされる 1 つ以上の（S, G）ペアが含まれています。 また、SA メッセージにカプセル化されたデータ パケットが含まれていることがあります。

SA 要求メッセージ

SA 要求メッセージを使用して、特定のグループにアクティブなソースのリストを要求します。 これらのメッセージは、SA キャッシュにアクティブな（S, G）ペアのリストを保持する MSDP SA キャッシュに送信されます。 グループ内のすべてのアクティブなソースが発信元の RP によって再アドバタイズされるまで待つ代わりに、SA 要求メッセージを使用してアクティブなソースのリストを要求すると、加入遅延を短縮できます。

SA 応答メッセージ

SA 応答メッセージは SA 要求メッセージに応答する MSDP ピアによって送信されます。 SA 応答メッセージには、発信元の RP の IP アドレスと、キャッシュに保存されている発信元 RP のドメイン内のアクティブなソースの 1 つ以上の（S, G）ペアが含まれています。

キープアライブ メッセージ

キープアライブ メッセージは60秒ごとに送信され、MSDPセッションをアクティブに保ちます。キープアライブ メッセージまたは SA メッセージを 75 秒間受信しなかった場合、MSDP セッションがリセットされます。

MSDP のデフォルト設定

MSDP はイネーブルになっていません。デフォルトの MSDP ピアはありません。

MSDP の設定方法

デフォルトの MSDP ピアの設定

はじめる前に

MSDP ピアを設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp default-peer***ip-address* | *name* [**prefix-list***list*] 例： `Router(config)# ip msdp`	すべての MSDP SA メッセージの受信元となるデフォルト ピアを定義します。 • *ip-address* | *name* には、MSDP デフォルト ピアの IP アドレスまたはドメイン ネーム システム（DNS）サーバ名を入力します。

	コマンドまたはアクション	目的
	`default-peer 10.1.1.1 prefix-list site-a`	• （任意）**prefix-list***list* を指定する場合は、リスト内のプレフィックス専用のデフォルト ピアとなるピアを指定するリスト名を入力します。 プレフィックス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。 **prefix-list** キーワードが指定された **ip msdp default-peer** コマンドを複数入力すると、複数の RP プレフィックスに対してすべてのデフォルト ピアが同時に使用されます。 この構文は通常、スタブ サイト クラウドに接続されたサービス プロバイダー クラウドで使用されます。 **prefix-list** キーワードを指定せずに **ip msdp default-peer** コマンドを複数入力すると、単一のアクティブ ピアですべての SA メッセージが受信されます。 このピアに障害がある場合は、次の設定済みデフォルト ピアですべての SA メッセージが受信されます。 この構文は通常、スタブ サイトで使用されます。
ステップ 4	**ip prefix-list***name* [**description***string*] | **seq***number* {**permit** | **deny**} *networklength* 例： `Router(config)# prefix-list site-a seq 3 permit 12 network length 128`	（任意）ステップ 2 で指定された名前を使用し、プレフィックス リストを作成します。 • （任意）**description***string* には、このプレフィックス リストを説明する 80 文字以下のテキストを入力します。 • **seq***number* には、エントリのシーケンス番号を入力します。 指定できる範囲は 1 ～ 4294967294 です。 • **deny** キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。 • **permit** キーワードを指定すると、条件が一致した場合にアクセスが許可されます。 • *network length* には、許可または拒否されているネットワークの番号およびネットワーク マスク長（ビット単位）を指定します。
ステップ 5	**ip msdp description** {*peer-name* | *peer-address*} *text* 例： `Router(config)# ip msdp description peer-name site-b`	（任意）設定内で、または **show** コマンド出力内で簡単に識別できるように、指定されたピアの説明を設定します。 デフォルトでは、MSDP ピアに説明は関連付けられていません。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SA ステートのキャッシング

メモリを消費して送信元情報の遅延を短縮する場合は、SA メッセージをキャッシュに格納するようにスイッチを設定できます。 送信元とグループのペアのキャッシングをイネーブルにするには、次の手順を実行します。

送信元とグループのペアのキャッシングをイネーブルにするには、次の手順に従います。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip msdp cache-sa-state** [**list***access-list-number*] 例： `Switch(config)# ip msdp cache-sa-state 100`	送信元とグループのペアのキャッシングをイネーブルにします（SA ステートを作成します）。アクセス リストを通過したこれらのペアがキャッシュに格納されます。 **list***access-list-number* を指定する場合、範囲は 100 ～ 199 です。 （注） このコマンドの代わりに、**ip msdp sa-reques** グローバル コンフィギュレーション コマンドを使用できます。この代替コマンドを使用すると、グループの新しいメンバがアクティブになった場合に、SA 要求メッセージがスイッチから MSDP ピアに送信されます。
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *protocolsourcesource-wildcarddestination destination-wildcard* 例： `Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255`	IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* の範囲は 100 ～ 199 です。 ステップ 2 で作成した番号と同じ値を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

MSDP ピアからの送信元情報の要求

グループへの送信元である接続 PIM SM ドメイン内のアクティブなマルチキャスト送信元を、グループの新しいメンバが学習する必要がある場合は、新しいメンバがグループに加入したときに、指定された MSDP ピアに SA 要求メッセージがスイッチから送信されるようにこのタスクを実行します。 ピアは SA キャッシュ内の情報に応答します。 ピアにキャッシュが設定されていない場合、このコマンドを実行しても何も起こりません。 この機能を設定すると加入遅延は短縮されますが、メモリが消費されます。

新しいメンバがグループに加入し、マルチキャスト トラフィックを受信する必要が生じた場合、MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定するには、次の手順を実行します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip msdp sa-request** {*ip-address* | *name*} 例： `Switch(config)# ip msdp sa-request 171.69.1.1`	指定された MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定します。 *ip-address* | *name* を指定する場合は、グループの新しいメンバがアクティブになるときにローカル スイッチの SA メッセージの要求元になる MSDP ピアの IP アドレス、または名前を入力します。 SA メッセージを送信する必要がある MSDP ピアごとに、このコマンドを繰り返します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

スイッチから発信される送信元情報の制御

スイッチから発信されるマルチキャスト送信元情報を制御できます。

- アドバタイズ対象の送信元（送信元ベース）
- 送信元情報のレシーバー（要求元認識ベース）

詳細については、送信元の再配信，（1298 ページ）およびSA 要求メッセージのフィルタリング，（1301 ページ）を参照してください。

送信元の再配信

SA メッセージは、送信元が登録されている RP で発信されます。 デフォルトでは、RP に登録されているすべての送信元がアドバタイズされます。 送信元が登録されている場合は、RP に *A* フ

ラグが設定されています。このフラグは、フィルタリングされる場合を除き、送信元が SA に格納されてアドバタイズされることを意味します。

アドバタイズされる登録済みの送信元をさらに制限するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp redistribute** [**list***access-list-name*] [**asn***aspath-access-list-number*] [**route-map***map*] 例： `Switch(config)# ip msdp redistribute list 21`	SA メッセージに格納されてアドバタイズされる、マルチキャスト ルーティング テーブル内の（S, G）エントリを設定します。 デフォルトでは、ローカル ドメイン内の送信元だけがアドバタイズされます。 • （任意）**list***access-list-name*：IP 標準または IP 拡張アクセス リストの名前または番号を入力します。 標準アクセス リストの範囲は 1 ～ 99、拡張アクセス リストの範囲は 100 ～ 199 です。 アクセス リストによって、アドバタイズされるローカルな送信元、および送信されるグループが制御されます。 • （任意）**asn***aspath-access-list-number*：1 ～ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。 このアクセス リスト番号は、**ip as-path access-list** コマンドでも設定する必要があります。 • （任意）**route-map***map*：1 ～ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。 このアクセス リスト番号は、**ip as-path access-list** コマンドでも設定する必要があります。 アクセス リストまたは自律システム パス アクセス リストに従って、スイッチが（S, G）ペアをアドバタイズします。
ステップ 4	次のいずれかを使用します。 • **access-list***access-list-number* {**deny**| **permit**} *source*	IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 または

	コマンドまたはアクション	目的

	[*source-wildcard*]
	
	• **access-list***access-list-number* {**deny**| **permit**} *protocol source source-wildcard destination destination-wildcard*
	
	例：
	`Switch(config)# access list 21 permit 194.1.22.0`
	
	または
	
	`Switch(config)# access list 21 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1`
		IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。
		
		• *access-list-number*：ステップ 2 で作成した同じ番号を入力します。 標準アクセス リストの範囲は 1 ～ 99、拡張アクセス リストの範囲は 100 ～ 199 です。
		
		• **deny**：条件に合致した場合にアクセスを拒否します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。
		
		• *protocol*：プロトコル名として **ip** を入力します。
		
		• *source*：パケットの送信元であるネットワークまたはホストの番号を入力します。
		
		• *source-wildcard*：送信元に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。
		
		• *destination*：パケットの宛先であるネットワークまたはホストの番号を入力します。
		
		• *destination-wildcard*：宛先に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。
		
		アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SA 要求メッセージのフィルタリング

デフォルトでは、SA 情報をキャッシングしているスイッチだけが、SA 要求に応答できます。 このようなスイッチでは、デフォルトでMSDPピアからのすべてのSA要求メッセージが採用され、アクティブな送信元の IP アドレスが取得されます。

ただし、MSDP ピアからの SA 要求をすべて無視するように、スイッチを設定できます。 標準アクセス リストに記述されたグループのピアからの SA 要求メッセージだけを採用することもできます。 アクセス リスト内のグループが指定された場合は、そのグループのピアからの SA 要求メッセージが受信されます。 他のグループのピアからの他のメッセージは、すべて無視されます。

デフォルト設定に戻すには、**no ip msdp filter-sa-request** {*ip-address*| *name*} グローバル コンフィギュレーション コマンドを使用します。

これらのオプションのいずれかを設定するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **ip msdp filter-sa-request** {*ip-address*| *name*} • **ip msdp filter-sa-request** {*ip-address*| *name*} **list***access-list-number* 例： `Switch(config)# ip msdp filter sa-request 171.69.2.2`	指定されたMSDPピアからのSA要求メッセージをすべてフィルタリングします。 または 標準アクセス リストを通過したグループに対して、指定された MSDP ピアからの SA 要求メッセージをフィルタリングします。 アクセスリストには、複数のグループアドレスが記述されています。 access-list-number の範囲は 1 ～ 99 です。

	コマンドまたはアクション	目的
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 1 permit 192.4.22.0 0.0.0.255`	IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチで転送される送信元情報の制御

デフォルトでは、スイッチで受信されたすべての SA メッセージが、すべての MSDP ピアに転送されます。 ただし、フィルタリングするか、または存続可能時間（TTL）値を設定し、発信メッセージがピアに転送されないようにできます。

フィルタの使用法

フィルタを作成すると、次のいずれかの処理を実行できます。

- すべての送信元とグループのペアのフィルタリング
- 特定の送信元とグループのペアだけが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **ip msdp sa-filter out** {*ip-address*| *name*} • **ip msdp sa-filter out** {*ip-address*| *name*} **list***access-list-number* • **ip msdp sa-filter out** {*ip-address*| *name*} **route-map***map-tag* 例： `Switch(config)# ip msdp sa-filter out switch.cisco.com`	• 指定された MSDP ピアへの SA メッセージをフィルタリングします。 • 指定したピアに対する IP 拡張アクセス リストを通過した SA メッセージのみを渡します。 拡張アクセスリスト番号の範囲は 100 ～ 199 です。 **list** と **route-map** の両方のキーワードを使用すると、すべての条件に一致しなければ、発信 SA メッセージ内のいずれの（S,G）ペアも通過できません。 • 指定された MSDP ピアへのルート マップ *map-tag* で一致基準を満たす SA メッセージのみを渡します。 すべての一致条件を満たす場合、ルート マップに **permit** が指定されていれば、ルートはフィルタを通過します。 **deny** が指定されていれば、ルートはフィルタリングされます。

	コマンドまたはアクション	目的

	または
	`Switch(config)# ip msdp sa-filter out list 100`
	または
	`Switch(config)# ip msdp sa-filter out switch.cisco.com route-map 22`	

ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *protocolsourcesource-wildcarddestination destination-wildcard* 例： `Switch(config)# access list 100 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1`	（任意）IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限

TTL 値を使用して、各送信元の最初の SA メッセージにカプセル化されるデータを制御できます。 IP ヘッダー TTL 値が *ttl* 引数以上であるマルチキャスト パケットだけが、指定された MSDP ピアに送信されます。 たとえば、内部トラフィックの TTL 値を 8 に制限できます。 他のグループを外部に送信する場合は、これらのパケットの TTL を 8 より大きく設定して送信する必要があります。

TTL しきい値を確立するには、次の手順に従います。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp ttl-threshold** {*ip-address* | *name*} *ttl* 例： `Switch(config)# ip msdp ttl-threshold switch.cisco.com 0`	指定された MSDP ピア宛ての最初の SA メッセージにカプセル化されるマルチキャスト データを制限します。 • *ip-address* | *name* には、TTL の制限が適用される MSDP ピアの IP アドレスまたは名前を入力します。 • *ttl* には、TTL 値を入力します。 デフォルトは 0 です。 この場合、すべてのマルチキャスト データ パケットは、TTL がなくなるまでピアに転送されます。 指定できる範囲は 0 ～ 255 です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

スイッチで受信される送信元情報の制御

デフォルトでは、スイッチは、MSDP の RPF ピアによって送信されたすべての SA メッセージを受信します。 ただし、着信 SA メッセージをフィルタリングし、MSDP ピアから受信する送信元情報を制御できます。 つまり、特定の着信 SA メッセージを受信しないようにスイッチを設定できます。

次のいずれかの処理を実行できます。

- MSDP ピアからのすべての着信 SA メッセージのフィルタリング
- 特定の送信元とグループのペアが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、次の手順を実行します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかを使用します。
	• **ip msdp sa-filter in** {*ip-address*| *name*}
	• **ip msdp sa-filter in** {*ip-address*| *name*} **list***access-list-number*
	• **ip msdp sa-filter in** {*ip-address*| *name*} **route-map***map-tag*
	
	例：
	`Switch(config)# ip msdp sa-filter in switch.cisco.com`
	または
	`Switch(config)# ip msdp sa-filter in list 100`
	または
	`Switch(config)# ip msdp sa-filter in switch.cisco.com route-map 22`
		• 指定された MSDP ピアへの SA メッセージをフィルタリングします。
		• IP 拡張アクセス リストを通過する、指定されたピアからの SA メッセージのみを通過させます。 拡張アクセス リスト *access-list-number* の範囲は 100 ～ 199 です。
		list と **route-map** の両方のキーワードを使用すると、すべての条件に一致しなければ、発信 SA メッセージ内のいずれの（S,G）ペアも通過できません。
		• ルート マップ *map-tag* 内の一致条件を満たす、指定された MSDP ピアからの SA メッセージのみを通過させます。
		すべての一致条件を満たす場合、ルート マップに **permit** が指定されていれば、ルートはフィルタを通過します。 **deny** が指定されていれば、ルートはフィルタリングされます。

ステップ 4	**access-list***access-list-number* {**deny** | **permit**} *protocolsourcesource-wildcarddestination destination-wildcard* 例： `Switch(config)# access list 100 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1`	（任意）IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 • *access-list-number*, enter the number specified in Step 2. • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *protocol* には、プロトコル名として **ip** を入力します。 • *source*には、パケットの送信元であるネットワークまたはホストの番号を入力します。

	コマンドまたはアクション	目的
		• *source-wildcard* には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 • *destination* には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • *destination-wildcard* には、宛先に適用するワイルドカードビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MSDP メッシュ グループの設定

MSDP メッシュ グループを設定するには、次の任意の作業を実行します。

（注） デバイスごとに複数のメッシュ グループを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*}
4. MSDP ピアをメッシュ グループのメンバとして追加するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*} 例： `Switch(config)# ip msdp mesh-group peermesh`	MSDP メッシュ グループを設定し、MSDP ピアがそのメッシュ グループに属することを指定します。 （注） メッシュ グループに参加しているデバイス上のすべての MSDP ピアは、そのグループ内の他のすべての MSDP ピアと完全にメッシュ構造になっている必要があります。 各デバイスの各 MSDP ピアは、**ip msdp peer** コマンドを使用してピアとして、また、 **ip msdp mesh-group** コマンドを使用してそのメッシュ グループのメンバとしても設定されている必要があります。
ステップ 4	MSDP ピアをメッシュ グループのメンバとして追加するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Switch(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP ピアのシャットダウン

MSDP ピアをシャットダウンするには、次の任意の作業を実行します。

複数の MSDP ピアを設定し、そのすべての設定が終了するまではどのピアもアクティブにしない場合は、それぞれのピアをシャットダウンし、ピアごとに設定して、後からそれぞれのピアを起動することができます。 その MSDP ピアの設定を失うことなく、MSDP セッションをシャットダウンすることもできます。

（注） MSDP ピアをシャットダウンすると、TCP 接続が終了します。**no ip msdp shutdown** コマンドを（指定したピアに対して）使用し、ピアを起動するまではこの接続は再開されません。

はじめる前に

MSDP が動作していて、MSDP ピアを設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipmsdpshutdown** {*peer-name* | *peer-address*}
4. 別の MSDP ピアをシャットダウンするには、ステップ 3 を繰り返します。
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ipmsdpshutdown** {*peer-name* | *peer-address*} 例： `Switch(config)# ip msdp shutdown 192.168.1.3`	指定された MSDP ピアを管理シャットダウンします。

	コマンドまたはアクション	目的
ステップ 4	別の MSDP ピアをシャットダウンするには、ステップ 3 を繰り返します。	--
ステップ 5	**end** 例： `Switch(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

境界 PIM デンス モード領域の MSDP への包含

デンス モード（DM）領域と PIM スパース モード（SM）領域の境界となるスイッチに MSDP を設定します。 デフォルトでは、DM 領域のアクティブな送信元は MSDP に加入しません。

（注） **ip msdp border sa-address** グローバル コンフィギュレーション コマンドの使用は推奨できません。 DM ドメイン内の送信元が SM ドメイン内の RP にプロキシ登録されるように SM ドメイン内の境界ルータを設定し、標準 MSDP 手順でこれらの送信元をアドバタイズするように SM ドメインを設定してください。

ip msdp originator-id グローバル コンフィギュレーション コマンドを実行すると、RP アドレスとして使用されるインターフェイスも識別されます。 **ip msdp border sa-address** と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスが RP アドレスを指定します。

DM 領域でアクティブな送信元の SA メッセージを MSDP ピアに送信するように境界ルータを設定するには、次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ip msdp border sa-address***interface-id* 例： `Switch(config)# ip msdp border sa-address 0/1`	DM 領域内のアクティブな送信元に関する SA メッセージを送信するように、DM 領域と SM 領域の境界スイッチを設定します。 *interface-id* には、SA メッセージ内の RP アドレスとして使用される、IP アドレスの配信元となるインターフェイスを指定します。 インターフェイスの IP アドレスは、SA メッセージ内の RP フィールド [Originator-ID] の値として使用されます。
ステップ 4	**ip msdp redistribute** [**list***access-list-name*] [**asn***aspath-access-list-number*] [**route-map***map*] 例： `Switch(config)# ip msdp redistribute list 100`	SA メッセージに格納されてアドバタイズされる、マルチキャストルーティングテーブル内の（S,G）エントリを設定します。 詳細については、送信元の再配信,（1298 ページ）を参照してください。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

RP アドレス以外の発信元アドレスの設定

SA メッセージを発信する MSDP スピーカーがそのインターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用できるようにするには、次の任意の作業を実行します。

また、次のいずれかの理由により、発信元 ID を変更できます。

- Anycast RP の MSDP メッシュ グループに複数のデバイスを設定する場合。
- デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にある場合。 デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にあり、PIM-DM ドメイン内のアクティブなソースをアドバタイズする場合は、SA メッセージ内の RP アドレスが発信元デバイスのインターフェイスのアドレスになるように設定します。

はじめる前に

MSDP がイネーブルになり、MSDP ピアが設定されます。 MSDP ピアの設定の詳細については、MSDP ピアの設定を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipmsdporiginator-id**
4. **exit**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdporiginator-id** 例： `Switch(config)# ip msdp originator-id ethernet 1`	発信元デバイスのインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。
ステップ 4	**exit** 例： `Switch(config)# exit`	グローバルコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MSDP のモニタリングおよびメンテナンス

MSDP のモニタリング

MSDP の SA メッセージ、ピア、ステート、およびピアのステータスをモニタリングするには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **debugipmsdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]
3. **debugipmsdpresets**
4. **showipmsdpcount** [*as-number*]
5. **showipmsdppeer** [*peer-address* | *peer-name*]
6. **showipmsdpsa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]
7. **showipmsdpsummary**

手順の詳細

ステップ 1 **enable**

例：

```
Device# enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **debugipmsdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]

このコマンドを使用して、MSDP アクティビティをデバッグします。

オプションの *peer-address* または *peer-name* 引数を使用して、デバッグ イベントをログに記録するピアを指定します。

次に、**debugipmsdp** コマンドの出力例を示します。

例：

```
Device# debug ip msdp
MSDP debugging is on
Device#
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.254: Received 1028-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1028, ec: 85, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1028-byte SA to peer
```

```
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.250: Received 56-byte message from peer
MSDP: 224.150.44.250: SA TLV, len: 56, ec: 4, RP: 192.168.76.241
MSDP: 224.150.44.250: Peer RPF check passed for 192.168.76.241, used EMBGP peer
MSDP: 224.150.44.254: Forward 56-byte SA to peer
MSDP: 224.150.44.254: Received 116-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 116, ec: 9, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 116-byte SA to peer
MSDP: 224.150.44.254: Received 32-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 32, ec: 2, RP: 172.31.3.78
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.78, used EMBGP peer
MSDP: 224.150.44.250: Forward 32-byte SA to peer
```

ステップ 3 **debugipmsdpresets**

このコマンドを使用して、MSDP ピアのリセット理由をデバッグします。

例：

```
Device# debug ip msdp resets
```

ステップ 4 **showipmsdpcount** [*as-number*]

このコマンドを使用して、MSDP SA メッセージ内で発信したソースおよびグループの数、および SA キャッシュ内の MSDP ピアからの SA メッセージの数を表示します。 **ipmsdpcache-sa-state** コマンドは、このコマンドによって出力が生成されるように設定する必要があります。

次に、**showipmsdpcount** コマンドの出力例を示します。

例：

```
Device# show ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
    192.168.4.4: 8
SA State per ASN Counters, <asn>: <# sources>/<# groups>
    Total entries: 8
    ?: 8/8
```

ステップ 5 **showipmsdppeer** [*peer-address* | *peer-name*]

このコマンドを使用して、MSDP ピアに関する詳細情報を表示します。

オプションの *peer-address* 引数または *peer-name* 引数を使用して、特定のピアに関する情報を表示します。

次に、**showipmsdppeer** コマンドの出力例を示します。

例：

```
Device# show ip msdp peer 192.168.4.4
MSDP Peer 192.168.4.4 (?), AS 64512 (configured AS)
  Connection status:
    State: Up, Resets: 0, Connection source: Loopback0 (2.2.2.2)
    Uptime(Downtime): 00:07:55, Messages sent/received: 8/18
    Output messages discarded: 0
    Connection and counters cleared 00:08:55 ago
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
```

```
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 8
  Input queue size: 0, Output queue size: 0
  MD5 signature protection on MSDP TCP connection: not enabled
```

ステップ 6 **showipmsdpsa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]

このコマンドを使用して、MSDP ピアから学習した (S, G) ステートを表示します。

次に、**showipmsdpsa-cache** コマンドの出力例を示します。

例：

```
Device# show ip msdp sa-cache
MSDP Source-Active Cache - 8 entries
(10.44.44.5, 239.232.1.0), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.1), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.2), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.3), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.4), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.5), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.6), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.7), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
```

ステップ 7 **showipmsdpsummary**

このコマンドを使用して、MSDP ピアのステータスを表示します。

次に、**showipmsdpsummary** コマンドの出力例を示します。

例：

```
Device# show ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
192.168.4.4      4     Up       00:08:05 0     8     ?
```

MSDP 接続統計情報および SA キャッシュ エントリの消去

MSDP 接続、統計情報または SA キャッシュ エントリを消去するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **clearipmsdppeer** [*peer-address* | *peer-name*]
3. **clearipmsdpstatistics** [*peer-address* | peer-name]
4. **clearipmsdpsa-cache** [*group-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clearipmsdppeer** [*peer-address* | *peer-name*] 例： `Device#` **clear ip msdp peer**	指定された MSDP ピアへの TCP 接続をクリアし、すべての MSDP メッセージ カウンタをリセットします。
ステップ 3	**clearipmsdpstatistics** [*peer-address* | peer-name] 例： `Device# clear ip msdp statistics`	指定された MSDP ピアの統計カウンタをクリアし、すべての MSDP メッセージ カウンタをリセットします。
ステップ 4	**clearipmsdpsa-cache** [*group-address*] 例： `Device# clear ip msdp sa-cache`	SA キャッシュ エントリを消去します。 • **clearipmsdpsa-cache** コマンドにオプションの *group-address* 引数または *source-address* 引数を指定した場合、すべての SA キャッシュ エントリが消去されます。 • 特定のグループに関連付けられたすべての SA キャッシュ エントリを消去するには、オプションの *group-address* 引数を使用します。

MSDP の設定例

デフォルト MSDP ピアの設定：例

次に、ルータ A およびルータ C の部分的な設定の例を示します。 これらの ISP にはそれぞれに複数のカスタマー（カスタマーと同様）がおり、 デフォルトのピアリング（BGP または MBGP なし）を使用しています。 この場合、両方の ISP で類似した設定となります。 つまり、両方の ISP では、対応するプレフィックス リストで SA が許可されている場合、デフォルト ピアからの SA だけが受信されます。

ルータ A

```
Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

ルータ C

```
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

SA ステートのキャッシング：例

次に、グループ 224.2.0.0/16 への送信元である 171.69.0.0/16 のすべての送信元のキャッシュ ステートをイネーブルにする例を示します。

```
Switch(config)# ip msdp cache-sa-state 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

MSDP ピアからの送信元情報の要求：例

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定する例を示します。

```
Switch(config)# ip msdp sa-request 171.69.1.1
```

スイッチから発信される送信元情報の制御：例

次に、171.69.2.2 の MSDP ピアからの SA 要求メッセージをフィルタリングするように、スイッチを設定する例を示します。 ネットワーク 192.4.22.0 の送信元からの SA 要求メッセージはアクセス リスト 1 に合格して、受信されます。その他のすべてのメッセージは無視されます。

```
Switch(config)# ip msdp filter sa-request 171.69.2.2 list 1
Switch(config)# access-list 1 permit 192.4.22.0 0.0.0.255
```

スイッチから転送される送信元情報の制御：例

次に、アクセス リスト 100 を通過する（S,G）ペアだけが SA メッセージに格納され、*switch.cisco.com* という名前のピアに転送されるように設定する例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
Switch(config)# ip msdp sa-filter out switch.cisco.com list 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

スイッチで受信される送信元情報の制御：例

次に、*switch.cisco.com* という名前のピアからのすべての SA メッセージをフィルタリングする例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
Switch(config)# ip msdp sa-filter in switch.cisco.com
```

例：MSDP メッシュ グループの設定

次に、3 台のデバイスを MSDP メッシュ グループのフル メッシュ メンバになるように設定する例を示します。

デバイス A の設定

```
ip msdp peer 10.2.2.2
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.2.2.2
ip msdp mesh-group test-mesh-group 10.3.3.3
```

デバイス B の設定

```
ip msdp peer 10.1.1.1
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.3.3.3
```

デバイス C の設定

```
ip msdp peer 10.1.1.1
ip msdp peer 10.2.2.2
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.2.2.2
```

MSDP ピアからの送信元情報の要求：例

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定する例を示します。

```
Switch(config)# ip msdp sa-request 171.69.1.1
```

第 IX 部

セキュリティ

- セキュリティ機能の概要，1323 ページ
- 不正アクセスの防止，1327 ページ
- パスワードおよび権限レベルによるスイッチ アクセスの制御，1329 ページ
- TACACS+ の設定，1349 ページ
- RADIUS の設定，1367 ページ
- Kerberos の設定，1405 ページ
- ローカル認証および許可の設定，1413 ページ
- セキュア シェル（SSH）の設定，1417 ページ
- Secure Socket Layer HTTP の設定，1427 ページ
- IPv4 ACL の設定，1439 ページ
- IPv6 ACL の設定，1497 ページ
- DHCP の設定，1507 ページ
- IP ソース ガードの設定，1533 ページ
- ダイナミック ARP インスペクションの設定，1543 ページ
- IEEE 802.1x ポートベースの認証の設定，1563 ページ
- Web ベース認証の設定，1665 ページ

- ポート単位のトラフィック制御の設定，1693 ページ
- IPv6 ファースト ホップ セキュリティの設定，1739 ページ
- FIPS の設定，1775 ページ

第 46 章

セキュリティ機能の概要

- セキュリティ機能の概要，1323 ページ

セキュリティ機能の概要

セキュリティ機能は次のとおりです。

- IPv6 ファースト ホップ セキュリティ：IPv6 ネットワークの持つ脆弱性から保護するためにファースト ホップ スイッチに適用されるセキュリティ機能のセット。 これらには、バインディング統合ガード（バインディング テーブル）、ルータ アドバタイズメント ガード（RA ガード）、DHCP ガード、IPv6 ネイバー探索検査（ND ガード）、および IPv6 ソース ガードなどがあります。
- Web 認証：Web ブラウザを使用して認証する IEEE 802.1x 機能をサポートしないサプリカント（クライアント）を許可します。
- ローカル Web 認証バナー：Web 認証ログイン画面に表示されるカスタム バナーまたはイメージ ファイル。
- ACL および RADIUS Filter-Id 属性を使った IEEE 802.1x 認証。
- 管理インターフェイス（デバイス マネージャ、Network Assistant、CLI）へのパスワード保護付きアクセス（読み取り専用および読み書きアクセス）。不正な設定変更を防止します。
- セキュリティ レベル、通知、および対応するアクションを選択できる、マルチレベル セキュリティ。
- セキュリティを確保できるスタティック MAC アドレッシング。
- 保護ポート オプション。同一スイッチ上の指定ポートへのトラフィック転送を制限します。
- ポートにアクセスできるステーションの MAC アドレスを制限または特定するポート セキュリティ オプション。
- 違反発生時に、ポート全体をシャットダウンするのではなく、そのポートの VLAN をシャットダウンする VLAN 対応ポート セキュリティ オプション。

- ポート セキュリティ エージング。ポートのセキュア アドレスにエージング タイムを設定します。
- 指定した入力割合を超えたパケットをドロップして、スイッチへの着信プロトコル トラフィックの割合を制御する、プロトコル ストーム プロテクション。
- BPDU ガード。無効なコンフィギュレーションが発生した場合に、PortFast が設定されているポートをシャットダウンします。
- 標準および拡張 IP アクセス コントロール リスト（ACL）は、レイヤ 2 インターフェイス（ポート ACL）でのインバウンドなセキュリティ ポリシーを定義します。
- MAC 拡張アクセス コントロール リスト。レイヤ 2 インターフェイスの着信方向のセキュリティ ポリシーを定義します。
- 非 IP トラフィックをフィルタリングする、送信元および宛先 MAC ベースの ACL。
- 信頼できないホストと DHCP サーバの間の信頼できない DHCP メッセージをフィルタリングする DHCP スヌーピング。
- DHCP スヌーピング データベース、および IP ソース バインディングに基づいてトラフィックをフィルタリングすることにより、非ルーテッドインターフェイスでのトラフィックを制限する IP ソース ガード。
- 不正な ARP 要求や応答を同じ VLAN 上のその他のポートにリレーしないことにより、スイッチに対する悪意のある攻撃を回避するためのダイナミック ARP インスペクション。
- IEEE 802.1x ポートベース認証。不正なデバイス（クライアント）によるネットワーク アクセスを防止します。 次の 802.1x 機能がサポートされます。
  - データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が、同じ IEEE 802.1x 対応スイッチ ポートにおいて、単独で認証できるようにするマルチドメイン認証（MDA）。
  - MDA のダイナミック音声 VLAN（仮想 LAN）。ダイナミック音声 VLAN が MDA 対応ポートで可能になります。
  - VLAN 割り当て。802.1x 認証ユーザを特定の VLAN に制限します。
  - マルチ認証モードで設定されたポートでの VLAN 割り当てのサポート。 RADIUS サーバは、ポートで最初に認証されるホストに VLAN を割り当て、後続のホストは同じ VLAN を使用します。 音声 VLAN 割り当ては、1 つの IP フォンに対してサポートされます。
  - ポート セキュリティ。802.1x ポートへのアクセスを制御します。
  - 音声 VLAN。ポートが許可ステートか無許可ステートかにかかわらず、Cisco IP Phone の音声 VLAN へのアクセスを許可します。
  - IP Phone 検出機能拡張。Cisco IP Phone を検出し識別します。
  - ゲスト VLAN。802.1x に適合しないユーザに限定的なサービスを提供します。

- 制限付き VLAN。802.1x に準拠はしているが、標準の 802.1x で認証するためのクレデンシャルを持っていないユーザに制限付きのサービスを提供します。
- 802.1x アカウンティング。ネットワーク使用をトラッキングします。
- 802.1x と LAN の Wake-on-LAN（WoL）機能。休止状態の PC に、特定のイーサネットフレームを送信して起動させます。
- 802.1x 準備状態チェック。スイッチで IEEE 802.1x を設定する前に、接続されたエンドホストの準備状態を判断します。
- セキュリティ違反が発生した VLAN だけでトラフィック違反アクションを適用するための音声認識 802.1x セキュリティ。
- MAC 認証バイパス（MAB）。クライアント MAC アドレスに基づいてクライアントを許可します。
- デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライアントのウイルス対策の状態またはポスチャに関する Network Admission Control（NAC）レイヤ 2 802.1x 検証。
- 802.1X スイッチ サプリカントを持つ Network Edge Access Topology（NEAT）、CISP を使ったホスト認証、および自動イネーブル化。これらにより、別のスイッチへのサプリカントとして、配線クローゼットの外のスイッチが認証されます。
- 認証される前にネットワークへのアクセスをホストに許可するための、オープンアクセスを使用した IEEE 802.1x。
- ダウンロード可能な ACL とリダイレクト URL を使用した IEEE 802.1x 認証。Cisco Secure ACS サーバから認証されたスイッチへのユーザ単位の ACL ダウンロードを使用できるようになります。
- スタティック ACL が設定されていないポートでの認証デフォルト ACL のダイナミックな作成または接続のサポート。
- 新しいホストを認証するときに、ポートが思考する認証メソッドの順序を設定するための柔軟な認証シーケンス。
- マルチユーザ認証。複数のホストが、802.1x 対応ポートを認証できるようになります。

- TACACS+。IPv4 および IPv6 対応の TACACS サーバを介してネットワーク セキュリティを管理する独自の機能。
- IPv4 および IPv6 対応の認証、許可、アカウンティング（AAA）サービスを使用して、リモートユーザの ID の検証、アクセスの許可、アクションの追跡を実行するための RADIUS。
- IPv6 上での機能向けに、RADIUS、TACACS+、および SSH を拡張。
- HTTP 1.1 サーバ認証、暗号化、メッセージ整合性、HTTP クライアント認証用に Secure Socket Layer（SSL）バージョン 3.0 がサポートされ、安全な HTTP 通信が可能になります（ソフトウェアの暗号化バージョンが必要）。
- ACL および RADIUS Filter-Id 属性を使った IEEE 802.1x 認証。

- スタティック ホストでの IP ソース ガードのサポート。
- RADIUS 認証の変更（CoA）。特定のセッション認証された後で、その属性を変更します。AAA でユーザ、またはユーザ グループのポリシーに変更がある場合、管理者は Cisco Identity Services Engine または Cisco Secure ACS などの AAA サーバから、RADIUS CoA パケットを送信し、新しいポリシーに適用することができます。
- IEEE 802.1x User Distribution。さまざまな VLAN にわたってユーザをロード バランシングすることにより、（ユーザ グループに対して）複数の VLAN を使った配置で、ネットワークのスケーラビリティを向上させることができます。認証されたユーザは、RADIUS サーバにより割り当てられた、グループ内で最も空いている VLAN に割り当てられます。
- マルチ ホスト認証を使った、重要な VLAN のサポート。これにより、ポートがマルチ認証用に設定され、AAA サーバが到達不能になった場合でも、重要なリソースへのアクセスができるように、このポートが重要な VLAN に配置されます。
- ポート ホスト モードを変更し、オーセンティケータのスイッチ ポートに標準ポート設定を適用するために Network Edge Access Topology（NEAT）をサポート。
- VLAN-ID ベースの MAC 認証。ユーザ認証のために VLAN と MAC のアドレス情報を結合して、許可されていない VLAN からのネットワーク アクセスを阻止します。
- MAC 移動。モビリティのイネーブル化を制約することなく、ホスト（IP フォンの背後で接続されたホストを含む）が同じスイッチ内のポート間を移動できるようになります。 MAC 移動では、もう 1 つのポートに同じ MAC アドレスが再登場した場合、スイッチはこれをまったく新しい MAC アドレスと同様に扱います。
- 簡易ネットワーク管理プロトコル バージョン 3（SNMPv3）を使った 3DES および AES のサポート。 このリリースでは、168 ビット Triple Data Encryption Standard（3DES）と、SNMPv3 への 128 ビット、192 ビット、および 256 ビットの Advanced Encryption Standard（AES）暗号化アルゴリズムに対するサポートが追加されます。

第 47 章

不正アクセスの防止

- 機能情報の確認，1327 ページ
- 不正アクセスの防止，1327 ページ

機能情報の確認

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

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

不正アクセスの防止

不正ユーザによる、スイッチの再設定や設定情報の閲覧を防止できます。 一般的には、ネットワーク管理者からスイッチへのアクセスを許可する一方、非同期ポートを用いてネットワーク外からダイヤルアップ接続するユーザや、シリアル ポートを通じてネットワーク外から接続するユーザ、またはローカル ネットワーク内の端末またはワークステーションから接続するユーザによるアクセスを制限します。

スイッチへの不正アクセスを防止するには、次のセキュリティ機能を 1 つまたは複数設定します。

- 最低限のセキュリティとして、各スイッチ ポートでパスワードおよび権限を設定します。 このパスワードは、スイッチにローカルに保存されます。 ユーザがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。

- 追加のセキュリティ レイヤとして、ユーザ名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。 このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。 権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。
- ユーザ名とパスワードのペアを使用したいが、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティ サーバ上のデータベースに保存できます。 これにより、複数のネットワーキングデバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。
- また、失敗したログイン試行をログに記録するログイン拡張機能もイネーブルにすることもできます。 ログイン拡張は、設定した回数のログインが失敗したあとに、それ以降のログイン試行をブロックするために設定することもできます。 詳細については、『Cisco IOS Login Enhancements』マニュアルを参照してください。

関連トピック

ユーザ名とパスワードのペアの設定, （1340 ページ）
TACACS+ およびスイッチ アクセス, （1351 ページ）
端末回線に対する Telnet パスワードの設定, （1338 ページ）

第 48 章

パスワードおよび権限レベルによるスイッチ アクセスの制御

- 機能情報の確認，1329 ページ
- パスワードおよび権限によるスイッチ アクセスの制御の制約事項，1329 ページ
- パスワードおよび権限レベルに関する情報，1330 ページ
- パスワードおよび権限レベルでスイッチ アクセスを制御する方法，1333 ページ
- スイッチ アクセスのモニタリング，1346 ページ
- パスワードおよび権限レベルの設定例，1347 ページ

機能情報の確認

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

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

パスワードおよび権限によるスイッチ アクセスの制御の制約事項

パスワードおよび権限によるスイッチ アクセスの制御の制約事項は、次のとおりです。

- パスワード回復のディセーブル化は、**boot manual** グローバル コンフィギュレーション コマンドを使用して手動でブートするようにスイッチを設定している場合は無効です。 このコマンドは、スイッチの電源の再投入後、ブートローダ プロンプト（*switch:*）を表示させます。

関連トピック

パスワード回復のディセーブル化, （1337 ページ）
パスワードの回復, （1331 ページ）

パスワードおよび権限レベルに関する情報

デフォルトのパスワードおよび権限レベル設定

ネットワークで端末のアクセス コントロールを行う簡単な方法は、パスワードを使用して権限レベルを割り当てることです。パスワード保護によって、ネットワークまたはネットワークデバイスへのアクセスが制限されます。 権限レベルによって、ネットワーク デバイスにログイン後、ユーザがどのようなコマンドを使用できるかが定義されます。

次の表に、デフォルトのパスワードおよび権限レベル設定を示します。

表 *123* : デフォルトのパスワードおよび権限レベル設定

機能	デフォルト設定
イネーブル パスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です（特権 EXEC レベル）。 パスワードは、コンフィギュレーション ファイル内では暗号化されていない状態です。
イネーブル シークレット パスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です（特権 EXEC レベル）。 パスワードは、暗号化されてからコンフィギュレーション ファイルに書き込まれます。
回線パスワード	パスワードは定義されていません。

追加のパスワード セキュリティ

追加のセキュリティ レイヤを、特にネットワークを越えるパスワードやTrivial File Transfer Protocol（TFTP）サーバに保存されているパスワードに対して設定する場合には、**enable password** または **enable secret** グローバル コンフィギュレーション コマンドを使用できます。 コマンドの作用はどちらも同じです。このコマンドにより、暗号化されたパスワードを設定できます。特権EXECモード（デフォルト設定）または特定の権限レベルにアクセスするユーザは、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムが使用されるので、**enable secret** コマンドを使用することを推奨します。

enable secret コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

パスワードの暗号化をイネーブルにすると、ユーザ名パスワード、認証キー パスワード、イネーブルコマンドパスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

関連トピック

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護, （1334 ページ）
例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護, （1347 ページ）

パスワードの回復

スイッチに物理的にアクセスできるエンド ユーザは、デフォルトで、スイッチの電源投入時にブート プロセスに割り込み、新しいパスワードを入力することによって、失われたパスワードを回復できます。

パスワード回復ディセーブル化機能では、この機能の一部をディセーブルにすることによりスイッチのパスワードへのアクセスを保護できます。 この機能がイネーブルの場合、エンドユーザは、システムをデフォルト設定に戻すことに同意した場合に限り、ブート プロセスに割り込むことができます。 パスワード回復をディセーブルにしても、ブートプロセスに割り込んでパスワードを変更できますが、コンフィギュレーション ファイル（config.text）およびVLANデータベース ファイル（vlan.dat）は削除されます。

パスワード回復をディセーブルにする場合は、エンドユーザがブートプロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。 スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。 VTP（VLAN トランキング プロトコル）トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。 スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

パスワードの回復を再びイネーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

パスワード回復のディセーブル化, （1337 ページ）
パスワードおよび権限によるスイッチ アクセスの制御の制約事項, （1329 ページ）

端末回線の Telnet 設定

初めてスイッチに電源を投入すると、自動セットアップ プログラムが起動して IP 情報を割り当て、この後続けて使用できるようにデフォルト設定を作成します。 さらに、セットアッププログラムは、パスワードによる Telnet アクセス用にスイッチを設定することを要求します。 セット

アップ プログラムの実行中にこのパスワードを設定しなかった場合は、端末回線に対する Telnet パスワードを設定するときに設定できます。

関連トピック

端末回線に対する Telnet パスワードの設定, （1338 ページ）
例：端末回線に対する Telnet パスワードの設定, （1347 ページ）

ユーザ名とパスワードのペア

ユーザ名とパスワードのペアを設定できます。このペアはスイッチ上でローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。 権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

関連トピック

ユーザ名とパスワードのペアの設定, （1340 ページ）

権限レベル

Cisco スイッチ（および他のデバイス）では、権限レベルを使用して、スイッチ動作の異なるレベルに対してパスワードセキュリティを提供します。 デフォルトでは、Cisco IOS ソフトウェアは、パスワードセキュリティの 2 つのモード（権限レベル）で動作します。ユーザ EXEC（レベル 1）および特権 EXEC（レベル 15）です。 各モードに、最大 16 個の階層レベルからなるコマンドを設定できます。 複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

回線の権限レベル

ユーザは、回線にログインし、別の権限レベルをイネーブルに設定することにより、**privilege level** ライン コンフィギュレーション コマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。 上位の権限レベルのパスワードがわかっていれば、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。 回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

たとえば、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 のセキュリティを割り当て、レベル 2 のパスワードを広範囲のユーザに配布できます。 また、**configure** コマンドへのアクセス制限を強化する場合は、レベル 3 のセキュリティを割り当て、そのパスワードを限られたユーザ グループに配布することもできます。

コマンド権限レベル

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。 たとえば、**show ip traffic** コマンドをレベル 15 に設定すると、**show** コマンドおよび **show ip** コマンドは、それぞれ別のレベルに設定しない限り、自動的にレベル 15 に設定されます。

関連トピック

コマンドの特権レベルの設定，（1342 ページ）
例：コマンドの権限レベルの設定，（1347 ページ）
回線のデフォルト特権レベルの変更，（1344 ページ）
権限レベルへのログインおよび終了，（1346 ページ）

パスワードおよび権限レベルでスイッチ アクセスを制御する方法

スタティック イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。 スタティック イネーブル パスワードを設定または変更するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **enable password***password*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**enable password***password* 例： `Switch(config)# enable password secret321`	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 デフォルトでは、パスワードは定義されません。 *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を

	コマンドまたはアクション	目的
		区別し、スペースを使用できますが、先行スペースは無視されます。 疑問符（?）は、パスワードを作成する場合に、疑問符の前にCtrl+v を入力すれば使用できます。たとえば、パスワード abc?123 を作成するときは、次のようにします。 **1** **abc** を入力します。 **2** Ctrl+v を入力します。 **3** **?123** を入力します。 システムからイネーブル パスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：スタティック イネーブル パスワードの設定または変更, （1347 ページ）

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

特権 EXEC モード（デフォルト）または指定された特権レベルにアクセスするためにユーザが入力する必要がある暗号化パスワードを確立するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. 次のいずれかを使用します。
   - **enable password**[**level***level*] {*password*| *encryption-type encrypted-password*}
   - **enable secret**[**level***level*] {*password*| *encryption-type encrypted-password*}
4. **service password-encryption**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **enable password**[**level***level*] {*password*| *encryption-type encrypted-password*} • **enable secret**[**level***level*] {*password*| *encryption-type encrypted-password*} 例： `Switch(config)# enable password example102`	• 特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 • シークレット パスワードを定義します。これは非可逆的な暗号化方式を使用して保存されます。 ◦（任意）*level* に指定できる範囲は 0 ～ 15 です。 レベル 1 が通常のユーザ EXEC モード権限です。 デフォルト レベルは 15 です（特権 EXEC モード権限）。 ◦ *password* には、1 ～ 25 文字の英数字のストリングを指定します。 ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。

	コマンドまたはアクション	目的
	または `Switch(config)# enable secret level 1 password secret123sample`	◦（任意）*encryption-type* には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか使用できません。 暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、別のスイッチの設定からコピーします。 （注） 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。
ステップ 4	**service password-encryption** 例： `Switch(config)# service password-encryption`	（任意）パスワードの定義時または設定の書き込み時に、パスワードを暗号化します。 暗号化を行うと、コンフィギュレーションファイル内でパスワードが読み取り可能な形式になるのを防止できます。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

追加のパスワード セキュリティ，（1330 ページ）

例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護，（1347 ページ）

パスワード回復のディセーブル化

パスワードの回復をディセーブルにしてスイッチのセキュリティを保護するには、次の手順を実行します。

はじめる前に

パスワード回復をディセーブルにする場合は、エンドユーザがブートプロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。 スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。 VTP（VLAN トランキング プロトコル）トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。 スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

手順の概要

1. **enable**
2. **configureterminal**
3. **no service password-recovery**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no service password-recovery** 例： `Switch(config)# no service`	パスワード回復をディセーブルにします。 この設定は、フラッシュ メモリの中で、ブートローダおよび Cisco IOS イメージがアクセスできる領域に保存されますが、ファイル システムには含まれません。また、ユーザがアクセスすることはできません。

	コマンドまたはアクション	目的
	password-recovery	
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

パスワードの回復を再びイネーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

パスワードの回復, （1331 ページ）

パスワードおよび権限によるスイッチ アクセスの制御の制約事項, （1329 ページ）

端末回線に対する Telnet パスワードの設定

接続された端末回線に対する Telnet パスワードを設定するには、ユーザ EXEC モードで次の手順を実行します。

はじめる前に

- エミュレーション ソフトウェアを備えた PC またはワークステーションをスイッチ コンソール ポートに接続するか、または PC をイーサネット管理ポートに接続します。
- コンソール ポートのデフォルトのデータ特性は、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなしです。 コマンドラインプロンプトが表示されるまで、Return キーを何回か押す必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **line vty 0 15**
4. **password***password*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	（注） パスワードが特権EXECモードへのアクセスに必要な場合は、その入力が求められます。 特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line vty 0 15** 例： `Switch(config)# line vty 0 15`	Telnetセッション（回線）の数を設定し、ライン コンフィギュレーション モードを開始します。 コマンド対応Switchでは、最大 16 のセッションが可能です。0 および 15 を指定すると、使用できる 16 の Telnet セッションすべてを設定することになります。
ステップ 4	**password***password* 例： `Switch(config-line)# password abcxyz543`	1 つまたは複数の回線に対応する Telnet パスワードを設定します。 *password* には、1 ～ 25 文字の英数字のストリングを指定します。 ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。 デフォルトでは、パスワードは定義されません。
ステップ 5	**end** 例： `Switch(config-line)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

不正アクセスの防止，（1327 ページ）
端末回線の Telnet 設定，（1331 ページ）
例：端末回線に対する Telnet パスワードの設定，（1347 ページ）

ユーザ名とパスワードのペアの設定

ユーザ名とパスワードのペアを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **username***name* [**privilege***level*] {**password***encryption-typepassword*}
4. 次のいずれかを使用します。
   - **line console 0**
   - **line vty 0 15**
5. **login local**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

ステップ 3	**username***name* [**privilege***level*] {**password***encryption-typepassword*}
	
	例：
	`Switch(config)# username adamsample privilege 1 password secret456`
	`Switch(config)# username 111111111111 mac attribute`
		各ユーザのユーザ名、権限レベル、パスワードを設定します。
		• *name* には、ユーザ ID を 1 ワードで指定するか、または MAC アドレスを指定します。 スペースと引用符は使用できません。
		• ユーザ名と MAC フィルタの両方に対し、最大 12000 のクライアントを個別に設定できます。
		• （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。 指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。
		• *encryption-type* には、暗号化されていないパスワードが後ろに続く場合は 0 を入力します。 暗号化されたパスワードが後ろに続く場合は 7 を指定します。
		• *password* には、ユーザがSwitchにアクセスする場合に入力する必要のあるパスワードを指定します。 パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。

ステップ 4	次のいずれかを使用します。 • **line console 0** • **line vty 0 15** 例： `Switch(config)# line console 0`	ライン コンフィギュレーション モードを開始し、コンソール ポート（回線 0）または VTY 回線（回線 0 ～ 15）を設定します。

	コマンドまたはアクション	目的
	または `Switch(config)# line vty 15`	
ステップ 5	**login local** 例： `Switch(config-line)# login local`	ログイン時のローカル パスワード チェックをイネーブルにします。 認証は、ステップ 3 で指定されたユーザ名に基づきます。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

不正アクセスの防止，（1327 ページ）
ユーザ名とパスワードのペア，（1332 ページ）

コマンドの特権レベルの設定

コマンドの権限レベルを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **privilege***mode***level***levelcommand*
4. **enable password level***levelpassword*
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**privilege***mode***level***levelcommand* 例： `Switch(config)# privilege exec level 14 configure`	コマンドの特権レベルを設定します。 • *mode* には、グローバル コンフィギュレーション モードの場合は **configure** を、EXEC モードの場合は **exec** を、インターフェイス コンフィギュレーション モードの場合は **interface** を、ライン コンフィギュレーション モードの場合は **line** をそれぞれ入力します。 • *level* の範囲は 0 ～ 15 です。 レベル 1 が通常のユーザ EXEC モード権限です。 レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。 • *command* には、アクセスを制限したいコマンドを指定します。
ステップ 4	**enable password level***levelpassword* 例： `Switch(config)# enable password level 14 SecretPswd14`	権限レベルをイネーブルにするためのパスワードを指定します。 • *level* の範囲は 0 ～ 15 です。 レベル 1 が通常のユーザ EXEC モード権限です。 • *password* には、1 ～ 25 文字の英数字のストリングを指定します。 ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペース

	コマンドまたはアクション	目的
		は無視されます。デフォルトでは、パスワードは定義されません。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

権限レベル，（1332 ページ）

例：コマンドの権限レベルの設定，（1347 ページ）

回線のデフォルト特権レベルの変更

指定した回線のデフォルトの権限レベルを変更するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **line vty***line*
4. **privilege level***level*
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line vty***line* 例： `Switch(config)# line vty 10`	アクセスを制限する仮想端末回線を選択します。
ステップ 4	**privilege level***level* 例： `Switch(config)# privilege level 15`	回線のデフォルト特権レベルを変更します。 *level* の範囲は 0 ～ 15 です。 レベル 1 が通常のユーザ EXEC モード権限です。 レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

ユーザは、回線にログインし、別の権限レベルをイネーブルに設定することにより、**privilege level** ライン コンフィギュレーション コマンドを使用して設定された権限レベルを上書きできます。 また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。 上位の権限レベルのパスワードがわかっていれば、ユーザはそのパスワードを使用して上位の権限レベ

ルをイネーブルにできます。 回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

関連トピック

権限レベル, （1332 ページ）

権限レベルへのログインおよび終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、ユーザ EXEC モードで次の手順を実行します。

手順の概要

1. **enable***level*
2. **disable***level*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable***level* 例： `Switch> enable 15`	指定された特権レベルにログインします。 この例で、レベル 15 は特権 EXEC モードです。 *level* に指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable***level* 例： `Switch# disable 1`	指定した特権レベルを終了します。 この例で、レベル 1 はユーザ EXEC モードです。 *level* に指定できる範囲は 0 ～ 15 です。

関連トピック

権限レベル, （1332 ページ）

スイッチ アクセスのモニタリング

表 *124*：*DHCP* 情報を表示するためのコマンド

show privilege	権限レベルの設定を表示します。

パスワードおよび権限レベルの設定例

例：スタティック イネーブル パスワードの設定または変更

次に、イネーブル パスワードを*l1u2c3k4y5* に変更する例を示します。 パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モード アクセス）。

```
Switch(config)# enable password l1u2c3k4y5
```

関連トピック

スタティック イネーブル パスワードの設定または変更，（1333 ページ）

例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

次に、権限レベル 2 に対して暗号化パスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

関連トピック

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護，（1334 ページ）
追加のパスワード セキュリティ，（1330 ページ）

例：端末回線に対する Telnet パスワードの設定

次に、Telnet パスワードを *let45me67in89* に設定する例を示します。

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

関連トピック

端末回線に対する Telnet パスワードの設定，（1338 ページ）
端末回線の Telnet 設定，（1331 ページ）

例：コマンドの権限レベルの設定

configure コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして *SecretPswd14* を定義する例を示します。

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```

関連トピック

コマンドの特権レベルの設定, （1342 ページ）
権限レベル, （1332 ページ）

第 49 章

TACACS+ の設定

- 機能情報の確認，1349 ページ
- Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件，1349 ページ
- TACACS+ の概要，1351 ページ
- TACACS+ を設定する方法，1356 ページ
- TACACS+ のモニタリング，1365 ページ

機能情報の確認

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

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

Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件

Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスのセットアップと設定の前提条件は、次のとおりです（示されている順序で実行する必要があります）。

1. スイッチに TACACS+ サーバ アドレスとスイッチを設定します。
2. 認証キーを設定します。

3 TACACS+ サーバでステップ 2 からキーを設定します。

4 AAA をイネーブルにします。

5 ログイン認証方式リストを作成します。

6 端末回線にリストを適用します。

7 認証およびアカウンティング方式のリストを作成します。

TACACS+ によるスイッチ アクセスの制御の前提条件は、次のとおりです。

- スイッチ上で TACACS+ 機能を設定するには、設定済みの TACACS+ サーバにアクセスする必要があります。 また、通常 LINUX または Windows ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されている TACACS+ サービスにもアクセスする必要があります。
- スイッチ スタックと TACACS+ サーバとの間に冗長接続を設定することを推奨します。 これによって、接続済みのスタック メンバの 1 つがスイッチ スタックから削除された場合でも、TACACS+ サーバにアクセスできます。
- スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼働するシステムが必要です。
- TACACS+ を使用するには、それをイネーブルにする必要があります。
- 許可は、使用するスイッチでイネーブルにする必要があります。
- ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
- この項または他の項で示す AAA コマンドを使用するには、まず **aaa new-model** コマンドを使用して AAA をイネーブルにする必要があります。
- 最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。 また、任意で TACACS+ 許可およびアカウンティングの方式リストを定義できます。
- 方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。 唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。 デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。 定義済みの方式リストは、デフォルトの方式リストに優先します。
- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。

関連トピック

TACACS+ の概要, （1351 ページ）
TACACS+ の動作, （1353 ページ）

TACACS+ を設定する方法, （1356 ページ）
方式リスト, （1354 ページ）
TACACS+ ログイン認証の設定, （1358 ページ）
TACACS+ ログイン認証, （1354 ページ）
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定, （1361 ページ）
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可, （1355 ページ）

TACACS+ の概要

TACACS+ およびスイッチ アクセス

ここでは、TACACS+について説明します。 TACACS+は詳細なアカウンティング情報を提供し、認証と許可のプロセスを柔軟に管理します。 TACACS+は、認証、許可、アカウンティング（AAA）機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用する必要があります。

関連トピック

不正アクセスの防止, （1327 ページ）
スイッチのローカル認証および許可の設定, （1413 ページ）
SSH サーバ、統合クライアント、およびサポートされているバージョン, （1419 ページ）

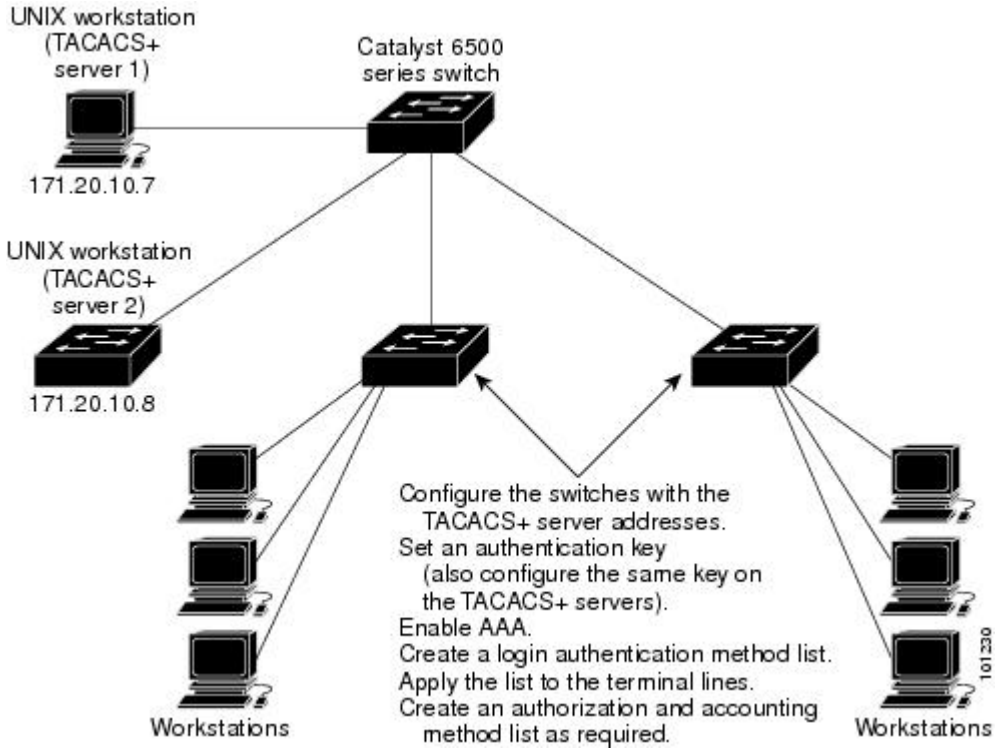
TACACS+ の概要

TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。 TACACS+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）が各サービス（認証、許可、およびアカウンティング）を別個に提供します。 各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ の目的は、1 つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。 スイッチは、他の Cisco ルータやアクセス サーバとともにネットワーク アクセス サーバにできます。

図 *89*：一般的な *TACACS+* ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージ サポートによって認証の完全制御を行います。

  認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードが入力された後、自宅の住所、母親の旧姓、サービスタイプ、社会保険番号などのいくつかの質問をすることによりユーザを試します）。 TACACS+ 認証サービスは、ユーザ画面にメッセージを送信することもできます。 たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。

- 許可：autocommand、アクセス コントロール、セッション期間、プロトコル サポートの設定といった、ユーザセッション時のユーザ機能についてきめ細かく制御します。 また、TACACS+ 許可機能によって、ユーザが実行できるコマンドを制限することもできます。

- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。 ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供した

りできます。 アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

関連トピック

Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件, （1349 ページ）

TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1. 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これをユーザに表示します。 ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワード プロンプトを取得します。 スイッチによってパスワード プロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

   TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。 デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。

   - ACCEPT：ユーザが認証され、サービスを開始できます。 許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
   - REJECT：ユーザは認証されません。 TACACS+ デーモンに応じて、ユーザはアクセスを拒否されるか、ログイン シーケンスを再試行するように求められます。
   - ERROR：デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。 ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
   - CONTINUE：ユーザは、さらに認証情報の入力を求められます。

   認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。 ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。 ACCEPT 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛ての属性の形式でデータが含まれています。

   - Telnet、セキュア シェル（SSH）、rlogin、または特権 EXEC サービス

- 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、および ユーザ タイムアウトを含む）

関連トピック

Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件, （1349 ページ）

方式リスト

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。 方式リストを使用して、使用するセキュリティ プロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。 ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。 このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

関連トピック

TACACS+ を設定する方法, （1356 ページ）
Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件, （1349 ページ）

TACACS+ 設定オプション

認証用に 1 つのサーバを使用することも、また、既存のサーバ ホストをグループ化するために AAA サーバ グループを使用するように設定することもできます。 サーバをグループ化して設定済みサーバホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。 サーバグループは、グローバル サーバ ホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストが含まれています。

関連トピック

TACACS+ サーバ ホストの指定および認証キーの設定, （1356 ページ）

TACACS+ ログイン認証

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。 認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。 ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。 このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。 この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否

すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

関連トピック

TACACS+ ログイン認証の設定, （1358 ページ）
Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件, （1349 ページ）

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可

AAA 許可によってユーザが使用できるサービスが制限されます。 AAA 許可がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザデータベースまたはセキュリティサーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

関連トピック

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定, （1361 ページ）
Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件, （1349 ページ）

TACACS+ アカウンティング

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。 AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。 このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

関連トピック

TACACS+ アカウンティングの起動, （1363 ページ）

TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。 TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

（注） TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

TACACS+ を設定する方法

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。

関連トピック

方式リスト，（1354 ページ）

Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件，（1349 ページ）

TACACS+ サーバ ホストの指定および認証キーの設定

TACACS+ サーバ ホストを特定し、認証キーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **tacacs-server host***hostname*
4. **aaa new-model**
5. **aaa group server tacacs+***group-name*
6. **server***ip-address*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**tacacs-server host***hostname* 例： `Switch(config)# tacacs-server host yourserver`	TACACS+ サーバを維持する IP ホストを特定します。 このコマンドを複数回入力して、優先ホストのリストを作成します。 ソフトウェアは、指定された順序でホストを検索します。 *hostname* には、ホストの名前または IP アドレスを指定します。
ステップ 4	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 5	**aaa group server tacacs+***group-name* 例： `Switch(config)# aaa group server tacacs+ your_server_group`	（任意）グループ名でAAAサーバグループを定義します。 このコマンドによって、Switchはサーバ グループ サブコンフィギュレーション モードになります。
ステップ 6	**server***ip-address* 例： `Switch(config)# server 10.1.2.3`	（任意）特定のTACACS+サーバを定義済みサーバ グループに関連付けます。 AAA サーバ グループの TACACS+ サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 3 で定義済みのものでなければなりません。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

TACACS+ 設定オプション，（1354 ページ）

TACACS+ ログイン認証の設定

TACACS+ ログイン認証を設定するには、次の手順を実行します。

はじめる前に

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。

（注） AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。 AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ip http authentication コマンドの詳細については、『*Cisco IOS Security Command Reference, Release 12.4*』を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
5. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
6. **login authentication** {**default** | *list-name*}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch>` **`enable`**	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch#` **`configure terminal`**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Switch(config)#` **`aaa new-model`**	AAA をイネーブルにします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Switch(config)#` **`aaa authentication login default tacacs+ local`**	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。 デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。 追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • *enable*：イネーブル パスワードを認証に使用します。 この認証方式を使用するには、あらかじめ **enable***password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 • *group tacacs+*：TACACS+ 認証を使用します。 この認証方式を使用するには、あらかじめ TACACS+ サーバを設定しておく必要があります。 詳細については、TACACS+ サーバ ホストの指定および認証キーの設定, （1356 ページ）を参照してください。

	コマンドまたはアクション	目的
		• *line*：回線パスワードを認証に使用します。 この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。 **password***password* ライン コンフィギュレーション コマンドを使用します。 • *local*：ローカルユーザ名データベースを認証に使用します。 データベースにユーザ名情報を入力しておく必要があります。 **username***password* グローバル コンフィギュレーション コマンドを使用します。 • *local-case*：大文字と小文字が区別されるローカルユーザ名データベースを認証に使用します。 **username***name* **password** グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 • *none*：ログインに認証を使用しません。
ステップ 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Switch(config)# line 2 4`	ライン コンフィギュレーションモードを開始し、認証リストを適用する回線を設定します。
ステップ 6	**login authentication** {**default** | *list-name*} 例： `Switch(config-line)# login authentication default`	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 7	**end** 例： `Switch(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	例： `Switch# copy running-config startup-config`	

関連トピック

TACACS+ ログイン認証, （1354 ページ）

Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件, （1349 ページ）

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

aaa authorization グローバル コンフィギュレーション コマンドと **tacacs+** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa authorization network tacacs+**
4. **aaa authorization exec tacacs+**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization network tacacs+** 例： `Switch(config)# aaa authorization network tacacs+`	ネットワーク関連のすべてのサービス要求に対してユーザ TACACS+ 認可を行うことを設定します。
ステップ 4	**aaa authorization exec tacacs+** 例： `Switch(config)# aaa authorization exec tacacs+`	ユーザの特権 EXEC アクセスに対してユーザ TACACS+ 認可を行うことを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可, （1355 ページ）

Terminal Access Controller Access Control System Plus（TACACS+）によるスイッチ アクセスの制御の前提条件, （1349 ページ）

TACACS+ アカウンティングの起動

TACACS+ アカウンティングを開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa accounting network start-stop tacacs+**
4. **aaa accounting exec start-stop tacacs+**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting network start-stop tacacs+** 例： `Switch(config)# aaa accounting network start-stop tacacs+`	ネットワーク関連のすべてのサービス要求について、TACACS+アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting exec start-stop tacacs+** 例： `Switch(config)# aaa accounting exec`	TACACS+ アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。

	コマンドまたはアクション	目的
	start-stop tacacs+	
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。 これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。 場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

関連トピック

TACACS+ アカウンティング，（1355 ページ）

AAA サーバが到達不能な場合のルータとのセッションの確立

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。 これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。 場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

TACACS+ のモニタリング

表 *125* : *TACACS+* 情報を表示するためのコマンド

コマンド	目的
show tacacs	TACACS+ サーバの統計情報を表示します。

第 50 章

RADIUS の設定

- 機能情報の確認，1367 ページ
- RADIUS によるSwitch アクセスの制御の前提条件，1367 ページ
- RADIUS によるSwitch アクセスの制御の制約事項，1368 ページ
- RADIUS に関する情報，1369 ページ
- RADIUS の設定方法，1380 ページ
- CoA 機能のモニタリング，1401 ページ
- RADIUS によるスイッチ アクセスの制御の設定例，1401 ページ

機能情報の確認

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

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

RADIUS によるSwitch アクセスの制御の前提条件

ここでは、RADIUS によるSwitch アクセスの制御の前提条件を示します。

全般：

- この章のいずれかのコンフィギュレーション コマンドを使用するには、RADIUS および AAA をイネーブルにする必要があります。

- RADIUS は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。
- 最低限、RADIUS サーバ ソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS 認証の方式リストを定義する必要があります。 また、任意で RADIUS 許可およびアカウンティングの方式リストを定義できます。
- Switch上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。
- RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアが稼働しているマルチユーザ システムです。 詳細については、RADIUS サーバのマニュアルを参照してください。
- Change-of-Authorization（CoA）インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。 CoA を使用すると、セッションの識別と接続解除要求を実行できます。 アップデートは、指定されたセッションにだけ作用します。

RADIUS 操作の場合：

- ユーザはRADIUS許可に進む前に、まずRADIUS認証を正常に完了する必要があります（イネーブルに設定されている場合）。

関連トピック

RADIUS およびスイッチ アクセス, （1369 ページ）
RADIUS の動作, （1370 ページ）

RADIUS によるSwitch アクセスの制御の制約事項

ここでは、RADIUS によるSwitch アクセスの制御の制約事項について説明します。

全般：

- セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用してRADIUS を設定することはできません。

RADIUS は次のネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。 RADIUS は、AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。 RADIUS は、双方向認証を行いません。 RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。 RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

関連トピック

RADIUS の概要, （1369 ページ）

RADIUS に関する情報

RADIUS およびスイッチ アクセス

この項では、RADIUS をイネーブルにし、設定する方法について説明します。 RADIUS を使用すると、アカウンティングの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます。

関連トピック

RADIUS によるSwitch アクセスの制御の前提条件, （1367 ページ）
スイッチのローカル認証および許可の設定, （1413 ページ）
SSH サーバ、統合クライアント、およびサポートされているバージョン, （1419 ページ）

RADIUS の概要

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。 RADIUS クライアントは、サポート対象の Cisco ルータおよびスイッチ上で稼働します。 クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。

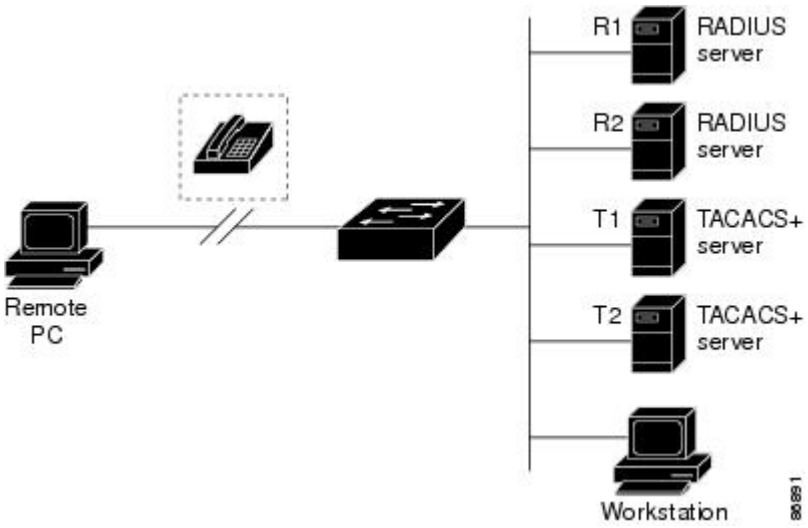
RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。 複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カード アクセス コントロール システムを使用するアクセス環境。 あるケースでは、RADIUS は Enigma のセキュリティ カードとともに使用してユーザを確認し、ネットワーク リソースのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。 RADIUS クライアント装備のシスコのSwitchをネットワークに追加できます。 これが TACACS+ サーバへの移行の最初のステップとなることもあります。 下の図 2「RADIUS サービスから TACACS+ サービスへの移行」を参照してください。
- ユーザが 1 つのサービスにしかアクセスできないネットワーク。 RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1x

などのプロトコルを使用するネットワークに制御できます。 このプロトコルの詳細については、第 11 章「IEEE 802.1x ポートベース認証の設定」を参照してください。

- リソース アカウンティングが必要なネットワーク。 RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。 RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。 インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェアバージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

図 *90*：***RADIUS*** サービスから ***TACACS+*** サービスへの移行



関連トピック

RADIUS によるSwitch アクセスの制御の制約事項, （1368 ページ）

RADIUS の動作

RADIUS サーバによってアクセス コントロールされるSwitchに、ユーザがログインおよび認証を試みると、次のイベントが発生します。

1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由でRADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   - ACCEPT：ユーザが認証されたことを表します。
   - REJECT：ユーザの認証が失敗し、ユーザ名およびパスワードの再入力が要求されるか、またはアクセスが拒否されます。

- CHALLENGE：ユーザに追加データを要求します。
- CHALLENGE PASSWORD：ユーザは新しいパスワードを選択するように要求されます。

ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。 ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

関連トピック

RADIUS によるSwitch アクセスの制御の前提条件, （1367 ページ）

RADIUS 許可の変更

ここでは、使用可能なプリミティブおよびそれらの Change of Authorization（CoA）での使用方法を含む、RADIUS インターフェイスの概要について説明します。

- Change-of-Authorization 要求
- CoA 要求応答コード
- CoA 要求コマンド
- セッション再認証
- セッション強制終了のスタック構成ガイドライン

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。 Catalyst スイッチは、通常プッシュ モデルで使用される RFC 5176 で規定された RADIUS Change of Authorization（CoA）拡張機能をサポートし、外部の認証、許可、アカウンティング（AAA）またはポリシーサーバからのセッションのダイナミック再設定ができるようにします。

スイッチは、次のセッション単位の CoA 要求をサポートしています。

- セッション再認証
- セッション終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了

この機能は、Cisco Secure Access Control Server (ACS) 5.1 に統合されています。

Catalyst スイッチでは、RADIUS インターフェイスはデフォルトでイネーブルに設定されています。 ただし、次の属性については、一部の基本的な設定が必要になります。

- セキュリティおよびパスワード：このガイドの「スイッチへの不正アクセスの防止」を参照してください。
- アカウンティング：このガイドの「スイッチベース認証の設定」の章の「RADIUS アカウンティングの起動」の項を参照してください。

Change-of-Authorization 要求

Change of Authorization（CoA）要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。 このモデルは、1 つの要求（CoA-Request）と 2 つの可能な応答コードで構成されています。

- CoA acknowledgment（ACK）[CoA-ACK]
- CoA non-acknowledgment（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から発信されて、リスナーとして動作するスイッチに送信されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してスイッチでサポートされています。

次の表に、この機能でサポートされている IETF 属性を示します。

表 *126*：サポートされている *IETF* 属性

属性番号	属性名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 *127*：*Error-Cause* の値

値	説明
201	削除された残留セッション コンテキスト

値	説明
202	無効な EAP パケット（無視）
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求（プロキシ）
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチセッションの選択がサポートされてない

CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。

関連トピック

CoA 要求コマンド, （1374 ページ）

セッションの識別

特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）

- Audit-Session-Id VSA（シスコの VSA）
- Acct-Session-Id（IETF 属性 #44）

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、スイッチは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

複数のセッション ID 属性がメッセージ含まれる場合は、すべての属性がセッションと一致しなければなりません。そうでない場合は、スイッチが Disconnect - negative acknowledgement（NAK）または CoA -NAK と、「Invalid Attribute Value」エラー コードを返します。

RFC 5176 で定義されている CoA 要求コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                         Authenticator                         |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

属性フィールドは、シスコのベンダー固有属性（VSA）を送信するために使用します。

関連トピック

CoA 接続解除要求, （1376 ページ）
CoA 要求：ホスト ポートのディセーブル化, （1376 ページ）
CoA 要求：バウンス ポート, （1376 ページ）

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。 CoA ACK 内で返される属性は CoA 要求によって異なり、個々の CoA コマンドで検討されます。

CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。 CoA が成功したかを確認するには、**show** コマンドを使用します。

CoA 要求コマンド

表 *128*：スイッチでサポートされる *CoA* コマンド

コマンド [10]	シスコの VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"

コマンド [10]	シスコの VSA
Terminate session	これは、VSA を要求しない、標準の接続解除要求です。
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

10 すべての CoA コマンドには、スイッチと CoA クライアント間のセッション識別情報が含まれている必要があります。

関連トピック

CoA 要求応答コード, （1373 ページ）

セッション再認証

不明な ID またはポスチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファイル（たとえば、ゲスト VLAN）に関連付けられると、AAA サーバは通常、セッション再認証要求を生成します。 再認証要求は、クレデンシャルが不明である場合にホストが適切な認証グループに配置されることを許可します。

セッション認証を開始するために、AAA サーバは *Cisco:Avpair="subscriber:command=reauthenticate"* の形式で Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。

現在のセッション ステートは、メッセージに対するスイッチの応答を決定します。 セッションが現在、IEEE 802.1x によって認証されている場合、スイッチは EAPOL（LAN 経由の拡張認証プロトコル）RequestId メッセージをサーバに送信することで応答します。

現在、セッションが MAC 認証バイパス（MAB）で認証されている場合は、スイッチはサーバにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

スイッチがコマンドを受信したときにセッション認証が実行中である場合は、スイッチはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションがまだ認証されてない、あるいはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認証されている場合は、再認証メッセージがアクセス コントロール方式を再開し、最初に試行されるように設定された方式で開始します。 セッションの現在の許可は、再認証によって異なる認証結果になるまで維持されます。

セッションの終了

セッションを終了させる 3 種類の CoA 要求があります。 CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。 このコマンドを使用すると、指定されたホストのオーセンティケータ ステートマシンが再初期化されますが、そのホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA の設定で CoA 要求を使用します。 このコマンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であ

り、そのホストに対してネットワークアクセスをただちにブロックする必要があります。 ポートへのネットワーク アクセスを復旧する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

プリンタなどのサプリカントを持たないデバイスが新しい IP アドレスを取得する必要がある場合（たとえば、VLAN 変更後）は、ポート バウンスでホスト ポート上のセッションを終了します（ポートを一時的にディセーブルした後、再びイネーブルにする）。

CoA 接続解除要求

このコマンドは標準の接続解除要求です。 セッションが見つからない場合、スイッチは Disconnect-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。 セッションがある場合は、スイッチはセッションを終了します。 セッションが完全に削除された後、スイッチは接続解除 ACK を返します。

スイッチがクライアントに接続解除 ACK を返す前にスタンバイ スイッチにフェールオーバーする場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。 再送信後もセッションが見つからない場合は、Disconnect-ACK と「Session Context Not Found」エラー コード属性が送信されます。

関連トピック

セッションの識別, （1373 ページ）

CoA 要求：ホスト ポートのディセーブル化

このコマンドは、次の新しい VSA が含まれている標準 CoA 要求メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

セッションが見つからない場合、スイッチは CoA-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。 このセッションがある場合は、スイッチはホスト ポートをディセーブルにし、CoA-ACK メッセージを返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。 スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

（注） 再送信コマンドの後に接続解除要求が失敗すると、（接続解除 ACK が送信されてない場合に）チェンジオーバー前にセッションが正常終了し、または元のコマンドが実行されてスタンバイ スイッチがアクティブになるまでの間に発生した他の方法（たとえば、リンク障害）によりセッションが終了することがあります。

関連トピック

セッションの識別, （1373 ページ）

CoA 要求：バウンス ポート

このコマンドは、次の VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、1 つ以上のセッション ID 属性とともに使用する必要があります。 セッションが見つからない場合、スイッチはCoA-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。 このセッションがある場合は、スイッチはホスト ポートを 10 秒間ディセーブルし、再びイネーブルにし（ポート バウンス）、CoA-ACK を返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。 スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

関連トピック

セッションの識別, （1373 ページ）

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。 RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

RADIUS サーバ ホスト

スイッチと RADIUS サーバの通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。 IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS ホストとして個々のポートを定義できます。 この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。 この例では、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、スイッチは「%RADIUS-4-RADIUS_DEAD」メッ

セージを表示し、その後、同じデバイス上で 2 番めに設定されたホスト エントリでアカウンティング サービスを試みます（RADIUS ホストエントリは、設定した順序に従って試行されます）。

RADIUS サーバとスイッチは、共有するシークレット テキスト ストリングを使用して、パスワードの暗号化および応答の交換を行います。 RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバ デーモンが稼働するホストと、そのホストがスイッチと共有するシークレット テキスト（キー）ストリングを指定する必要があります。

タイムアウト、再送信回数、および暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定することもできますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単位での設定を組み合わせることもできます。

関連トピック

RADIUS サーバ ホストの識別, （1380 ページ）
AAA サーバ グループの定義, （1386 ページ）
すべての RADIUS サーバの設定, （1393 ページ）
RADIUS ログイン認証の設定, （1383 ページ）

RADIUS ログイン認証

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。 方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。 唯一の例外は、デフォルトの方式リストです。 デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。 認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。 ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。 このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。 この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

関連トピック

RADIUS ログイン認証の設定, （1383 ページ）

AAA サーバ グループ

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。 設定済みのサーバホストのサブセットを選択して、それを特定のサービスに使用します。 サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバグループには、同じサーバの複数のホストエントリを含めることもできますが、各エントリが一意の ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。 同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。

関連トピック

AAA サーバ グループの定義, （1386 ページ）

AAA 許可

AAA 許可によってユーザが使用できるサービスが制限されます。 AAA 許可をイネーブルにすると、スイッチは（ローカル ユーザ データベースまたはセキュリティ サーバ上に存在する）ユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。 ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

関連トピック

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定, （1389 ページ）

RADIUS アカウンティング

AAA アカウンティング機能は、ユーザが使用したサービスと、消費したネットワーク リソース量を追跡します。 AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で RADIUS セキュリティ サーバに報告します。 各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。 これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。

関連トピック

RADIUS アカウンティングの起動, （1391 ページ）

ベンダー固有の RADIUS 属性

Internet Engineering Task Force（IETF）ドラフト規格に、ベンダー固有の属性（属性 26）を使用して、スイッチと RADIUS サーバ間でベンダー固有の情報を通信するための方式が定められています。 各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。 シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。 シス

コのベンダーIDは9であり、サポート対象のオプションはベンダータイプ1（名前は*cisco-avpair*）です。 この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

*protocol*は、特定の認可タイプに使用するシスコのプロトコル属性の値です。 *attribute*および*value*は、シスコのTACACS+仕様で定義されている適切な属性値（AV）ペアです。*sep*は、必須の属性の場合は=、任意指定の属性の場合は*です。 TACACS+許可で使用できるすべての機能は、RADIUSでも使用できます。

他のベンダーにも、それぞれ独自のベンダーID、オプション、および対応するVSAがあります。ベンダーIDおよびVSAの詳細については、RFC 2138『Remote Authentication Dial-In User Service（RADIUS）』を参照してください。

RADIUS属性の完全なリスト、またはベンダー固有の属性26の詳細については、『*Cisco IOS Security Configuration Guide*』の付録「RADIUS Attributes」を参照してください。

関連トピック

ベンダー固有のRADIUS属性を使用するスイッチ設定, （1394ページ）

ベンダー独自仕様の RADIUS サーバ通信

RADIUSに関するIETFドラフト規格では、スイッチとRADIUSサーバ間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS属性セットを独自に機能拡張しているベンダーもあります。 Cisco IOSソフトウェアは、ベンダー独自仕様のRADIUS属性のサブセットをサポートしています。

前述したように、RADIUS（ベンダーの独自仕様によるものか、IETFドラフトに準拠するものかを問わず）を設定するには、RADIUSサーバ デーモンが稼働しているホストと、そのホストがスイッチと共有するシークレット テキスト ストリングを指定する必要があります。 RADIUSホストおよびシークレット テキスト ストリングを指定するには、**radius-server** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

ベンダー独自のRADIUSサーバとの通信に関するスイッチ設定, （1396ページ）

RADIUS の設定方法

RADIUS サーバ ホストの識別

Switchと通信するすべてのRADIUSサーバに対して、これらの設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** の3つの固有のグローバル コンフィギュレーション コマンドを使用します。 これらの設定を特定のRADIUSサーバに適用するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。

既存のサーバ ホストを認証用にグループ化するため、AAAサーバ グループを使用するようにSwitchを設定できます。 詳細については、次の関連項目を参照してください。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。 これらの設定値としては、SwitchのIPアドレス、およびサーバとSwitchの双方で共有するキー ストリングがあります。 詳細については、RADIUS サーバのマニュアルを参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、次の手順を実行します。

はじめる前に

スイッチ上にグローバルな機能とサーバ単位での機能（タイムアウト、再送信回数、およびキーコマンド）を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、およびキーに関するコマンドは、グローバルに設定したタイムアウト、再送信回数、およびキーに関するコマンドを上書きします。 すべての RADIUS サーバに対してこれらの値を設定する方法については、次の関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port***port-number*] [**acct-port***port-number*] [**timeout***seconds*] [**retransmit***retries*] [**key***string*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port***port-number*] [**acct-port***port-number*] [**timeout***seconds*] [**retransmit***retries*] [**key***string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port***port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port***port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。

	コマンドまたはアクション	目的
	例： `Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1`	• （任意）**timeout***seconds* には、Switchが RADIUS サーバの応答を待機して再送信するまでの時間間隔を指定します。 指定できる範囲は 1 ～ 1000 です。 この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。 **radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit***retries* には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。 指定できる範囲は 1 ～ 1000 です。 **radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key***string* には、RADIUS サーバ上で動作する RADIUS デーモンとSwitchの間で使用する認証および暗号キーを指定します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。 先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 1 つの IP アドレスに対応する複数のホスト エントリをSwitchが認識するように設定するには、それぞれ異なる UDP ポート番号を使用して、このコマンドを必要な回数だけ入力します。 Switch ソフトウェアは、指定された順序に従って、ホストを検索します。 各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	例： `Switch# copy running-config startup-config`	

関連トピック

RADIUS サーバ ホスト，（1377 ページ）
AAA サーバ グループの定義，（1386 ページ）
すべての RADIUS サーバの設定，（1393 ページ）

RADIUS ログイン認証の設定

RADIUS ログイン認証を設定するには、次の手順を実行します。

はじめる前に

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。 AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
5. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
6. **login authentication** {**default** | *list-name*}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Switch(config)# aaa authentication login default local`	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。 デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。 追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 ◦ *enable*：イネーブル パスワードを認証に使用します。 この認証方式を使用するには、あらかじめ **enable***password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 ◦ *group radius*：RADIUS 認証を使用します。 この認証方式を使用するには、あらかじめ RADIUS サーバを設定しておく必要があります。 ◦ *line*：回線パスワードを認証に使用します。 この認証方式を使用するには、あらかじめ回線パスワードを定義しておく

	コマンドまたはアクション	目的
		必要があります。 **password***password* ライン コンフィギュレーション コマンドを使用します。 ◦ *local*：ローカルユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。 **username***name***password** グローバル コンフィギュレーション コマンドを使用します。 ◦ *local-case*：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。 **username***password* グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 ◦ *none*：ログインに認証を使用しません。
ステップ 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Switch(config)# line 1 4`	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 6	**login authentication** {**default** | *list-name*} 例： `Switch(config)# login authentication default`	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	例： `Switch# copy running-config startup-config`	

関連トピック

RADIUS ログイン認証, （1378 ページ）

RADIUS サーバ ホスト, （1377 ページ）

AAA サーバ グループの定義

定義したグループ サーバに特定のサーバを関連付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。 サーバを IP アドレスで特定することも、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホストインスタンスまたはエントリを特定することもできます。

AAA サーバ グループを定義するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port***port-number*] [**acct-port***port-number*] [**timeout***seconds*] [**retransmit***retries*] [**key***string*]
4. **aaa new-model**
5. **server***group-name*
6. **server***ip-address*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port***port-number*] [**acct-port***port-number*] [**timeout***seconds*] [**retransmit***retries*] [**key***string*] 例： `Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1`	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port***port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port***port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout***seconds* には、スイッチが RADIUS サーバの応答を待機して再送信するまでの時間間隔を指定します。 指定できる範囲は 1 ～ 1000 です。 この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。 **radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit***retries* には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。 指定できる範囲は 1 ～ 1000 です。 **radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key***string* には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。

	コマンドまたはアクション	目的
		（注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。 先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、それぞれ異なる UDP ポート番号を使用して、このコマンドを必要な回数だけ入力します。 スイッチ ソフトウェアは、指定された順序に従って、ホストを検索します。 各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
ステップ 4	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 5	**server***group-name* 例： `Switch(config)# aaa group server radius group1`	グループ名を指定して AAA サーバ グループを定義します。 このコマンドを使用すると、スイッチはサーバ グループ コンフィギュレーション モードになります。
ステップ 6	**server***ip-address* 例： `Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001`	特定の RADIUS サーバを定義済みのサーバ グループと関連付けます。 AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

RADIUS サーバ ホストの識別，（1380 ページ）
RADIUS サーバ ホスト，（1377 ページ）
AAA サーバ グループ，（1378 ページ）

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

ユーザ特権アクセスおよびネットワーク サービスに関する RADIUS 許可を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa authorization network radius**
4. **aaa authorization exec radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**aaa authorization network radius** 例： `Switch(config)# aaa authorization network radius`	ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。
ステップ 4	**aaa authorization exec radius** 例： `Switch(config)# aaa authorization exec radius`	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ RADIUS 許可をスイッチに設定します。 **exec** キーワードを指定すると、ユーザプロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

aaa authorization グローバル コンフィギュレーション コマンドと **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

関連トピック

AAA 許可, （1379 ページ）

RADIUS アカウンティングの起動

RADIUS アカウンティングを開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa accounting network start-stop radius**
4. **aaa accounting exec start-stop radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**aaa accounting network start-stop radius** 例： `Switch(config)# aaa accounting network start-stop radius`	ネットワーク関連のあらゆるサービス要求に関して、RADIUS アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting exec start-stop radius** 例： `Switch(config)# aaa accounting exec start-stop radius`	RADIUS アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。 このコマンドは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。 場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

関連トピック

RADIUS アカウンティング，（1379 ページ）

すべての RADIUS サーバの設定

すべての RADIUS サーバを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **radius-server key***string*
3. **radius-server retransmit***retries*
4. **radius-server timeout***seconds*
5. **radius-server deadtime***minutes*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server key***string* 例： `Switch(config)# radius-server key your_server_key`	スイッチとすべてのRADIUSサーバ間で共有されるシークレット テキスト ストリングを指定します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキストストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 3	**radius-server retransmit***retries* 例： `Switch(config)# radius-server retransmit 5`	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。 デフォルトは 3 です。指定できる範囲は 1 ～ 1000 です。
ステップ 4	**radius-server timeout***seconds* 例： `Switch(config)# radius-server`	スイッチが RADIUS 要求に対する応答を待って、要求を再送信するまでの時間（秒）を指定します。 デフォルトは 5 秒です。指定できる範囲は 1 ～ 1000 です。

	コマンドまたはアクション	目的
	`timeout 3`	
ステップ 5	**radius-server deadtime***minutes* 例： `Switch(config)# radius-server deadtime 0`	RADIUS サーバが認証要求に応答していない場合、このコマンドはそのサーバに対する要求を停止する時刻を指定します。これにより、要求がタイムアウトするまで待たずとも、次に設定されているサーバを試行することができます。 デフォルトは 0 です。指定できる範囲は 0 ～ 1440 分です。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

RADIUS サーバ ホストの識別, （1380 ページ）
RADIUS サーバ ホスト, （1377 ページ）

ベンダー固有の RADIUS 属性を使用するスイッチ設定

ベンダー固有仕様の RADIUS 属性を使用するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server vsa send** [**accounting** | **authentication**] 例： `Switch(config)# radius-server vsa send`	スイッチが VSA（RADIUS IETF 属性 26 で定義）を認識して使用できるようにします。 • （任意）認識されるベンダー固有属性の集合をアカウンティング属性だけに限定するには、**accounting** キーワードを使用します。 • （任意）認識されるベンダー固有属性の集合を認証属性だけに限定するには、**authentication** キーワードを使用します。 キーワードを指定せずにこのコマンドを入力すると、アカウンティングおよび認証のベンダー固有属性の両方が使用されます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ベンダー固有の RADIUS 属性, （1379 ページ）

ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定

ベンダー独自仕様の RADIUS サーバ通信を使用するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-server host** {*hostname* | *ip-address*} **non-standard**
4. **radius-server key***string*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} **non-standard** 例： `Switch(config)# radius-server host 172.20.30.15 nonstandard`	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、RADIUS のベンダー独自仕様の実装を使用することを指定します。
ステップ 4	**radius-server key***string* 例： `Switch(config)# radius-server key rad124`	スイッチとベンダー独自仕様の RADIUS サーバとの間で共有されるシークレット テキスト ストリングを指定します。 スイッチと RADIUS サーバはこのテキスト ストリングを使用してパスワードを暗号化し、応答を交換します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

この機能を使用すると、アクセス要求および認証要求を、サーバ グループ内のすべての RADIUS サーバに対して均等に送信できます。 詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「RADIUS Server Load Balancing」の章を参照してください。

関連トピック

ベンダー独自仕様の RADIUS サーバ通信, （1380 ページ）

スイッチ上での CoA の設定

CoA をスイッチで設定するには、次の手順を実行します。 この手順は必須です。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name*} [**vrf***vrfname*] [**server-key***string*]
6. **server-key** [**0** | **7**] *string*
7. **port***port-number*
8. **auth-type** {**any** | **all** | **session-key**}
9. **ignore session-key**
10. **ignore server-key**
11. **authentication command bounce-port ignore**
12. **authentication command disable-port ignore**
13. **end**
14. **show running-config**
15. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa server radius dynamic-author** 例： `Switch(config)# aaa server radius dynamic-author`	スイッチを認証、許可、アカウンティング（AAA）サーバに設定し、外部ポリシー サーバとの相互作用を促進します。
ステップ 5	**client** {*ip-address* | *name*} [**vrf***vrfname*] [**server-key***string*]	ダイナミック許可ローカル サーバ コンフィギュレーション モードを開始し、デバイスが CoA を受け取り、要求を取り外す RADIUS クライアントを指定します。
ステップ 6	**server-key** [**0** | **7**] *string* 例： `Switch(config-sg-radius)# server-key your_server_key`	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 7	**port***port-number* 例： `Switch(config-sg-radius)# port 25`	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。
ステップ 8	**auth-type** {**any** | **all** | **session-key**} 例： `Switch(config-sg-radius)# auth-type any`	スイッチが RADIUS クライアントに使用する許可のタイプを指定します。 クライアントは、許可用に設定されたすべての属性と一致していなければなりません。
ステップ 9	**ignore session-key**	（任意）セッション キーを無視するようにスイッチを設定します。 **ignore** コマンドの詳細については、Cisco.com 上の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。

	コマンドまたはアクション	目的
ステップ 10	**ignore server-key** 例： `Switch(config-sg-radius)# ignore server-key`	（任意）サーバ キーを無視するようにスイッチを設定します。 **ignore** コマンドの詳細については、Cisco.com 上の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。
ステップ 11	**authentication command bounce-port ignore** 例： `Switch(config-sg-radius)# authentication command bounce-port ignore`	（任意）CoA 要求を無視して、セッションをホスティングするポートを一時的にディセーブルにするようにスイッチを設定します。 ポートを一時的にディセーブルにする目的は、VLAN の変更が発生しても、その変更を検出するサプリカントがエンドポイント上にない場合に、ホストから DHCP 再ネゴシエーションを行わせることです。
ステップ 12	**authentication command disable-port ignore** 例： `Switch(config-sg-radius)# authentication command disable-port ignore`	（任意）セッションをホスティングしているポートを管理上のシャットダウン状態にすることを要求する非標準コマンドを無視するようにスイッチを設定します。 ポートをシャットダウンすると、セッションが終了します。 ポートを再びイネーブルにするには、標準の CLI または SNMP コマンドを使用します。
ステップ 13	**end** 例： `Switch(config-sg-radius)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 15	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

CoA 機能のモニタリング

表 *129*：特権 *EXEC* 表示コマンド

コマンド	目的
show aaa attributes protocol radius	RADIUS コマンドの AAA 属性を表示します。

表 *130*：グローバル トラブルシューティング コマンド

コマンド	目的
debug radius	RADIUS のトラブルシューティングを行うための情報を表示します。
debug aaa coa	CoA 処理のトラブルシューティングを行うための情報を表示します。
debug aaa pod	POD パケットのトラブルシューティングを行うための情報を表示します。
debug aaa subsys	POD パケットのトラブルシューティングを行うための情報を表示します。
debug cmdhd [**detail** | **error** | **events**]	コマンドヘッダーのトラブルシューティングを行うための情報を表示します。

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

RADIUS によるスイッチ アクセスの制御の設定例

例：RADIUS サーバ ホストの識別

次に、1 つの RADIUS サーバを認証用に、もう 1 つの RADIUS サーバをアカウンティング用に設定する例を示します。

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次に、*host1* を RADIUS サーバとして設定し、認証およびアカウンティングの両方にデフォルトのポートを使用するように設定する例を示します。

```
Switch(config)# radius-server host host1
```

例：2 台の異なる RADIUS グループ サーバの使用

次の例では、2 つの異なる RADIUS グループ サーバ（*group1* および *group2*）を認識するようにスイッチを設定しています。 group1 では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同じサービス用に設定しています。 2 番目のホスト エントリが、最初のエントリのフェールオーバー バックアップとして動作します。

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

例：ベンダー固有の RADIUS 属性を使用するスイッチ設定

たとえば、次の AV ペアを指定すると、IP 許可時（PPP の IPCP アドレスの割り当て時）に、シスコの複数の名前付き *IP* アドレス プール機能が有効になります。

```
cisco-avpair= ”ip:addr-pool=first“
```

次に、スイッチから特権 EXEC コマンドへの即時アクセスが可能となるユーザ ログインを提供する例を示します。

```
cisco-avpair= ”shell:priv-lvl=15“
```

次に、RADIUS サーバ データベース内の許可 VLAN を指定する例を示します。

```
cisco-avpair= ”tunnel-type(#64)=VLAN(13)”
cisco-avpair= ”tunnel-medium-type(#65)=802 media(6)”
cisco-avpair= ”tunnel-private-group-id(#81)=vlanid”
```

次に、この接続中に ASCII 形式の入力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= “ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0”
cisco-avpair= “ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any”
cisco-avpair= “mac:inacl#3=deny any any decnet-iv”
```

次に、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= “ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any”
```

例：ベンダー独自仕様の RADIUS サーバとの通信に関するスイッチ設定

次に、ベンダー独自仕様の RADIUS ホストを指定し、スイッチとサーバの間で *rad124* という秘密キーを使用する例を示します。

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

第 51 章

Kerberos の設定

- 機能情報の確認，1405 ページ
- Kerberos によるスイッチ アクセスの制御の前提条件，1405 ページ
- Kerberos に関する情報，1406 ページ
- Kerberos を設定する方法，1411 ページ
- Kerberos 設定のモニタリング，1411 ページ

機能情報の確認

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

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

Kerberos によるスイッチ アクセスの制御の前提条件

次に、Kerberos を使用してスイッチ アクセスを制御するための前提条件を示します。

- リモート ユーザがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定し、ユーザとネットワーク サービスの両方に通信を行い、相互に認証させる必要があります。 これを実現するには、互いの識別が必要です。 KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。 また、KDC データベースにユーザ用のエントリも作成します。

- Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるスイッチを使用できます。

ホストおよびユーザのエントリを追加または作成する場合の注意事項は次のとおりです。

- Kerberos プリンシパル名はすべて小文字でなければなりません。
- Kerberos インスタンス名はすべて小文字でなければなりません。
- Kerberos レルム名はすべて大文字でなければなりません。

Kerberos に関する情報

ここでは、Kerberos の情報を提供します。

Kerberos とスイッチ アクセス

ここでは、Kerberosセキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。

（注） Kerberos の設定例および『*Cisco IOS Security Command Reference, Release 12.4*』では、スイッチは、信頼できるサードパーティにすることができ、これはKerberosをサポートしていて、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証することができます。

Kerberos の概要

Kerberos はマサチューセッツ工科大学（MIT）が開発した秘密キーによるネットワーク認証プロトコルです。 データ暗号規格（DES）という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。 Kerberos は、信頼できるサードパーティという概念を使ってユーザとサービスに対してセキュリティの検証を実行します。 この信頼できるサードパーティをキー発行局（KDC）と呼びます。

Kerberos は、ユーザが誰であるか、そのユーザが使用しているネットワーク サービスは何であるかを検証します。 これを実行するために、KDC（つまり信頼できる Kerberos サーバ）がユーザにチケットを発行します。 これらのチケットには有効期限があり、ユーザクレデンシャルのキャッシュに保存されます。 Kerberos サーバは、ユーザ名やパスワードの代わりにチケットを使ってユーザとネットワーク サービスを認証します。

（注） Kerberos サーバには、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる スイッチを使用できます。

Kerberos のクレデンシャル発行スキームでは、*single logon* という手順を使用します。 この手順では、ユーザを 1 回認証すると、ユーザ クレデンシャルが有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、（UNIX サーバや PC などの）他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh

次の表に、一般的な Kerberos 関連用語とその定義を示します。

表 *131*：*Kerberos* の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。 たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
許可	ユーザがネットワークやスイッチにおいてどのような権限を有しており、またどのような動作を実行できるかを、スイッチが識別する手段
クレデンシャル	認証チケット（TSG[11]、サービス クレデンシャルなど）を表す総称。 Kerberos クレデンシャルで、ユーザまたはサービスの ID を検証します。 ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することにした場合、ユーザ名やパスワードを再入力する代わりにこれを使用できます。 証明書の有効期限は、8 時間がデフォルトの設定です。

用語	定義
インスタンス	Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、*user@REALM* という形式です（たとえば、smith@EXAMPLE.COM）。 Kerberos インスタンスのある Kerberos プリンシパルは、*user/instance@REALM* という形式です（たとえば、smith/admin@EXAMPLE.COM）。 Kerberos インスタンスは、認証が成功した場合のユーザの承認レベルを指定するために使用できます。各ネットワーク サービスのサーバは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。 （注） Kerberos プリンシパル名およびインスタンス名はすべて小文字でなければなりません。 （注） Kerberos レルム名はすべて大文字でなければなりません。
KDC[12]	ネットワーク ホストで稼働する Kerberos サーバおよびデータベース プログラムで構成されるキー発行局
Kerberos 対応	Kerberos クレデンシャルのインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。 Kerberos サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク サービスの ID を検証します。 （注） Kerberos レルム名はすべて大文字でなければなりません。
Kerberos サーバ	ネットワーク ホストで稼働しているデーモン。ユーザおよびネットワーク サービスはそれぞれ Kerberos サーバに ID を登録します。 ネットワーク サービスは Kerberos サーバにクエリーを送信して、他のネットワーク サービスの認証を得ます。

用語	定義
KEYTAB[13]	ネットワーク サービスが KDC と共有するパスワード。 Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス クレデンシャルを暗号解除して認証します。 Kerberos 5 よりも前のバージョンでは、KEYTAB はSRVTAB[14]と呼ばれます。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。 （注） Kerberos プリンシパル名はすべて小文字でなければなりません。
サービス クレデンシャル	ネットワーク サービスのクレデンシャル。 KDC からクレデンシャルが発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。 ユーザ TGT ともパスワードを共有します。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。 SRVTAB は、Kerberos 5 以降のバージョンでは KEYTAB と呼ばれています。
TGT	身分証明書のことで、KDC が認証済みユーザに発行するクレデンシャル。 TGT を受け取ったユーザは、KDC が示した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

11 チケット認可チケット
12 キー発行局
13 キー テーブル
14 サーバ テーブル

Kerberos の動作

Kerberos サーバには、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してリモートユーザを認証できるスイッチを使用できます。 Kerberos をカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモート ユーザは、3 つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

スイッチを Kerberos サーバとして使用してネットワーク サービスを認証するには、リモートユーザは次の手順を実行する必要があります。

1. 境界スイッチに対する認証の取得, （1410 ページ）
2. KDC からの TGT の取得, （1410 ページ）
3. ネットワーク サービスに対する認証の取得, （1410 ページ）

境界スイッチに対する認証の取得

ここでは、リモートユーザが通過しなければならない最初のセキュリティ レイヤについて説明します。 ユーザは、まず境界スイッチに対して認証を得なければなりません。 リモート ユーザが境界スイッチに対して認証を得る場合、次のプロセスが発生します。

1. ユーザが境界スイッチに対して、Kerberos 未対応の Telnet 接続を開始します。
2. ユーザ名とパスワードの入力を求めるプロンプトをスイッチが表示します。
3. スイッチが、このユーザの TGT を KDC に要求します。
4. KDC がユーザ ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使って TGT の暗号解除を試行します。
   - 暗号解除に成功した場合は、ユーザはスイッチに対して認証を得ます。
   - 暗号解除に成功しない場合は、ユーザ名とパスワードを再入力（Caps Lock または Num Lock のオン/オフに注意）するか、別のユーザ名とパスワードを入力してステップ 2 の手順を繰り返します。

Kerberos 未対応の Telnet セッションを開始し、境界スイッチの認証を得ているリモート ユーザはファイアウォールの内側にいますが、ネットワーク サービスにアクセスするには、KDC から直接認証を得る必要があります。 ユーザが KDC から認証を得なければならないのは、KDC が発行する TGT はスイッチに保存されており、ユーザがこのスイッチにログオンしないかぎり、追加の認証に使用できないからです。

KDC からの TGT の取得

ここでは、リモートユーザが通過しなければならない 2 番めのセキュリティ レイヤについて説明します。 ユーザは、ネットワーク サービスにアクセスするために、このレイヤで KDC の認証を得て、KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章にある「Obtaining a TGT from a KDC」を参照してください。

ネットワーク サービスに対する認証の取得

ここでは、リモートユーザが通過しなければならない 3 番めのセキュリティ レイヤについて説明します。 TGT を取得したユーザは、このレイヤで Kerberos レルム内のネットワーク サービスに対して認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章の「Authenticating to Network Services」を参照してください。

Kerberos を設定する方法

Kerberos 認証済みサーバ/クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

設定については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章にある「Kerberos Configuration Task List」を参照してください。

Kerberos 設定のモニタリング

Kerberos の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

第 52 章

ローカル認証および許可の設定

- 機能情報の確認，1413 ページ
- ローカル認証および許可の設定方法，1413 ページ
- ローカル認証および許可のモニタリング，1416 ページ

機能情報の確認

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

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

ローカル認証および許可の設定方法

スイッチのローカル認証および許可の設定

ローカル モードで AAA を実装するようにスイッチを設定すると、サーバがなくても動作するように AAA を設定できます。 この場合、スイッチは認証および許可の処理を行います。 この設定ではアカウンティング機能は使用できません。

（注） AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。 AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ローカル モードで AAA を実装するようにスイッチを設定して、サーバがなくても動作するように AAA を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa authentication login default local**
5. **aaa authorization exec local**
6. **aaa authorization network local**
7. **username***name* [**privilege***level*] {**password***encryption-typepassword*}
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**aaa authentication login default local** 例： `Switch(config)# aaa authentication login default local`	ローカル ユーザ名データベースを使用するログイン認証を設定します。 **default** キーワードにより、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ 5	**aaa authorization exec local** 例： `Switch(config)# aaa authorization exec local`	ユーザの AAA 許可を設定し、ローカル データベースを確認して、そのユーザに EXEC シェルの実行を許可します。
ステップ 6	**aaa authorization network local** 例： `Switch(config)# aaa authorization network local`	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。
ステップ 7	**username***name* [**privilege***level*] {**password***encryption-typepassword*} 例： `Switch(config)# username your_user_name privilege 1 password 7 secret567`	ローカル データベースを入力し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 • *name* には、ユーザ ID を 1 ワードで指定します。 スペースと引用符は使用できません。 • （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。 指定できる範囲は 0 ～ 15 です。 レベル 15 では特権 EXEC モードでのアクセスが可能です。 レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type* には、暗号化されていないパスワードが後ろに続く場合は 0 を、 暗号化されたパスワードが後ろに続く場合は 7 を指定します。 • *password* には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。 パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、 **username** コマンドの最後のオプションとして指定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

SSH サーバ、統合クライアント、およびサポートされているバージョン，（1419 ページ）
TACACS+ およびスイッチ アクセス，（1351 ページ）
RADIUS およびスイッチ アクセス，（1369 ページ）
SSH を実行するためのSwitchの設定，（1421 ページ）
SSH 設定時の注意事項，（1419 ページ）

ローカル認証および許可のモニタリング

ローカル認証および許可の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

第 53 章

セキュア シェル（SSH）の設定

- 機能情報の確認，1417 ページ
- セキュア シェル（SSH）およびセキュア コピープロトコル（SCP）用にスイッチを設定するための前提条件，1417 ページ
- SSH 用にSwitchを設定するための制約事項，1418 ページ
- SSH に関する情報，1418 ページ
- SSH の設定方法，1421 ページ
- SSH の設定およびステータスのモニタリング，1425 ページ

機能情報の確認

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

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

セキュア シェル（SSH）およびセキュア コピー プロトコル（SCP）用にスイッチを設定するための前提条件

セキュア シェル（SSH）用にスイッチを設定するための前提条件は、次のとおりです。

- SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。 これは SSH が必要なセキュア コピープロトコル（SCP）も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。
- SCP はセキュリティについて SSH に依存します。
- SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。
- ユーザが SCP を使用するには適切な許可が必要です。
- 適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System（IFS）のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには **copy** コマンドを使用します。 また、許可されている管理者もこの作業をワークステーションから実行できます。

関連トピック

Secure Copy Protocol（SCP）, （1421 ページ）

SSH 用にSwitchを設定するための制約事項

セキュア シェル用にSwitchを設定するための制約事項は、次のとおりです。

- スイッチは、Rivest, Shamir, and Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、DES（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアでのみサポートされます。
- Switchは、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES）暗号化アルゴリズムをサポートします。 ただし、キーを暗号化する対称暗号化 AES はサポートされません。
- このソフトウェア リリースは、IP Security（IPSec）をサポートしていません。
- SCP を使用する場合、**copy** コマンドにパスワードを入力することはできません。 プロンプトが表示されたときに、入力する必要があります。

関連トピック

Secure Copy Protocol（SCP）, （1421 ページ）

SSH に関する情報

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセ

キュリティを実現します。 このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

SSH およびスイッチ アクセス

セキュアシェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。 SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。 このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

IPv6 の SSH 機能は IPv4 における機能と同じです。 IPv6 の場合、SSH は IPv6 アドレスをサポートし、IPv6 トランスポート上において、リモート IPv6 ノードとのセキュリティ保護および暗号化された接続を有効化します。

SSH サーバ、統合クライアント、およびサポートされているバージョン

SSH 機能には SSH サーバおよび SSH 統合クライアントがあり、これらはスイッチ上で実行されるアプリケーションです。 SSH クライアントを使用すると、SSH サーバが稼働するスイッチに接続できます。 SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。 また、SSH クライアントは、このリリースでサポートされている SSH サーバおよび他社製の SSH サーバと使用します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは、SSHv1 クライアントをサポートしています。

SSH は、データ暗号規格（DES）暗号化アルゴリズム、Triple DES（3DES）暗号化アルゴリズム、およびパスワードベースの認証をサポートしています。

SSH は次のユーザ認証方式をサポートしています。

- TACACS+
- RADIUS
- ローカル認証および許可

関連トピック

スイッチのローカル認証および許可の設定，（1413 ページ）
TACACS+ およびスイッチ アクセス，（1351 ページ）
RADIUS およびスイッチ アクセス，（1369 ページ）

SSH 設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できます（逆の場合も同様です）。

- スタック マスターで SSH サーバが実行されている場合で、スタック マスターに障害が発生した場合、新しいスタック マスターでは、前のスタック マスターによって生成された RSA キー ペアが使用されます。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力した後、CLI エラー メッセージが表示される場合、RSA キーペアは生成されていません。 ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。 詳細については、次の関連項目を参照してください。
- RSA キーのペアを生成する場合に、メッセージ「No host name specified」が表示されることがあります。 このメッセージが表示された場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。 このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

関連トピック

SSH を実行するためのSwitchの設定, （1421 ページ）
スイッチのローカル認証および許可の設定, （1413 ページ）

セキュア コピー プロトコルの概要

Secure Copy Protocol（SCP）機能は、スイッチの設定やイメージ ファイルのコピーにセキュアな認証方式を提供します。 SCP にはセキュア シェル（SSH）が必要です（Berkeley の r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルです）。

SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。 これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

また、SSH には AAA 認証が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。

（注） SCP を使用する場合、copy コマンドにパスワードを入力することはできません。 プロンプトが表示されたときに、入力する必要があります。

Secure Copy Protocol（SCP）

Secure Copy Protocol（SCP）機能は、スイッチの設定やスイッチ イメージ ファイルのコピーにセキュアな認証方式を提供します。 SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol（RCP）と類似しています。 また、SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、スイッチはユーザが正しい権限レベルを保有しているか確認する必要があります。 Secure Copy 機能を設定するには、SCP の概念を理解する必要があります。

関連トピック

セキュア シェル（SSH）およびセキュア コピー プロトコル（SCP）用にスイッチを設定するための前提条件, （1417 ページ）

SSH 用にSwitchを設定するための制約事項, （1418 ページ）

SSH の設定方法

SSH を実行するためのSwitchの設定

SSH を実行するようにSwitchを設定するには、次の手順を実行します。

はじめる前に

ローカルアクセスまたはリモートアクセス用にユーザ認証を設定します。 この手順は必須です。詳細については、次の関連項目を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **hostname***hostname*
4. **ip domain-name***domain_name*
5. **crypto key generate rsa**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname***hostname* 例： `Switch(config)# hostname your_hostname`	Switchのホスト名および IP ドメイン名を設定します。 （注） この手順を実行するのは、Switchを SSH サーバとして設定する場合だけです。
ステップ 4	**ip domain-name***domain_name* 例： `Switch(config)# ip domain-name your_domain`	Switchのホスト ドメインを設定します。
ステップ 5	**crypto key generate rsa** 例： `Switch(config)# crypto key generate rsa`	Switch上でローカルおよびリモート認証用に SSH サーバをイネーブルにし、RSA キー ペアを生成します。 Switchの RSA キー ペアを生成すると、SSH が自動的にイネーブルになります。 最小モジュラス サイズは、1024 ビットにすることを推奨します。 RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。 モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。 （注） この手順を実行するのは、Switchを SSH サーバとして設定する場合だけです。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

SSH 設定時の注意事項，（1419 ページ）
スイッチのローカル認証および許可の設定，（1413 ページ）

SSH サーバの設定

SSH サーバを設定するには、次の手順を実行します。

（注） Switchを SSH サーバとして設定する場合にのみ、この手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip sshversion** [**1** | **2**]
4. **ip ssh** {**timeout***seconds* | **authentication-retries***number*}
5. 次のいずれかまたは両方を使用します。
   - **line vty***line_number*[*ending_line_number*]
   - **transport input ssh**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sshversion** [**1** | **2**] 例： `Switch(config)# ip ssh version 1`	（任意）SSH バージョン 1 または SSH バージョン 2 を実行するようにSwitchを設定します。 • **1**：SSH バージョン 1 を実行するようにSwitchを設定します。 • **2**：SSH バージョン 2 を実行するようにデバイスを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。 たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。
ステップ 4	**ip ssh** {**timeout***seconds* | **authentication-retries***number*} 例： `Switch(config)# ip ssh timeout 90 authentication-retries 2`	SSH 制御パラメータを設定します。 • タイムアウト値は秒単位で指定します（デフォルト値は 120 秒）。 指定できる範囲は 0 ～ 120 秒です。 このパラメータは、SSH ネゴシエーション フェーズに適用されます。 接続が確立されると、Switchは CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク上の複数の CLI ベース セッション（セッション 0 ～ 4）に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。 実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントをサーバへ再認証できる回数を指定します。 デフォルトは 3 です。指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。

	コマンドまたはアクション	目的

ステップ 5	次のいずれかまたは両方を使用します。
	• **line vty***line_number*[*ending_line_number*]
	• **transport input ssh**
	
	例：
	`Switch(config)# line vty 1 10`
	または
	`Switch(config-line)# transport input ssh`
		（任意）仮想端末回線設定を設定します。
		• ラインコンフィギュレーションモードを開始して、仮想端末回線設定を設定します。 *line_number* および *ending_line_number* には、回線のペアを指定します。 指定できる範囲は 0 ～ 15 です。
		• Switchで非 SSH Telnet 接続を回避するように設定します。 これにより、ルータは SSH 接続に限定されます。

ステップ 6	**end** 例： `Switch(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SSH の設定およびステータスのモニタリング

次の表に、SSH サーバの設定およびステータスを示します。

表 *132* : *SSH* サーバの設定およびステータスを表示するコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

第 54 章

Secure Socket Layer HTTP の設定

- 機能情報の確認，1427 ページ
- Secure Sockets Layer（SSL）HTTP に関する情報，1427 ページ
- セキュア HTTP サーバおよびクライアントの設定方法，1430 ページ
- セキュア HTTP サーバおよびクライアントのステータスのモニタリング，1437 ページ

機能情報の確認

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

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

Secure Sockets Layer（SSL）HTTP に関する情報

セキュア HTTP サーバおよびクライアントの概要

セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。 SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。 シスコが実装するセキュア HTTP サーバおよび HTTP クライアントでは、アプリケーション層の暗号化に SSL バージョン 3.0 を使用します。 HTTP over SSL は、HTTPS と省略されます（セキュアな接続の場合、URL が http://の代わりに https://で始まります）。

（注） SSL は 1999 年に Transport Layer Security（TLS）に発展しましたが、このような特定のコンテキストでまだ使用されています。

セキュア HTTP サーバ（スイッチ）の主な役割は、指定のポート（デフォルトの HTTPS ポートは 443）で HTTPS 要求を待ち受けて、HTTP 1.1 Web サーバへその要求を渡すことです。 HTTP 1.1 サーバはその要求を処理して、セキュア HTTP サーバへ応答（呼び出す）します。セキュア HTTP サーバは HTTP 1.1 サーバの代わりに、元の要求に応えます。

セキュア HTTP クライアント（Web ブラウザ）の主な役割は、Cisco IOS アプリケーション要求に応答して、そのアプリケーションが要求した HTTPS User Agent サービスを実行し、応答を（そのアプリケーションに）返すことです。

認証局のトラストポイント

認証局（CA）は、要求を認可して参加するネットワーク デバイスに証明書を発行します。 これらのサービスは、参加するデバイスに対する中央集中的なセキュリティ キーおよび証明書の管理を提供します。 特定の CA サーバはトラストポイントと呼ばれます。

接続が実行されると、HTTPS サーバは、トラストポイントとなる特定の CA から得た X.509v3 の証明書を発行することで、セキュアな接続をクライアントに提供します。 クライアント（通常、Web ブラウザ）は、その証明書の認証に必要な公開キーを保有しています。

セキュア HTTP 接続には、CA のトラストポイントを設定することを強く推奨します。 HTTPS サーバを実行しているデバイスに CA のトラストポイントが設定されていないと、サーバは自身を認証して必要な RSA のキーのペアを生成します。 自身で認証した（自己署名）証明書は適切なセキュリティではないので、接続するクライアントはその証明書が自己証明書であることを通知し、ユーザに接続の選択（確立または拒否）をさせる必要があります。 この選択肢は内部ネットワーク トポロジ（テスト用など）に役立ちます。

CA のトラストポイントを設定していないと、セキュア HTTP 接続を有効にした場合、そのセキュア HTTP サーバ（またはクライアント）に対する一時的または永続的な自己署名証明書が自動的に生成されます。

- スイッチにホスト名とドメイン名が設定されてない場合、生成される自己署名証明書は一時的なものです。 スイッチを再起動すると、この一時的な自己署名証明書は失われ、新たに自己署名証明書（一時的に）が割り当てられます。
- スイッチにホスト名とドメイン名が設定されている場合、生成される自己署名証明書は永続的なものです。 この証明書は、スイッチを再起動しても、セキュア HTTP サーバを無効にしても有効のままです。そのため、再度セキュア HTTP 接続を有効にしたときに使用できます。

（注） 認証局およびトラストポイントは、個々のデバイスで設定する必要があります。 他のデバイスからコピーすると、それらはスイッチ上で無効になります。

自己署名証明書が生成された場合、その情報は **show running-config** 特権 EXEC コマンドで出力できます。 自己署名証明書を表示するコマンドの出力（show running-config コマンド）を例として一部示します。

```
Switch# show running-config
Building configuration...

<output truncated>

crypto pki trustpoint TP-self-signed-3080755072
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3080755072
 revocation-check none
 rsakeypair TP-self-signed-3080755072
!
!
crypto ca certificate chain TP-self-signed-3080755072
 certificate self-signed 01
  3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109
  02161743 45322D33 3535302D 31332E73 756D6D30 342D3335 3530301E 170D3933
  30333031 30303030 35395A17 0D323030 31303130 30303030 305A3059 312F302D

<output truncated>
```

自己署名証明書は、セキュア HTTP サーバを無効にして、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで削除できます。 その後、セキュア HTTP サーバを再度有効にすると、自己署名証明書が新たに生成されます。

（注） *TP self-signed* の後ろに表示されている値は、デバイスのシリアル番号によって異なります。

オプションのコマンド（**ip http secure-client-auth**）を使用すると、HTTPS サーバがクライアントからの X.509v3 証明書を要求します。 クライアントの認証は、サーバ自身の認証よりも高いセキュリティを提供します。

認証局の詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Configuring Certification Authority Interoperability」の章を参照してください。

CipherSuite

CipherSuite は暗号化アルゴリズムおよびダイジェスト アルゴリズムを指定して、SSL 接続に使用します。 HTTPS サーバに接続すると、クライアントの Web ブラウザは、サポート対象の CipherSuite のリストを提供します。その後クライアントとサーバは、両方でサポートされている暗号化アルゴリズムで最適なものをリストから選択してネゴシエートします。 たとえば、Netscape Communicator 4.76 は、米国のセキュリティ（RSA 公開キー暗号 MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC）をサポートしています。

最適な暗号化には、128 ビット暗号化をサポートするクライアント ブラウザ（Microsoft Internet Explorer バージョン 5.5 以降または Netscape Communicator バージョン 4.76 以降など）が必要です。 SSL_RSA_WITH_DES_CBC_SHA CipherSuite は、128 ビット暗号化を提供しないため、他の CipherSuite よりもセキュリティが低くなります。

CipherSuite は、よりセキュリティが高く、複雑になればなるほど、わずかですが処理時間が必要になります。 次に、スイッチでサポートされる CipherSuite およびルータの処理負荷（速さ）による CipherSuite のランク（速い順）を定義します。

1. SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化に DES-CBC、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換（RSA 公開キー暗号化）
2. SSL_RSA_WITH_RC4_128_MD5：RC4 128 ビット暗号化、およびメッセージ ダイジェストに MD5 を使用した RSA のキー交換
3. SSL_RSA_WITH_RC4_128_SHA：RC4 128 ビット暗号化、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換（RSA 公開キー暗号化）

（暗号化およびダイジェスト アルゴリズムをそれぞれ指定して組み合わせた）RSA は、SSL 接続においてキーの生成および認証の両方に使用されます。 これは、CA のトラストポイントが設定されているかどうかにかかわりません。

SSL のデフォルト設定

標準の HTTP サーバはイネーブルに設定されています。

SSL はイネーブルに設定されています。

CA のトラストポイントは設定されていません。

自己署名証明書は生成されていません。

SSL の設定時の注意事項

SSL をスイッチ クラスタで使用すると、SSL セッションがクラスタ コマンダで終了します。 クラスタ メンバのスイッチは標準の HTTP で動作させる必要があります。

CA のトラストポイントを設定する前に、システム クロックが設定されていることを確認してください。 クロックが設定されていないと、不正な日付により証明書が拒否されます。

スイッチ スタック内のスタック マスターで、SSL セッションが強制終了されます。

セキュア HTTP サーバおよびクライアントの設定方法

CA のトラストポイントの設定

セキュア HTTP 接続には、CA のトラストポイントを正式に設定することを推奨します。 CA のトラストポイントは、自己署名証明書より高いセキュリティがあります。

CA のトラストポイントを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **hostname***hostname*
3. **ip domain-name***domain-name*
4. **crypto key generate rsa**
5. **crypto ca trustpoint***name*
6. **enrollment url***url*
7. **enrollment http-proxy***host-name port-number*
8. **crlquery***url*
9. **primary** *name*
10. **exit**
11. **crypto ca authentication***name*
12. **crypto ca enroll***name*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname***hostname* 例： `Switch(config)# hostname your_hostname`	スイッチのホスト名を指定します（以前ホスト名を設定していない場合のみ必須）。 ホスト名はセキュリティ キーと証明書に必要です。
ステップ 3	**ip domain-name***domain-name* 例： `Switch(config)# ip domain-name your_domain`	スイッチの IP ドメイン名を指定します（以前 IP ドメイン名を設定していない場合のみ必須）。 IP ドメイン名はセキュリティ キーと証明書に必要です。
ステップ 4	**crypto key generate rsa** 例： `Switch(config)# crypto key generate rsa`	（任意）RSA キー ペアを生成します。 RSA キーのペアは、スイッチの証明書を入手する前に必要です。 RSA キーのペアは自動的に生成されます。 必要であれば、このコマンドを使用してキーを再生成できます。

	コマンドまたはアクション	目的
ステップ 5	**crypto ca trustpoint***name* 例： `Switch(config)# crypto ca trustpoint your_trustpoint`	CA のトラストポイントにローカルの設定名を指定して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 6	**enrollment url***url* 例： `Switch(ca-trustpoint)# enrollment url http://your_server:80`	スイッチによる証明書要求の送信先の URL を指定します。
ステップ 7	**enrollment http-proxy***host-name port-number* 例： `Switch(ca-trustpoint)# enrollment http-proxy your_host 49`	（任意）HTTP プロキシ サーバを経由して CA から証明書を入手するようにスイッチを設定します。 • *host-name* には、CA を取得するために使用するプロキシ サーバを指定します。 • *port-number* には、CA にアクセスするために使用するポート番号を指定します。
ステップ 8	**crlquery***url* 例： `Switch(ca-trustpoint)# crl query ldap://your_host:49`	ピアの証明書が取り消されていないかを確認するために、証明書失効リスト（CRL）を要求するようにスイッチを設定します。
ステップ 9	**primary** *name* 例： `Switch(ca-trustpoint)# primary your_trustpoint`	（任意）トラストポイントが CA 要求に対してプライマリ（デフォルト）トラストポイントとして使用されるように指定します。 • *name* には、設定したトラストポイントを指定します。
ステップ 10	**exit** 例： `Switch(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 11	**crypto ca authentication***name* 例： `Switch(config)# crypto ca authentication your_trustpoint`	CA の公開キーを取得して CA を認証します。 ステップ 5 で使用した名前と同じものを使用します。

	コマンドまたはアクション	目的
ステップ 12	**crypto ca enroll***name* 例： `Switch(config)# crypto ca enroll your_trustpoint`	指定した CA トラストポイントから証明書を取得します。このコマンドは、各 RSA キーのペアに対して 1 つの署名入りの証明書を要求します。
ステップ 13	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

セキュア HTTP サーバの設定

セキュア HTTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

はじめる前に

証明に証明書の認証を使用する場合、前の手順を使用してスイッチの CA トラストポイントを設定してから、HTTP サーバを有効にする必要があります。CA のトラストポイントを設定していない場合、セキュア HTTP サーバを最初に有効にした時点で、自己署名証明書が生成されます。サーバを設定した後、標準およびセキュア HTTP サーバ両方に適用するオプション（パス、適用するアクセス リスト、最大接続数、またはタイムアウト ポリシー）を設定できます。

Web ブラウザを使用してセキュア HTTP 接続を確認するには、https://*URL* を入力します（URL は IP アドレス、またはサーバ スイッチのホスト名）。 デフォルト ポート以外のポートを設定している場合、URL の後ろにポート番号も指定する必要があります。 次に例を示します。

```
https://209.165.129:1026
```

または

```
https://host.domain.com:1026
```

手順の概要

1. **show ip http server status**
2. **configure terminal**
3. **ip http secure-server**
4. **ip http secure-port***port-number*
5. **ip http secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}
6. **ip http secure-client-auth**
7. **ip http secure-trustpoint***name*
8. **ip http path***path-name*
9. **ip http access-class***access-list-number*
10. **ip http max-connections***value*
11. **ip http timeout-policyidle***seconds***life***seconds***requests***value*
12. **end**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show ip http server status**
	
	例：
	`Switch# show ip http server status`
		（任意）HTTP サーバのステータスを表示して、セキュア HTTP サーバの機能がソフトウェアでサポートされているかどうかを判断します。 出力で、次のラインのどちらかを確認してください。
		
		`HTTP secure server capability: Present`
		
		または
		
		`HTTP secure server capability: Not present`

ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http secure-server** 例： `Switch(config)# ip http secure-server`	HTTPS サーバがディセーブルの場合、イネーブルにします。 HTTPS サーバは、デフォルトでイネーブルに設定されています。

	コマンドまたはアクション	目的
ステップ 4	**ip http secure-port***port-number* 例： `Switch(config)# ip http secure-port 443`	（任意）HTTPS サーバに使用するポート番号を指定します。 デフォルトのポート番号は 443 です。 443 または 1025 ～ 65535 の範囲で指定できます。
ステップ 5	**ip http secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]} 例： `Switch(config)# ip http secure-ciphersuite rc4-128-md5`	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。 特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。 これはデフォルトです。
ステップ 6	**ip http secure-client-auth** 例： `Switch(config)# ip http secure-client-auth`	（任意）HTTP サーバを設定して、接続処理の間、認証のために、クライアントからの X.509v3 証明書を要求します。 デフォルトでは、クライアントがサーバからの証明書を要求する設定になっていますが、サーバはクライアントを認証しないようになっています。
ステップ 7	**ip http secure-trustpoint***name* 例： `Switch(config)# ip http secure-trustpoint your_trustpoint`	X.509v3 セキュリティ証明書の取得およびクライアントの証明書接続の認証に使用する CA のトラストポイントを指定します。 （注） このコマンドの使用は、前の手順に従って CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。
ステップ 8	**ip http path***path-name* 例： `Switch(config)# ip http path /your_server:80`	（任意）HTML ファイルのベースとなる HTTP パスを設定します。 パスは、ローカル システムにある HTTP サーバ ファイルの場所を指定します（通常、システムのフラッシュ メモリを指定します）。
ステップ 9	**ip http access-class***access-list-number* 例： `Switch(config)# ip http access-class 2`	（任意）HTTP サーバへのアクセスの許可に使用するアクセス リストを指定します。
ステップ 10	**ip http max-connections***value* 例： `Switch(config)# ip http max-connections 4`	（任意）HTTP サーバへの同時最大接続数を指定します。 値は 10 以上にすることを推奨します。 これは、UI が想定どおりに機能するために必要な値です。

	コマンドまたはアクション	目的
ステップ 11	**ip http timeout-policyidle***seconds***life***seconds***requests***value* 例： `Switch(config)# ip http timeout-policy idle 120 life 240 requests 1`	（任意）指定の状況下における、HTTP サーバへの接続最大時間を指定します。 • **idle**：データの受信がないか、応答データが送信できない場合の最大時間。 指定できる範囲は 1 ～ 600 秒です。 デフォルト値は 180 秒（3 分）です。 • **life**：接続を確立している最大時間です。 指定できる範囲は 1 ～ 86400 秒（24 時間）です。 デフォルト値は 180 秒です。 • **requests**：永続的な接続で処理される要求の最大数。 最大値は 86400 です。 デフォルトは 1 です。
ステップ 12	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

セキュア HTTP クライアントの設定

セキュア HTTP クライアントを設定するには、特権 EXEC モードで次の手順を実行します。

はじめる前に

標準の HTTP クライアントおよびセキュア HTTP クライアントは常にイネーブルです。 証明書の認証にはセキュア HTTP クライアントの証明書が必要です。 次の手順では、前の手順で CA のトラストポイントをスイッチに設定していることを前提にしています。 CA のトラストポイントが設定されておらず、リモートの HTTPS サーバがクライアントの認証を要求した場合、セキュア HTTP クライアントへの接続は失敗します。

手順の概要

1. **configureterminal**
2. **ip http client secure-trustpoint***name*
3. **ip http client secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip http client secure-trustpoint***name* 例： `Switch(config)# ip http client secure-trustpoint your_trustpoint`	（任意）リモートの HTTP サーバがクライアント認証を要求した場合に使用する、CA のトラストポイントを指定します。このコマンドの使用は、前の手順を使用して CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。 クライアント認証が必要ない場合、またはプライマリのトラストポイントがすでに設定されている場合は、このコマンドは任意です。
ステップ 3	**ip http client secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]} 例： `Switch(config)# ip http client secure-ciphersuite rc4-128-md5`	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。 特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。 これはデフォルトです。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

セキュア HTTP サーバおよびクライアントのステータスのモニタリング

SSL セキュア サーバおよびクライアントのステータスをモニタするには、次の表の特権 EXEC コマンドを使用します。

表 *133*：*SSL* セキュア サーバおよびクライアントのステータスを表示するコマンド

コマンド	目的
show ip http client secure status	セキュア HTTP クライアントの設定を表示します。

コマンド	目的
show ip http server secure status	セキュア HTTP サーバの設定を表示します。
show running-config	セキュア HTTP 接続に対して生成された自己署名証明書を表示します。

第 55 章

IPv4 ACL の設定

- 機能情報の確認，1439 ページ
- ACL によるネットワーク セキュリティの設定の前提条件，1439 ページ
- ACL によるネットワーク セキュリティの設定の制約事項，1440 ページ
- ACL によるネットワーク セキュリティに関する情報，1441 ページ
- ACL の設定方法，1456 ページ
- IPv4 ACL のモニタリング，1479 ページ
- ACL の設定例，1481 ページ

機能情報の確認

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

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

ACL によるネットワーク セキュリティの設定の前提条件

ここでは、アクセス コントロール リスト（ACL）によるネットワーク セキュリティの設定の前提条件を示します。

- LAN ベース フィーチャ セットを実行しているスイッチでは、VLAN マップはサポートされません。

ACL によるネットワーク セキュリティの設定の制約事項

一般的なネットワーク セキュリティ

次は、ACL によるネットワーク セキュリティの設定の制約事項です。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。 インターフェイスのパケット フィルタおよびルート フィルタ用の ACL では、名前を使用できます。 また、VLAN マップでも名前を指定できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- **appletalk** は、コマンドラインのヘルプ ストリングに表示されますが、**deny** および **permit** MAC アクセス リスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。

IPv4 ACL ネットワーク インターフェイス

次の制限事項が、ネットワーク インターフェイスへの IPv4 ACL に適用されます。

- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2（ポート）ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。
- レイヤ 3 インターフェイスに ACL が適用され、スイッチ上でルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。
- レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。

（注） パケットがレイヤ 3 インターフェイスのアクセス グループによって拒否された場合、デフォルトでは、ルータはICMP到達不能メッセージを送信します。 アクセスグループによって拒否されたこれらのパケットはハードウェアでドロップされず、スイッチの CPU にブリッジングされて、ICMP 到達不能メッセージを生成します。 ポート ACL は ICMP 到達不能メッセージを生成しません。 ICMP 到達不能メッセージは、ルータ ACL で **no ip unreachables** インターフェイス コマンドを使用してディセーブルにできます。

レイヤ 2 インターフェイスの MAC ACL

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。 MAC ACL を適用するときには、次の注意事項に留意してください。

- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。 IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。 すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

（注） **mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用される場合のみ有効です。 このコマンドは、EtherChannel ポート チャネルでは使用できません。

関連トピック

インターフェイスへの IPv4 ACL の適用, （1469 ページ）
IPv4 ACL のインターフェイスに関する注意事項, （1455 ページ）
名前付き MAC 拡張 ACL の作成, （1470 ページ）
レイヤ 2 インターフェイスへの MAC ACL の適用, （1472 ページ）

ACL によるネットワーク セキュリティに関する情報

この章では、アクセス コントロール リスト（ACL）を使用して、スイッチのネットワーク セキュリティを設定する方法について説明します。コマンドや表では、ACL をアクセス リストと呼ぶこともあります。

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。 ACL はルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスまたは VLAN（仮想 LAN）でパケットを許可、または拒否します。 ACL は、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。 パケットがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。 アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。 最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。 スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。 一致する条件がない場合、スイッチはパケットを拒否します。 スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。 スイッチは、VLAN 内でブリッジングされるパケットを含めて、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ 3 スイッチにアクセス リストを設定します。 ACL を設定しなければ、スイッチを通過するすべてのパケットがネッ

トワークのあらゆる部分で許可される可能性があります。 ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラフィックの種類を決定したりできます。 たとえば、電子メール トラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。 ACL を着信トラフィック、発信トラフィック、またはその両方をブロックするように設定することもできます。

アクセス コントロール エントリ

ACL には、アクセス コントロール エントリ（ACE）の順序付けられたリストが含まれています。 各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。 *permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

ACL でサポートされるタイプ

スイッチは、IP ACL とイーサネット（MAC）ACL をサポートしています。

- IP ACL は、TCP、ユーザ データグラム プロトコル（UDP）、インターネット グループ管理プロトコル（IGMP）、およびインターネット制御メッセージ プロトコル（ICMP）などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

このスイッチは、Quality of Service（QoS）分類 ACL もサポートしています。

サポートされる ACL

スイッチでは、トラフィックをフィルタリングするために、次に示す 3 種類の ACL がサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。 レイヤ 2 インターフェイスに適用できるのは IP アクセス リストを 1 つと MAC アドレス リストを 1 つだけです。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御し、レイヤ 3 インターフェイスで特定の方向（着信または発信）に適用されます。
- VLAN ACL または VLAN マップは、すべてのパケット（ブリッジド パケットおよびルーテッド パケット）のアクセスを制御します。 VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。 VLAN マップは、IPv4 のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されています。 イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプロトコルがアクセス コントロールされます。 VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケット（ルーテッド パケットまたはブリッジド パケット）が VLAN マップと照合されます。 パケットは、スイッチ ポートを介して、または、ルーティングされたパケットの場合、ルーテッド ポートを介して、VLAN に入ることができます。

ACL 優先順位

VLAN マップ、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、フィルタの優先順位（最大から最小）はポート ACL、ルータ ACL、次に VLAN マップです。 次の例で、簡単な使用例を説明します。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。 その他のパケットは、VLAN マップによってフィルタリングされます。
- スイッチ仮想インターフェイス（SVI）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。 他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。 他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。 発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。 他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。 他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。 他のパケットには、VLAN マップのフィルタだけが適用されます。
- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。 発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。 他のパケットには、VLAN マップのフィルタだけが適用されます。

関連トピック

ACL によるネットワーク セキュリティの設定の制約事項, （1440 ページ）

ポート ACL

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。 ポート ACL を使用できるのは、物理インターフェイスだけです。EtherChannel インターフェイスでは使用できません。 ポート ACL は、発信および着信インターフェイスに適用できます。 次のアクセス リストがサポートされています。

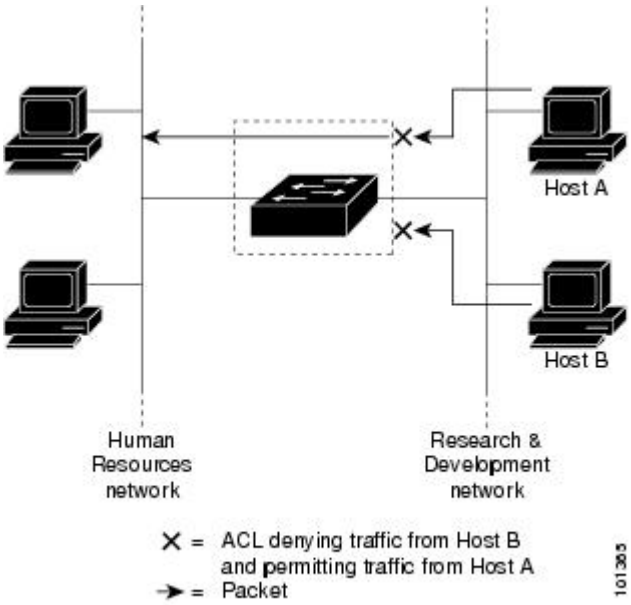
- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト

- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイス上の ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。 このように、ACLがネットワークまたはネットワークの部分へのアクセスを制御します。

次に、すべてのワークステーションが同じVLANにある場合にポートACLを使用してネットワークへのアクセスを制御する例を示します。 レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマン リソース ネットワークにアクセスすることを許可しますが、ホストBが同一のネットワークにアクセスすることは拒否します。 ポート ACL は、着信方向のレイヤ 2 インターフェイスだけに適用できます。

図 *91*：*ACL* によるネットワーク内のトラフィックの制御



ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。 ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。 同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。

（注） レイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。 すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスであるスイッチ仮想インターフェイス（SVI）、物理層 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。 ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。 1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

スイッチは、IPv4 トラフィックの次のアクセス リストをサポートしています。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチはインターフェイスに設定されている機能に関連付けられている ACL が照合されます。 パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。 パケットがルーティングされてからネクスト ホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセス コントロールが行えます。

VLAN マップ

VLAN ACL または VLAN マップを使用して、すべてのトラフィックをアクセス コントロールできます。 VLAN との間でルーティングされる、またはスイッチまたはスイッチ スタックの VLAN 内でブリッジングされるすべてのパケットに、VLAN マップを適用します。

VLAN マップはセキュリティ パケット フィルタリングに使用してください。 VLAN マップで方向（着信または発信）は定義されません。

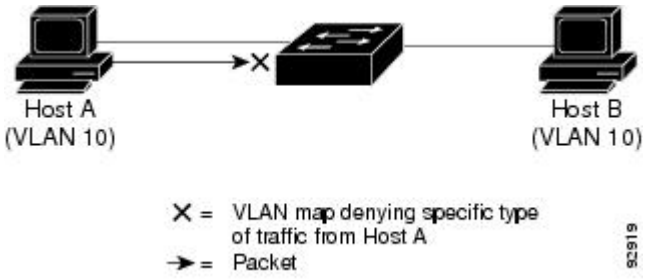
VLAN マップを設定して、IPv4 トラフィックのレイヤ 3 アドレスを照合できます。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます （IP トラフィックは、MAC VACL マップではアクセス制御されません）。 VLAN マップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

次に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。 各 VLAN には、VLAN マップを 1 つだけ適用できます。

図 *92*：*VLAN* マップによるトラフィックの制御



ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック

IP パケットは、ネットワークを通過するときにフラグメント化されることがあります。 その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。 他のフラグメントには、この情報はありません。

アクセス コントロール エントリ（ACE）には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。 レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。 フラグメントにレイヤ 4 情報が含まれておらず、ACE が一部のレイヤ 4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報（TCP や UDP などのプロトコル タイプを含む）をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。
- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

例：ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック

次のコマンドで構成され、フラグメント化された 3 つのパケットに適用されるアクセス リスト 102 を例に取って説明します。

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```

（注） 最初の 2 つの ACE には宛先アドレスの後に *eq* キーワードがありますが、これは既知の TCP 宛先ポート番号がそれぞれシンプル メール転送プロトコル（SMTP）および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。 このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE（permit）と一致します。 残りのフラグメントも最初の ACE と一致します。 これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ 3 情報だけをチェックするからです。 この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです。
- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。 このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて揃っているため、最初のフラグメントが 2 つめの ACE（deny）と一致します。 残りのフラグメントは、レイヤ 4 情報が含まれていないため、2 つめの ACE と一致しません。 残りのフラグメントは 3 つめの ACE（permit）と一致します。

  最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。 ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。
- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。 このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE（deny）と一致します。 ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

標準 IPv4 ACL および拡張 IPv4 ACL

ここでは、IP ACL について説明します。

ACL は、許可条件と拒否条件の順序付けられた集まりです。 スイッチは、アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。 最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。 スイッチは一致する最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。 一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、IPv4 について次の ACL（アクセス リスト）をサポートします。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることもできます。

IPv4 ACL スイッチでサポートされていない機能

このスイッチで IP v4ACL を設定する手順は、他の Cisco スイッチやルータで IP v4ACL を設定する手順と同じです。

このスイッチは、Cisco IOS ルータの ACL に関連する次の機能をサポートしていません。

- 非 IP プロトコル ACL
- IP アカウンティング
- 再帰 ACL およびダイナミック ACL はサポートされていません。
- ポート ACL および VLAN マップに関する ACL ロギング

アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。

次の一覧に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。 このスイッチは、IPv4標準アクセスリストおよび拡張アクセス リスト（1 ～ 199 および 1300 ～ 2699）をサポートします。

表 *134* : アクセス リスト番号

アクセス リスト番号	タイプ	サポートあり
1 ～ 99	IP 標準アクセス リスト	Yes
100 ～ 199	IP 拡張アクセス リスト	Yes
200 ～ 299	プロトコル タイプコード アクセス リスト	No
300 ～ 399	DECnet アクセス リスト	No
400 ～ 499	XNS 標準アクセス リスト	No
500 ～ 599	XNS 拡張アクセス リスト	No
600 ～ 699	AppleTalk アクセス リスト	No
700 ～ 799	48 ビット MAC アドレス アクセス リスト	No
800 ～ 899	IPX 標準アクセス リスト	No
900 ～ 999	IPX 拡張アクセス リスト	No
1000 ～ 1099	IPX SAP アクセス リスト	No

アクセス リスト番号	タイプ	サポートあり
1100 ～ 1199	拡張 48 ビット MAC サマリー アドレス アクセス リスト	No
1200 ～ 1299	IPX サマリー アドレス アクセス リスト	No
1300 ～ 1999	IP 標準アクセス リスト（拡張範囲）	Yes
2000 ～ 2699	IP 拡張アクセス リスト（拡張範囲）	Yes

番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。 標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。 番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

番号付き標準 IPv4 ACL

ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。 標準アクセス リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

スイッチは、**host** 一致条件があるエントリと *don't care* マスク 0.0.0.0 を含む一致条件があるエントリがリストの先頭に移動し、0 以外の *don't care* マスクを含むエントリよりも前に位置するように、標準アクセス リストの順序を書き換えます。 そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号付き標準 IPv4 ACL を VLAN、端末回線、またはインターフェイスに適用できます。

番号付き拡張 IPv4 ACL

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることができます。 番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。 番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

このスイッチは、ダイナミックまたはリフレクシブ アクセス リストをサポートしていません。 また、タイプ オブ サービス（ToS）の minimize-monetary-cost ビットに基づくフィルタリングもサポートしていません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

拡張 TCP、UDP、ICMP、IGMP、またはその他の IP ACL を定義できます。 また、このスイッチはこれらの IP プロトコルをサポートします。

（注） ICMP エコー応答はフィルタリングできません。 他の ICMP コードまたはタイプは、すべてフィルタリングできます。

これらの IP プロトコルがサポートされます。

- 認証ヘッダー プロトコル（**ahp**）
- 暗号ペイロード（**esp**）
- Enhanced Interior Gateway Routing Protocol（**eigrp**）
- 総称ルーティング カプセル化（**gre**）
- インターネット制御メッセージ プロトコル（**icmp**）
- インターネット グループ管理プロトコル（**igmp**）
- すべての内部プロトコル（**ip**）
- IP in IP トンネリング（**ipinip**）
- KA9Q NOS 互換 IP over IP トンネリング（**nos**）
- Open Shortest Path First ルーティング（**ospf**）
- ペイロード圧縮プロトコル（**pcp**）
- プロトコル独立型マルチキャスト（**pim**）
- 伝送制御プロトコル（**tcp**）
- ユーザ データグラム プロトコル（**udp**）

名前付き IPv4 ACL

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング（名前）を使用できます。名前付き ACL を使用すると、ルータ上で番号付きアクセス リストの場合より多くの IPv4 アクセス リストを設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付きアクセス リストで使用できるわけではありません。

（注） 標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。 標準 IP ACL の名前は 1 ～ 99 で、。 番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定するときには、次の注意事項に留意してください。

- また、番号付き ACL も使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。

- VLAN マップには、標準 ACL または拡張 ACL（名前付きまたは番号付き）を使用できます。

ACL ロギング

標準 IP アクセス リストによって許可または拒否されたパケットに関するログ メッセージが、スイッチのソフトウェアによって表示されます。 つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。 コンソールに表示されるメッセージのレベルは、Syslog メッセージを制御するロギング コンソール コマンドで制御されます。

（注） ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可（*permit*）または拒否（*deny*）ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。 ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

ハードウェアおよびソフトウェアによる IP ACL の処理

ACL 処理はハードウェアで実行されます。 ハードウェアで ACL の設定を保存する領域が不足すると、そのインターフェイス上のすべてのパケットがドロップします。

（注） スイッチまたはスタック メンバーのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受けるのは、スイッチに着信した該当 VLAN 内のトラフィックだけです。

ルータ ACL の場合は、次の場合にパケットが CPU に送信されることがあります。

- **log** キーワードを使用する。
- ICMP 到達不能メッセージを生成する。

トラフィック フローのロギングと転送の両方を行う場合、転送はハードウェアで処理されますが、ロギングはソフトウェアで処理する必要があります。 ハードウェアとソフトウェアではパケット処理能力が異なるため、ロギング中であるすべてのフロー（許可フローと拒否フロー）の合計帯域幅が非常に大きい場合は、転送されたパケットの一部をロギングできません。

show ip access-lists 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。 スイッチドパケットおよびルーテッドパケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、 **show platform acl counters hardware** 特権 EXEC コマンドを使用します。

ルータ ACL の機能は、次のとおりです。

- 標準 ACL および拡張 ACL（入力および出力）の許可アクションや拒否アクションをハードウェアで制御し、アクセス コントロールのセキュリティを強化します。
- *ip unreachables* がディセーブルの場合、**log** を指定しないと、セキュリティ ACL の *deny* ステートメントと一致するフローがハードウェアによってドロップされます。 *pemit* ステートメントと一致するフローは、ハードウェアでスイッチングされます。
- ルータ ACL の ACE に **log** キーワードを追加すると、パケットのコピーが CPU に送信され、ロギングだけが行われます。 ACE が *permit* ステートメントの場合も、パケットはハードウェアでスイッチングおよびルーティングされます。

VLAN マップの設定時の注意事項

VLAN マップは、VLAN 内でフィルタリングを制御する唯一の方法です。 VLAN マップには方向の指定がありません。 VLAN マップを使用して、特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。 VLAN マップ内に該当パケット タイプ（IP または MAC）に対する match 句がある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットはドロップされます。 該当パケットタイプに対する match コマンドがない場合、デフォルトでは、パケットが転送されます。

次は、VLAN マップ設定の注意事項です。

- インターフェイスでトラフィックを拒否するように設定された ACL がなく、VLAN マップが設定されていない場合、すべてのトラフィックが許可されます。
- 各 VLAN マップは一連のエントリで構成されます。 VLAN マップのエントリの順序は重要です。 スイッチに着信したパケットは、VLANマップの最初のエントリに対してテストされます。 一致した場合は、VLANマップのその部分に指定されたアクションが実行されます。 一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。
- 該当パケット タイプ（IP または MAC）に対する match 句が VLAN マップに 1 つまたは複数ある場合でも、パケットがそれらの match 句に一致しない場合、デフォルトではパケットがドロップされます。 該当パケット タイプに対する match 句が VLAN マップ内にない場合、デフォルトではパケットが転送されます。
- VLAN マップのロギングはサポートされていません。
- レイヤ 2 インターフェイスに適用された IP アクセス リストまたは MAC アクセス リストがスイッチにあって、ポートが属する VLAN に VLAN マップを適用する場合、ポート ACL が VLAN マップに優先します。
- ハードウェアにVLANマップの設定を適用できない場合は、そのVLAN内のすべてのパケットがドロップします。

VLAN マップとルータ ACL

ブリッジングされたトラフィックおよびルーティングされたトラフィックの両方に対してアクセス コントロールを行うには、VLAN マップを単独で使用するか、またはルータ ACL と VLAN マップを組み合わせて使用します。 入力と出力両方のルーテッド VLAN インターフェイスでルータ ACL を定義したり、ブリッジングされたトラフィックのアクセスをコントロールする VLAN マップを定義したりできます。

パケット フローが ACL 内 VLAN マップの deny ステートメントと一致した場合、ルータ ACL の設定に関係なく、パケット フローは拒否されます。

（注） ルータ ACL を VLAN マップと組み合わせて使用し、ルータ ACL でのロギングを必要とするパケットが VLAN マップで拒否された場合、これらのパケットはロギングされません。

該当パケット タイプ（IP または MAC）に対する match 句が VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトではパケットがドロップされます。 VLAN マップ内に match 句がなく、アクションが指定されていない場合、どの VLAN マップ エントリとも一致しないパケットは転送されます。

VLAN マップとルータ ACL の設定時の注意事項

ここに記載された注意事項は、ルータ ACL および VLAN マップを同じ VLAN 上で使用する必要がある設定に適用されます。 ルータ ACL および VLAN マップを異なる VLAN に割り当てる設定には、これらの注意事項は適用されません。

ルータ ACL および VLAN マップを同じ VLAN に設定する必要がある場合は、ルータ ACL と VLAN マップの両方の設定に関し、ここで説明する注意事項に従ってください。

- VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつに限り設定できます。
- 可能な限り、すべてのエントリのアクションが同一で、末尾のデフォルトアクションだけが反対のタイプとなるように ACL を記述します。 次のいずれかの形式を使用して、ACL を記述します。

  permit... permit... permit... deny ip any any

  または

  deny... deny... deny... permit ip any any
- ACL 内で複数のアクション（許可、拒否）を定義する場合は、それぞれのアクション タイプをまとめて、エントリ数を削減します。
- ACL 内にレイヤ 4 情報を指定しないでください。 レイヤ 4 情報を追加すると、統合プロセスが複雑になります。 ACL のフィルタリングが、full-flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）でなく、IP アドレス（送信元および宛先）に基づいて行われる場合に、最適な統合結果が得られます。 可能な限り、IP アドレスには *don't care* ビットを使用してください。

IP ACE とレイヤ 4 情報を含む TCP/UDP/ICMP ACE が両方とも ACL 内に存在し、full-flow モードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。 この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

VACL ロギング

VACL ロギングを設定する場合は、次の状況で拒否された IP パケットに対して Syslog メッセージが生成されます。

- 一致する最初のパケットを受信した場合
- 最後の 5 分間に一致するパケットを受信した場合
- 5 分経過する前にしきい値に達している場合

ログ メッセージはフロー単位で生成されます。 フローは、同じ IP アドレスおよびレイヤ 4（UDP または TCP）ポート番号を持つパケットとして定義されます。 フローで 5 分間パケットを受信しない場合、そのフローはキャッシュから削除されます。 Syslog メッセージが生成されると、タイマーおよびパケット カウンタがリセットされます。

VACL ロギングの制限事項は次のとおりです。

- 拒否された IP パケットだけが記録されます。
- 発信ポート ACL でロギングが必要なパケットは、VACL で拒否された場合、ロギングされません。

ACL の時間範囲

time-range グローバル コンフィギュレーション コマンドを使用することによって、時刻および曜日に基づいて拡張 ACL を選択的に適用できます。 まず、時間範囲の名前を定義し、その時間範囲内の時刻および日付または曜日を設定します。 次に、ACL を適用してアクセス リストに制限を設定するときに時間範囲を入力します。 時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間（指定期間内や指定曜日など）を定義できます。 **time-range** キーワードおよび引数については、名前付きおよび番号付き拡張ACLタスクの表を参照してください。

時間範囲を使用するいくつかの利点を次に示します。

- アプリケーションなどのリソース（IPアドレスとマスクのペア、およびポート番号で識別）へのユーザ アクセスをより厳密に許可または拒否できます。
- ログ メッセージを制御できます。 ACL エントリを使用して特定の時刻に関してのみトラフィックをロギングできるため、 ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセス リストを使用すると、CPU に負荷が生じます。これは、アクセス リストの新規設定を他の機能や、ハードウェア メモリにロードされた結合済みの設定とマージする必要が

あるためです。そのため、複数のアクセスリストが短期間に連続して（互いに数分以内に）有効となるような設定とならないように注意する必要があります。

（注） 時間範囲は、スイッチのシステム クロックに基づきます。したがって、信頼できるクロックソースが必要です。ネットワーク タイム プロトコル（NTP）を使用してスイッチ クロックを同期させることを推奨します。

関連トピック

ACL の時間範囲の設定, （1465 ページ）

IPv4 ACL のインターフェイスに関する注意事項

ip access-group インターフェイス コンフィギュレーション コマンドをレイヤ 3 インターフェイス（SVI、レイヤ 3 EtherChannel、またはルーテッド ポート）に適用するには、そのインターフェイスに IP アドレスが設定されている必要があります。レイヤ 3 アクセス グループは、CPU のレイヤ 3 プロセスによってルーティングまたは受信されるパケットをフィルタリングします。このグループは、VLAN 内でブリッジングされるパケットに影響を与えません。

着信 ACL の場合、パケットの受信後スイッチはパケットを ACL と照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

発信 ACL の場合、パケットを受信し制御対象インターフェイスにルーティングしたあと、スイッチはパケットを ACL と照合します。ACL がパケットを許可した場合は、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスの ACL または発信インターフェイスの ACL のいずれであっても、常に入力インターフェイスから ICMP 到達不能メッセージが送信されます。ICMP 到達不能メッセージは通常、入力インターフェイス 1 つにつき、0.5 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

関連トピック

インターフェイスへの IPv4 ACL の適用, （1469 ページ）
ACL によるネットワーク セキュリティの設定の制約事項, （1440 ページ）

ACL の設定方法

IPv4 ACL の設定

このスイッチで IP ACL を使用する手順は次のとおりです。

手順の概要

1. アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。
2. その ACL をインターフェイスまたは端末回線に適用します。 標準および拡張 IP ACL を VLAN マップに適用することもできます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。	
ステップ 2	その ACL をインターフェイスまたは端末回線に適用します。 標準および拡張 IP ACL を VLAN マップに適用することもできます。	

番号付き標準 ACL の作成

番号付き標準 ACL を作成するには、次の手順に従ってください。

手順の概要

1. **enable**
2. **configureterminal**
3. **access-list***access-list-number* {**deny** | **permit**} *source source-wildcard*[**log**]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list***access-list-number* {**deny** | **permit**} *source source-wildcard*[**log**] 例： `Switch(config)# access-list 2 deny your_host`	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。 *access-list-number* には、1 ～ 99 または 1300 ～ 1999 の 10 進数値を指定します。 条件が一致した場合にアクセスを拒否する場合は **deny**、許可する場合は **permit** を指定します。 *source* には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • キーワード **any** は 0.0.0.0 255.255.255.255 という *source* および *source-wildcard* の省略形です。 source-wildcard を入力する必要はありません。 • キーワード **host** は送信元および *source* 0.0.0.0 の *source-wildcard* の省略形です。 （任意）*source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 （任意）**log** を入力すると、エントリと一致するパケットの詳細を示すロギング メッセージがコンソールに送信されます。 （注） ロギングは、レイヤ 3 インターフェイスに割り当てられた ACL でだけサポートされます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN マップの設定, （1474 ページ）

番号付き拡張 ACL の作成

番号付き拡張 ACL を作成するには、次の手順に従ってください。

手順の概要

1. **configureterminal**
2. **access-list***access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence***precedence*] [**tos** tos] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*]
3. **access-list***access-list-number* {**deny** | **permit**} **tcp***sourcesource-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**established**] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*] [*flag*]
4. **access-list***access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*]
5. **access-list***access-list-number* {**deny** | **permit**} **icmp***sourcesource-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**time-range***time-range-name*] [**dscp***dscp*]
6. **access-list***access-list-number* {**deny** | **permit**} **igmp***sourcesource-wildcard destination destination-wildcard* [*igmp-type*] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list***access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence***precedence*] [**tos** tos] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*] 例： `Switch(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log`	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 *access-list-number* には、100 ～ 199 または 2000 ～ 2699 の 10 進数を指定します。 条件が一致した場合にパケットを拒否する場合は **deny**、許可する場合は **permit** を指定します。 *protocol* には、IP プロトコルの名前または番号を指定します。**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、または **udp**、あるいは IP プロトコル番号を表す 0～255 の範囲の整数を使用できます。一致条件としてインターネットプロトコル（ICMP、TCP、UDP など）を指定するには、キーワード **ip** を使用します。 （注） この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加の特定パラメータについては、次のステップを参照してください。 *source* には、パラメータの送信元であるネットワークまたはホストの番号を指定します。 *source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 *destination* には、パラメータの宛先であるネットワークまたはホストの番号を指定します。 *destination-wildcard* は、ワイルドカード ビットを宛先アドレスに適用します。 source、source-wildcard、destination、および destination-wildcard の値は、次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード **any**。 • 単一のホスト 0.0.0.0 を表すキーワード **host**。 その他のキーワードはオプションであり、次の意味を持ちます。 • **precedence**：パケットを 0 ～ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、**routine**（0）、

	コマンドまたはアクション	目的
		priority（1）、**immediate**（2）、**flash**（3）、**flash-override**（4）、**critical**（5）、**internet**（6）、**network**（7）です。 • **fragments**：2 つ目以降のフラグメントをチェックする場合に入力します。 • **tos**：パケットを 0 ～ 15 の番号または名前で指定するサービス タイプ レベルと一致させる場合に入力します。指定できる値は、**normal**（0）、**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）です。 • **log**：エントリと一致するパケットに関するログ通知メッセージを作成し、コンソールに送信します。**log-input** を指定すると、ログ エントリに入力インターフェイスが追加されます。 • **time-range**：時間範囲名を指定します。 • **dscp**：0 ～ 63 の番号で指定された DSCP 値を使用してパケットを照合します。疑問符（?）を使用すると、使用可能な値のリストが表示されます。 （注） **dscp** 値を入力した場合、**tos** または **precedence** は入力できません。 **dscp** を入力しない場合は、**tos** と **precedence** 値の両方を入力できます。
ステップ 3	**access-list***access-list-number* {**deny** | **permit**} **tcp***sourcesource-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**established**] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*] [*flag*] 例： `Switch(config)# access-list 101 permit tcp any any eq 500`	拡張 TCP アクセス リストおよびアクセス条件を定義します。 次に示す例外を除き、拡張 IPv4 ACL に対して説明するパラメータと同じパラメータを使用します。 （任意）*operator* および *port* を入力すると、送信元ポート（*source source-wildcard* の後に入力した場合）または宛先ポート（*destination destination-wildcard* の後に入力した場合）が比較されます。 使用可能な演算子は、**eq**（等しい）、**gt**（より大きい）、**lt**（より小さい）、**neq**（等しくない）、**range**（包含範囲）などです。 演算子にはポート番号を指定する必要があります（range の場合は 2 つのポート番号をスペースで区切って指定する必要があります）。 *port* には、10 進数（0 ～ 65535）のポート番号または TCP ポート名を入力します。 TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。 他のオプションのキーワードの意味は次のとおりです。 • **established**：確立された接続と照合する場合に入力します。 このキーワードは、**ack** または **rst** フラグでの照合と同じ機能を果たします。

	コマンドまたはアクション	目的
		• *flag*：指定された TCP ヘッダー ビットを基準にして照合します。入力できるフラグは、**ack**（確認応答）、**fin**（終了）、**psh**（プッシュ）、**rst**（リセット）、**syn**（同期）、または**urg**（緊急）です。
ステップ 4	**access-list***access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*] 例： `Switch(config)# access-list 101 permit udp any any eq 100`	（任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。 UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[operator [port]] ポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP では、**flag** および **established** キーワードは無効です。
ステップ 5	**access-list***access-list-number* {**deny** | **permit**} **icmp***sourcesource-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**time-range***time-range-name*] [**dscp***dscp*] 例： `Switch(config)# access-list 101 permit icmp any any 200`	拡張 ICMP アクセス リストおよびアクセス条件を定義します。 ICMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。 オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-code*：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。
ステップ 6	**access-list***access-list-number* {**deny** | **permit**} **igmp***sourcesource-wildcard destination destination-wildcard* [*igmp-type*] [**precedence***precedence*] [**tos***tos*] [**fragments**] [**log** [**log-input**] [**time-range***time-range-name*] [**dscp***dscp*] 例： `Switch(config)# access-list 101`	（任意）拡張IGMPアクセス リストおよびアクセス条件を定義します。 IGMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。 *igmp-type*：IGMP メッセージ タイプと照合するには、0 ～ 15 の番号を入力するか、またはメッセージ名である **dvmrp**、**host-query**、**host-report**、**pim**、または **trace** を入力します。

	コマンドまたはアクション	目的
	permit igmp any any 14	
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

VLAN マップの設定, （1474 ページ）

名前付き標準 ACL の作成

名前を使用して標準 ACL を作成するには、次の手順に従ってください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip access-list standard***name*
4. 次のいずれかを使用します。
   - **deny** {*source* [*source-wildcard*] | **host***source* | **any**} [**log**]
   - **permit** {*source* [*source-wildcard*] | **host***source* | **any**} [**log**]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list standard***name* 例： `Switch(config)# ip access-list standard 20`	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、1 ～ 99 の番号を使用できます。

ステップ 4	次のいずれかを使用します。
	• **deny** {*source* [*source-wildcard*] | **host***source* | **any**} [**log**]
	• **permit** {*source* [*source-wildcard*] | **host***source* | **any**} [**log**]
	
	例：
	`Switch(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255`
	または
	`Switch(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0`
		アクセス リスト コンフィギュレーション モードで、パケットを転送するのかドロップするのかを決定する 1 つ以上の拒否条件または許可条件を 指定します。
		• **host***source*：*source* 0.0.0.0.0.0.0.0 の送信元および送信元ワイルドカード。
		• **any**：source および source wildcard の値 0.0.0.0 255.255.255.255。

ステップ 5	**end** 例： `Switch(config-std-nacl)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

名前付き拡張 ACL の作成

名前を使用して拡張 ACL を作成するには、次の手順に従ってください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip access-list extended***name*
4. {**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host***source* | **any**} {*destination* [*destination-wildcard*] | host *destination* | **any**} [**precedence***precedence*] [**tos***tos*] [**established**] [**log**] [**time-range***time-range-name*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list extended***name* 例： `Switch(config)# ip access-list extended 150`	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、100 ～ 199 の番号を使用できます。
ステップ 4	{**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host***source* | **any**} {*destination* [*destination-wildcard*] | host *destination* | **any**} [**precedence***precedence*] [**tos***tos*] [**established**] [**log**] [**time-range***time-range-name*]	アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。 **log** キーワードを使用して、違反を含む、アクセス リスト ロギング メッセージを取得します。 • **host***source*：*source* 0.0.0.0.0.0.0.0 の送信元および送信元ワイルドカード。

	コマンドまたはアクション	目的
	例： `Switch(config-ext-nacl)# permit 0 any any`	• **host***destintation*：*destination* 0.0.0.0 の宛先および宛先ワイルドカード • **any**：source および source wildcard の値または destination および destination wildcard の値である 0.0.0.0 255.255.255.255
ステップ 5	**end** 例： `Switch(config-ext-nacl)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。 標準 ACL では、関連付けられた IP ホスト アドレス アクセス リストの指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。 ACL エントリを特定の ACL に選択的に追加できません。 ただし、**no permit** および **no deny** アクセス リスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

次の作業

作成した名前付き ACL は、インターフェイスまたは VLAN に適用できます。

ACL の時間範囲の設定

ACL の時間範囲パラメータを設定するには、次の手順に従ってください。

手順の概要

1. **enable**
2. **configureterminal**
3. **time-range***time-range-name*
4. 次のいずれかを使用します。
   - **absolute** [**start***time date*] [**end***time date*]
   - **periodic***day-of-the-week hh:mmto* [*day-of-the-week*] *hh:mm*
   - **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch(config)# enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**time-range***time-range-name* 例： `Switch(config)# time-range workhours`	作成する時間範囲には意味のある名前（*workhours* など）を割り当て、時間範囲コンフィギュレーション モードを開始します。 名前にスペースや疑問符を含めることはできません。また、文字から始める必要があります。
ステップ 4	次のいずれかを使用します。 • **absolute** [**start***time date*] [**end***time date*] • **periodic***day-of-the-week hh:mmto* [*day-of-the-week*] *hh:mm* • **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*	適用対象の機能がいつ動作可能になるかを指定します。 • 時間範囲には、**absolute** ステートメントを 1 つだけ使用できます。 複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。 • 複数の **periodic** ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。

	コマンドまたはアクション	目的

	例：
	`Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006`
	または
	`Switch(config-time-range)# periodic weekdays 8:00 to 12:00`
		設定例を参照してください。

ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

複数の項目をそれぞれ異なる時間に有効にする場合は、上記の手順を繰り返してください。

関連トピック

ACL の時間範囲, （1454 ページ）

端末回線への IPv4 ACL の適用

番号付き ACL を使用して、1 つまたは複数の端末回線へのアクセスを制御できます。 端末回線には名前付き ACL を適用できません。 すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

仮想端末回線と ACL に指定されたアドレス間の着信接続および発信接続を制限するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **line** [**console** | **vty**] *line-number*
4. **access-class***access-list-number* {**in** | **out**}
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch(config)# enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** [**console** | **vty**] *line-number* 例： `Switch(config)# line console 0`	設定する回線を指定し、インライン コンフィギュレーション モードを開始します。 • **console**：コンソール端末回線を指定します。 コンソール ポートは DCE です。 • **vty**：リモート コンソール アクセス用の仮想端末を指定します。 *line-number* は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。 指定できる範囲は 0 ～ 16です。
ステップ 4	**access-class***access-list-number* {**in** | **out**} 例： `Switch(config-line)# access-class 10 in`	（デバイスへの）特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信接続および発信接続を制限します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

インターフェイスへの IPv4 ACL の適用

ここでは、IPv4 ACL をネットワーク インターフェイスへ適用する方法について説明します。

インターフェイスへのアクセスを制御する管理には、特権EXECモードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **ip access-group** {*access-list-number* | *name*} {**in** | **out**}
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスには、レイヤ 2 インターフェイス（ポート ACL）またはレイヤ3インターフェイス（ルータ ACL）を指定できます。
ステップ 3	**ip access-group** {*access-list-number* | *name*} {**in** | **out**} 例： `Switch(config-if)# ip access-group 2 in`	指定されたインターフェイスへのアクセスを制御します。 **out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv4 ACL のインターフェイスに関する注意事項, （1455 ページ）

ACL によるネットワーク セキュリティの設定の制約事項, （1440 ページ）

名前付き MAC 拡張 ACL の作成

VLAN またはレイヤ 2 インターフェイスで非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。 その手順は、他の名前付き拡張 ACL を設定する場合と同様です。

名前付き MAC 拡張 ACL を作成するには、次の手順に従ってください。

手順の概要

1. **enable**
2. **configureterminal**
3. **mac access-list extended***name*
4. {**deny** | **permit**} {**any** | **host***source MAC address* | *source MAC address mask*} {**any** | **host***destination MAC address* | *destination MAC address mask*} [*type mask* | **lsap***lsap mask* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp** | 0-*65535*] [**cos***cos*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mac access-list extended***name* 例： `Switch(config)# mac access-list extended mac1`	名前を使用して MAC 拡張アクセス リストを定義します。
ステップ 4	{**deny** | **permit**} {**any** | **host***source MAC address* | *source MAC address mask*} {**any** | **host***destination MAC address* | *destination MAC address mask*} [*type mask* | **lsap***lsap mask* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp** | 0-*65535*] [**cos***cos*]	拡張 MAC アクセス リスト コンフィギュレーション モードでは、すべての（**any**）送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定のホスト（**host**）送信元 MAC アドレス、およびすべての（any）宛先 MAC アドレス、マスク付き宛先MACアドレス、または特定の宛先MAC アドレスに、**permit** または **deny** を指定します。 （任意）次のオプションを入力することもできます。 • *type mask*：Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号。10 進数、16 進数、

	コマンドまたはアクション	目的

	例：
	`Switch(config-ext-macl)# deny any any decnet-iv`
	または
	`Switch(config-ext-macl)# permit any any`
		または 8 進数で表記できます。一致検査の前に、任意で指定できる *don't care* ビットのマスクが EtherType に適用されます。
		• **lsap***lsap mask*：IEEE 802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。任意で *don't care* ビットのマスクを指定できます。
		• **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**—A non-IP protocol.
		• **cos***cos*：プライオリティを設定する 0 ～ 7 の IEEE 802.1Q CoS 番号。

ステップ 5	**end** 例： `Switch(config-ext-macl)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ACL によるネットワーク セキュリティの設定の制約事項, （1440 ページ）

VLAN マップの設定, （1474 ページ）

レイヤ 2 インターフェイスへの MAC ACL の適用

レイヤ2インターフェイスへのアクセスを制御するためにMACアクセス リストを適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **mac access-group** {*name*} {**in** | **out** }
5. **end**
6. **show mac access-group** [**interface***interface-id*]
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定するインターフェイスは物理レイヤ 2 インターフェイス（ポート ACL）でなければなりません。
ステップ 4	**mac access-group** {*name*} {**in** | **out** } 例： `Switch(config-if)# mac access-group mac1 in`	MAC アクセス リストを使用して、指定されたインターフェイスへのアクセスを制御します。 ポート ACL は発信および着信方向サポートされます。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show mac access-group** [**interface***interface-id*] 例： `Switch# show mac access-group interface gigabitethernet1/0/2`	そのインターフェイスまたはすべてのレイヤ2インターフェイスに適用されている MAC アクセス リストを表示します。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチは、パケットを受信すると、着信 ACL とパケットを照合します。 ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。 ACLがパケットを拒否する場合、スイッチはパケットを廃棄します。 未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。 ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

関連トピック

ACL によるネットワーク セキュリティの設定の制約事項, （1440 ページ）

VLAN マップの設定

VLANマップを作成して、1つまたは複数のVLANに適用するには、次のステップを実行します。

はじめる前に

VLAN に適用する標準 IPv4 ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。

手順の概要

1. **vlan access-map** *name* [**number**]
2. **match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*]
3. IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1 つ以上の ACL（標準または拡張）とそのパケットを照合するには、次のコマンドのいずれかを入力します。
   - **action** { **forward**}

     ```
     Switch(config-access-map)# action forward
     ```

   - **action** { **drop**}

     ```
     Switch(config-access-map)# action drop
     ```

4. **vlan filter** *mapname* **vlan-list** *list*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vlan access-map** *name* [**number**] 例： `Switch(config)# vlan access-map map_1 20`	VLAN マップを作成し、名前と、任意で番号を付けます。 番号は、マップ内のエントリのシーケンス番号です。 同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。 マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。 VLAN マップでは、特定の permit または deny キーワードを使用しません。 VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。 ACL 内の permit は、一致するという意味です。 ACL 内の deny は、一致しないという意味です。 このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。
ステップ 2	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*] 例： `Switch(config-access-map)# match ip address ip2`	1 つまたは複数の標準または拡張アクセス リストに対してパケットを照合します（IP または MAC アドレスを使用）。 パケットの照合は、対応するプロトコルタイプのアクセス リストに対してだけ行われます。 IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。 非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ照合されます。

	コマンドまたはアクション	目的
		（注） パケット タイプ（IP または MAC）に対する match 句が VLAN マップに設定されている場合で、そのマップ アクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。 match 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。

ステップ 3	IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1 つ以上の ACL（標準または拡張）とそのパケットを照合するには、次のコマンドのいずれかを入力します。
	• **action** { **forward**}
	`Switch(config-access-map)# action forward`
	• **action** { **drop**}
	`Switch(config-access-map)# action drop`
		マップ エントリに対するアクションを設定します。

ステップ 4	**vlan filter** *mapname* **vlan-list** *list* 例： `Switch(config)# vlan filter map 1 vlan-list 20-22`	VLAN マップを 1 つまたは複数の VLAN に適用します。 list には単一の VLAN ID（22）、連続した範囲（10 ～ 22）、または VLAN ID のストリング（12、22、30）を指定できます。 カンマやハイフンの前後にスペースを挿入することもできます。

関連トピック

番号付き標準 ACL の作成, （1456 ページ）
番号付き拡張 ACL の作成, （1458 ページ）
名前付き MAC 拡張 ACL の作成, （1470 ページ）
VLAN マップの作成, （1477 ページ）
VLAN への VLAN マップの適用, （1478 ページ）

VLAN マップの作成

各 VLAN マップは順番に並べられた一連のエントリで構成されます。 VLAN マップ エントリを作成、追加、または削除するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **vlan access-map** *name* [**number**]
3. **match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*]
4. **action** {**drop** | **forward**}
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan access-map** *name* [**number**] 例： `Switch(config)# vlan access-map map_1 20`	VLAN マップを作成し、名前と、任意で番号を付けます。 番号は、マップ内のエントリのシーケンス番号です。 同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。 マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。 VLAN マップでは、特定の permit または deny キーワードを使用しません。 VLANマップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。 ACL 内の permit は、一致するという意味です。 ACL 内の deny は、一致しないという意味です。 このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。
ステップ 3	**match** {**ip**	**mac**} **address** {*name*	*number*} [*name*	*number*] 例： `Switch(config-access-map)# match`	1 つまたは複数の標準または拡張アクセス リストに対してパケットを照合します（IP または MAC アドレスを使用）。 パケットの照合は、対応するプロトコルタイプのアクセスリストに対してだけ行われます。 IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。 非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ照合されます。

	コマンドまたはアクション	目的
	`ip address ip2`	
ステップ 4	**action {drop | forward}** 例： `Switch(config-access-map)# action forward`	（任意）マップ エントリに対するアクションを設定します。 デフォルトは転送（forward）です。
ステップ 5	**end** 例： `Switch(config-access-map)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	アクセス リストの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN マップの設定, （1474 ページ）

VLAN への VLAN マップの適用

1 つの VLAN マップを 1 つまたは複数の VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **vlan filter** *mapname* **vlan-list** *list*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan filter** *mapname* **vlan-list** *list* 例： `Switch(config)# vlan filter map 1 vlan-list 20-22`	VLAN マップを 1 つまたは複数の VLAN に適用します。 list には単一の VLAN ID（22）、連続した範囲（10 ～ 22）、または VLAN ID のストリング（12、22、30）を指定できます。 カンマやハイフンの前後にスペースを挿入することもできます。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** 例： `Switch# show running-config`	アクセス リストの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN マップの設定，（1474 ページ）

IPv4 ACL のモニタリング

スイッチに設定されている ACL、およびインターフェイスと VLAN に適用された ACL を表示して IPv4 ACL をモニタできます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 またはレイヤ 3 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセス グループを表示できます。 また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、次の表に記載された特権 EXEC コマンドを使用します。

表 *135* : アクセス リストおよびアクセス グループを表示するコマンド

コマンド	目的
show access-lists [*number* | *name*]	最新の IP および MAC アドレス アクセス リストの全体やその一部、または特定のアクセス リスト（番号付きまたは名前付き）の内容を表示します。
show ip access-lists [*number* | *name*]	最新の IP アクセス リスト全体、または特定の IP アクセス リスト（番号付きまたは名前付き）を表示します。
show ip interface*interface-id*	インターフェイスの詳細設定およびステータスを表示します。 IP がイネーブルになっているインターフェイスに、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示されます。
show running-config [**interface***interface-id*]	スイッチまたは指定されたインターフェイスのコンフィギュレーション ファイルの内容（設定されたすべての MAC および IP アクセス リストや、どのアクセス グループがインターフェイスに適用されたかなど）を表示します。
show mac access-group [**interface***interface-id*]	すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リスト を表示します。

また、VLAN アクセス マップまたは VLAN フィルタに関する情報を表示して、VLAN マップをモニタできます。 VLAN マップ情報を表示するには、次の表に記載された特権 EXEC コマンドを使用します。

表 *136* : *VLAN* マップ情報を表示するコマンド

コマンド	目的
show vlan access-map [*mapname*]	すべての VLAN アクセスマップまたは指定されたアクセスマップに関する情報を表示します。

コマンド	目的
show vlan filter [**access-map***name* | **vlan***vlan-id*]	VLAN フィルタすべてに関する情報、または特定の VLAN または VLAN アクセス マップに関する情報を表示します。

ACL の設定例

例：ACL での時間範囲を使用

次の例に、*workhours*（営業時間）の時間範囲および会社の休日（2006 年 1 月 1 日）を設定し、設定を確認する例を示します。

```
Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張ACL内に時間範囲名を入力します。次に、拡張アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての TCP トラフィックを許可します。

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
   10 deny tcp any any time-range new_year_day_2006 (inactive)
   20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list lpip_default
    10 permit ip any any
Extended IP access list deny_access
    10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
    10 permit tcp any any time-range workhours (inactive)
```

例：ACL へのコメントの挿入

remark キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント（注釈）を追加できます。 コメントを使用すると、ACL の理解とスキャンが容易になります。 1 つのコメント行の最大長は 100 文字です。

コメントは、permit ステートメントまたは deny ステートメントの前後どちらにでも配置できます。 コメントがどの permit ステートメントまたは deny ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。 たとえば、あるコメントは対応する permit または deny ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list** *access-list number* **remark** *remark* グローバル コンフィギュレーション コマンドを使用します。 コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith through
Switch(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリには、**remark** アクセス リスト コンフィギュレーション コマンドを使用します。 コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

IPv4 ACL の設定例

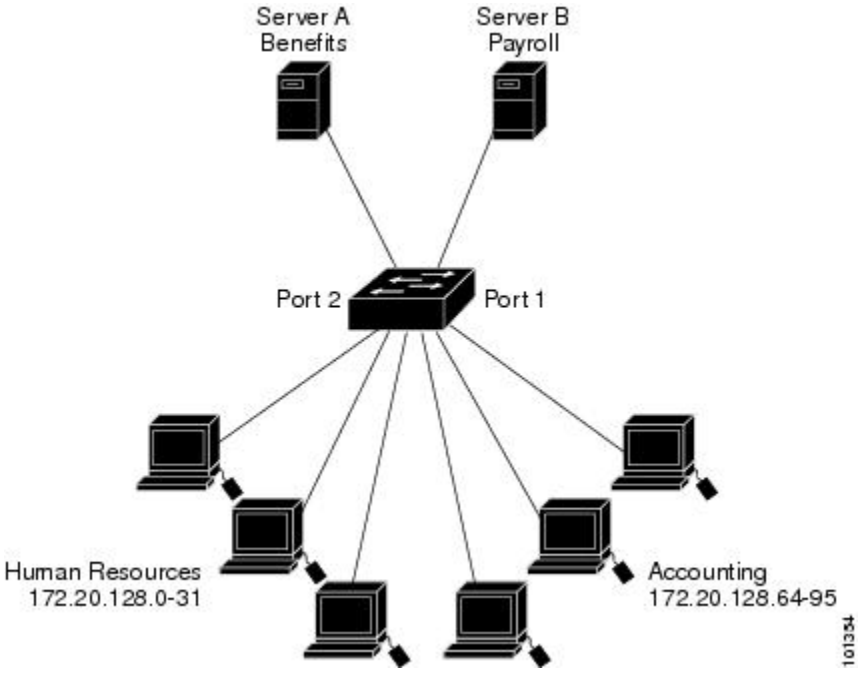
ここでは、IPv4 ACL を設定および適用する例を示します。 ACL のコンパイルに関する詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』および『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Adderssing and Services」の章にある「Configuring IP Services」の項を参照してください。

小規模ネットワークが構築されたオフィス用の ACL

次に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッド ポート 2 に接続されたサーバ A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。

サーバ A にはすべてのユーザがアクセスできますが、サーバ B にアクセスできるユーザは制限されています。

図 *93*：ルータ *ACL* によるトラフィックの制御



ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準ACLを作成し、ポート1からサーバに着信するトラフィックをフィルタリングします。
- 拡張ACLを作成し、サーバからポート1に着信するトラフィックをフィルタリングします。

例：小規模ネットワークが構築されたオフィスの ACL

次に、標準ACLを使用してポートからサーバBに着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ～ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。 この ACL は、指定された送信元アドレスを持つルーテッド ポート 1 から送信されるトラフィックに適用されます。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# how access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 6 out
```

次に、拡張ACLを使用してサーバBからポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバB）から経理部の宛先アドレス 172.20.128.64 ～ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。 この ACL は、ルーテッド ポート 1 に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可し

ます。 拡張ACLを使用する場合は、送信元および宛先情報の前に、プロトコル（IP）を入力する必要があります。

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 106 in
```

例：番号付き ACL

次の例のネットワーク 36.0.0.0 は、2 番めのオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネット マスクは 255.255.0.0 です。 ネットワーク アドレス 36.0.0.0 の 3 番めおよび 4 番めのオクテットは、特定のホストを指定します。 アクセス リスト 2 を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。 このアクセス リストの最終行は、ネットワーク 36.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。 この ACL は、ポートに着信するパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip access-group 2 in
```

例：拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。 2 番めの行は、ホスト 128.88.1.2 の SMTP ポートへの着信 TCP 接続を許可します。 3 番めの行は、エラーフィードバック用の着信 ICMP メッセージを許可します。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。 ただし、IP ホストからは、専用メール ホストのメール（SMTP）ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。 接続している間は、同じポート番号が使用されます。インターネットから着信するメールパケットの宛先ポートは 25 です。 発信パケットのポート番号は予約されています。安全なネットワークのシステムでは常にポート 25 でのメール接続が使用されているため、着信サービスと発信サービスを個別に制御できます。 ACL は発信インターフェイスの入力 ACL および着信インターフェイスの出力 ACL として設定される必要があります。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
```

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 102 in
```

次の例では、ネットワークはアドレスが 128.88.0.0 のクラス B ネットワークで、メール ホストのアドレスは 128.88.1.2 です。 **established** キーワードは、確立された接続を表示する TCP 専用のキーワードです。 TCP データグラムに ACK または RST ビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。 スタック メンバー 1 のギガビット イーサネット インターフェイス 1 は、ルータをインターネットに接続するインターフェイスです。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 102 in
```

例：名前付き ACL

名前付き標準 ACL および名前付き拡張 ACL の作成

次に、*Internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。 *Internet_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit
```

marketing_group ACL は、宛先アドレスとワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。 ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ～ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit
```

Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
Switch(config)# interface gigabitethernet3/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in
```

名前付き ACL からの個別 ACE の削除

次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

例：IP ACL に適用される時間範囲

次に、月曜日から金曜日の午前 8 時 ～午後 6 時（18 時）の間、IP の HTTP トラフィックを拒否する例を示します。 UDP トラフィックは、土曜日および日曜日の正午～午後 8 時（20 時）の間だけ許可されます。

```
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip access-group strict in
```

例：コメント付き IP ACL エントリ

次に示す番号付き ACL の例では、Jones が所有するワークステーションにはアクセスを許可し、Smith が所有するワークステーションにはアクセスを許可しません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しません。

```
Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www
```

次に示す名前付き ACL の例では、Jones のサブネットにアクセスを許可しません。

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次に示す名前付き ACL の例では、Jones のサブネットに発信 Telnet の使用を許可しません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
```

```
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

例：ACL ロギング

ルータ ACL では、2 種類のロギングがサポートされています。 **log** キーワードを指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。**log-input** キーワードを指定すると、ログ エントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセス リスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。**log** キーワードも指定されています。

```
Switch(config)# ip access-list standard stan1
Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 37 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 37 messages logged
    File logging: disabled
    Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems

<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次に、名前付き拡張アクセス リスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip access-group ext1 in
```

次に、拡張 ACL のログの例を示します。

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
01:26:12:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1 packet
01:31:33:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8 packets
```

IP ACL のすべてのロギング エントリは %SEC-6-IPACCESSLOG で開始します。エントリの形式は、一致した ACL やアクセス エントリの種類に応じて若干異なります。

次に、**log-input** キーワードを指定した場合の出力メッセージの例を示します。

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400)
 ->
10.1.1.61 (0/0), 1 packet
```

log キーワードを指定した場合、同様のパケットに関するログ メッセージには入力インターフェイス情報が含まれません。

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0), 1
 packet
```

ACL および VLAN マップの設定例

例：パケットを拒否する ACL および VLAN マップの作成

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。 最初のマップでは、*ip1* ACL（TCP パケット）に一致するすべてのパケットがドロップされます。 最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する *ip1* ACL を作成します。 VLAN マップには IP パケットに対する match 句が存在するため、デフォルトのアクションでは、どの match 句とも一致しない IP パケットがすべてドロップされます。

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

例：パケットを許可する ACL および VLAN マップの作成

次に、パケットを許可する VLAN マップを作成する例を示します。 ACL *ip2* は UDP パケットを許可し、*ip2* ACL と一致するすべてのパケットが転送されます。 このマップでは、これ以前のどの ACL とも一致しないすべての IP パケット（TCP でも UDP でもないパケット）がドロップされます。

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

例：IP パケットのドロップおよび MAC パケットの転送のデフォルト アクション

次の例の VLAN マップでは、デフォルトで IP パケットがドロップされ、MAC パケットが転送されます。 標準の ACL 101 および名前付き拡張アクセス リスト **igmp-match** および **tcp-match** をこのマップと組み合わせて使用すると、次のようになります。

- すべての UDP パケットが転送されます。

- すべての IGMP パケットがドロップされます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- すべての非 IP パケットが転送されます。

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any

Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```

例：MAC パケットのドロップおよび IP パケットの転送のデフォルト アクション

次の例の VLAN マップでは、デフォルトで MAC パケットがドロップされ、IP パケットが転送されます。 MAC 拡張アクセス リスト **good-hosts** および **good-protocols** をこのマップと組み合わせて使用すると、次のようになります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- decnet-iv または vines-ip プロトコルを使用する MAC パケットが転送されます。
- その他のすべての非 IP パケットがドロップされます。
- すべての IP パケットが転送されます。

```
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# action forward
Switch(config-ext-macl)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any vines-ip
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

例：すべてのパケットをドロップするデフォルト アクション

次の例の VLAN マップでは、デフォルトですべてのパケット（IP および非 IP）がドロップされます。 例 2 および例 3 のアクセス リスト **tcp-match** および **good-hosts** をこのマップと組み合わせて使用すると、次のようになります。

- すべての TCP パケットが転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- その他のすべての MAC パケットがドロップされます。

```
Switch(config)# vlan access-map drop-all-default 10
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```

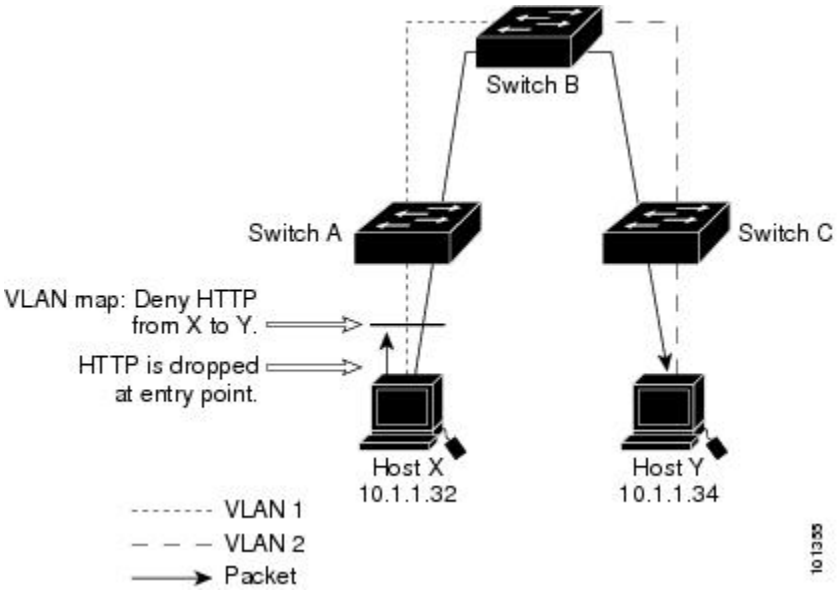
ネットワークでの VLAN マップの使用方法の設定例

例：ワイヤリング クローゼットの設定

ワイヤリング クローゼット構成では、ルーティングがスイッチ上でイネーブルにされていない場合があります。 ただし、この設定でも VLAN マップおよび QoS 分類 ACL はサポートされています。 ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリング クローゼット スイッチ A およびスイッチ C に接続されていると想定します。ホスト X からホスト Y へのトラフィックは、ルーティングがイネーブルに設定されたレイヤ 3 スイッチであるスイッチ B によって最終的にルー

ティングされます。 ホスト X からホスト Y へのトラフィックは、トラフィックのエントリ ポイントであるスイッチ A でアクセス コントロールできます。

図 *94*：ワイヤリング クローゼットの設定



HTTP トラフィックをホスト X からホスト Y へスイッチングしない場合は、ホスト X（IP アドレス 10.1.1.32）からホスト Y（IP アドレス 10.1.1.34）に向かうすべての HTTP トラフィックがスイッチ A でドロップされ、スイッチ B にブリッジングされないように、スイッチ A の VLAN マップを設定できます。

最初に、HTTP ポート上ですべての TCP トラフィックを許可（一致）する IP アクセス リスト *http* を定義します。

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

次に、*http* アクセス リストと一致するトラフィックがドロップされ、その他のすべての IP トラフィックが転送されるように、VLAN アクセス マップ *map2* を作成します。

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

次に、VLAN アクセス マップ *map2* を VLAN 1 に適用します。

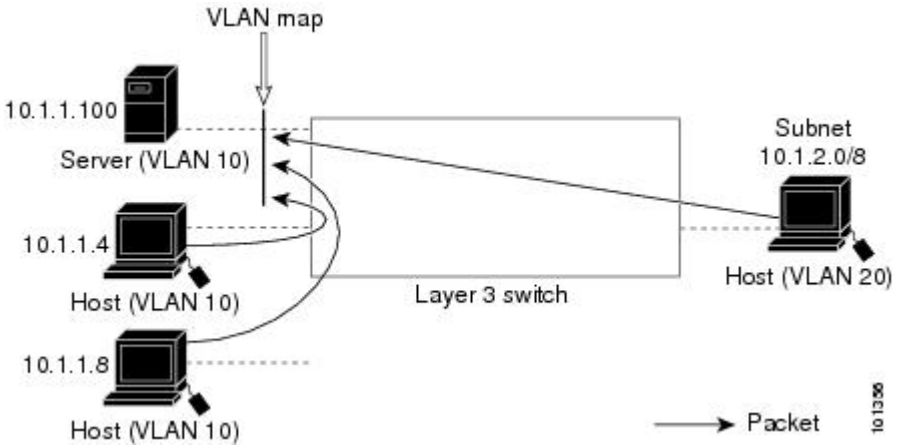
```
Switch(config)# vlan filter map2 vlan 1
```

例：別の VLAN にあるサーバへのアクセスの制限

別の VLAN にあるサーバへのアクセスを制限できます。 たとえば、VLAN 10 内のサーバ 10.1.1.100 では、次のホストへのアクセスを拒否する必要があります。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスを禁止します。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスを禁止します。

図 *95*：別の *VLAN* 上のサーバへのアクセスの制限



例：別の VLAN にあるサーバへのアクセスの拒否

次に、サブネット 10.1.2.0.8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 のアクセスを拒否し、その他の IP トラフィックを許可する VLAN マップ SERVER1-ACL を作成して、別の VLAN 内のサーバへのアクセスを拒否する例を示します。 最後のステップでは、マップ SERVER1 を VLAN 10 に適用します。

正しいパケットと一致する IP ACL を定義します。

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl))# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl))# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl))# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl))# exit
```

SERVER1_ACL と一致する IP パケットをドロップして、この ACL と一致しない IP パケットを転送する ACL を使用して、VLAN マップを定義します。

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

VLAN 10 に VLAN マップを適用します。

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10
```

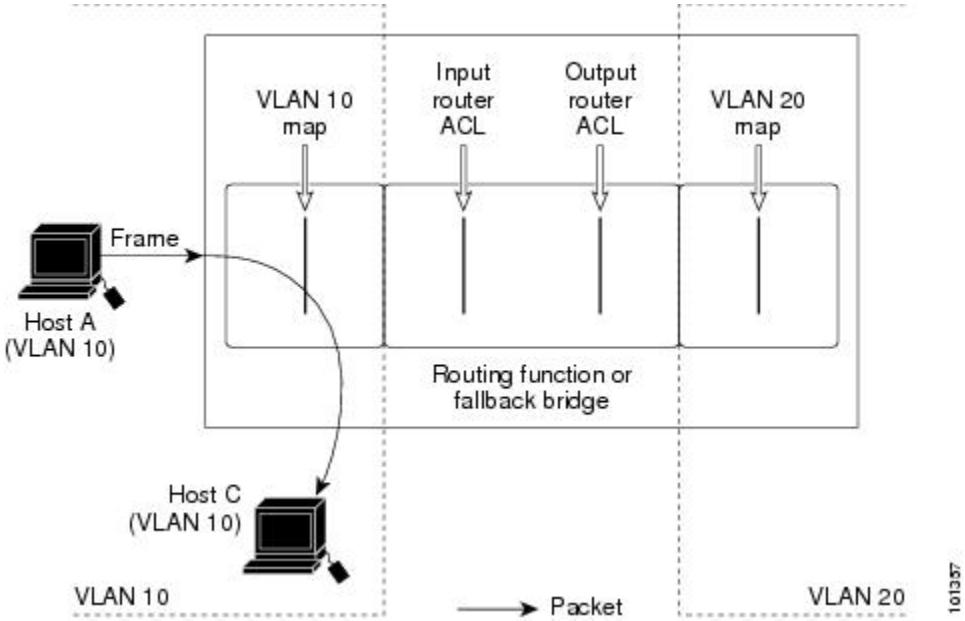
VLAN に適用されるルータ ACL と VLAN マップの設定例

ここでは、ルータ ACL および VLAN マップを VLAN に適用し、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットを処理する例を示します。次の図ではそれぞれの宛先に転送されるパケットを示します。パケットのパスが VLAN マップや ACL を示す線と交差するポイントで、パケットを転送せずにドロップする可能性もあります。

例：ACL およびスイッチド パケット

次の例に、VLAN 内でスイッチングされるパケットに ACL を適用する方法を示します。 フォールバック ブリッジングによってルーティングまたは転送されず、VLAN 内でスイッチングされるパケットには、入力 VLAN の VLAN マップだけが適用されます。

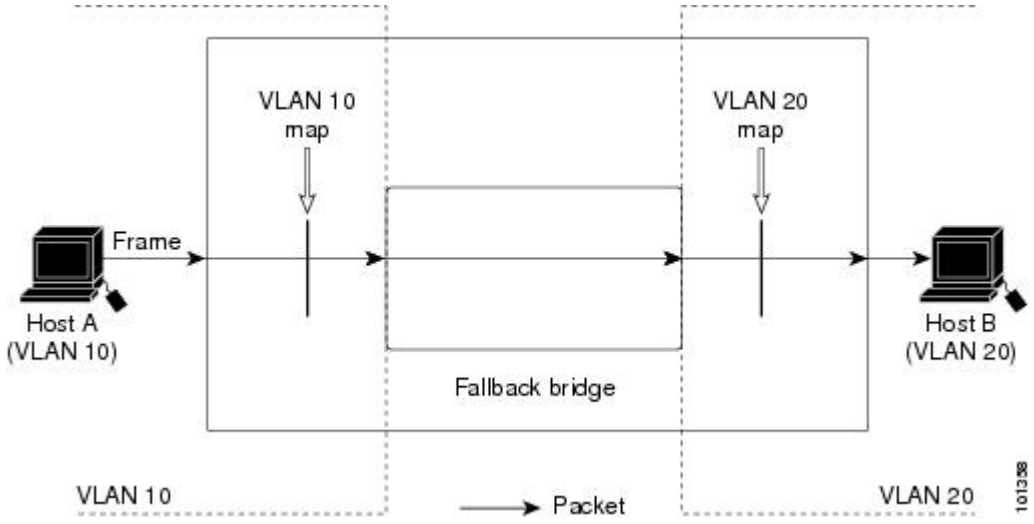
図 *96*：スイッチド パケットへの *ACL* の適用



例：ACL およびブリッジド パケット

次の例に、フォールバック ブリッジド パケットに ACL を適用する方法を示します。 ブリッジド パケットの場合は、入力 VLAN にレイヤ 2 ACL だけが適用されます。 また、非 IP および非 ARP パケットだけがフォールバック ブリッジド パケットとなります。

図 *97*：ブリッジド パケットへの *ACL* の適用

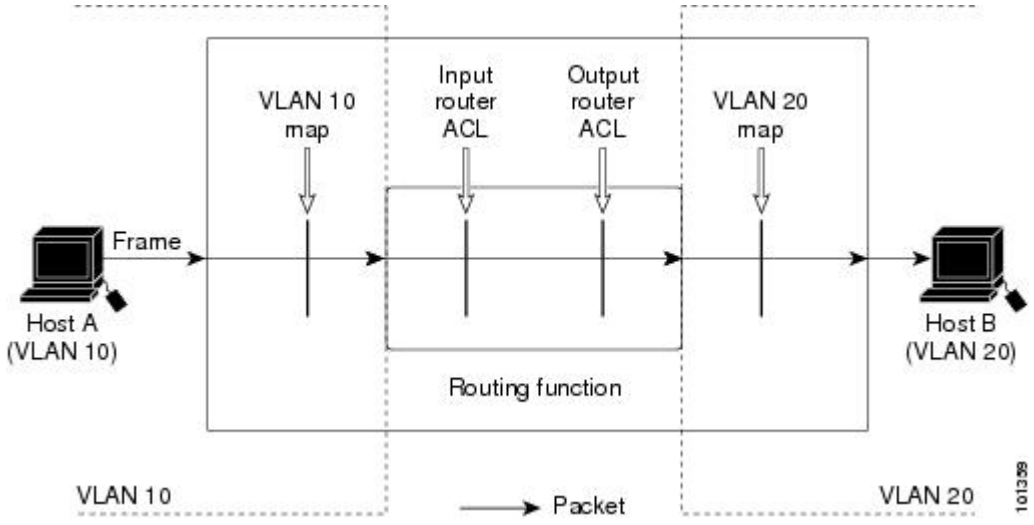


例：ACL およびルーテッド パケット

次の例に、ルーテッド パケットに ACL を適用する方法を示します。 ACL は次の順番で適用されます。

1. 入力 VLAN の VLAN マップ
2. 入力ルータ ACL
3. 出力ルータ ACL
4. 出力 VLAN の VLAN マップ

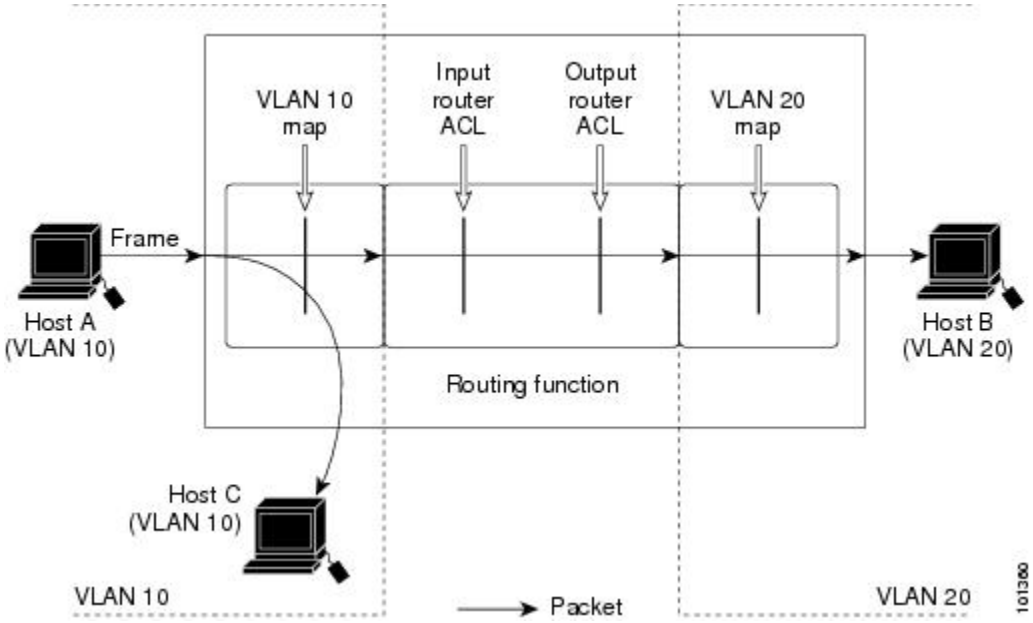
図 *98*：ルーテッド パケットへの *ACL* の適用



例：ACL およびマルチキャスト パケット

次の例に、IP マルチキャスト用に複製されたパケットに ACL を適用する方法を示します。 ルーティングされるマルチキャスト パケットには、2 つの異なるフィルタが適用されます。1 つは、宛先が入力 VLAN 内の他のポートである場合に使用され、もう 1 つは、宛先がパケットのルーティング先である別の VLAN 内にある場合に使用されます。 パケットは複数の出力 VLAN にルーティングされる場合がありますが、この場合は宛先 VLAN ごとに異なるルータ出力 ACL および VLAN マップが適用されます。 最終的に、パケットは一部の出力 VLAN 内で許可され、それ以外の VLAN で拒否されます。 パケットのコピーが、許可された宛先に転送されます。 ただし、入力 VLAN マップによってパケットがドロップされる場合、パケットのコピーは宛先に送信されません。

図 *99*：マルチキャスト パケットへの *ACL* の適用



第 56 章

IPv6 ACL の設定

- 機能情報の確認，1497 ページ
- IPv6 ACL の概要，1497 ページ
- IPv6 ACL の制限，1498 ページ
- IPv6 ACL のデフォルト設定，1499 ページ
- IPv6 ACL の設定，1500 ページ
- インターフェイスへの IPv6 ACL の付加，1504 ページ
- IPv6 ACL のモニタリング，1506 ページ

機能情報の確認

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

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

IPv6 ACL の概要

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。 また、スイッチで IP ベースおよび LAN ベース フィーチャ セットが稼働している場合、入力ルータ ACL を作成し、それを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

スイッチは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンド トラフィックまたはインバウンド トラフィックでサポートされます。 IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。
- IPv6 ポート ACL は、インバウンドおよびアウトバウンドのレイヤ 2 インターフェイスでトラフィックでサポートされます。 IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。

スイッチは、IPv6 トラフィックの Virtual LAN（VLAN）ACL（VLAN マップ）をサポートしません。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。 IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージプロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。 各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。 ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。
- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。 MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリに空きがない場合、パケットはインターフェイスでドロップされ、アンロードのエラー メッセージが記録されます。

IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。 IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは再起 ACL（**reflect** キーワード）をサポートしません。
- このリリースが IPv6 用にサポートしているのは、ポート ACL およびルータ ACL だけです。VLAN ACL（VLAN マップ）はサポートしていません。
- IPv6 の出力ルータ ACL および入力ポート ACL は、スイッチ スタックでだけサポートされています。 スイッチは、コントロール プレーン（着信）IPv6 ACL だけをサポートします。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- レイヤ 2 EtherChannel に IPv6 ポート ACL を適用できません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。 ハードウェア転送が必要なインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうか判別します。 サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ（ACE）を追加しようとする場合、スイッチは現在インターフェイスに適用されている ACL に ACE が追加されるのを許可しません。

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム（IPv4 では **fragments** キーワード）がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。
- スイッチのハードウェア スペースがなくなった場合、ACL に関連付けられたパケットはインターフェイスでドロップされます。
- ホップバイホップ オプションがあるルーテッド パケットまたはブリッジド パケットには、ソフトウェアで適用される IPv6 ACL が設定されます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。
- スイッチは、プレフィックス長の最大範囲の IPv6 アドレス一致をサポートしません。

IPv6 ACL のデフォルト設定

デフォルトの IPv6 ACL 設定は次のとおりです。

```
Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
```

```
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します

手順の概要

1. **enable**
2. **configureterminal**
3. {**ipv6 access-list***list-name*
4. {**deny** | **permit**} protocol {*source-ipv6-prefix/|prefix-length*|**any**| **host***source-ipv6-address*} [operator [*port-number*]] { *destination-ipv6-prefix/ prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]][**dscp***value*] [**fragments**] [**log**] [**log-input**] [**routing**][**sequence***value*] [**time-range***name*]
5. {**deny** | **permit**} **tcp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [**operator** [**port-number**]] {*destination-ipv6- prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [**ack**] [**dscp***value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {**port** | protocol}] [**psh**] [**range** {**port** | protocol}] [**rst**] [**routing**] [**sequence***value*] [**syn**] [**time-range***name*] [**urg**]
6. {**deny** | **permit**} **udp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [**dscp***value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**][**sequence***value*] [**time-range***name*]]
7. {**deny** | **permit**} **icmp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [*icmp-type* [*icmp-code*] | icmp-message] [**dscp***value*] [**log**] [**log-input**] [**routing**][**sequence***value*] [**time-range***name*]
8. **end**
9. **show ipv6 access-list**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	{**ipv6 access-list***list-name* 例： `Switch(config)# ipv6 access-list example_acl_list`	IPv6 ACL 名を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	{**deny** | **permit**} protocol {*source-ipv6-prefix/|prefix-length*|**any**| **host***source-ipv6-address*} [operator [*port-number*]] { *destination-ipv6-prefix/ prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]][**dscp***value*] [**fragments**] [**log**] [**log-input**] [**routing**][**sequence***value*] [**time-range***name*]	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。 次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、**udp**、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • *source-ipv6-prefix/prefix-length* または *destination-ipv6-prefix/ prefix-length* は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 • **host***source-ipv6-address* または *destination-ipv6-address* には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。 オペランドには、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、**range**（包含範囲）があります。 *source-ipv6-prefix/prefix-length* 引数のあとの operator は、送信元ポートに一致する必要があります。 *destination-ipv6-prefix/prefix-length* 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）**port-number** は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。 TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。 UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。

	コマンドまたはアクション	目的
		• （任意）**dscp** value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。 指定できる範囲は 0 ～ 63 です。 • （任意）**fragments** を入力して、先頭ではないフラグメントを確認します。 このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • （任意）**log** を指定すると、エントリと一致するパケットに関するログ メッセージがコンソールに送信されます。 **log-input** を指定すると、ログ エントリに入力インターフェイスが追加されます。 ロギングはルータ ACL でだけサポートされます。 • （任意）**routing** を入力して、IPv6 パケットのルーティングを指定します。 • （任意）**sequence***value* を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。 指定できる範囲は 1 ～ 4,294,967,295 です。 • （任意）**time-range** name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 5	{**deny** | **permit**} **tcp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [**operator** [**port-number**]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [**ack**] [**dscp***value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {**port** | protocol}] [**psh**] [**range** {**port** | protocol}] [**rst**] [**routing**] [**sequence***value*] [**syn**] [**time-range***name*] [**urg**]	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は **tcp** を入力します。 パラメータはステップ 3a で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 • **ack**：確認応答（ACK）ビット セット • **established**：確立された接続。 TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • **fin**：終了ビットセット。送信元からのデータはそれ以上ありません。 • **neq** {*port* | protocol}：所定のポート番号上にないパケットだけを照合します。 • **psh**：プッシュ機能ビット セット • **range** {*port* | protocol}：ポート番号の範囲内のパケットだけを照合します。 • **rst**：リセット ビット セット • **syn**：同期ビット セット

	コマンドまたはアクション	目的
		• **urg**：緊急ポインタ ビット セット
ステップ 6	{**deny** | **permit**} **udp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [**dscp***value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**][**sequence***value*] [**time-range***name*]]	（任意）UDP アクセス リストおよびアクセス条件を定義します。 ユーザ データグラム プロトコルの場合は、**udp** を入力します。 UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [*port*]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。
ステップ 7	{**deny** | **permit**} **icmp** {*source-ipv6-prefix/prefix-length* | **any** | **host***source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host***destination-ipv6-address*} [operator [*port-number*]] [*icmp-type* [*icmp-code*] | icmp-message] [**dscp***value*] [**log**] [**log-input**] [**routing**][**sequence***value*] [**time-range***name*]	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージ プロトコルの場合は、**icmp** を入力します。 ICMP パラメータはステップ 1 の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。 オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-code*：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。 ICMP メッセージのタイプ名およびコード名のリストについては、?キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ipv6 access-list**	アクセス リストの設定を確認します。
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

インターフェイスに IPv6 ACL をアタッチします。

インターフェイスへの IPv6 ACL の付加

レイヤ 3 インターフェイスで発信または着信トラフィックに、あるいはレイヤ 2 インターフェイスで着信トラフィックに ACL を適用できます。 レイヤ 3 インターフェイスで着信トラフィックにだけ ACL を適用できます。

インターフェイスへのアクセスを制御するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **no switchport**
5. **ipv6 address***ipv6-address*
6. **ipv6traffic-filter***access-list-name* {**in** | **out**}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id*	アクセス リストを適用するレイヤ2インターフェイス（ポート ACL 用）またはレイヤ 3 インターフェイス（ルータ ACL 用）を特定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no switchport**	ルータ ACL を適用する場合は、これによってインターフェイスがレイヤ 2 モード（デフォルト）からレイヤ 3 モードに変化します。
ステップ 5	**ipv6 address***ipv6-address*	レイヤ 3 インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。
ステップ 6	**ipv6traffic-filter***access-list-name* {**in** | **out**}	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。 （注） out キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 ACL のモニタリング

次の表に示された 1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

コマンド	目的
show access-lists	スイッチに設定されたすべてのアクセス リストを表示します。
show ipv6 access-list [*access-list-name*]	設定済みのすべての IPv6 アクセス リストまたは名前で指定されたアクセス リストを表示します。

次に、show access-lists 特権 EXEC コマンドの出力例を示します。 出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Switch # show access-lists
Extended IP access list hello
    10 permit ip any any
IPv6 access list ipv6
    permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。 出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet (15 matches) sequence 20
    permit udp any any sequence 30

IPv6 access list outbound
    deny udp any any sequence 10
    deny tcp any any eq telnet sequence 20
```

第 57 章

DHCP の設定

- 機能情報の確認，1507 ページ
- DHCP に関する情報，1507 ページ
- DHCP 機能の設定方法，1515 ページ
- DHCP サーバ ポートベースのアドレス割り当ての設定，1526 ページ

機能情報の確認

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

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

DHCP に関する情報

DHCP サーバ

DHCP サーバは、スイッチまたはルータ上の指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、それらのアドレスを管理します。 DHCP サーバがそのデータベースから要求された設定パラメータを取得して DHCP クライアントに渡すことができない場合は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに要求を転送します。 スイッチは、DHCP サーバとして機能できます。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送するレイヤ 3 デバイスです。 リレーエージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。 リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。 リレー エージェントは、DHCP メッセージを受け取ると、新しい DHCP メッセージを生成して、出力インターフェイス上で送信します。

DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと DHCP スヌーピング バインディング データベース（DHCP スヌーピング バインディング テーブルとも呼ばれる）の作成および管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。 DHCP スヌーピングを使用することにより、エンドユーザに接続された信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。

（注） DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。

信頼できない DHCP メッセージとは、信頼できないインターフェイス経由で送信されたメッセージのことです。 デフォルトでは、スイッチはすべてのインターフェイスを信頼できないものと見なします。 そのため、スイッチはいくつかのインターフェイスを信頼して DHCP スヌーピングを使用するように設定する必要があります。 サービスプロバイダー環境で DHCP スヌーピングを使用する場合は、カスタマーのスイッチなど、サービスプロバイダーネットワーク内には存在しないデバイスから送信されたメッセージが信頼できないメッセージとなります。 不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカル インターフェイスのインターフェイス情報が含まれています。 このデータベースには、信頼できるインターフェイスに接続されたホストの情報はありません。

サービスプロバイダーネットワークでは、信頼できるインターフェイスとして設定できるものの例として、同じネットワーク内のデバイスのポートに接続されたインターフェイスがあります。 信頼できないインターフェイスには、ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスがあります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。 アドレスが一致した場合（デフォルト）、スイッチはパケットを転送します。 アドレスが一致しない場合、スイッチはパケットをドロップします。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットをドロップします。

- DHCPOFFER パケット、DHCPACK パケット、DHCPNAK パケット、DHCPLEASEQUERY パケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスが一致しない。
- スイッチが DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バインディング データベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP Option 82 情報を挿入するエッジスイッチに接続されているスイッチは、Option 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットをドロップします。 DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジスイッチに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジ スイッチによって挿入された Option 82 情報を含むパケットを受け入れます。 集約スイッチは、信頼できないスイッチインターフェイスを介して接続されたホストのバインディングを認識します。 集約スイッチで、ダイナミック ARP インスペクションや IP ソース ガードなど、DHCP セキュリティ機能をイネーブルに設定することもできますが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない入力インターフェイスで受信します。 集約スイッチ上のエッジスイッチとの接続ポートは、信頼できるインターフェイスとして設定する必要があります。

通常、ワイヤレスクライアントにパケットをブロードキャストするのは望ましくありません。 したがって、DHCP スヌーピングは、宛先ブロードキャスト MAC アドレス（ffff.ffff.ffff）をサーバからワイヤレス クライアントに送信される DHCP パケットのユニキャスト MAC アドレスに置き換えます。 ユニキャスト MAC アドレスは DHCP ペイロードの CHADDR フィールドから取得されます。 この処理は、DHCP OFFER、DHCP ACK および DHCP NACK メッセージなどのクライアント パケットにサーバ用に適用されます。 **ip dhcp snooping wireless bootp-broadcast enable** は、この動作を戻すために使用できます。 ワイヤレス BOOTP ブロードキャストがイネーブルの場合、サーバからのブロードキャスト DHCP パケットは、宛先 MAC アドレスを変更せずにワイヤレス クライアントに転送されます。

関連トピック

DHCP スヌーピングおよび Option 82 を設定するための前提条件, （1520 ページ）

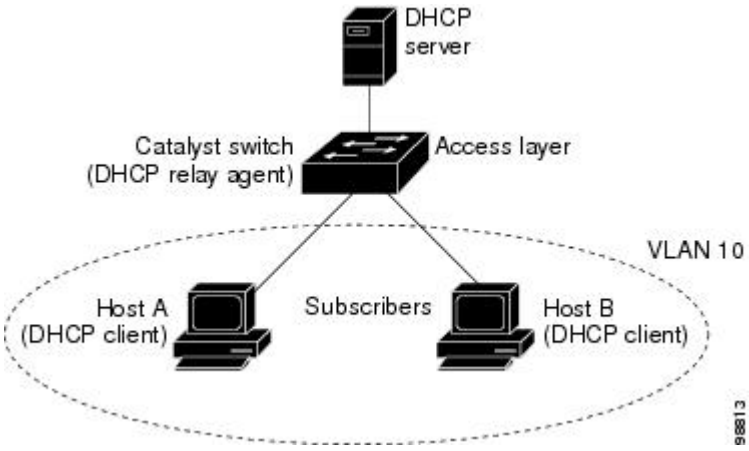
Option 82 データ挿入

住宅地域にあるメトロポリタン イーサネット アクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。 スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチ ポートによっても識別されます。 サブスクライバ LAN 上の複数のホストをアクセス スイッチの同じポートに接続できます。これらのホストは一意に識別されます。

（注） DHCP Option 82 機能は、DHCP スヌーピングがグローバルにイネーブルであり、Option 82 を使用する加入者装置が割り当てられた VLAN でイネーブルである場合に限りサポートされます。

次の図に、一元的な DHCP サーバがアクセス レイヤのスイッチに接続された加入者に IP アドレスを割り当てるメトロポリタン イーサネット ネットワークを示します。 DHCP クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレー エージェント（Catalyst スイッチ）にヘルパー アドレスを設定することにより、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 *100*：メトロポリタン イーサネット ネットワークにおける *DHCP* リレー エージェント



スイッチで DHCP スヌーピング情報 Option 82 をイネーブルにすると、次のイベントがこの順序で発生します。

- ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。 デフォルトでは、リモート ID サブオプションがスイッチの MAC アドレスで、回線 ID サブオプションはパケットを受信するポート ID（**vlan-mod-port**）です。リモート ID および回線 ID は設定できます。サブオプションの設定の詳細については、を参照してください。

- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。 Option 82 に対応しているサーバであれば、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するようなポリシーを実装したりできます。 次に DHCP サーバは、DHCP 応答内にオプション 82 フィールドをエコーします。
- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。 スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。 スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、次のフィールドの値は変化しません（図「サブオプションのパケット形式」を参照）。

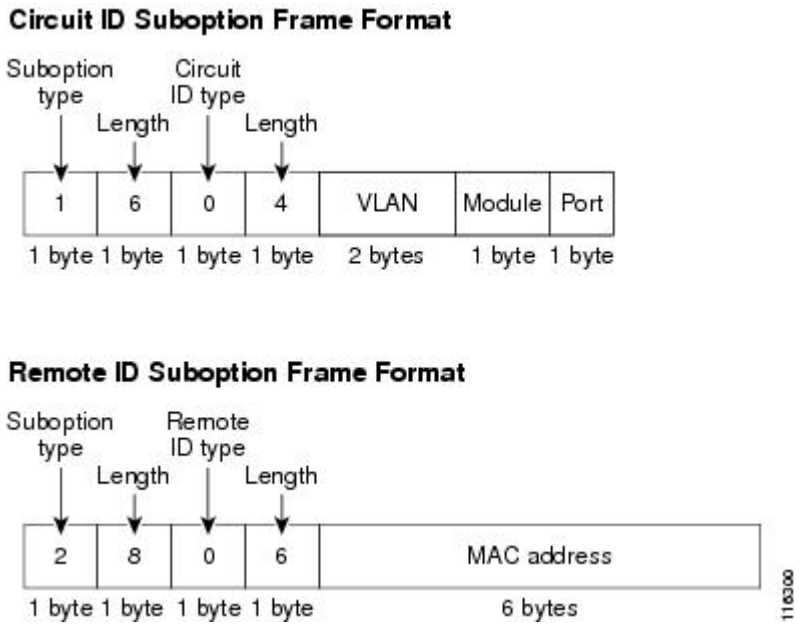
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号が 3 から始まります。 たとえば、24 個の 10/100/1000 ポートおよび 4 つの Small Form-Factor Pluggable（SFP）モジュール スロットを搭載するスイッチでは、ポート 3 がギガビット イーサネット 1/0/1 ポート、ポート 4 がギガビット イーサネット 1/0/2 ポートとなり、以降同様に続きます。 ポート 27 は SFP モジュール スロットのギガビット イーサネット 1/0/25 となり、以降同様に続きます。

図「サブオプションのパケット形式」に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。 回線 ID サブオプションでは、モジュール番号は、スタックにあるスイッチ番号に対応します。 スイッチがこれらのパケット形式を使用するのは、DHCP スヌーピングをグローバルにイネーブルにし、

ip dhcp snooping information option グローバル コンフィギュレーション コマンドを入力した場合です。

図 *101*：サブオプションのパケット形式



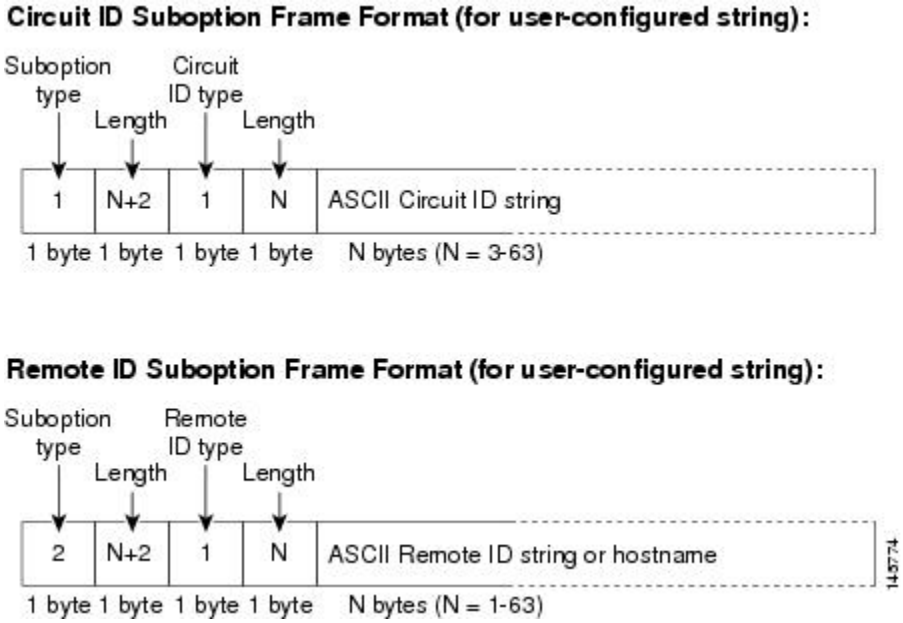
図「ユーザ設定のサブオプションのパケット形式」は、ユーザ設定のリモート ID サブオプション、および回線 ID サブオプションのパケット形式を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力した場合に、これらのパケット形式が使用されます。

パケットでは、リモート ID および回線 ID サブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

- 回線 ID サブオプション フィールド
  - 回線 ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
  - リモート ID タイプが 1 である。

- 設定した文字列の長さに応じて、長さの値が変化する。

図 *102*： ユーザ設定のサブオプションのパケット形式



Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。 これには IP アドレス、アドレス バインディング、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。 クライアント IP アドレスを手動で割り当てること、または、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てることが可能です。 手動および自動アドレス バインディングの詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章を参照してください。

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピング バインディング データベースに保存します。 データベースには、64,000 のバインディングを含めることができます。

各データベース エントリ（バインディング）は、IP アドレス、それに関連付けられた MAC アドレス、リース期間（16 進形式）、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。 データベース エージェントは、設定された場所のファイルにバインディングを保存します。 各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。 各エントリは、まず 72 バイトのデータがあり、その後に 1 つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。 エージェントがディセーブルで、ダイナミック ARP インスペクションまたは IP ソース ガードがイネーブルにされ、DHCP スヌーピング バインディング データベースがダイナミックバインディングされている場合、スイッチは接続を切断されます。 このエージェントがディセーブルで、DHCP スヌーピングだけがイネーブルである場合、スイッチの接続は切断されませんが、DHCP スヌーピングは DHCP スプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディング データベースを作成します。 スイッチは、データベースに変更が加えられたときにはバインディング ファイルを更新します。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、ただちにデータベース内のエントリを更新します。 スイッチはバインディング ファイル内のエントリも更新します。 バインディング ファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。 ファイルが指定された時間内（書き込み遅延および中断タイムアウトの値によって設定される）に更新されない場合、更新は停止します。

バインディングが含まれるファイルの形式は次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。 最初の行の initial-checksum エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Gi1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 584a38f0
END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを DHCP スヌーピング バインディング データベースに追加します。 次のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スイッチがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。 この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している（スイッチはリース期間の終了時にバインディング エントリを削除しないことがある）。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- インターフェイスがルーテッドインターフェイスまたはDHCPスヌーピングにおける信頼できるインターフェイスである。

DHCP 機能の設定方法

DHCP スヌーピングのデフォルト設定

表 *137* : ***DHCP*** のデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要[15]
DHCP リレー エージェント	イネーブル[16]
DHCP パケット転送アドレス	未設定
リレー エージェント情報の確認	イネーブル（無効なメッセージは廃棄）。
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置換。
DHCP スヌーピングをグローバルにイネーブル	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
パケットを信頼できない入力インターフェイスで受け取る DHCP スヌーピング オプション[17]	ディセーブル
DHCP スヌーピング レート制限	未設定
DHCP スヌーピング信頼状態	信頼できない

機能	デフォルト設定
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピングの MAC アドレス検証	イネーブル
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブル、設定が必要。 （注） スイッチは、DHCP サーバとして設定されているデバイスからだけ、ネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブル、設定が必要。 この機能は宛先が設定されている場合に限り有効。

15 スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。
16 スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。
17 この機能は、スイッチがエッジ スイッチによって Option 82 情報が挿入されたパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

- スイッチ ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチ ポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。
- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報を表示したり、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報をクリアしたりできるようになりました。

DHCP サーバの設定

スイッチは、DHCP サーバとして機能できます。

スイッチを DHCP サーバとして設定するときの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の項の「Configuring DHCP」を参照してください。

DHCP リレー エージェントの設定

スイッチ上で DHCP リレー エージェントをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **service dhcp**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service dhcp** 例： `Switch(config)# service dhcp`	スイッチ上で DHCP サーバおよび DHCP リレー エージェントをイネーブルにします。 デフォルトでは、この機能はイネーブルです。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

これらの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の「*Configuring DHCP*」の項を参照してください。

- リレー エージェント情報のチェック（検証）
- リレー エージェント転送ポリシーの設定

パケット転送アドレスの指定

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合、スイッチを **ip helper-address***address* インターフェイス コンフィギュレーション コマンドで設定する必要があります。 一般的なルールは、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。 **ip helper-address** コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスにすることができます。 ネットワーク アドレスを使用することで、どの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface vlan***vlan-id*
4. **ip address***ip-address subnet-mask*
5. **ip helper-address***address*
6. **end**
7. 次のいずれかを使用します。
   - **interface range***port-range*
   - **interface***interface-id*
8. **switchport mode access**
9. **switchport access vlan***vlan-id*
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**interface vlan***vlan-id* 例： `Switch(config)# interface vlan 1`	VLAN ID を入力してスイッチ仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address***ip-address subnet-mask* 例： `Switch(config-if)# ip address 192.108.1.27 255.255.255.0`	インターフェイスに IP アドレスおよび IP サブネットを設定します。
ステップ 5	**ip helper-address***address* 例： `Switch(config-if)# ip helper-address 172.16.1.2`	DHCP パケット転送アドレスを指定します。 ヘルパー アドレスは特定の DHCP サーバ アドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにすることができます。 ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 6	**end** 例： `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	次のいずれかを使用します。 • **interface range***port-range* • **interface***interface-id*	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス範囲コンフィギュレーションモードを開始します。 または

	コマンドまたはアクション	目的
	例： `Switch(config)# interface gigabitethernet1/0/2`	DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	ポートの VLAN メンバーシップ モードを定義します。
ステップ 9	**switchport access vlan***vlan-id* 例： `Switch(config-if)# switchport access vlan 1`	ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP スヌーピングおよび Option 82 を設定するための前提条件

DHCP スヌーピングおよび Option 82 の前提条件は次のとおりです。

- DHCP スヌーピングは、スイッチ上でグローバルにイネーブルにする必要があります。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレーエージェントとして機能するデバイスが設定され、イネーブルになっていることを確認してください。

- スイッチを DHCP 要求に応答するようにする場合は、DHCP サーバとして設定する必要があります。
- スイッチで DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能するデバイスを設定してください。 DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。 サービスプロバイダーネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。
- DHCP スヌーピングで Cisco IOS DHCP サーバ バインディング データベースを使用するには、Cisco IOS DHCP サーバ バインディング データベースを使用するようにスイッチを設定する必要があります。
- 信頼できない入力でパケットを受け入れる DHCP スヌーピング オプションを使用するには、スイッチがエッジ スイッチから Option 82 情報を含むパケットを受信する集約スイッチである必要があります。
- 次の前提条件が DHCP スヌーピング バインディング データベースの設定に適用されます。
  - DHCP スヌーピング用にスイッチを使用するには、DHCP スヌーピング バインディング データベースで宛先を設定する必要があります。
  - NVRAM とフラッシュ メモリは、いずれも記憶容量が限られているため、バインディング ファイルを TFTP サーバに保存することを推奨します。
  - ネットワーク ベースの URL（TFTP や FTP など）については、スイッチがバインディングをその URL のバインディング ファイルに初めて書き込む前に、設定された URL に空のファイルを作成する必要があります。 空のファイルをサーバ上に作成する必要があるかどうかについては、TFTP サーバのマニュアルを参照してください。TFTP サーバによっては、そのように設定できないことがあります。
  - データベースに正しいリース期間が記録されるように、ネットワーク タイム プロトコル（NTP）をイネーブルにし、設定することを推奨します。
  - NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディング ファイルに書き込みます。
- スイッチで DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスを設定してください。 DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、デバイスの DHCP オプションを設定するか、または DHCP データベース エージェントをセットアップする必要があります。
- スイッチが DHCP パケットをリレーするようにする場合は、DHCP サーバの IP アドレスは DHCP クライアントのスイッチ仮想インターフェイス（SVI）に設定する必要があります。

- スイッチ ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチ ポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。

関連トピック

DHCP スヌーピング, （1508 ページ）

DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチ上で DHCP スヌーピングをイネーブルにするには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip dhcp snooping**
4. **ip dhcp snooping vlan***vlan-range*
5. **ip dhcp snooping information option**
6. **ip dhcp snooping information option format remote-id** [**string***ASCII-string* | **hostname**]
7. **ip dhcp snooping information option allow-untrusted**
8. **interface***interface-id*
9. **ip dhcp snooping vlan***vlan***information option format-type circuit-id** [**override**] **string***ASCII-string*
10. **ip dhcp snooping trust**
11. **ip dhcp snooping limit rate***rate*
12. **exit**
13. **ip dhcp snooping verify mac-address**
14. **end**
15. **show running-config**
16. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp snooping** 例： `Switch(config)# ip dhcp snooping`	DHCP スヌーピングをグローバルにイネーブル化します。
ステップ 4	**ip dhcp snooping vlan***vlan-range* 例： `Switch(config)# ip dhcp snooping vlan 10`	VLAN または VLAN 範囲で DHCP スヌーピングをイネーブルにします。 指定できる範囲は 1 ～ 4094 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。 • VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。
ステップ 5	**ip dhcp snooping information option** 例： `Switch(config)# ip dhcp snooping information option`	スイッチが、転送された DHCP 要求メッセージにある DHCP リレー情報（オプション 82 フィールド）を DHCP サーバに挿入したり削除したりできるようにイネーブルにします。 これがデフォルト設定です。
ステップ 6	**ip dhcp snooping information option format remote-id** [**string***ASCII-string* | **hostname**] 例： `Switch(config)# ip dhcp snooping information option format remote-id string acsiistring2`	（任意）リモート ID サブオプションを設定します。 リモート ID は次のように設定できます。 • 63 文字までの ASCII 文字列（スペースなし） • スイッチに設定されたホスト名 （注） ホスト名が 64 文字以上の場合、リモート ID 設定で 63 文字に切り捨てられます。 デフォルトのリモート ID はスイッチ MAC アドレスです。

	コマンドまたはアクション	目的
ステップ 7	**ip dhcp snooping information option allow-untrusted** 例： `Switch(config)# ip dhcp snooping information option allow-untrusted`	（任意）スイッチが、エッジスイッチに接続された集約スイッチである場合、エッジ スイッチからのオプション 82 情報付き着信 DHCP スヌーピング パケットを受け入れるようにこのコマンドによってスイッチをイネーブルにします。 デフォルト設定では無効になっています。 （注） このコマンドは、信頼できるデバイスに接続された集約スイッチだけで入力してください。
ステップ 8	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip dhcp snooping vlan***vlan***information option format-type circuit-id** [**override**] **string***ASCII-string* 例： `Switch(config-if)# ip dhcp snooping vlan 1 information option format-type curcuit-id override string ovrride2`	（任意）指定したインターフェイスの回線 ID サブオプションを設定します。 1 ～ 4094 の範囲の VLAN ID を使用して、VLAN およびポート ID を指定します。 デフォルトの回線 ID はポート ID で、フォーマットは **vlan-mod-port** です。 回線 ID は 3 ～ 63 の ASCII 文字列（スペースなし）を設定できます。 （任意）**override** キーワードは、加入者情報を定義するための TLV 形式に回線 ID サブオプションを挿入したくない場合に使用します。
ステップ 10	**ip dhcp snooping trust** 例： `Switch(config-if)# ip dhcp snooping trust`	（任意）インターフェイスの信頼性を trusted または untrusted に設定します。 信頼できないクライアントからのメッセージを受信するようにインターフェイスを設定するには、**no** キーワードを使用します。 デフォルト設定は untrusted です。
ステップ 11	**ip dhcp snooping limit rate***rate* 例： `Switch(config-if)# ip dhcp snooping limit rate 100`	（任意）インターフェイスが受信できる 1 秒あたりの DHCP パケット数を設定します。 指定できる範囲は 1 ～ 2048 です。 デフォルトでは、レート制限は設定されません。 （注） 信頼できないインターフェイスのレート制限を 1 秒あたり 100 パケット以下に設定することを推奨します。 信頼できるインターフェイスのレート制限を設定する場合、DHCP スヌーピングを使った複数の VLAN に割り当てられたトランク ポートでは、レート制限の値を大きくすることが必要になることがあります。

	コマンドまたはアクション	目的
ステップ 12	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**ip dhcp snooping verify mac-address** 例： `Switch(config)# ip dhcp snooping verify mac-address`	（任意）信頼できないポートに着信した DHCP パケットの送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認するようにスイッチを設定します。デフォルトでは、送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認します。
ステップ 14	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 15	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 16	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『Cisco IOS IP Configuration Guide, Release 12.4』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

DHCP スヌーピング情報のモニタリング

表 *138*：*DHCP* 情報を表示するためのコマンド

show ip dhcp snooping	スイッチの DHCP スヌーピングの設定を表示します。

show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングだけを表示します。このようなバインディングは、バインディング テーブルとも呼ばれます。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピングの統計情報を要約または詳細形式で表示します。
show ip source binding	動的および静的に設定されたバインディングを表示します。

（注） DHCP スヌーピングがイネーブルでインターフェイスがダウン ステートに変更された場合、静的に設定されたバインディングは削除されません。

DHCP サーバ ポートベースのアドレス割り当ての設定

DHCP サーバ ポートベースのアドレス割り当ての設定の概要

DHCP サーバ ポートベースのアドレス割り当ては、接続されたデバイス クライアントの ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポートで同じ IP アドレスを維持できるようにする機能です。

ネットワークに導入されたイーサネット スイッチは、直接接続されたデバイスに接続を提供します。 工場の作業場など、一部の環境では、あるデバイスで不具合が発生した場合は、それと同時に、そのネットワークで代わりのデバイスが動作を開始しなければなりません。 現在の DHCP 実装では、この代わりのデバイスに、DHCP が同じ IP アドレスを提供する保証はありません。 コントロールやモニタリングなどを行うソフトウェアは、各デバイスに関連付けられた IP アドレスが一定であることを期待しています。 デバイスを交換した場合、DHCP クライアントが変更された場合でも、アドレスの割り当ては一定のままでなければなりません。

DHCP サーバ ポートベースのアドレス割り当て機能が設定されている場合、この機能により、ある接続ポートで受信された DHCP メッセージでクライアント ID やクライアント ハードウェア アドレスが変更されたとしても、同じ接続ポートには常に同じ IP アドレスが提供されることが保証されます。 DHCP プロトコルは、DHCP パケットのクライアント ID オプションにより、DHCP クライアントを識別します。 クライアント ID オプションを含まないクライアントは、クライアント ハードウェア アドレスにより識別されます。 この機能を設定すると、インターフェイスのポート名が、クライアント ID またはハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアント ID になります。

すべてのケースで、同じポートにイーサネット ケーブルを接続することにより、接続されたデバイスに、DHCP 経由で同じ IP アドレスが割り当てられます。

DHCP サーバ ポートベースのアドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけです。サードパーティ製のサーバではサポートされていません。

ポートベースのアドレス テーブルのデフォルト設定

デフォルトでは、DHCPサーバポートベースのアドレス割り当てはディセーブルにされています。

ポートベースのアドレス割り当て設定時の注意事項

- デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。
- DHCP プールから事前に設定された予約への割り当てを制限する（予約されていないアドレスはクライアントに提供されず、その他のクライアントはプールによるサービスを受けない）ために、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力することができます。

DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチ上でDHCPスヌーピングバインディングデータベースエージェントをイネーブルにし、設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip dhcp snooping database** {**flash**[*number*]**:**/*filename* | **ftp:**//*user***:***password***@***host*/*filename* | **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** | **rcp:**//*user***@***host*/*filename*}| **tftp:**//*host*/*filename*
4. **ip dhcp snooping database timeout***seconds*
5. **ip dhcp snooping database write-delay***seconds*
6. **end**
7. **ip dhcp snooping binding***mac-address***vlan***vlan-id***ip-address***interface***interface-id***expiry***seconds*
8. **show ip dhcp snooping database** [**detail**]
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp snooping database** {**flash**[*number*]**:**/*filename* | **ftp:**//*user***:***password***@***host*/*filename* | **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** | **rcp:**//*user***@***host*/*filename*}| **tftp:**//*host*/*filename* 例： `Switch(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2`	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイルの URL を指定します。 • **flash**[*number*]**:**/*filename* （任意）スタック マスターのスタック メンバ番号を指定するには、*number* パラメータを使用します。 *number* の指定できる範囲は 1 ～ 9 です。 • **ftp:**//*user***:***password***@***host*/*filename* • **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** • **rcp:**//*user***@***host*/*filename* • **tftp:**//*host*/*filename*
ステップ 4	**ip dhcp snooping database timeout***seconds* 例： `Switch(config)# ip dhcp snooping database timeout 300`	データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間（秒数）を指定します。 デフォルトは 300 秒です。 指定できる範囲は 0 ～ 86400 です。 無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。

	コマンドまたはアクション	目的
ステップ 5	**ip dhcp snooping database write-delay***seconds* 例： `Switch(config)# ip dhcp snooping database write-delay 15`	バインディングデータベースが変更されてから転送を開始するまでの遅延時間を指定します。 指定できる範囲は15 ～ 86400 秒です。 デフォルトは 300 秒（5 分）です。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**ip dhcp snooping binding***mac-address***vlan***vlan-id***ip***-address***interface***interface-id***expiry***seconds* 例： `Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000`	（任意）DHCP スヌーピング バインディングデータベースにバインディングエントリを追加します。 *vlan-id* に指定できる範囲は 1 ～ 4904 です。 *seconds* の範囲は 1 ～ 4294967295 です。 このコマンドは、追加するエントリごとに入力します。 このコマンドは、スイッチをテストまたはデバッグするときに使用します。
ステップ 8	**show ip dhcp snooping database** [**detail**] 例： `Switch# show ip dhcp snooping database detail`	DHCP スヌーピング バインディングデータベース エージェントのステータスおよび統計情報を表示します。
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルにイネーブル化し、インターフェイス上で加入者 ID を自動的に生成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip dhcp use subscriber-id client-id**
4. **ip dhcp subscriber-id interface-name**
5. **interface***interface-id*
6. **ip dhcp server use subscriber-id client-id**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp use subscriber-id client-id** 例： `Switch(config)# ip dhcp use subscriber-id client-id`	すべての着信 DHCP メッセージで、加入者 ID がクライアント ID としてグローバルに使用されるように DHCP サーバを設定します。
ステップ 4	**ip dhcp subscriber-id interface-name** 例： `Switch(config)# ip dhcp subscriber-id interface-name`	インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。 特定のインターフェイスで設定された加入者 ID は、このコマンドで優先されます。

	コマンドまたはアクション	目的
ステップ 5	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip dhcp server use subscriber-id client-id** 例： `Switch(config-if)# ip dhcp server use subscriber-id client-id`	インターフェイス上ですべての着信 DHCP メッセージで、加入者 ID がクライアント ID として使用されるように DHCP サーバを設定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

スイッチ上での DHCP ポートベースのアドレス割り当てをイネーブルにした後で、**ip dhcp pool** グローバルコンフィギュレーションコマンドを使用して、IP アドレスの事前割り当てと、クライアントへの関連付けを行います。

DHCP サーバ ポートベースのアドレス割り当てのモニタリング

表 *139*：*DHCP* ポートベースのアドレス割り当て情報を表示するためのコマンド

コマンド	目的
show interface*interface id*	特定のインターフェイスのステータスおよび設定を表示します。

コマンド	目的
show ip dhcp pool	DHCP アドレス プールを表示します。
show ip dhcp binding	Cisco IOS DHCP サーバのアドレス バインディングを表示します。

第 58 章

IP ソース ガードの設定

IP ソース ガード（IPSG）は、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックを制限するセキュリティ機能で、DHCP スヌーピング バインディング データベースと手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングすることで実現されます。

この章は、次の内容で構成されています。

- 機能情報の確認，1533 ページ
- IP ソース ガードの概要，1534 ページ
- IP ソース ガードの設定方法，1537 ページ
- IP ソース ガードのモニタリング，1540 ページ

機能情報の確認

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

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

IP ソース ガードの概要

IP ソース ガード

ネイバーの IP アドレスを使用する場合に、トラフィック攻撃を防ぐために IP ソース ガードを使用でき、そして信頼できないインターフェイスで DHCP スヌーピングがイネーブルの場合に、IP アドレスを使用しようとすると、IP ソース ガードをイネーブルにできます。

インターフェイス上でIPSGをイネーブルにすると、スイッチは、DHCPスヌーピングにより許可された DHCP パケットを除き、このインターフェイスで受信したすべての IP トラフィックをブロックします。

スイッチは IP アドレスをポートにバインドするためにハードウェアの発信元 IP 検索テーブルを使用します。 IP および MAC のフィルタリングでは、送信元 IP 検索と送信元 MAC 検索の組み合わせが使用されます。 送信元 IP アドレスを使用する IP トラフィックでは、バインディング テーブルが許可され、他のすべてのトラフィックは拒否されます。

IP ソース バインディング テーブルには、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング（スタティック IP送信元バインディング）があります。 このテーブルのエントリには IP アドレスと、関連 MAC アドレス、および関連 VLAN 番号があります。 スイッチは、IP ソース ガードがイネーブルにされている場合だけ、IP ソース バインディング テーブルを使用します。

IPSGは、アクセスポートおよびトランク ポートを含むレイヤ2ポートだけでサポートされます。送信元 IP アドレスと送信元 IP および MAC アドレス フィルタリングで IPSG を設定できます。

スタティック ホスト用 IP ソース ガード

（注） アップリンク ポート、またはトランク ポートで、スタティック ホスト用 IP ソース ガード（IPSG）を使用しないでください。

スタティック ホスト用 IPSG は、IPSG の機能を DHCP ではない、スタティックな環境に拡張するものです。 これまでの IPSG は、DHCP スヌーピングにより作成されたエントリを使用して、スイッチに接続されたホストを検証していました。 ホストから受信したトラフィックのうち、有効な DHCP を持たないものはすべてドロップされます。 このセキュリティ機能によって、ルーティングされないレイヤ2インターフェイス上の IP トラフィックが制限されます。 この機能は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングします。 前バージョンの IPSG では、IPSG を動作させるために DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしで IPSG を動作させることができます。 スタティック ホスト用 IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブル エントリに依存しています。 このスイッチは、指定されたポートで有効なホストのリストを維持するために、ARP リクエスト、またはその他の IP パケットに基づいてスタティック エントリを

作成します。 また、指定されたポートにトラフィックを送信できるホストの数を指定することもできます。 これはレイヤ 3 でのポート セキュリティと同じです。

スタティック ホスト用 IPSG はダイナミック ホストもサポートしています。 ダイナミック ホストが、IP DHCP スヌーピング テーブルに存在する DHCP が割り当てられた IP アドレスを受信すると、IP デバイス トラッキング テーブルは同じエントリを学習します。 スタック化環境では、マスターのフェールオーバーが発生すると、メンバ ポートに接続されたスタティック ホストの IP ソース ガード エントリは、そのまま残ります。 **show ip device tracking all** 特権 EXEC コマンドを入力すると、IP デバイス トラッキング テーブルには、これらのエントリが ACTIVE であると表示されます。

（注） 複数のネットワーク インターフェイスを持つ IP ホストの一部は、ネットワーク インターフェイスに無効なパケットを注入することができます。 この無効なパケットには、ソース アドレスとして、別のホスト ネットワーク インターフェイスの IP アドレス、または MAC アドレスが含まれます。 この無効パケットは、スタティック ホスト用 IPSG がホストに接続され、無効な IP アドレス バインディングまたは MAC アドレス バインディングが学習されて、有効なバインディングが拒否される原因となります。 ホストによる無効なパケットの注入を回避する方法については、対応するオペレーティング システムとネットワーク インターフェイスのベンダーにお問い合わせください。

最初、スタティック ホスト用 IPSG は ACL ベースのスヌーピング メカニズムを通じて、動的に IP バインディング、または MAC バインディングを学習します。 IP バインディング、または MAC バインディングは、ARP パケット、および IP パケットにより、スタティック ホストから学習されます。 これらはデバイス トラッキング データベースに保存されます。 指定されたポートで動的に学習、または静的に設定された IP アドレスの数が最大値に達した場合、新しい IP アドレスを持つパケットはすべて、ハードウェアによりドロップされます。 何らかの理由で移動された、またはなくなったホストを解決するために、スタティック ホスト用 IPSG は IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングをエージング アウトします。 この機能は、DHCP スヌーピングとともに使用できます。 複数バインディングは、DHCP ホストとスタティック ホストの両方に接続されたポートに確立されます。 たとえば、バインディングは、デバイス トラッキング データベースと DHCP スヌーピング バインディング データベースの両方に保存されます。

IP ソース ガードの設定時の注意事項

- スタティック IP バインディングは、非ルーテッド ポートだけで設定できます。 ルーテッド インターフェイスで **ip source binding***mac-address***vlan***vlan-id ip-address***interface***interface-id* グローバル コンフィギュレーション コマンドを入力すると、次のエラー メッセージが表示されます。

```
Static IP source binding can only be configured on switch port.
```

- 送信元 IP フィルタリング機能を持つ IP ソース ガードがインターフェイスでイネーブルにされている場合、このインターフェイスのアクセス VLAN で、DHCP スヌーピングをイネーブルにしておく必要があります。

- 複数の VLAN を持つトランク インターフェイス上で IP ソース ガードをイネーブルにし、これらすべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。

（注） IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切にトラフィックをフィルタリングできない可能性があります。

- この機能は、802.1x ポートベースの認証がイネーブルにされている場合にイネーブルにできます。
- IP ソース ガード スマート ロギングを設定すると、指定されたアドレスや DHCP によって学習されたアドレス以外の送信元アドレスを持つパケットは拒否され、そのパケットの内容が NetFlow 収集装置に送信されます。 この機能を設定する場合は、スマート ロギングがグローバルにイネーブルになっていることを確認してください。
- スイッチ スタックでは、IP ソース ガードがスタック メンバー インターフェイスに設定されていて、**noswitch***stack-member-number***provision** グローバル コンフィギュレーション コマンドの入力によりそのスイッチの設定を削除した場合、インターフェイス スタティック バインディングはバインディング テーブルから削除されますが、実行コンフィギュレーションからは削除されません。 **switch***stack-member-number***provision** コマンドを入力することによって、スイッチを再度プロビジョニングした場合、バインディングは復元されます。

  実行コンフィギュレーションからバインディングを削除するには、**no switch provision** コマンドを入力する前に IP ソース ガードをディセーブルにする必要があります。 インターフェイスがバインディング テーブルから削除される間にスイッチがリロードされると、設定も削除されます。

IP ソース ガードの設定方法

IP ソース ガードのイネーブル化

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip verify source** [**mac-check**]
5. **exit**
6. **ip source binding***mac-address***vlan***vlan-id ip-address***interface***interface-id*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip verify source** [**mac-check**] 例： `Switch(config-if)# ip verify source`	送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 （任意）**mac-check**：送信元 IP アドレスによる IP ソース ガードおよび MAC アドレス フィルタリングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip source binding***mac-address***vlan***vlan-id ip-address***interface***interface-id* 例： `Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1`	スタティック IP ソースバインディングを追加します。 スタティック バインディングごとにこのコマンドを入力します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定

スタティック ホスト用 IPSG を動作させるには、**ip device trackingmaximum***limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。 このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルにイネーブルにしていない、または IP device tracking maximum をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip device tracking**
4. **interface***interface-id*
5. **switchport mode access**
6. **switchport access vlan***vlan-id*
7. **ip verify source**[**tracking**] [**mac-check**]
8. **ip device tracking maximum***number*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip device tracking** 例： `Switch(config)# ip device tracking`	IP ホスト テーブルをオンにし、IP デバイス トラッキングをグローバルにイネーブルにします。
ステップ 4	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	アクセスとしてポートを設定します。

	コマンドまたはアクション	目的
ステップ 6	**switchport access vlan***vlan-id* 例： `Switch(config-if)# switchport access vlan 10`	このポートに VLAN を設定します。
ステップ 7	**ip verify source**[**tracking**] [**mac-check**] 例： `Switch(config-if)# ip verify source tracking mac-check`	送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 （任意）**tracking**：スタティック ホスト用 IP ソース ガードをイネーブルにします。 （任意）**mac-check**：MACアドレスフィルタリングをイネーブルにします。 **ip verify source tracking mac-check** コマンドは、MAC アドレス フィルタリングのあるスタティック ホストに対して IP ソース ガードをイネーブルにします。
ステップ 8	**ip device tracking maximum***number* 例： `Switch(config-if)# ip device tracking maximum 8`	そのポートで、IP デバイス トラッキング テーブルにより許可されるスタティック IP 数の上限を設定します。 指定できる範囲は 1 ～ 10 です。 最大値は 10 です。 （注） **ip device trackingmaximum***limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

IP ソース ガードのモニタリング

表 *140*：特権 *EXEC* 表示コマンド

コマンド	目的
show ip verify source [**interface***interface-id*]	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。
show ip device tracking { **all** | **interface***interface-id* | **ip***ip-address* | **mac***imac-address*}	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。

表 *141* : インターフェイス コンフィギュレーション コマンド

コマンド	目的
ip verify source tracking	データ ソースを確認します。

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

第 59 章

ダイナミック ARP インスペクションの設定

- 機能情報の確認，1543 ページ
- ダイナミック ARP インスペクションの制約事項，1544 ページ
- ダイナミック ARP インスペクションの概要，1545 ページ
- ダイナミック ARP インスペクションのデフォルト設定，1550 ページ
- ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ，1550 ページ
- 非 DHCP 環境での ARP ACL の設定 ，1551 ページ
- DHCP 環境でのダイナミック ARP インスペクションの設定，1554 ページ
- 着信 ARP パケットのレート制限，1556 ページ
- ダイナミック ARP インスペクション検証チェックの実行，1559 ページ
- DAI のモニタリング，1561 ページ
- DAI の設定の確認，1562 ページ

機能情報の確認

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

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

ダイナミック ARP インスペクションの制約事項

ここでは、スイッチにダイナミック ARP インスペクションを設定するときの制約事項および注意事項を示します。

- ダイナミック ARP インスペクションは入力セキュリティ機能です。出力チェックはまったく行いません。
- ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションをサポートしていないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されるホストに対しては有効ではありません。 中間者攻撃は単一のレイヤ 2 ブロードキャスト ドメインに制限されているため、チェックされないドメインと、ダイナミック ARP インスペクションによりチェックされるドメインは区別します。 このアクションは、ダイナミック ARP インスペクションのためにイネーブルにされているドメインでホストの ARP キャッシュを保護します。
- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。 IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

  DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可または拒否を行います。
- ダイナミック ARP インスペクションは、アクセス ポート、トランク ポート、および EtherChannel ポートでサポートされます。

  （注） RSPAN VLAN では、ダイナミック ARP インスペクションをイネーブルにしないでください。 RSPAN VLAN でダイナミック ARP インスペクションをイネーブルにすると、ダイナミック ARP インスペクション パケットが RSPAN 宛先ポートに届かない可能性があります。
- 物理ポートを EtherChannel ポートチャネルに結合するには、この物理ポートとチャネル ポートの信頼状態が一致する必要があります。 そうでない物理ポートは、ポート チャネル内で中断状態のままとなります。 ポート チャネルは、チャネルと結合された最初の物理ポートの信頼状態を継承します。 したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態と一致する必要はありません。

  逆に、ポートチャネルで信頼状態を変更すると、スイッチは、チャネルを構成するすべての物理ポートで新しい信頼状態を設定します。
- レート制限は、スイッチ スタックの各スイッチで別々に算出されます。 クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも高い可能性があることを意味します。 たとえば、レート制限が 30 pps に設定された EtherChannel で、スイッチ 1 に 1 つのポート、およびスイッチ 2 に 1 つのポートがある場合、EtherChannel が errdisable にならずに、各ポートは 29 pps でパケットを受信できます。

- ポート チャネルの動作レートは、チャネル内のすべての物理ポートによる累積値です。 たとえば、ポート チャネルの ARP レート制限を 400 pps に設定すると、このチャネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。 EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャネル メンバーからの受信パケット レートの合計となります。 EtherChannel ポートのレート制限は、各チャネル ポート メンバーが受信する ARP パケットのレートを確認してから設定してください。

  物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポート チャネルの設定に照合して検査されます。 ポート チャネルのレート制限設定は、物理ポートの設定には依存しません。

  EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャネル（すべての物理ポートを含む）は errdisable ステートとなります。

- 着信トランク ポートでは、ARP パケットを必ずレート制限してください。 トランク ポートの集約を反映し、複数のダイナミック ARP インスペクションがイネーブルにされた VLAN にわたってパケットを処理するために、トランク ポートのレートをより高く設定します。 また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用して、レートを無制限に設定することもできます。 1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。

- スイッチで、ダイナミック ARP インスペクションをイネーブルにすると、ARP トラフィックをポリシングするように設定されたポリサーの有効性は失われます。 この結果、すべての ARP トラフィックは CPU に送信されます。

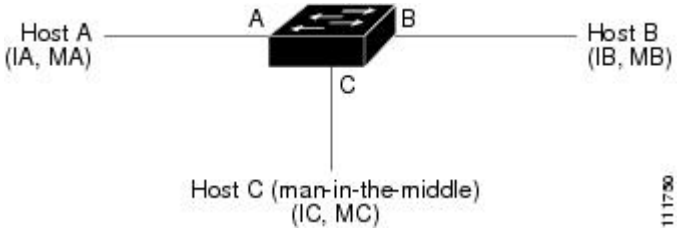
ダイナミック ARP インスペクションの概要

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。 たとえば、ホスト B はホスト A に情報を送信する必要がありますが、ARP キャッシュにホスト A の MAC アドレスを持っていないとします。 ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャスト ドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロードキャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。 しかし、ARP は、ARP 要求が受信されなった場合でも、ホストからの余分な応答を許可するため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生することがあります。 攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイ

ヤ2ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。図 26-1 に、ARP キャッシュ ポイズニングの例を示します。

図 *103* : *ARP* キャッシュ ポイズニング



ホストA、B、およびCは、インターフェイスA、B、およびC上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。 カッコ内に示されているのは、これらのIPアドレス、およびMACアドレスです。たとえば、ホストAが使用するIPアドレスはIA、MACアドレスはMA です。 ホストAがIPレイヤにあるホストBと通信する必要がある場合、ホストAはIPアドレスIBと関連付けられているMACアドレスにARP要求をブロードキャストします。スイッチとホストBは、このARP要求を受信すると、IPアドレスがIAで、MACアドレスがMAのホストに対するARPバインディングをARPキャッシュに読み込みます。たとえば、IPアドレスIAは、MACアドレスMAにバインドされています。 ホストBが応答すると、スイッチ、およびホストAは、IPアドレスがIBで、MACアドレスがMBのホストに対するバインディングをARPに読み込みます。

ホストCは、IPアドレスがIA（またはIB）で、MACアドレスがMCのホストに対するバインディングを持つ偽造ARP応答をブロードキャストすることにより、スイッチ、ホストA、およびホストBのARPキャッシュをポイズニングすることができます。 ARPキャッシュがポイズニングされたホストは、IAまたはIB宛てのトラフィックに、宛先MACアドレスとしてMACアドレスMCを使用します。 つまり、ホストCがこのトラフィックを代行受信することになります。ホストCはIAおよびIBに関連付けられた本物のMACアドレスを知っているため、正しいMACアドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。 ホストCは自身をホストAからホストBへのトラフィック ストリームに挿入します。従来の中間者攻撃です。

ダイナミック ARP インスペクションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。 不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。 この機能により、ネットワークをある種の中間者攻撃から保護することができます。

ダイナミック ARP インスペクションにより、有効な ARP 要求と応答だけが確実にリレーされるようになります。 スイッチが実行する機能は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカルARPキャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

ダイナミック ARP インスペクションは、信頼できるデータベースである DHCP スヌーピング バインディング データベースに格納されている有効な IP/MAC アドレス バインディングに基づいて、ARP パケットの正当性を判断します。 このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピングにより構築されます。 信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、このパケットを転送します。 信頼できないインターフェイスでは、スイッチはこのパケットが有効である場合だけ、このパケットを転送します。

ip arp inspection vlan *vlan-range* グローバル コンフィギュレーション コマンドを使用して、VLAN ごとにダイナミック ARP インスペクションをイネーブルにすることができます。

非 DHCP 環境では、ダイナミック ARP インスペクションは、静的に設定された IP アドレスを持つホストに対するユーザ設定の ARP アクセス コントロール リスト（ACL）と照らし合わせて、ARP パケットの正当性を確認することができます。 ARP ACL を定義するには、**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用します。

パケットの IP アドレスが無効である場合、または ARP パケットの本文にある MAC アドレスが、イーサネット ヘッダーで指定されたアドレスと一致しない場合、ARP パケットをドロップするようにダイナミック ARP インスペクションを設定することができます。 このためには、**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} グローバル コンフィギュレーション コマンドを使用します。

インターフェイスの信頼状態とネットワーク セキュリティ

ダイナミック ARP インスペクションは、スイッチの各インターフェイスに信頼状態を関連付けます。 信頼できるインターフェイスに到着するパケットは、ダイナミック ARP インスペクションの確認検査をすべてバイパスし、信頼できないインターフェイスに到着するパケットには、ダイナミック ARP インスペクションの検証プロセスを受けます。

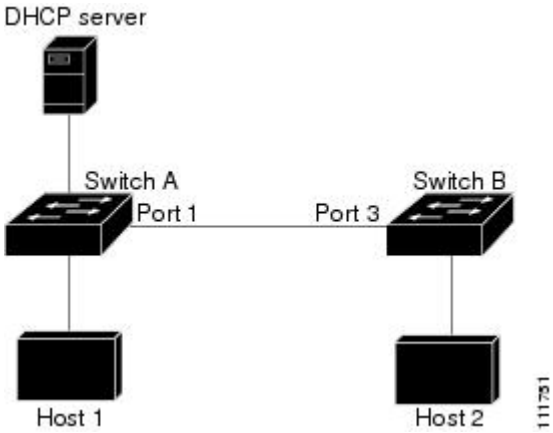
一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチ ポートすべてを信頼できるものに設定します。 この構成では、指定されたスイッチからネットワークに入ってくる ARP パケットはすべて、セキュリティ チェックをバイパスします。 VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。 信頼状態を設定するには、ip arp inspection trust インターフェイス コンフィギュレーション コマンドを使用します。

注意 信頼状態の設定は、慎重に行ってください。 信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

次の図では、スイッチ A とスイッチ B の両方が、ホスト 1 とホスト 2 を含む VLAN でダイナミック ARP インスペクションを実行しているとします。 ホスト 1 とホスト 2 が、スイッチ A に接続している DHCP サーバから IP アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。 したがって、スイッチ A とスイッチ B 間のインター

フェイスが信頼できない場合は、ホスト 1 からの ARP パケットはスイッチ B ではドロップされ、ホスト 1 およびホスト 2 の間の接続は切断されます。

図 *104*：ダイナミック *ARP* インスペクションのためにイネーブルにされた *VLAN* 上の *ARP* パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティ ホールが生じます。 スイッチ A でダイナミック ARP インスペクションが実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの間のリンクが信頼できるものとして設定されている場合はホスト 2）。 この状況は、スイッチ B がダイナミック ARP インスペクションを実行している場合でも発生します。

ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションを実行しているスイッチに接続された（信頼できないインターフェイス上の）ホストが、そのネットワークにあるその他のホストの ARP キャッシュをポイズニングしていないことを保証します。 しかし、ダイナミック ARP インスペクションにより、ネットワークの他の部分にあるホストが、ダイナミック ARP インスペクションを実行しているスイッチに接続されているホストのキャッシュをポイズニングできないようにすることはできません。

VLAN のスイッチの一部がダイナミック ARP インスペクションを実行し、残りのスイッチは実行していない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定します。 ただし、非ダイナミック ARP インスペクションスイッチからパケットのバインディングを検証するには、ARP ACL を使用して、ダイナミック ARP インスペクションを実行するスイッチを設定します。 このようなバインディングが判断できない場合は、レイヤ 3 で、ダイナミック ARP インスペクション スイッチを実行していないスイッチから、ダイナミック ARP インスペクションを実行しているスイッチを分離します。

（注） DHCP サーバとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。 デフォルトでは、信頼できないインターフェイスのレートは 15 パケット/秒（pps）です。 信頼できるインターフェイスはレート制限されません。 この設定を変更するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。 ユーザが介入するまで、ポートはこの状態を維持します。 **errdisable recovery** グローバル コンフィギュレーション コマンドを使用すると、errdisable ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。

（注） EtherChannel のレート制限は、スタックにある各スイッチに個別に適用されます。 たとえば、EtherChannel で 20 pps の制限が設定されている場合、EtherChannel にあるポートの各スイッチでは、最大 20 pps まで実行できます。 スイッチが制限を超過した場合、EtherChannel 全体が errdisable ステートになります。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。 スイッチが ACL を使用するのは、ACL が **ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用して設定されている場合だけです。 スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。 DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

廃棄パケットのロギング

スイッチがパケットをドロップすると、ログ バッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。 メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。 各ログ エントリには、受信側の VLAN、ポート番号、送信元 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定します。 記録されるパケットの種類を指定するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ARP インスペクションのデフォルト設定

機能	デフォルト設定
ダイナミック ARP インスペクション	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
着信 ARP パケットのレート制限	1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチドネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。 信頼できるすべてのインターフェイスでは、レート制限は行われません。 バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。
ログ バッファ	ダイナミック ARP インスペクションがイネーブル化されると、拒否またはドロップされた ARP パケットはすべてが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは 1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。 スイッチが ACL を使用するのは、ACL が ip arp inspection filter vlan グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。 スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。 DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

非 DHCP 環境での ARP ACL の設定

この手順は、図 2 に示すスイッチ B がダイナミック ARP インスペクション、または DHCP スヌーピングをサポートしていないときにダイナミック ARP インスペクションを設定する方法を示しています。

スイッチ A のポート 1 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、スイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが作り出されます。 これを阻止するには、スイッチ A のポート 1 を信頼できないものとして設定する必要があります。 ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。 ホスト 2 の IP アドレスがスタティックではない（スイッチ A で ACL 設定を適用することは不可能である）場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを使用してパケットをルートする必要があります。

スイッチ A で ARP ACL を設定するには、次の手順を実行します。この手順は、非 DHCP 環境では必須です。

手順の概要

1. **enable**
2. **configureterminal**
3. **arp access-list***acl-name*
4. **permit ip host***sender-ip***mac host***sender-mac*
5. **exit**
6. **ip arp inspection filter***arp-acl-name* **vlan***vlan-range* [**static**]
7. **interface***interface-id*
8. **no ip arp inspection trust**
9. **end**
10. 次の show コマンドを使用します。
    - **show arp access-list**acl-name
    - **show ip arp inspection vlan***vlan-range*
    - **show ip arp inspection interfaces**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**arp access-list***acl-name*	ARP ACL を定義し、ARP アクセス リスト コンフィギュレーション モードを開始します。 デフォルトでは、ARP アクセス リストは定義されません。 （注） ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。
ステップ 4	**permit ip host***sender-ip***mac host***sender-mac*	指定されたホスト（ホスト 2）からの ARP パケットを許可します。 • *sender-ip* には、ホスト 2 の IP アドレスを入力します。 • *sender-mac* には、ホスト 2 の MAC アドレスを入力します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip arp inspection filter***arp-acl-name* **vlan***vlan-range* [**static**]	VLAN に ARP ACL を適用します。 デフォルトでは、定義済みの ARP ACL は、どのような VLAN にも適用されません。 • *arp-acl-name* には、ステップ 2 で作成した ACL の名前を指定します。 • *vlan-range* では、スイッチとホストが存在する VLAN を指定します。 VLAN ID 番号により識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • （任意）**static** を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットは廃棄されます。 DHCP バインディングは使用されません。 このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。

	コマンドまたはアクション	目的
		IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。 パケットは、アクセス リストで許可された場合だけに許可されます。
ステップ 7	**interface***interface-id*	スイッチ B に接続されたスイッチ A のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**no ip arp inspection trust**	スイッチ B に接続されたスイッチ A のインターフェイスを untrusted として設定します。 デフォルトでは、すべてのインターフェイスは信頼できません。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。 ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。 スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	次の show コマンドを使用します。 • **show arp access-list**acl-name • **show ip arp inspection vlan***vlan-range* • **show ip arp inspection interfaces**	入力を確認します。
ステップ 11	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP 環境でのダイナミック ARP インスペクションの設定

はじめる前に

この手順では、2つのスイッチがダイナミック ARPインスペクションをサポートしているときに、この機能を設定する方法を示します。 ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B にそれぞれ接続されています。スイッチは両方とも、ホストが配置されている VLAN 1 でダイナミック ARP インスペクションを実行しています。 DHCP サーバはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。 したがって、スイッチ A はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。

（注） 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。 IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

ダイナミック ARPインスペクションを設定するには、次の手順を実行します。 この処理は、両方のスイッチで行う必要があります。 この手順は必須です。

手順の概要

1. **enable**
2. **show cdp neighbors**
3. **configureterminal**
4. **ip arp inspection vlan***vlan-range*
5. **Interface***interface-id*
6. **ip arp inspection trust**
7. **end**
8. **show ip arp inspection interfaces**
9. **show ip arp inspection vlan***vlan-range*
10. **show ip dhcp snooping binding**
11. **show ip arp inspection statistics vlan***vlan-range*
12. **configureterminal**
13. **configureterminal**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**show cdp neighbors** 例： `Switch(config-if)#show cdp neighbors`	スイッチ間の接続を確認します。
ステップ 3	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**ip arp inspection vlan***vlan-range* 例： `Switch(config)# ip arp inspection vlan 1`	VLAN 単位で、ダイナミック ARP インスペクションをイネーブルにします。 デフォルトでは、すべての VLAN 上でダイナミック ARP インスペクションはディセーブルになっています。 vlan-range には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 両方のスイッチに同じ VLAN ID を指定します。
ステップ 5	**Interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	他のスイッチに接続されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip arp inspection trust** 例： `Switch(config-if)#ip arp inspection trust`	スイッチ間の接続を trusted に設定します。 デフォルトでは、すべてのインターフェイスは信頼できません。 スイッチは、信頼できるインターフェイスにあるもう 1 つのスイッチから受信した ARP パケットは確認しません。 この場合、パケットはそのまま転送されます。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。 ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。 スイッチは、無効なパケットをドロップし、ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Switch(config-if)#end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip arp inspection interfaces** 例：	インターフェイスでダイナミック ARP インスペクションの設定を検証します。
ステップ 9	**show ip arp inspection vlan***vlan-range* 例： `Switch(config-if)#show ip arp inspection vlan 1`	VLAN でダイナミック ARP インスペクションの設定を検証します。
ステップ 10	**show ip dhcp snooping binding** 例： `Switch(config-if)#show ip dhcp snooping binding`	DHCP バインディングを確認します。
ステップ 11	**show ip arp inspection statistics vlan***vlan-range* 例： `Switch(config-if)#show ip arp inspection statistics vlan 1`	VLAN でダイナミック ARP インスペクションの統計情報を確認します。
ステップ 12	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

着信 ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。 errordisable 回復をイネーブルにして、指定されたタイムアウト時間の後にポートがこのステートから自動的に抜け出すようにするまで、ポートはこのステートのままです。

（注） インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、レート制限をその信頼状態のデフォルト値に変更することになります。 レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。 **no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

着信 ARP パケットのレートを制限するには、次の手順を実行します。 この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **ip arp inspection limit {rate pps [burst interval seconds] | none}**
5. **exit**
6. 次のコマンドを使用します。
   - **errdisable detect cause arp-inspection**
   - **errdisable recovery cause arp-inspection**
   - **errdisable recovery interval** *interval*
7. **exit**
8. 次の show コマンドを使用します。
   - **show ip arp inspection interfaces**
   - **show errdisable recovery**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id*	レート制限されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip arp inspection limit {rate pps [burst interval seconds] | none}**	インターフェイス上の着信 ARP 要求および ARP 応答のレートを制限します。 デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。 バースト インターバルは 1 秒です。 キーワードの意味は次のとおりです。 • **rate***pps* には、1 秒あたりに処理される着信パケット数の上限を指定します。 有効な範囲は 0 ～ 2048 pps です。 • （任意）**burst interval***seconds* は、レートの高い ARP パケットの有無についてインターフェイスがモニタリングされる間隔（秒）を指定します。 指定できる範囲は 1 ～ 15 です。 • **rate none** では、処理できる着信 ARP パケットのレートの上限を設定しません。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	次のコマンドを使用します。 • **errdisable detect cause arp-inspection** • **errdisable recovery cause arp-inspection** • **errdisable recovery interval** *interval*	（任意）ダイナミック ARP インスペクションの errdisable ステートからのエラー回復をイネーブルにし、ダイナミック ARP インスペクションの回復メカニズムで使用する変数を設定します。 デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。 **interval***interval* には、error-disabled ステートから回復する時間を秒単位で指定します。 指定できる範囲は 30 ～ 86400 です。
ステップ 7	**exit**	特権 EXEC モードに戻ります。
ステップ 8	次の show コマンドを使用します。 • **show ip arp inspection interfaces** • **show errdisable recovery**	設定を確認します。

	コマンドまたはアクション	目的
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ダイナミック ARP インスペクション検証チェックの実行

ダイナミック ARP インスペクションは、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。 宛先 MAC アドレス、送信側および宛先の IP アドレス、および送信元 MAC アドレスで追加検証を実行するように、スイッチを設定できます。

着信 ARP パケットで特定のチェックを実行するには、次の手順を実行します。 この手順は任意です。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip arp inspection validate {[src-mac] [dst-mac] [ip]}**
4. **exit**
5. **show ip arp inspection vlan***vlan-range*
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip arp inspection validate {[src-mac] [dst-mac] [ip]}**	着信 ARP パケットで特定の検査を実行します。 デフォルトでは、検証は実行されません。 キーワードの意味は次のとおりです。 • **src-mac** では、イーサネット ヘッダーの送信元 MAC アドレスと ARP 本文の送信元 MAC アドレスが比較されます。 この検査は、ARP 要求および ARP 応答の両方に対して実行されます。 イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **dst-mac** では、イーサネット ヘッダーの宛先 MAC アドレスと ARP 本文の宛先 MAC アドレスが比較されます。 この検査は、ARP 応答に対して実行されます。 イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **ip** では、ARP 本文から、無効な IP アドレスや予期しない IP アドレスがないかを確認します。 アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。 送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。 少なくとも 1 つのキーワードを指定する必要があります。 コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが src および dst mac の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番めのコマンドによって src および dst mac の検証がディセーブルになります。
ステップ 4	**exit**	特権 EXEC モードに戻ります。
ステップ 5	**show ip arp inspection vlan***vlan-range*	設定を確認します。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

DAI のモニタリング

DAI をモニタするには、次のコマンドを使用します。

コマンド	説明
clear ip arp inspection statistics	ダイナミック ARP インスペクション統計情報をクリアします。
show ip arp inspection statistics [**vlan** *vlan-range*]	指定の VLAN において、転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。 VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。
clear ip arp inspection log	ダイナミック ARP インスペクション ログ バッファをクリアします。
show ip arp inspection log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

show ip arp inspection statistics コマンドでは、スイッチは信頼されたダイナミック ARP インスペクション ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。 スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

DAI の設定の確認

DAI の設定を表示して確認するには、次のコマンドを使用します。

コマンド	説明
show arp access-list [*acl-name*]	ARP ACL についての詳細情報を表示します。
show ip arp inspection interfaces [interface-id]	指定されたインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。
show ip arp inspection vlan *vlan-range*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。 VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。

第 60 章

IEEE 802.1x ポートベースの認証の設定

この章では、IEEE 802.1x ポート ベース認証を設定する方法について説明します。 IEEE 802.1x 認証は、不正なデバイス（クライアント）によるネットワーク アクセスを防止します。 特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチまたはスイッチ スタックを意味します。

- 機能情報の確認，1563 ページ
- 802.1x ポートベース認証について，1563 ページ
- 802.1x ポートベース認証の設定方法，1601 ページ
- 802.1x の統計情報およびステータスのモニタリング，1663 ページ

機能情報の確認

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

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

802.1x ポートベース認証について

802.1x 規格では、一般の人がアクセス可能なポートから不正なクライアントが LAN に接続しないように規制する（適切に認証されている場合を除く）、クライアント/サーバ型のアクセス コントロールおよび認証プロトコルを定めています。 認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN が提供するサービスを利用できるようにします。

802.1x アクセス コントロールでは、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、およびスパニングツリー プロトコル（STP）トラフィックしか許可されません。 認証に成功すると、通常のトラフィックはポートを通過できるようになります。

（注） この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference, Release 12.4*』の「RADIUS Commands」の項およびこのリリースに対応するコマンド リファレンスを参照してください。

ポートベース認証プロセス

802.1x ポートベース認証がイネーブルであり、クライアントが 802.1x 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

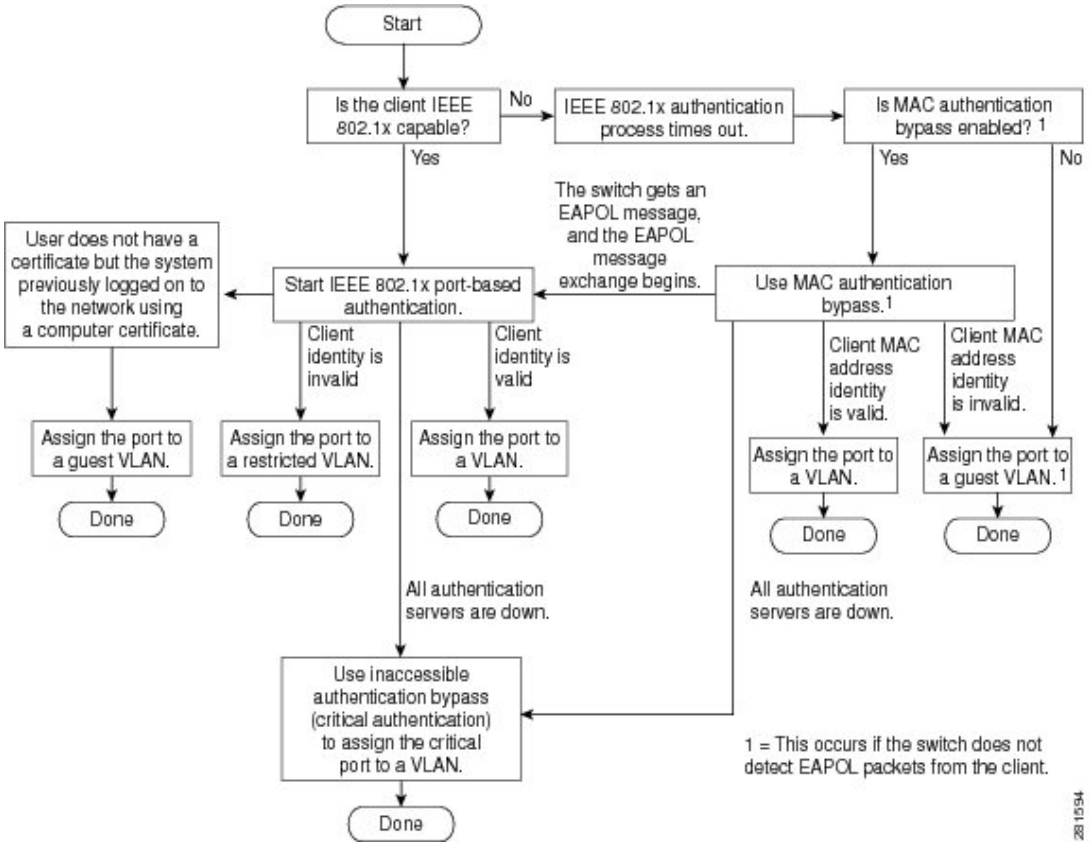
- クライアント ID が有効で 802.1x 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。 このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。 クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。

（注） アクセスできない認証バイパスは、クリティカル認証、または AAA 失敗ポリシーとも呼ばれます。

ポートで Multi Domain Authentication（MDA）がイネーブルになっている場合、音声許可に該当する例外をいくつか伴ったフローを使用できます。

次の図は認証プロセスを示します。

図 *105*：認証フローチャート



次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

  スイッチ固有の値を使用するか、RADIUS サーバからの値に基づいて再認証タイマーを設定できます。

  RADIUS サーバを使用した 802.1x 認証の後で、スイッチは Session-Timeout RADIUS 属性（Attribute[27]）、および Termination-Action RADIUS 属性（Attribute[29]）に基づいてタイマーを使用します。

  Session-Timeout RADIUS 属性（Attribute[27]）には再認証が行われるまでの時間を指定します。

  Termination-Action RADIUS 属性（Attribute[29]）には、再認証中に行われるアクションを指定します。 アクションは *Initialize* および *ReAuthenticate* に設定できます。 アクションに *Initialize*（属性値は *DEFAULT*）を設定した場合、802.1x セッションは終了し、認証中、接続は失われます。 アクションに *ReAuthenticate*（属性値は RADIUS-Request）を設定した場合、セッションは再認証による影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface***interface-id* 特権 EXEC コマンドを入力します。

ポートベース認証の開始およびメッセージ交換

802.1x 認証中に、スイッチまたはクライアントは認証を開始できます。 **authentication port-control auto** インターフェイスコンフィギュレーションコマンドを使用してポート上で認証をイネーブルにすると、スイッチは、リンク ステートがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。 スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。 クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

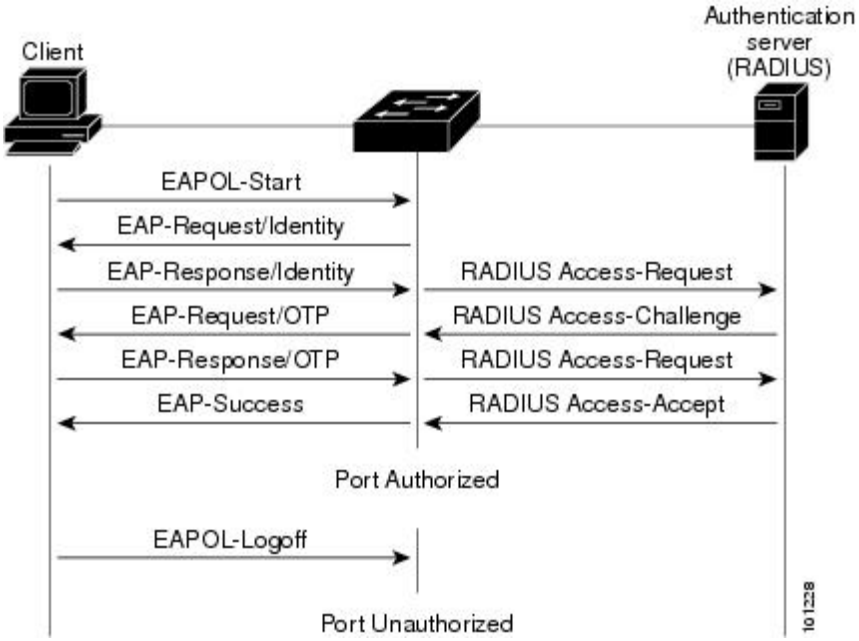
（注） ネットワーク アクセス デバイスで 802.1x 認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。 ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。 認証が成功すると、スイッチ ポートは許可ステートになります。 認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。

次の図に、クライアントがRADIUSサーバとの間でOTP（ワンタイム パスワード）認証方式を使用する際に行われるメッセージ交換を示します。

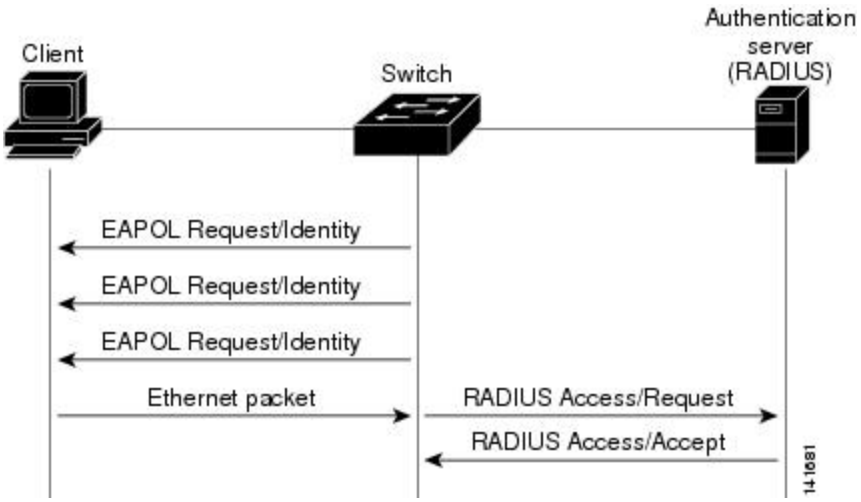
図 *106*：メッセージ交換



EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネット パケットを検出するとそのクライアントを認証できます。 スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS Access/Request フレームにこの情報を保存します。 サーバがスイッチに RADIUS Access/Accept フレームを送信（認証が成功）すると、ポートが許可されます。 認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。 イーサネット パケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、802.1x 認証を開始します。

次の図に、MAC 認証バイパス中のメッセージ交換を示します。

図 *107* : ***MAC*** 認証バイパス中のメッセージ交換



ポートベース認証の認証マネージャ

ポートベースの認証方法

表 *142* : ***802.1x*** 機能

認証方法	モード			
	シングル ホスト	マルチ ホスト	**MDA**	複数認証
802.1x	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[18] リダイレクト URL	VLAN 割り当て	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL

認証方法	モード			
	シングル ホスト	マルチ ホスト	MDA	複数認証
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL
スタンドアロン Web 認証	プロキシ ACL、Filter-ID 属性、ダウンロード可能 ACL			
NAC レイヤ 2 IP 検証	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL
フォールバック方式としての Web 認証[19]	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL	Proxy ACL Filter-ID 属性 ダウンロード可能 ACL

18 Cisco IOS Release 12.2(50)SE 以降でサポートされています。
19 802.1x 認証をサポートしないクライアント用。

ユーザ単位 ACL および Filter-Id

（注） **any** は、ACL の発信元としてだけ設定できます。

（注） マルチホスト モードで設定された ACL では、ステートメントの発信元部分は *any* でなければなりません。 （たとえば、**permit icmp** *any* **host 10.10.1.1**）

定義された ACL の発信元ポートには **any** を指定する必要があります。 指定しない場合、ACL は適用できず、認証は失敗します。 シングルホストは唯一例外的に後方互換性をサポートします。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。 ホストに適用される ACL ポリシーは、別のホストのトラフィックには影響を与えません。 マルチ ホスト ポートで認証されるホストが 1 つだけで、他のホストが認証なしでネットワーク アクセスを取得する場合、発信元アドレスに any を指定することで、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

ポートベース認証マネージャ CLI コマンド

認証マネージャ インターフェイス コンフィギュレーション コマンドは、802.1x、MAC 認証バイパスおよび Web 認証など、すべての認証方法を制御します。 認証マネージャ コマンドは、接続ホストに適用される認証方法のプライオリティと順序を決定します。

認証マネージャ コマンドは、ホストモード、違反モードおよび認証タイマーなど、一般的な認証機能を制御します。 一般的な認証コマンドには、**authentication host-mode**、**authentication violation** および **authentication timer** インターフェイス コンフィギュレーション コマンドがあります。

802.1x 専用コマンドは、先頭に **dot1x** キーワードが付きます。 たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにします。 ただし、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドは常にグローバルに 802.1x 認証をイネーブルまたはディセーブルにします。

（注） 802.1x 認証がグローバルにディセーブル化されても、Web 認証など他の認証方法はそのポートでイネーブルのままです。

authentication manager コマンドは従来の 802.1x コマンドと同様の機能を提供します。

認証マネージャが生成する冗長なシステム メッセージをフィルタリングすると、通常は、フィルタリングされた内容が認証の成功に結びつきます。 802.1x 認証および MAB 認証の冗長なメッセージをフィルタリングすることもできます。 認証方式ごとに異なるコマンドが用意されています。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの冗長なメッセージをフィルタリングします。
- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1x 認証の冗長なメッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC 認証バイパス（MAB）の冗長なメッセージをフィルタリングします。

表 *143*：認証マネージャ コマンドおよび以前の *802.1x* コマンド

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
authentication control-direction {**both** | **in**}	**dot1x control-direction** {**both** | **in**}	Wake-on-LAN（WoL）機能を使用して 802.1x 認証をイネーブルにし、ポート制御を単一方向または双方向に設定します。
authentication event	**dot1x auth-fail vlan** **dot1x critical**（インターフェイスコンフィギュレーション） **dot1x guest-vlan6**	ポート上で制限付き VLAN をイネーブルにします。 アクセス不能認証バイパス機能をイネーブルにします。 アクティブ VLAN を 802.1x ゲスト VLAN として指定します。
authentication fallback*fallback-profile*	**dot1x fallback***fallback-profile*	802.1x 認証をサポートしていないクライアント用に、Web 認証をフォールバック方式として使用するようにポートを設定します。
authentication host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]	**dot1x host-mode** {**single-host** | **multi-host** | **multi-domain**}	802.1x 許可ポートで単一のホスト（クライアント）または複数のホストの接続を許可します。
authentication order	**mab**	使用される認証方法の順序を柔軟に定義できるようにします。
authentication periodic	**dot1x reauthentication**	クライアントの定期的再認証をイネーブルにします。
authentication port-control {**auto** | **force-authorized** | **force-un authorized**}	**dot1x port-control** {**auto** | **force-authorized** | **force-unauthorized**}	ポートの許可ステートの手動制御をイネーブルにします。
authentication timer	**dot1x timeout**	802.1x タイマーを設定します。
authentication violation {**protect** | **restrict** | **shutdown**}	**dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続された後に新しいデバイスがそのポートに接続された場合に発生する違反モードを設定します。

許可ステートおよび無許可ステートのポート

802.1x 認証中に、スイッチのポート ステートによって、スイッチはネットワークへのクライアントアクセスを許可します。 ポートは最初、無許可ステートです。 このステートでは、音声VLAN（仮想 LAN）ポートとして設定されていないポートは 802.1x 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。 クライアントの認証が成功すると、ポートは許可ステートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。 ポートが音声 VLAN ポートとして設定されている場合、VoIP トラフィックおよび 802.1x プロトコル パケットが許可された後クライアントが正常に認証されます。

802.1x をサポートしていないクライアントが、無許可ステートの 802.1x ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。 この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x 対応のクライアントが、802.1x 標準が稼働していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。 応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。 応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

authentication port-control インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized**：802.1x 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。 ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。 これがデフォルト設定です。
- **force-unauthorized**：クライアントからの認証の試みをすべて無視し、ポートを無許可ステートのままにします。 スイッチはポートを介してクライアントに認証サービスを提供できません。
- **auto**：802.1x 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。 ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。 スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。 スイッチはクライアントの MAC アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。 認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。 認証サーバに到達できない場合、スイッチは要求を再送信します。 所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

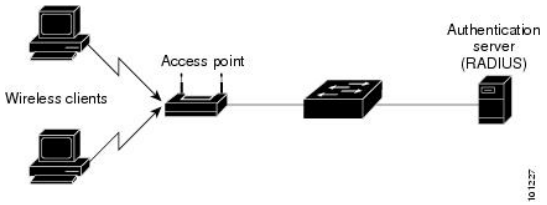
ポートのリンク ステートがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信した場合に、ポートは無許可ステートに戻ります。

802.1X のホスト モード

802.1x ポートは、シングル ホスト モードまたはマルチ ホスト モードで設定できます。 シングル ホスト モードでは、802.1x 対応のスイッチ ポートに接続できるのはクライアント 1 つだけです。 スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。 クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチ ホスト モードでは、複数のホストを単一の 802.1x 対応ポートに接続できます。 このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。 ポートが無許可ステートになると（再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。 このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

図 *108*：マルチ ホスト モードの例



（注） すべてのホスト モードで、ポートベース認証が設定されている場合、ライン プロトコルは許可の前にアップのままです。

スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチ ポートに接続できます。

802.1x 複数認証モード

複数認証（multiauth）モードでは、データ VLAN で複数のクライアントを認証できます。 各ホストは個別に認証されます。 音声 VLAN が設定されている場合、このモードでは、VLAN で 1 クライアントだけ認証できます （ポートが他の音声クライアントを検出すると、これらはポートから廃棄されますが、違反エラーは発生しません）。

ハブまたはアクセス ポイントが 802.1x 対応ポートに接続されている場合、接続されている各クライアントを認証する必要があります。 802.1x 以外のデバイスでは、MAC 認証バイパスまたは Web

認証をホスト単位認証フォールバック メソッドとして使用し、単一のポートで異なる方法で異なるホストを認証できます。

複数認証ポートで認証できるデータ ホストの数には制限はありません。 ただし、音声 VLAN が設定されている場合、許可される音声デバイスは 1 台だけです。 ホスト制限がないため、定義された違反はトリガーされません。たとえば、別の音声デバイスが検出された場合、これは通知なしで廃棄され、違反はトリガーされません。 音声 VLAN の MDA 機能の場合、複数認証モードでは、認証サーバから受け取ったVSAに応じて、認証されたデバイスがデータまたは音声のいずれかの VLAN に割り当てられます。

（注） ポートがマルチ認証モードの場合、ゲスト VLAN、および認証失敗 VLAN 機能はアクティブになりません。

次の条件で、RADIUS サーバから提供された VLAN をマルチ認証モードで割り当てることができます。

- ホストがポートで最初に許可されたホストであり、RADIUS サーバが VLAN 情報を提供している。
- 後続のホストが、動作 VLAN に一致する VLAN を使用して許可される。
- ホストは VLAN が割り当てられていないポートで許可され、後続のホストでは VLAN 割り当てが設定されていないか、VLAN 情報が動作 VLAN と一致している。
- ポートで最初に許可されたホストにはグループ VLAN が割り当てられ、後続のホストでは VLAN 割り当てが設定されていないか、グループ VLAN がポート上のグループ VLAN と一致している。 後続のホストが、最初のホストと同じ VLAN グループの VLAN を使用する必要がある。 VLAN リストが使用されている場合、すべてのホストは VLAN リストで指定された条件に従う。
- マルチ認証ポート上で、1 つの音声 VLAN 割り当てのみがサポートされている。
- VLANがポート上のホストに割り当てられると、後続のホストは一致するVLAN情報を持つ必要があり、この情報がなければポートへのアクセスを拒否される。
- ゲスト VLAN または認証失敗 VLAN をマルチ認証モードに設定できない。
- クリティカル認証 VLAN の動作が、マルチ認証モード用に変更されない。 ホストが認証を試みたときにサーバに到達できない場合、許可されたすべてのホストは、設定された VLAN で再初期化される。

ユーザごとのマルチ認証 VLAN 割り当て

ユーザごとのマルチ認証VLAN割り当て機能を使用すると、単一の設定済みアクセスVLANを持つポート上のクライアントに割り当てられたVLANに基づいて複数の運用アクセスVLANを作成することができます。 データ ドメインに関連付けられたすべての VLAN に対するトラフィックが dot1q とタグ付けされていないアクセス ポートとして設定されているポートおよびこれらの VLAN は、ネイティブ VLAN として処理されます。

マルチ認証ポート 1 つあたりのホストの数は 8 ですが、さらに多くのホストが存在する場合があります。

（注） ユーザごとのマルチ認証VLAN割り当て機能は、音声ドメインではサポートされません。 ポート上の音声ドメインのすべてのクライアントが同じ VLAN を使用する必要があります。

次のシナリオは、ユーザごとのマルチ認証 VLAN 割り当てに関連しています。

シナリオ 1

ハブがアクセスポートに接続されている場合、およびポートがアクセスVLAN（V0）で設定されている場合。

ホスト（H1）は、ハブを介して VLAN（V1）に割り当てられます。 ポートの運用 VLAN は V1 に変更されます。 この動作は、単一ホストポートまたはマルチドメイン認証ポートで同様です。

2 番目のホスト（H2）が接続され、VLAN（V2）に割り当てられる場合、ポートには 2 つの運用 VLAN があります（V1 および V2）。 H1 と H2 がタグなし入力トラフィックを送信すると、H1 トラフィックは VLAN（V1）に、H2 トラフィックは VLAN（V2）にマッピングされ、VLAN（V1）および VLAN（V2）のポートからの出トラフィックはすべてタグなしになります。

両方のホスト H1 と H2 がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN（V1）と VLAN（V2）がポートから削除され、設定された VLAN（V0）がポートに復元されます。

シナリオ 2

ハブがアクセスポートに接続されている場合、およびポートがアクセスVLAN（V0）で設定されている場合。 ホスト（H1）は、ハブを介して VLAN（V1）に割り当てられます。 ポートの運用 VLAN は V1 に変更されます。

2 番目のホスト（H2）が接続され明示的な VLAN ポリシーなしで承認されると、H2 はポート上で復元される設定済み VLAN（V0）を使用することを予期されます。 2 つの運用 VLAN、VLAN（V0）および VLAN（V1）からの出トラフィックはすべてタグなしになります。

ホスト（H2）がログアウトするか、またはセッションがなんらかの理由で削除されると、設定された VLAN（V0）がポートから削除され、VLAN（V1）がそのポートでの唯一の運用 VLAN になります。

シナリオ 3

ハブがオープンモードでアクセスポートに接続されている場合、およびポートがアクセスVLAN（V0）で設定されている場合。

ホスト（H1）は、ハブを介して VLAN（V1）に割り当てられます。 ポートの運用 VLAN は V1 に変更されます。 2 番目のホスト（H2）が接続され無許可のままだと、オープンモードにより、運用 VLAN（V1）に引き続きアクセスできます。

ホスト H1 がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN（V1）はポートから削除され、ホスト（H2）は VLAN（V0）に割り当てられます。

（注） オープン モードと VLAN 割り当ての組み合わせは、ホスト（H2）に悪影響を与えます。そのホストは VLAN（V1）に対応するサブネット内に IP アドレスを含んでいるからです。

ユーザごとのマルチ認証 *VLAN* 割り当ての制限

ユーザごとのマルチ認証 VLAN 割り当て機能では、複数の VLAN からの出トラフィックは、ホストが自分宛てではないトラフィックを受信するポート上ではタグなしになります。 これは、ブロードキャストおよびマルチキャスト トラフィックで問題になる可能性があります。

- **IPv4 ARP**：ホストは他のサブネットからの ARP パケットを受信します。 これは、IP アドレス範囲が重複する異なる仮想ルーティングおよび転送（VRF）テーブルの 2 個のサブネットがポート上でアクティブな場合に問題となります。 ホストの ARP キャッシュが無効なエントリを受け取る可能性があります。
- **IPv6 制御パケット**：IPv6 の導入環境では、ルータ アドバタイズメント（RA）は、その受信を想定されていないホストによって処理されます。 ある VLAN からのホストが別の VLAN からの RA を受信すると、ホストはそれ自身に間違った IPv6 アドレスを割り当てます。 このようなホストは、ネットワークにアクセスできません。

  回避策は、IPv6 ファースト ホップ セキュリティをイネーブルにして、ブロードキャスト ICMPv6 パケットがユニキャストに変換され、マルチ認証がイネーブルのポートから送信されるようにすることです。 パケットは VLAN に属するマルチ認証ポートの各クライアント用に複製され、宛先 MAC が個々のクライアントに設定されます。 1 つの VLAN を持つポートで、ICMPv6 パケットは正常にブロードキャストされます。
- **IP マルチキャスト**：送信先のマルチキャスト グループへのマルチキャスト トラフィックは、異なる VLAN 上のホストがそのマルチキャスト グループに参加している場合それらの VLAN 用に複製されます。 異なる VLAN の 2 つのホストが（同じマルチ認証ポート上の）マルチキャスト グループに参加している場合、各マルチキャスト パケットのコピー 2 部がそのポートから送信されます。

MAC 移動

あるスイッチ ポートで MAC アドレスが認証されると、そのアドレスは同じスイッチの別の認証マネージャ対応ポートでは許可されません。 スイッチが同じ MAC アドレスを別の認証マネージャ対応ポートで検出すると、そのアドレスは許可されなくなります。

場合によっては、MAC アドレスを同じスイッチ上のポート間で移動する必要があります。 たとえば、認証ホストとスイッチ ポート間に別のデバイス（ハブまたは IP Phone など）がある場合、ホストをデバイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC 移動をグローバルにイネーブルにできます。 ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再認証されます。 MAC 移動はすべてのホスト モードでサポートされます （認証ホストは、ポートでイネーブルにされているホスト モードに関係なく、スイッチの任意のポートに移動できます）。 MAC アドレスがあるポートから別のポートに移動すると、スイッチは元のポート

で認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。 MAC 移動の機能は、音声およびデータ ホストの両方に適用されます。

（注） オープン認証モードでは、MACアドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

MAC 置換

MAC置換機能は、ホストが、別のホストがすでに認証済みであるポートに接続しようとすると発生する違反に対処するように設定できます。

（注） 違反はマルチ認証モードでは発生しないため、マルチ認証モードのポートにこの機能は適用されません。 マルチホスト モードで認証が必要なのは最初のホストだけなので、この機能はこのモードのポートには適用されません。

replace キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、マルチドメイン モードのポートでの認証プロセスは、次のようになります。

- 既存の認証済み MAC アドレスを使用するポートで新しい MAC アドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータ ホストの MAC アドレスを、新しい MAC アドレスで置き換えます。
- 認証マネージャは、新しい MAC アドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MACアドレスはただちにMACアドレステーブルに追加されます。

802.1x アカウンティング

802.1x 標準では、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。 802.1x アカウンティングは、デフォルトでディセーブルです。 802.1x アカウンティングをイネーブルにすると、次の処理を 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。

- 再認証が失敗します。

スイッチは 802.1x アカウンティング情報を記録しません。 その代わり、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティング メッセージを記録するように設定する必要があります。

802.1x アカウンティング属性値ペア

RADIUS サーバに送信された情報は、属性値（AV）ペアの形式で表示されます。 これらの AV ペアのデータは、各種アプリケーションによって使用されます （たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性の情報が必要です）。

AV ペアは、802.1x アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START：新規ユーザ セッションが始まると送信されます。
- INTERIM：既存のセッションが更新されると送信されます。
- STOP：セッションが終了すると送信されます。

スイッチによって送信された AV ペアは、**debug radius accounting** 特権 EXEC コマンドを入力することで表示できます。 このコマンドの詳細については、『*Cisco IOS Debug Command Reference, Release 12.4*』を参照してください。

次の表に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 *144*：アカウンティング *AV* ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	常時送信	常時送信	常時送信
属性 [4]	NAS-IP-Address	常時送信	常時送信	常時送信
属性 [5]	NAS-Port	常時送信	常時送信	常時送信
属性 [8]	Framed-IP-Address	非送信	条件に応じて送信[20]	条件に応じて送信
属性 [25]	クラス	常時送信	常時送信	常時送信
属性 [30]	Called-Station-ID	常時送信	常時送信	常時送信

属性番号	AV ペア名	START	INTERIM	STOP
属性 [31]	Calling-Station-ID	常時送信	常時送信	常時送信
属性 [40]	Acct-Status-Type	常時送信	常時送信	常時送信
属性 [41]	Acct-Delay-Time	常時送信	常時送信	常時送信
属性 [42]	Acct-Input-Octets	非送信	常時送信	常時送信
属性 [43]	Acct-Output-Octets	非送信	常時送信	常時送信
属性 [44]	Acct-Session-ID	常時送信	常時送信	常時送信
属性 [45]	Acct-Authentic	常時送信	常時送信	常時送信
属性 [46]	Acct-Session-Time	非送信	常時送信	常時送信
属性 [49]	Acct-Terminate-Cause	非送信	非送信	常時送信
属性 [61]	NAS-Port-Type	常時送信	常時送信	常時送信

20 ホストに対して有効な Dynamic Host Control Protocol（DHCP）バインディングが DHCP スヌーピング バインディング テーブルに存在している場合にのみ、Framed-IP-Address の AV ペアは送信されます。

スイッチによって送信された AV ペアは、**debug radius accounting** 特権 EXEC コマンドを入力することで表示できます。

802.1x 準備状態チェック

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。 この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。 802.1x 機能をサポートしていないデバイスでは、MAC 認証バイパスまたは Web 認証などの代替認証を使用します。

この機能が有用なのは、クライアントのサプリカントで NOTIFY EAP 通知パケットでのクエリーがサポートされている場合だけです。 クライアントは、802.1x タイムアウト値内に応答しなければなりません。

関連トピック

802.1x 準備状態チェックの設定, （1605 ページ）

スイッチと RADIUS サーバ間の通信

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。 IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。 同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホストエントリのフェールオーバーバックアップとして動作します。 RADIUS ホスト エントリは、設定した順序に従って試行されます。

関連トピック

スイッチと RADIUS サーバ間の通信の設定, （1615 ページ）

VLAN 割り当てを使用した 802.1x 認証

スイッチは、VLAN 割り当てを使用した 802.1x 認証をサポートしています。 ポートの 802.1x 認証が成功すると、RADIUS サーバは VLAN 割り当てを送信し、スイッチ ポートを設定します。 RADIUS サーバ データベースは、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに接続するクライアントのユーザ名に基づいて VLAN を割り当てます。 この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

音声デバイス認証は、Cisco IOS Release 12.2(37)SE のマルチドメイン ホスト モードでサポートされています。 Cisco IOS Release 12.2(40)SE 以降、音声デバイスが許可されており、RADIUS サーバが許可された VLAN を返した場合、割り当てられた音声 VLAN 上でパケットを送受信するようにポート上の音声 VLAN が設定されます。 音声 VLAN 割り当ては、マルチドメイン認証（MDA）対応のポートでのデータ VLAN 割り当てと同じように機能します。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 802.1x 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1x 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。 アクセス VLAN とは、アクセス ポートに割り当てられた VLAN です。 このポート上で送受信されるパケットはすべて、この VLAN に所属します。
- 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。 これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

  設定エラーには、ルーテッド ポートの VLAN、間違った VLAN ID、存在しないまたは内部（ルーテッド ポート）の VLAN ID、RSPAN VLAN、シャットダウンしている VLAN、あるいは一時停止している VLAN ID の指定などがあります。 マルチドメイン ホスト ポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行（またはその逆）のために発生するものもあります。

- 802.1x 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。
- 802.1x ポートでマルチ ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN（RADIUS サーバにより指定）に配置されます。
- ポート セキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。 マルチドメイン ホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
  - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
  - 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を dot1p または untagged に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウン ステートの場合、ポートは設定済みのアクセス VLAN に配置されます。

802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。

- あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済または割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
- 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウン ステートの場合、ポートは設定済みのアクセス VLAN に配置されます。

トランク ポート、ダイナミック ポート、または VLAN メンバーシップ ポリシー サーバ（VMPS）によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。 （アクセス ポートで 802.1x 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル属性を割り当てます。 RADIUS サーバは次の属性をスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN 名または VLAN ID
  - [83] Tunnel-Preference

  属性 [64] は、値 *VLAN*（タイプ 13）でなければなりません。 属性 [65] は、値*802*（タイプ 6）でなければなりません。 属性 [81] は、IEEE 802.1x 認証ユーザに割り当てられた *VLAN* 名または *VLAN ID* を指定します。

ユーザ単位 ACL を使用した 802.1x 認証

ユーザ単位アクセス コントロール リスト（ACL）をイネーブルにして、異なるレベルのネットワーク アクセスおよびサービスを 802.1x 認証ユーザに提供できます。 RADIUS サーバは、802.1x ポートに接続されるユーザを認証する場合、ユーザ ID に基づいて ACL 属性を受け取り、これらをスイッチに送信します。 スイッチは、ユーザ セッションの期間中、その属性を 802.1x ポートに適用します。 セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザ単位 ACL 設定が削除されます。 スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションには保存しません。 ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

ユーザは同一のスイッチ上で、ルータ ACL および入力ポート ACL を使用できます。 ただし、ポートの ACL はルータ ACL より優先されます。 入力ポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力ルータ ACL よりも優先されます。 ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。 その他のポートに着信したルーテッドパケットは、ルータ ACL によってフィルタリングされます。 発信するルーテッド パケットには、ルータ ACL のフィルタが適用されます。 コンフィギュレーションの矛盾を回避するには、RADIUS サーバに保存するユーザ プロファイルを慎重に計画しなければなりません。

RADIUS は、ベンダー固有属性などのユーザ単位属性をサポートします。 ベンダー固有属性（VSA）は、オクテットストリング形式で、認証プロセス中にスイッチに渡されます。 ユーザ単位 ACL に使用される VSA は、入力方向では inacl#<*n*> で、出力方向では outacl#<*n*> です。 MAC ACL は、入力方向に限りサポートされます。 VSA は入力方向に限りサポートされます。 レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザ単位コンフィギュレーションを定義します。 RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。 ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。 属性には、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す *.in* または *.out* が含まれています。 RADIUS サーバが *.in* または *.out* 構文を許可しない場合、アクセス リストはデフォルトで発信 ACL に適用されます。 スイッチでの Cisco IOS のアクセス リストに関するサポートが制限されているため、Filter-ID 属性は 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL および IP 拡張 ACL）に対してだけサポートされます。

ユーザ単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズにより制限されます。

ユーザ単位の ACL を設定するには、次の手順に従います。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- 802.1x ポートをシングル ホスト モードに設定します。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証

ACL およびリダイレクト URL は、ホストの 802.1x 認証または MAC 認証バイパス中に、RADIUS サーバからスイッチにダウンロードできます。 また、Web 認証中に ACL をダウンロードすることもできます。

（注） ダウンロード可能な ACL は *dACL* とも呼ばれます。

複数のホストが認証され、それらのホストがシングル ホスト モード、MDA モード、またはマルチ認証モードである場合、スイッチは ACL の送信元アドレスをホスト IP アドレスに変更します。

ACL およびリダイレクト URL は、802.1x 対応のポートに接続されるすべてのデバイスに適用できます。

ACL が 802.1x 認証中にダウンロードされない場合、スイッチは、ポートのスタティック デフォルト ACL をホストに適用します。 マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、スイッチは ACL を認証ポリシーの一部として電話にだけ適用します。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、ポート上にスタティック ACL がない場合、ダイナミックな認証デフォルト ACL が作成され、dACL がダウンロードされて適用される前にポリシーが実施されます。

（注） 認証デフォルト ACL は、実行コンフィギュレーションでは表示されません。

認証デフォルト ACL は、ポートで許可ポリシーを持つホストが 1 つ以上検出されると作成されます。 認証デフォルト ACL は、最後の認証セッションが終了すると削除されます。 認証デフォルト ACL は、**ip access-list extended auth-default-acl** グローバル コンフィギュレーション コマンドを使用して設定できます。

（注） 認証デフォルト ACL は、シングル ホスト モードの Cisco Discovery Protocol（CDP）バイパスをサポートしていません。 CDP バイパスをサポートするには、インターフェイス上のスタティック ACL を設定する必要があります。

802.1x および MAB 認証方式では、オープンおよびクローズの 2 つの認証方式がサポートされます。 クローズ認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL が作成されます。
- 認証デフォルト ACL は、ポリシーが実施されるまで DHCP トラフィックのみを許可します。
- 最初のホスト認証では、許可ポリシーは IP アドレスを挿入せずに適用されます。
- 別のホストが検出されると、最初のホストのポリシーがリフレッシュされ、最初のセッションと後続セッションのポリシーが IP アドレスを挿入して実施されます。

オープン認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL-OPEN が作成され、すべてのトラフィックが許可されます。
- セキュリティ違反を防ぐために、IP アドレスを挿入してポリシーが実施されます。
- Web 認証は、認証デフォルト ACL-OPEN に従います。

許可ポリシーのないホストへのアクセスを制御するために、ディレクティブを設定することができます。 サポートされているディレクティブの値は、*open* と *default* です。 *open* ディレクティブを設定すると、すべてのトラフィックが許可されます。 *default* ディレクティブは、ポートから提供されるアクセスにトラフィックを従わせます。 ディレクティブは、AAA サーバ上のユーザ プロファイル、またはスイッチ上のいずれかで設定できます。 AAA サーバ上でディレクティブを設定するには、**authz-directive =<open/default>** グローバル コマンドを使用します。 スイッチ上でディレクティブを設定するには、**epm access-control open** グローバル コンフィギュレーション コマンドを使用します。

（注） ディレクティブのデフォルト値は *default* です。

設定された ACL なしでポート上の Web 認証にホストがフォールバックする場合は、次のようになります。

- ポートがオープン認証モードの場合、認証デフォルト ACL-OPEN が作成されます。

- ポートがクローズ認証モードの場合、認証デフォルト ACL が作成されます。

フォールバック ACL のアクセス コントロール エントリ（ACE）は、ユーザ単位のエントリに変換されます。 設定されたフォールバック プロファイルにフォールバック ACL が含まれていない場合、ホストはポートに関連付けられた認証デフォルト ACL に従います。

（注） Web 認証でカスタム ロゴを使用し、それを外部サーバに格納する場合、認証の前にポートの ACL で外部サーバへのアクセスを許可する必要があります。 外部サーバに適切なアクセスを提供するには、スタティック ポート ACL を設定するか、認証デフォルト ACL を変更する必要があります。

Cisco Secure ACS およびリダイレクト URL の属性と値のペア

スイッチはこれらの *cisco-av-pair* VSA を使用します。

- url-redirect は HTTP URL または HTTPS URL です。
- url-redirect-acl はスイッチ ACL 名または番号です。

スイッチは、CiscoSecure-defined-ACL 属性値ペアを使用して、エンド ポイントからの HTTP または HTTPS リクエストを代行受信します。 スイッチは、クライアント Web ブラウザを指定されたリダイレクト アドレスに転送します。 Cisco Secure ACS 上の url-redirect AV ペアには、Web ブラウザがリダイレクトされる URL が格納されます。 url-redirect-acl 属性値ペアには、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号が含まれます。

（注）
- ACL の permit ACE と一致するトラフィックがリダイレクトされます。
- スイッチの URL リダイレクト ACL およびデフォルト ポート ACL を定義します。

リダイレクトURLが認証サーバのクライアントに設定される場合は、接続されるクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア

Cisco Secure ACS で、RADIUS cisco-av-pair ベンダー固有属性（VSA）を使用して、CiscoSecure-Defined-ACL 属性と値（AV）ペアを設定できます。 このペアは、#ACL#-IP-name-number 属性を使って、Cisco Secure ACS でダウンロード可能な ACL の名前を指定します。

- *name* は ACL の名前です。
- *number* はバージョン番号（たとえば 3f783768）です。

ダウンロード可能なACLが認証サーバのクライアントに設定される場合、接続されるクライアント スイッチ ポートのデフォルト ポート ACL も設定する必要があります。

デフォルト ACL がスイッチで設定されている場合、Cisco Secure ACS がホスト アクセス ポリシーをスイッチに送信すると、スイッチは、スイッチ ポートに接続されるホストからのトラフィックにこのポリシーを適用します。 ポリシーが適用されない場合、デフォルト ACL が適用されます。 Cisco Secure ACS がダウンロード可能な ACL をスイッチに送信する場合、この ACL は、スイッチ ポートに設定されているデフォルト ACL より優先されます。 ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信し、デフォルト ACL が設定されていない場合、許可失敗が宣言されます。

VLAN ID ベース MAC 認証

ダウンロード可能な VLAN ではなくスタティック VLAN ID に基づいてホストを認証する場合、VLAN ID ベース MAC 認証を使用できます。 スタティック VLAN ポリシーがスイッチで設定されている場合、認証用の各ホストの MAC アドレスとともに、VLAN 情報が IAS（Microsoft）RADIUS サーバに送信されます。 接続ポートに設定されている VLAN ID は MAC 認証に使用されます。 VLAN ID ベース MAC 認証を IAS サーバで使用することで、ネットワークで一定数の VLAN を使用できます。

機能は、STP によってモニタおよび処理される VLAN の数も制限します。 ネットワークは固定 VLAN として管理できます。

（注） この機能は Cisco ACS Server ではサポートされていません （ACS サーバは、新しいホストに送信される VLAN-ID を無視して、MAC アドレスに基づいた認証だけを行います）。

ゲスト VLAN を使用した 802.1x 認証

スイッチ上の各 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます（802.1x クライアントのダウンロードなど）。 これらのクライアントは 802.1x 認証用にシステムをアップグレードできる場合がありますが、一部のホスト（Windows 98 システムなど）は IEEE 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチは EAPOL パケット履歴を保持します。 EAPOL パケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが IEEE 802.1x 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。 インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。 EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

スイッチが 802.1x 対応の音声デバイスを許可しようとしたが、AAA サーバが使用できない場合、許可は失敗します。ただし、EAPOL パケットの検出は EAPOL 履歴に保存されます。 この音声デバイスは、AAA サーバが使用可能になると許可されます。 ただし、他のデバイスによるゲスト

VLAN へのアクセスは許可されなくなります。 この状況を防ぐには、次のいずれかのコマンドシーケンスを使用します。

- **authentication event no-response action authorize vlan***vlan-id* インターフェイス コンフィギュレーション コマンドを入力し、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。

（注） インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1x 非対応クライアントはすべてアクセスを許可されます。 ゲスト VLAN が設定されているポートに 802.1x 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、単一のホスト、複数のホスト、複数認証、またはマルチドメイン モードにおける 802.1x ポートでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x ゲスト VLAN として設定できます。 ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

スイッチは *MAC* 認証バイパス をサポートします。 MAC 認証バイパスが 802.1x ポートでイネーブルの場合、スイッチは、IEEE 802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。 スイッチは、802.1x ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。 スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。 認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。 認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。

制限付き VLAN による 802.1x 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチ スタックまたはスイッチの各 IEEE 802.1x ポートに対して制限付き VLAN（認証失敗 *VLAN* と呼ばれることもあります）を設定できます。 これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1x 対応クライアントです。 制限付き VLAN を使用すると、認証サーバの有効なクレデンシャルを持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。 管理者は制限付き VLAN のサービスを制御できます。

（注） 両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチ ポートがスパニングツリーのブロッキング ステートから変わることができなくなります。 制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。 このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。 失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。 ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。 VLAN 内のポートは設定された間隔に従って再認証を試みます（デフォルトは 60 秒）。 再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。 再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。 再認証はディセーブルにすることもできますが、 ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しない限り、ポートの認証プロセスを再起動できません。 クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。 クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の疑似メッセージがクライアントに送信されます。 このメッセージによって、繰り返し実行している再認証を停止させることができます。 クライアントによっては（Windows XP が稼働しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、すべてのホスト モードでの 802.1x ポート上、およびレイヤ 2 ポート上でサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x 制限付き VLAN として設定できます。 制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセスポート上でだけサポートされます。

ダイナミック ARP インスペクション、DHCP スヌーピング、IP 送信元ガードなどの他のセキュリティ ポート機能は、制限付き VLAN に対して個別に設定できます。

アクセス不能認証バイパスを使用した 802.1x 認証

スイッチが設定された RADIUS サーバに到達できず、新しいホストを認証できない場合、アクセス不能認証バイパス機能を使用します。この機能は、クリティカル認証または *AAA* 失敗ポリシーとも呼ばれます。 これらのホストをクリティカルポートに接続するようにスイッチを設定できます。

新しいホストがクリティカル ポートに接続しようとすると、そのホストはユーザ指定のアクセス VLAN、クリティカル *VLAN* に移動されます。 管理者はこれらのホストに制限付き認証を付与します。

スイッチは、クリティカル ポートに接続されているホストを認証しようとする場合、設定されている RADIUS サーバのステータスをチェックします。 利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。 ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワーク アクセスを許可して、ポートを認証ステートの特別なケースであるクリティカル認証ステートにします。

複数認証ポートのアクセス不能認証バイパスのサポート

ポートが任意のホスト モードで設定されていて、AAA サーバを使用できない場合、ポートはマルチホスト モードに設定され、クリティカル VLAN に移動されます。 マルチ認証（multiauth）ポートで、このアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan** *vlan-id* コマンドを使用します。 新しいホストがクリティカル ポートに接続しようとすると、そのポートは再初期化され、接続されているすべてのホストがユーザ指定のアクセス VLAN に移動されます。

このコマンドは、すべてのホスト モードでサポートされます。

アクセス不能認証バイパスの認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカル ポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカル ポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイム アウトとなり、スイッチは次の認証試行の間にクリティカル ポートをクリティカル認証ステートとします。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、クリティカル VLAN から移動するように、クリティカル ポートを設定できます。 このように設定した場合、クリティカル認証ステートのすべてのクリティカル ポートは自動的に再認証されます。

アクセス不能認証バイパス機能の相互作用

アクセス不能認証バイパスは、次の機能と相互に作用します。

- ゲスト VLAN：アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。 ゲスト VLAN が 8021.x ポートでイネーブルの場合、この機能は次のように相互に作用します。

- スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
- すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカル ポートを RADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
- すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
- すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。

- 制限付き VLAN：ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- 802.1x アカウンティング：RADIUS サーバが使用できない場合、アカウンティングは影響を受けません。
- プライベート VLAN：プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。 アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声VLAN：アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer（RSPAN）：アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

802.1x クリティカル音声 VLAN

ポートに接続されている IP Phone がアクセス コントロール サーバ（ACS）によって認証されるとき、電話機は音声ドメインに参加します。 ACS が到達不能である場合、スイッチはデバイスが音声デバイスなのかどうかを判断できません。 サーバが使用できない場合、電話機は音声ネットワークにアクセスできないため、動作できません。

データ トラフィックの場合、アクセス不能認証バイパス（クリティカル認証）を設定し、サーバが使用できない場合にトラフィックがネイティブ VLAN を通過できるようにすることができます。 RADIUS 認証サーバが使用できず（ダウンしていて）、アクセスできない認証バイパスがイネーブルの場合、スイッチは、クライアントにネットワークのアクセスを許可し、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN でポートをクリティカル認証ステートにします。 設定された RADIUS サーバにスイッチが到達できず、新しいホストを認証できない場合、スイッチはこれらのホストをクリティカル ポートに接続します。 クリティカル ポートに接続を試行している

新しいホストは、ユーザ指定のアクセス VLAN（クリティカル VLAN）に移動され、制限付き認証を許可されます。

authentication event server dead action authorize voice インターフェイス コンフィギュレーション コマンドを使用して、クリティカル音声 VLAN 機能を設定できます。 ACS が応答しない場合、ポートはクリティカル認証モードになります。 ホストからのトラフィックが音声 VLAN でタグ付けされると、接続デバイス（電話機）は、ポートに対して設定された音声 VLAN に配置されます。 IP Phone は CDP（シスコ デバイス）や LLDP または DHCP を介して音声 VLAN ID を学習します。

switchport voice vlan*vlan-id* インターフェイス コンフィギュレーション コマンドを入力して、ポートの音声 VLAN を設定できます。

この機能は、マルチドメイン モードおよびマルチ認証ホスト モードでサポートされます。 スイッチがシングルホスト モードまたはマルチホスト モードの場合にコマンドを入力できますが、デバイスがマルチドメインまたはマルチ認証ホスト モードに変わらない限りコマンドは有効になりません。

802.1x ユーザ ディストリビューション

802.1x ユーザ ディストリビューションを設定すると、複数の異なる VLAN で同じグループ名のユーザのロード バランシングを行うことができます。

VLAN は、RADIUS サーバにより提供されるか、VLAN グループ名でスイッチ CLI を介して設定します。

- RADIUS サーバを設定して、ユーザの複数の VLAN 名を送信します。 複数の VLAN 名は、ユーザへの応答の一部として送信できます。 802.1x ユーザ ディストリビューションは、特定の VLAN のすべてのユーザを追跡し、許可されたユーザをユーザ数が最も少ない VLAN に移動することでロード バランシングを行います。
- RADIUS サーバを設定してユーザの VLAN グループ名を送信します。 VLAN グループ名は、ユーザへの応答の一部として送信できます。 スイッチ CLI を使用して設定した VLAN グループ名で、選択された VLAN グループ名を検索できます。 VLAN グループ名が検出されると、この VLAN グループ名で対応する VLAN を検索して、ユーザ数が最も少ない VLAN が検出されます。 ロード バランシングは、対応する許可済みユーザをその VLAN に移動することで行われます。

（注） RADIUS サーバは、VLAN-ID、VLAN 名または VLAN グループを任意に組み合わせて VLAN 情報を送信できます。

802.1x ユーザ ディストリビューションの設定時の注意事項

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされることを確認してください。
- 複数の VLAN を VLAN グループにマッピングできます。

- VLAN を追加または削除することで、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアする場合、VLAN の認証済みポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブ VLAN がグループにマッピングされても VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内で任意の VLAN の認証ステートであるポートまたはユーザはクリアされませんが、VLAN の VLAN グループへのマッピングはクリアされます。

音声 VLAN ポートを使用した IEEE 802.1x 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の 2 つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。 VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータ トラフィックを伝送する PVID。 PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、IP Phone は IEEE 802.1x 認証とは独立して動作できます。

シングル ホスト モードでは、IP Phone だけが音声 VLAN で許可されます。 マルチ ホスト モードでは、サプリカントが PVID で認証された後、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。 マルチホストモードがイネーブルの場合、サプリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。 Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。 その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。 音声 VLAN ポートで IEEE 802.1x 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

IEEE 802.1x 認証をスイッチ ポート上でイネーブルにすると、音声 VLAN でもあるアクセス ポート VLAN を設定できます。

IP 電話がシングル ホスト モードで 802.1x 対応のスイッチ ポートに接続されている場合、スイッチは認証を行わずに電話ネットワーク アクセスを承認します。 ポートで Multidomain Authentication（MDA）を使用して、データ デバイスと IP フォンなどの音声デバイスの両方を認証することを推奨します。

（注） 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

ポート セキュリティを使用した IEEE 802.1x 認証

通常、IEEE 802.1x がイネーブルの場合に、ポートセキュリティをイネーブルにすることは推奨されません。 IEEE 802.1x ではポート単位（IP テレフォニーに MDA が設定されている場合は VLAN 単位）で単一の MAC アドレスが適用されるため、ポートセキュリティは冗長であり、場合によっては期待される IEEE 802.1x の動作と干渉することがあります。

WoL 機能を使用した IEEE 802.1x 認証

IEEE 802.1x 認証の Wake-on-LAN（WoL）機能を使用すると、スイッチにマジック パケットと呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが IEEE 802.1x ポートを通じて接続され、ホストの電源がオフになると、IEEE 802.1x ポートは無許可になります。 無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。 さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした IEEE 802.1x 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の IEEE 802.1x ポートに転送します。 ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。 ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。

（注） PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

authentication control-direction in インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向に設定すると、そのポートはスパニングツリーフォワーディング ステートに変わります。 ポートは、ホストにパケットを送信できますが、受信はできません。

authentication control-direction both インターフェイス コンフィギュレーション コマンドを使用してポートを双方向に設定すると、そのポートのアクセスが双方向で制御されます。 ポートは、ホストとの間でパケットを送受信しません。

MAC 認証バイパスを使用した IEEE 802.1x 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレスに基づいてクライアントを許可するようにスイッチを設定できます。 たとえば、プリンタなどのデバイスに接続された IEEE 802.1x ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が IEEE 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。 認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。 スイッチは、IEEE 802.1x ポート上のクライ

アントを検出した後で、クライアントからのイーサネットパケットを待機します。 スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。 認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。 許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。 このプロセスは、ほとんどのクライアント デバイスで動作します。ただし、代替の MAC アドレス形式を使用しているクライアントでは動作しません。 標準の形式とは異なる MAC アドレスを持つクライアントに対して MAB 認証をどのように実行するかや、RADIUS の設定のどこでユーザ名とパスワードが異なることが要求されるかを設定できます。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが 802.1x 対応サプリカントであることを確認し、（MAC 認証バイパス機能ではなく）802.1x 認証を使用してインターフェイスを認証します。 インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、IEEE 802.1x サプリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。 再認証が発生するときに、Termination-Action RADIUS 属性値が DEFAULT であるために前のセッションが終了した場合、スイッチはポートに設定されている認証または再認証手法を使用します。

MAC 認証バイパスで認証されたクライアントは再認証できます。 再認証プロセスは、IEEE 802.1x を使用して認証されたクライアントに対するプロセスと同じです。 再認証中は、ポートは前に割り当てられた VLAN のままです。 再認証に成功すると、スイッチはポートを同じ VLAN に保持します。 再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS 属性（Attribute[27]）、および Termination-Action RADIUS 属性（Attribute[29]）に基づいて行われるときに、Termination-Action RADIUS 属性（Attribute[29]）のアクションが *Initialize*（属性値は *DEFAULT*）である場合、MAC 認証バイパス セッションは終了し、再認証の間の接続は失われます。 MAC 認証バイパス機能が IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。 これらの AV ペアの詳細については、RFC 3580『IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- IEEE 802.1x 認証：802.1x 認証がポートでイネーブルの場合にのみ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：IEEE 802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ
- 音声 VLAN
- VLAN メンバーシップ ポリシー サーバ（VMPS）：IEEE 802.1x および VMPS は相互に排他的です。
- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。

- Network Edge Access Topology（NEAT）：MAB と NEAT は相互に排他的です。 インターフェイス上で NEAT がイネーブルの場合は、MAB をイネーブルにできません。また、インターフェイス上で MAB がイネーブルの場合は、NEAT をイネーブルにできません。

Cisco IOS Release 12.2(55)SE 以降では、冗長 MAB システム メッセージのフィルタリングをサポートします。

Network Admission Control レイヤ 2 IEEE 802.1x 検証

スイッチは、デバイスのネットワークアクセスを許可する前にエンドポイントシステムやクライアントのウイルス対策の状態またはポスチャを調べる Network Admission Control（NAC）レイヤ 2 IEEE 802.1x 検証をサポートしています。 NAC レイヤ 2 IEEE 802.1x 検証を使用すると、以下の作業を実行できます。

- Session-Timeout RADIUS 属性（属性 [27]）と Termination-Action RADIUS 属性（属性 [29]）を認証サーバからダウンロードします。
- Session-Timeout RADIUS 属性（属性 [27]）の値として再認証試行間の秒数を指定し、RADIUS サーバからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS 属性（属性[29]）を使用してクライアントを再認証する際のアクションを設定します。 値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。 値が RADIUS 要求の場合、再認証プロセスが開始します。
- VLAN の番号や名前、または VLAN グループ名のリストを Tunnel Group Private ID（属性 [81]）の値として設定し、VLAN の番号や名前、または VLAN グループ名のプリファレンスを Tunnel Preference（属性 [83]）の値として設定します。 Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID（属性 [81]）属性がリストから選択されます。
- **show authentication** 特権 EXEC コマンドを使用して、クライアントのポスチャを表示する NAC ポスチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 IEEE 802.1x 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があることを除いて、IEEE 802.1x ポートベース認証と似ています。

柔軟な認証の順序設定

柔軟な認証の順序設定を使用して、ポートが新しいホストを認証するときに使用する方法の順序を設定できます。 MAC 認証バイパスおよび 802.1x は、プライマリまたはセカンダリ認証方法として使用し、Web 認証は、これらの認証のいずれか、または両方が失敗した場合のフォールバック方法として使用できます。

関連トピック

柔軟な認証順序の設定, （1657 ページ）

Open1x 認証

Open1x認証によって、デバイスが認証される前に、そのデバイスがポートにアクセスできるようになります。 オープン認証が設定されている場合、新しいホストはポートに定義されているアクセス コントロール リスト（ACL）に基づいてトラフィックを渡します。 ホストが認証されると、RADIUS サーバに設定されているポリシーがそのホストに適用されます。

オープン認証を次の状況で設定できます。

- シングル ホスト モードでのオープン認証：1 人のユーザだけが認証の前後にネットワークにアクセスできます。
- MDA モードでのオープン認証：音声ドメインの 1 人のユーザだけ、およびデータ ドメインの 1 人のユーザだけが許可されます。
- マルチ ホスト モードでのオープン認証：任意のホストがネットワークにアクセスできます。
- 複数認証モードでのオープン認証：MDA の場合と似ていますが、複数のホストを認証できます。

（注） オープン認証が設定されている場合は、他の認証制御よりも優先されます。これは、**authentication open** インターフェイス コンフィギュレーション コマンドを使用した場合、**authentication port-control** インターフェイス コンフィギュレーション コマンドに関係なく、ポートがホストにアクセス権を付与することを意味します。

関連トピック

Open1x の設定, （1658 ページ）

マルチドメイン認証

スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチ ポート上で認証できます。 ポートはデータ ドメインと音声ドメインに分割されます。

（注） すべてのホスト モードで、ポートベース認証が設定されている場合、ライン プロトコルは許可の前にアップのままです。

MDA では、デバイス認証の順序が指定されません。 ただし、最適な結果を得るには、MDA 対応のポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA のスイッチ ポートを設定する必要があります。

- ホストモードがマルチドメインに設定されている場合、IP Phone の音声 VLAN を設定する必要があります。
- MDA 対応ポートでの音声 VLAN 割り当ては、Cisco IOS Release 12.2(40)SE 以降でサポートされています。

（注） MDA 対応のスイッチポートで音声デバイスにダイナミック VLAN を割り当てることができますが、スイッチポートに設定されたスタティック音声 VLAN が RADIUS サーバの音声デバイスに割り当てられたダイナミック VLAN と同じである場合、その音声デバイスの認証は失敗します。

- 音声デバイスを認可するには、値を *device-traffic-class=voice* に設定した Cisco 属性値（AV）ペア属性を送信するように AAA サーバを設定する必要があります。 この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応のポートのデータ デバイスだけに適用されます。 許可に失敗した音声デバイスは、データ デバイスとして扱われます。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、errordisable になります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。 他社製 IP Phone または音声デバイスはデータおよび音声 VLAN の両方に許可されます。 データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。 音声デバイスが 音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポートセキュリティ MAC アドレス制限にカウントされません。
- データ デバイスにだけ RADIUS サーバからダイナミック VLAN 割り当てを使用できます。
- MDA では、IEEE 802.1x 認証をサポートしていないデバイスへのスイッチ ポートの接続を許可するフォールバック メカニズムとして、MAC 認証バイパスを使用できます。
- データまたは音声デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。 許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスがデータ VLAN で検出された場合や、複数の音声デバイスが音声 VLAN で検出された場合、ポートは errdisable になります。
- ポートのホスト モードをシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変更すると、ポートでは許可されたデータ デバイスは許可されたままになります。 ただし、ポートの音声 VLAN で許可されている Cisco IP Phone は自動的に削除されるので、そのポートでは再認証を行う必要があります。
- ゲスト VLAN や制限付き VLAN などのアクティブ フォールバック メカニズムは、ポートをシングル モードまたはマルチホスト モードからマルチドメイン モードに変更したあとでも設定されたままになります。

- ポートのホスト モードをマルチドメイン モードからシングル モードまたはマルチホスト モードに変更すると、許可されているすべてのデバイスがポートから削除されます。
- まずデータ ドメインを許可してゲスト VLAN に参加させる場合、IEEE 802.1x 非対応の音声デバイスは、音声 VLAN のパケットをタグ付けして、認証を開始する必要があります。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。 ユーザ単位 ACL ポリシーを備えた、許可されたデバイスは、ポートの音声 VLAN とデータ VLAN の両方のトラフィックに影響を与えることがあります。 このようなデバイスを使用する場合は、ポートでユーザ単位 ACL を適用するデバイスは 1 台だけにしてください。

Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ

Network Edge Access Topology（NEAT）機能は、ワイヤリング クローゼット（会議室など）外の領域まで識別を拡張します。 これにより、任意のタイプのデバイスをポートで認証できます。

- 802.1x スイッチ サプリカント：802.1x サプリカント機能を使用することで、別のスイッチのサプリカントとして機能するようにスイッチを設定できます。 この設定は、たとえば、スイッチがワイヤリング クローゼット外にあり、トランク ポートを介してアップストリーム スイッチに接続される場合に役に立ちます。 802.1x スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチで認証します。 サプリカント スイッチが認証に成功すると、ポート モードがアクセスからトランクに変更されます。
- アクセス VLAN は、オーセンティケータ スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

デフォルトでは、BPDU ガードがイネーブルにされたオーセンティケータ スイッチにサプリカントのスイッチを接続する場合、オーセンティケータのポートはサプリカント スイッチが認証する前にスパニングツリー プロトコル（STP）のブリッジ プロトコル データ ユニット（BPDU）を受信した場合、errdisable 状態になる可能性があります。 Cisco IOS Release 15.0(1) SE 以降では、認証中にサプリカントのポートから送信されるトラフィックを制御できます。 **dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証が完了する前にオーセンティケータ ポートがシャットダウンすることがないように、認証中に一時的にサプリカントのポートをブロックします。 認証に失敗すると、サプリカントのポートが開きます。 **no dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証期間中にサプリカント ポートが開きます。 これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドによりオーセンティケータのスイッチ ポートでイネーブルになっている場合、サプリカント スイッチで **dot1x supplicant controlled transient** コマンドを使用することを強く推奨します。

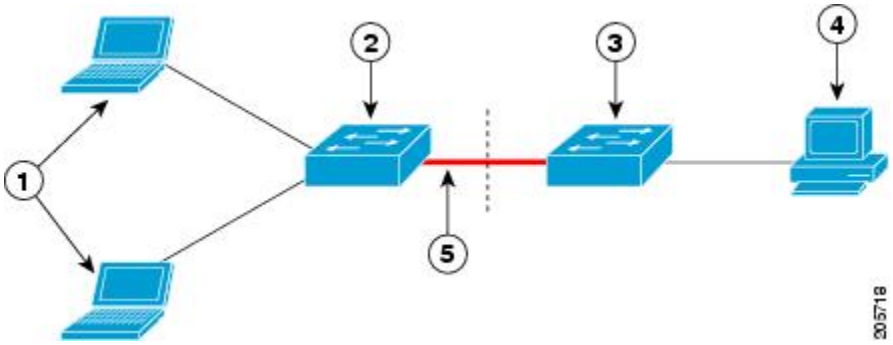
（注） **spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用して、グローバルにオーセンティケータ スイッチで BPDU ガードをイネーブルにした場合、**dot1x supplicant controlled transient** コマンドを入力すると、BPDU の違反が避けられなくなります。

1 つ以上のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで MDA または multiauth モードをイネーブルにできます。 マルチホスト モードはオーセンティケータ スイッチ インターフェイスではサポートされていません。

すべてのホスト モードで機能するように **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを Network Edge Access Topology（NEAT）のサプリカント スイッチで使用します。

- ホスト許可：許可済み（サプリカントでスイッチに接続する）ホストからのトラフィックだけがネットワークで許可されます。 これらのスイッチは、Client Information Signalling Protocol（CISP）を使用して、サプリカント スイッチに接続する MAC アドレスをオーセンティケータ スイッチに送信します。
- 自動イネーブル化：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的にイネーブル化します。これにより、サプリカントスイッチから着信する複数のVLANのユーザ トラフィックが許可されます。 ACS で cisco-av-pair を *device-traffic-class=switch* として設定します （この設定は *group* または *user* 設定で行うことができます）。

図 *109*：*CISP* を使用したオーセンティケータまたはサプリカント スイッチ



1	ワークステーション（クライアント）	2	サプリカント スイッチ（ワイヤリング クローゼット外）
3	オーセンティケータ スイッチ	4	Access Control Server（ACS）
5	トランク ポート		

（注） **switchport nonegotiate** コマンドは、NEAT を使用したサプリカントおよびオーセンティケータスイッチではサポートされません。 このコマンドは、トポロジのサプリカント側で設定しないでください。 オーセンティケータ サーバ側で設定した場合は、内部マクロによってポートからこのコマンドが自動的に削除されます。

音声認識 802.1x セキュリティ

（注） 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにするようにスイッチを設定します。 以前のリリースでは、セキュリティ違反の原因であるデータ クライアントを認証しようとすると、ポート全体がシャットダウンし、接続が完全に切断されます。

この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。 データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。 音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

関連トピック

音声認識 802.1x セキュリティの設定, （1607 ページ）

コモン セッション ID

認証マネージャは、使用された認証方式が何であれ、クライアントの単一のセッション ID（共通セッション ID）を使用します。 この ID は、表示コマンドや MIB などのすべてのレポートに使用されます。 セッション ID は、セッション単位のすべての Syslog メッセージに表示されます。

セッション ID には、次の情報が含まれます。

- ネットワーク アクセス デバイス（NAD）の IP アドレス
- 一意の 32 ビット整数（機械的に増加します）
- セッション開始タイム スタンプ（32 ビット整数）

次に、show authentication コマンドの出力に表示されたセッション ID の例を示します。 この例では、セッション ID は 160000050000000B288508E5 です。

```
Switch# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

次に、Syslog 出力にセッション ID が表示される例を示します。 この例でも、セッション ID は 160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

セッション ID は、NAD、AAA サーバ、その他のレポート分析アプリケーションでクライアントを識別するために使用されます。 ID は自動的に表示されます。 設定は必要ありません。

802.1x ポートベース認証の設定方法

802.1x 認証のデフォルト設定

表 *145*：*802.1x* 認証のデフォルト設定

機能	デフォルト設定
スイッチの 802.1x イネーブル ステート	ディセーブル
ポート単位の 802.1x イネーブル ステート	ディセーブル（force-authorized） ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • Key	• 指定なし • 1812 • 指定なし
ホスト モード	シングル ホスト モード
制御方向	双方向制御
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
再認証回数	2 回（ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数）

機能	デフォルト設定
待機時間	60 秒（スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数）
再送信時間	30 秒（スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数）
最大再送信回数	2 回（スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数）
クライアント タイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間）
認証サーバ タイムアウト時間	30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間） dot1x timeout server-timeout インターフェイス コンフィギュレーション コマンドを使用して、このタイムアウト時間を変更できます。
無活動タイムアウト	ディセーブル
ゲスト VLAN	指定なし
アクセス不能認証バイパス	ディセーブル
制限付き VLAN	指定なし
オーセンティケータ（スイッチ）モード	指定なし
MAC 認証バイパス	ディセーブル
音声認識セキュリティ	ディセーブル

802.1x 認証設定時の注意事項

802.1X 認証

802.1x 認証を設定する場合の注意事項は、次のとおりです。

- 802.1x 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。 たとえば、ポートが RADIUS サーバに割り当てられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

  802.1x ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。 たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除された後、ポートは無許可になります。
- 802.1x プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポート タイプではサポートされません。
  - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。 ダイナミック ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。 802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
  - EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバを 802.1x ポートとして設定しないでください。 EtherChannel ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。
  - スイッチド ポート アナライザ（SPAN）およびリモート SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートの 802.1x 認証をイネーブルにすることができます。 ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1x 認証はディセーブルになります。 SPAN または RSPAN 送信元ポートでは 802.1x 認証をイネーブルにすることができます。
- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x 認証をグローバルにイネーブルにする前に、802.1x 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- Cisco IOS Release 12.2(55)SE 以降のリリースでは、802.1x 認証に関連するシステム メッセージのフィルタリングがサポートされています。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、およびアクセス不能認証バイパス設定時の注意事項は、次のとおりです。

- 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x ゲスト VLAN として設定できます。 ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。
- DHCP クライアントが接続されている 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。 クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1x 認証プロセスを再起動する設定を変更できます。 802.1x 認証プロセスの設定を軽減します（**authentication timer inactivity** および **authentication timer reauthentication** インターフェイス コンフィギュレーション コマンド）。 設定の減少量は、接続された 802.1x クライアントのタイプによって異なります。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
  - この機能はシングル ホスト モードおよびマルチホスト モードの 802.1x ポートでサポートされます。
  - Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステートの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
  - Windows XP クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。
  - アクセス不能認証バイパス機能および制限 VLAN を 802.1x ポート上に設定できます。スイッチが制限付き VLAN 内でクリティカル ポートを再認証しようとし、すべての RADIUS サーバが利用不可能な場合、スイッチはポート ステートをクリティカル認証ステートに変更し、制限付き VLAN に残ります。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定できます。 制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

MAC 認証バイパス

MAC 認証バイパス設定時の注意事項は次のとおりです。

- 特に明記していないかぎり、MAC認証バイパスの注意事項は802.1x認証のものと同じです。
- ポートが MAC アドレスで許可された後に、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバ データベースにない場合、ポートは未許可ステートのままです。 ただし、クライアント MAC アドレスが

データベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。

- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を設定できます。 指定できる範囲は 1 ～ 65535 秒です。

ポートあたりのデバイスの最大数

802.1x 対応のポートに接続できるデバイスの最大数です。

- シングル ホスト モードの場合、アクセス VLAN で接続できるデバイスは 1 台だけです。 ポートが音声 VLAN でも設定されている場合、音声 VLAN を介して送受信できる Cisco IP Phone の数には制限はありません。
- マルチドメイン認証（MDA）モードの場合、アクセス VLAN で 1 台のデバイス、音声 VLAN で 1 台の IP Phone が許可されます。
- マルチホスト モードでは、1 つの 802.1x サプリカントだけがポートで許可されますが、非 802.1x ホストは数に制限なく、アクセス VLAN で許可されます。 音声 VLAN で許可されるデバイスの数には制限はありません。

802.1x 準備状態チェックの設定

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。 この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。

802.1x 準備状態チェックは、802.1x で設定できるすべてのポートで使用できます。 準備状態チェックは、**dot1x force-unauthorized** として設定されるポートでは使用できません。

802.1x 準備状態チェックをスイッチでイネーブルにする場合には、次の手順に従ってください。

はじめる前に

準備状態チェックをスイッチでイネーブルにする場合、次の注意事項に従ってください。

- 準備状態チェックは通常、802.1x がスイッチでイネーブルにされる前に使用されます。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用すると、スイッチ スタックのすべてのポートがテストされます。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。 クライアントが通知パケットに応答すると、802.1x 対応です。 クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。 クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。 Syslog メッセージは生成されません。

- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。 クライアントが通知パケットに応答すると、802.1x 対応です。 クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。 クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。 Syslog メッセージは生成されません。
- 準備状態チェックは、複数のホスト（たとえば、IP Phone に接続される PC）を扱うポートに送信できます。 Syslog メッセージは、タイマー時間内に準備状態チェックに応答する各クライアントに生成されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **dot1x test eapol-capable** [**interface***interface-id*]
4. **dot1x test timeout***timeout*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

ステップ 3	**dot1x test eapol-capable** [**interface***interface-id*]
	
	例：
	`Switch# dot1x test eapol-capable interface gigabitethernet1/0/13`
	`DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable`
		スイッチ上で 802.1x 準備状態チェックをイネーブルにします。
		
		（任意）*interface-id* では、IEEE 802.1x の準備状態をチェックするポートを指定します。
		
		（注） オプションの **interface** キーワードを省略した場合、スイッチのすべてのインターフェイスがテストされます。

	コマンドまたはアクション	目的
ステップ 4	**dot1x test timeout***timeout*	（任意）EAPOL 応答の待機に使用するタイムアウトを設定します。 範囲は 1 ～ 65535 秒です。 デフォルトは 10 秒です。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

802.1x 準備状態チェック，（1579 ページ）

音声認識 802.1x セキュリティの設定

（注） 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能をスイッチで使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにします。 この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。 データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。 音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

スイッチで音声認識 802.1x 音声セキュリティを設定する場合、次の注意事項に従ってください。

- **errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力して、音声認識 802.1x セキュリティをイネーブルにします。 音声認識 802.1x

セキュリティをディセーブルにするには、このコマンドの **no** バージョンを入力します。 このコマンドは、スイッチの 802.1x 設定ポートのすべてに適用されます。

（注） **shutdown vlan** キーワードを指定しない場合、error-disabled ステートになったときにポート全体がシャットダウンされます。

- **errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して、error-disabled リカバリを設定すると、ポートは自動的に再びイネーブルにされます。error-disabled リカバリがポートで設定されていない場合、**shutdown** および **no-shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。
- 個々の VLAN を再びイネーブルにするには、**clear errdisable interface***interface-id***vlan** [*vlan-list*] 特権 EXEC コマンドを使用します。 範囲を指定しない場合、ポートのすべての VLAN がイネーブルにされます。

音声認識 802.1x セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **errdisable detect cause security-violation shutdown vlan**
3. **errdisable recovery cause security-violation**
4. **clear errdisable interface***interface-id***vlan***[vlan-list]*
5. 次を入力します。
   - **shutdown**
   - **no shutdown**
6. **end**
7. **show errdisable detect**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**errdisable detect cause security-violation shutdown vlan**	セキュリティ違反エラーが発生したすべての VLAN をシャットダウンします。 （注） **shutdown vlan** キーワードを指定しない場合、すべてのポートが errdisable ステートになり、シャットダウンされます。

	コマンドまたはアクション	目的
ステップ 3	**errdisable recovery cause security-violation**	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**clear errdisable interface***interface-id***vlan***[vlan-list]*	（任意）errordisable になっている個々の VLAN を再びイネーブルにします。 • interface-id の場合、個々の VLAN を再びイネーブルにするポートを指定します。 • （任意）vlan-list の場合、再びイネーブルにする VLAN のリストを指定します。 vlan-list を指定しない場合は、すべての VLAN が再びイネーブルになります。
ステップ 5	次を入力します。 • **shutdown** • **no shutdown**	（任意）errordisable の VLAN を再びイネーブルにして、すべての errordisable 指示をクリアします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show errdisable detect**	入力内容を確認します。

次に、セキュリティ違反エラーが発生した任意の VLAN をシャットダウンするようにスイッチを設定する例を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次に、ポート ギガビット イーサネット 40/2 で errdisable ステートであったすべての VLAN を再度イネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet4/0/2
vlan
```

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

関連トピック

音声認識 802.1x セキュリティ，（1600 ページ）

802.1x 違反モードの設定

次に示す状況で、シャットダウン、Syslog エラーを生成、または新しいデバイスからのパケットを廃棄するように 802.1x ポートを設定できます。

- デバイスが 802.1x 対応のポートに接続した
- ポートで認証されるデバイスの最大数に達した

スイッチ上にセキュリティ違反アクションを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **aaa new-model**
3. **aaa authentication dot1x** {**default**} *method1*
4. **interface** *interface-id*
5. **switchport mode access**
6. **authentication violation** {**shutdown** | **restrict** | **protect** | **replace**}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1* 例： `Switch(config)# aaa authentication dot1x default group radius`	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。 （注） **group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4	**interface** *interface-id* 例： `Switch(config)# interface`	IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	gigabitethernet1/0/4	
ステップ 5	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	ポートをアクセス モードに設定します。
ステップ 6	**authentication violation {shutdown | restrict | protect | replace}** 例： `Switch(config-if)# authentication violation restrict`	違反モードを設定します。 キーワードの意味は次のとおりです。 • **shutdown**：ポートを errordisable にします。 • **restrict**：syslog エラーを生成します。 • **protect**：トラフィックをポートに送信するすべての新しいデバイスからパケットをドロップします。 • **replace**：現在のセッションを削除し、新しいホストで認証します。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

802.1X 認証の設定

ユーザ単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1x の AAA プロセスを示します。

はじめる前に

802.1x ポートベース認証を設定するには、認証、許可、アカウンティング（AAA）をイネーブルにして認証方式リストを指定する必要があります。 方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

手順の概要

1. ユーザがスイッチのポートに接続します。
2. 認証が実行されます。
3. RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。
4. スイッチが開始メッセージをアカウンティング サーバに送信します。
5. 必要に応じて、再認証が実行されます。
6. スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバに送信します。
7. ユーザがポートから切断します。
8. スイッチが停止メッセージをアカウンティング サーバに送信します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ユーザがスイッチのポートに接続します。	
ステップ 2	認証が実行されます。	
ステップ 3	RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。	
ステップ 4	スイッチが開始メッセージをアカウンティング サーバに送信します。	
ステップ 5	必要に応じて、再認証が実行されます。	
ステップ 6	スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバに送信します。	
ステップ 7	ユーザがポートから切断します。	
ステップ 8	スイッチが停止メッセージをアカウンティング サーバに送信します。	

802.1x ポートベース認証の設定

802.1x ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **aaa new-model**
3. **aaa authentication dot1x** {**default**} *method1*
4. **dot1x system-auth-control**
5. **aaa authorization network** {**default**} **group radius**
6. **radius-server host** *ip-address*
7. **radius-server key** *string*
8. **interface** *interface-i*d
9. **switchport mode access**
10. **authentication port-control auto**
11. **dot1x pae authenticator**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1* 例： `Switch(config)# aaa authentication dot1x default group radius`	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。 デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。 （注） **group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

	コマンドまたはアクション	目的
ステップ 4	**dot1x system-auth-control** 例： `Switch(config)# dot1x system-auth-control`	スイッチで802.1x認証をグローバルにイネーブルにします。
ステップ 5	**aaa authorization network {default} group radius** 例： `Switch(config)# aaa authorization network default group radius`	（任意）ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザRADIUS許可をスイッチに設定します。 （注） ユーザ単位ACLを設定するには、シングルホストモードを設定する必要があります。 この設定は、デフォルトです。
ステップ 6	**radius-server host** *ip-address* 例： `Switch(config)# radius-server host 124.2.2.12`	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 7	**radius-server key** *string* 例： `Switch(config)# radius-server key abc1234`	（任意）RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。
ステップ 8	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	（任意）ステップ 6 および 7 で RADIUS サーバを設定した場合のみ、ポートをアクセス モードに設定します。
ステップ 10	**authentication port-control auto** 例： `Switch(config-if)# authentication port-control auto`	ポートでの 802.1x 認証をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**dot1x pae authenticator** 例： `Switch(config-if)# dot1x pae authenticator`	インターフェイスのポート アクセス エンティティを、オーセンティケータとしてのみ動作し、サプリカント用のメッセージは無視するように設定します。
ステップ 12	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

スイッチと RADIUS サーバ間の通信の設定

radius-server host グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号化キーの値を、すべての RADIUS サーバにグローバルに設定できます。 これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。 これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングがあります。 詳細については、RADIUS サーバのマニュアルを参照してください。

スイッチで RADIUS サーバのパラメータを設定するには、次の手順を実行します。 この手順は必須です。

はじめる前に

認証、許可、およびアカウンティング（AAA）をイネーブルにし、認証方式リストを指定する必要があります。 方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-server host** {*hostname* | *ip-address*} **auth-port***port-number***key***string*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} **auth-port***port-number***key***string* 例： `Switch(config)# radius-server host 125.5.5.43 auth-port 1812 key string`	RADIUS サーバ パラメータを設定します。 *hostname* | *ip-address* には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **auth-port***port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1812 です。 指定できる範囲は 0 ～ 65536 です。 **key***string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。 キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 （注） キーの先行スペースは無視されますが、途中および末尾のスペースは有効なので、キーは必ず **radius-server host** コマンド構文の最後の項目として設定してください。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 キーは RADIUS デーモンで使用する暗号に一致している必要があります。 複数の RADIUS サーバを使用する場合には、このコマンドを繰り返し入力します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

スイッチと RADIUS サーバ間の通信, （1580 ページ）

ホスト モードの設定

authentication port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている IEEE 802.1x 許可ポート上で、複数のホスト（クライアント）を許可するには、特権 EXEC モードで次の手順を実行します。 MDA を設定してイネーブルにするには、**multi-domain** キーワードを使用します。これにより、ホスト デバイス、および IP Phone（シスコ製または他社製）など音声デバイスの両方が同じスイッチ ポートで許可されます。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] 例： `Switch(config-if)# authentication host-mode multi-host`	単一の 802.1x 許可ポートで複数のホスト（クライアント）を許可することができます。 キーワードの意味は次のとおりです。 • **multi-auth**：音声 VLAN で 1 クライアント、データ VLAN で複数の認証クライアントを許可します。 （注） **multi-auth** キーワードを使用できるのは、**authentication host-mode** コマンドだけです。 • **multi-host**：シングル ホストの認証後に 802.1x 許可ポートで複数のホストの接続を許可します。 • **multi-domain**：ホスト デバイスと IP Phone（シスコ製または他社製）など音声デバイスの両方が、IEEE 802.1x 許可ポートで認証されるようにします。

	コマンドまたはアクション	目的
		（注） ホストモードが **multi-domain** に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。 指定したインターフェイスで **authentication port-control** インターフェイスコンフィギュレーションコマンドが **auto** に設定されていることを確認してください。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

定期的な再認証の設定

802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。 再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証を行う間隔（秒）を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **authentication periodic**
4. **authentication timer** {{[**inactivity** | **reauthenticate** | **restart**]} {*value*}}
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication periodic** 例： `Switch(config-if)# authentication periodic`	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。 （注） デフォルト値は 3600 秒です。 再認証タイマーの値を変更するか、スイッチでRADIUS-providedセッションタイムアウトを使用するようにするには、**authentication timer reauthenticate** コマンドを入力します。
ステップ 4	**authentication timer** {{[**inactivity** | **reauthenticate** | **restart**]} {*value*}} 例： `Switch(config-if)# authentication timer reauthenticate 180`	再認証の試行の間隔（秒）を設定します。 **authentication timer** キーワードの意味は次のとおりです。 • **inactivity**：クライアントからのアクティビティがなくなり無許可になるまでの間隔（秒単位）。 • **reauthenticate**：自動再認証試行が開始されるまでの時間（秒） • **restart** *value*：無許可ポートの認証を試行するまでの間隔（秒単位）。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。 **authentication timer inactivity** インターフェイス コンフィギュレーション コマンドは、アイドル状態の期間を制御します。 認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。 デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **authentication timer inactivity** *seconds*
4. **end**
5. **show authentication sessions interface** *interface-id*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication timer inactivity** *seconds* 例： `Switch(config-if)# authentication timer inactivity 30`	クライアントとの認証のやり取りに失敗した場合に、スイッチが待機状態のままでいる秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 60 秒です。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show authentication sessions interface** *interface-id* 例： `Switch# show authentication sessions interface gigabitethernet2/0/1`	入力を確認します。

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

スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。 スイッチがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、その後フレームを再送信します。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチがクライアントからの通知を待機する時間を変更するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **authentication timer reauthenticate** *seconds*
4. **end**
5. **show authentication sessions interface** *interface-id*
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication timer reauthenticate** *seconds* 例： `Switch(config-if)# authentication timer reauthenticate 60`	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 5 秒です。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show authentication sessions interface** *interface-id* 例： `Switch# show authentication sessions interface gigabitethernet2/0/1`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチからクライアントへのフレーム再送信回数の設定

スイッチからクライアントへの再送信時間を変更できるだけでなく、（クライアントから応答が得られなかった場合に）スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチからクライアントへのフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **dot1x max-reauth-req** *count*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-req** *count* 例： `Switch(config-if)# dot1x max-reauth-req 5`	スイッチが認証処理を再開するまでに、クライアントへ EAP 要求/アイデンティティ フレームを送信する回数を変更できます。 指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

再認証回数の設定

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **dot1x max-req** *count*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**dot1x max-req** *count* 例： `Switch(config-if)# dot1x max-req 4`	ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。 指定できる範囲は 0 ～ 10 です。デフォルトは 2 です。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

MAC 移動のイネーブル化

MAC 移動を使用すると、認証されたホストをスイッチのポート間で移動できます。

スイッチで MAC 移動をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **authentication mac-move permit**
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**authentication mac-move permit** 例： `Switch(config)# authentication mac-move permit`	スイッチで MAC 移動をイネーブルにします。 デフォルトは deny です。 セッション認識ネットワーク モードでは、デフォルト CLI は **access-session mac-move deny** です。 セッション認識ネットワークで MAC 移動をイネーブルにするには、**no access-session mac-move** グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

MAC 置換のイネーブル化

MAC 置換を使用すると、ホストはポート上の認証ホストを置換できます。

インターフェイス上で MAC 置換をイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **authentication violation** {**protect** | **replace** | **restrict** | **shutdown**}
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication violation** {**protect** | **replace** | **restrict** | **shutdown**} 例： `Switch(config-if)# authentication violation replace`	インターフェイス上でMAC置換をイネーブルにするには、**replace** キーワードを使用します。 ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。 他のキーワードは、次のような機能があります。 • **protect**：ポートは、システム メッセージを生成せずに、予期しない MAC を使用するパケットをドロップします。 • **restrict**：違反パケットが CPU によってドロップされ、システム メッセージが生成されます。 • **shutdown**：ポートは、予期しない MAC アドレスを受信すると error disabled になります。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

IEEE 802.1x アカウンティングの設定

802.1xアカウンティングを使用して、AAAシステムアカウンティングをイネーブルにすると、ロギングのためにシステムリロードイベントをアカウンティングRADIUSサーバに送信できます。サーバは、アクティブな802.1xセッションすべてが終了したものと判断します。

RADIUSは信頼性の低いUDPトランスポートプロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティングメッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチがRADIUSサーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップメッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

（注） ロギングの開始、停止、仮のアップデートメッセージ、タイムスタンプなどのアカウンティングタスクを実行するように、RADIUSサーバを設定する必要があります。 これらの機能をオンにするには、RADIUSサーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。 次に、RADIUSサーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

AAAがスイッチでイネーブルになった後、802.1xアカウンティングを設定するには、特権EXECモードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **aaa accounting dot1x default start-stop group radius**
4. **aaa accounting system default start-stop group radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/3`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting dot1x default start-stop group radius** 例： `Switch(config-if)# aaa accounting dot1x default start-stop group radius`	すべての RADIUS サーバのリストを使用して 802.1x アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting system default start-stop group radius** 例： `Switch(config-if)# aaa accounting system default start-stop group radius`	（任意）システムアカウンティングをイネーブルにし（すべての RADIUS サーバのリストを使用）、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1x 対応でないクライアントはゲスト VLAN に配置されます。 802.1x 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。 スイッチは、シングル ホスト モードまたはマルチ ホスト モードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. 次のいずれかを使用します。
   - **switchport mode access**
   - **switchport mode private-vlan host**
4. **authentication event no-response action authorize vlan***vlan-id*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **switchport mode access** • **switchport mode private-vlan host**	• ポートをアクセス モードに設定します。 • レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。

	コマンドまたはアクション	目的
	例： `Switch(config-if)# switchport mode private-vlan host`	
ステップ 4	**authentication event no-response action authorize vlan***vlan-id* 例： `Switch(config-if)# authentication event no-response action authorize vlan 2`	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。 指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

制限付き VLAN の設定

スイッチ スタックまたはスイッチ上に制限付き VLAN を設定している場合、認証サーバが有効なユーザ名またはパスワードを受信できないと、IEEE 802.1x に準拠しているクライアントは制限付き VLAN に移されます。 スイッチは、シングル ホスト モードでのみ制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. 次のいずれかを使用します。
   - **switchport mode access**
   - **switchport mode private-vlan host**
4. **authentication port-control auto**
5. **authentication event fail action authorize vlan***vlan-id*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/2`	設定するポートを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **switchport mode access** • **switchport mode private-vlan host** 例： `Switch(config-if)# switchport mode access`	• ポートをアクセス モードに設定します。 • レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** 例： `Switch(config-if)# authentication port-control auto`	ポートでの 802.1x 認証をイネーブルにします。
ステップ 5	**authentication event fail action authorize vlan***vlan-id* 例： `Switch(config-if)# authentication event fail action authorize vlan 2`	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。 指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

制限付き VLAN の認証試行回数の設定

ユーザを制限付き VLAN に割り当てる前に、**authentication event retry***retry count* インターフェイス コンフィギュレーション コマンドを使用して、認証試行の最大回数を設定できます。 指定できる試行回数は 1 ～ 3 です。 デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. 次のいずれかを使用します。
   - **switchport mode access**
   - **switchport mode private-vlan host**
4. **authentication port-control auto**
5. **authentication event fail action authorize vlan***vlan-id*
6. **authentication event retry***retry count*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/3`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • **switchport mode access** • **switchport mode private-vlan host** 例：	• ポートをアクセス モードに設定します。 • レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。

	コマンドまたはアクション	目的
	または `Switch(config-if)# switchport mode access`	
ステップ 4	**authentication port-control auto** 例： `Switch(config-if)# authentication port-control auto`	ポートでの 802.1x 認証をイネーブルにします。
ステップ 5	**authentication event fail action authorize vlan***vlan-id* 例： `Switch(config-if)# authentication event fail action authorize vlan 8`	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。 指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。
ステップ 6	**authentication event retry***retry count* 例： `Switch(config-if)# authentication event retry 2`	ポートが制限付き VLAN に移行するための認証試行回数を指定します。 指定できる範囲は 1 ～ 3 秒です。デフォルトは 3 回に設定されています。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定

ポートにクリティカル音声 VLAN を設定し、アクセス不能認証バイパス機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **aaa new-model**
3. **radius-server dead-criteria**{**time** *seconds* } [**tries** *number*]
4. **radius-serverdeadtime***minutes*
5. **radius-server host ip-address** *address*[**acct-port** *udp-port*][**auth-port** *udp-port*] [**testusername** *name*[**idle-time** *time*] [**ignore-acct-port**][**ignore auth-port**]] [**key** *string*]
6. **dot1x critical** {**eapol** | **recovery delay** *milliseconds*}
7. **interface** *interface-id*
8. **authentication event server dead action** {**authorize** | **reinitialize**} **vlan** *vlan-id*]
9. **switchport voice vlan** *vlan-id*
10. **authentication event server dead action authorize voice**
11. **show authentication interface** *interface-id*
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	**radius-server dead-criteria**{**time** *seconds* } [**tries** *number*] 例： `Switch(config)# radius-server dead-criteria time 20 tries 10`	RADIUS サーバが使用不可またはダウン（切断）と見なされる条件を設定します。 • **time**：1 ～ 120 秒。 スイッチは、デフォルトの *seconds* 値を 10 ～ 60 の間で動的に決定します。 • **number**：1 ～ 100 の試行回数。 スイッチは、デフォルトの **tries***number* を 10 ～ 100 の間で動的に決定します。
ステップ 4	**radius-serverdeadtime***minutes* 例： `Switch(config)# radius-server`	（任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分（24 時間）です。 デフォルト値は 0 分です。

	コマンドまたはアクション	目的
	deadtime 60	
ステップ 5	**radius-server host ip-address** *address*[**acct-port** *udp-port*][**auth-port** *udp-port*] [**testusername** *name*[**idle-time** *time*] [**ignore-acct-port**][**ignore auth-port**]] [**key** *string*] 例： `Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username user1 idle-time 30 key abc1234`	（任意）次のキーワードを使用してRADIUSサーバパラメータを設定します。 • **acct-port***udp-port*：RADIUS アカウンティング サーバの UDP ポートを指定します。 UDP ポート番号の範囲は 0 ～ 65536 です。 デフォルトは 1646 です。 • **auth-port***udp-port*：RADIUS 認証サーバの UDP ポートを指定します。 UDP ポート番号の範囲は 0 ～ 65536 です。 デフォルトは 1645 です。 （注） RADIUS アカウンティング サーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。 • **test username***name*：RADIUS サーバ ステータスの自動テストをイネーブルにして、使用するユーザ名を指定します。 • **idle-time** time：スイッチがテスト パケットをサーバに送信した後の間隔を分数で設定します。 範囲は 1 ～ 35791 分です。 デフォルトは 60 分（1 時間）です。 • **ignore-acct-port**：RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。 • **ignore-auth-port**：RADIUS サーバ認証ポートのテストをディセーブルにします。 • **key***string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。 キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 （注） キーの先行スペースは無視されますが、途中および末尾のスペースは有効なので、キーは必ず **radius-server host** コマンド構文の最後の項目として設定してください。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 キーは RADIUS デーモンで使用する暗号に一致している必要があります。 **radius-server key** {**0**string | **7***string* | *string*} グローバル コンフィギュレーション コマンドを使用しても認証および暗号キーを設定できます。

	コマンドまたはアクション	目的

ステップ 6	**dot1x critical** {**eapol** | **recovery delay** *milliseconds*}
	
	例：
	
	`Switch(config)# dot1x critical eapol`
	`(config)# dot1x critical recovery delay 2000`
		（任意）アクセス不能認証バイパスのパラメータを設定します。
		• **eapol**：スイッチがクリティカルポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。
		• **recovery delay***milliseconds*：使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカルポートを再初期化するために待機する回復遅延期間を設定します。 指定できる範囲は 1 ～ 10000 ミリ秒です。 デフォルトは 1000 ミリ秒です（ポートは毎秒再初期化できます）。

ステップ 7	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**authentication event server dead action** {**authorize** | **reinitialize**} **vlan** *vlan-id*] 例： `Switch(config-if)# authentication event server dead action reinitialicze vlan 20`	これらのキーワードを使用して、RADIUS サーバが到達不能な場合にポートでホストを移動します。 • **authorize**：認証しようとする新しいホストをユーザ指定のクリティカル VLAN に移動します。 • **reinitialize**：ポートのすべての許可済みホストをユーザ指定のクリティカル VLAN に移動します。
ステップ 9	**switchport voice vlan** *vlan-id* 例： `Switch(config-if)# switchport voice vlan`	ポートの音声 VLAN を指定します。 音声 VLAN はステップ 6 で設定されたクリティカル データ VLAN と同じにはできません。
ステップ 10	**authentication event server dead action authorize voice** 例： `Switch(config-if)# authentication event server dead action authorize voice`	RADIUS サーバが到達不能な場合、ポートのデータ トラフィックを音声 VLAN に移動するために、クリティカル音声 VLAN を設定します。
ステップ 11	**show authentication interface** *interface-id*	（任意）設定を確認します。

	コマンドまたはアクション	目的
	例： `Switch(config-if)# do show authentication interface gigabit 1/0/1`	
ステップ 12	**copy running-config startup-config** 例： `Switch(config-if)# do copy running-config startup-config`	（任意）設定を確認します。

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server host** グローバル コンフィギュレーション コマンドを使用します。 アクセス不能な認証バイパスをディセーブルにするには、**no authentication event server dead action** インターフェイス コンフィギュレーション コマンドを使用します。 クリティカル音声 VLAN をディセーブルにするには、**authentication event server dead action authorize voice** インターフェイス コンフィギュレーション コマンドを使用します。

アクセス不能認証バイパスの設定例

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username user1
 idle-time 30 key abc1234
Switch(config)# dot1x critical eapol
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

WoL を使用した 802.1x 認証の設定

WoL を使用した 802.1x 認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **authentication control-direction** {**both** | **in**}
4. **end**
5. **show authentication sessions interface** *interface-id*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/3`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication control-direction** {**both** | **in**} 例： `Switch(config-if)# authentication control-direction both`	ポートで WoL を使用して 802.1x 認証をイネーブルにし、次のキーワードを使用してポートを双方向または単方向に設定します。 • **both**：ポートを双方向に設定します。 ポートは、ホストにパケットを送受信できません。 デフォルトでは、ポートは双方向です。 • **in**：ポートを単方向に設定します。 ポートは、ホストにパケットを送信できますが、受信はできません。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show authentication sessions interface** *interface-id*	入力を確認します。

	コマンドまたはアクション	目的
	例： `Switch# show authentication sessions interface gigabitethernet2/0/3`	
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **authentication port-control auto**
4. **mab** [**eap**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**authentication port-control auto** 例： `Switch(config-if)# authentication port-control auto`	ポートでの 802.1x 認証をイネーブルにします。
ステップ 4	**mab** [**eap**] 例： `Switch(config-if)# mab`	MAC 認証バイパスをイネーブルにします。 （任意）**eap** キーワードを使用して、スイッチが認可に EAP を使用するように設定します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

MAC 認証バイパスのユーザ名とパスワードの形式作成

オプションの **mab request format** コマンドを使用して認証サーバによって受け入れられる形式で MAB のユーザ名とパスワードをフォーマットします。 ユーザ名とパスワードは通常、クライアントの MAC アドレスです。 認証サーバ設定の中には、ユーザ名と異なるパスワードを必要とするものがあります。

MAC 認証バイパス ユーザ名およびパスワードを形式作成するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **mab request format attribute 1 groupsize** {**1** | **2** | **4** |**12**} [**separator** {**-** | **:** | **.**} {**lowercase** | **uppercase**}]
3. **mab request format attribute2** {**0** | **7**} *text*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mab request format attribute 1 groupsize** {**1** | **2** | **4** |**12**} [**separator** {**-** | **:** | **.**} {**lowercase** | **uppercase**}] 例： `Switch(config)# mab request format attribute 1 groupsize 12`	MAB で生成された Access-Request パケットの User-Name 属性内の MAC アドレスの形式を指定します。 1：MAC アドレスの 12 桁の十六進数のユーザ名形式を設定します。 group size：区切り文字の挿入の前に連結する 16 進ニブルの数。 有効なグループ サイズは、1、2、4、12 のいずれかである必要があります。 separator：グループ サイズに従って 16 進ニブルを区切る文字。 有効な区切り文字は、ハイフン、コロン、ピリオドのいずれかである必要があります。 12 のグループ サイズでは、区切り文字は使用されません。 {lowercase | uppercase}：数字以外の 16 進ニブルを小文字または大文字のどちらにするかを指定します。
ステップ 3	**mab request format attribute2** {**0** | **7**} *text* 例： `Switch(config)# mab request format attribute 2 7 A02f44E18B12`	**2**：MAB で生成された Access-Request パケット内の User-Password 属性のカスタム（デフォルト以外の）値を指定します。 **0**：追跡するクリア テキスト パスワードを指定します。 **7**：追跡する暗号化パスワードを指定します。 *text*：User-Password 属性で使用するパスワードを指定します。 （注） 設定情報を電子メールで送信する場合、タイプ 7 のパスワード情報を削除してください。 **show tech-support** コマンドは、デフォルトで出力からこの情報を削除します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

802.1x ユーザ ディストリビューションの設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **vlan group** *vlan-group-name* **vlan-list** *vlan-list*
3. **end**
4. **no vlan group** *vlan-group-name* **vlan-list** *vlan-list*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan group** *vlan-group-name* **vlan-list** *vlan-list* 例： `Switch(config)# vlan group eng-dept vlan-list 10`	VLAN グループを設定し、単一の VLAN または VLANの範囲をそのグループにマッピングします。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**no vlan group** *vlan-group-name* **vlan-list** *vlan-list* 例： `Switch(config)# no vlan group eng-dept vlan-list 10`	VLAN グループ コンフィギュレーションまたは VLAN グループ コンフィギュレーションの要素をクリアします。

VLAN グループの設定例

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ コンフィギュレーションおよび指定 VLAN とのマッピングを確認する例を示します。

```
Switch(config)# vlan group eng-dept vlan-list 10

Switch(config)# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10

Switch(config)# show dot1x vlan-group all
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10
hr-dept                         20
```

次に、VLAN を既存の VLAN グループに追加し、VLAN が追加されたことを確認する例を示します。

```
Switch(config)# vlan group eng-dept vlan-list 30
Switch(config)# show vlan group eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10,30
```

次に、VLAN を VLAN グループから削除する例を示します。

```
Switch# no vlan group eng-dept vlan-list 10
```

次に、すべての VLAN が VLAN グループからクリアされたときに、その VLAN グループもクリアされる例を示します。

```
Switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

Switch(config)# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループをクリアする方法を示します。

```
Switch(config)# no vlan group end-dept vlan-list all
Switch(config)# show vlan-group all
```

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

NAC レイヤ 2 802.1x 検証の設定

NAC レイヤ 2 802.1x 検証を設定できます。これは、RADIUS サーバを使用した 802.1x 認証とも呼ばれます。

NAC レイヤ 2 802.1x 検証を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **authentication event no-response action authorize vlan** *vlan-id*
5. **authentication periodic**
6. **authentication timer reauthenticate**
7. **end**
8. **show authentication sessions interface** *interface-id*
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/3`	設定するポートを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**authentication event no-response action authorize vlan** *vlan-id* 例： `Switch(config-if)# authentication event no-response action authorize vlan 8`	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。 指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。
ステップ 5	**authentication periodic** 例： `Switch(config-if)# authentication periodic`	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**authentication timer reauthenticate** 例： `Switch(config-if)# authentication timer reauthenticate`	クライアントに対する再認証試行を設定します（1 時間に設定）。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show authentication sessions interface** *interface-id* 例： `Switch# show authentication sessions interface gigabitethernet2/0/3`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

NEAT を使用したオーセンティケータ スイッチの設定

この機能を設定するには、ワイヤリング クローゼット外の 1 つのスイッチがサプリカントとして設定され、オーセンティケータ スイッチに接続されている必要があります。

（注） *cisco-av-pairs* は、ACS で *device-traffic-class=switch* として設定されている必要があります。これは、サプリカントが正常に認証された後でトランクとしてインターフェイスを設定します。

スイッチをオーセンティケータに設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **cisp enable**
3. **interface** *interface-id*
4. **switchport mode access**
5. **authentication port-control auto**
6. **dot1x pae authenticator**
7. **spanning-tree portfast**
8. **end**
9. **show running-config interface** *interface-id*
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable** 例： `Switch(config)# cisp enable`	CISP をイネーブルにします。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	ポート モードを **access** に設定します。
ステップ 5	**authentication port-control auto** 例： `Switch(config-if)# authentication port-control auto`	ポート認証モードを auto に設定します。

	コマンドまたはアクション	目的
ステップ 6	**dot1x pae authenticator** 例： `Switch(config-if)# dot1x pae authenticator`	インターフェイスをポート アクセス エンティティ（PAE）オーセンティケータとして設定します。
ステップ 7	**spanning-tree portfast** 例： `Switch(config-if)# spanning-tree portfast trunk`	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で Port Fast をイネーブルにします。
ステップ 8	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config interface** *interface-id* 例： `Switch# show running-config interface gigabitethernet2/0/1`	設定を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

NEAT を使用したサプリカント スイッチの設定

スイッチをサプリカントに設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **cisp enable**
3. **dot1x credentials** *profile*
4. **username** *suppswitch*
5. **password** *password*
6. **dot1x supplicant force-multicast**
7. **interface** *interface-id*
8. **switchport trunk encapsulation dot1q**
9. **switchport mode trunk**
10. **dot1x pae supplicant**
11. **dot1x credentials** *profile-name*
12. **end**
13. **show running-config interface** *interface-id*
14. **copy running-config startup-config**
15. Auto Smartport マクロを使用した NEAT の設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable** 例： `Switch(config)# cisp enable`	CISP をイネーブルにします。
ステップ 3	**dot1x credentials** *profile* 例： `Switch(config)# dot1x credentials test`	802.1x クレデンシャル プロファイルを作成します。これは、サプリカントとして設定されるポートに接続する必要があります。
ステップ 4	**username** *suppswitch* 例： `Switch(config)# username suppswitch`	ユーザ名を作成します。

	コマンドまたはアクション	目的
ステップ 5	**password** *password* 例： `Switch(config)# password myswitch`	新しいユーザ名のパスワードを作成します。
ステップ 6	**dot1x supplicant force-multicast** 例： `Switch(config)# dot1x supplicant force-multicast`	ユニキャストまたはマルチキャスト パケットのいずれかを受信した場合にスイッチに強制的にマルチキャスト EAPOL だけを送信させます。 これにより、NEAT がすべてのホスト モードでのサプリカントスイッチで機能できるようにもなります。
ステップ 7	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するポートを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 8	**switchport trunk encapsulation dot1q** 例： `Switch(config-if)# switchport trunk encapsulation dot1q`	ポートをトランク モードに設定します。
ステップ 9	**switchport mode trunk** 例： `Switch(config-if)# switchport mode trunk`	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	**dot1x pae supplicant** 例： `Switch(config-if)# dot1x pae supplicant`	インターフェイスをポート アクセス エンティティ（PAE）サプリカントとして設定します。
ステップ 11	**dot1x credentials** *profile-name* 例： `Switch(config-if)# dot1x credentials test`	802.1x クレデンシャル プロファイルをインターフェイスに対応付けます。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show running-config interface** *interface-id* 例： `Switch# show running-config interface gigabitethernet1/0/1`	設定を確認します。
ステップ 14	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 15	Auto Smartport マクロを使用した NEAT の設定	スイッチ VSA ではなく Auto Smartport ユーザ定義マクロを使用して、オーセンティケータ スイッチを設定することもできます。 詳細については、このリリースに対応する『*Auto Smartports Configuration Guide*』を参照してください。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定

スイッチで 802.1x 認証を設定するほか、ACS を設定する必要があります。 情報については、『*Configuration Guide for Cisco Secure ACS 4.2*』を参照してください。
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs_config.pdf

（注） スイッチにダウンロードする前に、ダウンロード可能な ACL を ACS で設定する必要があります。

ポートでの認証後、**show ip access-list** 特権 EXEC コマンドを使用して、ポートにダウンロードした ACL を表示できます。

ダウンロード可能な ACL の設定

これらのポリシーは、クライアントが認証され、クライアント IP アドレスが IP デバイス トラッキング テーブルに追加された後で有効になります。 その後スイッチがダウンロード可能な ACL をポートに適用します。

特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **ip device tracking**
3. **aaa new-model**
4. **aaa authorization network default local group radius**
5. **radius-server vsa send authentication**
6. **interface** *interface-id*
7. **ip access-group** *acl-id* **in**
8. **show running-config interface** *interface-id*
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip device tracking** 例： `Switch(config)# ip device tracking`	IP デバイス トラッキング テーブルを設定します。
ステップ 3	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa authorization network default local group radius** 例： `Switch(config)# aaa authorization network`	許可の方法をローカルに設定します。 認証方法を削除するには、**no aaa authorization network default local group radius** コマンドを使用します。

	コマンドまたはアクション	目的
	default local group radius	
ステップ 5	**radius-server vsa send authentication** 例： `Switch(config)# radius-server vsa send authentication`	RADIUS VSA 送信認証を設定します。
ステップ 6	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/4`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip access-group** *acl-id* **in** 例： `Switch(config-if)# ip access-group default_acl in`	ポートの入力方向のデフォルト ACL を設定します。 （注） *acl-id* はアクセス リストの名前または番号です。
ステップ 8	**show running-config interface** *interface-id* 例： `Switch(config-if)# show running-config interface gigabitethernet2/0/4`	設定を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ダウンロード ポリシーの設定

特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **access-list** *access-list-number* **{ deny | permit } { hostname | any | host } log**
3. **interface** *interface-id*
4. **ip access-group** *acl-id* **in**
5. **exit**
6. **aaa new-model**
7. **aaa authorization network default group radius**
8. **ip device tracking**
9. **ip device tracking probe** [**count** | **interval** | **use-svi**]
10. **radius-server vsa send authentication**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **{ deny | permit } { hostname | any | host } log** 例： `Switch(config)# access-list 1 deny any log`	デフォルト ポート ACL を定義します。 access-list-number には、1 ～ 99 または 1300 ～ 1999 の 10 進数値を指定します。 条件が一致した場合にアクセスを拒否する場合は **deny**、許可する場合は **permit** を指定します。 source は、次のようなパケットを送信するネットワークまたはホストの送信元アドレスです。 • **hostname**：ドット付き 10 進表記による 32 ビット長の値。 • **any**：source および source-wildcard の値 0.0.0.0 255.255.255.255 の省略形を意味するキーワード any。 source-wildcard 値を入力する必要はありません。 • **host**：source および source-wildcard の値 source 0.0.0.0 の省略形を意味するキーワード host。 （任意）source-wildcard ビットを送信元アドレスに適用します。 （任意）ログを入力して、エントリと一致するパケットに関する情報ロギング メッセージをコンソールに送信します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/2`	インターフェイスコンフィギュレーションモードを開始します。
ステップ 4	**ip access-group** *acl-id* **in** 例： `Switch(config-if)# ip access-group default_acl in`	ポートの入力方向のデフォルト ACL を設定します。 （注） acl-id はアクセス リストの名前または番号です。
ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 7	**aaa authorization network default group radius** 例： `Switch(config)# aaa authorization network default group radius`	許可の方法をローカルに設定します。 許可の方法を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 8	**ip device tracking** 例： `Switch(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。 IP デバイス トラッキング テーブルをディセーブルにするには、**no ip device tracking** グローバル コンフィギュレーション コマンドを使用します。
ステップ 9	**ip device tracking probe** [**count** | **interval** | **use-svi**] 例： `Switch(config)# ip device tracking probe count`	（任意）IP デバイス トラッキング テーブルを設定します。 • **count** *count*：スイッチが ARP プローブを送信する回数を設定します。 指定できる範囲は 1 ～ 5 です。 デフォルトは 3 です。 • **interval** *interval*：スイッチが ARP プローブを再送信するまでに応答を待機する時間（秒単位）を設定します。 範囲は 30 ～ 300 秒です。 デフォルトは 30 秒です。

	コマンドまたはアクション	目的
		• **use-svi**：スイッチ仮想インターフェイス（SVI）の IP アドレスを ARP プローブの送信元として使用します。
ステップ 10	**radius-server vsa send authentication** 例： `Switch(config)# radius-server vsa send authentication`	ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。 （注） ダウンロード可能な ACL が機能する必要があります。
ステップ 11	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

VLAN ID ベース MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **mab request format attribute 32 vlan access-vlan**
3. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mab request format attribute 32 vlan access-vlan** 例： `Switch(config)# mab request format attribute 32 vlan access-vlan`	VLAN ID ベース MAC 認証をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

柔軟な認証順序の設定

下の手順で使用される例は、MAB が IEEE 802.1x 認証（dot1x）の前に試行されるように柔軟な認証の順序設定の順序を変更します。 MAB は最初の認証方式として設定されているため、MAB に他のすべての認証方式よりも優先されます。

（注） これらの認証方式のデフォルトの順序とプライオリティを変更する前に、これらの変更による潜在的な結果を理解する必要があります。 詳細について、http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/application_note_c27-573287_ps6638_Products_White_Paper.html を参照してください。

特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **authentication order** [**dot1x** | **mab**] | {**webauth**}
5. **authentication priority** [**dot1x** | **mab**] | {**webauth**}
6. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**authentication order [dot1x | mab] | {webauth}** 例： `Switch(config-if)# authentication order mab dot1x`	（任意）ポート上で使用される認証方式の順序を設定します。
ステップ 5	**authentication priority [dot1x | mab] | {webauth}** 例： `Switch(config-if)# authentication priority mab dot1x`	（任意）認証方式をポート プライオリティ リストに追加します。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

柔軟な認証の順序設定，（1595 ページ）

Open1x の設定

ポートの許可ステートの手動制御をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **authentication control-direction** {**both** | **in**}
5. **authentication fallback** *name*
6. **authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]
7. **authentication open**
8. **authentication order** [**dot1x** | **mab**] | {**webauth**}
9. **authentication periodic**
10. **authentication port-control** {**auto** | **force-authorized** | **force-un authorized**}
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**authentication control-direction** {**both**	**in**} 例： `Switch(config-if)# authentication control-direction both`	（任意）ポート制御を単一方向モードまたは双方向モードに設定します。

	コマンドまたはアクション	目的
ステップ 5	**authentication fallback** *name* 例： `Switch(config-if)# authentication fallback profile1`	（任意）802.1x 認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。
ステップ 6	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] 例： `Switch(config-if)# authentication host-mode multi-auth`	（任意）ポート上で認証マネージャ モードを設定します。
ステップ 7	**authentication open** 例： `Switch(config-if)# authentication open`	（任意）ポート上でオープンアクセスをイネーブルまたはディセーブルにします。
ステップ 8	**authentication order** [**dot1x** | **mab**] | {**webauth**} 例： `Switch(config-if)# authentication order dot1x webauth`	（任意）ポート上で使用される認証方式の順序を設定します。
ステップ 9	**authentication periodic** 例： `Switch(config-if)# authentication periodic`	（任意）ポート上で再認証をイネーブルまたはディセーブルにします。
ステップ 10	**authentication port-control** {**auto** | **force-authorized** | **force-un authorized**} 例： `Switch(config-if)# authentication port-control auto`	（任意）ポートの許可ステートの手動制御をイネーブルにします。
ステップ 11	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

Open1x 認証, （1596 ページ）

ポート上での 802.1x 認証のディセーブル化

802.1x 認証をポートでディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで 802.1x 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **no dot1x pae authenticator**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	（任意）RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	**no dot1x pae authenticator** 例： `Switch(config-if)# no dot1x pae`	ポートでの 802.1x 認証をディセーブルにします。

	コマンドまたはアクション	目的
	authenticator	
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

802.1x 認証設定のデフォルト値へのリセット

802.1x 認証設定をデフォルト値に戻すには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **dot1x default**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ 3	**dot1x default** 例： `Switch(config-if)# dot1x default`	設定可能な 802.1x のパラメータをデフォルト値へ戻します。

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

802.1x の統計情報およびステータスのモニタリング

表 *146*：特権 *EXEC* 表示コマンド

コマンド	目的
show dot1x all statistics	すべてのポートの 802.1x 統計情報を表示します。
show dot1x interface *interface-id* **statistics**	指定されたポートの 802.1x 統計情報を表示します。
show dot1x all [**count** | **details** | **statistics** | **summary**]	スイッチの 802.1x 管理ステータスおよび動作ステータスを表示します。
show dot1x interface *interface-id*	指定されたポートの 802.1x 管理ステータスおよび動作ステータスを表示します。

表 *147*：グローバル コンフィギュレーション コマンド

コマンド	目的
no dot1x logging verbose	冗長な 802.1x 認証メッセージをフィルタに掛けます（Cisco IOS Release 12.2(55) SE 以降）

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

第 61 章

Web ベース認証の設定

この章では、Web ベースの認証を設定する方法について説明します。 この章の内容は、次のとおりです。

- 機能情報の確認，1665 ページ
- Web ベース認証について，1665 ページ
- Web ベース認証の設定方法，1676 ページ
- Web ベース認証ステータスのモニタリング，1691 ページ

機能情報の確認

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

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

Web ベース認証について

IEEE 802.1x サプリカントが実行されていないホスト システムのエンド ユーザを認証するには、Web 認証プロキシと呼ばれる Web ベース認証機能を使用します。

（注） Web ベース認証は、レイヤ 2 およびレイヤ 3 インターフェイス上に設定できます。

HTTP セッションを開始すると、Web ベース認証は、ホストからの入力 HTTP パケットを代行受信し、ユーザに HTML ログイン ページを送信します。 ユーザはクレデンシャルを入力します。このクレデンシャルは、Web ベース認証機能により、認証のために認証、許可、アカウンティング（AAA）サーバに送信されます。

認証が成功すると、Web ベース認証はログイン成功 HTML ページをホストに送信し、AAA サーバから返されたアクセス ポリシーを適用します。

認証に失敗した場合、Web ベース認証は、ログインの失敗を示す HTML ページをユーザに転送し、ログインを再試行するように、ユーザにプロンプトを表示します。 最大試行回数を超過した場合、Web ベース認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザは待機期間中、ウォッチ リストに載せられます。

ここでは、AAA の一部としての Web ベース認証の役割について説明します。

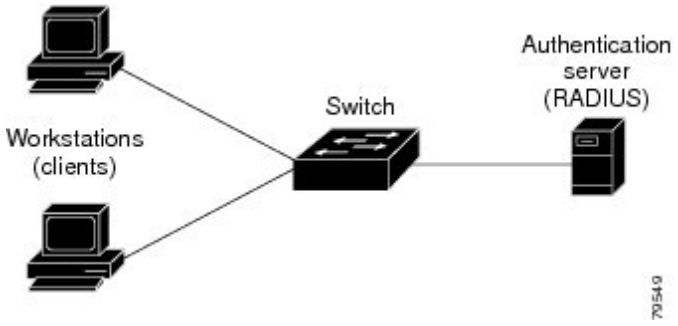
デバイスのロール

Web ベース認証では、ネットワーク上のデバイスに次のような固有の役割があります。

- クライアント：LANおよびサービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。 このワークステーションでは、Java Script がイネーブルに設定された HTML ブラウザが実行されている必要があります。
- 認証サーバ：クライアントを認証します。 認証サーバはクライアントの識別情報を確認し、そのクライアントが LAN およびスイッチのサービスへのアクセスを許可されたか、あるいはクライアントが拒否されたのかをスイッチに通知します。
- スイッチ：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。 スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。

次の図は、ネットワーク上でのこれらのデバイスの役割を示します。

図 *110*：*Web* ベース認証デバイスの役割



ホストの検出

スイッチは、検出されたホストに関する情報を格納するために、IPデバイストラッキングテーブルを維持します。

（注） デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルにされています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

レイヤ 2 インターフェイスでは、Web ベース認証は、これらのメカニズムを使用して、IP ホストを検出します。

- ARP ベースのトリガー：ARP リダイレクト ACL により、Web ベース認証は、スタティック IP アドレス、またはダイナミック IP アドレスを持つホストを検出できます。
- ダイナミック ARP インスペクション
- DHCP スヌーピング：スイッチがホストの DHCP バインディング エントリを作成するときに Web ベース認証が通知されます。

セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストをレビューします。

  ホスト IP が例外リストに含まれている場合、この例外リスト エントリからポリシーが適用され、セッションが確立されます。

- 認証バイパスをレビューします。

  ホスト IP が例外リストに含まれていない場合、Web ベース認証は応答しないホスト（NRH）要求をサーバに送信します。

  サーバの応答が access accepted であった場合、認証はこのホストにバイパスされます。 セッションが確立されます。

- HTTP インターセプト ACL を設定します。

  NRH 要求に対するサーバの応答が access rejected であった場合、HTTP インターセプト ACL がアクティブ化され、セッションはホストからの HTTP トラフィックを待機します。

認証プロセス

Web ベース認証をイネーブルにすると、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。

- HTTP トラフィックが代行受信され、認証が開始されます。 スイッチは、ユーザにログインページを送信します。 ユーザはユーザ名とパスワードを入力します。スイッチはこのエントリを認証サーバに送信します。
- 認証に成功した場合、スイッチは認証サーバからこのユーザのアクセス ポリシーをダウンロードし、アクティブ化します。 ログインの成功ページがユーザに送信されます
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。 ユーザはログインを再試行します。 失敗の回数が試行回数の最大値に達した場合、スイッチはログイン期限切れページを送信します。このホストはウォッチ リストに入れられます。 ウォッチ リストのタイム アウト後、ユーザは認証プロセスを再試行することができます。
- 認証サーバがスイッチに応答せず、AAA 失敗ポリシーが設定されている場合、スイッチはホストに失敗アクセス ポリシーを適用します。 ログインの成功ページがユーザに送信されます
- ホストがレイヤ2インターフェイス上のARPプローブに応答しなかった場合、またはホストがレイヤ3インターフェイスでアイドルタイムアウト内にトラフィックを送信しなかった場合、スイッチはクライアントを再認証します。
- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッションタイムアウトを適用します。
- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信します。Termination-Action は、サーバからの応答に含まれます。
- Termination-Actionがデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除されます。

ローカル Web 認証バナー

Web 認証を使用して、デフォルトのカスタマイズ済み Web ブラウザ バナーを作成して、スイッチにログインしたときに表示するようにできます。

このバナーは、ログイン ページと認証結果ポップアップ ページの両方に表示されます。 デフォルトのバナー メッセージは次のとおりです。

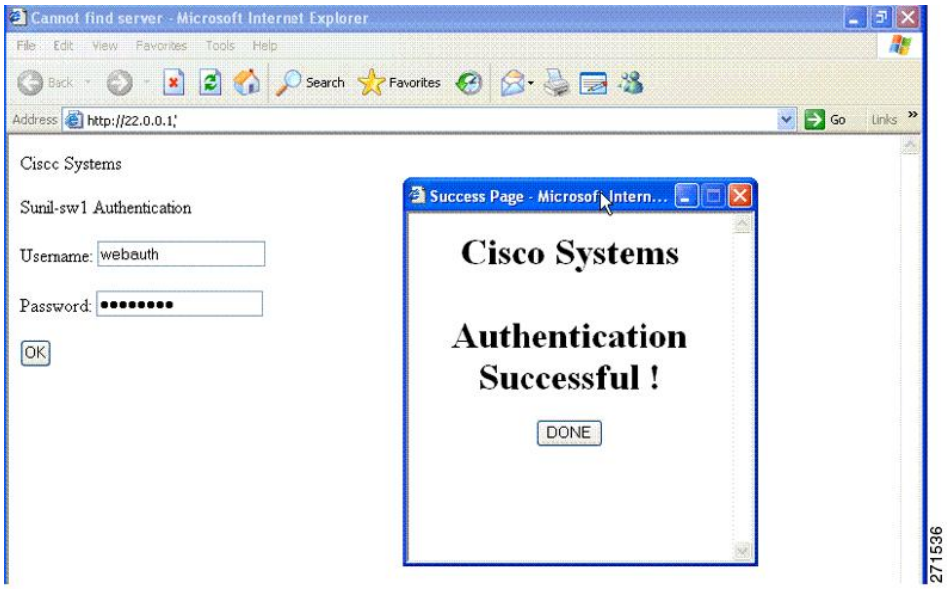
- 認証成功
- *Authentication Failed*
- 認証期限切れ

ローカル ネットワーク認証バナーは、レガシーおよび新スタイル（セッション アウェア）の CLI で次のように設定できます。

- レガシー モード：**ip admission auth-proxy-banner http** グローバル コンフィギュレーション コマンドを使用します。
- 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。

ログイン ページには、デフォルトのバナー、*Cisco Systems*、および *Switch host-name Authentication* が表示されます。 *Cisco Systems* は認証結果ポップアップ ページに表示されます。

図 *111*：認証成功バナー

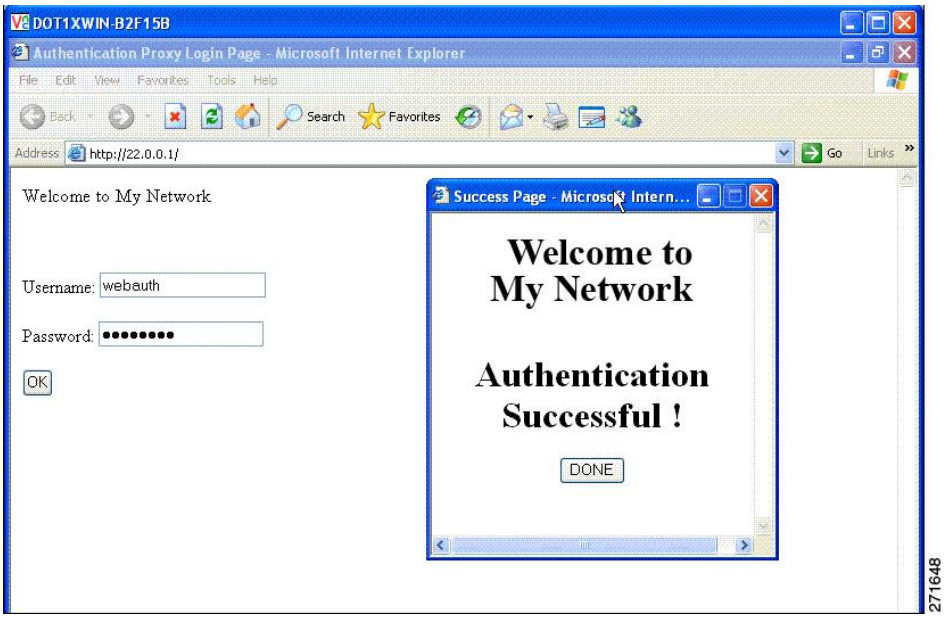


バナーは次のようにカスタマイズ可能です。

- スイッチ名、ルータ名、または会社名などのメッセージをバナーに追加する。
  - レガシー モード：**ip admission auth-proxy-banner http** *banner-text* グローバル コンフィギュレーション コマンドを使用します。
  - 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。
- ロゴまたはテキスト ファイルをバナーに追加する。
  - レガシー モード：**ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用します。

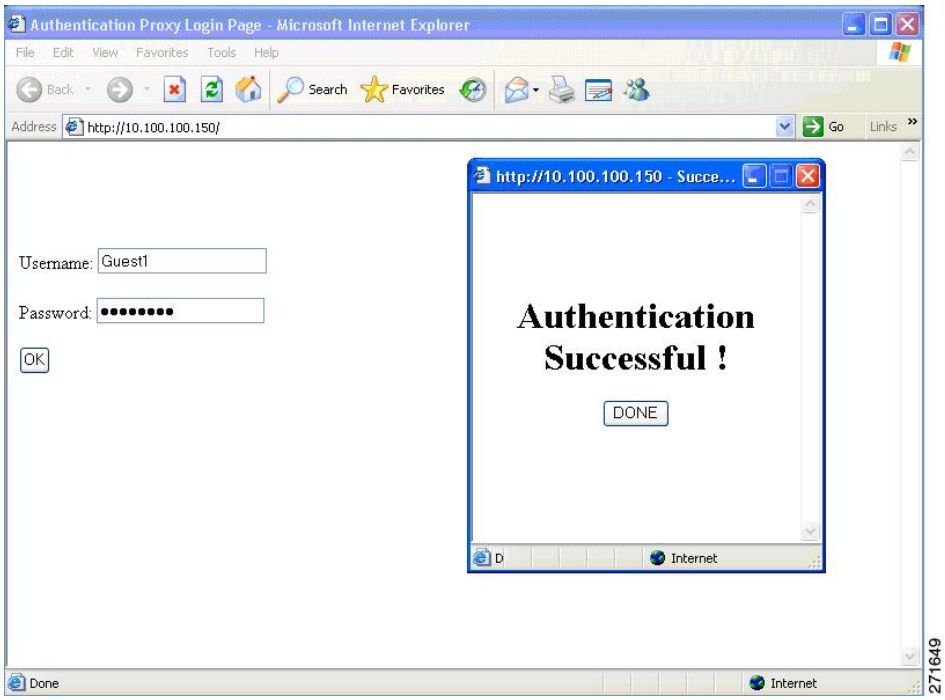
- 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。

図 *112*：カスタマイズされた *Web* バナー



バナーがイネーブルにされていない場合、Web 認証ログイン画面にはユーザ名とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはバナーは表示されません。

図 *113*：バナーが表示されていないログイン画面



Web 認証カスタマイズ可能な Web ページ

Web ベース認証プロセスでは、スイッチ内部の HTTP サーバは、認証中のクライアントに配信される 4 種類の HTML ページをホストします。 サーバはこれらのページを使用して、ユーザに次の 4 種類の認証プロセス ステートを通知します。

- ログイン：資格情報が要求されています。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：ログインの失敗回数が多すぎて、ログインセッションが期限切れになりました。

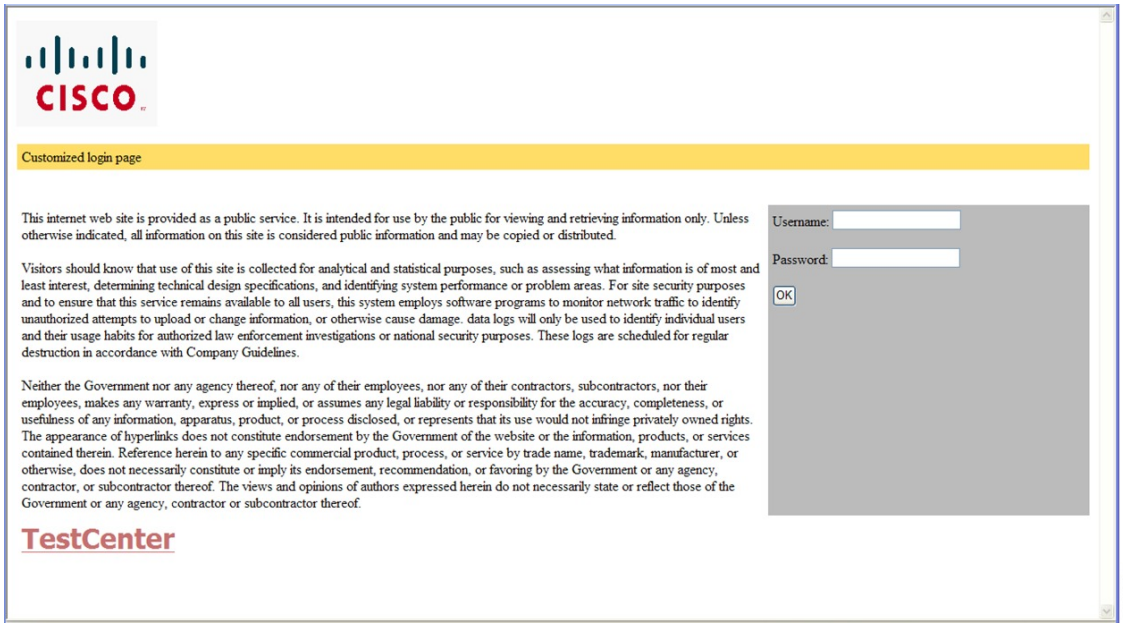
ガイドライン

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。
- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。

- バナー ページで、ログイン ページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。
- この URL 文字列は有効な URL（例：http://www.cisco.com）でなければなりません。 不完全な URL は、Web ブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド（例：ページのタイム アウトを設定、暗号化されたパスワードの設定、同じページが 2 回送信されていないことの確認など）を記入する必要があります.
- 設定されたログイン フォームがイネーブルにされている場合、特定の URL にユーザをリダイレクトする CLI コマンドは使用できません。 管理者は、Web ページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定の URL にユーザをリダイレクトする CLI コマンドを入力してから、Web ページを設定するコマンドを入力した場合、特定の URL にユーザをリダイレクトする CLI コマンドは効力を持ちません。
- 設定された Web ページは、スイッチのブート フラッシュ、またはフラッシュにコピーできます。
- スタック可能なスイッチでは、スタック マスターまたはスタック メンバーのフラッシュから設定済みのページにアクセスできます。
- ログイン ページを 1 つのフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、スタック マスター、またはメンバのフラッシュ）にすることができます。
- 4 ページすべてを設定する必要があります。
- Web ページを使ってバナー ページを設定した場合、このバナー ページには効果はありません。
- システム ディレクトリ（たとえば、flash、disk0、disk）に保存されていて、ログイン ページに表示する必要のあるロゴファイル（イメージ、フラッシュ、オーディオ、ビデオなど）すべてには、必ず、*web_auth_<filename>* の形式で名前をつけてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

デフォルトの内部 HTML ページの代わりに、自分の HTML ページを使用することができます。認証後のユーザのリダイレクト先で、内部成功ページの代わりとなる URL を指定することもできます。

図 *114*：カスタマイズ可能な認証ページ



認証プロキシ Web ページの注意事項

カスタマイズされた認証プロキシ Web ページを設定する際には、次の注意事項に従ってください。

- カスタム Web ページ機能をイネーブルにするには、カスタム HTML ファイルを 4 個すべて指定します。 指定したファイルの数が 4 個未満の場合、内部デフォルト HTML ページが使用されます。
- これら 4 個のカスタム HTML ファイルは、スイッチのフラッシュ メモリ内に存在しなければなりません。 各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページ上のイメージはすべて、アクセス可能は HTTP サーバ上に存在しなければなりません。 インターセプト ACL は、管理ルール内で設定します。
- カスタム ページからの外部リンクはすべて、管理ルール内でのインターセプト ACL の設定を必要とします。
- 有効な DNS サーバにアクセスするには、外部リンクまたはイメージに必要な名前解決で、管理ルール内にインターセプト ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルに設定されている場合、設定された auth-proxy-banner は使用されません。

- カスタム Web ページ機能がイネーブルに設定されている場合、ログインの成功に対するリダイレクション URL は使用できません。
- カスタム ファイルの指定を解除するには、このコマンドの **no** 形式を使用します。

カスタム ログイン ページはパブリック Web フォームであるため、このページについては、次の注意事項に従ってください。

- ログインフォームは、ユーザによるユーザ名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

関連トピック

認証プロキシ Web ページのカスタマイズ, （1685 ページ）

成功ログインに対するリダイレクト URL の注意事項

成功ログインに対するリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルに設定されている場合、リダイレクション URL 機能はディセーブルにされ、CLI では使用できません。 リダイレクションは、カスタム ログイン成功ページで実行できます。
- リダイレクション URL 機能がイネーブルに設定されている場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの **no** 形式を使用します。
- Web ベースの認証クライアントが正常に認証された後にリダイレクション URL が必要な場合、URL 文字列は有効な URL（たとえば http://）で開始し、その後に URL 情報が続く必要があります。 http:// を含まない URL が指定されると、正常に認証が行われても、そのリダイレクション URL によって Web ブラウザでページが見つからないまたは同様のエラーが生じる場合があります。

関連トピック

成功ログインに対するリダイレクション URL の指定, （1687 ページ）

その他の機能と Web ベース認証の相互作用

ポート セキュリティ

Web ベース認証とポート セキュリティは、同じポートに設定できます。 Web ベース認証はポートを認証し、ポート セキュリティは、クライアントの MAC アドレスを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。 この場合、このポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

関連トピック

ポート セキュリティのイネーブル化および設定, （1714 ページ）

LAN ポート IP

LAN ポート IP（LPIP）とレイヤ 2 Web ベース認証は、同じポートに設定できます。 ホストは、まず Web ベース認証、次に LPIP ポスチャ検証を使用して認証されます。 LPIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

Web ベース認証のアイドル時間が満了すると、NAC ポリシーは削除されます。 ホストが認証され、ポスチャが再度検証されます。

ゲートウェイ IP

VLAN のいずれかのスイッチ ポートで Web ベース認証が設定されている場合、レイヤ 3 VLAN インターフェイス上にゲートウェイ IP（GWIP）を設定することはできません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。 ソフトウェアで、両方の機能のホスト ポリシーが適用されます。 GWIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

ACL

インターフェイスで VLAN ACL、または Cisco IOS ACL を設定した場合、ACL は、Web ベース認証のホスト ポリシーが適用された後だけ、ホスト トラフィックに適用されます。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの入力トラフィックについて、ポート ACL（PACL）をデフォルトのアクセス ポリシーとして設定することが必須ではないものの、より安全です。 認証後、Web ベース認証のホスト ポリシーは、PACL に優先されます。 ポートに設定された ACL がなくても、ポリシー ACL はセッションに適用されます。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN が VACL キャプチャ用に設定されているポートには Web ベース認証は設定できません。

コンテキストベース アクセス コントロール

コンテキストベース アクセス コントロール（CBAC）が、ポート VLAN のレイヤ 3 VLAN インターフェイスで設定されている場合、レイヤ 2 ポートで Web ベース認証は設定できません。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。 Web ベース認証設定は、すべてのメンバ チャネルに適用されます。

Web ベース認証の設定方法

デフォルトの Web ベース認証の設定

次の表に、デフォルトの Web ベース認証の設定を示しています。

表 *148* : デフォルトの *Web* ベース認証の設定

機能	デフォルト設定
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • Key	• 指定なし • 1645 • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

Web ベース認証の設定に関する注意事項と制約事項

- Web ベース認証は入力だけの機能です。
- Web ベース認証は、アクセス ポートだけで設定できます。 Web ベース認証は、トランク ポート、EtherChannel メンバ ポート、またはダイナミック トランク ポートではサポートされていません。
- スタティックな ARP キャッシュが割り当てられているレイヤ 2 インターフェイス上のホストは認証できません。 これらのホストは ARP メッセージを送信しないため、Web ベース認証機能では検出されません。
- デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。 Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。
- スイッチ HTTP サーバを実行するには、IP アドレスを少なくとも 1 つ設定する必要があります。 また、各ホスト IP アドレスに到達するようにルートを設定する必要もあります。 HTTP サーバは、ホストに HTTP ログイン ページを送信します。
- 2 ホップ以上離れたところにあるホストでは、STP トポロジの変更により、ホスト トラフィックの到着するポートが変わってしまった場合、トラフィックが停止する可能性があります。

これは、レイヤ 2（STP）トポロジの変更後に、ARP および DHCP の更新が送信されていない場合に発生します。

- Web ベース認証は、ダウンロード可能なホストポリシーとして、VLAN 割り当てをサポートしていません。
- Web ベース認証はセッション認識型ポリシー モードで IPv6 をサポートします。 IPv6 Web 認証には、スイッチで設定された少なくても 1 つの IPv6 アドレスおよびスイッチ ポートに設定設定された IPv6 スヌーピングが必要です。
- Web ベース認証および Network Edge Access Topology（NEAT）は、相互に排他的です。 インターフェイス上で NEAT がイネーブルの場合、Web ベース認証を使用できず、インターフェイス上で Web ベース認証が実行されている場合は、NEAT を使用できません。
- パスワード認証プロトコル（PAP）のみがコントローラの Web ベースの RADIUS 認証でサポートされます。 チャレンジハンドシェイク認証プロトコル（CHAP）は、コントローラの Web ベースの RADIUS 認証でサポートされません。
- スイッチから RADIUS サーバへの通信の設定に使用される次の RADIUS セキュリティ サーバ設定を確認します。
  - ホスト名
  - ホスト IP アドレス
  - ホスト名と特定の UDP ポート番号
  - IP アドレスと特定の UDP ポート番号

  IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。 同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。 RADIUS ホスト エントリは、設定した順序に従って選択されます。
- RADIUS サーバ パラメータを設定する場合は、次の点に注意してください。
  - 別のコマンドラインに **key***string* を指定します。
  - **key***string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。 キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。
  - **key***string* を指定する場合、キーの中間、および末尾にスペースを使用します。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 キーは RADIUS デーモンで使用する暗号に一致している必要があります。
  - すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号キー値をグローバルに設定するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。 これらのオプションをサーバ単位で設定するには、**radius-server**

timeout、radius-server transmit、および radius-server key グローバル コンフィギュレーション コマンドを使用します。 詳細については、『*Cisco IOS Security Configuration Guide*, Release 12.4』および『*Cisco IOS Security Command Reference*, Release 12.4』を参照してください。

（注） RADIUS サーバでは、スイッチの IP アドレス、サーバとスイッチで共有される key string、およびダウンロード可能な ACL（DACL）などの設定を行う必要があります。 詳細については、RADIUS サーバのマニュアルを参照してください。

認証ルールとインターフェイスの設定

認証ルールおよびインターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admissionname***name***proxyhttp**
4. **interface***typeslot/port*
5. **ip access-group***name*
6. **ip admission***name*
7. **exit**
8. **ip device tracking**
9. **end**
10. **show ip admission status**
11. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ip admissionname***name***proxyhttp** 例： `Switch(config)# ip admission name webauth1 proxy http`	Web ベース許可の認証ルールを設定します。
ステップ 4	**interface***typeslot/port* 例： `Switch(config)# interface gigabitEthernet1/0/1`	インターフェイスコンフィギュレーションモードを開始し、Web ベース認証をイネーブルにする入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。 *type* には、fastethernet、gigabit ethernet、または tengigabitethernet を指定できます。
ステップ 5	**ip access-group***name* 例： `Switch(config-if)# ip access-group webauthag`	デフォルト ACL を適用します。
ステップ 6	**ip admission***name* 例： `Switch(config-if)# ip admission webauth1`	指定されたインターフェイスにWebベース認証を設定します。
ステップ 7	**exit** 例： `Switch(config-if)# exit`	コンフィギュレーション モードに戻ります。
ステップ 8	**ip device tracking** 例： `Switch(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip admission status** 例： `Switch# show ip admission status`	設定を表示します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

AAA 認証の設定

AAA 認証を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa authentication login default group** {**tacacs+** | **radius**}
5. **aaa authorization auth-proxy default group** {**tacacs+** | **radius**}
6. **tacacs-server host** {*hostname* | *ip_address*}
7. **tacacs-server key** {*key-data*}
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA 機能をイネーブルにします。
ステップ 4	**aaa authentication login default group** {**tacacs+** | **radius**} 例： `Switch(config)# aaa authentication login default group tacacs+`	ログイン時の認証方法のリストを定義します。
ステップ 5	**aaa authorization auth-proxy default group** {**tacacs+** | **radius**} 例： `Switch(config)# aaa authorization auth-proxy default group tacacs+`	Web ベース許可の許可方式リストを作成します。
ステップ 6	**tacacs-server host** {*hostname* | *ip_address*} 例： `Switch(config)# tacacs-server host 10.1.1.1`	AAA サーバを指定します。
ステップ 7	**tacacs-server key** {*key-data*} 例： `Switch(config)# tacacs-server key`	スイッチと TACACS サーバとの間で使用される許可および暗号キーを設定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ/RADIUS サーバ間通信の設定

RADIUS サーバのパラメータを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip radius source-interfacevlan***vlan interface number*
4. **radius-server host** {*hostname* | *ip-address*} **test username***username*
5. **radius-server key***string*
6. **radius-server dead-criteria tries***num-tries*
7. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip radius source-interfacevlan***vlan interface number* 例： `Switch(config)# ip radius source-interface vlan 80`	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 4	**radius-server host** {*hostname* | *ip-address*} **test username***username* 例： `Switch(config)# radius-server host 172.120.39.46 test username user1`	リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **test username***username* は、RADIUS サーバ接続の自動テストをイネーブルにするオプションです。 指定された *username* は有効なユーザ名である必要はありません。 **key** オプションは、スイッチと RADIUS サーバの間で使用される認証と暗号キーを指定します。 複数の RADIUS サーバを使用するには、それぞれのサーバでこのコマンドを入力してください。
ステップ 5	**radius-server key***string* 例： `Switch(config)# radius-server key rad123`	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。
ステップ 6	**radius-server dead-criteria tries***num-tries* 例： `Switch(config)# radius-server dead-criteria tries 30`	RADIUS サーバに送信されたメッセージへの応答がない場合に、このサーバが非アクティブであると見なすまでの送信回数を指定します。 指定できる *num-tries* の範囲は 1 ～ 100 です。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

HTTP サーバの設定

Web ベース認証を使用するには、Switchで HTTP サーバをイネーブルにする必要があります。 このサーバは HTTP または HTTPS のいずれかについてイネーブルにできます。

HTTP または HTTPS のいずれかでサーバをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip http server**
4. **ip http secure-server**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http server** 例： `Switch(config)# ip http server`	HTTP サーバをイネーブルにします。 Web ベース認証機能は、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。
ステップ 4	**ip http secure-server** 例： `Switch(config)# ip http secure-server`	HTTPS をイネーブルにします。 カスタム認証プロキシ Web ページを設定するか、成功ログインのリダイレクション URL を指定します。 （注） **ip http secure-server** コマンドを入力したときに、セキュア認証が確実に行われるようにするには、ユーザが HTTP 要求を送信した場合でも、ログイン ページは必ず HTTPS（セキュア HTTP）形式になるようにします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

認証プロキシ Web ページのカスタマイズ

Web ベースの認証中、Switchのデフォルト HTML ページではなく、代わりの HTML ページがユーザに表示されるように、Web 認証を設定できます。

この機能のための同等のセッション認識型ネットワーク設定の例については、『*Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』マニュアルの「アイデンティティ制御ポリシーの設定」の章の「Web ベース認証のパラメータ マップの設定」の項を参照してください。

カスタム認証プロキシ Web ページの使用を指定するには、次の手順を実行してください。

はじめる前に

Switchのフラッシュ メモリにカスタム HTML ファイルを保存します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admission proxy http login page file***device:login-filename*
4. **ip admission proxy http success page file***device:success-filename*
5. **ip admission proxy http failure page file***device:fail-filename*
6. **ip admission proxy http login expired page file***device:expired-filename*
7. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admission proxy http login page file***device:login-filename* 例： `Switch(config)# ip admission proxy http login page file disk1:login.htm`	Switchのメモリ ファイル システム内で、デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの場所を指定します。 *device:* はフラッシュ メモリです。
ステップ 4	**ip admission proxy http success page file***device:success-filename* 例： `Switch(config)# ip admission proxy http success page file disk1:success.htm`	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 5	**ip admission proxy http failure page file***device:fail-filename* 例： `Switch(config)# ip admission proxy http fail page file disk1:fail.htm`	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 6	**ip admission proxy http login expired page file***device:expired-filename* 例： `Switch(config)# ip admission proxy http login expired page file disk1:expired.htm`	デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

認証プロキシ Web ページの注意事項, （1673 ページ）

成功ログインに対するリダイレクション URL の指定

認証後に内部成功 HTML ページを効果的に置き換えユーザのリダイレクト先となる URL を指定するためには、次の手順を実行してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admission proxy http success redirect***url-string*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admission proxy http success redirect***url-string* 例： `Switch(config)# ip admission proxy http success redirect www.example.com`	デフォルトのログイン成功ページの代わりにユーザをリダイレクトする URL を指定します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

成功ログインに対するリダイレクト URL の注意事項, （1674 ページ）

Web ベース認証パラメータの設定

クライアントが待機時間中にウォッチ リストに掲載されるまで許容される失敗ログイン試行の最大回数を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admission max-login-attempts***number*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admission max-login-attempts***number* 例： `Switch(config)# ip admission max-login-attempts 10`	失敗ログイン試行の最大回数を設定します。 指定できる範囲は 1 ～ 2147483647 回です。 デフォルトは 5 分です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。

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

Web 認証ローカル バナーの設定

Web 認証が設定されているスイッチにローカル バナーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admission auth-proxy-banner http** [*banner-text* | *file-path*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip admission auth-proxy-banner http** [*banner-text*	*file-path*] 例： `Switch(config)# ip admission`	ローカル バナーをイネーブルにします。 （任意）*C banner-text C*（*C* は区切り文字）、またはバナーに表示されるファイル（たとえば、ロゴまたはテキスト ファイル）のファイル パスを入力して、カスタム バナーを作成します。

	コマンドまたはアクション	目的
	auth-proxy-banner http C My Switch C	
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

Web ベース認証キャッシュ エントリの削除

Web ベース認証キャッシュ エントリを削除するには、次の手順を実行します。

手順の概要

1. **enable**
2. **clear ip auth-proxy cache** {* | *host ip address*}
3. **clear ip admission cache** {* | *host ip address*}

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**clear ip auth-proxy cache** {* | *host ip address*} 例： `Switch# clear ip auth-proxy cache 192.168.4.5`	Delete 認証プロキシエントリを削除します。 キャッシュ エントリすべてを削除するには、アスタリスクを使用します。 シングルホストのエントリを削除するには、具体的な IP アドレスを入力します。
ステップ 3	**clear ip admission cache** {* | *host ip address*} 例： `Switch# clear ip admission cache 192.168.4.5`	Delete 認証プロキシエントリを削除します。 キャッシュ エントリすべてを削除するには、アスタリスクを使用します。 シングルホストのエントリを削除するには、具体的な IP アドレスを入力します。

Web ベース認証ステータスのモニタリング

すべてのインターフェイスまたは特定のポートに対する Web ベース認証設定を表示するには、このトピックのコマンドを使用します。

表 *149*：特権 *EXEC* 表示コマンド

コマンド	目的
show authentication sessions method webauth	FastEthernet、ギガビットイーサネット、または 10 ギガビットイーサネットのすべてのインターフェイスに対する Web ベースの認証設定を表示します。
show authentication sessions interface *type slot/port*[**details**]	FastEthernet、ギガビットイーサネット、または 10 ギガビット イーサネットの特定のインターフェイスに対する Web ベースの認証設定を表示します。 セッション認識型ネットワーク モードでは、**show access-session interface** コマンドを使用します。

第 62 章

ポート単位のトラフィック制御の設定

- ポートベースのトラフィック制御の概要，1694 ページ
- 機能情報の確認，1694 ページ
- ストーム制御に関する情報，1694 ページ
- ストーム制御の設定方法，1697 ページ
- 保護ポートに関する情報，1702 ページ
- 保護ポートの設定方法，1703 ページ
- 保護ポートのモニタリング，1705 ページ
- 次の作業，1705 ページ
- ポート ブロッキングに関する情報，1705 ページ
- ポート ブロッキングの設定方法，1706 ページ
- ポート ブロッキングのモニタリング，1708 ページ
- ポート セキュリティの前提条件，1708 ページ
- ポート セキュリティの制約事項，1708 ページ
- ポート セキュリティの概要，1708 ページ
- ポート セキュリティの設定方法，1714 ページ
- ポート セキュリティの設定例，1735 ページ
- プロトコル ストーム プロテクションに関する情報，1736 ページ
- プロトコル ストーム プロテクションの設定方法，1737 ページ
- プロトコル ストーム プロテクションのモニタリング，1738 ページ

ポートベースのトラフィック制御の概要

ポートベースのトラフィック制御は、特定トラフィック状態に応じてポート レベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。 次のポート ベースのトラフィック制御機能が、このガイドの記述対象の Cisco IOS リリースでサポートされます。

- ストーム制御
- 保護ポート
- ポート ブロッキング
- ポート セキュリティ
- プロトコル ストーム プロテクション

機能情報の確認

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

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

ストーム制御に関する情報

ストーム制御

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。 LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。 プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム制御（またはトラフィック抑制）は、インターフェイスからスイッチング バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。 スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

トラフィック アクティビティの測定方法

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 秒単位で受信するビット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 小さいフレームのトラフィック レートの秒単位のパケット数。 この機能は、グローバルにイネーブルです。 小さいフレームのしきい値は、各インターフェイスで設定されます。

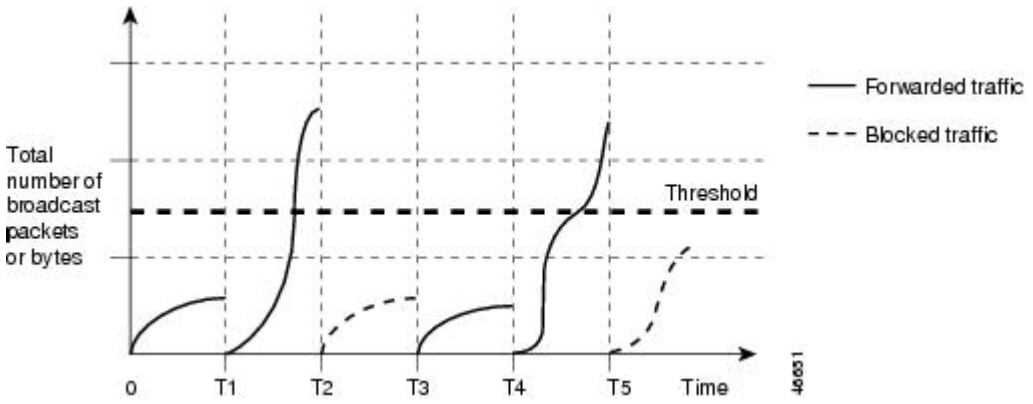
上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。 トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。 下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。 一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

（注） マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジ プロトコル データ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。 ただし、スイッチでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

トラフィック パターン

次の例は、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。

図 *115*：ブロードキャスト ストーム制御の例



T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。 指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。 したがって、T2 と T5 の後のインターバルの間、ブロードキャスト トラフィックがブロックされます。 その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を制御します。 しきい値が高いほど、通過できるパケット数が多くなります。 しきい値が 100% であれば、トラフィックに対する制限はありません。 値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。

（注） パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御の設定方法

ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。 着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数 % の差異が生じる可能性があります。

（注） ストーム制御は、物理インターフェイスでサポートされています。 また、EtherChannel でもストーム制御を設定できます。 ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、次の手順を実行します。

はじめる前に

ストーム制御は、物理インターフェイスでサポートされています。 また、EtherChannel でもストーム制御を設定できます。 ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps***bps* [*bps-low*] | **pps***pps* [*pps-low*]}
5. **storm-control action** {**shutdown** | **trap**}
6. **end**
7. **show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps***bps* [*bps-low*] | **pps***pps* [*pps-low*]} 例： `Switch(config-if)# storm-control unicast level 87 65`	ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。 デフォルトでは、ストーム制御はディセーブルに設定されています。 キーワードの意味は次のとおりです。 • *level* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。 上限しきい値に到達すると、ポートはトラフィックをブロックします。 指定できる範囲は 0.00 ～ 100.00 です。 • （任意）*level-low* には、下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。 この値は上限抑制値より小さいか、または等しくなければなりません。 トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。 下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。 指定できる範囲は 0.00 ～ 100.00 です。 しきい値に最大値（100%）を指定した場合、トラフィックの制限はなくなります。 しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。 • **bps***bps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをビット/秒で指定します（小数点第1位まで）。 上限しきい値に到達すると、ポートはトラフィックをブロックします。 指定できる範囲は 0.0 ～ 10000000000.0 です。

	コマンドまたはアクション	目的
		• （任意）*bps-low* には、下限しきい値レベルをビット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。 指定できる範囲は 0.0 ～ 10000000000.0 です。 • **pps***pps* には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。 指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low* には、下限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。 トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。 指定できる範囲は **0.0 ～** 10000000000.0 です。 BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号（k、m、g など）を使用できます。
ステップ 5	**storm-control action** {**shutdown** | **trap**} 例： `Switch(config-if)#` **`storm-control action trap`**	ストーム検出時に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。 • ストーム中、ポートを error-disable の状態にするには、**shutdown** キーワードを選択します。 • ストームが検出された場合、SNMP（簡易ネットワーク管理プロトコル）トラップを生成するには、**trap** キーワードを選択します。
ステップ 6	**end** 例： `Switch(config-if)#` **`end`**	特権 EXEC モードに戻ります。
ステップ 7	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**] 例： `Switch#` **`show storm-control gigabitethernet1/0/1 unicast`**	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。 トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御の設定が表示されます。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	例： `Switch# copy running-config startup-config`	

スモール フレーム到着レートの設定

67 バイト未満の着信 VLAN タグ付きパケットは、小さいフレームと見なされます。 このパケットはスイッチにより転送されますが、スイッチ ストーム制御カウンタを増加させません。

スイッチ上の小さいフレームの着信機能をグローバルにイネーブルにして、各インターフェイスのパケットの小さいフレームのしきい値を設定します。 最小サイズよりも小さく、指定されたレート（しきい値）で着信するパケットは、ポートがディセーブルにされた後はドロップされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **errdisable detect cause small-frame**
4. **errdisable recovery interval***interval*
5. **errdisable recovery cause small-frame**
6. **interface***interface-id*
7. **small-frame violation-rate***pps*
8. **end**
9. **show interfaces***interface-id*
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**errdisable detect cause small-frame** 例： `Switch(config)# errdisable detect cause small-frame`	スイッチ上の小さいフレームの着信レート機能をイネーブルにします。
ステップ 4	**errdisable recovery interval***interval* 例： `Switch(config)# errdisable recovery interval 60`	（任意）指定された errdisable ステートから回復する時間を指定します。
ステップ 5	**errdisable recovery cause small-frame** 例： `Switch(config)# errdisable recovery cause small-frame`	（任意）小さいフレームの着信によりポートが errdisable になった後、そのポートを自動的に再イネーブルにするリカバリ時間を設定します。 ストーム制御は、物理インターフェイスでサポートされています。 また、EtherChannel でもストーム制御を設定できます。 ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。
ステップ 6	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 7	**small-frame violation-rate***pps* 例： `Switch(config-if)# small-frame violation rate 10000`	インターフェイスが着信パケットをドロップしてポートを errdisable にするようにしきい値レートを設定します。範囲は、1 ～ 10,000 パケット/秒（pps）です。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**show interfaces***interface-id* 例： `Switch# show interfaces gigabitethernet1/0/2`	設定を確認します。
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

保護ポートに関する情報

保護ポート

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ 2 トラフィックが転送されないように設定する必要があります。 このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。 データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。 保護ポート間を通過するすべてのデータ トラフィックは、レイヤ 3 デバイスを介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

スイッチ スタックは論理的には 1 つのスイッチを表しているため、レイヤ 2 トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチ スタックの保護ポート間では転送されません。

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

保護ポートのガイドライン

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。 ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

保護ポートの設定方法

保護ポートの設定

はじめる前に

保護ポートは事前定義されていません。 これは設定する必要があるタスクです。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport protected**
5. **end**
6. **show interfaces***interface-id***switchport**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport protected** 例： `Switch(config-if)# switchport protected`	インターフェイスを保護ポートとして設定します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

保護ポートのモニタリング

表 *150*：保護ポートの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

次の作業

•

ポート ブロッキングに関する情報

ポート ブロッキング

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。 未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。 未知のユニキャストおよびマルチキャスト トラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにします。

（注） マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。 ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

ポート ブロッキングの設定方法

インターフェイスでのフラッディング トラフィックのブロッキング

はじめる前に

インターフェイスは物理インターフェイスまたは EtherChannel グループのいずれも可能です。ポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport block multicast**
5. **switchport block unicast**
6. **end**
7. **show interfaces***interface-id***switchport**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**switchport block multicast** 例： `Switch(config-if)# switchport block multicast`	ポートからの未知のマルチキャストの転送をブロックします。 （注） 純粋なレイヤ 2 マルチキャスト トラフィックだけがブロックされます。 ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。
ステップ 5	**switchport block unicast** 例： `Switch(config-if)# switchport block unicast`	ポートからの未知のユニキャストの転送をブロックします。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ポート ブロッキングのモニタリング

表 *151* : ポート ブロッキングの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

ポート セキュリティの前提条件

（注） 最大値をインターフェイス上ですでに設定されているセキュア アドレスの数より小さい値に設定しようとすると、コマンドが拒否されます。

ポート セキュリティの制約事項

スイッチまたはスイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。 この数は、アクティブ スイッチ データベース管理（SDM）テンプレートによって決まります。この数は使用可能な MAC アドレスの合計で、他のレイヤ 2 機能で使用されるものや、インターフェイスで設定されたその他のセキュアな MAC アドレスが含まれています。

ポート セキュリティの概要

ポート セキュリティ

ポート セキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。 セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレス グループ以外の送信元アドレスを持つパケットを転送しません。 セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュア ポートとしてポートを設定し、セキュア MAC アドレスが最大数に達した場合、ポートにアクセスを試みるステーションの MAC アドレスが識別されたセキュア MAC アドレスのいずれとも一致しないので、セキュリティ違反が発生します。また、あるセキュア ポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュア ポートにアクセスしようとしたときにも、違反のフラグが立てられます。

関連トピック

ポート セキュリティのイネーブル化および設定, （1714 ページ）
ポート セキュリティの設定例, （1735 ページ）

セキュア MAC アドレスのタイプ

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- スタティック セキュア MAC アドレス：**switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレス テーブルに保存されたのち、スイッチの実行コンフィギュレーションに追加されます。
- ダイナミック セキュア MAC アドレス：動的に設定されてアドレス テーブルにのみ保存され、スイッチの再起動時に削除されます。
- スティッキー セキュア MAC アドレス：動的に学習することも、手動で設定することもできます。アドレス テーブルに保存され、実行コンフィギュレーションに追加されます。 このアドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

スティッキ セキュア MAC アドレス

スティッキー ラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキー セキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。インターフェイスはスティッキ ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキー セキュア MAC アドレスに変換します。 すべてのスティッキー セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキー セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション）に、自動的には反映されません。 スティッキー セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。 スティッキセキュア アドレスを保存しない場合、アドレスは失われます。

スティッキ ラーニングがディセーブルの場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレス テーブルに追加されている状態で、アドレス テーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。

違反が発生した場合の対処に基づいて、次の 3 種類の違反モードのいずれかにインターフェイスを設定できます。

- protect（保護）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。

（注） トランク ポートに protect 違反モードを設定することは推奨しません。 保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

- restrict（制限）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。 SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
- shutdown（シャットダウン）：ポート セキュリティ違反により、インターフェイスが error-disabled になり、ただちにシャットダウンされます。そのあと、ポートの LED が消灯します。 セキュア ポートが error-disabled ステートの場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこのステートを解除するか、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにできます。 これは、デフォルトのモードです。
- shutdown vlan（VLAN シャットダウン）：VLAN 単位でセキュリティ違反モードを設定するために使用します。 このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。

次の表に、ポート セキュリティをインターフェイスに設定した場合の違反モードおよび対処について示します。

表 *152*：セキュリティ違反モードの処置

違反モード	トラフィックの転送 [21]	SNMP トラップの送信	Syslog メッセージの送信	エラー メッセージの表示 [22]	違反カウンタの増加	ポートのシャットダウン
protect	No	No	No	No	No	No
restrict	No	Yes	Yes	No	Yes	No
shutdown	No	No	No	No	Yes	Yes
shutdown vlan	No	No	Yes	No	Yes	No [23]

21 十分な数のセキュア MAC アドレスを削除するまで未知の送信元アドレスを持つパケットがドロップされます。
22 セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラー メッセージを返します。
23 違反が発生した VLAN のみシャットダウンします。

ポート セキュリティ エージング

ポート上のすべてのセキュア アドレスにエージング タイムを設定するには、ポート セキュリティ エージングを使用します。 ポートごとに 2 つのタイプのエージングがサポートされています。

- absolute：指定されたエージング タイムの経過後に、ポート上のセキュア アドレスが削除されます。
- inactivity：指定されたエージング タイムの間、セキュア アドレスが非アクティブであった場合に限り、ポート上のセキュア アドレスが削除されます。

関連トピック

ポート セキュリティ エージングのイネーブル化および設定, （1720 ページ）

デフォルトのポート セキュリティ設定

表 *153*：デフォルトのポート セキュリティ設定

機能	デフォルト設定
ポート セキュリティ	ポート上でディセーブル
スティッキー アドレス ラーニング	ディセーブル

機能	デフォルト設定
ポートあたりのセキュア MAC アドレスの最大数	1。
違反モード	shutdown。 セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。
ポート セキュリティ エージング	ディセーブル エージング タイムは 0 スタティック エージングはディセーブル タイプは absolute

ポート セキュリティの設定時の注意事項

- ポート セキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。 セキュア ポートをダイナミック アクセス ポートにすることはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- （注） 音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。 ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。 Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。 1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。 複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュア アドレスを設定する必要があります。
- トランク ポートがポート セキュリティで設定され、データ トラフィックのアクセス VLAN および音声トラフィックのアクセス VLAN に割り当てられている場合は、**switchport voice** および **switchport priority extend** インターフェイス コンフィギュレーション コマンドを入力しても効果はありません。

  接続装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレス、音声 VLAN の IP アドレスの順に要求すると、アクセス VLAN だけが IP アドレスに割り当てられます。
- インターフェイスの最大セキュア アドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。 新しい値が前

回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。

- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングをサポートしていません。

次の表に、他のポートベース機能と互換性のあるポート セキュリティについてまとめます。

表 *154*：ポート セキュリティと他のポートベース機能との互換性

ポート タイプまたはポートの機能	ポート セキュリティとの互換性
DTP [24] ポート[25]	No
トランク ポート	Yes
ダイナミックアクセス ポート[26]	No
ルーテッド ポート	No
SPAN 送信元ポート	Yes
SPAN 宛先ポート	No
EtherChannel	Yes
トンネリング ポート	Yes
保護ポート	Yes
IEEE 802.1x ポート	Yes
音声 VLAN ポート[27]	Yes
IP ソース ガード	Yes
ダイナミック アドレス解決プロトコル（ARP）インスペクション	Yes
Flex Link	Yes

24 DTP = Dynamic Trunking Protocol
25 **switchport mode dynamic** インターフェイス コンフィギュレーション コマンドで設定されたポート。
26 **switchport access vlan-dynamic** インターフェイス コンフィギュレーション コマンドで設定される Vlan Query Protocol（VQP）ポート。
27 ポートに最大限可能なセキュアなアドレスを設定します（アクセス VLAN で可能なセキュアなアドレスの最大数に 2 を加えた数）。

ポートベースのトラフィック制御の概要

ポートベースのトラフィック制御は、特定トラフィック状態に応じてポート レベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。 次のポート ベースのトラフィック制御機能が、このガイドの記述対象の Cisco IOS リリースでサポートされます。

- ストーム制御
- 保護ポート
- ポート ブロッキング
- ポート セキュリティ
- プロトコル ストーム プロテクション

ポート セキュリティの設定方法

ポート セキュリティのイネーブル化および設定

はじめる前に

このタスクは、ポートにアクセスできるステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制約します。

手順の概要

1. **enable**
2. **configureterminal**
3. **port-security mac-address forbidden***mac address*
4. **interface***interface-id*
5. **switchport mode** {**access** | **trunk**}
6. **switchport voice vlan***vlan-id*
7. **switchport port-security**
8. **switchport port-security [maximum***value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]
9. **switchport port-security violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}
10. **switchport port-security [mac-address***mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}]
11. **switchport port-security mac-address sticky**
12. **switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]
13. **switchport port-security mac-address forbidden***mac address*
14. **end**
15. **show port-security**
16. **show running-config**
17. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**port-security mac-address forbidden***mac address* 例： `Switch(config)# port-security mac-address forbidden 2.2.2`	すべてのインターフェイスのポートセキュリティで禁止するMACアドレスを指定します。

	コマンドまたはアクション	目的
ステップ 4	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport mode** {**access** | **trunk**} 例： `Switch(config-if)# switchport mode access`	インターフェイス スイッチポート モードを access または trunk に設定します。デフォルトモード（dynamic auto）のインターフェイスは、セキュア ポートとして設定できません。
ステップ 6	**switchport voice vlan***vlan-id* 例： `Switch(config-if)# switchport voice vlan 22`	ポート上で音声 VLAN をイネーブルにします。 vlan-id：音声トラフィックに使用する VLAN を指定します。
ステップ 7	**switchport port-security** 例： `Switch(config-if)# switchport port-security`	インターフェイス上でポート セキュリティをイネーブルにします。
ステップ 8	**switchport port-security** [**maximum***value* [**vlan** {*vlan-list* | {**access** | **voice**}}]] 例： `Switch(config-if)# switchport port-security maximum 20`	（任意）インターフェイスの最大セキュア MAC アドレス数を設定します。 スイッチまたはスイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。 この値は、アクティブなスイッチングデータベース管理（SDM）テンプレートによって決まります。この値は、使用可能な MAC アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数を表します。 （任意）**vlan**：VLAN 当たりの最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-list*：トランク ポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、VLAN 単位の最大値を設定できます。 VLAN を指定しない場合、VLAN ごとの最大値が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。

	コマンドまたはアクション	目的
		• **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。
ステップ 9	**switchport port-security violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**} 例： `Switch(config-if)# switchport port-security violation restrict`	（任意）違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。 • **protect**：ポート セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。 （注） トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。 • **restrict**：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。 SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。 • **shutdown**：違反が発生すると、インターフェイスが error-disabled になり、ポートの LED が消灯します。 SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。 • **shutdown vlan**：VLAN 単位でセキュリティ違反モードを設定するために使用します。 このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。 （注） セキュア ポートが error-disabled ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力して、このステートから回復させることができます。手動で再びイネーブルにするには、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface vlan** 特権 EXEC コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 10	**switchport port-security [mac-address***mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}] 例： `Switch(config-if)# switchport port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice`	（任意）インターフェイスのセキュアMACアドレスを入力します。 このコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。 設定したセキュアMACアドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。 （注） このコマンドの入力後にスティッキー ラーニングをイネーブルにすると、動的に学習されたセキュア アドレスがスティッキー セキュア MAC アドレスに変換されて実行コンフィギュレーションに追加されます。 （任意）**vlan**：VLAN 当たりの最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポートで、VLAN ID および MAC アドレスを指定できます。 VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。 インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。
ステップ 11	**switchport port-security mac-address sticky** 例： `Switch(config-if)# switchport port-security mac-address sticky`	（任意）インターフェイス上でスティッキ ラーニングをイネーブルにします。
ステップ 12	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}] 例： `Switch(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice`	（任意）スティッキーセキュアMACアドレスを入力し、必要な回数だけコマンドを繰り返します。 設定したセキュアMACアドレスの数が最大数より少ない場合、残りのMACアドレスは動的に学習されてスティッキーセキュアMACアドレスに変換され、実行コンフィギュレーションに追加されます。 （注） このコマンドの入力前にスティッキー ラーニングをイネーブルにしないと、エラー メッセージが表示されてスティッキー セキュア MAC アドレスを入力できません。 （任意）**vlan**：VLAN 当たりの最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。

	コマンドまたはアクション	目的
		• *vlan-id*：トランク ポートで、VLAN ID および MAC アドレスを指定できます。 VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。
ステップ 13	**switchport port-security mac-address forbidden***mac address* 例： `Switch(config-if)# switchport port-security mac-address forbidden 2.2.2`	特定のインターフェイスのポート セキュリティで禁止する MAC アドレスを指定します。
ステップ 14	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 15	**show port-security** 例： `Switch# show port-security`	入力を確認します。
ステップ 16	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 17	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ポート セキュリティ，（1674 ページ）
ポート セキュリティ，（1708 ページ）
ポート セキュリティの設定例，（1735 ページ）

ポート セキュリティ エージングのイネーブル化および設定

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュア ポート上のデバイスを削除および追加し、なおかつポート上のセキュア アドレス数を制限できます。セキュア アドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport port-security aging** {**static** | **time***time* | **type** {**absolute** | **inactivity**}}
5. **end**
6. **show port-security** [**interface***interface-id*] [**address**]
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
	gigabitethernet1/0/1	
ステップ 4	**switchport port-security aging** {**static** | **time***time* | **type** {**absolute** | **inactivity**}} 例： `Switch(config-if)# switchport port-security aging time 120`	セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにします。またはエージング タイムやタイプを設定します。 （注） スイッチは、スティッキー セキュア アドレスのポートセキュリティ エージングをサポートしていません。 このポートに、スタティックに設定されたセキュア アドレスのエージングをイネーブルにする場合は、**static** を入力します。 *time* には、このポートのエージング タイムを指定します。 有効な範囲は、0 ～ 1440 分です。 **type** には、次のキーワードのいずれか 1 つを選択します。 • **absolute**：エージング タイプを絶対エージングとして設定します。 このポートのセキュア アドレスはすべて、指定した時間（分単位）が経過すると期限切れになり、セキュア アドレス リストから削除されます。 • **inactivity**：エージング タイプを非アクティブ エージングとして設定します。 指定された time 期間中にセキュア送信元アドレスからのデータ トラフィックがない場合に限り、このポートのセキュア アドレスが期限切れになります。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show port-security** [**interface***interface-id*] [**address**] 例： `Switch# show port-security interface gigabitethernet1/0/1`	入力を確認します。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ポート セキュリティ エージング，（1711 ページ）

機能情報の確認

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

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

ストーム制御に関する情報

ストーム制御

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。 LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。 プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム制御（またはトラフィック抑制）は、インターフェイスからスイッチング バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。 スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

トラフィック アクティビティの測定方法

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 秒単位で受信するビット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 小さいフレームのトラフィック レートの秒単位のパケット数。 この機能は、グローバルにイネーブルです。 小さいフレームのしきい値は、各インターフェイスで設定されます。

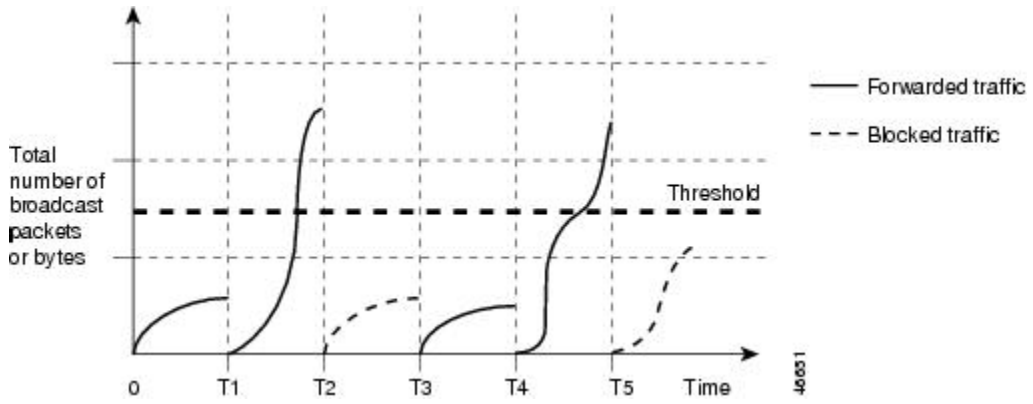
上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。 トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。 下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。 一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

（注） マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジ プロトコル データ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。 ただし、スイッチでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

トラフィック パターン

次の例は、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。

図 *116*：ブロードキャスト ストーム制御の例



T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。 指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。 したがって、T2 と T5 の後のインターバルの間、ブロードキャストトラフィックがブロックされます。 その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を制御します。 しきい値が高いほど、通過できるパケット数が多くなります。 しきい値が 100% であれば、トラフィックに対する制限はありません。 値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。

（注） パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御の設定方法

ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。 着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数 % の差異が生じる可能性があります。

（注） ストーム制御は、物理インターフェイスでサポートされています。 また、EtherChannel でもストーム制御を設定できます。 ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、次の手順を実行します。

はじめる前に

ストーム制御は、物理インターフェイスでサポートされています。 また、EtherChannel でもストーム制御を設定できます。 ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps***bps* [*bps-low*] | **pps***pps* [*pps-low*]}
5. **storm-control action** {**shutdown** | **trap**}
6. **end**
7. **show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps***bps* [*bps-low*] | **pps***pps* [*pps-low*]} 例： `Switch(config-if)# storm-control unicast level 87 65`	ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。 デフォルトでは、ストーム制御はディセーブルに設定されています。 キーワードの意味は次のとおりです。 • *level* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。 上限しきい値に到達すると、ポートはトラフィックをブロックします。 指定できる範囲は 0.00 ～ 100.00 です。 • （任意）*level-low* には、下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。 この値は上限抑制値より小さ

	コマンドまたはアクション	目的
		いか、または等しくなければなりません。 トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。 下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。 指定できる範囲は 0.00 ～ 100.00 です。 しきい値に最大値（100%）を指定した場合、トラフィックの制限はなくなります。 しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャストトラフィックがブロックされます。 • **bps***bps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをビット/秒で指定します（小数点第1位まで）。 上限しきい値に到達すると、ポートはトラフィックをブロックします。 指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*bps-low* には、下限しきい値レベルをビット/秒で指定します（小数点第1位まで）。 この値は上限しきい値レベル以下の値である必要があります。 トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。 指定できる範囲は 0.0 ～ 10000000000.0 です。 • **pps***pps* には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。 上限しきい値に到達すると、ポートはトラフィックをブロックします。 指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low* には、下限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。 この値は上限しきい値レベル以下の値である必要があります。 トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。 指定できる範囲は **0.0 ～** 10000000000.0 です。 BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号（k、m、g など）を使用できます。
ステップ 5	**storm-control action {shutdown | trap}** 例： `Switch(config-if)#` **`storm-control action trap`**	ストーム検出時に実行するアクションを指定します。 デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。 • ストーム中、ポートを error-disable の状態にするには、**shutdown** キーワードを選択します。 • ストームが検出された場合、SNMP（簡易ネットワーク管理プロトコル）トラップを生成するには、**trap** キーワードを選択します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**] 例： `Switch# show storm-control gigabitethernet1/0/1 unicast`	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。 トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御の設定が表示されます。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スモール フレーム到着レートの設定

67 バイト未満の着信 VLAN タグ付きパケットは、小さいフレームと見なされます。 このパケットはスイッチにより転送されますが、スイッチ ストーム制御カウンタを増加させません。

スイッチ上の小さいフレームの着信機能をグローバルにイネーブルにして、各インターフェイスのパケットの小さいフレームのしきい値を設定します。 最小サイズよりも小さく、指定されたレート（しきい値）で着信するパケットは、ポートがディセーブルにされた後はドロップされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **errdisable detect cause small-frame**
4. **errdisable recovery interval***interval*
5. **errdisable recovery cause small-frame**
6. **interface***interface-id*
7. **small-frame violation-rate***pps*
8. **end**
9. **show interfaces***interface-id*
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**errdisable detect cause small-frame** 例： `Switch(config)# errdisable detect cause small-frame`	スイッチ上の小さいフレームの着信レート機能をイネーブルにします。
ステップ 4	**errdisable recovery interval***interval* 例： `Switch(config)# errdisable recovery interval 60`	（任意）指定された errdisable ステートから回復する時間を指定します。

	コマンドまたはアクション	目的
ステップ 5	**errdisable recovery cause small-frame** 例： `Switch(config)# errdisable recovery cause small-frame`	（任意）小さいフレームの着信によりポートが errdisable になった後、そのポートを自動的に再イネーブルにするリカバリ時間を設定します。 ストーム制御は、物理インターフェイスでサポートされています。 また、EtherChannel でもストーム制御を設定できます。 ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。
ステップ 6	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 7	**small-frame violation-rate***pps* 例： `Switch(config-if)# small-frame violation rate 10000`	インターフェイスが着信パケットをドロップしてポートを errdisable にするようにしきい値レートを設定します。範囲は、1 ～ 10,000 パケット/秒（pps）です。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show interfaces***interface-id* 例： `Switch# show interfaces gigabitethernet1/0/2`	設定を確認します。
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

保護ポートに関する情報

保護ポート

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ 2 トラフィックが転送されないように設定する必要があります。 このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。 データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。 保護ポート間を通過するすべてのデータ トラフィックは、レイヤ 3 デバイスを介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

スイッチ スタックは論理的には 1 つのスイッチを表しているため、レイヤ 2 トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチ スタックの保護ポート間では転送されません。

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

保護ポートのガイドライン

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。 ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

保護ポートの設定方法

保護ポートの設定

はじめる前に

保護ポートは事前定義されていません。 これは設定する必要があるタスクです。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport protected**
5. **end**
6. **show interfaces***interface-id***switchport**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport protected** 例： `Switch(config-if)# switchport protected`	インターフェイスを保護ポートとして設定します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ **6**	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。
ステップ **7**	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ **8**	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

保護ポートのモニタリング

表 ***155***：保護ポートの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

次の作業

•

ポート ブロッキングに関する情報

ポート ブロッキング

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。 未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。 未知のユニキャストおよびマルチキャスト トラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにします。

（注） マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。 ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

ポート ブロッキングの設定方法

インターフェイスでのフラッディング トラフィックのブロッキング

はじめる前に

インターフェイスは物理インターフェイスまたは EtherChannel グループのいずれも可能です。ポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport block multicast**
5. **switchport block unicast**
6. **end**
7. **show interfaces***interface-id***switchport**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport block multicast** 例： `Switch(config-if)# switchport block multicast`	ポートからの未知のマルチキャストの転送をブロックします。 （注） 純粋なレイヤ 2 マルチキャスト トラフィックだけがブロックされます。 ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。
ステップ 5	**switchport block unicast** 例： `Switch(config-if)# switchport block unicast`	ポートからの未知のユニキャストの転送をブロックします。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。

	コマンドまたはアクション	目的
ステップ **8**	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ **9**	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ポート ブロッキングのモニタリング

表 ***156***：ポート ブロッキングの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。

ポート セキュリティの設定例

次に、ポート上でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する例を示します。 違反モードはデフォルトです。スタティック セキュア MAC アドレスは設定せず、スティッキー ラーニングはイネーブルです。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 上にスタティック セキュア MAC アドレスを設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.0200.0004 vlan 3
```

次に、ポートのスティッキーポートセキュリティをイネーブルにする例を示します。データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュア アドレスの総数を 20 に設定します（データ VLAN に 10、音声 VLAN に 10 を割り当てます）。

```
Switch(config)# interface tengigabitethernet1/0/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

関連トピック

ポート セキュリティ，（1708 ページ）
ポート セキュリティのイネーブル化および設定，（1714 ページ）

プロトコル ストーム プロテクションに関する情報

プロトコル ストーム プロテクション

スイッチがアドレス解決プロトコル（ARP）または制御パケットでフラッドされると、CPU の高い使用率により CPU のオーバーロードが発生する可能性があります。 これらの問題は、次のように発生します。

- プロトコル制御パケットが受信されず、ネイバーの隣接がドロップされるため、ルーティング プロトコルがフラップする場合があります。
- スパニングツリープロトコル（STP）ブリッジプロトコルデータ ユニット（BPDU）が送受信されないため、STP が再収束します。
- CLI が遅くなるか応答しなくなります。

プロトコル ストーム プロテクションを使用すると、パケットのフロー レートの上限しきい値を指定して、制御パケットが送信されるレートを制御できます。 サポートされるプロトコルは、ARP、ARP スヌーピング、Dynamic Host Configuration Protocol（DHCP）v4、DHCP スヌーピング、インターネット グループ管理プロトコル（IGMP）、および IGMP スヌーピングです。

パケットのレートが定義されたしきい値を超えると、スイッチは指定されたポートに着信したすべてのトラフィックを 30 秒間ドロップします。 パケット レートが再度計測され、必要な場合はプロトコル ストーム プロテクションが再度適用されます。

より強力な保護が必要な場合は、仮想ポートを手動で errdisable にし、その仮想ポートのすべての着信トラフィックをブロックできます。 また、手動で仮想ポートをイネーブルにしたり、仮想ポートの自動再イネーブル化の時間間隔を設定することもできます。

（注） 超過したパケットは、2 つ以下の仮想ポートにおいてドロップされます。

仮想ポートのエラー ディセーブル化は、EtherChannel インターフェイスと Flexlink インターフェイスではサポートされません。

デフォルトのプロトコル ストーム プロテクションの設定

プロトコル ストーム プロテクションはデフォルトでディセーブルです。 これがイネーブルになると、仮想ポートの自動リカバリがデフォルトでディセーブルになります。

プロトコル ストーム プロテクションの設定方法

プロトコル ストーム プロテクションのイネーブル化

手順の概要

1. **enable**
2. **configureterminal**
3. **psp** {**arp** | **dhcp** | **igmp**} pps *value*
4. **errdisable detect cause psp**
5. **errdisable recovery interval***time*
6. **end**
7. **show psp config** {**arp** | **dhcp** | **igmp**}

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**psp** {**arp** | **dhcp** | **igmp**} pps *value* 例： `Switch(config)# psp dhcp pps 35`	ARP、IGMP、またはDHCPに対してプロトコル ストーム プロテクションを設定します。 *value*には、1秒あたりのパケット数のしきい値を指定します。トラフィックがこの値を超えると、プロトコル ストーム プロテクションが適用されます。 範囲は毎秒5～50パケットです。
ステップ 4	**errdisable detect cause psp** 例： `Switch(config)# errdisable detect cause psp`	（任意）プロトコル ストーム プロテクションの errdisable 検出をイネーブルにします。 この機能がイネーブルになると、仮想ポートが errdisable になります。 この機能がディセーブルになると、そのポートは、ポートを errdisable にせずに超過したパケットをドロップします。
ステップ 5	**errdisable recovery interval***time* 例： `Switch`	（任意）errdisable の仮想ポートの自動リカバリ時間を秒単位で設定します。 仮想ポートが errdisable の場合、この時間を過ぎるとスイッチは自動的にリカバリします。 指定できる範囲は 30 ～ 86400 秒です。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show psp config** {**arp** | **dhcp** | **igmp**} 例： `Switch# show psp config dhcp`	入力を確認します。

プロトコル ストーム プロテクションのモニタリング

コマンド	目的
show psp config {**arp** | **dhcp** | **igmp**}	入力内容を確認します。

第 63 章

IPv6 ファーストホップセキュリティの設定

- 機能情報の確認，1739 ページ
- IPv6 でのファーストホップセキュリティの前提条件，1740 ページ
- IPv6 でのファーストホップセキュリティの制約事項，1740 ページ
- IPv6 でのファーストホップセキュリティに関する情報，1740 ページ
- IPv6 スヌーピングポリシーの設定方法，1743 ページ
- IPv6 バインディングテーブルの内容を設定する方法，1747 ページ
- IPv6 ネイバー探索インスペクションポリシーの設定方法，1749 ページ
- IPv6 ルータアドバタイズメントガードポリシーの設定方法，1753 ページ
- IPv6 DHCP ガードポリシーの設定方法，1759 ページ
- IPv6 ソースガードの設定方法，1764 ページ
- IPv6 ソースガードの設定方法，1766 ページ
- IPv6 プレフィックスガードの設定方法，1770 ページ

機能情報の確認

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

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

IPv6 でのファースト ホップ セキュリティの前提条件

- IPv6 がイネーブルになった必要な SDM テンプレートが設定されていること。
- IPv6 ネイバー探索機能についての知識が必要です。

IPv6 でのファースト ホップ セキュリティの制約事項

- 次の制限は、FHS ポリシーを EtherChannel インターフェイスに適用する場合に該当します（ポート チャネル）。
  - FHS ポリシーがアタッチされた物理ポートは EtherChannel グループに参加することができません。
  - FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。

IPv6 でのファースト ホップ セキュリティに関する情報

IPv6 のファーストホップ セキュリティ（FHS IPv6）は、ポリシーを物理インターフェイス、または VLAN にアタッチできる一連の IPv6 セキュリティ機能です。 IPv6 ソフトウェア ポリシー データベース サービスは、これらのポリシーを保存しアクセスします。 ポリシーを設定または変更すると、ポリシー属性はソフトウェア ポリシーデータベースに保存または更新され、その後指定したとおりに適用されます。 次の IPv6 ポリシーが現在サポートされています。

- IPv6 スヌーピング ポリシー：IPv6 スヌーピング ポリシーは、IPv6 内の FHS で使用できるほとんどの機能をイネーブルにできるコンテナ ポリシーとして機能します。
- IPv6 FHS バインディング テーブルの内容：スイッチに接続された IPv6 ネイバーのデータベース テーブルはネイバー探索（ND）プロトコル スヌーピングなどの情報ソースから作成されます。 このデータベースまたはバインディング テーブルは、リンク層アドレス（LLA）、IPv4 または IPv6 アドレス、およびスプーフィングやリダイレクト攻撃を防止するためにネイバーのプレフィックス バインディングを検証するために、さまざまな IPv6 ガード機能（IPv6 ND インスペクションなど）によって使用されます。
- IPv6 ネイバー探索インスペクション：IPv6 ND インスペクションは、レイヤ 2 ネイバー テーブル内のステートレス自動設定アドレスのバインディングを学習し、保護します。 IPv6 ND 検査は、信頼できるバインディング テーブル データベースを構築するためにネイバー探索メッセージを分析します。準拠していない IPv6 ネイバー探索メッセージはドロップされます。 ND メッセージは、その IPv6 からメディア アクセス コントロール（MAC）へのマッピングが検証可能な場合に信頼できると見なされます。
  この機能によって、DAD、アドレス解決、ルータ ディスカバリ、ネイバー キャッシュに対する攻撃などの、ND メカニズムに固有の脆弱性のいくつかが軽減されます。

- IPv6 ルータ アドバタイズメント ガード：IPv6 ルータ アドバタイズメント（RA）ガード機能を使用すると、ネットワーク管理者は、ネットワーク スイッチ プラットフォームに到着した不要または不正な RA ガード メッセージをブロックまたは拒否できます。 RA は、リンクで自身をアナウンスするためにルータによって使用されます。 RA ガード機能は、これらの RA を分析して、未承認のルータによって送信された偽の RA をフィルタリングして除外します。 ホスト モードでは、ポートではルータ アドバタイズメントとルータ リダイレクト メッセージはすべて許可されません。 RA ガード機能は、レイヤ 2 デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。 レイヤ 2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。 RA フレームの内容が検証されない場合は、RA はドロップされます。
- IPv6 DHCP ガード：IPv6 DHCP ガード機能は、承認されない DHCPv6 サーバおよびリレーエージェントからの返信およびアドバタイズメントメッセージをブロックします。 IPv6 DHCP ガードは、偽造されたメッセージがバインディング テーブルに入るのを防ぎ、DHCPv6 サーバまたは DHCP リレーからデータを受信することが明示的に設定されていないポートで受信された DHCPv6 サーバ メッセージをブロックできます。 この機能を使用するには、ポリシーを設定してインターフェイスまたは VLAN にアタッチします。 DHCP ガード パケットをデバッグするには、**debug ipv6 snooping dhcp-guard** 特権 EXEC コマンドを使用します。
- IPv6 ソース ガード：IPv4 ソース ガードと同様、IPv6 ソース ガードは送信元アドレス スプーフィングを防ぐために、送信元アドレスまたはプレフィックスを検証します。

  ソース ガードでは、送信元または宛先アドレスに基づいてトラフィックを許可または拒否するようにハードウェアをプログラムします。 ここでは、データ パケットのトラフィックのみを処理します。

  IPv6 ソース ガードとは、IPv6 バインディング テーブルを使用して PACL をインストールし、ホストが無効な IPv6 送信元アドレスを持つパケットを送信しないようにする機能です。

  ソース ガード パケットをデバッグするには、debug ipv6 snooping source-guard 特権 EXEC コマンドを使用します。

  （注） IPv6 PACL 機能は、入力方向だけでサポートされ、出力方向ではサポートされません。

  次の制約事項が適用されます。

  - FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。
  - IPv6 ソース ガードがスイッチ ポートでイネーブルになっている場合は、そのスイッチ ポートが属するインターフェイスで NDP または DHCP スヌーピングをイネーブルにする必要があります。 そうしないと、このポートからのすべてのデータ トラフィックがブロックされます。
  - IPv6 ソース ガード ポリシーを VLAN に適用することはできません。 インターフェイス レベルのみでサポートされています。

- IPv6 ソースガードとプレフィックスガードは同時に使用できません。 ポリシーをインターフェイスに付加する際は、「アドレスを確認」するか「プレフィックスを確認」する必要はありますが、両方を確認する必要はありません。
- PVLAN と送信元/プレフィックスガードは同時に適用できません。

IPv6 送信元ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Source Guard」の章を参照してください。

- IPv6 プレフィックスガード：IPv6 プレフィックスガードは、IPv6 送信元ガード機能内で動作し、デバイスがトポロジに不正なアドレスから発信されたトラフィックを拒否できるようにします。 IPv6 プレフィックスガードは、IPv6 プレフィックスが DHCP プレフィックス委任を使用してデバイス（ホームゲートウェイなど）に委任される場合によく使用されています。 この機能は、リンクに割り当てられたアドレスの範囲を検出し、この範囲に入っていないアドレスを発信元とするトラフィックをブロックします。

  IPv6 プレフィックスガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Prefix Guard」の章を参照してください。

- IPv6 宛先ガード：IPv6 宛先ガード機能は、IPv6 ネイバー探索で動作し、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決します。 アドレスグリーニング機能に依存して、リンク上でアクティブなすべての宛先をバインディングテーブルに挿入してから、バインディングテーブルで宛先が見つからなかったときに実行される解決をブロックします。

  （注） IPv6 宛先ガードはレイヤ 3 にのみ推奨されます。 レイヤ 2 については推奨しません。

  IPv6 宛先ガードに関する詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Destination Guard」の章を参照してください。

- IPv6 ネイバー検索マルチキャスト抑制：IPv6 ネイバー検索マルチキャスト抑制機能は、IPv6 のスヌーピング機能で、スイッチまたはワイヤレスコントローラで実行し、適切なリンク動作に必要な制御トラフィック量を削減するために使用されます。

- DHCPv6 リレー：Lightweight DHCPv6 リレーエージェント：Lightweight DHCPv6 リレーエージェント機能を使用するとリンクレイヤブリッジング（非ルーティング）機能を実行するアクセスノードによってリレーエージェント情報が挿入されます。 Lightweight DHCPv6 リレーエージェント（LDRA）機能は、DSL アクセスマルチプレクサ（DSLAM）や IPv6 制御やルーティング機能をサポートしないイーサネットスイッチなどの既存のアクセスノードに実装できます。 LDRA を使用して、DHCP バージョン 6（DHCPv6）メッセージ交換にリレーエージェントオプションを挿入して、主にクライアント側のインターフェイスを特定します。 LDRA 機能は、インターフェイスと VLAN でイネーブルにできます。

  DHCPv6 リレーの詳細については、『IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15.1SG』の「DHCPv6 Relay—Lightweight DHCPv6 Relay Agent」の項を参照してください。

IPv6 スヌーピング ポリシーの設定方法

IPv6 スヌーピング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **ipv6 snooping policy***policy-name*
3. {[**default**] | [**device-role** {**node**| **switch**}] | [**limit address-count***value*] | [**no**] | [**protocol**{**dhcp** | **ndp**}] | [**security-level** {**glean**| **guard**| **inspect**}] | [**tracking** {**disable**[**stale-lifetime**[*seconds* | **infinite**] | **enable**[**reachable-lifetime**[*seconds* | **infinite**] }] | [**trusted-port**] }
4. **end**
5. **show ipv6 snooping policy** *policy-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 snooping policy***policy-name* 例： `Switch(config)# ipv6 snooping policy example_policy`	スヌーピング ポリシーを作成し、IPv6 スヌーピング ポリシー コンフィギュレーション モードに移行します。
ステップ 3	{[**default**]	[**device-role** {**node**| **switch**}]	[**limit address-count***value*]	[**no**]	[**protocol**{**dhcp**	**ndp**}]	[**security-level** {**glean**| **guard**| **inspect**}]	[**tracking** {**disable**[**stale-lifetime**[*seconds*	**infinite**]	**enable**[**reachable-lifetime**[*seconds*	**infinite**] }]	[**trusted-port**] } 例： Switch(config-ipv6-snooping)# security-level inspect 例： Switch(config-ipv6-snooping)# trusted-port	データ アドレス グリーニングをイネーブルにし、さまざまな条件に対してメッセージを検証し、メッセージのセキュリティ レベルを指定します。 • （任意）**default**：すべてをデフォルト オプションに設定します。 • （任意）**device-role**{**node**]	**switch**}：ポートに接続されたデバイスのロールを指定します。 デフォルトは **node** です。 • （任意）**limit address-count***value*：ターゲットごとに許可されるアドレス数を制限します。 • （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。 • （任意）**protocol**{**dhcp**	**ndp**}：分析のために、スヌーピング機能にどのプロトコルをリダイレクトするかを指定します。デフォルトは、**dhcp** および **ndp** です。 デフォルトを変更するには、**no protocol** コマンドを使用します。

	コマンドまたはアクション	目的
		• （任意）**security-level**{**glean**|**guard**|**inspect**}：この機能によって適用されるセキュリティのレベルを指定します。 デフォルトは **guard** です。 **glean**：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。 **guard**：アドレスを収集し、メッセージを検査します。 さらに、RA および DHCP サーバ メッセージを拒否します。 これがデフォルトのオプションです。 **inspect**：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。 • （任意）**tracking** {**disable** | **enable**}：デフォルトのトラッキング動作を上書きし、トラッキング オプションを指定します。 • （任意）**trusted-port**：信頼できるポートを設定します。 これにより、該当するターゲットに対するガードがディセーブルになります。 信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。 テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。
ステップ 4	**end** 例： `Switch(config-ipv6-snooping)# exit`	コンフィギュレーション モードから特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 snooping policy** *policy-name* 例： `Switch#show ipv6 snooping policy example_policy`	スヌーピング ポリシー設定を表示します。

次の作業

IPv6 スヌーピング ポリシーをインターフェイスまたは VLAN にアタッチします。

IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法

インターフェイスまたは VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **switchport**
4. **ipv6 snooping** [**attach-policy** *policy_name* [**vlan** {*vlan_id* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids*}] | **vlan** {*vlan_id* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
5. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `Switch(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport** 例： `Switch(config-if)# switchport`	switchport モードを開始します。 （注） インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに switchport インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。 これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。 レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。 switchport コンフィギュレーション モードではコマンド プロンプトは（config-if）# と表示されます。
ステップ 4	**ipv6 snooping** [**attach-policy** *policy_name* [**vlan** {*vlan_id* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids*}] | **vlan** {*vlan_id* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]	インターフェイスまたはそのインターフェイス上の特定の VLAN にカスタム IPv6 スヌーピング ポリシーをアタッチします。 デフォルト ポリシーをインターフェイスにアタッチするには、**attach-policy** キーワードを指定せずに **ipv6 snooping** コマンドを使用します。 デフォルト ポリシーをインターフェイス上の VLAN にアタッチするには、**ipv6 snooping vlan** コマンドを使用します。

	コマンドまたはアクション	目的

	例：
	`Switch(config-if)# ipv6 snooping`
	
	or
	
	`Switch(config-if)# ipv6 snooping attach-policy example_policy`
	
	or
	`Switch(config-if)# ipv6 snooping vlan 111,112`
	
	or
	
	`Switch(config-if)# ipv6 snooping attach-policy example_policy vlan 111,112`
		デフォルト ポリシーは、セキュリティ レベル **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。

ステップ 5	**do show running-config** 例： `Switch#(config-if)# do show running-config`	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range***Interface_name*
3. **ipv6snooping** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_id*s | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
4. **do show running-configinterface***portchannel_interface_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range***Interface_name* 例： `Switch(config)# interface Po11`	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。 インターフェイス範囲コンフィギュレーションモードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。

ステップ 3	**ipv6snooping** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
	
	例：
	`Switch(config-if-range)# ipv6 snooping attach-policy example_policy`
	
	or
	
	`Switch(config-if-range)# ipv6 snooping attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Switch(config-if-range)#ipv6 snooping vlan 222, 223,224`
		IPv6 スヌーピング ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： `Switch#(config-if-range)# do show running-config int po11`	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 バインディング テーブルの内容を設定する方法

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. [**no**] **ipv6 neighbor binding** [**vlan***vlan-id*{*ipv6-address***interface** interface_type *stack/module/porthw_address* [**reachable-lifetimevalue**[*seconds* | **default** | **infinite**] | [**tracking**{ [default | disable] [**reachable-lifetimevalue**[*seconds* | **default** | **infinite**] | [**enable** [**reachable-lifetimevalue**[*seconds* | **default** | **infinite**] | [**retry-interval** {*seconds*| **default** [**reachable-lifetimevalue**[*seconds* | **default** | **infinite**] }]
3. [**no**] **ipv6 neighbor binding max-entries***number* [**mac-limit***number* | **port-limit***number* [**mac-limit***number*] | **vlan-limit***number* [[**mac-limit***number*] | [**port-limit***number* [**mac-limit***number*]]]]
4. **ipv6 neighbor bindinglogging**
5. **exit**
6. **show ipv6 neighbor binding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ipv6 neighbor binding** [**vlan***vlan-id*{*ipv6-address***interface** interface_type *stack/module/porthw_address* [**reachable-lifetimevalue**[*seconds*	**default**	**infinite**]	[**tracking**{ [default	disable] [**reachable-lifetimevalue**[*seconds*	**default**	**infinite**]	[**enable** [**reachable-lifetimevalue**[*seconds*	**default**	**infinite**]	[**retry-interval** {*seconds*| **default** [**reachable-lifetimevalue**[*seconds*	**default**	**infinite**] }] 例： `Switch(config)# ipv6 neighbor binding`	バインディング テーブル データベースにスタティック エントリを追加します。
ステップ 3	[**no**] **ipv6 neighbor binding max-entries***number* [**mac-limit***number*	**port-limit***number* [**mac-limit***number*]	**vlan-limit***number* [[**mac-limit***number*]	[**port-limit***number* [**mac-limit***number*]]]] 例： `Switch(config)# ipv6 neighbor binding max-entries 30000`	バインディング テーブル キャッシュに挿入できるエントリの最大数を指定します。
ステップ 4	**ipv6 neighbor bindinglogging** 例： `Switch(config)# ipv6 neighbor binding logging`	バインディング テーブル メイン イベントのロギングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Switch(config)# exit`	グローバル コンフィギュレーション モードを終了して、ルータを特権 EXEC モードにします。
ステップ 6	**show ipv6 neighbor binding** 例： `Switch# show ipv6 neighbor binding`	バインディング テーブルの内容を表示します。

IPv6 ネイバー探索インスペクション ポリシーの設定方法

特権 EXEC モードから、IPv6 ND インスペクション ポリシーを設定するには、次の手順に従ってください。

手順の概要

1. **configure terminal**
2. [**no**]**ipv6 nd inspectionpolicy***policy-name*
3. **device-role** {**host** | **monitor** | **router** | **switch**}
4. **drop-unsecure**
5. **limit address-count***value*
6. **sec-level minimum***value*
7. **tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}
8. **trusted-port**
9. **validate source-mac**
10. **no** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**}
11. **default** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**}
12. **do show ipv6 nd inspection policy***policy_name*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	[**no**]**ipv6 nd inspectionpolicy***policy-name* 例： `Switch(config)# ipv6 nd inspection policy example_policy`	ND インスペクション ポリシー名を指定し、ND インスペクション ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**device-role** {**host** | **monitor** | **router** | **switch**} 例： `Switch(config-nd-inspection)# device-role switch`	ポートに接続されているデバイスのロールを指定します。 デフォルトは **host** です。
ステップ 4	**drop-unsecure** 例： `Switch(config-nd-inspection)# drop-unsecure`	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
ステップ 5	**limit address-count***value* 例： `Switch(config-nd-inspection)# limit address-count 1000`	1 ～ 10,000 を入力します。
ステップ 6	**sec-level minimum***value* 例： `Switch(config-nd-inspection)# limit address-count 1000`	暗号化生成アドレス（CGA）オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
ステップ 7	**tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]} 例： `Switch(config-nd-inspection)# tracking disable stale-lifetime infinite`	ポートでデフォルトのトラッキング ポリシーを上書きします。
ステップ 8	**trusted-port** 例： `Switch(config-nd-inspection)# trusted-port`	信頼できるポートにするポートを設定します。
ステップ 9	**validate source-mac** 例： `Switch(config-nd-inspection)# validate source-mac`	送信元 Media Access Control（MAC）アドレスをリンク層アドレスと照合します。
ステップ 10	**no** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**} 例： `Switch(config-nd-inspection)# no validate source-mac`	このコマンドの **no** 形式を使用してパラメータの現在の設定を削除します。

	コマンドまたはアクション	目的
ステップ 11	**default** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**} 例： `Switch(config-nd-inspection)# default limit address-count`	設定をデフォルト値に戻します。
ステップ 12	**do show ipv6 nd inspection policy***policy_name* 例： `Switch(config-nd-inspection)# do show ipv6 nd inspection policy example_policy`	ND インスペクション コンフィギュレーション モードを終了しないで ND インスペクションの設定を確認します。

IPv6 ネイバー探索インスペクション ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェース上の VLAN に IPv6 ND 検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `Switch(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	
	例：
	`Switch(config-if)# ipv6 nd inspection attach-policy example_policy`
	
	or
	
	`Switch(config-if)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Switch(config-if)# ipv6 nd inspection vlan 222, 223,224`
		ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-config** 例： `Switch#(config-if)# do show running-config`	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 ネイバー探索インスペクション ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ネイバー探索検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range***Interface_name*
3. **ipv6ndinspection** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
4. **do show running-configinterface***portchannel_interface_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range***Interface_name* 例： `Switch(config)# interface Po11`	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。 インターフェイス範囲コンフィギュレーションモードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。

ステップ 3	**ipv6ndinspection** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
	
	例：
	`Switch(config-if-range)# ipv6 nd inspection attach-policy example_policy`
	
	or
	
	`Switch(config-if-range)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Switch(config-if-range)#ipv6 nd inspection vlan 222, 223,224`
		ND インスペクション ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： `Switch#(config-if-range)# do show running-config int po11`	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法

IPv6 ルータ アドバタイズメント ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. [**no**]**ipv6 nd raguardpolicy***policy-name*
3. [**no**]**device-role** {**host** | **monitor** | **router** | **switch**}
4. [**no**]**hop-limit** {**maximum** | **minimum**} *value*
5. [**no**]**managed-config-flag** {**off** | **on**}
6. [**no**]**match** {**ipv6 access-list***list* | **ra prefix-list***list*}
7. [**no**]**other-config-flag** {**on** | **off**}
8. [**no**]**router-preference maximum** {**high** | **medium** | **low**}
9. [**no**]**trusted-port**
10. **default** {**device-role** | **hop-limit** {**maximum** | **minimum**} | **managed-config-flag** | **match** {**ipv6 access-list** | **ra prefix-list** } | **other-config-flag** | **router-preference maximum**| **trusted-port**}
11. **do show ipv6 nd raguard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**]**ipv6 nd raguardpolicy***policy-name* 例： `Switch(config)# ipv6 nd raguard policy example_policy`	RA ガード ポリシー名を指定し、RA ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 3	[**no**]**device-role** {**host**	**monitor**	**router**	**switch**} 例： `Switch(config-nd-raguard)# device-role switch`	ポートに接続されているデバイスのロールを指定します。 デフォルトは **host** です。
ステップ 4	[**no**]**hop-limit** {**maximum**	**minimum**} *value* 例： `Switch(config-nd-raguard)# hop-limit maximum 33`	（1 ～ 255）最大および最小のホップ制限値の範囲。 ホップ制限値によるルータ アドバタイズメント メッセージのフィルタリングをイネーブルにします。 不正 RA メッセージは低いホップ制限値（IPv4 の Time to Live と同じ）を持つ可能性があるため、ホストによって受け入れられると、ホストが不正 RA メッセージジェネレータを超えて宛先にトラフィックを生成することができなくなります。 指定されていないホップ制限値を持つ RA メッセージはブロックされます。 設定されていない場合、このフィルタはディセーブルになります。 「**minimum**」を設定して、指定する値より低いホップ制限

	コマンドまたはアクション	目的
		値を持つ RA メッセージをブロックします。 「**maximum**」を設定して、指定する値より高いホップ制限値を持つ RA メッセージをブロックします。
ステップ 5	[**no**]**managed-config-flag** {**off** | **on**} 例： `Switch(config-nd-raguard)#` **`managed-config-flag on`**	管理アドレス設定（「M」フラグ）フィールドに基づいてルータ アドバタイズメントメッセージのフィルタリングをイネーブルにします。 「M」フィールドが 1 の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバを使用する場合があります。 設定されていない場合、このフィルタはディセーブルになります。 **On**：「M」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。 **Off**：「M」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。
ステップ 6	[**no**]**match** {**ipv6 access-list***list* | **ra prefix-list***list*} 例： `Switch(config-nd-raguard)#` **`match ipv6 access-list example_list`**	指定したプレフィックス リストまたはアクセス リストと照合します。
ステップ 7	[**no**]**other-config-flag** {**on** | **off**} 例： `Switch(config-nd-raguard)#` **`other-config-flag on`**	その他の設定（「O」フラグ）フィールドに基づくルータ アドバタイズメント メッセージのフィルタリングをイネーブルにします。 「O」フィールドが 1 の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバを使用する場合があります。 設定されていない場合、このフィルタはディセーブルになります。 **On**：「O」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。 **Off**：「O」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。
ステップ 8	[**no**]**router-preference maximum** {**high** | **medium** | **low**} 例： `Switch(config-nd-raguard)#` **`router-preference maximum high`**	「Router Preference」フラグを使用したルータ アドバタイズメント メッセージのフィルタリングをイネーブルにします。 設定されていない場合、このフィルタはディセーブルになります。 • **high**：「Router Preference」が「high」、「medium」、または「low」に設定された RA メッセージを受け入れます。 • **medium**：「Router Preference」が「high」に設定された RA メッセージをブロックします。 • **low**：「Router Preference」が「medium」または「high」に設定された RA メッセージをブロックします。

	コマンドまたはアクション	目的
ステップ 9	[**no**]**trusted-port** 例： `Switch(config-nd-raguard)# trusted-port`	信頼できるポートとして設定すると、すべての接続デバイスが信頼され、より詳細なメッセージ検証は実行されません。
ステップ 10	**default** {**device-role** | **hop-limit** {**maximum** | **minimum**} | **managed-config-flag** | **match** {**ipv6 access-list** | **ra prefix-list** } | **other-config-flag** | **router-preference maximum**| **trusted-port**} 例： `Switch(config-nd-raguard)# default hop-limit`	コマンドをデフォルト値に戻します。
ステップ 11	**do show ipv6 nd raguard policy***policy_name* 例： `Switch(config-nd-raguard)# do show ipv6 nd raguard policy example_policy`	（任意）：RA ガード ポリシー コンフィギュレーション モードを終了しないで ND ガード ポリシー設定を表示します。

IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェース上の VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 nd raguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `Switch(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよびIDを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**ipv6 nd raguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	
	例：
	`Switch(config-if)# ipv6 nd raguard attach-policy example_policy`
	
	or
	
	`Switch(config-if)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Switch(config-if)# ipv6 nd raguard vlan 222, 223,224`
		ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 4	**do show running-config** 例： `Switch#(config-if)# do show running-config`	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ルータ アドバタイズメント ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range***Interface_name*
3. **ipv6ndraguard** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_id*s | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
4. **do show running-configinterface***portchannel_interface_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range***Interface_name* 例： `Switch(config)# interface Po11`	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。 インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。

ステップ 3	**ipv6ndraguard** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_id*s | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
	
	例：
	`Switch(config-if-range)# ipv6 nd raguard attach-policy example_policy`
	
	or
	
	`Switch(config-if-range)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Switch(config-if-range)#ipv6 nd raguard vlan 222, 223,224`
		RA ガード ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

	コマンドまたはアクション	目的
ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： `Switch#(config-if-range)# do show running-config int po11`	コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 DHCP ガード ポリシーの設定方法

IPv6 DHCP（DHCPv6）ガード ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. [**no**]**ipv6 dhcp guardpolicy***policy-name*
3. [**no**]**device-role** {**client** | **server**}
4. [**no**] **matchserveraccess-list***ipv6-access-list-name*
5. [**no**] **matchreplyprefix-list***ipv6-prefix-list-name*
6. [**no**]**preference**{ **max***limit* | **min***limit* }
7. [**no**] **trusted-port**
8. **default** {**device-role** | **trusted-port**}
9. **do show ipv6 dhcp guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**]**ipv6 dhcp guardpolicy***policy-name* 例： `Switch(config)# ipv6 dhcp guard policy example_policy`	DHCPv6 ガード ポリシー名を指定し、DHCPv6 ガード ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	[**no**]**device-role** {**client** | **server**} 例： `Switch(config-dhcp-guard)# device-role server`	（任意）特定のロールのデバイスからのものではないポート上の DHCPv6 応答および DHCPv6 アドバタイズメントをフィルタします。 デフォルトは **client** です。 • **client**：デフォルト値。アタッチされたデバイスがクライアントであることを指定します。 サーバ メッセージにはこのポートでドロップされます。 • **server**：適用されたデバイスが DHCPv6 サーバであることを指定します。 このポートでは、サーバ メッセージが許可されます。

ステップ 4	[**no**] **matchserveraccess-list***ipv6-access-list-name*
	
	例：
	`;;Assume a preconfigured IPv6 Access List as follows:`
	`Switch(config)# ipv6 access-list my_acls`
	`Switch(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any`
	
	`;;configure DCHPv6 Guard to match approved access list.`
	`Switch(config-dhcp-guard)# match server access-list my_acls`
		（任意）。 アドバタイズされた DHCPv6 サーバまたはリレーアドレスが認証されたサーバのアクセス リストからのものであることの確認をイネーブルにします（アクセス リストの宛先アドレスは「any」です）。 設定されていない場合、このチェックは回避されます。 空のアクセス リストは、permit all として処理されます。

ステップ 5	[**no**] **matchreplyprefix-list***ipv6-prefix-list-name*
	
	例：
	`;;Assume a preconfigured IPv6 prefix list as follows:`
	`Switch(config)# ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128`
	
	`;; Configure DCHPv6 Guard to match prefix`
	`Switch(config-dhcp-guard)# match reply prefix-list my_prefix`
		（任意）DHCPv6応答メッセージ内のアドバタイズされたプレフィクスが設定された承認プレフィクスリストからのものであることの確認をイネーブルにします。 設定されていない場合、このチェックは回避されます。 空のプレフィクス リストは、permit として処理されます。

ステップ 6	[**no**]**preference**{ **max***limit* | **min***limit* }
	
	例：
	`Switch(config-dhcp-guard)# preference max 250`
	`Switch(config-dhcp-guard)#preference min 150`
		device-role が **server** である場合に **max** および **min** を設定して、DHCPv6 サーバ アドバタイズメント値をサーバ優先度値に基づいてフィルタします。 デフォルトではすべてのアドバタイズメントが許可されます。
		
		max*limit*：（0 ～ 255）（任意）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限未満であるかどうかの検証をイネーブルにします。 デフォルトは 255 です。 設定されていない場合、このチェックは回避されます。

	コマンドまたはアクション	目的
		min*limit*：（0～255）（任意）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限を超過しているかどうかの検証をイネーブルにします。デフォルトは0です。 設定されていない場合、このチェックは回避されます。
ステップ 7	[**no**] **trusted-port** 例： `Switch(config-dhcp-guard)# trusted-port`	（任意）**trusted-port**：ポートを信頼モードに設定します。 このポートでは、これ以上のポリシングは実行されません。 （注） 信頼できるポートを設定した場合、device-role オプションは使用できません。
ステップ 8	**default** {**device-role** | **trusted-port**} 例： `Switch(config-dhcp-guard)# default device-role`	（任意）**default**：コマンドをデフォルトに設定します。
ステップ 9	**do show ipv6 dhcp guard policy***policy_name* 例： `Switch(config-dhcp-guard)# do show ipv6 dhcp guard policy example_policy`	（任意）コンフィギュレーション サブモードを終了せずに IPv6 DHCP のガード ポリシーの設定を表示します。 *policy_name* 変数を省略すると、すべての DHCPv6 ポリシーが表示されます。

DHCPv6 ガード設定の例

```
enable
configure terminal
ipv6 access-list acl1
 permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy pol1
 device-role server
 match server access-list acl1
 match reply prefix-list abc
 preference min 0
 preference max 255
 trusted-port
interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy pol1 vlan add 1
 vlan 1
  ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
4. **do show running-config interface** Interface_type *stack/module/port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `Switch(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**ipv6 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	
	例：
	`Switch(config-if)# ipv6 dhcp guard attach-policy example_policy`
	
	or
	
	`Switch(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Switch(config-if)# ipv6 dhcp guard vlan 222, 223,224`
		DHCP ガードポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 **attach-policy** オプションを使用しない場合、デフォルトポリシーがアタッチされます。

ステップ 4	**do show running-config interface** Interface_type *stack/module/port* 例： `Switch#(config-if)# do show running-config gig 1/1/4`	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 DHCP ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range***Interface_name*
3. **ipv6dhcpguard** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
4. **do show running-configinterface***portchannel_interface_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range***Interface_name* 例： `Switch(config)# interface Po11`	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。 インターフェイス範囲コンフィギュレーションモードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。

ステップ 3	**ipv6dhcpguard** [**attach-policy***policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove***vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove***vlan_ids* | **all**}]
	
	例：
	`Switch(config-if-range)# ipv6 dhcp guard attach-policy example_policy`
	
	or
	
	`Switch(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Switch(config-if-range)#ipv6 dhcp guard vlan`
		DHCP ガードポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

	コマンドまたはアクション	目的
	`222, 223,224`	
ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： `Switch#(config-if-range)# do show running-config int po11`	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 ソース ガードの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. [**no**] **ipv6 source-guard policy***policy_name*
4. [**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }]
5. **end**
6. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**] **ipv6 source-guard policy***policy_name* 例： `Switch(config)# ipv6 source-guard policy example_policy`	IPv6 ソース ガード ポリシー名を指定し、IPv6 ソース ガード ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	[**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }] 例： `Switch(config-sisf-sourceguard)# deny global-autoconf`	（任意）IPv6 ソース ガード ポリシーを定義します。 • **deny global-autoconf**：自動設定されたグローバル アドレスからのデータ トラフィックを拒否します。 これは、リンク上のすべてのグローバル アドレスが DHCP によって割り当てられているときに、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。 • **permit link-local**：リンクローカル アドレスから送信されたすべてのデータ トラフィックを許可します。 （注） ソース ガード ポリシーに基づく信頼できるオプションはサポートされません。
ステップ 5	**end** 例： `Switch(config-sisf-sourceguard)# end`	IPv6 ソース ガード ポリシー コンフィギュレーション モードを終了します。
ステップ 6	**show ipv6 source-guard policy***policy_name* 例： `Switch# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

次の作業

インターフェイスに IPv6 ソース ガード ポリシーを適用します。

IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** Interface_type *stack/module/port*
4. **ipv6 source-guard**[**attach-policy**<*policy_name*>]
5. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** Interface_type *stack/module/port* 例： `Switch(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 source-guard**[**attach-policy**<*policy_name*>] 例： `Switch(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy***policy_name* 例： `Switch#(config-if)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 ソース ガードの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. [**no**] **ipv6 source-guard policy***policy_name*
4. [**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }]
5. **end**
6. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**] **ipv6 source-guard policy***policy_name* 例： `Switch(config)# ipv6 source-guard policy example_policy`	IPv6 ソース ガード ポリシー名を指定し、IPv6 ソース ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	[**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }] 例： `Switch(config-sisf-sourceguard)# deny global-autoconf`	（任意）IPv6 ソース ガード ポリシーを定義します。 • **deny global-autoconf**：自動設定されたグローバル アドレスからのデータ トラフィックを拒否します。 これは、リンク上のすべてのグローバル アドレスが DHCP によって割り当てられているときに、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。 • **permit link-local**：リンクローカル アドレスから送信されたすべてのデータ トラフィックを許可します。 （注） ソース ガード ポリシーに基づく信頼できるオプションはサポートされません。
ステップ 5	**end** 例： `Switch(config-sisf-sourceguard)# end`	IPv6 ソース ガード ポリシー コンフィギュレーション モードを終了します。
ステップ 6	**show ipv6 source-guard policy***policy_name* 例： `Switch# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

次の作業

インターフェイスに IPv6 ソース ガード ポリシーを適用します。

IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** Interface_type *stack/module/port*
4. **ipv6 source-guard**[**attach-policy**<*policy_name*>]
5. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** Interface_type *stack/module/port* 例： `Switch(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 source-guard**[**attach-policy**<*policy_name*>] 例： `Switch(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy***policy_name* 例： `Switch#(config-if)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel***port-channel-number*
4. **ipv6 source-guard**[**attach-policy**<*policy_name*>]
5. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel***port-channel-number* 例： `Switch (config)# interface Po4`	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。
ステップ 4	**ipv6 source-guard**[**attach-policy**<*policy_name*>] 例： `Switch(config-if) # ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy***policy_name* 例： `Switch(config-if) #show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 プレフィックス ガードの設定方法

（注） プレフィックス ガードが適用されている場合にリンクローカル アドレスから送信されたルーティング プロトコル制御パケットを許可するには、ソースガード ポリシー コンフィギュレーション モードで permit link-local コマンドをイネーブルにします。

手順の概要

1. **enable**
2. **configureterminal**
3. [**no**]**ipv6 source-guard policy***source-guard-policy*
4. [**no**]**validate address**
5. **validate prefix**
6. **exit**
7. **show ipv6 source-guard policy**[*source-guard-policy*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**]**ipv6 source-guard policy***source-guard-policy* 例： `Switch (config)# ipv6 source-guard policy my_snooping_policy`	IPv6 ソースガード ポリシー名を定義して、スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	[**no**]**validate address** 例： `Switch (config-sisf-sourceguard)# no validate address`	アドレス検証機能をディセーブルにし、IPv6プレフィックス ガード機能を設定できるようにします。

	コマンドまたはアクション	目的
ステップ 5	**validate prefix** 例： `Switch (config-sisf-sourceguard)# validate prefix`	IPv6 ソース ガードをイネーブルにし、IPv6 プレフィックスガード動作を実行します。
ステップ 6	**exit** 例： `Switch (config-sisf-sourceguard)# exit`	スイッチ統合セキュリティ機能のソースガードポリシーコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 source-guard policy**[*source-guard-policy*] 例： `Switch # show ipv6 source-guard policy policy1`	IPv6 ソースガード ポリシー設定を表示します。

IPv6 プレフィックス ガード ポリシーをインターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** Interface_type *stack/module/port*
4. **ipv6 source-guard attach-policy***policy_name*
5. **show ipv6 source-guard policy***policy_name*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface** Interface_type *stack/module/port* 例： `Switch(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 source-guard attach-policy***policy_name* 例： `Switch(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy***policy_name* 例： `Switch(config-if)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel***port-channel-number*
4. **ipv6 source-guard**[**attach-policy**<*policy_name*>]
5. **show ipv6 source-guard policy***policy_name*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface port-channel***port-channel-number* 例： `Switch (config)# interface Po4`	インターフェイスのタイプとポート番号を指定し、スイッチをポートチャネル コンフィギュレーション モードにします。
ステップ 4	**ipv6 source-guard**[**attach-policy**<*policy_name*>] 例： `Switch(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**show ipv6 source-guard policy***policy_name* 例： `Switch(config-if)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

第 64 章

FIPS の設定

- FIPS および共通基準に関する情報，1775 ページ

FIPS および共通基準に関する情報

Cisco Catalyst シリーズ スイッチに対する、連邦情報処理標準（FIPS）認証ドキュメントは、次の Web サイトで公開されています。

http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_fips140.html

統合された検証証明書とセキュリティ ポリシーのドキュメントを表示するには、証明書の列のリンクをクリックします。 セキュリティ ポリシーのドキュメントでは、FIPS の実装、ハードウェアの設置、ファームウェア初期化、およびFIPS操作のためのソフトウェア設定手順について説明します。

Common Criteria はコンピュータ セキュリティ証明書向け国際基準（ISO/IEC 15408）です。 この規格は一連の要件、テスト、評価方法から成り、評価のターゲットが特定の保護プロファイルまたはカスタム セキュリティ ターゲットに準拠していることを保証します。 詳細については、特定の Cisco Catalyst スイッチ モデルおよび Cisco IOS リリースに対応するセキュリティを目的としたマニュアルを次の URL で参照してください。
http://www.niap-ccevs.org/CCEVS_Products/pcl.cfm?tech_name=Network+Switch

第 X 部

システム管理

- システムの管理，1779 ページ
- スイッチのセットアップ設定の実行，1817 ページ
- スイッチのクラスタリング，1849 ページ
- スイッチのクラスタリング，1859 ページ
- SDM テンプレートの設定，1877 ページ
- システム メッセージ ログの設定，1883 ページ
- オンライン診断の設定，1899 ページ
- ソフトウェア設定のトラブルシューティング，1911 ページ

第 65 章

システムの管理

- スイッチの管理に関する情報，1779 ページ
- スイッチを管理する方法，1787 ページ
- スイッチのモニタリングおよび保守の管理，1812 ページ
- スイッチ管理の設定例，1813 ページ

スイッチの管理に関する情報

システム日時管理に関する情報

スイッチのシステム日時は自動設定方式（RTC および NTP）または手動設定方式を使用して管理できます。

（注） ここで使用するコマンドの構文および使用方法の詳細については、*Cisco.com* で、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

システム クロック

時刻サービスの基本となるのはシステムクロックです。このクロックはシステムがスタートアップした瞬間から稼働し、日時を常時トラッキングします。

システム クロックは、次のソースにより設定できます。

- RTC
- NTP
- 手動設定

システム クロックは、次のサービスに時刻を提供します。

- ユーザの **show** コマンド
- ログおよびデバッグ メッセージ

システムクロックは、グリニッジ標準時（GMT）とも呼ばれる協定世界時（UTC）に基づいて内部的に時刻を追跡します。 ローカルのタイムゾーンおよび夏時間に関する情報を設定することにより、時刻がローカルのタイム ゾーンに応じて正確に表示されるようにできます。

システム クロックは、時刻に信頼性があるかどうか（つまり、信頼できると見なされるタイム ソースによって時刻が設定されているか）を常時トラッキングします。 信頼性のない場合は、時刻は表示目的でのみ使用され、再配信されません。

Real Time Clock（リアルタイム クロック）

リアルタイム クロック（RTC）は、スイッチの現在時刻を追跡します。 スイッチはクロッキング パラメータを再設定するまでは GMT 時間に設定された RTC を装備しています。

RTC の利点は次のとおりです。

- RTC はバッテリ電源式です。
- システム時刻は、停電時およびシステム リブート時に保持されます。

RTC と NTP クロックはスイッチに統合されます。 NTP をイネーブルにすると、RTC 時間が NTP クロックと定期的に同期化され、精度が保たれます。

ネットワーク タイム プロトコル

NTPは、ネットワーク上のデバイス間の時刻の同期化を目的に設計されています。 NTPはユーザ データグラム プロトコル（UDP）で稼働し、UDP は IP 上で稼働します。 NTP は RFC 1305 で規定されています。

NTP ネットワークは通常、タイム サーバに接続されたラジオ クロックやアトミック クロックなど、正規の時刻源から時刻を取得します。 NTPは、ネットワークにこの時刻を分配します。 NTP はきわめて効率的で、1 分間に 1 パケットを使用するだけで、2 台のデバイスを 1 ミリ秒以内に同期化できます。

NTPでは、信頼できるタイム ソースから各マシンが何NTP「ホップ」隔たっているかを表すために、ストラタムという概念が使用されます。 ストラタム 1 タイム サーバには、ラジオ クロックまたは原子時計が直接接続されており、ストラタム 2 タイム サーバは、NTP を使用してストラタム 1 タイム サーバから時刻を取得します（以降のストラタムも同様です）。 NTPが稼働するデバイスは、タイム ソースとして、NTP を使用して通信するストラタム番号が最小のデバイスを自動的に選択します。 この方法によって、NTP 時刻配信の自動編成型ツリーが効率的に構築されます。

NTP では、同期化されていないデバイスと同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。 また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

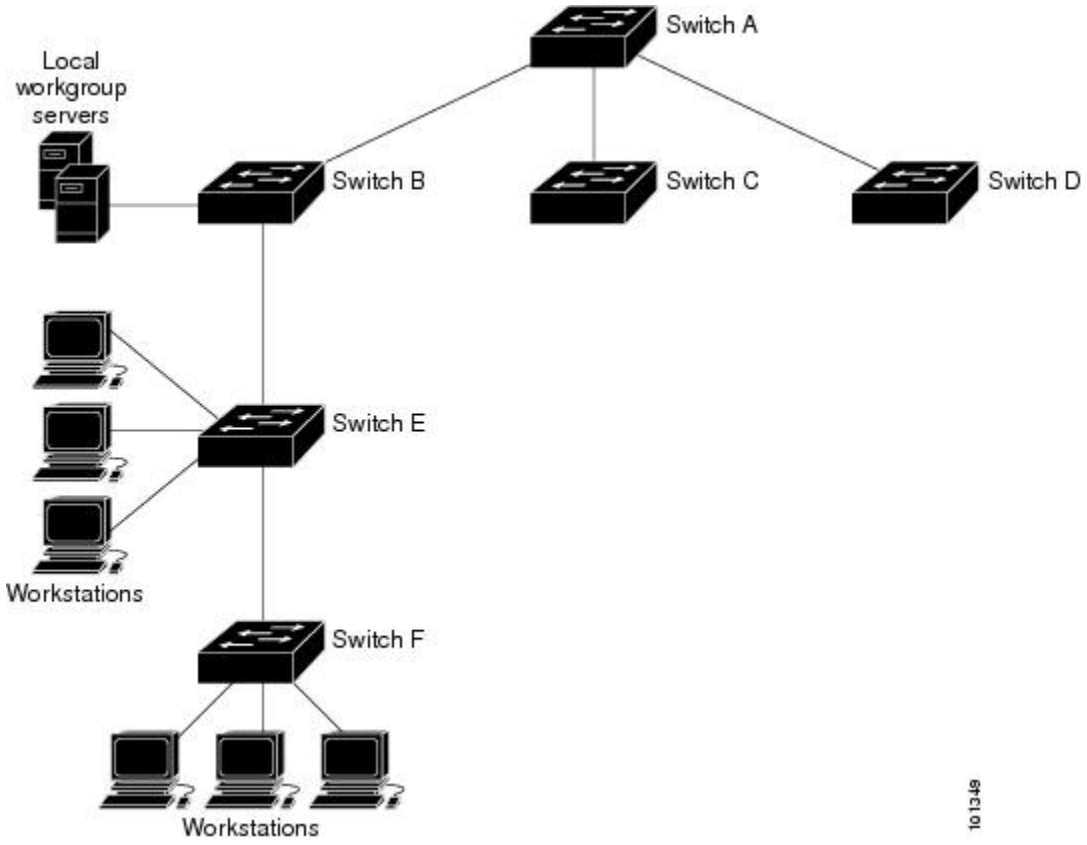
NTP が稼働するデバイス間の通信（アソシエーション）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスのIPアドレスが与えられます。アソシエーションのペアとなるデバイス間でNTPメッセージを交換することによって、正確な時刻の維持が可能になります。 ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。 各デバイスを、単にブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。 ただし、情報の流れは一方向に限られます。

デバイス上で維持される時刻は、重要なリソースです。NTP のセキュリティ機能を使用して、不正確な時刻が誤って、あるいは意図的に設定されることがないようにしてください。 その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

シスコによるNTPの実装では、ストラタム1サービスをサポートしていないため、ラジオクロックまたは原子時計に接続できません。 ネットワークの時刻サービスは、IPインターネット上のパブリック NTP サーバから取得することを推奨します。

次の図に NTP を使用した一般的なネットワークの例を示します。 スイッチ A は、NTP サーバモードで設定した**スイッチ** B、C、D の NTP マスターです。スイッチ B、C、D とスイッチ A の間にはサーバ アソシエーションが設定されています。スイッチ E はアップストリームおよびダウンストリーム スイッチ、スイッチ B およびスイッチ F それぞれの NTP ピアとして設定されます。

図 *117*：一般的な *NTP* ネットワークの構成



ネットワークがインターネットから切り離されている場合、シスコのNTPによって、実際には、他の方法で時刻を学習しているにもかかわらず、デバイスがNTPを使用して同期化しているように動作を設定できます。 他のデバイスは、NTPによりこのデバイスと同期化されます。

複数のタイム ソースがある場合は、NTPは常に、より信頼性があると見なされます。 NTPの時刻は、他の方法による時刻に優先します。

自社のホスト システムにNTPソフトウェアを組み込んでいるメーカーが数社あり、UNIXシステム用のバージョンやその派生ソフトウェアも一般に入手できます。 このソフトウェアによって、ホスト システムも時間が同期化されます。

NTPストラタム

NTPでは、信頼できるタイム ソースから各マシンが何NTP「ホップ」隔たっているかを表すために、ストラタムという概念が使用されます。 ストラタム1タイム サーバには、ラジオ クロックまたは原子時計が直接接続されており、ストラタム2タイム サーバは、NTPを使用してストラタム1タイム サーバから時刻を取得します（以降のストラタムも同様です）。 NTPが稼働するデバイスは、タイム ソースとして、NTPを使用して通信するストラタム番号が最小のデバイスを自動的に選択します。 この方法によって、NTP時刻配信の自動編成型ツリーが効率的に構築されます。

NTPでは、同期化されていないデバイスと同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。 また、NTPでは、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

NTPアソシエーション

NTPが稼働するデバイス間の通信（アソシエーション）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスのIPアドレスが与えられます。アソシエーションのペアとなるデバイス間でNTPメッセージを交換することによって、正確な時刻の維持が可能になります。 ただし、LAN環境では、代わりにIPブロードキャスト メッセージを使用するようにNTPを設定できます。 各デバイスを、単にブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。 ただし、情報の流れは一方向に限られます。

NTPセキュリティ

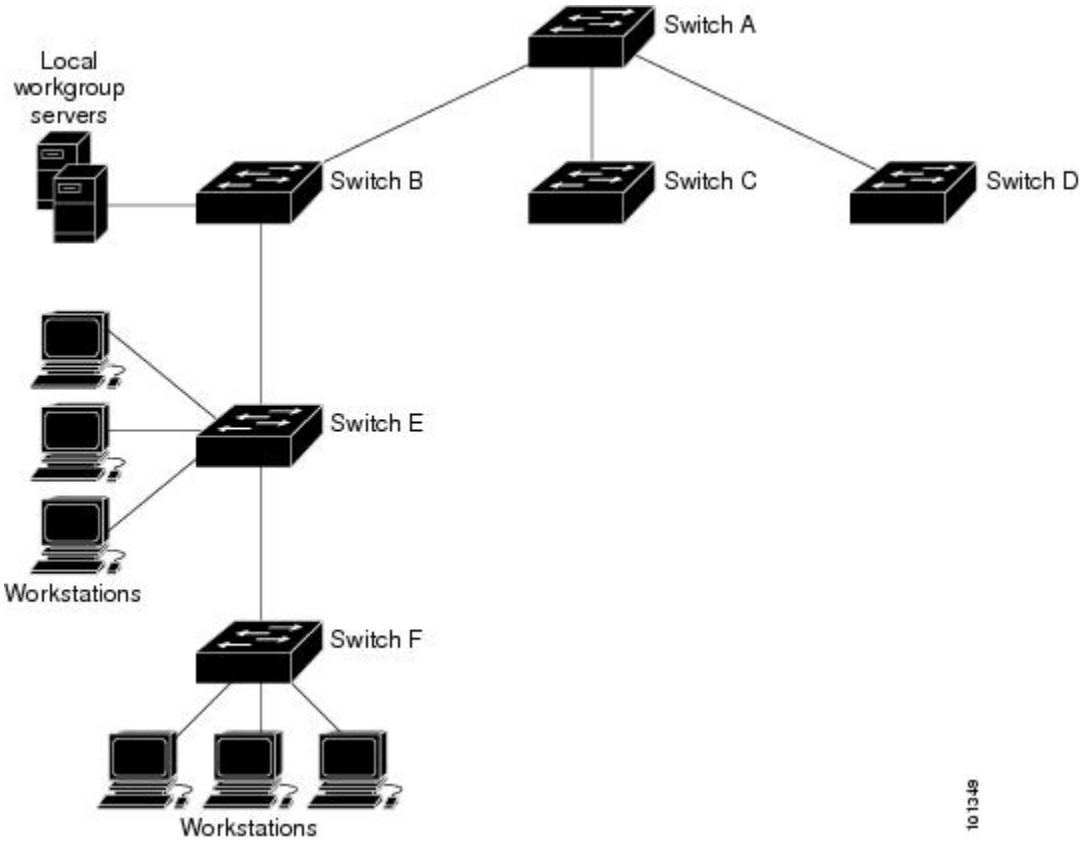
デバイス上で維持される時刻は、重要なリソースです。NTPのセキュリティ機能を使用して、不正確な時刻が誤って、あるいは意図的に設定されることがないようにしてください。 その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

NTPの実装

NTPの実装では、ストラタム1サービスがサポートされないため、ラジオ クロックまたは原子時計に接続できません。 ネットワークの時刻サービスは、IPインターネット上のパブリック NTPサーバから取得することを推奨します。

次の図に NTP を使用した一般的なネットワークの例を示します。 スイッチ A は、NTP サーバモードで設定したスイッチ B、C、D の NTP マスターです。スイッチ B、C、D とスイッチ A の間にはサーバ アソシエーションが設定されています。スイッチ E はアップストリームおよびダウンストリーム スイッチ、スイッチ B およびスイッチ F それぞれの NTP ピアとして設定されます。

図 *118*：一般的な *NTP* ネットワークの構成



ネットワークがインターネットから切り離されている場合、NTP によって、実際には、他の方法で時刻を取得している場合でも、NTP を使用した同期化と同様にデバイスの動作を設定できます。他のデバイスは、NTP によりこのデバイスと同期化されます。

複数のタイム ソースがある場合は、NTP は常に、より信頼性があると見なされます。 NTP の時刻は、他の方法による時刻に優先します。

自社のホスト システムに NTP ソフトウェアを組み込んでいるメーカーが数社あり、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。 このソフトウェアによって、ホスト システムも時間が同期化されます。

NTP バージョン 4

スイッチには、NTP バージョン 4 が実装されています。 NTPv4 は NTP バージョン 3 の拡張版です。 NTPv4 は IPv4 と IPv6 の両方をサポートし、NTPv3 との下位互換性があります。

NTPv4 は次の互換性を提供します。

- IPv6 のサポート。
- NTPv3 よりさらに向上したセキュリティ。 NTPv4 プロトコルは、公開キー暗号化および標準 X509 認証に基づくセキュリティ フレームワークを提供します。
- ネットワークに対する時間分布ヒエラルキーの自動計算。 特定のマルチキャスト グループを使用して、NTPv4 は、最も低い帯域幅コストで最高の時間精度を達成するサーバのヒエラルキーを自動的に設定します。 この機能では、サイトローカル IPv6 マルチキャスト アドレスが活用されます。

NTPv4 の設定の詳細については、『*Cisco IOS IPv6 Configuration Guide, Release 12.4T*』の「*Implementing NTPv4 in IPv6*」の章を参照してください。

システム名およびシステム プロンプト

スイッチを識別するシステム名を設定します。デフォルトでは、システム名およびシステムプロンプトは スイッチ です。

システム プロンプトを設定していない場合は、システム名の最初の 20 文字がシステム プロンプトとして使用されます。 大なり記号（>）が付加されます。 システム名が変更されると、プロンプトは更新されます。

ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*, *Release 12.4*』および『*Cisco IOS IP Command Reference*, *Volume 2 of 3: Routing Protocols*, *Release 12.4*』を参照してください。

デフォルトのシステム名とプロンプトの設定

デフォルトのスイッチのシステム名およびプロンプトは *Switch* です。

DNS

DNS プロトコルは、ドメイン ネーム システム（DNS）を制御します。DNS とは分散型データベースであり、ホスト名を IP アドレスにマッピングできます。 スイッチに DNS を設定すると、**ping**、**telnet**、**connect** などのすべての IP コマンドおよび関連する Telnet サポート操作で IP アドレスの代わりにホスト名を使用できます。

IP によって定義される階層型の命名方式では、デバイスを場所またはドメインで特定できます。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。 たとえば、シスコは、IP で *com* というドメイン名に分類される商業組織なので、ドメイン名は *cisco.com* となります。 このドメイン内の特定のデバイス、たとえばファイル転送プロトコル（FTP）システムは、*ftp.cisco.com* で表されます。

IP ではドメイン名をトラッキングするために、ドメイン ネーム サーバという概念が定義されています。 ドメイン ネーム サーバの役割は、名前から IP アドレスへのマッピングをキャッシュ（またはデータベース）に保存することです。 ドメイン名を IP アドレスにマッピングするには、まず、ホスト名を明示し、ネットワーク上に存在するネーム サーバを指定し、DNS をイネーブルにします。

DNS のデフォルト設定値

表 *157*：*DNS* のデフォルト設定値

機能	デフォルト設定
DNS イネーブル ステート	イネーブル
DNS デフォルト ドメイン名	未設定
DNS サーバ	ネーム サーバのアドレスが未設定

ログイン バナー

Message-of-The-Day（MoTD）バナーおよびログイン バナーを作成できます。 MOTD バナーはログイン時に、接続されたすべての端末に表示されます。すべてのネットワーク ユーザに影響するメッセージ（差し迫ったシステム シャットダウンの通知など）を送信する場合に便利です。

ログイン バナーも接続されたすべての端末に表示されます。 表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

（注） ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*』を参照してください。

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

MAC Address Table

MAC アドレス テーブルには、スイッチがポート間のトラフィック転送に使用するアドレス情報が含まれています。 このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応しています。 アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

- ダイナミック アドレス：スイッチが取得し、使用されなくなった時点で期限切れとなる送信元の MAC アドレス
- スタティック アドレス：手動で入力され、期限切れにならず、スイッチのリセット時にも消去されないユニキャスト アドレス

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN（仮想 LAN）ID、アドレスに対応付けられたポート番号、およびタイプ（スタティックまたはダイナミック）のリストです。

（注） ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

MAC アドレス テーブルの作成

すべてのポートでサポートされる複数の MAC アドレスを使用して、他のネットワーク デバイスにスイッチ上のすべてのポートを接続できます。 スイッチは、各ポートで受信するパケットの送信元アドレスを学習し、アドレス テーブルにアドレスとそれに関連付けられたポート番号を追加することによって、動的なアドレス指定を行います。 ネットワークでデバイスの追加または削除が行われると、スイッチによってアドレステーブルが更新され、新しいダイナミック アドレスが追加され、使用されていないアドレスは期限切れになります。

エージング インターバルは、グローバルに設定されています。 ただし、スイッチは VLAN ごとにアドレス テーブルを維持し、STP によって VLAN 単位で有効期間を短縮できます。

スイッチは、受信したパケットの宛先アドレスに基づいて、任意の組み合わせのポート間でパケットを送信します。 スイッチは、MAC アドレス テーブルを使用することによって、宛先アドレスに関連付けられたポートに限定してパケットを転送します。 宛先アドレスがパケットを送信したポート上にある場合は、パケットはフィルタリング処理され、転送されません。 スイッチは、常にストアアンドフォワード方式を使用します。このため、完全なパケットをいったん保存してエラーがないか検査してから転送します。

MAC アドレスおよび VLAN

すべてのアドレスは VLAN と関連付けされます。 1 つのアドレスを複数の VLAN に対応付け、それぞれで異なる宛先を設定できます。 たとえば、ユニキャスト アドレスを VLAN 1 のポート 1 および VLAN 5 のポート 9、10、1 に転送するといったことが可能です。

VLAN ごとに、独自の論理アドレス テーブルが維持されます。 ある VLAN で認識されているアドレスが別の VLAN で認識されるには、別の VLAN 内のポートによって学習されるか、または別の VLAN 内のポートにスタティックに対応付けられる必要があります。

MAC アドレス テーブルのデフォルト設定

次の表に、MAC アドレス テーブルのデフォルト設定を示します。

表 *158*： *MAC* アドレスのデフォルト設定

機能	デフォルト設定
エージング タイム	300 秒
ダイナミック アドレス	自動学習
スタティック アドレス	未設定

ARP テーブルの管理

デバイスと通信するには（イーサネット上のデバイスなど）、ソフトウェアは最初にそのデバイスの48ビットMACアドレスまたはローカルデータ リンク アドレスを学習する必要があります。IP アドレスからローカル データ リンク アドレスを学習するプロセスを、アドレス解決といいます。

アドレス解決プロトコル（ARP）は、ホスト IP アドレスを、該当するメディアまたは MAC アドレスおよび VLAN ID に対応付けます。 IP アドレスを使用して、ARP は対応する MAC アドレスを見つけます。 MAC アドレスが見つかると、IP と MAC アドレスとの対応を ARP キャッシュに格納し、すばやく検索できるようにします。 その後、IPデータグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。 イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化および ARP 要求/応答については、サブネットワーク アクセス プロトコル（SNAP）で規定されています。 IP インターフェイスでは、標準的なイーサネット形式の ARP カプセル化（**arpa** キーワードで表される）がデフォルトでイネーブルに設定されています。

手動でテーブルに追加された ARP エントリは期限切れにならないので、手動で削除する必要があります。

CLI（コマンドライン インターフェイス）の手順については、*Cisco.com* で Cisco IOS Release 12.4 のマニュアルを参照してください。

スイッチを管理する方法

手動による日付と時刻の設定

再開と再起動により正確なシステム時刻が保持されますが、システムが再開した後で日付と時刻を手動で設定できます。

手動設定は必要な場合にのみ使用することを推奨します。 スイッチが同期できる外部ソースがある場合は、システム クロックを手動で設定する必要はありません。

（注） アクティブ スイッチに障害が発生し、別のスタック メンバがアクティブ スイッチの役割を引き継ぐ前に手動でシステム クロックを設定している場合は、この設定を再設定する必要があります。

システム クロックの設定

ネットワーク上に、NTP サーバなどの時刻サービスを提供する外部ソースがある場合、手動でシステム クロックを設定する必要はありません。

システム クロックを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. 次のいずれかを使用します。
   - **clock set***hh:mm:ss day month year*
   - **clock set** *hh:mm:ss month day year*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかを使用します。 • **clock set***hh:mm:ss day month year* • **clock set** *hh:mm:ss month day year* 例： `Switch# clock set 13:32:00 23 March 2013`	次のいずれかの書式を使ってシステム クロックを手動で設定します。 • *hh:mm:ss*：時間（24 時間形式）、分、秒を指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • *day*：月の日で日付を指定します。 • *month*：月を名前で指定します。 • *year*：年を指定します（略式表記で指定しないでください）。

タイム ゾーンの設定

タイム ゾーンを手動で設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **clock timezone***zone hours-offset* [*minutes-offset*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**clock timezone***zone hours-offset* [*minutes-offset*] 例： `Switch(config)# clock timezone AST -3 30`	時間帯を設定します。 内部時間は、協定世界時（UTC）で維持されるため、このコマンドは表示専用で、時刻を手動で設定するときだけに使用されます。 • *zone*：標準時が適用されているときに表示されるタイムゾーンの名前を入力します。 デフォルトは UTC です。 • *hours-offset*：UTC からのオフセット時間数を入力します。 • （任意）*minutes-offset*：UTC からのオフセット分数を入力します。 ローカル タイム ゾーンが UTC と 1 時間の差の割合である場合に指定できます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

夏時間の設定

毎年特定の日に夏時間が開始および終了する地域に夏時間を設定するには、次の作業を行います。

手順の概要

1. **enable**
2. **configureterminal**
3. **clock summer-time***zone***date***date month year hh:mm date month year hh:mm* [*offset*]]
4. **clock summer-time***zone***recurring** [*week day month hh:mm week day month hh:mm* [*offset*]]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ **3**	**clock summer-time***zone***date***date month year hh:mm date month year hh:mm* [*offset*]] 例： `Switch(config)# clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00`	毎年指定された日に開始および終了する夏時間を設定します。
ステップ **4**	**clock summer-time***zone***recurring** [*week day month hh:mm week day month hh:mm* [*offset*]] 例： `Switch(config)# clock summer-time PDT recurring 10 March 2013 2:00 3 November 2013 2:00`	毎年指定された日に開始および終了する夏時間を設定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。 終了時間は夏時間を基準にしています。 夏時間はデフォルトでディセーブルに設定されています。 パラメータなしで **clock summer-time***zone***recurring** を指定すると、夏時間のルールはデフォルトにより米国のルールになります。 開始月が終了月より後の場合は、システムでは南半球にいると見なされます。 • *zone*：夏時間が有効な場合に表示される時間帯名（PDT など）を指定します。 • （任意）*week*：月の週（1 ～ 4、**first**、または **last**）を指定します。 • （任意）*day*：曜日（Sunday、Monday など）を指定します。 • （任意）*month*：月（January、February など）を指定します。 • （任意）*hh:mm*：時および分単位で時間（24 時間形式）を指定します。 • （任意）*offset*：夏時間中に追加する分数を指定します。デフォルトは 60 です。
ステップ **5**	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ユーザの居住地域の夏時間が定期的なパターンに従わない（次の夏時間のイベントの正確な日時を設定する）場合は、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **clock summer-time***zone***date**[*month date year hh:mm month date year hh:mm* [*offset*]]or**clock summer-time***zone***date** [*date month year hh:mm date month year hh:mm* [*offset*]]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**clock summer-time***zone***date**[*month date year hh:mm month date year hh:mm* [*offset*]]or**clock summer-time***zone***date** [*date month year hh:mm date month year hh:mm* [*offset*]]	最初の日付で夏時間開始の日付を、2 番めの日付で終了の日付を設定します。 夏時間はデフォルトでディセーブルに設定されています。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前（たとえば PDT）を入力します。 • （任意）*week* には、月の何週目かを指定します（1 ～ 5、または last）。 • （任意）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh:mm* には、時刻を時間（24 時間形式）と分で指定します。 • （任意）*offset* には、夏時間の間、追加する分数を指定します。 デフォルトは 60 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

システム名の設定

システム名を手動で設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **hostname***name*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**hostname***name* 例： `Switch(config)# hostname remote-users`	システム名を設定します。 システム名を設定すると、システム プロンプトとしても使用されます。 デフォルト設定はSwitchです。 名前はARPANETホスト名のルールに従う必要があります。このルールではホスト名は文字で始まり、文字または数字で終わり、その間には文字、数字、またはハイフンしか使用できません。 名前には 63 文字まで使用できます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。

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

DNS の設定

スイッチのIPアドレスをホスト名として使用する場合、このIPアドレスが使用されるため、DNS クエリは発生しません。 ピリオド（.）なしでホスト名を設定すると、ピリオドと、それに続くデフォルトのドメイン名がホスト名に追加され、その後で DNS クエリーが行われ、名前を IP アドレスにマッピングします。 デフォルトのドメイン名は、グローバル コンフィギュレーション コマンド **ip domain-name** で設定される値です。 ホスト名にピリオド（.）がある場合は、Cisco IOS ソフトウェアは、ホスト名にデフォルトのドメイン名を追加せずに IP アドレスを検索します。

DNS を使用するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip domain-name***name*
4. **ip name-server***server-address1* [*server-address2 ... server-address6*]
5. **ip domain-lookup** [**nsap** | **source-interface***interface*]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip domain-name***name* 例： `Switch(config)# ip domain-name Cisco.com`	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 ブート時にはドメイン名は設定されていませんが、スイッチの設定が BOOTP または Dynamic Host Configuration Protocol（DHCP）サーバから行われている場合、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（この情報がサーバに設定されている場合）。
ステップ 4	**ip name-server***server-address1* [*server-address2 ... server-address6*] 例： `Switch(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300`	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。 各サーバ アドレスはスペースで区切ります。 最初に指定されたサーバが、プライマリ サーバです。 スイッチは、最初にプライマリ サーバへ DNS クエリを送信します。 そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 5	**ip domain-lookup** [**nsap** | **source-interface***interface*] 例： `Switch(config)# ip domain-lookup`	（任意） スイッチ上で、DNS に基づくホスト名からアドレスへの変換をイネーブルにします。 この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

Message-of-the-Day ログイン バナーの設定

スイッチにログインしたときに画面に表示される 1 行以上のメッセージ バナーを作成できます。MOTD ログイン バナーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **banner motd***cmessage c*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**banner motd***cmessage c*
	
	例：
	
	`Switch(config)# banner motd #`
	`This is a secure site. Only`
	`authorized users are allowed.`
	`For access, contact technical`
	`support.`
	`#`
		MoTD を指定します。
		
		c：ポンド記号（#）など、目的のデリミタを入力して **Return** キーを押します。 区切り文字はバナー テキストの始まりと終わりを表します。 終わりの区切り文字の後ろの文字は廃棄されます。
		
		message：255 文字までのバナー メッセージを入力します。 メッセージ内には区切り文字を使用できません。

ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ログイン バナーの設定

接続されたすべての端末でログインバナーが表示されるように設定できます。 バナーが表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

ログイン バナーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **banner login***c message c*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

ステップ 3	**banner login***c message c*
	
	例：
	
	`Switch(config)# banner login $`
	`Access for authorized users only.`
	`Please enter your username and`
	`password.`
	`$`
		ログイン メッセージを指定します。
		
		c：ポンド記号（#）など、目的のデリミタを入力して **Return** キーを押します。 区切り文字はバナー テキストの始まりと終わりを表します。 終わりの区切り文字の後ろの文字は廃棄されます。
		
		message：255 文字までのログイン メッセージを入力します。 メッセージ内には区切り文字を使用できません。

ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。

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

MAC アドレス テーブルの管理

アドレス エージング タイムの変更

ダイナミック アドレス テーブルのエージング タイムを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **mac address-table aging-time** [*0* | *10-1000000*] [**routed-mac** | **vlan***vlan-id*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**mac address-table aging-time** [*0* | *10-1000000*] [**routed-mac** | **vlan***vlan-id*] 例： `Switch(config)# mac address-table aging-time 500 vlan 2`	ダイナミック エントリが使用または更新された後、MAC アドレス テーブル内に保持される時間を設定します。 指定できる範囲は 10 ～ 1000000 秒です。 デフォルトは 300 です。 0 を入力して期限切れをディセーブルにすることもできます。 スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。 *vlan-id*：有効な ID は 1 ～ 4094 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

MAC アドレス変更通知トラップの設定

NMS ホストに MAC アドレス変更通知トラップを送信するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server host***host-addrcommunity-string notification-type* { **informs** | **traps** } {**version** {**1** | **2c** | **3**}} {**vrf***vrf instance name*}
4. **snmp-server enable traps mac-notification change**
5. **mac address-table notification change**
6. **mac address-table notification change** [**interval***value*] [**history-size***value*]
7. **interface***interface-id*
8. **snmp trap mac-notification change** {**added** | **removed**}
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server host***host-addrcommunity-string notification-type* { **informs** | **traps** } {**version** {**1** | **2c** | **3**}} {**vrf***vrf instance name*} 例： `Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification`	トラップ メッセージの受信側を指定します。 • *host-addr*：NMS の名前またはアドレスを指定します。 • **traps**（デフォルト）：ホストに SNMP トラップを送信します。 • **informs**：ホストに SNMP インフォームを送信します。 • **version**：サポートする SNMP バージョンを指定します。informs にはバージョン 1（デフォルト）を使用できません。 • *community-string*：通知処理で送信する文字列を指定します。 **snmp-server host** コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、

	コマンドまたはアクション	目的
		snmp-server community コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type*：**mac-notification** キーワードを使用します。 • **vrf***vrf instance name*：ホストの VPN ルーティング/転送インスタンスを指定します。
ステップ 4	**snmp-server enable traps mac-notification change** 例： `Switch(config)# snmp-server enable traps mac-notification change`	スイッチが MAC アドレス変更通知トラップを送信できるようにします。
ステップ 5	**mac address-table notification change** 例： `Switch(config)# mac address-table notification change`	MAC アドレス変更通知機能をイネーブルにします。

ステップ 6	**mac address-table notification change** [**interval***value*] [**history-size***value*]
	
	例：
	
	`Switch(config)# mac address-table notification change interval 123`
	`Switch(config)#mac address-table notification change history-size 100`
		トラップインターバルタイムと履歴テーブルのサイズを入力します。
		• （任意）**interval***value*：NMS に生成されるトラップの各セット間の通知トラップインターバルを秒単位で指定します。 指定できる範囲は 0 ～ 2147483647 秒です。デフォルトは 1 秒です。
		• （任意）**history-size***value*：MAC 通知履歴テーブルの最大エントリ数を指定します。 指定できる範囲は 0 ～ 500 です。デフォルトは 1 です。

ステップ 7	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	インターフェイスコンフィギュレーションモードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 8	**snmp trap mac-notification change {added | removed}** 例： `Switch(config-if)# snmp trap mac-notification change added`	インターフェイス上で MAC アドレス変更通知トラップをイネーブルにします。 • MAC アドレスがインターフェイスに追加された（**added**）場合にトラップをイネーブルにします。 • MAC アドレスがインターフェイスから削除された（**removed**）場合に MAC 通知トラップをイネーブルにします。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

MAC アドレス移動通知トラップの設定

MAC 移動通知を設定する場合は、MAC アドレスが、同じ VLAN 内のあるポートから別のポートに移動すると常に、SNMP 通知が生成されてネットワーク管理システムに送信されます。

NMS ホストに MAC アドレス移動通知トラップを送信するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server host***host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*
4. **snmp-server enable traps mac-notification move**
5. **mac address-table notification mac-move**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**snmp-server host***host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type* 例： `Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification`	トラップ メッセージの受信側を指定します。 • *host-addr*：NMS の名前またはアドレスを指定します。 • **traps**（デフォルト）：ホストに SNMP トラップを送信します。 • **informs**：ホストにSNMPインフォームを送信します。 • **version**：サポートする SNMP バージョンを指定します。 informs にはバージョン 1（デフォルト）を使用できません。 • *community-string*：通知処理で送信する文字列を指定します。 **snmp-server host** コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。

	コマンドまたはアクション	目的
		• *notification-type*：**mac-notification** キーワードを使用します。
ステップ 4	**snmp-server enable traps mac-notification move** 例： `Switch(config)# snmp-server enable traps mac-notification move`	スイッチが NMS に MAC アドレス移動通知トラップを送信できるようにします。
ステップ 5	**mac address-table notification mac-move** 例： `Switch(config)# mac address-table notification mac-move`	MAC アドレス移動通知機能をイネーブルにします。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

スイッチによるMACアドレス移動通知トラップの送信をディセーブルにするには、**no snmp-server enable traps mac-notification move** グローバル コンフィギュレーション コマンドを使用します。MACアドレス変更通知機能をディセーブルにするには、**no mac address-table notification mac-move** グローバル コンフィギュレーション コマンドを使用します。

show mac address-table notification mac-move 特権 EXEC コマンドを入力して、設定を確認することができます。

MAC しきい値通知トラップの設定

MAC しきい値通知を設定する場合は、MAC アドレス テーブルのしきい値の制限値に達するか、その値を超えると、SNMP 通知が生成されてネットワーク管理システムに送信されます。

NMS ホストに MAC アドレス テーブルしきい値通知トラップを送信するようにスイッチを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server host***host-addr* {**traps**|**informs**} {**version** {**1** | **2c**| **3**}} *community-string notification-type*
4. **snmp-server enable traps mac-notification threshold**
5. **mac address-table notification threshold**
6. **mac address-table notification threshold** [**limit***percentage*] | [**interval***time*]
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server host***host-addr* {**traps**|**informs**} {**version** {**1** | **2c**| **3**}} *community-string notification-type* 例： `Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification`	トラップ メッセージの受信側を指定します。 • *host-addr*：NMS の名前またはアドレスを指定します。 • **traps**（デフォルト）：ホストに SNMP トラップを送信します。 • **informs**：ホストに SNMP インフォームを送信します。 • **version**：サポートする SNMP バージョンを指定します。 informs にはバージョン 1（デフォルト）を使用できません。

	コマンドまたはアクション	目的
		• *community-string*：通知処理で送信する文字列を指定します。 **snmp-server host** コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、**snmp-server community** コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 • *notification-type*：**mac-notification** キーワードを使用します。
ステップ 4	**snmp-server enable traps mac-notification threshold** 例： `Switch(config)# snmp-server enable traps mac-notification threshold`	NMS への MAC しきい値通知トラップをイネーブルにします。
ステップ 5	**mac address-table notification threshold** 例： `Switch(config)# mac address-table notification threshold`	MAC アドレスしきい値通知機能をイネーブルにします。

ステップ 6	**mac address-table notification threshold** [**limit***percentage*] | [**interval***time*]
	
	例：
	`Switch(config)# mac address-table notification threshold interval 123`
	`Switch(config)# mac address-table notification threshold limit 78`
		MAC アドレスしきい値使用状況モニタリングのしきい値を入力します。
		• （任意）**limit***percentage*：MAC アドレス テーブルの使用率を指定します。有効値は 1 ～ 100 % です。 デフォルト値は 50% です。
		• （任意）**interval***time*：通知の間隔を指定します。有効値は 120 秒以上です。 デフォルトは 120 秒です。

ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

スタティック アドレス エントリの追加および削除

スタティック アドレスを追加するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **mac address-table static***mac-addr***vlan***vlan-id***interface***interface-id*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**mac address-table static***mac-addr***vlan***vlan-id***interface***interface-id* 例： `Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1`	MAC アドレス テーブルにスタティック アドレスを追加します。 • *mac-addr*：アドレス テーブルに追加する宛先 MAC ユニキャストアドレスを指定します。 この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。 • *vlan-id*：指定された MAC アドレスを持つパケットを受信する VLAN を指定します。 指定できる VLAN ID の範囲は 1 ～ 4094 です。 • *interface-id*：受信パケットが転送されるインターフェイスを指定します。 有効なインターフェイスは、物理ポートまたはポート チャネルです。 スタティック マルチキャストアドレスの場合、複数のインターフェイス ID を入力できます。 スタティック ユニキャストアドレスの場合、インターフェイスは同時に 1 つしか入力できません。ただし、同じ MAC アドレスおよび VLAN ID を指定すると、コマンドを複数回入力できます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ユニキャスト MAC アドレス フィルタリングの設定

スイッチが送信元または宛先ユニキャスト スタティック アドレスをドロップするよう設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **mac address-table static***mac-addr***vlan***vlan-id***drop**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mac address-table static***mac-addr***vlan***vlan-id***drop** 例： `Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop`	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、スイッチが指定した送信元または宛先ユニキャスト スタティック アドレスを持つパケットをドロップするように設定します。 • *mac-addr*：送信元または宛先ユニキャスト MAC アドレス（48 ビット）を指定します。 この MAC アドレスを持つパケットはドロップされます。 • *vlan-id*：指定された MAC アドレスを持つパケットを受信する VLAN を指定します。 指定できる VLAN ID の範囲は 1 ～ 4094 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチのモニタリングおよび保守の管理

コマンド	目的
clear mac address-table dynamic	すべてのダイナミック エントリを削除します。
clear mac address-table dynamic address *mac-address*	特定の MAC アドレスを削除します。
clear mac address-table dynamic interface *interface-id*	指定された物理ポートまたはポートチャネル上のすべてのアドレスを削除します。
clear mac address-table dynamic vlan *vlan-id*	指定された VLAN 上のすべてのアドレスを削除します。
show clock [*detail*]	時刻と日付の設定を表示します。
show ip igmp snooping groups	すべての VLAN または指定された VLAN に対するレイヤ 2 マルチキャストエントリを表示します。
show mac address-table address *mac-address*	指定された MAC アドレスの MAC アドレステーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。

コマンド	目的
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface *interface-name*	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table move update	MAC アドレス テーブル移動更新情報を表示します。
show mac address-table multicast	マルチキャストの MAC アドレスのリストを表示します。
show mac address-table notification {change | mac-move | threshold}	MAC 通知パラメータおよび履歴テーブルを表示します。
show mac address-table secure	セキュア MAC アドレスを表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan *vlan-id*	指定された VLAN の MAC アドレス テーブル情報を表示します。

スイッチ管理の設定例

例：システム クロックの設定

次の例は、システム クロックを手動で設定する方法を示しています。

```
Switch# clock set 13:32:00 23 July 2013
```

例：サマー タイムの設定

次に、サマータイムが 3 月 10 日の 02:00 に開始され、11 月 3 日の 02:00 に終了するように指定する方法の例を示します。

```
Switch(config)# clock summer-time PDT recurring PST date
10 March 2013 2:00 3 November 2013 2:00
```

次に、サマータイムの開始日と終了日を設定する例を示します。

```
Switch(config)#clock summer-time PST date
20 March 2013 2:00 20 November 2013 2:00
```

例：MOTD バナーの設定

次の例は、開始および終了デリミタにポンド記号（#）を使用して、MOTDバナーを設定する方法を示しています。

```
Switch(config)# banner motd #

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

#

Switch(config)#
```

次に、前の設定により表示されたバナーの例を示します。

```
Unix> telnet 192.0.2.15

Trying 192.0.2.15...

Connected to 192.0.2.15.

Escape character is '^]'.

This is a secure site. Only authorized users are allowed.

For access, contact technical support.

User Access Verification

Password:
```

例：ログイン バナーの設定

次の例は、開始および終了デリミタにドル記号（$）を使用して、にログイン バナーを設定する方法を示しています。

```
Switch(config)# banner login $

Access for authorized users only. Please enter your username and password.

$

Switch(config)#
```

例：MAC アドレス変更通知トラップの設定

次に、NMS として 172.20.10.10 を指定し、NMS への MAC アドレス通知トラップの送信をイネーブルにし、MAC アドレス変更通知機能をイネーブルにし、インターバル タイムを 123 秒に設定

し、履歴サイズを 100 エントリに設定し、特定のポートで MAC アドレスが追加された場合のトラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet1/2/1
Switch(config-if)# snmp trap mac-notification change added
```

例：MAC しきい値通知トラップの設定

次に、NMS として 172.20.10.10 を指定し、MAC アドレスしきい値通知機能をイネーブルにし、インターバル タイムを 123 秒に設定し、制限を 78% に設定する例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification threshold
Switch(config)# mac address-table notification threshold
Switch(config)# mac address-table notification threshold interval 123
Switch(config)# mac address-table notification threshold limit 78
```

例：MAC アドレス テーブルへのスタティック アドレスの追加

次の例では、MAC アドレス テーブルにスタティック アドレス c2f3.220a.12f4 を追加する方法を示します。 VLAN 4 でこの MAC アドレスを宛先アドレスとして持つパケットを受信すると、パケットは指定されたポートに転送されます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet1/1/1
```

例：ユニキャスト MAC アドレス フィルタリングの設定

次に、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つドロップパケットを設定する例を示します。 送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

第 66 章

スイッチのセットアップ設定の実行

- スイッチセットアップ設定の実行に関する情報，1817 ページ
- スイッチ設定コンフィギュレーションの実行方法，1829 ページ
- スイッチのセットアップ設定のモニタリング，1845 ページ
- スイッチ のセットアップを実行する場合の設定例，1846 ページ

スイッチセットアップ設定の実行に関する情報

IP アドレスの割り当ておよび DHCP 自動設定を含む初期スイッチ設定タスクを実行する前に、このモジュールの各項を確認してください。

ブート プロセス

スイッチを起動するには、スタートアップ ガイドやハードウェア インストレーション ガイドの手順にしたがって、スイッチを設置して電源をオンにし、スイッチの初期設定（IP アドレス、サブネット マスク、デフォルト ゲートウェイ、シークレット、Telnet パスワードなど）を行う必要があります。

ブートローダ ソフトウェアは、通常の起動プロセスを実行します。これには、次のアクティビティが含まれています。

- バンドルまたはインストール パッケージ セットでブート可能（基本）パッケージを検索します。
- 下位レベルの CPU 初期化を行います。 CPU レジスタを初期化することにより、物理メモリがマッピングされる場所、容量、速度などを制御します。
- CPU サブシステムの電源投入時セルフ テスト（POST）を実行し、システム DRAM をテストします。
- システム ボード上のファイル システムを初期化します。

- デフォルトのオペレーティング システム ソフトウェア イメージをメモリにロードし、スイッチを起動します。

ブートローダによってフラッシュ ファイル システムにアクセスしてから、オペレーティング システムをロードします。ブートローダの使用目的は通常、オペレーティング システムのロード、展開、および起動に限定されます。 オペレーティング システムが CPU を制御できるようになると、ブートローダは、次にシステムがリセットされるか電源が投入されるまでは非アクティブになります。

また、オペレーティング システムが使用不可能になるほどの重大な障害が発生した場合は、ブートローダはシステムにトラップドアからアクセスします。 トラップドアからシステムへアクセスして、必要があれば、フラッシュ ファイル システムをフォーマットし、XMODEM プロトコルを使用してオペレーティング システムのソフトウェアイメージを再インストールし、失われたパスワードを回復し、最終的にオペレーティング システムを再起動できます。

スイッチ情報を割り当てるには、PC または端末をコンソール ポートに接続するか、PC をイーサネット管理ポートに接続して、PC または端末エミュレーション ソフトウェアのボーレートおよびキャラクタ フォーマットをスイッチのコンソールポートの設定と一致させておく必要があります。

- デフォルトのボーレートは 9600 です。
- デフォルトのデータ ビットは 8 です。

（注） データ ビット オプションを 8 に設定した場合、パリティ オプションは「なし」に設定します。

- デフォルトのストップ ビットは 2（マイナー）です。
- デフォルトのパリティ設定は「なし」です。

スイッチ情報の割り当て

IP 情報を割り当てるには、スイッチのセットアップ プログラムを使用する方法、Dynamic Host Configuration Protocol（DHCP）サーバを使用する方法、または手動で実行する方法があります。

特定の IP 情報の設定が必要な場合、スイッチのセットアップ プログラムを使用してください。このプログラムを使用すると、ホスト名とイネーブルシークレットパスワードを設定することもできます。

また、任意で、Telnet パスワードを割り当てたり（リモート管理中のセキュリティ確保のため）、スイッチをクラスタのコマンドまたはメンバスイッチとして、あるいはスタンドアロンスイッチとして設定したりできます。

サーバの設定後は DHCP サーバを使用して、IP 情報の集中管理と自動割り当てを行います。

（注） DHCP を使用している場合は、スイッチが動的に割り当てられた IP アドレスを受信してコンフィギュレーション ファイルを読み込むまでは、セットアップ プログラムからの質問に応答しないでください。

スイッチの設定手順を熟知している経験豊富なユーザの場合は、スイッチを手動で設定してください。 それ以外のユーザは、「ブート プロセス」で説明したセットアップ プログラムを使用してください。

デフォルトのスイッチ情報

表 *159* : デフォルトのスイッチ情報

機能	デフォルト設定
IP アドレスおよびサブネット マスク	IP アドレスまたはサブネット マスクは定義されていません。
デフォルト ゲートウェイ	デフォルト ゲートウェイは定義されていません。
イネーブル シークレット パスワード	パスワードは定義されていません。
ホスト名	出荷時に割り当てられるデフォルトのホスト名は、スイッチ です。
Telnet パスワード	パスワードは定義されていません。
クラスタ コマンド スイッチ機能	ディセーブル
クラスタ名	クラスタ名は定義されません。

DHCP ベースの自動設定の概要

DHCP は、インターネットホストおよびインターネットワーキング デバイスに設定情報を提供します。 このプロトコルには、2 つのコンポーネントがあります。1 つは DHCP サーバからデバイスにコンフィギュレーション パラメータを提供するコンポーネント、もう 1 つはデバイスにネットワーク アドレスを割り当てるコンポーネントです。 DHCP はクライアント/サーバ モデルに基づいています。指定された DHCP サーバが、動的に設定されるデバイスに対して、ネットワーク アドレスを割り当て、コンフィギュレーション パラメータを提供します。 スイッチは、DHCP クライアントおよび DHCP サーバとして機能できます。

DHCP ベースの自動設定では、スイッチ（DHCP クライアント）は起動時に、IP アドレス情報およびコンフィギュレーション ファイルを使用して自動的に設定されます。

DHCP ベースの自動設定を使用すると、スイッチ上で DHCP クライアント側の設定を行う必要はありません。 ただし、DHCP サーバで、IP アドレスに関連した各種リース オプションを設定する必要があります。

DHCP を使用してネットワーク上のコンフィギュレーション ファイルの場所をリレーする場合は、TFTP サーバおよびドメイン ネーム システム（DNS）サーバの設定が必要になることがあります。

スイッチの DHCP サーバは、スイッチと同じ LAN 上に配置することも、そのスイッチとは別の LAN 上に配置することもできます。 DHCP サーバが異なる LAN 上で動作している場合、スイッチと DHCP サーバ間に、DHCP のリレー デバイスを設定する必要があります。 リレー デバイスは、直接接続されている 2 つの LAN 間でブロードキャスト トラフィックを転送します。 ルータはブロードキャスト パケットを転送しませんが、受信したパケットの宛先 IP アドレスに基づいてパケットを転送します。

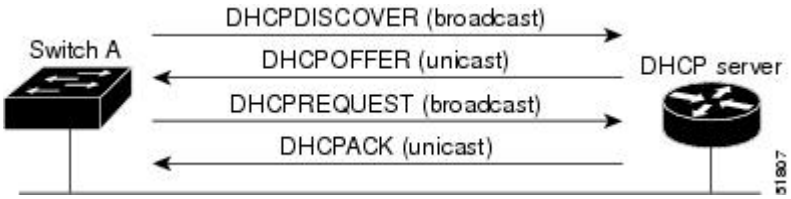
DHCP ベースの自動設定は、スイッチの BOOTP クライアント機能に代わるものです。

DHCP クライアント要求プロセス

スイッチを起動したときに、スイッチにコンフィギュレーション ファイルがない場合、DHCP クライアントが呼び出され、DHCP クライアントが DHCP サーバに設定情報を要求します。 コンフィギュレーション ファイルが存在し、その設定に特定のルーテッド インターフェイスの **ip address dhcp** インターフェイス コンフィギュレーション コマンドが含まれる場合、DHCP クライアントが呼び出され、DHCP クライアントがインターフェイスに IP アドレス情報を要求します。

次は、DHCP クライアントと DHCP サーバの間で交換される一連のメッセージです。

図 *119*：*DHCP* クライアント/サーバ間のメッセージ交換



クライアントであるスイッチ A は、DHCP サーバの場所を特定するために、DHCPDISCOVER メッセージをブロードキャストします。 DHCP サーバは、DHCPOFFER ユニキャスト メッセージによって、使用可能なコンフィギュレーション パラメータ（IP アドレス、サブネット マスク、ゲートウェイ IP アドレス、DNS IP アドレス、IP アドレス用のリースなど）をクライアントに提示します。

DHCPREQUEST ブロードキャスト メッセージでは、クライアントは、提示された設定情報に対して、DHCP サーバに正式な要求を戻します。 この正式な要求はブロードキャストされるため、クライアントから DHCPDISCOVER ブロードキャスト メッセージを受信した他のすべての DHCP サーバは、クライアントに提示した IP アドレスを再利用できます。

DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに戻すことで、IP アドレスがクライアントに割り当てられたことを確認します。 このメッセージによって、クライアントとサーバはバウンドされ、クライアントはサーバから受信した設定情報を使用します。 スイッチの受信する情報量は、DHCP サーバの設定方法によって異なります。

DHCPOFFERユニキャストメッセージによって送信されたコンフィギュレーション パラメータが無効である（コンフィギュレーション エラーがある）場合、クライアントは DHCP サーバに、DHCPDECLINE ブロードキャスト メッセージを戻します。

DHCP サーバはクライアントに、提示されたコンフィギュレーション パラメータが割り当てられていない、パラメータのネゴシエーション中にエラーが発生した、または DHCPOFFER メッセージに対するクライアントの応答が遅れている（DHCP サーバがパラメータを別のクライアントに割り当てた）という意味の DHCPNAK 拒否ブロードキャスト メッセージを送信します。

DHCP クライアントは、複数の DHCP サーバまたは BOOTP サーバから提示を受け取り、そのうちの任意の 1 つを受け入れることができますが、通常は最初に受け取った提示を受け入れます。DHCP サーバから提示された IP アドレスが必ずしもクライアントに割り当てられるわけではありません。ただし、サーバは通常、クライアントが正式にアドレスを要求するまではアドレスを確保しておきます。 スイッチがBOOTPサーバからの応答を受け入れ、自身を設定する場合、スイッチはスイッチ コンフィギュレーション ファイルを取得するために、TFTP 要求をユニキャストするのではなくブロードキャストします。

DHCP ホスト名オプションにより、スイッチのグループはホスト名および標準コンフィギュレーションを集中管理型DHCPサーバから取得できます。 クライアント（スイッチ）はDCHPDISCOVERメッセージ内に、DHCP サーバからのホスト名および他のコンフィギュレーション パラメータの要求に使用される Option 12 フィールドを加えます。 すべてのクライアントのコンフィギュレーション ファイルは、DHCP から取得したホスト名を除き、まったく同じです。

クライアントにデフォルトのホスト名がある場合（**hostname***name* グローバル コンフィギュレーション コマンドを設定していないか、**no hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を削除していない場合）は、**ip address dhcp** インターフェイス コンフィギュレーション コマンドを入力すると、DHCP のホスト名オプションがパケットに含まれません。 この場合、インターフェイスの IP アドレスを取得中にクライアントが DHCP との相互作用で DHCP ホスト名オプションを受信した場合、クライアントは DHCP ホスト名オプションを受け入れて、システムに設定済みのホスト名があることを示すフラグが設定されます。

DHCP ベースの自動設定およびイメージ アップデート

DHCP イメージ アップグレード機能を使用すると、ネットワーク内の 1 つ以上のスイッチに新しいイメージ ファイルおよび新しいコンフィギュレーション ファイルをダウンロードするように DHCP サーバを設定できます。 ネットワーク内のすべてのスイッチでのイメージおよびコンフィギュレーションの同時アップグレードによって、ネットワークに加えられたそれぞれの新しいスイッチが、同じイメージとコンフィギュレーションを確実に受信するようになります。

DHCP イメージ アップグレードには、自動設定およびイメージ アップデートの 2 つのタイプがあります。

DHCP ベースの自動設定の制約事項

- ネットワーク内に割り当てられた IP アドレスがなく、1 つ以上のレイヤ 3 インターフェイスが起動してない場合は、設定プロセスが保存された DHCP ベースの自動設定は停止します。

- タイムアウトを設定しない限り、設定機能を備えている DHCP ベースの自動設定は IP アドレスのダウンロードを無期限に繰り返します。
- コンフィギュレーション ファイルをダウンロードできないか破損している場合は、自動インストールプロセスが停止します。
- TFTP からダウンロードされたコンフィギュレーション ファイルは、実行コンフィギュレーション内の既存コンフィギュレーションとマージされますが、**write memory** または **copy running-configuration startup-configuration** 特権 EXEC コマンドを入力しない限り、NVRAM に保存されません。 ダウンロードされたコンフィギュレーションがスタートアップコンフィギュレーションに保存された場合、後続のシステム再起動中にこの機能はトリガーされません。

DHCP 自動設定

DHCP 自動設定は、コンフィギュレーション ファイルを DHCP サーバからネットワーク内の 1 つ以上のスイッチにダウンロードします。 ダウンロードされたコンフィギュレーション ファイルは、スイッチの実行コンフィギュレーションファイルになります。 このファイルは、スイッチがリロードされるまで、フラッシュ メモリに保存されたブートアップ コンフィギュレーションを上書きしません。

DHCP 自動イメージ アップデート

DHCP 自動設定とともに DHCP 自動イメージ アップグレードを使用すると、コンフィギュレーションおよび新しいイメージをネットワーク内の 1 つ以上のスイッチにダウンロードできます。 新しいコンフィギュレーションおよび新しいイメージをダウンロードしている 1 つのスイッチスイッチ（または複数のスイッチ）は、ブランク（つまり、出荷時のデフォルト設定がロードされている状態）にできます。

コンフィギュレーションをすでに持っているスイッチに新しいコンフィギュレーションをダウンロードすると、ダウンロードされたコンフィギュレーションは、スイッチに保存されているコンフィギュレーション ファイルに追加されます（どの既存のコンフィギュレーション ファイルも、ダウンロードされたファイルに上書きされません）。

スイッチの DHCP 自動イメージアップデートをイネーブルにするには、イメージ ファイルおよびコンフィギュレーション ファイルがある TFTP サーバを、正しいオプション 67（コンフィギュレーション ファイル名）、オプション 66（DHCP サーバ ホスト名）、オプション 150（TFTP サーバ アドレス）、およびオプション 125（Cisco IOS イメージ ファイルの説明）の設定で設定する必要があります。

スイッチをネットワークに設置すると、自動イメージ アップデート機能が開始します。 ダウンロードされたコンフィギュレーション ファイルはスイッチの実行コンフィギュレーションに保存され、新しいイメージがダウンロードされてスイッチにインストールされます。 スイッチを再起動すると、このコンフィギュレーションがスイッチのコンフィギュレーションに保存されます。

DHCP サーバ設定時の注意事項

デバイスを DHCP サーバとして設定する場合、次の注意事項に従ってください。

- DHCP サーバには、スイッチのハードウェア アドレスによって各スイッチと結び付けられている予約済みのリースを設定する必要があります。
- スイッチに IP アドレス情報を受信させるには、DHCP サーバに次のリース オプションを設定する必要があります。
  - クライアントの IP アドレス（必須）
  - クライアントのサブネット マスク（必須）
  - DNS サーバの IP アドレス（任意）
  - ルータの IP アドレス（スイッチで使用するデフォルト ゲートウェイ アドレス）（必須）
- スイッチに TFTP サーバからコンフィギュレーション ファイルを受信させる場合は、DHCP サーバに次のリース オプションを設定する必要があります。
  - TFTP サーバ名（必須）
  - ブート ファイル名（クライアントが必要とするコンフィギュレーション ファイル名）（推奨）
  - ホスト名（任意）
- DHCP サーバの設定によっては、スイッチは IP アドレス情報またはコンフィギュレーション ファイル、あるいはその両方を受信できます。
- 前述のリース オプションを設定しなかった場合、DHCP サーバは、設定されたパラメータのみを使用してクライアントの要求に応答します。 IP アドレスおよびサブネット マスクが応答に含まれていないと、スイッチは設定されません。 ルータの IP アドレスまたは TFTP サーバ名が見つからなかった場合、スイッチは TFTP 要求をユニキャストしないでブロードキャストする場合があります。 その他のリース オプションは、使用できなくても自動設定には影響しません。
- スイッチは DHCP サーバとして動作可能です。 デフォルトでは、Cisco IOS DHCP サーバおよびDHCP リレーエージェント機能はスイッチ上でイネーブルにされていますが、設定されていません。 （これらの機能は動作しません。）

DNS サーバの目的

DHCP サーバは、DNS サーバを使用して TFTP サーバ名を IP アドレスに変換します。 DNS サーバ上で、TFTP サーバ名から IP アドレスへのマッピングを設定する必要があります。 TFTP サーバには、スイッチのコンフィギュレーション ファイルが存在します。

DHCP の応答時に IP アドレスを取得する DHCP サーバのリース データベースに、DNS サーバの IP アドレスを設定できます。 リース データベースには、DNS サーバの IP アドレスを 2 つまで入力できます。

DNS サーバは、スイッチと同じ LAN 上に配置することも、別の LAN 上に配置することもできます。 DNS サーバが別の LAN 上に存在する場合、スイッチはルータを介して DNS サーバにアクセスできなければなりません。

コンフィギュレーション ファイルの入手方法

IP アドレスおよびコンフィギュレーション ファイル名が DHCP で専用のリースとして取得できるかどうかに応じて、スイッチは次の方法で設定情報を入手します。

- IP アドレスおよびコンフィギュレーション ファイル名が、スイッチ用に予約され、DHCP 応答（1 ファイル読み込み方式）で提供されている場合

  スイッチは DHCP サーバから、IP アドレス、サブネット マスク、TFTP サーバ アドレス、およびコンフィギュレーション ファイル名を受信します。 スイッチは、TFTP サーバにユニキャスト メッセージを送信し、指定されたコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、ブートアップ プロセスを完了します。

- スイッチの IP アドレスおよびコンフィギュレーション ファイル名が予約されているが、DHCP 応答に TFTP サーバ アドレスが含まれていない場合（1 ファイル読み込み方式）。

  スイッチは DHCP サーバから、IP アドレス、サブネット マスク、およびコンフィギュレーション ファイル名を受信します。 スイッチは、TFTP サーバにブロードキャスト メッセージを送信し、指定されたコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、ブートアップ プロセスを完了します。

- IP アドレスだけがスイッチ用に予約され、DHCP 応答で提供されており、 コンフィギュレーション ファイル名は提供されない場合（2 ファイル読み込み方式）

  スイッチ は DHCP サーバから、IP アドレス、サブネット マスク、および TFTP サーバ アドレスを受信します。 スイッチは、TFTP サーバにユニキャストメッセージを送信し、network-confg または cisconet.cfg のデフォルト コンフィギュレーション ファイルを取得します （network-confg ファイルが読み込めない場合、スイッチは cisconet.cfg ファイルを読み込みます）。

  デフォルト コンフィギュレーション ファイルには、スイッチのホスト名から IP アドレスへのマッピングが含まれています。 スイッチは、ファイルの情報をホスト テーブルに書き込み、ホスト名を入手します。 ファイルにホスト名がない場合、スイッチは DHCP 応答で指定されたホスト名を使用します。 DHCP 応答でホスト名が指定されていない場合、スイッチはデフォルトのスイッチをホスト名として使用します。

  デフォルトのコンフィギュレーション ファイルまたは DHCP 応答からホスト名を入手した後、スイッチはホスト名と同じ名前のコンフィギュレーション ファイル（network-confg または cisconet.cfg のどちらが先に読み込まれたかに応じて、*hostname*-confg または *hostname*.cfg）を TFTP サーバから読み込みます。 cisconet.cfg ファイルが読み込まれている場合は、ホストのファイル名は 8 文字に切り捨てられます。

network-confg、cisconet.cfg、またはホスト名と同じ名前のファイルを読み込むことができない場合、スイッチは router-confg ファイルを読み込みます。 router-confg ファイルを読み込むことができない場合、スイッチは ciscortr.cfg ファイルを読み込みます。

（注） DHCP 応答から TFTP サーバを入手できなかった場合、ユニキャスト伝送によるコンフィギュレーション ファイルの読み込みにすべて失敗した場合、または TFTP サーバ名を IP アドレスに変換できない場合には、スイッチは TFTP サーバ要求をブロードキャストします。

環境変数の制御方法

通常動作のスイッチでは、コンソール接続のみを通じてブート ローダ モードを開始します。 スイッチの電源コードを取り外してから、もう一度電源コードを接続します。 ブートローダ スイッチのプロンプトが表示されるまで [MODE] を押し続けます。

スイッチのブートローダ ソフトウェアは不揮発性の環境変数をサポートするため、これらの環境変数を使用して、ブート ローダまたはシステムで稼働する他のソフトウェアの機能を制御できます。 ブートローダの環境変数は、UNIX または DOS システムで設定できる環境変数と類似しています。

値を持つ環境変数は、フラッシュ ファイル システムの外にあるフラッシュ メモリに保存されます。

ファイルの各行には、環境変数名と等号に続いて、その変数の値が指定されます。 変数が存在しない場合は、変数の値はありません。値がヌル ストリングと表示された場合は、変数に値が設定されています。 ヌル ストリング（たとえば " "）が設定されている変数は、値が設定された変数です。 多くの環境変数は事前に定義されており、デフォルト値が設定されています。

環境変数には 2 種類のデータが保存されます。

- Cisco IOS コンフィギュレーション ファイルを読み取らないコードを制御するデータ。 たとえば、ブートローダの機能を拡張したり、パッチを適用したりするブートローダ ヘルパー ファイルの名前は、環境変数として保存できます。
- Cisco IOS コンフィギュレーション ファイルを読み取るコードを制御するデータ。 たとえば、Cisco IOS コンフィギュレーション ファイル名は環境変数として保存できます。

環境変数の設定を変更するには、ブートローダにアクセスするか、Cisco IOS コマンドを使用します。 通常の環境では、環境変数の設定を変更する必要はありません。

一般的な環境変数

この表では、最も一般的な環境変数の機能について説明します。

表 *160*：一般的な環境変数

変数	ブートローダコマンド	Cisco IOS グローバル コンフィギュレーション コマンド
BOOT	**set BOOT***filesystem***:/***file-url* ... 自動起動時にロードして実行を試みる、セミコロンで区切られた実行可能ファイルのリスト。 BOOT 環境変数が設定されていない場合、システムは、フラッシュファイルシステム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュ ファイルシステムで最初に検出した起動可能なファイルを起動しようとします。	**boot system** {*filesystem***:/***file-url* ... 次の起動時にロードする Cisco IOS イメージと、イメージがロードされるスタックメンバーを指定します。 このコマンドは、BOOT 環境変数の設定を変更します。

変数	ブートローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
MANUAL_BOOT	**set MANUAL_BOOT yes** スイッチの起動を自動で行うか手動で行うかを決定します。 有効な値は1、yes、0、および no です。no または 0 に設定されている場合、ブートローダはシステムを自動的に起動しようとします。それ以外の値に設定されている場合は、ブートローダ モードから手動でスイッチを起動する必要があります。	**boot manual** 次回の起動時にスイッチを手動で起動できるようにします。MANUAL_BOOT 環境変数の設定が変更されます。 次回のシステム再起動時には、スイッチはブートローダ モードになります。システムを起動するには、**boot flash:***filesystem***:/***file-url* ブートローダ コマンドを使用し、起動可能イメージの名前を指定します。
CONFIG_FILE	**set CONFIG_FILE flash:/***file-url* Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を変更します。	**boot config-file flash:/***file-url* Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。このコマンドによって、CONFIG_FILE 環境変数が変更されます。
SWITCH_NUMBER	**set SWITCH_NUMBER** *current-member-number* スタック メンバのメンバ番号を変更します。	**switch** *current-stack-member-number* **renumber** *new-stack-member-number* スタック メンバのメンバ番号を変更します。
SWITCH_PRIORITY	**set SWITCH_PRIORITY** *current-member-number* スタック メンバのプライオリティ値を変更します。	**switch** *stack-member-number* **priority** *priority-number* スタック メンバのプライオリティ値を変更します。

変数	ブートローダコマンド	Cisco IOS グローバル コンフィギュレーション コマンド
BAUD	**set BAUD** *baud-rate*	**line console 0** **speed***speed-value* ボー レートを設定します。
ENABLE_BREAK	**set ENABLE_BREAK yes/no**	**boot enable-break switch yes/no** このコマンドは、**ENABLE_BREAK** が **yes** に設定されている場合にフラッシュ ファイル システムを初期化するときに発行できます。

TFTP の環境変数

イーサネット管理ポートを通してスイッチに PC を接続していると、TFTP でブートローダに対してコンフィギュレーションファイルのアップロードまたはダウンロードができます。 このテーブルの環境変数が設定されていることを確認します。

表 *161*：*TFTP* の環境変数

変数	説明
MAC_ADDR	スイッチの MAC アドレスを指定します。 （注） 変数は変更しないことを推奨します。 ただし、ブートローダを稼働している場合、またはこの変数が保存されている値と異なる場合は、TFTP を使用する前にこのコマンドを入力します。
IP_ADDR	スイッチの関連付けられた IP サブネットに IP アドレスおよびサブネット マスクを指定します。
DEFAULT_ROUTER	デフォルト ゲートウェイに IP アドレスおよびサブネット マスクを指定します。

ソフトウェア イメージのリロードのスケジューリング

スイッチ上でソフトウェア イメージのリロードを後で（深夜、週末などスイッチをあまり使用しないときに）行うように、スケジュールを設定できます。または（ネットワーク内のすべてのスイッチでソフトウェアをアップグレードする場合など）ネットワーク全体でリロードを同時に行うことができます。

（注） リロードのスケジュールは、約 24 日以内に設定する必要があります。

リロード オプションには以下のものがあります。

- 指定した分数、または時間および分数が経過したときに、ソフトウェアがリロードされます。 リロードは、約 24 時間以内に実行する必要があります。 最大 255 文字で、リロードの理由を指定できます。
- ソフトウェアのリロードが（24 時間制で）指定された時間に有効になります。 月日を指定すると、指定された日時にリロードが行われるようにスケジュールが設定されます。 月日を指定しなかった場合、リロードは当日の指定時刻に行われます（指定時刻が現時刻より後の場合）。または翌日の指定時刻に行われます（指定時刻が現在時刻よりも前の場合）。 00:00 を指定すると、深夜 0 時のリロードが設定されます。

reload コマンドはシステムを停止させます。 手動で起動することが設定されていない限り、システムは自動的に再起動します。

手動で起動するようにスイッチが設定されている場合、仮想端末からリロードを実行しないでください。 これは、スイッチがブート ローダ モードになり、そのため、リモート ユーザが制御を失うことを防止するためです。

コンフィギュレーション ファイルを変更すると、リロードの前にコンフィギュレーションを保存するように指示するプロンプトがスイッチにより表示されます。 保存操作時に、CONFIG_FILE 環境変数がすでに存在しないスタートアップ コンフィギュレーション ファイルを示していた場合、保存を続行するかどうかという問い合わせがシステムから出されます。 その状況のまま続けると、リロード時にセットアップ モードが開始されます。

スケジュールがすでに設定されたリロードを取り消すには、**reload cancel** 特権 EXEC コマンドを使用します。

スイッチ設定コンフィギュレーションの実行方法

DHCP を使用してスイッチに新しいイメージおよび新しいコンフィギュレーションをダウンロードするには、少なくとも 2 つのスイッチ を設定する必要があります。 1 つ目のスイッチは DHCP サーバおよびTFTP サーバと同じように機能し、2つ目のスイッチ（クライアント）は新しいコンフィギュレーション ファイル、または新しいコンフィギュレーション ファイルおよび新しいイメージ ファイルをダウンロードするように設定されています。

DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定

このタスクでは、新しいスイッチの自動設定をサポートできるように、ネットワーク内の既存のスイッチで TFTP や DHCP の設定の DHCP 自動設定を行う方法を示します。

手順の概要

1. **configure terminal**
2. **ip dhcp pool***poolname*
3. **boot***filename*
4. **network***network-number mask prefix-length*
5. **default-router***address*
6. **option 150***address*
7. **exit**
8. **tftp-server flash**:*filename.text*
9. **interface***interface-id*
10. **no switchport**
11. **ip address***address mask*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**ip dhcp pool***poolname* 例： `Switch(config)# ip dhcp pool pool`	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**boot***filename* 例： `Switch(dhcp-config)# boot config-boot.text`	ブート イメージとして使用されるコンフィギュレーション ファイルの名前を指定します。

	コマンドまたはアクション	目的
ステップ 4	**network***network-number mask prefix-length* 例： `Switch(dhcp-config)# network 10.10.10.0 255.255.255.0`	DHCP アドレス プールのサブネット ネットワーク番号およびマスクを指定します。 （注） プレフィックス長は、アドレスプレフィックスを構成するビット数を指定します。 プレフィックスは、クライアントのネットワークマスクを指定する二者択一の方法です。プレフィックス長は、スラッシュ（/）で開始する必要があります。
ステップ 5	**default-router***address* 例： `Switch(dhcp-config)# default-router 10.10.10.1`	DHCP クライアントのデフォルト ルータの IPアドレスを指定します。
ステップ 6	**option 150***address* 例： `Switch(dhcp-config)# option 150 10.10.10.1`	TFTP サーバの IP アドレスを指定します。
ステップ 7	**exit** 例： `Switch(dhcp-config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**tftp-server flash**:*filename.text* 例： `Switch(config)# tftp-server flash:config-boot.text`	TFTP サーバ上のコンフィギュレーション ファイルを指定します。
ステップ 9	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/4`	コンフィギュレーション ファイルを受信するクライアントのアドレスを指定します。
ステップ 10	**no switchport** 例： `Switch(config-if)# no switchport`	インターフェイスをレイヤ 3 モードにします。

	コマンドまたはアクション	目的
ステップ 11	**ip address***address mask* 例： `Switch(config-if)# ip address 10.10.10.1 255.255.255.0`	IPアドレスとインターフェイスのマスクを指定します。
ステップ 12	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

例：DHCP サーバとしてのスイッチの設定, （1846 ページ）

DHCP 自動イメージ アップデート（コンフィギュレーション ファイルおよびイメージ）の設定

このタスクでは、新しいスイッチのインストールをサポートするように既存のスイッチで TFTP および DHCP を設定する DHCP 自動設定について説明します。

はじめる前に

最初にスイッチにアップロードするテキスト ファイル（たとえば、autoinstall_dhcp）を作成します。 テキスト ファイルに、ダウンロードするイメージの名前を指定します（たとえば、c3750e-ipservices-mz.122-44.3.SE.tarc3750x-ipservices-mz.122-53.3.SE2.tar）。 このイメージは、bin ファイルでなく、tar ファイルである必要があります。

手順の概要

1. **configure terminal**
2. **ip dhcp pool***poolname*
3. **boot***filename*
4. **network***network-number mask prefix-length*
5. **default-router***address*
6. **option 150***address*
7. **option 125***hex*
8. **copy tftp flash***filename.txt*
9. **copy tftp flash***imagename.bin*
10. **exit**
11. **tftp-server flash:***config.text*
12. **tftp-server flash:***imagename.bin*
13. **tftp-server flash:***filename.txt*
14. **interface***interface-id*
15. **no switchport**
16. **ip address***address mask*
17. **end**
18. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**ip dhcp pool***poolname* 例： `Switch(config)# ip dhcp pool pool1`	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	**boot***filename* 例： `Switch(dhcp-config)# boot config-boot.text`	ブート イメージとして使用されるファイルの名前を指定します。

	コマンドまたはアクション	目的
ステップ 4	**network***network-number mask prefix-length* 例： `Switch(dhcp-config)# network 10.10.10.0 255.255.255.0`	DHCPアドレスプールのサブネットネットワーク番号およびマスクを指定します。 （注） プレフィックス長は、アドレス プレフィックスを構成するビット数を指定します。 プレフィックスは、クライアントのネットワーク マスクを指定する二者択一の方法です。 プレフィックス長は、スラッシュ（/）で開始する必要があります。
ステップ 5	**default-router***address* 例： `Switch(dhcp-config)# default-router 10.10.10.1`	DHCP クライアントのデフォルト ルータの IPアドレスを指定します。
ステップ 6	**option 150***address* 例： `Switch(dhcp-config)# option 150 10.10.10.1`	TFTP サーバの IP アドレスを指定します。
ステップ 7	**option 125***hex* 例： `Switch(dhcp-config)# option 125 hex 0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370`	イメージ ファイルのパスを記述したテキスト ファイルのパスを指定します。
ステップ 8	**copy tftp flash***filename.txt* 例： `Switch(config)# copy tftp flash image.bin`	スイッチに、テキスト ファイルをアップロードします。
ステップ 9	**copy tftp flash***imagename.bin* 例： `Switch(config)# copy tftp flash image.bin`	スイッチに、新しいイメージの tar ファイルをアップロードします。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Switch(dhcp-config)# exit`	グローバルコンフィギュレーションモードに戻ります。
ステップ 11	**tftp-server flash:***config.text* 例： `Switch(config)# tftp-server flash:config-boot.text`	TFTP サーバ上の Cisco IOS コンフィギュレーション ファイルを指定します。
ステップ 12	**tftp-server flash:***imagename.bin* 例： `Switch(config)# tftp-server flash:image.bin`	TFTP サーバ上のイメージ名を指定します。
ステップ 13	**tftp-server flash:***filename.txt* 例： `Switch(config)# tftp-server flash:boot-config.text`	ダウンロードするイメージ ファイルの名前を記述したテキスト ファイルを指定します。
ステップ 14	**interface***interface-id* 例： `Switch(config)# interface gigabitEthernet1/0/4`	コンフィギュレーション ファイルを受信するクライアントのアドレスを指定します。
ステップ 15	**no switchport** 例： `Switch(config-if)# no switchport`	インターフェイスをレイヤ 3 モードにします。
ステップ 16	**ip address***address mask* 例： `Switch(config-if)# ip address 10.10.10.1 255.255.255.0`	IP アドレスとインターフェイスのマスクを指定します。
ステップ 17	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 18	**copyrunning-configstartup-config** 例： `Switch(config-if)# end`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

例：DHCP 自動イメージ アップデートの設定, （1846 ページ）

DHCP サーバからファイルをダウンロードするクライアントの設定

（注） レイヤ 3 インターフェイスだけを設定してイネーブルにする必要があります。 保存されているコンフィギュレーションの DHCP ベースの自動設定に IP アドレスを割り当てないでください。

手順の概要

1. **configure terminal**
2. **boot host dhcp**
3. **boot host retry timeout***timeout-value*
4. **banner config-save ^C***warning-message***^C**
5. **end**
6. **show boot**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**boot host dhcp** 例： `Switch(conf)# boot host dhcp`	保存されているコンフィギュレーションで自動設定をイネーブルにします。
ステップ 3	**boot host retry timeout***timeout-value* 例： `Switch(conf)# boot host retry timeout 300`	（任意）システムがコンフィギュレーション ファイルをダウンロードしようとする時間を設定します。 （注） タイムアウトを設定しないと、システムは無期限に DHCP サーバから IP アドレスを取得しようとします。
ステップ 4	**banner config-save ^C***warning-message***^C** 例： `Switch(conf)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause You to No longer Automatically Download Configuration Files at Reboot^C`	（任意）コンフィギュレーションファイルをNVRAMに保存しようとするときに表示される警告メッセージを作成します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show boot** 例： `Switch# show boot`	設定を確認します。

関連トピック

例：DHCP サーバから設定をダウンロードするためのスイッチの設定，（1846 ページ）

複数の SVI への IP 情報の手動割り当て

このタスクでは、複数のスイッチ仮想インターフェイス（SVI）に IP 情報を手動で割り当てる方法について説明します。

手順の概要

1. **configure terminal**
2. **interface vlan***vlan-id*
3. **ip address***ip-address subnet-mask*
4. **exit**
5. **ip default-gateway***ip-address*
6. **end**
7. **show interfaces vlan***vlan-id*
8. **show ip redirects**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan***vlan-id* 例： `Switch(config)# interface vlan 99`	インターフェイスコンフィギュレーションモードを開始し、IP 情報を割り当てる VLAN を入力します。 指定できる範囲は 1 ～ 4094 です。
ステップ 3	**ip address***ip-address subnet-mask* 例： `Switch(config-vlan)# ip address 10.10.10.2 255.255.255.0`	IP アドレスとサブネット マスクを入力します。
ステップ 4	**exit** 例： `Switch(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip default-gateway***ip-address* 例： `Switch(config)# ip default-gateway 10.10.10.1`	スイッチに直接接続しているネクスト ホップのルータ インターフェイスの IP アドレスを入力します。このスイッチにはデフォルト ゲートウェイが設定されています。 デフォルト ゲートウェイは、スイッチスイッチから宛先 IP アドレスを取得していない IP パケットを受信します。

	コマンドまたはアクション	目的
		デフォルト ゲートウェイが設定されると、スイッチは、ホストが接続する必要のあるリモート ネットワークに接続できます。 （注） IP でルーティングするようにスイッチを設定した場合、デフォルト ゲートウェイの設定は不要です。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces vlan***vlan-id* 例： `Switch# show interfaces vlan 99`	設定された IP アドレスを確認します。
ステップ 8	**show ip redirects** 例： `Switch# show ip redirects`	設定されたデフォルト ゲートウェイを確認します。

NVRAM バッファ サイズの設定

デフォルトの NVRAM バッファ サイズは 512 KB です。 コンフィギュレーション ファイルが大きすぎて NVRAM に保存できない場合があります。 一般的に、この状態はスイッチ スタック内に多くのスイッチがある場合に発生します。 より大きいコンフィギュレーションファイルをサポートできるように、NVRAM バッファのサイズを設定できます。 新しい NVRAM バッファ サイズは、現在および新しいすべてのメンバ スイッチに同期されます。

（注） NVRAM バッファ サイズを設定後、スイッチまたはスイッチ スタックをリロードします。

スイッチをスタックに追加し、NVRAM サイズが異なる場合、新しいスイッチはスタックに同期化し、自動的にリロードされます。

手順の概要

1. **configure terminal**
2. **boot buffersize***size*
3. **end**
4. **showboot**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot buffersize***size* 例： `Switch(config)# boot buffersize 524288`	NVRAM のバッファ サイズを KB 単位で設定します。 *size* の有効な範囲は、4096 ～ 1048576 です。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**showboot** 例： `Switch# show boot`	設定を確認します。

関連トピック

例：NVRAM バッファ サイズの設定，（1847 ページ）

スイッチのスタートアップ コンフィギュレーションの変更

システム コンフィギュレーションを読み書きするためのファイル名の指定

Cisco IOS ソフトウェアは、デフォルトで config.text ファイルを使用して、システム コンフィギュレーションの不揮発性コピーを読み書きします。 別のファイル名を指定することもできます。次回の起動時には、その名前のファイルが読み込まれます。

はじめる前に

このタスクではスタンドアロンの スイッチ を使用します。

手順の概要

1. **configure terminal**
2. **boot config-file** file name
3. **end**
4. **show boot**
5. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot config-file** file name 例： `Switch(config)# boot config-file config.text`	次回の起動時に読み込むコンフィギュレーション ファイルを指定します。 *file-url*：パス（ディレクトリ）およびコンフィギュレーション ファイル名。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**show boot** 例： `Switch# show boot`	入力を確認します。 **boot** グローバル コンフィギュレーション コマンドによって、CONFIG_FILE 環境変数の設定が変更されます。
ステップ 5	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチの手動による起動

スイッチはデフォルトで自動的に起動しますが、手動で起動するように設定することもできます。

はじめる前に

このタスクのスタンドアロン スイッチを使用します。

手順の概要

1. **configure terminal**
2. **boot manual**
3. **end**
4. **show boot**
5. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**boot manual** 例： `Switch(config)# boot manual`	次回の起動時に、スイッチを手動で起動できるようにします。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show boot** 例： `Switch# show boot`	入力を確認します。 **boot manual** グローバル コンフィギュレーション コマンドによって、MANUAL_BOOT 環境変数の設定が変更されます。 次回、システムを再起動したときには、スイッチはブートローダモードになり、ブートローダ モードであることが *switch:* プロンプトによって示されます。 システムを起動するには、**boot***filesystem:/file-url* ブート ローダ コマンドを使用します。 • *filesystem*：システム ボードのフラッシュ デバイスに flash: を使用します。 スイッチ: **boot flash:** • *file-url*：パス（ディレクトリ）および起動可能なイメージの名前を指定します。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ステップ 5	**copyrunning-configstartup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ソフトウェア イメージのリロードのスケジュール設定

このタスクでは、ソフトウェア イメージを後でリロードするようにスイッチを設定する方法について説明します。

手順の概要

1. **configure terminal**
2. **copy running-config startup-config**
3. **reload in** [*hh*:]*mm* [*text*]
4. **reload at** *hh*: *mm* [*month day* | *day month*] [*text*]
5. **reload cancel**
6. **show reload**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**copy running-config startup-config** 例： `copy running-config startup-config`	**reload** コマンドを使用する前に、スイッチの設定情報をスタートアップ コンフィギュレーションに保存する必要があります。

ステップ 3	**reload in** [*hh*:]*mm* [*text*]
	
	例：
	`Switch(config)# reload in 12`
	
	`System configuration has been modified. Save? [yes/no]: y`
		指定した分数、または時間および分数が経過したときに、ソフトウェアがリロードされるようにスケジュールを設定します。リロードは、約 24 日以内に実行する必要があります。 最大 255 文字で、リロードの理由を指定できます。

ステップ 4	**reload at** *hh*: *mm* [*month day* | *day month*] [*text*] 例： `Switch(config)# reload at 14:00`	リロードを実行する時間を、時間数と分数で指定します。 （注） **at** キーワードを使用するのは、スイッチのシステムクロックが（ネットワーク タイムプロトコル（NTP）、ハードウェア カレンダー、または手動で）設定されている場合だけです。 時刻は、スイッチに設定されたタイムゾーンに基づきます。 リロードが複数のスイッチで同時に行われるようにスケジューリングするには、各スイッチの時間が NTP と同期している必要があります。
ステップ 5	**reload cancel** 例： `Switch(config)# reload cancel`	以前にスケジューリングされたリロードをキャンセルします。

	コマンドまたはアクション	目的
ステップ 6	**show reload** 例： **show reload**	以前スイッチにスケジューリングされたリロードに関する情報、またはリロードがスケジューリングされているかを表示します。

スイッチのセットアップ設定のモニタリング

例：スイッチ実行コンフィギュレーションの確認

```
Switch# show running-config
Building configuration...

Current configuration: 1363 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Stack1
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxE0
!
.
<output truncated>
.
interface gigabitethernet6/0/2
mvr type source

<output truncated>

...!
interface VLAN1
 ip address 172.20.137.50 255.255.255.0
 no ip directed-broadcast
!
ip default-gateway 172.20.137.1 !
!
snmp-server community private RW
snmp-server community public RO
snmp-server community private@es0 RW
snmp-server community public@es0 RO
snmp-server chassis-id 0x12
!
end
```

例：ソフトウェア インストールの表示

この例では、インストール モードでのソフトウェア ブートアップの表示を示します。

```
switch# boot flash:/c3560cx-universalk9-mz.152-3.E/c3560cx-universalk9-tar.152-3.E.bin
```

スイッチ のセットアップを実行する場合の設定例

例：DHCP サーバとしてのスイッチの設定

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# boot config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

関連トピック

DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定, （1830 ページ）

例：DHCP 自動イメージ アップデートの設定

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# boot config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# option 125 hex 0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370

Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# tftp-server flash:image_name
Switch(config)# tftp-server flash:boot-config.text
Switch(config)# tftp-server flash: autoinstall_dhcp
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

関連トピック

DHCP 自動イメージ アップデート（コンフィギュレーション ファイルおよびイメージ）の設定, （1832 ページ）

例：DHCP サーバから設定をダウンロードするためのスイッチの設定

次に、VLAN 99 上のレイヤ 3 SVI インターフェイスを使用し、保存されているコンフィギュレーションで DHCP ベースの自動設定をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# boot host dhcp
```

```
Switch(config)# boot host retry timeout 300
Switch(config)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause
 You to No longer Automatically Download Configuration Files at Reboot^C
Switch(config)# vlan 99
Switch(config-vlan)# interface vlan 99
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# show boot
BOOT path-list:
Config file:          flash:/config.text
Private Config file:  flash:/private-config.text
Enable Break:         no
Manual Boot:          no
HELPER path-list:
NVRAM/Config file
      buffer size:    32768
Timeout for Config
          Download:    300 seconds
Config Download
       via DHCP:       enabled (next boot: enabled)
Switch#
```

関連トピック

DHCP サーバからファイルをダウンロードするクライアントの設定, （1836 ページ）

例：NVRAM バッファ サイズの設定

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# boot buffersize 600000
Switch(config)# end
Switch# show boot
BOOT path-list      :
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : no
HELPER path-list    :
Auto upgrade        : yes
Auto upgrade path   :
NVRAM/Config file
      buffer size:   600000
Timeout for Config
          Download:    300 seconds
Config Download
       via DHCP:       enabled (next boot: enabled)
Switch#
```

関連トピック

NVRAM バッファ サイズの設定, （1839 ページ）

第 67 章

スイッチのクラスタリング

- 機能情報の確認，1849 ページ
- RTU ライセンスの設定に関する制約事項，1849 ページ
- RTU ライセンスの設定に関する情報，1850 ページ
- RTU ライセンスの設定方法，1852 ページ
- RTU ライセンスのモニタリングおよびメンテナンス，1856 ページ
- RTU ライセンスの設定例，1857 ページ

機能情報の確認

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

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

RTU ライセンスの設定に関する制約事項

次に、RTU ライセンスの設定および使用に関する制約事項を示します。

- AP-Count ライセンスは注文が可能で、スイッチ上で事前にアクティブ化できます。
- イメージベースのライセンスはアップグレードできます。 AP-Count ライセンスは非アクティブ化したり、スイッチとコントローラとの間で移動したりできます。

- 永久ライセンスをアクティブ化するには、新しいイメージ レベルを設定した後にスイッチを再起動する必要があります。 AP-Count ライセンスをアクティブ化するために再起動する必要はありません。
- 期限切れのイメージ ベースの評価ライセンスは、再起動後は再アクティブ化できません。
- スイッチ スタックのスタック メンバは同一のライセンス レベルを実行する必要があります。
- スイッチは、注文したイメージとともに事前にインストールされています。 イメージを事前に注文していなかった場合、スイッチはデフォルトで LAN ベース イメージで起動します。
- 追加 AP-Count ライセンスは、工場出荷時にインストールされます。

関連トピック

イメージ ベース ライセンスのアクティブ化, （1852 ページ）

例：RTU イメージ ベースのライセンスのアクティブ化, （1857 ページ）

RTU ライセンスの設定に関する情報

Right-To-Use ライセンス

Right-To-Use（RTU）ライセンスでは、特定のライセンス タイプおよびレベルを注文してアクティブ化し、ライセンスの使用状況をスイッチで管理することができます。 注文できるライセンスは次のとおりです。

- 永久ライセンス：特定の機能を備え、有効期限のないライセンスを購入できます。
- 評価ライセンス：スイッチに事前にインストールされています。使用有効期間は90 日です。

永久ライセンスまたは評価ライセンスをアクティブ化するには、エンドユーザ ライセンス契約（EULA）を承認する必要があります。 評価ライセンスの場合は、90 日の期限が切れる前に永久ライセンスを購入するか、ライセンスを非アクティブ化するように通知されます。

永久ライセンスは 1 つのデバイスから別のデバイスに移動できます。 ライセンスをアクティブ化するには、スイッチを再起動する必要があります。

評価ライセンスはスイッチのマニュファクチャリング イメージであり、別のスイッチに移動できません。 このタイプのライセンスは、再起動後は再アクティブ化できません。

関連トピック

イメージ ベース ライセンスのアクティブ化, （1852 ページ）

例：RTU イメージ ベースのライセンスのアクティブ化, （1857 ページ）

Right-To-Use イメージ ベースのライセンス

Right-To-Use イメージ ライセンスは、特定のイメージ ベースに基づき、次の一連の機能をサポートします。

- LAN Base：レイヤ 2 の機能。
- IP Base：レイヤ 2 およびレイヤ 3 の機能。
- IP Services：レイヤ 2、レイヤ 3、IPv6 の機能 （スイッチにのみ適用され、コントローラには適用されません）。

デフォルトのイメージ ベースのライセンスは LAN Base です。

Right-To-Use ライセンスの状態

特定のライセンス タイプとレベルを設定した後は、ライセンスの状態をモニタすることでライセンスを管理できます。

表 *162*： *RTU* ライセンスの状態

ライセンスの状態	説明
Active, In Use	EULA が承認され、デバイス再起動後にライセンスが使用されています。
Active, Not In Use	EULA が承認され、ライセンスがイネーブルになった時点でスイッチを使用する準備が整っています。
Not Activated	EULA が承認されませんでした。

イメージ ベースのライセンスの状態をモニタする場合の注意事項は次のとおりです。

- 購入したライセンスはスイッチの再起動後のみに *Active, In Use* 状態に設定されます。
- 複数のライセンスを購入した場合は、再起動すると最も高い機能セットのライセンスがアクティブ化されます。 たとえば、IP Services ライセンスがアクティブ化され、LAN Base ライセンスはアクティブ化されません。
- スイッチの再起動後、購入済みの残りのライセンスは **Active, Not In Use** 状態のままになります。

（注） AP-Count ライセンスの場合に状態を「Active, In Use」に変更するには、まず、評価 AP-Count ライセンスが非アクティブ化されていることを確認する必要があります。

モビリティ コントローラ モード

スイッチがモビリティ コントローラ モードになっている場合にのみ、AP-Count ライセンスを使用します。 MCは、AP-CountAP-Count ライセンスをトラッキングするゲートキーパであり、アクセス ポイント参加を許可または拒否できます。

AP-Count ライセンスは、CLI から設定可能なモビリティ コントローラ モードのスイッチを実行して管理します。

Right-To-Use Adder AP-Count 再ホスト ライセンス

あるデバイスのライセンスを無効にして、別のデバイスにインストールする操作を再ホストと呼びます。 デバイスの目的を変更するために、ライセンスのリホストが必要になる場合があります。

ライセンスを再ホストするには、あるデバイスの Adder AP-Count ライセンスを非アクティブ化し、別のデバイスで同じライセンスをアクティブ化します。

評価ライセンスを再ホストすることはできません。

RTU ライセンスの設定方法

イメージ ベース ライセンスのアクティブ化

手順の概要

1. **license right-to-use activate**{**ipbase** |**ipservices** | **lanbase**} {**all** | **evaluation all** } [**slot** *slot-number*] [**acceptEULA**]
2. **reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]
3. **show license right-to-use usage** [**slot** *slot-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use activate**{**ipbase** |**ipservices**	**lanbase**} {**all**	**evaluation all** } [**slot** *slot-number*] [**acceptEULA**] 例： `Switch# license right-to-use activate ipservices all acceptEULA`	イメージ ベース ライセンスのタイプをアクティブ化します。 すべてのスイッチ上でアクティブ化され、EULA への同意が含まれることもあります。

	コマンドまたはアクション	目的
		（注） EULA に同意しない場合は、変更した設定はリロード後に反映されません。デフォルトのライセンス（または非アクティブ化されたライセンス）がリロード後にアクティブになります。

ステップ 2	**reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]
	
	例：
	`Switch# reload slot 1`
	`Proceed with reload? [confirm] y`
		特定のスタック メンバをリロードし、RTU 追加 AP-Count ライセンスのアクティブ化プロセスを完了します。
		（注） これまでに同意していなかった場合は、リロード後に同意を促すメッセージが表示されます。

ステップ 3	**show license right-to-use usage** [**slot** *slot-number*]
	
	例：
	`Switch# show license right-to-use usage`
	
	`Slot# License Name Type usage-duration(y:m:d) In-Use EULA`
	`----------`
	`1 ipservices permanent 0 :10 :0 yes yes`
	`1 ipbase permanent 0 :0 :0 no no`
	`1 ipbase evaluation 0 :0 :0 no no`
	`1 lanbase permanent 0 :0 :7 no yes`
	`1 apcount evaluation 0 :0 :0 no no`
	`1 apcount base 0 :0 :0 no no`
	`1 apcount adder 0 :0 :0 no no`
	
	`Switch#`
		詳細な使用状況に関する情報を表示します。

関連トピック

RTU ライセンスの設定に関する制約事項，（1849 ページ）
Right-To-Use ライセンス，（1850 ページ）
RTU ライセンスのモニタリングおよびメンテナンス，（1856 ページ）
例：RTU イメージ ベースのライセンスのアクティブ化，（1857 ページ）

ap-count ライセンスのアクティブ化

手順の概要

1. **license right-to-use activate**{**apcount** *ap-number* **slot** *slot-num*} | **evaluation**} [**acceptEULA**]
2. **show license right-to-use usage** [**slot** *slot-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use activate**{**apcount** *ap-number* **slot** *slot-num*} | **evaluation**} [**acceptEULA**] 例： `Switch# license right to use activate apcount 5 slot 1 acceptEULA`	1 つ以上の追加 AP-Count ライセンスをアクティブ化し、EULA にすぐに同意します。

ステップ 2	**show license right-to-use usage** [**slot** *slot-number*]
	
	例：
	
	`Switch# show license right-to-use usage`
	
	`Slot# License Name Type usage-duration(y:m:d) In-Use EULA`
	`----------`
	
	`1 ipservices permanent 0 :3 :29 yes yes`
	`1 ipservices evaluation 0 :0 :0 no no`
	`1 ipbase permanent 0 :0 :0 no no`
	`1 ipbase evaluation 0 :0 :0 no no`
	`1 lanbase permanent 0 :0 :0 no no`
	`1 apcount evaluation 0 :3 :11 no no`
	`1 apcount base 0 :0 :0 no yes`
	`1 apcount adder 0 :0 :17 yes yes`
	
	`Switch#`
		詳細な使用状況に関する情報を表示します。

関連トピック

RTU ライセンスのモニタリングおよびメンテナンス, （1856 ページ）

Right-To-Use AP-Count ライセンス

Right-to-Use AP-Count 評価ライセンス

アップグレード ライセンスまたはキャパシティ Adder ライセンスの取得

キャパシティ Adder ライセンスを使用すれば、スイッチがサポートするアクセス ポイントの数が増やせます。

手順の概要

1. **license right-to-use** {**activate** | **deactivate**} **apcount** {*ap-number* | **evaluation** } **slot** *slot-num* [**acceptEULA**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use** {**activate** | **deactivate**} **apcount** {*ap-number* | **evaluation** } **slot** *slot-num* [**acceptEULA**] 例： `Switch# license right to use activate apcount 5 slot 2 acceptEULA`	1 つ以上の追加 AP-Count ライセンスをアクティブ化し、EULA にすぐに同意します。

関連トピック

Right-to-Use AP-Count 評価ライセンス

Right-To-Use AP-Count ライセンス

ライセンスの再ホスト

ライセンスを再ホストするには、1 つのスイッチのライセンスを非アクティブ化し、別のスイッチで同じライセンスをアクティブ化します。

手順の概要

1. **license right-to-use deactivate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**]
2. **license right-to-use activate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**license right-to-use deactivate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**] 例： `Switch# license right to use deactivate apcount 1 slot 1 acceptEULA`	1 つのスイッチのライセンスを非アクティブ化します。

	コマンドまたはアクション	目的
ステップ 2	**license right-to-use activate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**] 例： `Switch# license right to use activate apcount 2 slot 2 acceptEULA`	別のスイッチのライセンスをアクティブ化します。

関連トピック

Right-To-Use AP-Count ライセンス
Right-to-Use AP-Count 評価ライセンス

RTU ライセンスのモニタリングおよびメンテナンス

コマンド	目的
show license right-to-use default	デフォルトのライセンス情報を表示します。
show license right-to-use detail	スイッチスタック内のすべてのライセンスの詳細情報を表示します。
show license right-to-use eula {adder | evaluation | permanent}	エンドユーザ ライセンス契約を表示します。
show license right-to-use mismatch	一致しないライセンス情報を表示します。
show license right-to-use slot *slot-number*	スイッチスタック内の特定のスロットのライセンス情報を表示します。
show license right-to-use summary	スイッチスタック全体のライセンス情報の要約を表示します。
show license right-to-use usage [**slot** *slot-number*]	スイッチスタック内のすべてのライセンスの使用状況に関する詳細情報を表示します。
show switch	ライセンスのステータスを含むスイッチスタック内のすべてのメンバの詳細情報を表示します。

関連トピック

イメージ ベース ライセンスのアクティブ化, （1852 ページ）
例：RTU イメージ ベースのライセンスのアクティブ化, （1857 ページ）
ap-count ライセンスのアクティブ化, （1854 ページ）

RTU ライセンスの設定例

例：RTU イメージ ベースのライセンスのアクティブ化

次に、IP Services イメージ ライセンスをアクティブ化し、特定のスロットの EULA を受け入れる例を示します。

```
Switch# license right-to-use activate ipservices slot 1 acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

次に、評価用ライセンスをアクティブ化する例を示します。

```
Switch# license right-to-use activate ipservices evaluation acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

関連トピック

イメージ ベース ライセンスのアクティブ化, （1852 ページ）
RTU ライセンスの設定に関する制約事項, （1849 ページ）
Right-To-Use ライセンス, （1850 ページ）
RTU ライセンスのモニタリングおよびメンテナンス, （1856 ページ）

例：RTU ライセンス情報の表示

例：RTU ライセンスの詳細の表示

次に、スロット 1 の RTU ライセンスのすべての詳細情報の例を示します。

例：RTU ライセンスの不一致の表示

この例では、スタック内のスイッチのライセンス情報と、メンバ スイッチの不一致ステータスを示します。 メンバ スイッチがアクティブ スイッチと一致している必要があります。

```
Switch# show switch
```

```
Switch/Stack Mac Address : 6400.f125.0c80
                                                    H/W   Current
Switch#   Role        Mac Address     Priority Version  State
-----------------------------------------------------------------------------
 1       Standby     6400.f125.1b00     1      0        Ready
*2       Active      6400.f125.0c80     1      V01      Ready
 3       Member      6400.f125.1780     1      0        Lic-Mismatch
```

（注） ライセンスの不一致を解決するには、まず、RTU ライセンスのサマリーを確認します。

```
Switch# show switch right-to-use summary
```

次に、アクティブ スイッチと同じライセンス レベルとなるように、一致していないスイッチのライセンス レベルを変更します。 この例では、アクティブ スイッチと一致するように IP Base ライセンスをメンバ スイッチに対してアクティブ化したことを示します。

```
Switch# license right-to-use activate ipbase slot 1 acceptEULA
```

例：RTU ライセンス使用状況の表示

第 68 章

スイッチのクラスタリング

- スイッチ クラスタの概要，1859 ページ
- スイッチ クラスタのプランニング，1862 ページ
- CLI を使用したスイッチ クラスタの管理，1873 ページ
- SNMP を使用したスイッチ クラスタの管理，1874 ページ

スイッチ クラスタの概要

スイッチ クラスタは、最大 16 個の接続されたクラスタ対応 Catalyst スイッチで、単一エンティティとして管理されます。 クラスタ内のSwitchは、Switch クラスタ化テクノロジーによって、単一の IP アドレスから異なる Catalyst デスクトップ Switch プラットフォームで構成されたグループを設定したり、トラブルシューティングを行ったりできます。

Switch クラスタでは、1 台のSwitchがクラスタ コマンド Switchとして動作する必要があり、最大で 15 台の他のSwitchがクラスタ メンバ スイッチとして動作できます。 1 つのクラスタ内のSwitchの総数は、16 Switchを超えることはできません。 クラスタ コマンド Switchは、クラスタ メンバ Switchの設定、管理、およびモニタを実行できる唯一のスイッチです。 クラスタ メンバは、一度に 1 つのクラスタにしか所属できません。

（注） Switch クラスタはスイッチ スタックとは異なります。 スイッチ スタックとは、スタック ポート経由で接続された Catalyst 3750-X、Catalyst 3750-E、または Catalyst 3750 Switchのセットです。

Switchのクラスタ化には次のような利点があります。

- 相互接続メディアや物理的な場所に左右されず Catalyst Switchの管理ができます。 Switchは同じ場所に設置することも、レイヤ 2 またはレイヤ 3 ネットワークを介して設置することもできます（Catalyst 3560、Catalyst 3750、Catalyst 3560-E、Catalyst 3750-E、Catalyst 3560-X、または Catalyst 3750-X Switchを、クラスタのレイヤ 2 Switchの間に設置するレイヤ 3 のルータとして使用している場合）。

- コマンドスイッチに冗長性を持たせることで、コマンド Switchに障害が発生した場合でも対応できます。 1 つまたは複数のSwitchをスタンバイ クラスタ コマンド スイッチに指定すると、クラスタ メンバ間の競合を回避できます。 クラスタ スタンバイ グループは、スタンバイ クラスタ コマンド Switchのグループです。
- さまざまな Catalyst Switchを 1 つの IP アドレスで管理できます。 これは、特に IP アドレスの数が限られている場合に効果があります。 スイッチ クラスタとの通信はすべてクラスタ コマンド Switchの IP アドレスで行われます。

下の表に、Switchのクラスタ化に対応している Catalyst スイッチを示します。クラスタ コマンド スイッチになれるスイッチおよびクラスタ メンバ スイッチにしかなれないスイッチ、さらに、それらに必要なソフトウェア バージョンも示します。

表 *163* : スイッチ ソフトウェアおよびクラスタへの対応性

スイッチ	Cisco IOS リリース	クラスタへの対応性
Catalyst 3750-X	12.2(53)SE2 以降	メンバまたはコマンド スイッチ
Catalyst 3750-E	12.2(35)SE2 以降	メンバまたはコマンド スイッチ
Catalyst 3750	12.1(11)AX 以降	メンバまたはコマンド スイッチ
Catalyst 3560-X	12.2(53)SE1 以降	メンバまたはコマンド スイッチ
Catalyst 3560-E	12.2(35)SE2 以降	メンバまたはコマンド スイッチ
Catalyst 3560	12.1(19)EA1b 以降	メンバまたはコマンド スイッチ
Catalyst 3550	12.1(4)EA1 以降	メンバまたはコマンド スイッチ
Catalyst 2970	12.1(11)AX 以降	メンバまたはコマンド スイッチ
Catalyst 2960	12.2(25)FX 以降	メンバまたはコマンド スイッチ
Catalyst 2955	12.1(12c)EA1 以降	メンバまたはコマンド スイッチ
Catalyst 2950	12.0(5.2)WC(1) 以降	メンバまたはコマンド スイッチ
Catalyst 2950 LRE	12.1(11)JY 以降	メンバまたはコマンド スイッチ
Catalyst 2940	12.1(13)AY 以降	メンバまたはコマンド スイッチ
Catalyst 3500 XL	12.0(5.1)XU 以降	メンバまたはコマンド スイッチ
Catalyst 2900 XL（8 MB スイッチ）	12.0(5.1)XU 以降	メンバまたはコマンド スイッチ
Catalyst 2900 XL（4 MB スイッチ）	11.2(8.5)SA6（推奨）	メンバ スイッチのみ

Catalyst 1900 および Catalyst 2820	9.00（-A または -EN）以降	メンバ スイッチのみ

クラスタ コマンド スイッチの特性

クラスタ コマンド Switchは次の要件を満たす必要があります。

- サポート対象のソフトウェア リリースを実行している。
- IP アドレスが指定されている。
- Cisco Discovery Protocol（CDP）バージョン 2 がイネーブル（デフォルト）に設定されている。
- 別のクラスタのコマンドまたはクラスタ メンバのSwitchではない。
- 管理 VLAN を介してスタンバイ クラスタ コマンド Switchに、共通 VLAN を介してクラスタ メンバ Switchに接続されている。

スタンバイ クラスタ コマンド スイッチの特性

スタンバイ クラスタ コマンド Switchは次の要件を満たす必要があります。

- サポート対象のソフトウェア リリースを実行している。
- IP アドレスが指定されている。
- CDP バージョン 2 がイネーブルに設定されている。
- 管理 VLAN を介してコマンド Switchに接続されていて、なおかつ他のスタンバイ コマンド Switchに接続されている。
- 共通 VLAN を介して（クラスタ コマンドおよびスタンバイ コマンド Switchを除く）他のすべてのクラスタ メンバ Switchに接続されている。
- クラスタ メンバ Switchとの接続能力を維持するために、クラスタに冗長接続されている。
- 他のクラスタのコマンドまたはメンバ Switchではない。

（注） スタンバイ クラスタ コマンド Switchは、クラスタ コマンド Switchと同タイプのSwitchでなければなりません。 たとえば、クラスタ コマンド Switchが Catalyst 3750-E Switchの場合、スタンバイ クラスタ コマンド Switchも Catalyst 3750-E Switchにする必要があります。 スタンバイ クラスタ コマンドSwitchの要件については、他のクラスタ対応Switchのコンフィギュレーション ガイドを参照してください。

候補スイッチおよびクラスタ メンバ スイッチの特性

候補スイッチとは、クラスタにまだ追加されていないクラスタ対応SwitchおよびSwitch スタックです。 クラスタ メンバ Switchは、Switch クラスタにすでに追加されているスイッチおよびスイッチ スタックです。 候補またはクラスタ メンバのSwitchには独自の IP アドレスおよびパスワードを指定できますが、必須ではありません。

クラスタに加入するには、候補Switchが次の要件を満たしている必要があります。

- クラスタ対応のソフトウェアが稼働している。
- CDP バージョン 2 がイネーブルに設定されている。
- 別のクラスタのコマンドまたはクラスタ メンバのSwitchではない。
- クラスタ スタンバイ グループが存在する場合、少なくとも 1 つの共通 VLAN を介して、すべてのスタンバイ クラスタ コマンド Switchに接続されている。 各スタンバイ クラスタ コマンド Switchに対応する VLAN は、異なる場合があります。
- **ip http** グローバル コンフィギュレーション コマンドはSwitchで設定する必要があります。
- 少なくとも 1 つの共通 VLAN を介して、クラスタ コマンド Switchに接続されている。

（注） Catalyst 1900、Catalyst 2820、Catalyst 2900 XL、Catalyst 2940、Catalyst 2950、および Catalyst 3500 XL 候補およびクラスタ メンバ Switchは、管理 VLAN を介してクラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチに接続する必要があります。 スイッチ クラスタ環境におけるこれらのSwitchの詳細情報は、該当するスイッチのソフトウェア コンフィギュレーション ガイドを参照してください。 Catalyst 2960、Catalyst 2970、Catalyst 3550、Catalyst 3560、Catalyst 3560-E、Catalyst 3750、Catalyst 3750-E、Catalyst 3650-X、または Catalyst 3750-X クラスタ コマンド スイッチを使用する場合、この要件は当てはまりません。 候補およびクラスタ メンバ Switchは、クラスタ コマンド スイッチと共通の任意の VLAN を介して接続できます。

スイッチ クラスタのプランニング

複数のスイッチをクラスタで管理する場合、予想される競合や互換性の問題解決に重点を置きます。 ここでは、クラスタを作成する前に理解すべき注意事項、要件、および警告について説明します。

クラスタに対応している Catalyst スイッチについては、各スイッチのリリース ノートを参照してください。リリース ノートでは、クラスタ コマンド スイッチになれるスイッチとクラスタ メンバー スイッチにしかなれないスイッチ、また、それらに必要なソフトウェア バージョンやブラウザだけでなく、Java プラグインの設定も参照できます。

クラスタ候補およびメンバの自動検出

クラスタ コマンド スイッチは Cisco Discovery Protocol（CDP）を使用して、複数の VLAN の中からクラスタ メンバ スイッチ、候補スイッチ、ネイバー スイッチクラスタ、エッジ デバイスを検出します。また、スター型のトポロジやカスケード型のトポロジ内からも検出できます。

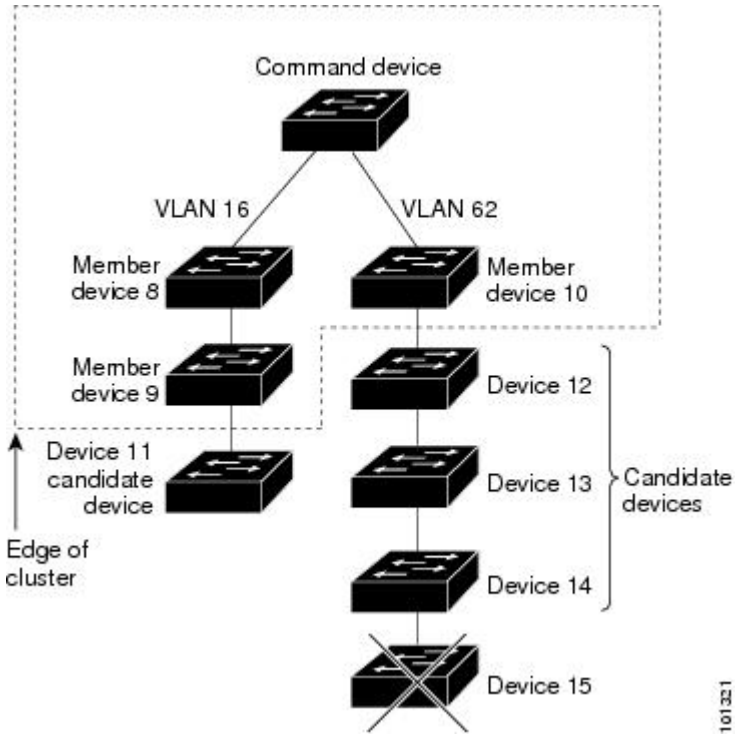
（注） クラスタ コマンド スイッチを使用してクラスタに対応したスイッチを検出する場合、クラスタ コマンド スイッチ、クラスタ メンバ、またはクラスタ対応スイッチの CDP を無効にしないでください。

CDP ホップによる検出

クラスタ コマンド スイッチは CDP を使用して、クラスタ エッジから最大 7 CDP ホップ（デフォルトは 3 ホップ）までスイッチを検出できます。 クラスタ エッジは、クラスタや候補スイッチに接続している最後のクラスタ スイッチの部分を指します。 たとえば、図のクラスタ メンバ スイッチ 9 と 10 はクラスタのエッジにあります。

この図では、クラスタ コマンド スイッチには VLAN 16 と 62 に割り当てられたポートがあります。 CDP ホップのカウントは 3 です。 クラスタ エッジから 3 ホップ以内にあるので、クラスタ コマンド スイッチはスイッチ 11、12、13、14 を検出します。 スイッチ 15 はクラスタ エッジから 4 ホップ先なので検出されません。

図 *120*：*CDP* ホップによる検出

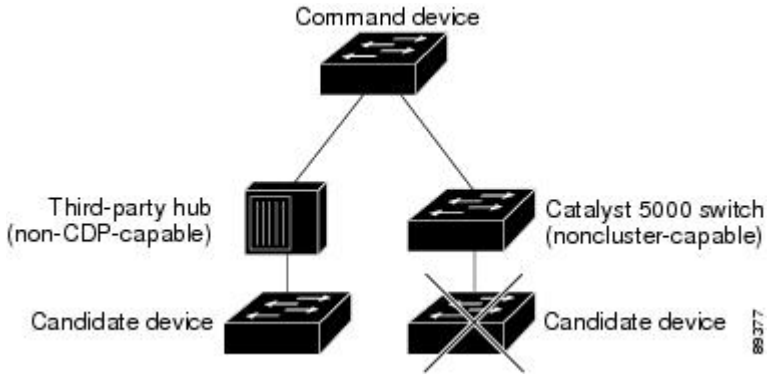


CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出

クラスタ コマンド スイッチを *CDP* 非対応のサードパーティ製のハブ（他社製のハブなど）に接続している場合、そのサードパーティ製のハブを介して接続しているクラスタ対応デバイスを検出できます。 ただし、クラスタ コマンド スイッチをクラスタ非対応のシスコ デバイスに接続している場合、クラスタ非対応のシスコ デバイスより先にあるクラスタ対応のデバイスは検出できません。

下の図に、サードパーティ製のハブに接続したスイッチを検出するクラスタ コマンド スイッチを示します。 ただし、クラスタ コマンド スイッチは Catalyst 5000 スイッチに接続しているスイッチは検出しません。

図 *121*：*CDP* 非対応デバイスおよびクラスタ非対応デバイスからの検出



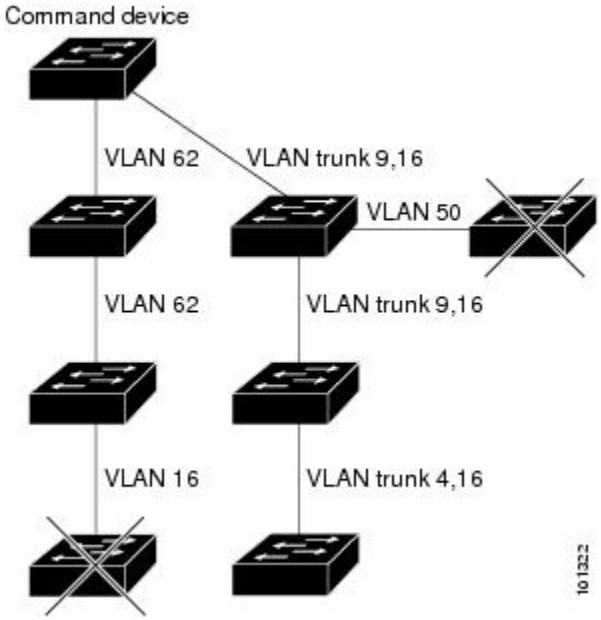
異なる VLAN からの検出

クラスタ コマンドスイッチが、Catalyst 3560-E、Catalyst 3750-E、Catalyst 3560-X、または Catalyst 3750-X スイッチの場合、クラスタは、異なる VLAN にあるスイッチをクラスタ メンバにすることができます。 クラスタ メンバ スイッチとして、Catalyst スイッチもクラスタ コマンド スイッチと共通の VLAN に少なくとも 1 つは接続している必要があります。 図のクラスタ コマンド スイッチのポートは VLAN 9、16、62 に割り当てられているため、これらの VLAN のスイッチが検出されます。 VLAN 50 にあるスイッチは検出されません。 また、最初の列の VLAN 16 にあるスイッチも、クラスタ コマンド スイッチに VLAN が接続されていないため検出されません。

Catalyst 2900 XL、Catalyst 2950、および Catalyst 3500 XL のクラスタ メンバ スイッチは、それぞれの管理 VLAN を介してクラスタ コマンド スイッチに接続している必要があります。

（注） スイッチ スタックにある VLAN の考慮事項については、「スイッチ クラスタおよびスイッチ スタック」を参照してください。

図 *122*：異なる *VLAN* からの検出



異なる管理 VLAN からの検出

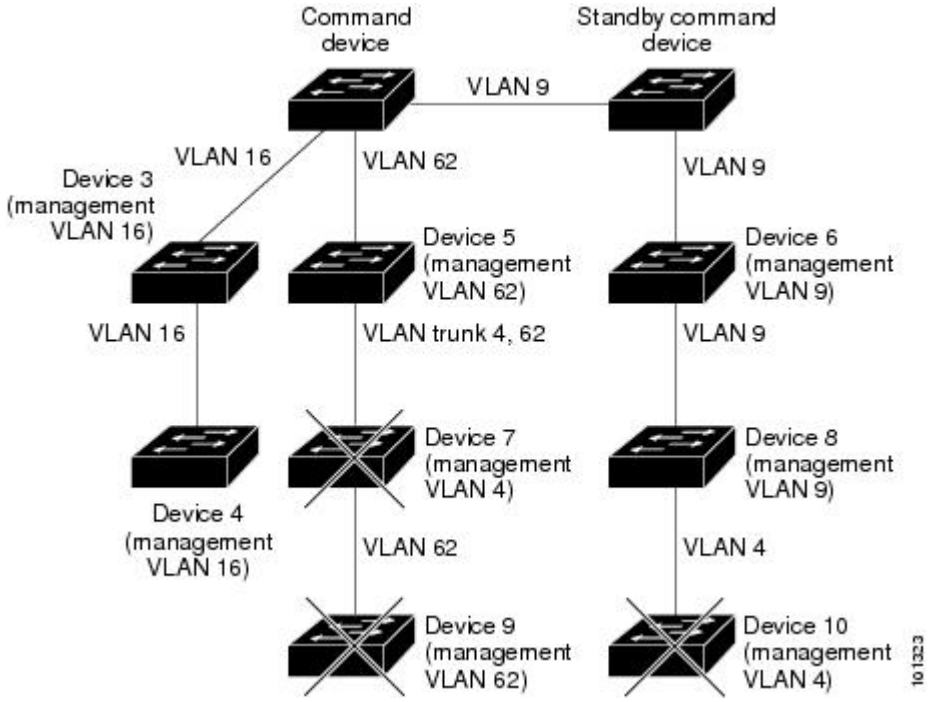
Catalyst 2960、Catalyst 2970、Catalyst 3550、Catalyst 3560、Catalyst 3560-E、Catalyst 3750、Catalyst 3750-E、Catalyst 3560-X、または Catalyst 3750-X クラスタ コマンド スイッチは、異なる VLAN や管理 VLAN のクラスタ メンバ スイッチを検出して管理できます。 クラスタ メンバ スイッチとして、Catalyst スイッチもクラスタ コマンド スイッチと共通の VLAN に少なくとも 1 つは接続している必要があります。 ただし、管理 VLAN を介してクラスタ コマンド スイッチに接続する必要はありません。 デフォルトの管理 VLAN は VLAN 1 です。

（注） スイッチ クラスタに Catalyst 3750-E スイッチ、Catalyst 3750-X スイッチまたはスイッチ スタックがある場合、スイッチまたはスイッチ スタックをクラスタ コマンド スイッチにする必要があります。

図に示されているクラスタ コマンドスイッチおよびスタンバイ コマンドスイッチ（Catalyst 2960、Catalyst 2970、Catalyst 3550、Catalyst 3560、Catalyst 3560-E、Catalyst 3750、Catalyst 3750-E、Catalyst 3560-X、または Catalyst 3750-X と想定します）のポートには、VLAN 9、16、および 62 が割り当てられています。 クラスタ コマンド スイッチの管理 VLAN は VLAN 9 です。 各クラスタ コマンド スイッチは、次の例外を除き、異なる管理 VLAN のスイッチを検出します。

- スイッチ 7 およびスイッチ 10（管理 VLAN 4 のスイッチ）。クラスタ コマンド スイッチと共通の VLAN（VLAN 62 および VLAN 9）に接続していないため検出されません。
- スイッチ 9。自動検出は非候補デバイス（スイッチ 7）より先は検出できないため、検出されません。

図 *123*：レイヤ *3* クラスタ コマンド スイッチを使用した異なる管理 *VLAN* からの検出



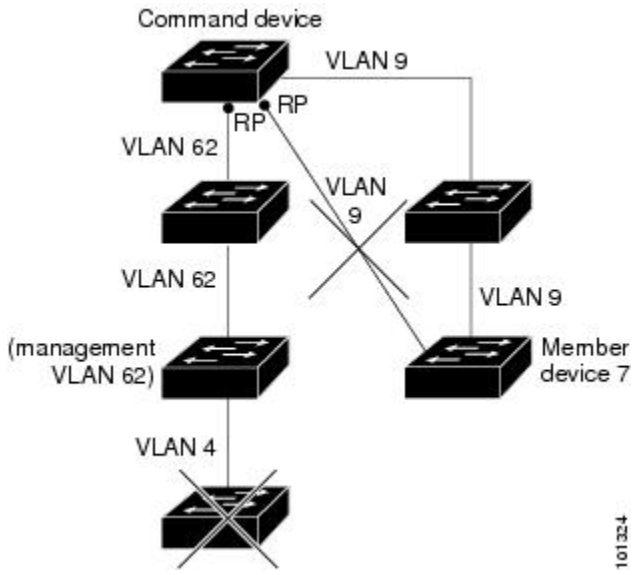
ルーテッド ポートからの検出

ルーテッド ポート（RP）が設定されているクラスタ コマンド スイッチは、RP と同じ VLAN 内の候補スイッチおよびクラスタ メンバ スイッチだけを検出します。

図のレイヤ 3 クラスタ コマンド スイッチにより、VLAN 9 および 62 のスイッチは検出されますが、VLAN 4 のスイッチは検出されません。 クラスタ コマンドスイッチとクラスタ メンバスイッ

チ 7 間の RP パスが損失している場合、VLAN 9 を介する冗長パスがあるため、クラスタ メンバ スイッチ 7 との接続は維持されます。

図 *124* : ルーテッド ポートからの検出



新しく設置したスイッチの検出

新しいアウトオブボックス スイッチをクラスタに加入させるには、アクセスポートの 1 つを介してクラスタに接続する必要があります。 アクセス ポート（AP）は 1 つの VLAN にのみ属し、そのトラフィックを転送します。 デフォルトでは、新しいスイッチとそのアクセス ポートが VLAN 1 に割り当てられます。

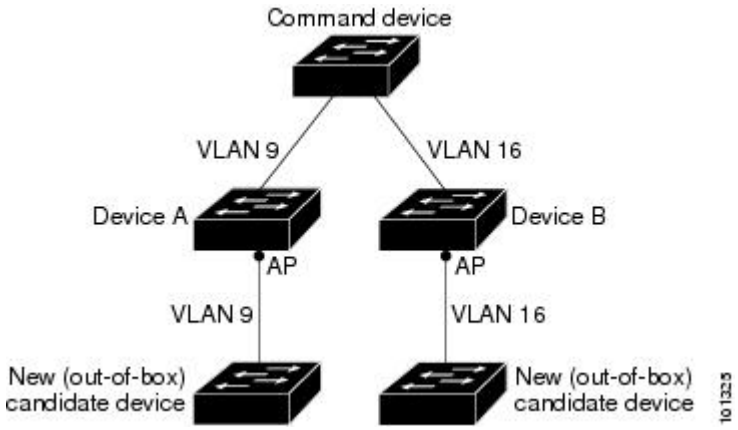
新しいスイッチがクラスタに加入すると、デフォルトの VLAN は即座にアップストリーム ネイバーの VLAN に変わります。 また、新しいスイッチも自身のアクセス ポートを変更して、そのネイバーの VLAN に加わります。

図のクラスタ コマンド スイッチは、VLAN 9 および 16 に加入しています。 新しいクラスタ対応のスイッチがクラスタに加入すると、次の処理が行われます。

- 1 つのクラスタ対応のスイッチとそのアクセス ポートが VLAN 9 に割り当てられます。

- 他のクラスタ対応のスイッチとそのアクセス ポートが管理 VLAN 16 に割り当てられます。

図 *125*：新しく設置したスイッチの検出



HSRP およびスタンバイ クラスタ コマンド スイッチ

スイッチは Hot Standby Router Protocol（HSRP）をサポートしているため、スタンバイ クラスタ コマンド スイッチのグループを設定できます。 クラスタ コマンド スイッチは、すべての通信の転送と、すべてのクラスタ メンバスイッチの設定情報を管理しているため、次のような環境設定を推奨します。

- クラスタ コマンドのスイッチ スタックには、スイッチ スタック全体に障害が発生する場合に備えて、スタンバイ クラスタ コマンド スイッチが必要です。 ただし、コマンド スイッチのスタック マスターだけに障害が発生した場合は、スイッチ スタックで新しいスタック マスターを選出し、クラスタ コマンド スイッチ スタックとしての機能を引き継がせることができます。
- スタンドアロンのクラスタ コマンド スイッチの場合、プライマリ クラスタ コマンド スイッチの障害に備え、スタンバイ クラスタ コマンド スイッチを設定してその機能を引き継がせるようにします。

クラスタ スタンバイ グループは、「スタンバイ クラスタ コマンド スイッチの特性」の項で説明している要件を満たしたコマンド対応スイッチのグループです。 クラスタごとに、1 つのクラスタ スタンバイ グループのみ割り当てることができます。

（注） クラスタ スタンバイ グループは HSRP グループです。 HSRP をディセーブルにすると、クラスタ スタンバイ グループがディセーブルになります。

クラスタ スタンバイ グループのスイッチは、HSRP プライオリティに基づいてランク付けされています。 グループ内でプライオリティが最も高いスイッチは、アクティブ クラスタ コマンド スイッチ（AC）です。 グループ内で次にプライオリティの高いスイッチは、スタンバイ クラスタ コマンド スイッチ（SC）です。 クラスタ スタンバイ グループの他のスイッチは、パッシブ クラ

スタ コマンド スイッチ（PC）です。 アクティブ クラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチが同時にディセーブルになった場合、パッシブ クラスタ コマンド スイッチの中でプライオリティが一番高いものがアクティブ クラスタ コマンド スイッチになります。 クラスタ スタンバイ グループのメンバおよびルータ冗長グループのメンバのプライオリティの変更には、同じ HSRP **standby priority** インターフェイス コンフィギュレーション コマンドを使用します。

（注） HSRP のスタンバイ中止間隔は、hello タイム間隔の 3 倍以上必要です。 デフォルトの HSRP スタンバイ中止間隔は 10 秒です。 デフォルトの HSRP スタンバイ hello タイム インターバルは 3 秒です。

仮想 IP アドレス

クラスタ スタンバイ グループには、一意の仮想 IP アドレス、グループ番号、グループ名を割り当てる必要があります。 この情報は、特定の VLAN またはアクティブ クラスタ コマンド スイッチのルーテッド ポートで設定します。 アクティブ クラスタ コマンド スイッチは、仮想 IP アドレス宛てのトラフィックを受信します。 クラスタを管理するには、コマンドスイッチの IP アドレスからではなく、仮想 IP アドレスからアクティブ クラスタ コマンド スイッチにアクセスする必要があります。 （アクティブ クラスタ コマンド スイッチの IP アドレスがクラスタ スタンバイ グループの仮想 IP アドレスと異なる場合）。

アクティブ クラスタ コマンド スイッチに障害が発生すると、スタンバイ クラスタ コマンド スイッチが仮想 IP アドレスを使用して、アクティブ クラスタ コマンド スイッチになります。 クラスタ スタンバイ グループのパッシブ スイッチは、それぞれ割り当てられたプライオリティを比較し、新しいスタンバイ クラスタ コマンド スイッチを選出します。 その後、プライオリティの一番高いパッシブ スタンバイ スイッチがスタンバイ クラスタ コマンド スイッチになります。 前回アクティブ クラスタ コマンド スイッチだったスイッチが再びアクティブになると、アクティブ クラスタ コマンド スイッチの役割を再開します。そのため、現在アクティブ クラスタ コマンド スイッチを担当しているスイッチは再びスタンバイ クラスタ コマンド スイッチになります。 スイッチ クラスタの IP アドレスの詳細については、「IP アドレス」の項を参照してください。

クラスタ スタンバイ グループに関する他の考慮事項

次の要件も満たす必要があります。

- スタンバイ クラスタ コマンド スイッチは、クラスタ コマンド スイッチと同タイプのスイッチでなければなりません。 たとえば、クラスタ コマンド スイッチが Catalyst 3750-E または Catalyst 3750-X スイッチの場合、スタンバイ クラスタ コマンド スイッチも Catalyst 3750-E か Catalyst 3750-X スイッチにする必要があります。 スタンバイ クラスタ コマンド スイッチの要件については、他のクラスタ対応スイッチのコンフィギュレーション ガイドを参照してください。

  スイッチ クラスタに Catalyst 3750-X スイッチまたはスイッチ スタックが含まれている場合、それをクラスタ コマンド スイッチにする必要があります。 含まれていない場合、クラスタ

にCatalyst 3750-Eスイッチまたはスイッチ スタックがあれば、そのスイッチをクラスタ コマンド スイッチにします。

- クラスタごとに、1つのクラスタ スタンバイ グループのみ割り当てることができます。ルータ冗長スタンバイ グループは複数作成できます。

  1 つの HSRP グループをクラスタ スタンバイ グループとルータ冗長構成グループの両方にすることができます。ただし、ルータ冗長構成グループがクラスタ スタンバイ グループになった場合、そのグループ上でのルータ冗長構成はディセーブルになります。CLI を使用すれば、冗長構成を再びイネーブルにすることができます。

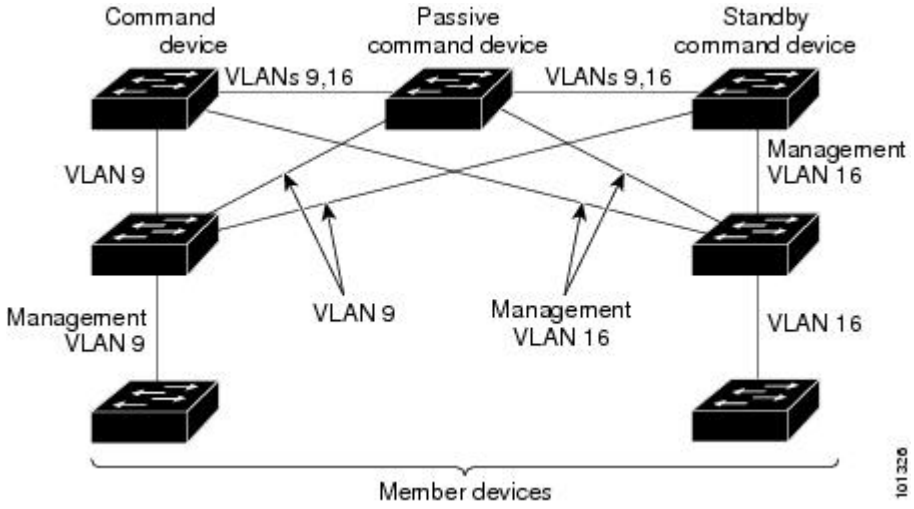
- すべてのスタンバイグループ メンバはそのクラスタのメンバである必要があります。

（注） スタンバイ クラスタ コマンド スイッチとして割り当てることができるスイッチ数に制限はありません。ただし、クラスタのスイッチの総数（アクティブ クラスタ コマンド スイッチ、スタンバイ グループ メンバ、およびクラスタ メンバ スイッチを含む）は 16 以内にする必要があります。

- 各スタンバイグループのメンバ（下の図を参照）は、同じ VLAN を介してクラスタ コマンド スイッチに接続されている必要があります。この例では、クラスタ コマンド スイッチとスタンバイ クラスタ コマンド スイッチが Catalyst 3560-E、Catalyst 3750-E、Catalyst 3560-X、または Catalyst 3750-X クラスタ コマンド スイッチです。各スタンバイグループのメンバも、スイッチ クラスタと同じ VLAN を最低 1 つは介在させて、冗長性を持たせながら相互接続する必要があります。

  Catalyst 1900、Catalyst 2820、Catalyst 2900 XL、Catalyst 2950、Catalyst 3500 XL クラスタ メンバ スイッチは、それぞれの管理 VLAN を介してクラスタ スタンバイ グループに接続する必要があります。

図 *126*：スタンバイグループ メンバとクラスタ メンバ間の *VLAN* 接続



クラスタ設定の自動回復

アクティブ クラスタ コマンド スイッチは、クラスタ設定情報をスタンバイ クラスタ コマンド スイッチに継続的に送信します（デバイス設定情報は送信しません）。 アクティブ クラスタ コマンドスイッチに障害が発生した場合は、この情報をもとに、スタンバイクラスタコマンドスイッチが即座にクラスタを引き継ぎます。

自動検出には次のような制限があります。

- この制限は、Catalyst 2950、Catalyst 2960、Catalyst 2970、Catalyst 3550、Catalyst 3560、Catalyst 3560-E、Catalyst 3560-X、Catalyst 3750、Catalyst 3750-E、および Catalyst 3750-X コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチを備えたクラスタだけに該当します。 アクティブ クラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチが同時にディセーブルになった場合、パッシブクラスタコマンドスイッチの中でプライオリティが一番高いものがアクティブ クラスタ コマンド スイッチになります。 ただし、パッシブ スタンバイ クラスタ コマンド スイッチだったため、以前のクラスタ コマンド スイッチはクラスタ設定情報を送信していません。 アクティブ クラスタ コマンド スイッチは、スタンバイ クラスタ コマンド スイッチにクラスタ設定情報のみ送信します。 そのため、クラスタを再設定する必要があります。
- クラスタ スタンバイ グループに複数のスイッチを持つアクティブ クラスタ コマンド スイッチに障害が発生した場合、新しいクラスタ コマンド スイッチは、いかなる Catalyst 1900、Catalyst 2820、および Catalyst 2916M XL のクラスタ メンバ スイッチも検出しません。 これらのクラスタ メンバ スイッチをクラスタにもう一度追加する必要があります。
- アクティブ クラスタ コマンド スイッチに障害が発生してダウンした後、再びアクティブになった場合、そのスイッチはいかなる Catalyst 1900、Catalyst 2820、および Catalyst 2916M XL クラスタ メンバ スイッチも検出しません。 これらのクラスタ メンバ スイッチをクラスタにもう一度追加する必要があります。

以前アクティブ クラスタ コマンド スイッチだったスイッチが再びアクティブになった場合、そのスイッチは最新のクラスタ設定のコピー（ダウン中に追加されたメンバを含む）をアクティブ クラスタ コマンド スイッチから受信します。 アクティブ クラスタ コマンド スイッチは、クラスタ スタンバイ グループにクラスタ設定のコピーを送信します。

IP Addresses

IP 情報をクラスタ コマンド スイッチに割り当てる必要があります。 クラスタ コマンド スイッチには複数の IP アドレスを割り当てることができます。クラスタには、これらのコマンドスイッチの IP アドレスを介してアクセスできます。 クラスタ スタンバイ グループを設定する場合、アクティブ クラスタ コマンド スイッチからスタンバイグループの仮想 IP アドレスを使用して、クラスタを管理する必要があります。 仮想 IP アドレスを使用すると、アクティブ クラスタ コマンド スイッチに障害が発生してスタンバイ クラスタ コマンド スイッチがアクティブ クラスタ コマンド スイッチになった場合でも、クラスタへの接続を確保できます。

アクティブ クラスタ コマンド スイッチに障害が発生してスタンバイ クラスタ コマンド スイッチがその役割を引き継いだ場合、クラスタのアクセスには、スタンバイグループの仮想 IP アドレスも、新しいアクティブ クラスタ コマンド スイッチで使える IP アドレスも使用できます。

必須ではありませんが、IP アドレスはクラスタ対応のスイッチにも割り当てることができます。クラスタ メンバ スイッチは、コマンドスイッチの IP アドレスを使用して管理され、他のクラスタ メンバ スイッチと通信します。 IP アドレスが割り当てられていないクラスタ メンバ スイッチがそのクラスタを離れる場合、スタンドアロンスイッチとして管理するIPアドレスを割り当てる必要があります。

ホスト名

クラスタ コマンド スイッチと対象のクラスタ メンバにはホスト名を割り当てる必要はありません。 ただし、クラスタ コマンド スイッチに割り当てられたホスト名は、スイッチ クラスタを識別するのに役立ちます。 スイッチのデフォルトのホスト名は *Switch* です。

クラスタに加入するスイッチにホスト名がない場合、クラスタコマンドスイッチは一意のメンバ番号を自身のホスト名に追加し、そのスイッチに割り当てます。この処理はクラスタに加入するスイッチごとに順番に行われます。 ここでいう番号とは、スイッチがクラスタに追加された順番を指します。 たとえば、*eng-cluster* という名前のクラスタ コマンド スイッチでは、5 番目のクラスタ メンバとして *eng-cluster-5* という名前が割り当てられます。

スイッチにホスト名がある場合、クラスタへの加入時もクラスタからの脱退時もその名前が使用されます。

クラスタ脱退時、または新しいクラスタへの加入時にそのメンバ番号（*5* など）を確保するため、クラスタ コマンド スイッチからスイッチにホスト名を送信した場合、それを受信したスイッチは、新しいクラスタのクラスタ コマンド スイッチのホスト名（*mkg-cluster-5* など）で古いホスト名（*eng-cluster-5* など）を上書きします。 新しいクラスタではスイッチのメンバ番号を変更する場合（*3* など）、スイッチは前回の名前（*eng-cluster-5*）を確保します。

パスワード

クラスタのメンバになるスイッチにはパスワードを割り当てる必要はありません。 スイッチはコマンドスイッチのパスワードを継承してクラスタに加入し、脱退するときもその情報を保有したまま離れます。 コマンドスイッチのパスワードが設定されていない場合、クラスタ メンバ スイッチはヌル パスワードを代わりに継承します。 クラスタ メンバ スイッチが継承するのはコマンドスイッチのパスワードのみです。

コマンドスイッチのパスワードと異なるメンバスイッチのパスワードを指定してその設定を保存してしまうと、クラスタコマンドスイッチからそのスイッチを管理できなくなります。この状態はメンバスイッチのパスワードをコマンドスイッチのパスワードに戻すまで続きます。 メンバスイッチを再起動しても、パスワードは元のコマンドスイッチパスワードには戻りません。 スイッチをクラスタに加入させた後は、メンバスイッチ パスワードを変更しないことを推奨します。

Catalyst 1900 および Catalyst 2820 スイッチ固有のパスワードの考慮事項については、これらのスイッチのインストレーションおよびコンフィギュレーション ガイドを参照してください。

SNMP コミュニティ ストリング

クラスタ メンバ スイッチは、次のように *@esN* をコミュニティ ストリングの後ろに追加してコマンドスイッチの Read-Only（RO）と Read-Write（RW）のコミュニティ ストリングを継承します。

- *command-switch-readonly-community-string@esN*（N はメンバスイッチ番号）
- *command-switch-readwrite-community-string@esN*（N はメンバスイッチ番号）

クラスタ コマンド スイッチに複数の Read-Only または Read-Write コミュニティ ストリングがある場合、クラスタ メンバ スイッチには最初の Read-Only または Read-Write ストリングのみ伝播されます。

スイッチのコミュニティ ストリング数とその長さには制限がありません。

Catalyst 1900 および Catalyst 2820 スイッチ固有の SNMP の考慮事項については、これらのスイッチのインストレーション コンフィギュレーション ガイドを参照してください。

TACACS+ および RADIUS

Terminal Access Controller Access Control System Plus（TACACS+）をクラスタ メンバに設定する場合、すべてのクラスタ メンバに設定する必要があります。 同様に、RADIUS をクラスタ メンバに設定する場合、すべてのクラスタ メンバに設定する必要があります。 また、TACACS+ を設定したメンバと RADIUS を設定した他のメンバを同じスイッチ クラスタには追加できません。

LRE プロファイル

スイッチ クラスタに、個人のプロファイルと公開プロファイルの両方を使用した Long-Reach Ethernet（LRE）スイッチがある場合、設定の競合が発生します。 クラスタの 1 つの LRE スイッチに公開プロファイルが割り当てられている場合、クラスタ内のすべての LRE スイッチにも同じプロファイルを割り当てる必要があります。 LRE スイッチをクラスタに追加する前に、クラスタ内の他の LRE スイッチが同じ公開プロファイルを使用しているかどうかを確認してください。

クラスタ内に異なる個人プロファイルを使用している LRE スイッチを混在させることはできます。

CLI を使用したスイッチ クラスタの管理

クラスタ コマンド スイッチにログインすることにより、CLI からクラスタ メンバ スイッチを設定できます。 **rcommand** ユーザ EXEC コマンドおよびクラスタ メンバ スイッチ番号を入力して、（コンソールまたは Telnet 接続を経由して）Telnet セッションを開始し、クラスタ メンバ スイッチの CLI にアクセスします。 コマンド モードが変更され、通常どおりに Cisco IOS コマンドを使用できるようになります。 クラスタ メンバ スイッチで **exit** 特権 EXEC コマンドを入力すると、コマンド スイッチの CLI に戻ります。

次に、コマンド スイッチの CLI からメンバ スイッチ 3 にログインする例を示します。

```
switch# rcommand 3
```

メンバ スイッチ番号が不明の場合は、クラスタ コマンド スイッチで **show cluster members** 特権 EXEC コマンドを入力します。 **rcommand** コマンドおよび他のすべてのクラスタ コマンドの詳細については、スイッチ コマンド リファレンスを参照してください。

Telnet セッションは、クラスタ コマンド スイッチと同じ権限レベルでメンバ スイッチの CLI にアクセスします。 その後、Cisco IOS コマンドを通常どおりに使用できます。

（注） CLI により、最大 16 までのスイッチ クラスタの作成と管理がサポートされます。

Catalyst 1900 および Catalyst 2820 の CLI に関する考慮事項

スイッチ クラスタに Standard Edition ソフトウェアが稼働している Catalyst 1900 および Catalyst 2820 スイッチがある場合、クラスタ コマンド スイッチの権限レベルが 15 であれば、Telnet セッションは管理コンソール（メニュー方式インターフェイス）にアクセスします。クラスタ コマンド スイッチの権限レベルが 1 ～ 14 であれば、パスワードの入力を要求するプロンプトが表示され、入力後にメニュー コンソールにアクセスできます。

コマンド スイッチの権限レベルと、Catalyst 1900 および Catalyst 2820 クラスタ メンバ スイッチ（Standard および Enterprise Edition ソフトウェアが稼働）との対応関係は、次のとおりです。

- コマンド スイッチの権限レベルが 1 ～ 14 の場合、クラスタ メンバ スイッチへのアクセスは権限レベル 1 で行われます。
- コマンド スイッチの権限レベルが 15 の場合、クラスタ メンバ スイッチへのアクセスは権限レベル 15 で行われます。

（注） Catalyst 1900 および Catalyst 2820 の CLI は、Enterprise Edition ソフトウェアが稼働しているスイッチに限って使用できます。

Catalyst 1900 および Catalyst 2820 スイッチの詳細については、これらのスイッチのインストレーション コンフィギュレーション ガイドを参照してください。

SNMP を使用したスイッチ クラスタの管理

スイッチの最初の起動時にセットアッププログラムを使用して IP 情報を入力し、提示されたコンフィギュレーションを採用した場合、SNMP はイネーブルに設定されています。 セットアッププログラムを使用して IP 情報を入力していない場合は、SNMP はイネーブルではありません。その場合は、「SNMP の設定」の説明に従って、SNMP をイネーブルに設定します。 Catalyst 1900 および Catalyst 2820 スイッチでは、SNMP はデフォルトでイネーブルに設定されています。

クラスタを作成すると、クラスタ コマンド スイッチがクラスタ メンバ スイッチと SNMP アプリケーション間のメッセージ交換を管理します。 クラスタ コマンド スイッチ上のクラスタ ソフトウェアは、クラスタ コマンド スイッチ上で最初に設定された Read-Write および Read-Only コミュニティ ストリングにクラスタ メンバ スイッチ番号（*@esN*、N はスイッチ番号）を追加し、これ

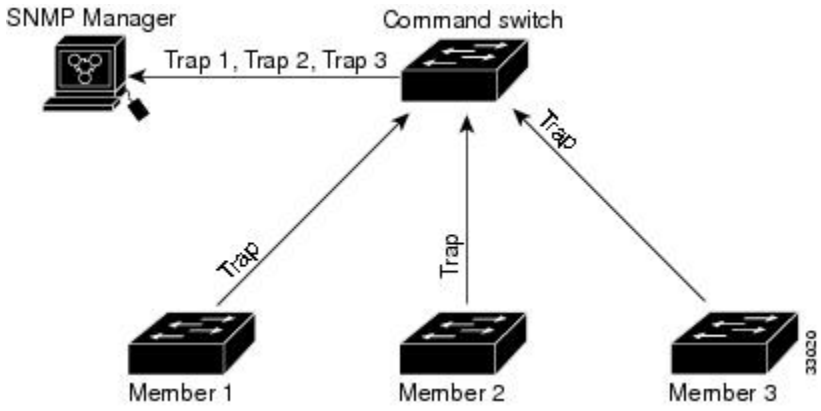
らのストリングをクラスタ メンバ スイッチに送信します。 クラスタ コマンド スイッチは、このコミュニティ ストリングを使用して、SNMP管理ステーションとクラスタ メンバスイッチ間で、get、set、および get-next メッセージの転送を制御します。

（注） クラスタ スタンバイ グループを設定すると、ユーザが気付かないうちにクラスタ コマンド スイッチが変更される場合があります。 クラスタにクラスタ スタンバイ グループを設定している場合は、クラスタ コマンド スイッチとの通信には、最初に設定された Read-Write および Read-Only コミュニティ ストリングを使用してください。

クラスタ メンバ スイッチに IP アドレスが割り当てられていない場合、図に示すように、クラスタ コマンド スイッチはクラスタ メンバ スイッチからのトラップを管理ステーションにリダイレクトします。 クラスタ メンバ スイッチに専用の IP アドレスおよびコミュニティ ストリングが割り当てられている場合、そのクラスタ メンバスイッチはクラスタ コマンドスイッチを経由せず、管理ステーションに直接トラップを送信できます。

クラスタ メンバ スイッチに専用の IP アドレスとコミュニティ ストリングが割り当てられている場合、クラスタ コマンド スイッチによるアクセスの他に、その IP アドレスとコミュニティ ストリングも使用できます。

図 *127* : ***SNMP*** によるクラスタ管理



第 69 章

SDM テンプレートの設定

- 機能情報の確認，1877 ページ
- SDM テンプレートの設定に関する情報，1877 ページ
- SDM テンプレートの設定方法，1880 ページ
- SDM テンプレートの設定例，1881 ページ

機能情報の確認

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

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

SDM テンプレートの設定に関する情報

SDM テンプレートの制約事項

次に、SDM テンプレートを使用している場合の制約事項を示します。

- デフォルト テンプレートは、サポートされる唯一のテンプレートです。

SDM テンプレート

Switch Database Management（SDM）テンプレートを使用してシステム リソースを設定し、特定の機能に対するサポートをネットワーク内でのデバイスの使用方法に応じて最適化することができます。

Ternary CAM（TCAM）リソースをさまざまな用途に割り当てるために、スイッチ SDM テンプレートはシステム リソースにプライオリティを設定して、特定の機能のサポートを最適化します。 デバイスでサポートされているテンプレートは次のとおりです。

- デフォルト：デフォルトテンプレートは、すべての機能に均等にリソースを割り当てます。

Catalyst 2960-CX のデフォルト テンプレート

Catalyst 2960-CX スイッチのテンプレートには LAN Base ライセンスが適用されます。

表 *164*：テンプレートで許容される機能リソースの概算

リソース	デフォルト
ユニキャスト MAC アドレス	16 K
アクティブ VLAN/VLAN ID	255/4096
NetFlow エントリ	16 K
スタックあたりの EtherChannel グループ数	6
IPv4 IGMP または IPv6 グループ	1K IPv4 1K IPv6
直接ルート	2K IPv4 2K IPv6
間接ルート	1K IPv4 1K IPv6 （16 スタティック ルートのみ）
IPv4 または IPv6 ポリシーベース ルーティング ACE	0（IPv4 PBR） 0（IPv6 PBR）
IPv4 または IPv6 MAC QoS ACE	0.375K（IPv4 QoS） 0.25K（IPv6 QoS）

リソース	デフォルト
IPv4 または IPv6 ポートあるいは MAC Security ACE	0.375K（IPv4 ACL） 0.375K（IPv6 ACL）

関連トピック

例：SDM テンプレートの表示,（1881 ページ）

Catalyst 3560-CX のデフォルト テンプレート

Catalyst 3560-CX スイッチのテンプレートには IP Base および IP Services のライセンスが適用されます。

表 *165*：テンプレートで許容される機能リソースの概算

Resource	デフォルト
ユニキャスト MAC アドレス	16 K
アクティブ VLAN/VLAN ID	1K/4096
スタックあたりの EtherChannel グループ数	6
IPv4 IGMP または IPv6 グループ	1K IPv4 1K IPv6
直接ルート	4K IPv4 4K IPv6
間接ルート	1K IPv4 1K IPv6
IPv4 または IPv6 ポリシーベース ルーティング ACE	0.25K（IPv4 PBR） 0.25K（IPv6 PBR）
IPv4 または IPv6 QoS ACE	0.375K（IPv4 QoS） 0.25K（IPv6 QoS）
IPv4 または IPv6 ポートあるいは MAC Security ACE	0.375K（IPv4 ACL） 0.375K（IPv6 ACL）

関連トピック

SDM テンプレートの設定, （1880 ページ）

SDM テンプレートの設定方法

SDM テンプレートの設定

SDM テンプレートを使用して機能動作を最適にサポートするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **sdm prefer** {**default** }
4. **end**
5. **reload**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**sdm prefer** {**default** } 例： `Switch(config)# sdm prefer lanbase-routing`	スイッチで使用する SDM テンプレートを指定します。 キーワードの意味は次のとおりです。 • **default**：デフォルトテンプレートでは、レイヤ 2、IPv4、IPv6 のすべての機能のバランスを取ることができます。 • **lanbase-default**：LAN Base のデフォルトテンプレートは IPv4 と IPv6 の両方のスタティック ルーティング機能を提供します。

	コマンドまたはアクション	目的
		スイッチをデフォルトテンプレートに設定するには、**no sdm prefer** コマンドを使用します。デフォルト テンプレートはシステム リソースを均等に割り当てます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**reload** 例： `Switch# reload`	オペレーティング システムをリロードします。

SDM テンプレートの設定例

例：SDM テンプレートの表示

次に、デフォルトのテンプレート情報を表示した出力例を示します。

これは、Catalyst 3560-CX スイッチのデフォルト テンプレート情報を表示した出力例です。

```
Switch# show sdm prefer

The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  16K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    5K
  number of directly-connected IPv4 hosts:          4K
  number of indirect IPv4 routes:                   1K
  number of IPv6 multicast groups:                  1K
  number of IPv6 unicast routes:                    5K
  number of directly-connected IPv6 addresses:      4K
  number of indirect IPv6 unicast routes:           1K
  number of IPv4 policy based routing aces:         0.25K
  number of IPv4/MAC qos aces:                      0.375k
  number of IPv4/MAC security aces:                 0.375k
  number of IPv6 policy based routing aces:         0.25K
  number of IPv6 qos aces:                          0.25K
  number of IPv6 security aces:                     0.375k
```

これは、Catalyst 2960-CX スイッチのデフォルト テンプレート情報を表示した出力例です。

```
Switch# show sdm prefer

The current template is "default" template.
 The selected template optimizes the resources in
```

```
 the switch to support this level of features for
 0 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                  16K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    3K
  number of directly-connected IPv4 hosts:          2K
  number of indirect IPv4 routes:                   1K
  number of IPv6 multicast groups:                  1K
  number of IPv6 unicast routes:                    3K
  number of directly-connected IPv6 addresses:      2K
  number of indirect IPv6 unicast routes:           1K
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.375k
  number of IPv4/MAC security aces:                 0.375k
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0.25K
  number of IPv6 security aces:                     0.375k
```

例：SDM テンプレートの設定

次に、VLAN テンプレートの設定方法の例を示します。

```
Switch(config)# sdm prefer lanbase-routing
Switch(config)# exit
Switch# reload
  Proceed with reload? [confirm]
```

第 70 章

システム メッセージ ログの設定

- システム メッセージ ログの設定に関する情報，1883 ページ
- システム メッセージ ログの設定方法，1886 ページ
- システム メッセージ ログのモニタリングおよびメンテナンス，1896 ページ
- システム メッセージ ログの設定例，1897 ページ

システム メッセージ ログの設定に関する情報

システム メッセージ ロギング

スイッチはデフォルトで、システム メッセージおよび **debug** 特権 EXEC コマンドの出力をロギング プロセスに送信します。 スタック メンバーはシステム メッセージをトリガーできます。 システム メッセージを生成するスタック メンバは、ホスト名を hostname-n の形式で付加し（n は 1 ～ 9 のスイッチ 1 ～ 8 の範囲）、出力をアクティブ スイッチのロギング プロセスにリダイレクトします。 アクティブ スイッチはスタック メンバですが、そのホスト名はシステム メッセージの末尾に追加されません。 ロギング プロセスはログ メッセージを各宛先（設定に応じて、ログ バッファ、端末回線、UNIX Syslog サーバなど）に配信する処理を制御します。 ロギング プロセスは、コンソールにもメッセージを送信します。

ロギング プロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。 メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。 メッセージがアクティブなコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。 ログ メッセージにタイム スタンプを設定したり、Syslog 送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。 表示されるメッセージについては、このリリースに対応するシステム メッセージ ガイドを参照してください。

ロギングされたシステム メッセージにアクセスするには、スイッチのコマンドライン インターフェイス（CLI）を使用するか、または適切に設定された Syslog サーバにこれらのシステム メッ

セージを保存します。 スイッチ ソフトウェアは、Syslog メッセージをスタンドアロン スイッチ上の内部バッファに保存します。スイッチスタックの場合は、アクティブスイッチ上に保存します。 スタンドアロン スイッチまたはスタック マスターに障害が発生すると、ログをフラッシュメモリに保存していなかった場合、ログは失われます。

システム メッセージをリモートで監視するには、Syslog サーバ上でログを表示するか、あるいは Telnet、コンソール ポート、またはイーサネット管理ポート経由でスイッチにアクセスします。スイッチ スタックでは、すべてのスタック メンバ コンソールにより、同じコンソール出力が用意されます。

（注） Syslog フォーマットは 4.3 Berkeley Standard Distribution（BSD）UNIX と互換性があります。

システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字とパーセント記号（%）、およびその前に配置されるオプションのシーケンス番号やタイム スタンプ情報（設定されている場合）で構成されています。スイッチに応じて、メッセージは次のいずれかの形式で表示されます。

- *seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)*
- *seq no:timestamp: %facility-severity-MNEMONIC:description*

パーセント記号の前にあるメッセージの部分は、次のグローバル コンフィギュレーション コマンドの設定によって異なります。

- **service sequence-numbers**
- **service timestamps log datetime**
- **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]
- **service timestamps log uptime**

表 *166* : システム ログ メッセージの要素

要素	説明
seq no:	**service sequence-numbers** グローバル コンフィギュレーション コマンドが設定されている場合だけ、ログ メッセージにシーケンス番号をスタンプします。

要素	説明
timestamp のフォーマット： *mm/dd hh:mm:ss* または *hh:mm:ss*（短時間） または *d h*（長時間）	メッセージまたはイベントの日時です。 **service timestamps log** [**datetime** | **log**] グローバル コンフィギュレーション コマンドが設定されている場合だけ、この情報が表示されます。
facility	メッセージが参照する機能（SNMP、SYS など）です。
severity	メッセージの重大度を示す 0 ～ 7 の 1 桁のコードです。
MNEMONIC	メッセージを一意に示すテキスト ストリングです。
description	レポートされているイベントの詳細を示すテキスト ストリングです。
hostname-n	スタック メンバーのホスト名およびスタック内のスイッチ番号。アクティブ スイッチはスタック メンバですが、そのホスト名はシステム メッセージの末尾に追加されません。

デフォルトのシステム メッセージ ロギングの設定

表 *167* : デフォルトのシステム メッセージ ロギングの設定

機能	デフォルト設定
コンソールへのシステム メッセージ ロギング	イネーブル
コンソールの重大度	デバッグ
ログ ファイル設定	ファイル名の指定なし
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1 メッセージ
タイム スタンプ	ディセーブル

機能	デフォルト設定
同期ロギング	ディセーブル
ロギング サーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
サーバ機能	local7
サーバの重大度	Informational

syslog メッセージの制限

snmp-server enable trap グローバル コンフィギュレーション コマンドを使用して、SNMP ネットワーク管理ステーション（NMS）に送信されるようにSyslogメッセージ トラップがイネーブルに設定されている場合は、スイッチの履歴テーブルに送信および格納されるメッセージの重大度を変更できます。 また、履歴テーブルに格納されるメッセージの数を変更することもできます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。 デフォルトでは、Syslog トラップがイネーブルでない場合も、レベルが **warning** であるメッセージや数値的に下位レベルのメッセージの 1 つが履歴テーブルに格納されます。

履歴テーブルがいっぱいの場合（**logging history size** グローバル コンフィギュレーション コマンドで指定した最大メッセージエントリ数が格納されている場合）は、新しいメッセージエントリを格納できるように、最も古いエントリがテーブルから削除されます。

履歴テーブルは、level キーワードおよび重大度を示します。 SNMP を使用している場合は、重大度の値が 1 だけ増えます。 たとえば、*emergencies* は 0 ではなく 1 に、*critical* は 2 ではなく 3 になります。

システム メッセージ ログの設定方法

メッセージ表示宛先デバイスの設定

メッセージ ロギングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **logging buffered** [*size*]
3. **logging***host*
4. **logging file flash:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]
5. **end**
6. **terminalmonitor**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging buffered** [*size*] 例： `Switch(config)# logging buffered 8192`	スイッチまたはスタンドアロン スイッチ（スイッチ スタックの場合はアクティブ スイッチ）の内部バッファにメッセージをロギングします。 指定できる範囲は 4096 ～ 2147483647 バイトです。 デフォルトのバッファ サイズは 4096 バイトです。 スタンドアロン スイッチまたはアクティブ スイッチに障害が発生すると、フラッシュ メモリに保存されていないログは失われます。 ステップ 4 を参照してください。 （注） バッファ サイズを大きすぎる値に設定しないでください。他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサ メモリを表示するには、**show memory** 特権 EXEC コマンドを使用します。 ただし、表示される値は使用できる最大値であるため、バッファ サイズをこの値に設定しないでください。
ステップ 3	**logging***host* 例： `Switch(config)# logging 125.1.1.100`	UNIX Syslog サーバ ホストにメッセージを保存します。 *host* には、syslog サーバとして使用するホストの名前または IP アドレスを指定します。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。

	コマンドまたはアクション	目的
ステップ 4	**logging file flash:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*] 例： `Switch(config)# logging file flash:log_msg.txt 40960 4096 3`	スタンドアロン スイッチ上か、または、スイッチ スタックの場合はアクティブ スイッチ上で、フラッシュ メモリにあるファイルにログ メッセージを保存します。 • *filename*：ログ メッセージのファイル名を入力します。 • （任意）**max-file-size** ：ログ ファイルの最大サイズを指定します。 指定できる範囲は 4096 ～ 2147483647 です。 デフォルトは 4096 バイトです。 • （任意）*min-file-size*：ログ ファイルの最小サイズを指定します。 指定できる範囲は 1024 ～ 2147483647 です。 デフォルトは 2048 バイトです。 • （任意）*severity-level-number* | *type*：ロギングの重大度またはロギング タイプを指定します。 重大度に指定できる範囲は 0 ～ 7 です。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**terminalmonitor** 例： `Switch# terminal monitor`	現在のセッション間、非コンソール端末にメッセージを保存します。 端末パラメータ コンフィギュレーション コマンドはローカルに設定され、セッションの終了後は無効になります。 デバッグ メッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。

ログ メッセージの同期化

特定のコンソール ポート回線または仮想端末回線に対して、非送信請求メッセージおよび **debug** 特権 EXEC コマンドの出力を送信請求デバイスの出力およびプロンプトと同期させることができます。 重大度に応じて非同期に出力されるメッセージのタイプを特定できます。 また、端末の非同期メッセージが削除されるまで保存しておくバッファの最大数を設定することもできます。

非送信請求メッセージおよび **debug** コマンド出力の同期ロギングがイネーブルの場合、送信請求デバイス出力がコンソールに表示または印刷された後に、非送信請求デバイスからの出力が表示または印刷されます。 非送信請求メッセージおよび **debug** コマンドの出力は、ユーザ入力用プロンプトが返された後に、コンソールに表示されます。 したがって、非送信請求メッセージおよび **debug** コマンドの出力は、送信請求デバイス出力およびプロンプトに割り込まれることはありません。 非送信請求メッセージが表示された後に、コンソールはユーザ プロンプトを再表示します。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **line** [**console** | **vty**] *line-number* [*ending-line-number*]
3. **logging synchronous** [**level** [*severity-level* | **all**] | **limit***number-of-buffers*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console** | **vty**] *line-number* [*ending-line-number*] 例： `Switch(config)# line console`	メッセージの同期ロギングに設定する回線を指定します。 • **console**：スイッチ コンソール ポートまたはイーサネット管理ポートでの設定を指定します。 • **line vty***line-number*：どの vty 行の同期ロギングをイネーブルにするかを指定します。 Telnet セッションを介して行われる設定には、vty 接続を使用します。 回線番号に指定できる範囲は 0 ～ 15 です。 16 個の vty 回線の設定をすべて一度に変更するには、次のように入力します。 line vty 0 15 また、現在の接続に使用されている 1 つの vty 回線の設定を変更することもできます。 たとえば、vty 回線 2 の設定を変更するには、次のように入力します。 line vty 2 このコマンドを入力すると、ライン コンフィギュレーション モードになります。
ステップ 3	**logging synchronous** [**level** [*severity-level* | **all**] | **limit***number-of-buffers*] 例： `Switch(config)# logging synchronous level 3 limit 1000`	メッセージの同期ロギングをイネーブルにします。 • （任意）**level***severity-level*：メッセージの重大度を指定します。 重大度がこの値以上であるメッセージは、非同期に出力されます。 値が小さいほど重大度は大きく、値が大きいほど重大度は小さくなります。 デフォルトは 2 です。 • （任意）**level all**：重大度に関係なく、すべてのメッセージが非同期に出力されます。

	コマンドまたはアクション	目的
		• （任意）**limit***number-of-buffers*：キューイングされる端末のバッファ数を指定します。これを超える新しいメッセージは廃棄されます。指定できる範囲は 0 ～ 2147483647 です。 デフォルトは 20 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

メッセージ ロギングのディセーブル化

メッセージロギングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージ ロギングをイネーブルにする必要があります。 メッセージ ロギングがイネーブルの場合、ログ メッセージはロギング プロセスに送信されます。ロギング プロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

ロギング プロセスをディセーブルにすると、メッセージがコンソールに書き込まれるまでプロセスは処理続行を待機する必要があるため、スイッチの処理速度が低下することがあります。 ロギング プロセスがディセーブルの場合、メッセージは生成後すぐに（通常はコマンド出力に割り込む形で）コンソールに表示されます。

logging synchronous グローバル コンフィギュレーション コマンドも、コンソールへのメッセージ表示に影響します。 このコマンドをイネーブルにすると、Return を押さなければメッセージが表示されません。

メッセージ ロギングをディセーブルにした後に再びイネーブルにするには、**logging on** グローバル コンフィギュレーション コマンドを使用します。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **no logging console**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no logging console** 例： `Switch(config)# no logging console`	メッセージ ロギングをディセーブルにします。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化

デフォルトでは、ログ メッセージにはタイム スタンプが適用されません。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを使用します。
   - **servicetimestampsloguptime**
   - **service timestamps log datetime**[**msec** | **localtime** | **show-timezone**]
3. **end**

手順の詳細

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

ステップ 2	次のいずれかのコマンドを使用します。
	• **servicetimestampsloguptime**
	• **service timestamps log datetime**[**msec** | **localtime** | **show-timezone**]
	
	例：
	`Switch(config)# service timestamps log uptime`
	または
	`Switch(config)# service timestamps log datetime`
		ログのタイムスタンプをイネーブルにします。
		• **log uptime**：ログ メッセージのタイムスタンプをイネーブルにして、システムの再起動以降の経過時間を表示します。
		• **log datetime**：ログ メッセージのタイムスタンプをイネーブルにします。 選択したオプションに応じて、ローカルタイムゾーンを基準とした日付、時間（ミリ秒）、タイムゾーン名をタイムスタンプとして表示できます。

ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

タイムスタンプが同じログ メッセージが複数ある場合、これらのメッセージを表示するには、シーケンス番号を使用してメッセージを表示できます。デフォルトでは、ログメッセージにシーケンス番号は表示されません。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **service sequence-numbers**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service sequence-numbers** 例： `Switch(config)# service sequence-numbers`	シーケンス番号をイネーブルにします。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

メッセージ重大度の定義

メッセージの重大度を指定して、選択したデバイスに表示されるメッセージを制限します。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **logging console***level*
3. **logging monitor***level*
4. **logging trap***level*
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**logging console***level* 例： `Switch(config)# logging console 3`	コンソールに保存するメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 3	**logging monitor***level* 例： `Switch(config)# logging monitor 3`	端末回線に出力するメッセージを制限します。 デフォルトで、端末はデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 4	**logging trap***level* 例： `Switch(config)# logging trap 3`	Syslog サーバに保存するメッセージを制限します。 デフォルトで、Syslog サーバは通知メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

履歴テーブルおよび SNMP に送信される syslog メッセージの制限

このタスクでは、履歴テーブルおよび SNMP に送信される syslog メッセージを制限する方法について説明します。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **logging history***level*
3. **logging history size***number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging history***level* 例： `Switch(config)# logging history 3`	履歴ファイルに保存され、SNMP サーバに送信される syslog メッセージのデフォルト レベルを変更します。 デフォルトでは、**warnings**、**errors**、**critical**、**alerts**、および **emergencies** のメッセージが送信されます。
ステップ 3	**logging history size***number* 例： `Switch(config)# logging history size 200`	履歴テーブルに保存できる Syslog メッセージの数を指定します。 デフォルトでは 1 つのメッセージが格納されます。 指定できる範囲は 0 ～ 500 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

UNIX Syslog デーモンへのメッセージのロギング

このタスクはオプションです。

（注） 最新バージョンの UNIX Syslog デーモンの中には、デフォルトでネットワークからの Syslog パケットを受け入れないものがあります。 このようなシステムの場合に、Syslog メッセージのリモート ロギングをイネーブルにするには、Syslog コマンド ラインに追加または削除する必要があるオプションを、UNIX の **man syslogd** コマンドを使用して判別します。

はじめる前に

- root でログインします。
- システム ログ メッセージを UNIX Syslog サーバに送信する前に、UNIX サーバ上で Syslog デーモンを設定する必要があります。

手順の概要

1. /etc/syslog.conf ファイルに次の行を追加します。
2. UNIX シェル プロンプトに次のコマンドを入力します。
3. Syslog デーモンに新しい設定を認識させます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	/etc/syslog.conf ファイルに次の行を追加します。 例： **local7.debug /usr/adm/logs/***cisco.log*	• **local7**：ロギング機能を指定します。 • **debug**：syslog レベルを指定します。 このファイルは、syslog デーモンに書き込み権限がある既存ファイルである必要があります。
ステップ 2	UNIX シェル プロンプトに次のコマンドを入力します。 例： $ **touch /var/log/***cisco.log* $ **chmod 666 /var/log/***cisco.log*	ログ ファイルを作成します。 syslog デーモンは、このレベルまたはこのファイルのより高い重大度レベルでメッセージを送信します。
ステップ 3	Syslogデーモンに新しい設定を認識させます。 例： $ **kill -HUP `cat /etc/syslog.pid`**	詳細については、ご使用の UNIX システムの **man syslog.conf** および **man syslogd** コマンドを参照してください。

システム メッセージ ログのモニタリングおよびメンテナンス

コンフィギュレーション アーカイブ ログのモニタリング

コマンド	目的
show archive log config {**all** | **number** [*end-number*] | **user***username* [**session***number*] *number* [*end-number*] | **statistics**} [**provisioning**]	コンフィギュレーション ログ全体、または指定されたパラメータのログを表示します。

システム メッセージ ログの設定例

例：スイッチ システム メッセージ

次に、スイッチ上のスイッチ システム メッセージの一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
 to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

例：サービス タイムスタンプ ログの表示

次に、**service timestamps log datetime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
(Switch-2)
```

次に、**service timestamps log uptime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のロギング表示（一部）の例を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up (Switch-2)
```

次に、シーケンス番号をイネーブルにした場合のロギング表示の一部を示します。

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) (Switch-2)
```

第 71 章

オンライン診断の設定

- オンライン診断の設定に関する情報，1899 ページ
- オンライン診断の設定方法，1900 ページ
- オンライン診断のモニタリングおよびメンテナンス，1905 ページ
- オンライン診断テストの設定例，1906 ページ

オンライン診断の設定に関する情報

オンライン診断

オンライン診断では、スイッチが稼働中のネットワークに接続している間に、スイッチのハードウェア機能をテストし、確認できます。

オンライン診断には、異なるハードウェア コンポーネントをチェックするパケット交換テストが含まれ、データ パスおよび制御信号が確認されます。

オンライン診断では、次の領域の問題が検出されます。

- ハードウェア コンポーネント
- インターフェイス（イーサネット ポートなど）
- はんだ接合

オンライン診断は、オンデマンド診断、スケジュール診断、ヘルスモニタリング診断に分類できます。 オンデマンド診断は、CLI から実行されます。スケジュールされた診断は、動作中のネットワークにスイッチが接続されているときに、ユーザが指定した間隔または指定した時刻に実行されます。ヘルスモニタリングは、バックグラウンドでユーザが指定した間隔で実行されます。デフォルトでは、30 秒ごとにヘルス モニタリング テストが実行されます。

オンライン診断を設定したあと、手動で診断テストを開始したり、テスト結果を表示したりできます。また、スイッチまたはスイッチスタックに設定されているテストの種類、およびすでに実行された診断テスト名を確認できます。

オンライン診断の設定方法

オンライン診断テストの開始

スイッチで実行する診断テストを設定したあと、**diagnostic start** 特権 EXEC コマンドを使用して診断テストを開始します。

テストを開始したら、テスト プロセスの停止はできません。

手動でオンライン診断テストを開始するには、次の特権 EXEC コマンドを使用します。

手順の概要

1. **diagnostic start switch***number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive** }

手順の詳細

	コマンドまたはアクション	目的
ステップ **1**	**diagnostic start switch***number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive** } 例： `Switch# diagnostic start switch 2 test basic`	診断テストを開始します。 **switch***number* キーワードは、スタック構成スイッチだけでサポートされます。 有効な範囲は 1 ～ 8 です。 次のいずれかのオプションを使用してテストを指定できます。 • *name*：テストの名前を入力します。 • *test-id*：テストの ID 番号を入力します。 • *test-id-range*：カンマとハイフンで区切ってテスト ID の範囲を整数で入力します。 • **all**：すべてのテストを開始します。 • **basic**： 基本テスト スイートを開始します。 • **non-disruptive**：ノンディスラプティブ テスト スイートを開始します。

オンライン診断の設定

診断モニタリングをイネーブルにする前に、障害しきい値およびテストの間隔を設定する必要があります。

オンライン診断のスケジューリング

特定のスイッチについて指定した時間、または日、週、月単位でオンライン診断をスケジューリングできます。 スケジューリングを削除するには、コマンドの **no** 形式を入力します。

手順の概要

1. **configure terminal**
2. **diagnostic schedule switch***number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive** |} {**daily** | **on***mm dd yyyy hh:mm* | **weekly***day-of-week hh:mm*}

手順の詳細

	コマンドまたはアクション	目的
ステップ **1**	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ **2**	**diagnostic schedule switch***number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive** |} {**daily** | **on***mm dd yyyy hh:mm* | **weekly***day-of-week hh:mm*} 例： `Switch(config)# diagnostic schedule switch 1 test 1-5 on July 3 2013 23:10`	特定日時のオンデマンド診断テストをスケジュールします。 **switch***number* キーワードは、スタック構成スイッチだけでサポートされます。 有効な範囲は 1 ～ 8 です。 スケジュールするテストを指定する場合は、次のオプションを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべてのテスト ID です。 • **basic**：基本的なオンデマンドの診断テストを開始します。 • **non-disruptive**：ノンディスラプティブ テスト スイートを開始します。 テストは次のようにスケジュールできます。 • 毎日：**daily***hh:mm* パラメータを使用します。 • 特定日時：**on***mm dd yyyy hh:mm* パラメータを使用します。

	コマンドまたはアクション	目的
		• 毎週：**weekly***day-of-week hh:mm* パラメータを使用します。

ヘルス モニタリング診断の設定

スイッチが稼働中のネットワークに接続されている間に、スイッチに対しヘルス モニタリング診断テストを設定できます。 ヘルス モニタリング テストの実行間隔を設定したり、テスト失敗時のスイッチの syslog メッセージ生成をイネーブルにしたり、特定のテストをイネーブルにできます。
テストをディセーブルにするには、コマンドの **no** 形式を入力します。

デフォルトでは、ヘルスモニタリングはディセーブルですが、スイッチはテストの失敗時にSyslogメッセージを生成します。

ヘルス モニタリング診断テストを設定し、イネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **diagnostic monitor interval switch***number***test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day*
4. **diagnostic monitor syslog**
5. **diagnostic monitor threshold switch***number***test** {*name* | *test-id* | *test-id-range* | **all**} **failure count***count*
6. **diagnostic monitor switch***number***test** {*name* | *test-id* | *test-id-range* | **all**}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**diagnostic monitor interval switch***number***test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day* 例： `Switch(config)# diagnostic monitor interval switch 2 test 1 12:30:00 750 5`	指定のテストに対し、ヘルス モニタリングの実行間隔を設定します。 **switch***number* キーワードは、スタック構成スイッチだけでサポートされます。 テストを指定する場合は、次のいずれかのパラメータを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべての診断テスト。 間隔を指定する場合は、次のパラメータを設定します。 • *hh:mm:ss*：モニタリング間隔（時間、分、秒）。 指定できる範囲は *hh* が 0 ~ 24、*mm* および *ss* が 0 ~ 60 です。 • *milliseconds*：モニタリング間隔（ミリ秒（ms））。 指定できる範囲は 0 ～ 999 です。 • *day*：モニタリング間隔（日数）。 指定できる範囲は 0 ～ 20 です。
ステップ 4	**diagnostic monitor syslog** 例： `Switch(config)# diagnostic monitor syslog`	（任意）ヘルス モニタリング テストの失敗時にスイッチが Syslog メッセージを生成するように設定します。
ステップ 5	**diagnostic monitor threshold switch***number***test** {*name* | *test-id* | *test-id-range* | **all**} **failure count***count*	（任意）ヘルス モニタリング テストの失敗しきい値を設定します。 テストを指定する場合は、次のいずれかのパラメータを使用します。

	コマンドまたはアクション	目的
	例： `Switch(config)# diagnostic monitor threshold switch 2 test 1 failure count 20`	• *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべての診断テスト。 失敗しきい値 *count* に指定できる範囲は 0 ～ 99 です。
ステップ 6	**diagnostic monitor switch***number***test** {*name* | *test-id* | *test-id-range* | **all**} 例： `Switch(config)# diagnostic monitor switch 2 test 1`	指定のヘルス モニタリング テストをイネーブルにします。 **switch***number* キーワードは、スタック構成スイッチだけでサポートされます。 指定できる範囲は 1 ～ 9 です。 テストを指定する場合は、次のいずれかのパラメータを使用します。 • *name*：**show diagnostic content** コマンドの出力に表示されるテストの名前です。 • *test-id*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • *test-id-range*：**show diagnostic content** コマンドの出力に表示されるテストの ID 番号です。 • **all**：すべての診断テスト。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

間隔をデフォルトの値またはゼロに変更するには、**no diagnostic monitor interval test***test-id* | *test-id-range* } グローバル コンフィギュレーション コマンドを使用します。 ヘルスモニタリングテストに失敗した場合、**no diagnostic monitor syslog** コマンドを使用して、Syslog メッセージの生成をディセーブルに設定します。 失敗しきい値を削除するには、**diagnostic monitor threshold test***test-id* | *test-id-range* }**failure count** コマンドを使用します。

オンライン診断のモニタリングおよびメンテナンス

オンライン診断テストとテスト結果の表示

スイッチまたはスイッチ スタックに設定されているオンライン診断テストを表示し、この表に示す **show** 特権 EXEC コマンドを使用してテスト結果を確認することができます。

表 ***168*** : 診断テストの設定および結果用のコマンド

コマンド	目的
show diagnostic content switch [*number* | **all**]	スイッチに対して設定されたオンライン診断を表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic status	現在実行中の診断テストを表示します。
show diagnostic result switch [*number* | **all**] [**detail** | **test** {*name* | *test-id* | *test-id-range* | **all**} [**detail**]]	オンライン診断テストの結果を表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic switch [*number* | **all**] [**detail**]	オンライン診断テストの結果を表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。
show diagnostic schedule switch [*number* | **all**]	オンライン診断テストのスケジュールを表示します。 **switch** [*number* | **all**] パラメータは、スタック構成スイッチだけでサポートされます。

コマンド	目的
show diagnostic post	POST 結果を表示します （この出力は、**show post** コマンドの出力と同じです）。

オンライン診断テストの設定例

オンライン診断テストの開始

スイッチで実行する診断テストを設定したあと、**diagnostic start** 特権 EXEC コマンドを使用して診断テストを開始します。

テストを開始したら、テスト プロセスの停止はできません。

手動でオンライン診断テストを開始するには、次の特権 EXEC コマンドを使用します。

手順の概要

1. **diagnostic start switch***number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive** }

手順の詳細

	コマンドまたはアクション	目的
ステップ **1**	**diagnostic start switch***number***test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive** } 例： `Switch# diagnostic start switch 2 test basic`	診断テストを開始します。 **switch***number* キーワードは、スタック構成スイッチだけでサポートされます。 有効な範囲は 1 ～ 8 です。 次のいずれかのオプションを使用してテストを指定できます。 • *name*：テストの名前を入力します。 • *test-id*：テストの ID 番号を入力します。 • *test-id-range*：カンマとハイフンで区切ってテスト ID の範囲を整数で入力します。 • **all**：すべてのテストを開始します。 • **basic**： 基本テスト スイートを開始します。 • **non-disruptive**：ノンディスラプティブ テスト スイートを開始します。

例：ヘルス モニタリング テストの設定

次に、ヘルス モニタリング テストを設定する例を示します。

```
Switch(config)# diagnostic monitor threshold switch 1 test 1 failure count 50
Switch(config)# diagnostic monitor interval switch 1 test TestPortAsicStackPortLoopback
```

例：診断テストのスケジューリング

次に、特定のスイッチに対して、特定の日時に診断テストを実行するようにスケジューリングする例を示します。

```
Switch(config)# diagnostic schedule test DiagThermalTest on June 3 2013  22:25
```

次の例では、指定されたスイッチで毎週特定の時間に診断テストを実行するようにスケジューリングする方法を示します。

```
Switch(config)# diagnostic schedule switch 1 test 1,2,4-6 weekly saturday 10:30
```

オンライン診断の表示：例

次の例では、特定のスイッチのオンライン診断の詳細情報を表示する方法を示します。

```
Switch# show diagnostic switch 1 detail

Switch 1: SerialNo :

Overall Diagnostic Result for Switch 1 : UNTESTED

Test results: (. = Pass, F = Fail, U = Untested)

___________________________________________________________________________

1) TestPortAsicStackPortLoopback ---> U

Error code ------------------> 3 (DIAG_SKIPPED)
Total run count -------------> 0
Last test testing type ------> n/a
Last test execution time ----> n/a
First test failure time -----> n/a
Last test failure time ------> n/a
Last test pass time ---------> n/a
Total failure count ---------> 0
Consecutive failure count ---> 0
___________________________________________________________________________

2) TestPortAsicLoopback ------------> U

Error code ------------------> 3 (DIAG_SKIPPED)
Total run count -------------> 0
Last test testing type ------> n/a
Last test execution time ----> n/a
First test failure time -----> n/a
Last test failure time ------> n/a
Last test pass time ---------> n/a
Total failure count ---------> 0
Consecutive failure count ---> 0
```

```
-----------------------------------------------------------------------------

3) TestPortAsicCam -----------------> U

Error code ------------------> 3 (DIAG_SKIPPED)
Total run count -------------> 0
Last test testing type ------> n/a
Last test execution time ----> n/a
First test failure time -----> n/a
Last test failure time ------> n/a
Last test pass time ---------> n/a
Total failure count ---------> 0
Consecutive failure count ---> 0

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

4) TestPortAsicMem -----------------> U

Error code ------------------> 3 (DIAG_SKIPPED)
Total run count -------------> 0
Last test testing type ------> n/a
Last test execution time ----> n/a
First test failure time -----> n/a
Last test failure time ------> n/a
Last test pass time ---------> n/a
Total failure count ---------> 0
Consecutive failure count ---> 0

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

5) TestInlinePwrCtlr ---------------> U

Error code ------------------> 3 (DIAG_SKIPPED)
Total run count -------------> 0
Last test testing type ------> n/a
Last test execution time ----> n/a
First test failure time -----> n/a
Last test failure time ------> n/a
Last test pass time ---------> n/a
Total failure count ---------> 0
Consecutive failure count ---> 0

-----------------------------------------------------------------------------
```

次の例では、特定のスイッチに設定されているオンライン診断を表示する方法を示します。

```
Switch# show diagnostic content switch 3

Switch 1:
Diagnostics test suite attributes:
    B/* - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
    S/* - Only applicable to standby unit / NA
    X/* - Not a health monitoring test / NA
    F/* - Fixed monitoring interval test / NA
    E/* - Always enabled monitoring test / NA
    A/I - Monitoring is active / Monitoring is inactive
    R/* - Switch will reload after test list completion / NA
    P/* - will partition stack / NA

                                                        Test Interval   Thre-
ID   Test Name                            Attributes    day hh:mm:ss.ms shold
==== ================================== ============   =============== =====
  1) TestPortAsicStackPortLoopback ---> B*N****I**     not configured  n/a
  2) TestPortAsicLoopback ------------> B*D*X**IR*     not configured  n/a
  3) TestPortAsicCam -----------------> B*D*X**IR*     not configured  n/a
  4) TestPortAsicRingLoopback --------> B*D*X**IR*     not configured  n/a
  5) TestMicRingLoopback -------------> B*D*X**IR*     not configured  n/a
  6) TestPortAsicMem -----------------> B*D*X**IR*     not configured  n/a
```

次の例では、スイッチのオンライン診断結果を表示する方法を示します。

```
Switch# show diagnostic result

Switch 1: SerialNo :
Overall diagnostic result: PASS
Test results: (. = Pass, F = Fail, U = Untested)
1) TestPortAsicStackPortLoopback ---> .
2) TestPortAsicLoopback ------------> .
3) TestPortAsicCam -----------------> .
4) TestPortAsicRingLoopback --------> .
5) TestMicRingLoopback -------------> .
6) TestPortAsicMem -----------------> .
```

次の例では、オンライン診断テストのステータスを表示する方法を示します。

```
Switch# show diagnostic status

<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics
====== ================================ ============================== ======
Card   Description                      Current Running Test            Run by
------ -------------------------------- ---------------------          ------
1                                        N/A                            N/A
2                                        TestPortAsicStackPortLoopback  <OD>
                                         TestPortAsicLoopback           <OD>
                                         TestPortAsicCam                <OD>
                                         TestPortAsicRingLoopback       <OD>
                                         TestMicRingLoopback            <OD>
                                         TestPortAsicMem                <OD>
3                                        N/A                            N/A
4                                        N/A                            N/A
====== ================================ ============================== ======
Switch#
```

次の例では、スイッチのオンライン診断のテスト スケジュールを表示する方法を示します。

```
Switch# show diagnostic schedule switch 1

Current Time = 14:39:49 PST Tue May 5 2013
Diagnostic for Switch 1:
Schedule #1:
To be run daily 12:00
Test ID(s) to be executed: 1.
```

第 72 章

ソフトウェア設定のトラブルシューティング

この章では、スイッチが稼働する Cisco IOS ソフトウェアに関連する問題を特定し、解決する方法について説明します。 問題の性質に応じて、コマンドライン インターフェイス（CLI）、デバイス マネージャ、または Network Assistant を使用して、問題を特定し解決できます。

LED の説明など、トラブルシューティングの詳細については、ハードウェア インストレーション ガイドを参照してください。

- ソフトウェア設定のトラブルシューティングに関する情報，1911 ページ
- ソフトウェア設定のトラブルシューティング方法，1919 ページ
- ソフトウェア設定のトラブルシューティングの確認，1935 ページ
- ソフトウェア設定のトラブルシューティングのシナリオ，1938 ページ
- ソフトウェアのトラブルシューティングの設定例，1942 ページ

ソフトウェア設定のトラブルシューティングに関する情報

スイッチのソフトウェア障害

スイッチ ソフトウェアがアップグレード中に破損する原因として、間違ったファイルがスイッチにダウンロードされた場合やイメージ ファイルが削除された場合があります。 いずれの場合にも、スイッチは電源投入時自己診断テスト（POST）に失敗し、接続できなくなります。

関連トピック

ソフトウェア障害からの回復

スイッチのパスワードを紛失したか忘れた場合

スイッチのデフォルト設定では、スイッチに物理的にアクセスしているエンドエンドユーザは、スイッチの電源投入中に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復できます。 ここで紹介する回復手順を実行するには、スイッチに物理的にアクセスする必要があります。

（注） これらのスイッチでは、システム管理者は、デフォルト設定に戻すことに同意した場合に限り、エンドユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできます。 パスワード回復がディセーブルになっている場合に、エンドユーザがパスワードをリセットしようとすると、ステータス メッセージで回復プロセスの間はデフォルトの設定に戻すように指示されます。

関連トピック

パスワードを忘れた場合の回復

Power over Ethernet（PoE）ポート

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

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

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

受電装置を検出すると、スイッチは受電装置の電力要件を判断し、受電装置への電力供給を許可または拒否します。 また、スイッチは消費電力をモニタリングおよびポリシングすることで、装置の電力の消費をリアルタイムに検知できます。

関連トピック

Power over Ethernet（PoE）に関するトラブルシューティングのシナリオ, （1938 ページ）

電力消失によるポートの障害

PoE スイッチ ポートに接続され、AC 電源から電力が供給されている受電デバイス（Cisco IP Phone 7910 など）に AC 電源から電力が供給されない場合、そのデバイスは errdisable ステートになることがあります。 error-disabled ステートから回復するには、**shutdown** インターフェイス コンフィ

ギュレーション コマンドを入力してから、**no shutdown** インターフェイス コマンドを入力します。 スイッチで自動回復を設定し、error-disabled ステートから回復することもできます。

スイッチの場合、**errdisable recovery cause loopback** および **errdisable recovery interval***seconds* グローバル コンフィギュレーション コマンドは、指定した期間が経過したあと自動的にインターフェイスを error-disabled ステートから復帰させます。

PoE ポート ステータスのモニタリング

- **show controllers power inline** 特権 EXEC コマンド
- **show power inline** EXEC コマンド
- **debug ilpower** 特権 EXEC コマンド

不正リンク アップによるポート障害

シスコ受電デバイスをポートに接続し、**power inline never** インターフェイス コンフィギュレーション コマンドを使用してポートを設定した場合は、不正リンク アップが発生し、ポートが error-disabled ステートになることがあります。 ポートを error-disabled ステートから回復するには、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

power inline never コマンドで設定したポートにシスコ受電デバイスを接続しないでください。

ping

スイッチは IP の ping をサポートしており、これを使ってリモート ホストへの接続をテストできます。 ping はアドレスにエコー要求パケットを送信し、応答を待ちます。 ping は次のいずれかの応答を返します。

- 正常な応答：正常な応答（*hostname* が存在する）は、ネットワーク トラフィックにもよりますが、1 ～ 10 秒以内で発生します。
- 宛先の応答なし：ホストが応答しない場合、*no-answer* メッセージが返されます。
- 不明なホスト：ホストが存在しない場合、*unknown host* メッセージが返されます。
- 宛先到達不能：デフォルト ゲートウェイが指定されたネットワークに到達できない場合、*destination-unreachable* メッセージが返されます。
- ネットワークまたはホストへの到達不能：ルートテーブルにホストまたはネットワークのエントリがない場合、*network or host unreachable* メッセージが返されます。

関連トピック

ping の実行, （1931 ページ）

例：IP ホストの ping, （1942 ページ）

レイヤ 2 Traceroute

レイヤ 2 traceroute 機能により、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを識別できます。 レイヤ 2 traceroute は、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。 transroute は、パス内にあるスイッチの MAC アドレス テーブルを使用してパスを識別します。 スイッチがパス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 trace クエリーを送信し続け、タイムアウトにします。

スイッチは、送信元デバイスから宛先デバイスへのパスのみを識別できます。 パケットが通過する、送信元ホストから送信元デバイスまで、または宛先デバイスから宛先ホストまでのパスは識別できません。

レイヤ 2 の traceroute のガイドライン

- ネットワーク内のすべてのデバイスで、Cisco Discovery Protocol（CDP）をイネーブルにする必要があります。 レイヤ 2 traceroute が適切に動作するために、CDP をディセーブルにしないでください。

  物理パス内のデバイスが CDP に対して透過的な場合、スイッチはこれらのデバイスを通過するパスを識別できません。

- **ping** 特権 EXEC コマンドを使用して接続をテストできれば、このスイッチは別のスイッチから到達可能といえます。 物理パス内のすべてのスイッチは、他のスイッチから相互に到達可能でなければなりません。

- パス内で識別可能な最大ホップ数は 10 です。

- 送信元デバイスと宛先デバイスの間の物理パス内にないスイッチで、**traceroute mac** または **traceroute mac ip** の特権 EXEC コマンドを実行できます。 パス内のすべてのスイッチは、このスイッチから到達可能でなければなりません。

- **traceroute mac** コマンドの出力結果としてレイヤ 2 パスが表示されるのは、指定の送信元および宛先 MAC アドレスが、同一の VLAN に属している場合だけです。 指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。

- マルチキャストの送信元または宛先 MAC アドレスを指定すると、パスは識別されず、エラー メッセージが表示されます。

- 送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。 VLAN を指定しないと、パスは識別されず、エラー メッセージが表示されます。

- 指定した送信元および宛先の IP アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力にレイヤ 2 パスが表示されます。 IP アドレスを指定した場合、スイッチは Address Resolution Protocol（ARP）を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を関連付けます。

  - 指定の IP アドレスの ARP のエントリが存在している場合、スイッチは関連付けられた MAC アドレスを使用して、物理パスを識別します。

- ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。 IP アドレスが解決されない場合は、パスは識別されず、エラーメッセージが表示されます。

- 複数のデバイスがハブを介して 1 つのポートに接続されている場合（たとえば複数の CDP ネイバーがポートで検出された場合）、レイヤ 2 traceroute 機能はサポートされません。 複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされません。

IP Traceroute

IP traceroute を使用すると、ネットワーク上でパケットが通過するパスをホップバイホップで識別できます。 このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク層（レイヤ 3）デバイスが表示されます。

スイッチは、**traceroute** 特権 EXEC コマンドの送信元または宛先として指定できます。また、スイッチは **traceroute** コマンドの出力でホップとして表示される場合があります。 スイッチを traceroute の宛先とすると、スイッチは、traceroute の出力で最終の宛先として表示されます。 中間スイッチが同じ VLAN 内でポート間のパケットのブリッジングだけを行う場合、traceroute の出力に中間スイッチは表示されません。 ただし、中間スイッチが、特定のパケットをルーティングするマルチレイヤ スイッチの場合、中間スイッチは traceroute の出力にホップとして表示されます。

traceroute 特権 EXEC コマンドは、IP ヘッダーの存続可能時間（TTL）フィールドを使用して、ルータおよびサーバで特定のリターン メッセージが生成されるようにします。 traceroute の実行は、ユーザ データグラム プロトコル（UDP）データグラムを、TTL フィールドが 1 に設定されている宛先ホストへ送信することから始まります。 ルータで TTL 値が 1 または 0 であることを検出すると、データグラムをドロップし、インターネット制御メッセージ プロトコル（ICMP）time-to-live-exceeded メッセージを送信元に送信します。 traceroute は、ICMP time-to-live-exceeded メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判別します。

ネクスト ホップを識別するために、traceroute は TTL 値が 2 の UDP パケットを送信します。 1 番めのルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。 2 番めのルータは、TTL 値が 1 であることを確認すると、このデータグラムを廃棄し、time-to-live-exceeded メッセージを送信元へ返します。 このように、データグラムが宛先ホストに到達するまで（または TTL の最大値に達するまで）TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを学習するために、traceroute は、データグラムの UDP 宛先ポート番号を、宛先ホストが使用する可能性のない大きな値に設定します。 ホストが、ローカルで使用されない宛先ポート番号を持つ自分自身宛てのデータグラムを受信すると、送信元に ICMP ポート到達不能エラーを送信します。 ポート到達不能エラーを除くすべてのエラーは中間ホップから送信されるため、ポート到達不能エラーを受信するということは、このメッセージが宛先ポートから送信されたことを意味します。

関連トピック

IP traceroute の実行, （1933 ページ）

例：IP ホストに対する traceroute の実行, （1943 ページ）

Time Domain Reflector ガイドライン

Time Domain Reflector（TDR）機能を使用すると、ケーブル配線の問題を診断して解決できます。TDR稼働時、ローカルデバイスはケーブルを介して信号を送信して、最初に送信した信号と反射された信号を比べます。

TDR は 10/100/1000 の銅線イーサネット ポート上でだけサポートされます。 10 ギガビット イーサネット ポートまたは SFP モジュール ポートではサポートされません。

TDR は次のケーブル障害を検出します。

- ツイストペア ケーブルの導線のオープン、損傷、切断：導線がリモート デバイスからの導線に接続されていない状態。
- ツイストペア ケーブルの導線のショート：導線が互いに接触している状態、またはリモート デバイスからの導線に接触している状態。 たとえば、ツイスト ペア ケーブルの一方の導線が、もう一方の導線にはんだ付けされている場合、ツイストペア ケーブルのショートが発生します。

ツイストペアの導線の一方がオープンになっている場合、TDR はオープンになっている導線の長さを検出できます。

次の状況で TDR を使用して、ケーブル障害を診断および解決してください。

- スイッチの交換
- 配線クローゼットの設定
- リンクが確立できない、または適切に動作していない場合における、2 つのデバイス間の接続のトラブルシューティング

TDR の実行時、次の場合にスイッチは正確な情報をレポートします。

- ギガビット リンク用のケーブルが単線コア ケーブル
- オープンエンド ケーブルが未終端

TDR の実行時、次の場合にスイッチは正確な情報をレポートしません。

- ギガビットリンク用のケーブルがツイストペア ケーブルまたは連続接続された単線コア ケーブル
- リンクが 10 Mb または 100 Mb
- より線ケーブル
- リンク パートナーが Cisco IP Phone

- リンク パートナーが IEEE 802.3 に準拠していない

debug コマンド

注意 デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。 したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。 ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。 デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

debug コマンドはすべて特権 EXEC モードで実行します。ほとんどの **debug** コマンドは引数を取りません。

関連トピック

デバッグおよびエラー メッセージ出力のリダイレクト，（1933 ページ）

例：すべてのシステム診断をイネーブルにする，（1944 ページ）

スイッチのオンボード障害ロギング

オンボード障害ロギング（OBFL）機能を使用すれば、スイッチに関する情報を収集できます。この情報には稼働時間、温度、電圧などの情報が含まれており、シスコのテクニカル サポート担当者がスイッチの問題をトラブルシューティングする際に役立ちます。 OBFL はイネーブルにしておき、フラッシュ メモリに保存されたデータは消さないようにすることを推奨します。

OBFL は、デフォルトでイネーブルになっています。 スイッチおよび Small Form-Factor Pluggable（SFP）モジュールに関する情報が収集されます。 スイッチは、次の情報をフラッシュ メモリに保存します。

- CLI コマンド：スタンドアロン スイッチに入力された OBFL CLI コマンドの記録
- 環境データ：スタンドアロン スイッチおよび接続されているすべての FRU デバイスの一意のデバイス ID（UDI）情報、製品 ID（PID）、バージョン ID（VID）、およびシリアル番号
- メッセージ：スタンドアロン スイッチにより生成されたハードウェア関連のシステム メッセージの記録
- イーサネット経由の電源供給（PoE）：スタンドアロン スイッチまたはの PoE ポートの消費電力の記録
- 温度：スタンドアロン スイッチの温度
- 稼働時間：スタンドアロン スイッチが起動されたときの時刻、スイッチが再起動された理由、およびスイッチが最後に再起動されて以来の稼働時間
- 電圧：スタンドアロン スイッチのシステム電圧

システム時計は、手動で時刻を設定するか、またはネットワーク タイム プロトコル（NTP）を使用するように設定します。

スイッチの稼働中には、**show logging onboard** 特権 EXEC コマンドを使用することにより、OBFL データを取得できます。 スイッチに障害が発生した場合のデータの取得方法については、お客様担当のシスコ テクニカル サポート担当者にお問い合わせください。

OBFL がイネーブルになっているスイッチが再起動された場合、新しいデータの記録が開始するまでに 10 分間の遅延があります。

関連トピック

OBFL の設定, （1934 ページ）

OBFL 情報の表示

CPU 使用率が高い場合に起こりうる症状

CPU 使用率が高すぎることで次の症状が発生する可能性がありますが、他の原因で発生する場合もあります。

- スパニングツリー トポロジの変更
- 通信が切断されたために EtherChannel リンクがダウンした
- 管理要求（ICMP ping、SNMP のタイムアウト、低速な Telnet または SSH セッション）に応答できない
- UDLD フラッピング
- SLA の応答が許容可能なしきい値を超えたことによる IP SLA の失敗
- スイッチが要求を転送しない、または要求に応答しない場合の DHCP または IEEE 802.1x の処理の失敗

レイヤ 3 スイッチの場合：

- ソフトウェアでルーティングされるパケットのドロップまたは遅延の増加
- BGP または OSPF ルーティング トポロジの変更
- HSRP フラッピング

（注）

ソフトウェア設定のトラブルシューティング方法

ソフトウェア障害からの回復

スイッチ ソフトウェアが破損する状況としては、アップグレードを行った場合、スイッチに誤ったファイルをダウンロードした場合、イメージファイルを削除した場合などが考えられます。いずれの場合にも、スイッチは電源投入時自己診断テスト（POST）に失敗し、接続できなくなります。

次の手順では、XMODEM プロトコルを使用して、破損したイメージ ファイルまたは間違ったイメージファイルを回復します。 XMODEM プロトコルをサポートするソフトウェア パッケージは多数あり、使用するエミュレーション ソフトウェアによって、この手順は異なります。

ここで紹介する回復手順を実行するには、スイッチを直接操作する必要があります。

ステップ 1 PC 上で、Cisco.com から tar 形式のソフトウェア イメージ ファイル（*image_filename.tar*）をダウンロードします。 Cisco IOS イメージは、tar ファイルのディレクトリ内に bin ファイルとして格納されます。 Cisco.com 上のソフトウェアイメージファイルの検索方法については、リリース ノートを参照してください。

ステップ 2 tar ファイルから bin ファイルを抽出します。 Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。 zip プログラムを使用して移動します。 Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。 zip プログラムを使用して移動します。 UNIX を使用している場合は、次の手順に従ってください。

a) **tar -tvf** <*image_filename.tar*> UNIX コマンドを使用して、tar ファイルの内容を表示します。

例：
```
unix-1% tar -tvf image_filename.tar
```

b) **tar -xvf** <*image_filename.tar*> <*image_filename.bin*> UNIX コマンドを使用して、bin ファイルを特定し、抽出します。

例：
```
unix-1% tar -xvf image_filename.tar image_filename.bin
x c2960x-universalk9-mz-150-2.EX1/c2960x-universalk9-mz-150-2.EX1.bin, 2928176 bytes, 5720
tape blocks
```

c) **ls -l** <*image_filename.bin*> UNIX コマンドを使用して、bin ファイルが抽出されたことを確認します。

例：
```
unix-1% ls -l image_filename.bin
-rw-r--r--   1 boba      2928176 Apr 21 12:01
```

```
c2960x-universalk9-mz.150-2.0.66.UCP/c2960x-universalk9-mz.150-2.0.66.UCP.bin
```

ステップ 3 XMODEM プロトコルをサポートする端末エミュレーション ソフトウェアを備えた PC を、スイッチのコンソール ポートに接続します。

ステップ 4 エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 5 スイッチの電源コードを取り外します。

ステップ 6 [Mode] ボタンを押しながら、電源コードを再度スイッチに接続します。 ポート 1 の上の LED が消灯してから 1 ～ 2 秒後に、[Mode] ボタンを放します。 ソフトウェアに関する数行分の情報と指示が表示されます。

例：

```
The system has been interrupted prior to initializing the flash file system. The following
commands will initialize the flash file system, and finish loading the operating system
software#

flash_init

load_helper

boot
```

ステップ 7 フラッシュ ファイル システムを初期化します。

例：

```
switch: flash_init
```

ステップ 8 コンソール ポートの速度を 9600 以外に設定していた場合、9600 にリセットされます。 エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。

ステップ 9 ヘルパー ファイルがある場合にはロードします。

例：

```
switch: load_helper
```

ステップ 10 XMODEM プロトコルを使用して、ファイル転送を開始します。

例：

```
switch: copy xmodem: flash:image_filename.bin
```

ステップ 11 XMODEM 要求が表示されたら、端末エミュレーション ソフトウェアに適切なコマンドを使用して、転送を開始し、ソフトウェア イメージをフラッシュ メモリにコピーします。

ステップ 12 新規にダウンロードされた Cisco IOS イメージを起動します。

例：
```
switch: boot flash:image_filename.bin
```

ステップ 13 **archive download-sw** 特権 EXEC コマンドを使用して、スイッチまたはスイッチ スタックにソフトウェア イメージをダウンロードします。

ステップ 14 **reload** 特権 EXEC コマンドを使用してスイッチを再起動し、新しいソフトウェア イメージが適切に動作していることを確認します。

ステップ 15 スイッチから、**flash**:*image_filename.bin* ファイルを削除します。

パスワードを忘れた場合の回復

スイッチのデフォルト設定では、スイッチを直接操作するエンド ユーザが、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復できます。 ここで紹介する回復手順を実行するには、スイッチを直接操作してください。

（注） これらのスイッチでは、システム管理者はデフォルト設定に戻す場合に限りエンド ユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできます。 パスワード回復がディセーブルになっている場合に、エンドユーザがパスワードをリセットしようとすると、回復プロセスの間、ステータス メッセージにその旨が表示されます。

パスワードの回復をイネーブルまたはディセーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。

ステップ 1 端末または PC をスイッチに接続します。

- 端末または端末エミュレーション ソフトウェアが稼働している PC をスイッチのコンソール ポートに接続します。

  または

- PC をイーサネット管理ポートに接続します。

ステップ 2 エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 3 スイッチでスイッチの電源を切断します。

ステップ 4 スイッチに電源コードを再接続します。 15 秒以内に [**Mode**] ボタンを押します。このときシステム LED はグリーンに点滅しています。 すべてのシステム LED が点灯した状態になるまで、[**Mode**] ボタンを押し続けます。その後、[**Mode**] ボタンを放します。

ソフトウェアについての情報および指示が数行表示され、パスワード回復手順がディセーブルであるかどうかが示されます。

- 次のステートメントで始まるメッセージが表示された場合

  ```
  The system has been interrupted prior to initializing the flash file system. The following
  commands will initialize the flash file system
  ```

  「パスワード回復がイネーブルになっている場合の手順」セクションに記載されている手順を実行します。

- 次のステートメントで始まるメッセージが表示された場合

  ```
  The password-recovery mechanism has been triggered, but is currently disabled.
  ```

  「パスワード回復がディセーブルになっている場合の手順」に記載されている手順を実行します。

ステップ 5 パスワードの回復後、スイッチをリロードします。
スイッチの場合

```
Switch> reload
Proceed with reload? [confirm] y
```

パスワード回復がイネーブルになっている場合の手順

パスワード回復動作がイネーブルになっている場合は、次のメッセージが表示されます。

```
The system has been interrupted prior to initializing the flash file system. The following
 commands will initialize the flash file system, and finish loading the operating system
software:

flash_init
load_helper
boot
```

ステップ 1 フラッシュ ファイル システムを初期化します。

```
Switch: flash_init
```

ステップ 2 コンソール ポートの速度を 9600 以外の値に設定していた場合、9600 にリセットされます。 エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。

ステップ 3 ヘルパー ファイルがある場合にはロードします。

```
Switch: load_helper
```

ステップ 4 フラッシュ メモリの内容を表示します。

```
Switch: dir: flash:
Directory of flash:
```

```
   13  drwx         192   Mar 01 2013 22:30:48
c2960x-universalk9-mz-150-2.EX1/c2960x-universalk9-mz-150-2.EX1.bin
   11  -rwx        5825   Mar 01 2013 22:31:59  config.text

16128000 bytes total (10003456 bytes free)
```

ステップ 5 コンフィギュレーション ファイルの名前を config.text.old に変更します。
このファイルには、パスワード定義が収められています。

```
Switch: rename flash: config.text flash: config.text.old
```

ステップ 6 システムを起動します。

```
Switch: boot
```

セットアップ プログラムを起動するように求められます。 プロンプトに **N** を入力します。

```
Continue with the configuration dialog?? [yes/no]: No
```

ステップ 7 スイッチ プロンプトで、特権 EXEC モードを開始します。

```
Switch> enable
Switch#
```

ステップ 8 コンフィギュレーション ファイルを元の名前に戻します。

```
Switch# rename flash: config.text.old flash: config.text
```

（注） ステップ 9 に進む前に、接続されているすべてのスタック メンバの電源を入れ、それらが完全に初期化されるまで待ちます。 このステップに従わなかった場合は、スイッチの設定によっては設定を失う可能性もあります。

ステップ 9 コンフィギュレーション ファイルをメモリにコピーします。

```
Switch# copy flash: config.text system: running-config
Source filename [config.text]?
Destination filename [running-config]?
```

確認を求めるプロンプトに、Return を押して応答します。 これで、コンフィギュレーション ファイルがリロードされ、パスワードを変更できるようになります。

ステップ 10 グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 11 パスワードを変更します。

```
Switch(config)# enable secret password
```

シークレット パスワードは 1 ～ 25 文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 12 特権 EXEC モードに戻ります。

```
Switch(config)# exit
Switch#
```

ステップ 13 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Switch# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。

（注） 上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウン ステートになることがあります。 このステートになっているインターフェイスを調べるには、**show running-config** 特権 EXEC コマンドを入力します。 インターフェイスを再びイネーブルにするには、**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを入力して、シャットダウン インターフェイスの VLAN ID を指定します。 スイッチがインターフェイス コンフィギュレーション モードの状態で、**no shutdown** コマンドを入力します。

ステップ 14 *packages.conf* ファイルでスイッチをフラッシュからブートします。

```
Switch: boot flash:packages.conf
```

ステップ 15 スイッチ スタックをリロードします。

```
Switch# reload
```

パスワード回復がディセーブルになっている場合の手順

パスワード回復メカニズムがディセーブルの場合、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

注意 スイッチをデフォルト設定に戻すと、既存の設定がすべて失われます。 システム管理者に問い合わせて、バックアップ スイッチと VLAN（仮想 LAN）コンフィギュレーション ファイルがあるかどうかを確認してください。

- **n**（no）を入力すると、Modeボタンを押さなかった場合と同様に、通常のブートプロセスが継続されます。ブートローダプロンプトにはアクセスできません。したがって、新しいパスワードを入力できません。 次のメッセージが表示されます。

  ```
  Press Enter to continue........
  ```

- **y**（yes）を入力すると、フラッシュメモリ内のコンフィギュレーションファイルおよびVLANデータベース ファイルが削除されます。 デフォルト設定がロードされるときに、パスワードをリセットできます。

ステップ 1 パスワード回復手順の継続を選択すると、既存の設定が失われます。

```
Would you like to reset the system back to the default configuration (y/n)? Y
```

ステップ 2 フラッシュ メモリの内容を表示します。

```
Switch: dir flash:
```

スイッチのファイル システムが表示されます。

```
Directory of flash:
   13  drwx         192   Mar 01 2013 22:30:48  c2960x-universalk9-mz.150-2.0.63.UCP.bin
16128000 bytes total (10003456 bytes free)
```

ステップ 3 システムを起動します。

```
Switch: boot
```

セットアップ プログラムを起動するように求められます。 パスワード回復手順を継続するには、プロンプトに **N** を入力します。

```
Continue with the configuration dialog? [yes/no]: N
```

ステップ 4 スイッチ プロンプトで、特権 EXEC モードを開始します。

```
Switch> enable
```

ステップ 5 グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 6 パスワードを変更します。

```
Switch(config)# enable secret password
```

シークレット パスワードは 1 ～ 25 文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 7 特権 EXEC モードに戻ります。

```
Switch(config)# exit
Switch#
```

ステップ 8 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Switch# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。

ステップ 9 ここでスイッチを再設定する必要があります。 システム管理者によって、バックアップスイッチとVLAN コンフィギュレーション ファイルが使用可能に設定されている場合は、これらを使用します。

コマンド スイッチで障害が発生した場合の回復

ここでは、コマンドスイッチで障害が発生した場合の回復手順について説明します。 ホットスタンバイ ルータ プロトコル（HSRP）を使用すると、冗長コマンド スイッチ グループを設定できます。

スタンバイ コマンド スイッチが未設定で、かつコマンド スイッチで電源故障などの障害が発生した場合には、メンバスイッチとの管理接続が失われるので、新しいコマンドスイッチに交換する必要があります。 ただし、接続されているスイッチ間の接続は影響を受けません。また、メンバ スイッチも通常どおりにパケットを転送します。 メンバ スイッチは、コンソール ポートを介してスタンドアロンのスイッチとして管理できます。また、IPアドレスが与えられている場合は、他の管理インターフェイスを使用して管理できます。

コマンド対応メンバ スイッチまたは他のスイッチに IP アドレスを割り当て、コマンド スイッチのパスワードを書き留め、メンバスイッチと交換用コマンドスイッチ間の冗長接続が得られるようにクラスタを配置することにより、コマンドスイッチ障害に備えます。 ここでは、故障したコマンド スイッチの交換方法を 2 通り紹介します。

- 故障したコマンド スイッチをクラスタ メンバーと交換する場合
- 故障したコマンド スイッチを他のスイッチと交換する場合

ここで紹介する回復手順を実行するには、スイッチを直接操作してください。 コマンド対応スイッチについては、リリース ノートを参照してください。

故障したコマンド スイッチをクラスタ メンバーと交換する場合

故障したコマンドスイッチを同じクラスタ内のコマンド対応メンバスイッチに交換するには、次の手順に従ってください。

ステップ 1 メンバスイッチからコマンドスイッチを外し、クラスタからコマンドスイッチを物理的に取り外します。

ステップ 2 故障したコマンド スイッチの代わりに新しいメンバ スイッチを取り付け、コマンド スイッチとクラスタ メンバ間の接続を復元します。

ステップ 3 新しいコマンド スイッチで CLI セッションを開始します。
CLI にはコンソール ポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet を使用してアクセスできます。 コンソール ポートの詳しい使用方法については、*Catalyst 2960-X Switch Hardware Installation Guide*を参照してください。*Catalyst 3560-CX and 2960-CX Switch Hardware Installation Guide*

ステップ 4 スイッチ プロンプトで、特権 EXEC モードを開始します。

例：
```
Switch> enable
Switch#
```

ステップ 5 故障したコマンド スイッチのパスワードを入力します。

ステップ 6 グローバル コンフィギュレーション モードを開始します。

例：
```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
```

ステップ 7 クラスタからメンバスイッチを削除します。

例：
```
Switch(config)# no cluster commander-address
```

ステップ 8 特権 EXEC モードに戻ります。

例：
```
Switch(config)# end
Switch#
```

ステップ 9 セットアップ プログラムを使用して、スイッチの IP 情報を設定します。 IP アドレス情報およびパスワードを入力するように要求されます。 特権 EXEC モードで **setup** と入力し、[Return] キーを押します。

例：
```
Switch# setup

 --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
```

```
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]:
```

ステップ 10 最初のプロンプトに **Y** を入力します。

例：

```
The prompts in the setup program vary depending on the member switch that you selected to be the
command switch:
Continue with configuration dialog? [yes/no]: y

or

Configuring global parameters:
```

このプロンプトが表示されなければ、**enable** と入力し、Return を押してください。 セットアップ プログラムを開始するには、**setup** と入力し、Return を押してください。

ステップ 11 セットアップ プログラムの質問に応答します。
ホスト名を入力するように要求された場合、メンバ スイッチで入力できる文字数は 28 ~ 31 文字に制限されます。 どのスイッチでも、ホスト名の最終文字として *-n*（*n* は数字）を使用しないでください。 Telnet（仮想端末）パスワードを入力するように要求された場合、パスワードには 1 ～ 25 文字の英数字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 12 **enable secret** および **enable** パスワードを入力するように要求された場合、故障したコマンド スイッチのパスワードを再び入力します。

ステップ 13 要求された場合は、スイッチをクラスタ コマンド スイッチとしてイネーブルにすることを確認し、Return を押します。

ステップ 14 要求された場合は、クラスタに名前を指定し、Return を押します。
クラスタ名には 1 ～ 31 文字の英数字、ダッシュ、または下線を使用できます。

ステップ 15 初期設定が表示されたら、アドレスが正しいことを確認してください。

ステップ 16 表示された情報が正しい場合は、**Y** を入力し、Return を押します。
情報に誤りがある場合には、**N** を入力し、[Return] キーを押して、ステップ 9 からやり直します。

ステップ 17 ブラウザを起動し、新しいコマンド スイッチの IP アドレスを入力します。

ステップ 18 クラスタ メニューから [Add to Cluster] を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

故障したコマンド スイッチを他のスイッチと交換する場合

故障したコマンド スイッチを、クラスタに組み込まれていないコマンド対応スイッチと交換する場合、次の手順に従ってください。

ステップ 1 故障したコマンド スイッチの代わりに新しいスイッチを取り付け、コマンド スイッチとクラスタ メンバ間の接続を復元します。

ステップ 2 CLI にはコンソール ポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet を使用してアクセスできます。 コンソール ポートの詳しい使用方法については、スイッチのハードウェア インストレーション ガイドを参照してください。

ステップ 3 スイッチ プロンプトで、特権 EXEC モードを開始します。

例：

```
Switch> enable
Switch#
```

ステップ 4 故障したコマンド スイッチのパスワードを入力します。

ステップ 5 セットアップ プログラムを使用して、スイッチの IP 情報を設定します。 IP アドレス情報およびパスワードを入力するように要求されます。 特権 EXEC モードで **setup** と入力し、[Return] キーを押します。

例：

```
Switch# setup

 --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]:
```

ステップ 6 最初のプロンプトに **Y** を入力します。

例：

```
The prompts in the setup program vary depending on the member switch that you selected to be the
command switch:
Continue with configuration dialog? [yes/no]: y

or

Configuring global parameters:
```

このプロンプトが表示されなければ、**enable** と入力し、Return を押してください。 セットアップ プログラムを開始するには、**setup** と入力し、Return を押してください。

ステップ 7 セットアップ プログラムの質問に応答します。
ホスト名を入力するように要求された場合、メンバ スイッチで入力できる文字数は 28 ~ 31 文字に制限されます。 どのスイッチでも、ホスト名の最終文字として *-n*（*n* は数字）を使用しないでください。 Telnet

（仮想端末）パスワードを入力するように要求された場合、パスワードには 1 ～ 25 文字の英数字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 8 **enable secret** および **enable** パスワードを入力するように要求された場合、故障したコマンドスイッチのパスワードを再び入力します。

ステップ 9 要求された場合は、スイッチをクラスタ コマンドスイッチとしてイネーブルにすることを確認し、Return を押します。

ステップ 10 要求された場合は、クラスタに名前を指定し、Return を押します。
クラスタ名には 1 ～ 31 文字の英数字、ダッシュ、または下線を使用できます。

ステップ 11 初期設定が表示されたら、アドレスが正しいことを確認してください。

ステップ 12 表示された情報が正しい場合は、**Y** を入力し、Return を押します。
情報に誤りがある場合には、**N** を入力し、[Return] キーを押して、ステップ 9 からやり直します。

ステップ 13 ブラウザを起動し、新しいコマンド スイッチの IP アドレスを入力します。

ステップ 14 クラスタ メニューから [Add to Cluster] を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

自動ネゴシエーションの不一致の防止

IEEE 802.3ab 自動ネゴシエーション プロトコルは速度（10 Mbps、100 Mbps、および SFP モジュール ポート以外の 1000 Mbps）およびデュプレックス（半二重または全二重）に関するスイッチの設定を管理します。 このプロトコルは設定を適切に調整しないことがあり、その場合はパフォーマンスが低下します。 不一致は次の条件で発生します。

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動で設定された速度またはデュプレックスのパラメータと異なっている場合。
- ポートを自動ネゴシエーションに設定したが、接続先ポートは自動ネゴシエーションを使用しない全二重に設定されている場合。

スイッチのパフォーマンスを最大限に引き出してリンクを確保するには、次のいずれかの注意事項に従って、デュプレックスおよび速度の設定を変更してください。

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 接続の両側でポートの速度とデュプレックスのパラメータを手動で設定します。

（注） 接続先装置が自動ネゴシエーションを実行しない場合は、2 つのポートのデュプレックス設定を一致させます。 速度パラメータは、接続先のポートが自動ネゴシエーションを実行しない場合でも自動調整が可能です。

SFP モジュールのセキュリティと識別に関するトラブルシューティング

シスコの Small Form-Factor Pluggable（SFP）モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリティ コード、および巡回冗長検査（CRC）が格納されたシリアル EEPROM（電気的に消去可能でプログラミング可能な ROM）を備えています。 スイッチに SFP モジュールを装着すると、スイッチ ソフトウェアは、EEPROM を読み取ってシリアル番号、ベンダー名、およびベンダー ID を確認し、セキュリティ コードおよび CRC を再計算します。 シリアル番号、ベンダー名、ベンダー ID、セキュリティ コード、または CRC が無効な場合、ソフトウェアは、セキュリティ エラー メッセージを生成し、インターフェイスを errdisable ステートにします。

（注） セキュリティ エラー メッセージは、GBIC_SECURITY 機能を参照します。 スイッチは、SFP モジュールをサポートしていますが、GBIC（ギガビット インターフェイス コンバータ）モジュールはサポートしていません。 エラー メッセージ テキストは、GBIC インターフェイスおよびモジュールを参照しますが、セキュリティ メッセージは、実際は SFP モジュールおよびモジュール インターフェイスを参照します。

他社の SFP モジュールを使用している場合、スイッチから SFP モジュールを取り外し、シスコのモジュールに交換します。 シスコの SFP モジュールを装着したら、**errdisable recovery cause gbic-invalid** グローバル コンフィギュレーション コマンドを使用してポート ステータスを確認し、error-disabled ステートから回復する時間間隔を入力します。 この時間間隔が経過すると、スイッチは error-disabled ステートからインターフェイスを復帰させ、操作を再試行します。 **errdisable recovery** コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

モジュールがシスコ製 SFP モジュールとして識別されたにもかかわらず、システムがベンダーデータ情報を読み取ってその情報が正確かどうかを確認できないと、SFP モジュール エラー メッセージが生成されます。 この場合、SFP モジュールを取り外して再び装着してください。 それでも障害が発生する場合は、SFP モジュールが不良品である可能性があります。

SFP モジュール ステータスのモニタリング

show interfaces transceiver 特権 EXEC コマンドを使用すると、SFP モジュールの物理または動作ステータスを確認できます。 このコマンドは、温度や特定のインターフェイス上の SFP モジュールの現状などの動作ステータスと、アラーム ステータスを表示します。 また、このコマンドを使用して SFP モジュールの速度およびデュプレックス設定も確認できます。 詳細については、このリリースのコマンド リファレンスに記載された **show interfaces transceiver** コマンドの説明を参照してください。

ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティック ルートを定義するか、またはこれらのサブネット間でルーティングされるように IP ルーティングを設定する必要があります。

IP ルーティングは、デフォルトではすべてのスイッチでディセーブルになります。

（注） **ping** コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

このコマンドは、スイッチからネットワーク上の他のデバイスに ping を実行する目的で使用します。

コマンド	目的
ping ip*host* | *address* `Switch# ping 172.20.52.3`	IP またはホスト名やネットワーク アドレスを指定してリモート ホストに ping を実行します。

関連トピック

ping, （1913 ページ）
例：IP ホストの ping, （1942 ページ）

温度のモニタリング

スイッチは温度条件をモニタし、温度情報を使用してファンを制御します。

温度の値、状態、しきい値を表示するには、**show env temperature status** 特権 EXEC コマンドを使用します。 温度の値は、スイッチ内の温度であり、外部の温度ではありません。**system env temperature threshold yellow** *value* グローバル コンフィギュレーション コマンドを使用してイエローのしきい値レベル（摂氏）だけを設定し、イエローのしきい値およびレッドのしきい値の差を設定できます。 グリーンまたはレッドのしきい値は設定できません。 詳細については、このリリースのコマンド リファレンスを参照してください。

物理パスのモニタリング

次のいずれかの特権 EXEC コマンドを使用して、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスをモニタできます。

表 *169*：物理パスのモニタリング

コマンド	目的
tracetroute mac [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]	指定の送信元 MAC アドレスから、指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示します。

コマンド	目的
tracetroute mac ip {*source-ip-address* | *source-hostname*}{*destination-ip-address* | *destination-hostname*} [**detail**]	指定の送信元IPアドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示します。

IP traceroute の実行

（注） **traceroute** 特権 EXEC コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

コマンド	目的
traceroute ip*host* `Switch# traceroute ip 192.51.100.1`	ネットワーク上でパケットが通過するパスを追跡します。

関連トピック

IP Traceroute, （1915 ページ）
例：IP ホストに対する traceroute の実行, （1943 ページ）

TDR の実行および結果の表示

TDR を実行する場合、**test cable-diagnostics tdr interface***interface-id* 特権 EXEC コマンドを入力します。

TDR の結果を表示するには、**show cable-diagnostics tdr interface***interface-id* 特権 EXEC コマンドを入力します。

デバッグおよびエラー メッセージ出力のリダイレクト

ネットワーク サーバはデフォルトで、**debug** コマンドおよびシステム エラー メッセージの出力をコンソールに送信します。 このデフォルトの設定を使用する場合は、コンソール ポートまたはイーサネット管理ポートに接続する代わりに、仮想端末接続によってデバッグ出力をモニタできます。

指定できる宛先として、コンソール、仮想端末、内部バッファ、および syslog サーバを実行している UNIX ホストがあります。 Syslog フォーマットは、4.3 BSD UNIX およびそのバリエーションと互換性があります。

（注） デバッグの出力先がシステムのオーバーヘッドに影響を与えることがないように注意してください。 メッセージをコンソールに記録すると、非常に高いオーバーヘッドが発生します。 仮想端末にメッセージを記録すると、発生するオーバーヘッドは低くなります。 Syslog サーバでメッセージ ロギングを行うと、オーバーヘッドはさらに小さくなり、内部バッファであれば最小限ですみます。

システム メッセージのロギングに関する詳細については、「システム メッセージ ロギングの設定」を参照してください。

関連トピック

debug コマンド, （1917 ページ）

show platform forward コマンドの使用

show platform forward 特権 EXEC コマンドの出力からは、インターフェイスに入るパケットがシステムを介して送信された場合、転送結果に関して、有意義な情報がいくつか得られます。 パケットに関して入力されたパラメータに応じて、参照テーブル結果、転送宛先の計算に使用されるポート マップ、ビットマップ、および出力側の情報が表示されます。

このコマンドで出力される情報のほとんどは、主に、スイッチの用途別集積回路（ASIC）に関する詳細情報を使用するテクニカルサポート担当者に役立つものです。 ただし、パケット転送情報はトラブルシューティングにも役立ちます。

OBFL の設定

注意 OBFL はディセーブルにせず、フラッシュ メモリに保存されたデータは削除しないことを推奨します。

- OBFL をイネーブルにするには、**hw-switch switch** [*switch-number*] **logging onboard** [**message level***level*] グローバル コンフィギュレーション コマンドを使用します。 スイッチの場合、*switch-number* に指定できる範囲は 1 ～ 9 です。 スイッチが生成してフラッシュ メモリに保存するハードウェア関連のメッセージの重大度を指定するには、**message level***level* パラメータを使用します。
- OBFL データをローカル ネットワークまたは指定したファイル システムにコピーするには、**copy onboard switch***switch-number***url***url-destination* 特権 EXEC コマンドを使用します。
- OBFL をディセーブルにするには、**no hw-switch switch** [*switch-number*] **logging onboard** [**message level**] グローバル コンフィギュレーション コマンドを使用します。
- フラッシュ メモリ内の稼働時間と CLI コマンド情報以外のすべての OBFL データをクリアするには、**clear onboard switch***switch-number* 特権 EXEC コマンドを使用します。

- アクティブ スイッチのメンバ スイッチの OBFL をイネーブルまたはディセーブルにできます。

ここで説明した各コマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

関連トピック

スイッチのオンボード障害ロギング, （1917 ページ）

OBFL 情報の表示

ソフトウェア設定のトラブルシューティングの確認

OBFL 情報の表示

表 *170* : *OBFL* 情報を表示するためのコマンド

コマンド	目的
show logging onboard [**module**[*switch-number*]]**clilog** `Switch# show logging onboard  1 clilog`	スタンドアロン スイッチまたはで入力された OBFL CLI コマンドを表示します。
show logging onboard [**module**[*switch-number*]] **environment** `Switch# show logging onboard 1 environment`	スタンドアロン スイッチおよび接続されているすべての FRU デバイスの UDI 情報、PID、VID、およびシリアル番号を表示します。
show logging onboard [**module**[*switch-number*]] **message** `Switch# show logging onboard 1 message`	スタンドアロン スイッチによって生成されたハードウェア関連のメッセージを表示します。
show logging onboard [**module**[*switch-number*]] **poe** `Switch# show logging onboard 1 poe`	スタンドアロン スイッチの PoE ポートの消費電力を表示します。
show logging onboard [**module**[*switch-number*]] **temperature** `Switch# show logging onboard 1 temperature`	スタンドアロン スイッチの温度を表示します。

コマンド	目的
show logging onboard [**module**[*switch-number*]] **uptime** `Switch# show logging onboard 1 uptime`	スタンドアロンスイッチまたは指定されたスタックメンバが起動した時刻、スタンドアロンスイッチまたは指定されたスタックメンバが再起動された理由、およびスタンドアロンスイッチが最後に再起動されて以来の稼働時間を表示します。
show logging onboard [**module**[*switch-number*]] **voltage** `Switch# show logging onboard 1 voltage`	スタンドアロンスイッチのシステム電圧を表示します。
show logging onboard [**module**[*switch-number*]] **continuous** `Switch# show logging onboard 1 continuous`	連続ファイルのデータを表示します。
show logging onboard [**module**[*switch-number*]] **detail** `Switch# show logging onboard 1 detail`	連続データおよびサマリーデータの両方を表示します。

show logging onboard [**module**[*switch-number*]] **end***hh:mm:ss*
`Switch# show logging onboard 1`
`end 13:00:15 jul 2013`
	スタンドアロンスイッチの終了日時を表示します。

show logging onboard [**module**[*switch-number*]]
`Switch# show logging`
`onboard 1`
	システム内で指定されているスイッチに関する OBFL 情報を表示します。

show logging onboard [**module**[*switch-number*]] **raw**
`Switch# show logging`
`onboard 1 raw`
	スタンドアロンスイッチの raw 情報を表示します。

show logging onboard [**module**[*switch-number*]] **start**
`Switch# show logging`
`onboard 1 start  13:00:10 jul 2013`
	スタンドアロンスイッチの開始日時を表示します。

show logging onboard [**module**[*switch-number*]] **status** `Switch# show logging onboard 1 status`	スタンドアロンスイッチのステータス情報を表示します。
show logging onboard [**module**[*switch-number*]] **summary** `Switch# show logging onboard 1 summary`	サマリーファイルの両方のデータを表示します。

例：高い CPU 使用率に関する問題と原因の確認

CPU 使用率が高いことが問題となっているかどうか判別するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。 出力例の 1 行目にある下線が付いた部分に注目してください。

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

この例は、正常な CPU 使用率を示しています。 この出力によると、最後の 5 秒間の使用率が 8%/0% となっていますが、この意味は次のとおりです。

- Cisco IOS の処理時間と割り込みの処理にかかった時間を合わせた CPU の合計の使用率は全体の 8%
- 割り込みの処理にかかった時間は全体の 0%

表 *171*：*CPU* 使用率に関する問題のトラブルシューティング

問題のタイプ	Cause	修正措置
割り込みのパーセント値が合計の CPU 使用率の値とほぼ同程度に高い	CPU がネットワークから受信するパケット数が多すぎる。	ネットワーク パケットのソースを判別する。 データの流れを遮断するか、スイッチの設定を変更します。 「Analyzing Network Traffic（ネットワークトラフィックの解析）」の項を参照してください。
割り込みの所要時間は最小限であったにもかかわらず CPU の合計使用率が 50% を超える	CPU 時間を過度に消費する Cisco IOS 処理が 1 つ以上存在する。 これは通常、処理をアクティブ化するイベントによって始動されます。	異常なイベントを特定して根本的な原因を解消する。 「Debugging Active Processes（アクティブなプロセスのデバッグ）」のセクションを参照してください。

ソフトウェア設定のトラブルシューティングのシナリオ

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

表 *172*：*Power over Ethernet* に関するトラブルシューティングのシナリオ

症状または問題	考えられる原因と解決法
PoE がないポートは 1 つに限りません。 1 つのスイッチ ポートに限り問題が発生する。 このポートでは PoE 装置と PoE 非対応の装置のいずれも動作しないが、他のポートでは動作します。	この受電デバイスが他の PoE ポートで動作するかを確認する。 **show run**、または **show interface status** ユーザ EXEC コマンドを使用して、ポートがシャットダウンしていないか、または error-disabled になっていないかを確認します。 （注） ほとんどのスイッチはポートがシャットダウンしているときはポートの電力供給をオフにします。これは、IEEE 仕様でこれがオプションに指定されている場合も同様です。 受電デバイスからスイッチ ポートまでのイーサネット ケーブルの動作が正常であることを確認します。具体的には、既知の正常な PoE 非対応のイーサネット装置とイーサネット ケーブルを接続して、受電デバイスがリンクを確立し他のホストとトラフィックを交換することを確認します。 スイッチのフロント パネルから受電デバイスまでのケーブル長の合計が 100 メートル以下であることを確認します。 スイッチ ポートからイーサネット ケーブルを外します。 短いイーサネット ケーブルを使用して、既知の正常なイーサネット装置を、スイッチのフロント パネルの（パッチ パネルではない）このポートに直接接続します。 これによってイーサネット リンクが確立され他のホストとトラフィックを交換できることを確認します。あるいは、ポートの VLAN SVI で ping を実行してください。 次に、受電デバイスをこのポートに接続し、電源がオンになることを確認します。 パッチ コードをスイッチ ポートに接続しても受電デバイスの電源がオンにならない場合、接続する受電デバイスの合計数とスイッチの電力バジェット（使用可能な PoE）とを比較してください。 **show inline power** コマンドを使用して利用可能な電力量を確認します。

症状または問題	考えられる原因と解決法
すべてのポートまたは 1 つのポートグループでPoEが機能しない。 すべてのスイッチポートで問題が発生する。電力が供給されていないイーサネット装置がどのポートでもイーサネットリンクを確立できず、PoE 装置の電源がオンになりません。	

症状または問題	考えられる原因と解決法
	電力に関するアラームが継続的に発生する、断続的に発生する、または再発する場合は、可能であれば電源モジュールを交換します（現場交換可能ユニットです）。 そうでない場合はスイッチを交換してください。 連続する複数のポートで問題があるものの、すべてのポートで問題が発生するわけではない場合、電源の故障ではないと考えられ、スイッチのPoEレギュレータに関連した異常の可能性があります。 PoEの状況やステータスの変更について過去に報告されているアラームまたはシステムメッセージを確認するには、**show log** 特権 EXEC コマンドを使用します。 アラームがない場合は、**show interface status** コマンドを使用して、ポートがシャットダウンしていないかerrdisableになっていないかを確認します。 ポートが error-disabled の場合、**shut** および **no shut** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。 特権 EXEC コマンドの **show env power** および **show power inline** を使用して、PoE のステータスおよび電力バジェット（使用可能な PoE）を調べます。 実行コンフィギュレーションを調べて **power inline never** がこのポートに設定されていないことを確認します。 受電していないイーサネット装置をスイッチ ポートに直接接続します。 接続には短いパッチ コードだけを使用します。 既存の配線ケーブルは使用しないでください。 **shut** および **no shut** インターフェイス コンフィギュレーション コマンドを入力し、イーサネット リンクが確立されていることを確認します。 正しく接続している場合、短いパッチ コードを使用して受電デバイスをこのポートに接続し、電源がオンになることを確認します。 装置の電源がオンになったら、すべての中間パッチ パネルが正しく接続されているか確認してください。 1 本を除くすべてのイーサネット ケーブルをスイッチ ポートから抜きます。 短いパッチ コードを使用して、1 つの PoE ポートにだけ受電デバイスを接続します。 スイッチ ポートからの受電に比較して、受電デバイスが多くの電力を必要としないことを確認してください。 **show power inline** 特権 EXEC コマンドを使用して、ポートがシャットダウンしていない場合に、受電デバイスに電力が供給されることを確認します。 あるいは、受電デバイスを観察して電源がオンになることを確認してください。

症状または問題	考えられる原因と解決法
	1 台の受電デバイスだけがスイッチに接続しているときに電力が供給される場合、残りのポートで **shut** および **no shut** インターフェイス コンフィギュレーション コマンドを入力してから、イーサネット ケーブルをスイッチの PoE ポートに 1 本ずつ再び接続してください。 show interface status および **show power inline** 特権 EXEC コマンドを使用して、インライン電力統計およびポート ステータスをモニタします。 すべてのポートで、まだPoEが機能しない場合は、電源装置のPoEセクションでヒューズを開くことができる場合があります。 この場合、アラームが生成されるのが一般的です。過去にシステム メッセージでアラームが報告されていないか、ログをもう一度チェックしてください。
Cisco IP Phone が切断またはリセットされる。 正常に動作した後で、Cisco phone またはワイヤレスアクセスポイントが断続的にリロードしたり、PoE から切断されたりします。	スイッチから受電デバイスまでのすべての電気系統を確認してください。 信頼性の低い接続は、電力供給の中断や受電デバイスの機能が不安定になる原因となり、受電デバイスの断続的な切断やリロードなどが発生します。 スイッチ ポートから受電デバイスまでのケーブル長が 100 メートル以下であることを確認してください。 スイッチが配置されている場所で電気環境にどのような変化があるか、切断時に、受電デバイスに何が起きるかについて注意してください。 切断と同時にエラー メッセージが表示されたか注意します。 **show log** 特権 EXEC コマンドを使用してエラー メッセージを確認します。 リロードの発生直前に IP Phone から Call Manager へのアクセスが失われていないか確認してください（PoE の障害ではなくネットワークに問題が発生している場合があります）。 受電デバイスを PoE 非対応の装置に交換し、装置が正しく動作することを確認します。 PoE 非対応の装置にリンク障害または高いエラー率がある場合、スイッチ ポートと受電デバイスを接続する信頼性の低いケーブル接続が問題の可能性があります。

症状または問題	考えられる原因と解決法
シスコ以外の受電デバイスがシスコ PoE スイッチで動作しない。 シスコ PoE スイッチに接続するシスコ以外の受電デバイスに電源が供給されないか、電源投入後すぐに電源が切れます。 PoE 非対応装置は正常に動作します。	**show power inline** コマンドを使用して、受電デバイスの接続前後に、スイッチの電力バジェット（使用可能な PoE）が使い果たされていないか確認してください。 受電デバイスを接続する前に、このタイプの装置に十分な電力が使用可能であることを確認します。 **show interface status** コマンドを使用して、接続されている受電デバイスをスイッチが検出することを確認します。 **show log** コマンドを使用して、ポートの過電流状態を報告したシステム メッセージがないか確認します。 症状を正確に特定してください。最初に電力が受電デバイスに供給され、その後、切断される状態ですか。 その場合は、問題は最初のサージ電流（突入電流）が原因で、ポートの電流上限しきい値が超過した可能性があります。

関連トピック

Power over Ethernet（PoE）ポート，（1912 ページ）

ソフトウェアのトラブルシューティングの設定例

例：IP ホストの ping

次に、IP ホストに ping を実行する例を示します。

```
Switch# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#
```

表 *173*：*ping* の出力表示文字

文字	説明
!	感嘆符 1 個につき 1 回の応答を受信したことを示します。
.	ピリオド 1 個につき応答待ちの間にネットワーク サーバのタイムアウトが 1 回発生したことを示します。

文字	説明
U	宛先到達不能エラー PDU を受信したことを示します。
C	輻輳に遭遇したパケットを受信したことを示します。
I	ユーザによりテストが中断されたことを示します。
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

ping セッションを終了するには、エスケープ シーケンス（デフォルトでは Ctrl+^ X）を入力してください。 Ctrl キー、Shift キー、および 6 キーを同時に押してから放し、その後 X キーを押します。

関連トピック

ping, （1913 ページ）
ping の実行, （1931 ページ）

例：IP ホストに対する traceroute の実行

次に、IP ホストに **traceroute** を実行する例を示します。

```
Switch# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

  1 192.0.2.1 0 msec 0 msec 4 msec
  2 192.0.2.203 12 msec 8 msec 0 msec
  3 192.0.2.100 4 msec 0 msec 0 msec
  4 192.0.2.10 0 msec 4 msec 0 msec
```

ディスプレイには、送信される 3 つのプローブごとに、ホップ カウント、ルータの IP アドレス、およびラウンドトリップ タイム（ミリ秒単位）が表示されます。

表 *174*：*traceroute* の出力表示文字

文字	説明
*	プローブがタイムアウトになりました。
?	パケット タイプが不明です。

文字	説明
A	管理上、到達不能です。 通常、この出力は、アクセスリストがトラフィックをブロックしていることを表しています。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	発信元。
U	ポートが到達不能です。

実行中の追跡を終了するには、エスケープ シーケンス（デフォルトでは Ctrl+^ X）を入力してください。 Ctrl キー、Shift キー、および 6 キーを同時に押してから放し、その後 X キーを押します。

関連トピック

IP Traceroute, （1915 ページ）
IP traceroute の実行, （1933 ページ）

例：すべてのシステム診断をイネーブルにする

注意 デバッグ出力は他のネットワーク トラフィックより優先され、**debug all** 特権 EXEC コマンドは他の **debug** コマンドより出力が大量になるので、スイッチのパフォーマンスが極度に低下したり、場合によっては使用不能になったりすることがあります。 状況にかかわらず、特定性の高い **debug** コマンドを使用するのが原則です。

このコマンドは、すべてのシステム診断をディセーブルにします。

```
Switch# debug all
```

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。いずれかの **debug** コマンドが誤ってイネーブルのままにならないようにするには、**no debug all** コマンドを使用すると便利です。

関連トピック

debug コマンド, （1917 ページ）

第 XI 部

VLAN

- VTP の設定，1947 ページ
- VLAN の設定，1975 ページ
- VLAN トランクの設定，1997 ページ
- VMPS の設定，2021 ページ
- 音声 VLAN の設定，2037 ページ
- プライベート VLAN の設定，2049 ページ

第 73 章

VTP の設定

- 機能情報の確認，1947 ページ
- VTP の前提条件，1947 ページ
- VTP の制約事項，1948 ページ
- VTP の概要，1948 ページ
- VTP の設定方法，1958 ページ
- VTP のモニタ，1971 ページ
- VTP の設定例，1971 ページ
- 次の作業，1973 ページ

機能情報の確認

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

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

VTP の前提条件

VLAN を作成する前に、ネットワークで VLAN Trunking Protocol（VTP）を使用するかどうかを決定する必要があります。 VTP を使用すると、1 つまたは複数のスイッチ上で中央集約的に設定変更を行い、その変更を自動的にネットワーク上の他のスイッチに伝達できます。 VTP を使用しない場合、VLAN 情報を他のスイッチに送信することはできません。

VTP は、1 つのスイッチで行われた更新が VTP を介してドメイン内の他のスイッチに送信される環境で動作するように設計されています。 VLAN データベースに対する複数の更新が同一ドメイン内のスイッチ上で同時に発生する環境の場合、VTP は適切に機能せず、VLAN データベースの不整合が生じます。

スイッチは合計 1000 の VLAN をサポートします。 ただし、ルーテッド ポート、SVI、およびその他の設定済み機能の個数によって、スイッチハードウェアの使用状況は左右されます。 VTP が新しい VLAN をスイッチに通知し、スイッチが使用可能な最大限のハードウェア リソースをすでに使用している場合、コントローラはハードウェア リソース不足を伝えるメッセージを送信して、VLAN をシャットダウンします。 **show vlan** ユーザ EXEC コマンドの出力に、サスペンド ステートの VLAN が示されます。

トランク ポートは VTP アドバタイズを送受信するので、スイッチ上で少なくとも 1 つのトランク ポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。 そうでない場合、スイッチは VTP アドバタイズを受信できません。

VTP の制約事項

（注） VTP クライアントスイッチを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より小さいことを確認してください。 VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。 VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。

次に、VTP を設定する際の制約事項を示します。

- 1K VLAN は Lan Base のデフォルト テンプレートが設定された LAN Base イメージを実行しているスイッチ上でのみサポートされます。
- 標準範囲の VLAN 設定の CPU 使用率が高いことを示す警告メッセージを回避するには、使用する VLAN を 256 までにすることを推奨します。

  この場合、約10 のアクセス インターフェイス、または 5つのトランク インターフェイスが同時にフラップできます。 これによる CPU 使用率への影響はごくわずかです（同時にフラップするインターフェイスが多い場合は、CPU 使用率が非常に高くなる場合があります）。

VTP の概要

VTP

VTP は、レイヤ 2 のメッセージ プロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。 VTP により、VLAN

名の重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。

VTP バージョン 1 およびバージョン 2 は、標準範囲の VLAN（VLAN ID 1 ～ 1005）だけをサポートします。 VTP バージョン 3 は、VLAN 範囲全体（VLAN 1 ～ 4094）をサポートします。 拡張範囲 VLAN（VLAN 1006 ～ 4094）は、VTP バージョン 3 でだけサポートされます。

拡張 VLAN がドメインに設定されている場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。

VTP ドメイン

VTP ドメイン（別名 VLAN 管理ドメイン）は、1 つのスイッチ、または同じ VTP ドメイン名を共有して同一管理下にある相互接続された複数のスイッチで構成されます。 スイッチは、1 つの VTP ドメインにだけ所属できます。 そのドメインに対してグローバル VLAN の設定を変更します。

デフォルトの設定では、トランク リンク（複数 VLAN のトラフィックを伝送するリンク）を介してドメインについてのアドバタイズを受信しない限り、またはユーザがドメイン名を設定しない限り、スイッチは VTP 非管理ドメイン ステートです。 管理ドメイン名を指定するか学習するまでは、VTP サーバ上で VLAN を作成または変更できません。また、VLAN 情報はネットワークを介して伝播されません。

スイッチが、トランク リンクを介して VTP アドバタイズを受信した場合、管理ドメイン名および VTP 設定のリビジョン番号を継承します。 その後スイッチは、別のドメイン名または古いコンフィギュレーション リビジョン番号が指定されたアドバタイズについては、すべて無視します。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのスイッチに伝播されます。 VTP アドバタイズは、IEEE 802.1Q を含め、すべての IEEE トランク接続に送信されます。 VTP は、複数の LAN タイプにわたり、固有の名前と内部インデックスの対応によって VLAN を動的にマッピングします。 このマッピングにより、ネットワーク管理者がデバイスを管理するための作業負担が大幅に軽減されます。

VTP トランスペアレント モードでスイッチを設定した場合、VLAN の作成および変更は可能ですが、その変更はドメイン内の他のスイッチには送信されません。また、変更が作用するのは、個々のスイッチに限られます。 ただし、スイッチがこのモードのときに設定を変更すると、変更内容がスイッチの実行コンフィギュレーションに保存されます。この変更はスイッチのスタートアップ コンフィギュレーション ファイルに保存することもできます。

関連トピック

VTP ドメインへの VTP クライアント スイッチの追加, （1968 ページ）

VTP の前提条件

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング, （2068 ページ）

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする, （2072 ページ）

VTP モード

表 *175* : *VTP* モード

VTP Mode	説明
VTP サーバ	VTP サーバ モードでは、VLAN の作成、変更、削除ができます。また、VTP ドメイン全体に対して他のコンフィギュレーション パラメータ（VTP バージョンなど）を指定できます。 VTP サーバは、同一 VTP ドメイン内の他のスイッチに自身の VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズに基づいて、自身の VLAN 設定を他のスイッチと同期させます。 VTP サーバがデフォルトのモードです。 VTP サーバ モードでは、VLAN 設定は NVRAM に保存されます。 スイッチがコンフィギュレーションを NVRAM に書き込んでいる間に障害を検出すると、VTP モードはサーバ モードからクライアント モードに自動的に移行します。 この場合、NVRAM が正常に動作するまで、スイッチを VTP サーバ モードに戻すことはできません。
VTP クライアント	VTP クライアントは VTP サーバと同様に機能し、そのトランクで VTP アップデートを送受信しますが、VTP クライアント上で VLAN の作成、変更、削除を行うことはできません。 VLAN は、ドメインに含まれる、他のサーバ モードのスイッチで設定します。 VTP バージョン 1 および 2 の VTP クライアント モードでは、VLAN 設定は NVRAM に保存されません。 VTP バージョン 3 では、VLAN 設定はクライアント モードで NVRAM に保存されます。

VTP Mode	説明
VTP トランスペアレント	VTP トランスペアレント スイッチは、VTP に参加しません。 VTP トランスペアレント スイッチは自身の VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて自身の VLAN 設定を同期させることもありません。 ただし、VTP バージョン 2 またはバージョン 3 では、トランスペアレント スイッチは、トランク インターフェイスを介して他のスイッチから受信した VTP アドバタイズを転送します。 VTP トランスペアレント モードでは、スイッチ上の VLAN を作成、変更、削除できます。 VTP バージョン 1 および 2 では、プライベート VLAN を作成するときに、スイッチは VTP トランスペアレント モードにする必要があります。また、このプライベート VLAN の設定後は VTP モードをトランスペアレント モードからクライアント モードやサーバ モードに変更しないでください。 VTP バージョン 3 では、クライアント モードとサーバ モードでもプライベート VLAN をサポートします。プライベート VLAN が設定されている場合、VTP モードをトランスペアレントからクライアント モードやサーバ モードに変更しないでください。 スイッチが VTP トランスペアレント モードの場合、VTP および VLAN の設定は NVRAM に保存されますが、他のスイッチにはアドバタイズされません。 このモードでは、VTP モードおよびドメイン名はスイッチの実行コンフィギュレーションに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。
VTP オフ	VTP オフ モードでのスイッチの機能は、トランクを介して VTP アドバタイズを転送しないことを除くと VTP トランスペアレント スイッチとしての機能と同じです。

関連トピック

VTP の前提条件
VTP モードの設定, （1958 ページ）
例：VTP サーバとしてのスイッチの設定, （1972 ページ）

VTP アドバタイズ

VTP ドメイン内の各スイッチは、専用のマルチキャスト アドレスに対して、それぞれのトランク ポートからグローバル コンフィギュレーション アドバタイズを定期的に送信します。 ネイバー スイッチは、このようなアドバタイズを受信し、必要に応じて各自の VTP および VLAN 設定をアップデートします。

トランク ポートは VTP アドバタイズを送受信するので、スイッチ スタック上で少なくとも 1 つのトランクポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接

続されていることを確認する必要があります。そうでない場合、スイッチはVTPアドバタイズを受信できません。

VTP アドバタイズにより、次のグローバル ドメイン情報が配信されます。

- VTP ドメイン名
- VTP 設定のリビジョン番号
- アップデート ID およびアップデート タイムスタンプ
- 各 VLAN の最大伝送単位（MTU）サイズを含む MD5 ダイジェスト VLAN コンフィギュレーション
- フレーム形式

VTP アドバタイズではさらに、設定されている各 VLAN について、次の VLAN 情報が配信されます。

- VLAN ID（IEEE 802.1Q を含む）
- VLAN 名
- VLAN タイプ
- VLAN ステート
- VLAN タイプ固有のその他の VLAN 設定情報

VTP バージョン 3 では、VTP アドバタイズにはプライマリ サーバ ID、インスタンス番号、および開始インデックスも含まれます。

関連トピック

VTP の前提条件

VTP バージョン 2

ネットワークで VTP を使用する場合、VTP のどのバージョンを使用するかを決定する必要があります。 デフォルトでは、バージョン 1 の VTP が動作します。

VTP バージョン 1 でサポートされず、バージョン 2 でサポートされる機能は、次のとおりです。

- トークンリング サポート：VTP バージョン 2 は、トークンリング ブリッジ リレー機能（TrBRF）およびトークンリング コンセントレータ リレー機能（TrCRF）VLAN をサポートします。
- 認識不能な Type-Length-Value（TLV）のサポート：VTP サーバまたは VTP クライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。 認識されなかった TLV は、スイッチが VTP サーバ モードで動作している場合、NVRAM に保存されます。
- バージョン依存型トランスペアレント モード：VTP バージョン 1 の場合、VTP トランスペアレント スイッチが VTP メッセージ中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限りメッセージを転送します。 VTP バージョン 2 がサ

ポートするドメインは 1 つだけですが、VTP バージョン 2 トランスペアレント スイッチは、ドメイン名が一致した場合のみメッセージを転送します。

- 整合性検査：VTP バージョン 2 の場合、CLI（コマンドライン インターフェイス）、または SNMP（簡易ネットワーク管理プロトコル）を介して新しい情報が入力された場合に限り、VLAN 整合性検査（VLAN 名、値など）を行います。 VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。 受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

関連トピック

VTP バージョンのイネーブル化, （1963 ページ）

VTP バージョン 3

VTP バージョン 1 または 2 でサポートされず、バージョン 3 でサポートされる機能は、次のとおりです。

- 拡張認証：認証を **hidden** または **secret** として設定できます。 設定を **hidden** にしている場合、パスワード文字列からの秘密キーは VLAN のデータベース ファイルに保存されますが、設定においてプレーン テキストで表示されることはありません。 代わりに、パスワードに関連付けられているキーが 16 進表記で実行コンフィギュレーションに保存されます。 ドメインにテイクオーバー コマンドを入力するときは、パスワードを再入力する必要があります。 キーワード **secret** を入力する場合、パスワードに秘密キーを直接設定できます。
- 拡張範囲 VLAN （VLAN 1006 ～ 4094）データベース伝播のサポート：VTP バージョン 1 および 2 では VLAN 1 ～ 1005 だけが伝播されます。

（注） VTP プルーニングは引き続き VLAN 1 ～ 1005 にだけ適用され、VLAN 1002 ～ 1005 は予約されたままで変更できません。

- プライベート VLAN のサポート。
- ドメイン内のデータベースのサポート：VTP 情報の伝播に加え、バージョン 3 では、Multiple Spanning Tree（MST）プロトコル データベース情報も伝播できます。 VTP プロトコルの個別インスタンスが VTP を使用する各アプリケーションで実行されます。
- VTP プライマリ サーバと VTP セカンダリ サーバ：VTP プライマリ サーバは、データベース情報を更新し、システム内のすべてのデバイスに適用されるアップデートを送信します。 VTP セカンダリ サーバで実行できるのは、プライマリ サーバから NVRAM に受け取ったアップデート済み VTP コンフィギュレーションのバックアップだけです。

  デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。 **vtp primary** 特権 EXEC コマンドを入力してプライマリ サーバを指定することができます。 プライマリ サーバのステータスは、管理者がドメインでテイクオーバー メッセージを発行する場合、データベースのアップデート用に必要となるだけです。 プライマリ サーバなしで実用 VTP ドメインを持つことができます。 プライマリ サーバのステータスは、スイッチにパスワードが設

定されている場合でも、装置がリロードしたり、ドメインのパラメータが変更したりすると失われます。

- VTP をトランク単位（ポート単位）でオンまたはオフにするオプション：ポート単位で VTP をイネーブルまたはディセーブルにするには、[**no**] **vtp** インターフェイス コンフィギュレーション コマンドを入力します。 トランク ポート上で VTP をディセーブルにすると、そのポートのすべての VTP インスタンスがディセーブルになります。 VTP の設定を、MST データベースには *off* にする一方で、同じポートの VLAN データベースには *on* にすることはできません。

  グローバルに VTP モードをオフに設定すると、システムのすべてのトランク ポートにこの設定が適用されます。 ただし、VTP インスタンス ベースでこのモードのオンまたはオフを指定することはできます。 たとえば、VLAN データベースには、スイッチを VTP サーバとして設定する一方で、MST データベースには VTP を *off* に設定することができます。

関連トピック

VTP バージョンのイネーブル化, （1963 ページ）

VTP プルーニング

VTP プルーニングを使用すると、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されるので、使用可能なネットワーク帯域幅が増えます。 VTP プルーニングを使用しない場合、スイッチは受信側のスイッチで廃棄される可能性があっても、VTP ドメイン内のすべてのトランク リンクに、ブロードキャスト、マルチキャスト、および不明のユニキャスト トラフィックをフラッディングします。 VTP プルーニングはデフォルトでディセーブルです。

VTP プルーニングは、プルーニング適格リストに指定された VLAN トランク ポートへの不要なフラッディング トラフィックを阻止します。 プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。 デフォルトでは、スイッチのトランク ポート上で VLAN 2 ～ 1001 がプルーニング適格です。 プルーニング不適格として設定した VLAN については、引き続きフラッディングが行われます。 VTP プルーニングはすべてのバージョンの VTP でサポートされます。

VTP バージョン 1 および 2 では、VTP サーバでプルーニングをイネーブルにすると、その VTP ドメイン全体でプルーニングがイネーブルになります。 VTP バージョン 3 では、ドメイン内の各スイッチ上で手動によってプルーニングをイネーブルにする必要があります。 VLAN をプルーニング適格または不適格として設定する場合、影響を受けるのは、そのトランク上の VLAN のプルーニングだけです（VTP ドメイン内のすべてのスイッチに影響するわけではありません）。

VTP プルーニングは、イネーブルにしてから数秒後に有効になります。 VTP プルーニング不適格の VLAN からのトラフィックは、プルーニングの対象になりません。 VLAN 1 および VLAN 1002 ～ 1005 は常にプルーニング不適格です。 これらの VLAN からのトラフィックはプルーニングできません。 拡張範囲 VLAN（1005 を超える VLAN ID）もプルーニング不適格です。

関連トピック

VTP プルーニングのイネーブル化, （1965 ページ）

VTP 設定時の注意事項

VTP の設定要件

VTP を設定する場合は、スイッチがドメイン内の他のスイッチと VTP アドバタイズを送受信できるように、トランク ポートを設定する必要があります。

VTP バージョン 1 および 2 ではプライベート VLAN をサポートしません。 VTP バージョン 3 ではプライベート VLAN をサポートします。 プライベート VLAN を設定した場合、スイッチは VTP トランスペアレント モードでなければなりません。 プライベート VLAN がスイッチに設定されている場合、VTP モードをトランスペアレント モードからクライアント モードやサーバ モードに変更しないでください。

VTP の設定

VTP 情報は VTP VLAN データベースに保存されます。 VTP モードがトランスペアレントである場合、VTP ドメイン名およびモードはスイッチの実行コンフィギュレーション ファイルにも保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。 スイッチをリセットした場合にも、VTP モードをトランスペアレントとして保存するには、このコマンドを使用する必要があります。

スイッチのスタートアップ コンフィギュレーション ファイルに VTP 情報を保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。 VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

関連トピック

ポート単位の VTP の設定, （1966 ページ）

VTP バージョン 3 のプライマリ サーバの設定, （1962 ページ）

VTP 設定のためのドメイン名

VTP を初めて設定するときは、必ずドメイン名を割り当てる必要があります。 また、VTP ドメイン内のすべてのスイッチを、同じドメイン名で設定しなければなりません。 VTP トランスペアレントモードのスイッチは、他のスイッチと VTP メッセージを交換しません。これらのコントローラについては VTP ドメイン名を設定する必要はありません。

（注） NVRAM および DRAM の記憶域が十分にある場合は、VTP ドメイン内のすべてのスイッチを VTP サーバ モードにする必要があります。

注意 すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメインを設定しないでください。 ドメインを設定すると、そのドメインの VLAN 設定を変更できなくなります。 VTP ドメイン内の少なくとも 1 台のスイッチを VTP サーバ モードに設定してください。

関連トピック

VTP ドメインへの VTP クライアント スイッチの追加, （1968 ページ）

VTP ドメインのパスワード

VTP ドメインのパスワードは設定できますが、必須ではありません。 ドメインパスワードを設定する場合は、すべてのドメイン スイッチで同じパスワードを共有し、管理ドメイン内のスイッチごとにパスワードを設定する必要があります。 パスワードのないスイッチ、またはパスワードが不正なコントローラは、VTP アドバタイズを拒否します。

ドメインに VTP パスワードを設定する場合、VTP 設定なしで起動したスイッチは、正しいパスワードを使用して設定しない限り、VTP アドバタイズを受信しません。 設定後、スイッチは同じパスワードおよびドメイン名を使用した次の VTP アドバタイズを受信します。

VTP 機能を持つ既存のネットワークに新しいスイッチを追加した場合、その新しいスイッチに適切なパスワードを設定して初めて、そのコントローラはドメイン名を学習します。

注意 VTP ドメイン パスワードを設定したにもかかわらず、ドメイン内の各スイッチに管理ドメイン パスワードを割り当てなかった場合には、管理ドメインが正常に動作しません。

関連トピック

VTP バージョン 3 のパスワードの設定, （1961 ページ）

例：スイッチをプライマリ サーバとして設定する, （1971 ページ）

VTP バージョン

実装する VTP バージョンを決定する場合は、次の注意事項に従ってください。

- VTP ドメイン内のすべてのスイッチは同じドメイン名を使用する必要がありますが、すべてが同じ VTP バージョンを実行する必要はありません。
- VTP バージョン 2 対応のスイッチ上で VTP バージョン 2 がディセーブルに設定されている場合、VTP バージョン 2 対応スイッチは、VTP バージョン 1 を実行しているスイッチと同じ

VTP ドメインで動作できます（デフォルトでは VTP バージョン 2 はディセーブルになっています）。

- VTP バージョン 1 を実行しているものの、VTP バージョン 2 に対応可能なスイッチが VTP バージョン 3 アドバタイズを受信すると、このコントローラは VTP バージョン 2 に自動的に移行します。
- VTP バージョン 3 を実行しているスイッチが VTP バージョン 1 を実行しているスイッチに接続すると、VTP バージョン 1 のスイッチは VTP バージョン 2 に移行し、VTP バージョン 3 のスイッチは、スケールダウンしたバージョンの VTP パケットを送信するため、VTP バージョン 2 スイッチは自身のデータベースをアップデートできます。
- VTP バージョン 3 を実行するスイッチは、拡張 VLAN を持つ場合はバージョン 1 または 2 に移行できません。
- 同一 VTP ドメイン内のすべてのスイッチがバージョン 2 に対応可能な場合を除いて、スイッチ上で VTP バージョン 2 をイネーブルにしないでください。 1 つのスイッチでバージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応スイッチでバージョン 2 がイネーブルになります。 バージョン 1 専用のスイッチがドメインに含まれている場合、そのコントローラはバージョン 2 対応スイッチとの間で VTP 情報を交換できません。
- VTP バージョン 1 および 2 スイッチは、VTP バージョン 3 アドバタイズメントを転送できないため、ネットワークのエッジに配置することをお勧めします。
- 使用環境に TrBRF および TrCRF トークンリング ネットワークが含まれている場合に、トークンリング VLAN スイッチング機能を正しく動作させるには、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。 トークンリングおよびトークンリング Net を実行する場合は、VTP バージョン 2 をディセーブルにします。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN（VLAN 1006 ～ 4094）の設定情報を伝播しません。 これらの VLAN は各装置で手動によって設定する必要があります。 VTP バージョン 3 は拡張範囲 VLAN と、拡張範囲 VLAN データベースの伝播をサポートします。
- VTP バージョン 3 装置のトランク ポートが VTP バージョン 2 装置からのメッセージを受信した場合、この装置は、VLAN データベースをスケールダウンし、その特定のトランク上で VTP バージョン 2 フォーマットを使用して送信します。 VTP バージョン 3 装置は、最初にそのトランク ポートで VTP バージョン 2 パケットを受信しない限り、VTP バージョン 2 フォーマットのパケットを送信しません。
- VTP バージョン 3 装置が、あるトランク ポートで VTP バージョン 2 装置を検出した場合、両方のネイバーが同一トランク上で共存できるように、VTP バージョン 2 パケットだけでなく VTP バージョン 3 パケットの送信も継続します。
- VTP バージョン 3 装置は、VTP バージョン 2 またはバージョン 1 の装置からの設定情報は受け入れません。
- 2 つの VTP バージョン 3 リージョンは、VTP バージョン 1 リージョンまたはバージョン 2 リージョンでは、トランスペアレント モードでだけ通信できます。
- VTP バージョン 1 にだけ対応する装置は、VTP バージョン 3 装置との相互運用はできません。

- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN（VLAN 1006 ～ 4094）の設定情報を伝播しません。 これらの VLAN を各装置上に手動で設定する必要があります。

関連トピック

VTP バージョンのイネーブル化, （1963 ページ）

VTP のデフォルト設定

次の表に、VTP のデフォルト設定を記載します。

表 *176*：*VTP* のデフォルト設定

機能	デフォルト設定
VTP ドメイン名	ヌル
VTP モード（VTP バージョン 1 およびバージョン 2）	サーバ
VTP モード（VTP バージョン 3）	このモードは、VTP バージョン 3 に変換する前のバージョン 1 または 2 のモードと同じです。
VTP バージョン	Version 1
MST データベース モード	トランスペアレント
VTP バージョン 3 のサーバ タイプ	セカンダリ
VTP パスワード	なし
VTP プルーニング	ディセーブル

VTP の設定方法

VTP モードの設定

次のいずれかに VTP モードを設定できます。

- VTP サーバ モード：VTP サーバ モードでは、VLAN の設定を変更し、ネットワーク全体に伝播させることができます。
- VTP クライアント モード：VTP クライアント モードでは、VLAN の設定を変更できません。クライアント スイッチは、VTP ドメイン内の VTP サーバから VTP アップデート情報を受信し、それに基づいて設定を変更します。

- VTP トランスペアレント モード：VTP トランスペアレント モードでは、スイッチで VTP がディセーブルになります。 スイッチは VTP アップデートを送信せず、他のスイッチから受信した VTP アップデートにも反応しません。 ただし、VTP バージョン 2 を実行する VTP トランスペアレント モードのスイッチは、対応するトランク リンクで、受信した VTP アドバタイズを転送します。
- VTP オフ モード：VTP オフ モードは、VTP アドバタイズが転送されない以外は、VTP トランスペアレント モードと同じです。

設定したドメイン名は、削除できません。別のドメインにスイッチを再び割り当てるしかありません。

手順の概要

1. **enable**
2. **configureterminal**
3. **vtp domain***domain-name*
4. **vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}
5. **vtp password***password*
6. **end**
7. **show vtp status**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp domain***domain-name* 例： `Switch(config)# vtp domain eng_group`	VTP 管理ドメイン名を設定します。 1 ～ 32 文字の名前を使用できます。 同一管理下にある VTP サーバ モードまたはクライアント モードのスイッチは、すべて同じドメイン名に設定する必要があります。 サーバ モード以外にはこのコマンドは任意です。 VTP サーバ モードではドメイン名が必要です。 スイッチが VTP ドメインにトラン

	コマンドまたはアクション	目的
		ク接続されている場合、スイッチはドメイン内の VTP サーバからドメイン名を取得します。 他の VTP パラメータを設定する前に、VTP ドメインを設定する必要があります。 （注）
ステップ 4	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**} 例： `Switch(config)# vtp mode server`	VTP モード（クライアント、サーバ、トランスペアレント、またはオフ）のスイッチの設定。 • **vlan**：何も設定されていない場合は VLAN データベースがデフォルトです。 • **mst**：マルチ スパニング ツリー（MST）データベース。 • **unknown**：データベース タイプは不明。
ステップ 5	**vtp password***password* 例： `Switch(config)# vtp password mypassword`	（任意）VTP ドメイン用のパスワードを設定します。 パスワードに使用できる文字数は 8 ～ 64 文字です。 VTP パスワードを設定したにもかかわらず、ドメイン内の各スイッチに同じパスワードを割り当てなかった場合には、VTP ドメインが正常に動作しません。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show vtp status** 例： `Switch# show vtp status`	表示された *[VTP Operating Mode]* および *[VTP Domain Name]* フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）スタートアップ コンフィギュレーション ファイルに設定を保存します。 スイッチの実行コンフィギュレーションに保存され、スタートアップ コンフィギュレーション ファイルにコピーできるのは、VTP モードおよびドメイン名だけです。

関連トピック

VTP モード，（1950 ページ）

例：VTP サーバとしてのスイッチの設定，（1972 ページ）

VTP バージョン 3 のパスワードの設定

スイッチで VTP バージョン 3 のパスワードを設定できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vtp password***password* [**hidden** | **secret**]
4. **end**
5. **show vtp password**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp password***password* [**hidden** | **secret**] 例： `Switch(config)# vtp password mypassword hidden`	（任意）VTP ドメイン用のパスワードを設定します。 パスワードに使用できる文字数は 8 ～ 64 文字です。 • （任意）**hidden**：パスワード文字列から生成される秘密キーが、nvram:vlan.dat ファイルに保存されます。 VTP プライマリ サーバを設定してテイクオーバーを設定しようとすると、パスワードの再入力を要求されます。 • （任意）**secret**：パスワードを直接設定します。 シークレット パスワードには 16 進数文字を 32 個含める必要があります。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp password** 例： `Switch# show vtp password`	入力を確認します。 次のような出力が表示されます。 VTP password: 89914640C8D90868B6A0D8103847A733
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VTP ドメインのパスワード，（1956 ページ）
例：スイッチをプライマリ サーバとして設定する，（1971 ページ）

VTP バージョン 3 のプライマリ サーバの設定

VTP サーバを VTP プライマリ サーバとして設定すると、テイクオーバー操作が開始されます。

手順の概要

1. **vtp primary** [**vlan** | **mst**] [**force**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vtp primary** [**vlan** | **mst**] [**force**] 例： `Switch# vtp primary vlan force`	スイッチの動作ステートをセカンダリ サーバ（デフォルト）からプライマリ サーバに変更し、その設定をドメインにアドバタイズします。 スイッチのパスワードが **hidden** に設定されている場合は、パスワードの再入力を要求されます。 • （任意）**vlan**：テイクオーバー機能として VLAN データベースを選択します。 これはデフォルトです。

	コマンドまたはアクション	目的
		• （任意）**mst**：テイクオーバー機能としてマルチ スパニング ツリー（MST）データベースを選択します。 • （任意）**force**：競合するサーバの設定が上書きされます。 **force** を入力しない場合、テイクオーバーの実行前に確認を求められます。

関連トピック

VTP の設定, （1955 ページ）

VTP バージョンのイネーブル化

デフォルトで VTP バージョン 2 およびバージョン 3 はディセーブルになっています。

- 1 つのスイッチ上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内の VTP バージョン 2 に対応可能なすべてのスイッチでバージョン 2 がイネーブルになります。 VTP バージョン 3 をイネーブルにするには、各スイッチ上で手動によって設定する必要があります。
- VTP バージョン 1 および 2 では、このバージョンを設定できるのは、VTP サーバ モードまたはトランスペアレント モードのスイッチだけです。 スイッチが VTP バージョン 3 を実行し、かつスイッチがクライアント モードの場合、既存の拡張 VLAN や既存のプライベート VLAN がなく、パスワードが非表示に設定されていないときであれば、バージョン 2 に変更できます。

  注意 同一 VTP ドメイン内のスイッチ上で、VTP バージョン 1 と VTP バージョン 2 は相互運用できません。 VTP ドメイン内のすべてのスイッチが VTP バージョン 2 をサポートしている場合を除き、VTP バージョン 2 をイネーブルにはしないでください。

- TrCRF および TrBRF トークンリング環境では、トークンリング VLAN スイッチング機能を正しく動作させるために、VTP バージョン 2 または VTP バージョン 3 をイネーブルにする必要があります。 トークンリングおよびトークンリング Net メディアの場合は、VTP バージョン 2 をディセーブルにします。
- **注意** VTP バージョン 3 では、プライマリ サーバとセカンダリ サーバの両方がドメイン内の 1 つのインスタンスに存在できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vtp version {1 | 2 | 3}**
4. **end**
5. **show vtp status**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp version {1 | 2 | 3}** 例： `Switch(config)# vtp version 2`	スイッチで VTP バージョンをイネーブルにします。デフォルトは VTP バージョン 1 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例： `Switch# show vtp status`	設定された VTP バージョンがイネーブルであることを確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

関連トピック

VTP バージョン, （1956 ページ）
VTP バージョン 2, （1952 ページ）
VTP バージョン 3, （1953 ページ）

VTP プルーニングのイネーブル化

はじめる前に

VTP プルーニングは VTP トランスペアレント モードでは機能しないように設計されています。ネットワーク内に VTP トランスペアレント モードのスイッチが 1 台または複数存在する場合は、次のいずれかの操作を実行する必要があります。

- ネットワーク全体の VTP プルーニングをオフにします。
- VTP トランスペアレント スイッチのアップストリーム側にあるスイッチのトランク上で、すべての VLAN をプルーニング不適格にすることによって、VTP プルーニングをオフにします。

インターフェイスに VTP プルーニングを設定するには、**switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します。 VTP プルーニングは、インターフェイスがトランキングを実行している場合に作用します。 VLAN プルーニングの適格性は、VTP ドメインで VTP プルーニングがイネーブルであるかどうか、特定の VLAN が存在するかどうか、およびインターフェイスが現在トランキングを実行しているかどうかにかかわらず、設定できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vtp pruning**
4. **end**
5. **show vtp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp pruning** 例： `Switch(config)# vtp pruning`	VTP 管理ドメインでプルーニングをイネーブルにします。 プルーニングは、デフォルトではディセーブルに設定されています。 VTP サーバ モードの 1 台のスイッチ上に限ってプルーニングをイネーブルにする必要があります。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例： `Switch# show vtp status`	表示された [VTP Pruning Mode] フィールドの設定を確認します。

関連トピック

VTP プルーニング, （1954 ページ）

ポート単位の VTP の設定

VTP バージョン 3 では、ポート単位で VTP をイネーブルまたはディセーブルにできます。 VTP は、トランク モードのポート上でだけイネーブルにできます。 VTP トラフィックの着信または発信はブロックされ、転送されません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **vtp**
5. **end**
6. **show running-config interface***interface-id*
7. **show vtp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**vtp** 例： `Switch(config)# vtp`	指定したポートの VTP をイネーブルにします。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config interface***interface-id* 例： `Switch# show running-config interface gigabitethernet1/0/1`	ポートの変更を確認します。
ステップ 7	**show vtp status** 例： `Switch# show vtp status`	設定を確認します。

関連トピック

VTP の設定, （1955 ページ）

VTP ドメインへの VTP クライアント スイッチの追加

VTP ドメインに追加する前にスイッチ上で VTP コンフィギュレーション リビジョン番号を確認およびリセットするには、次の手順に従います。

はじめる前に

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より小さいことを確認してください。 VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。 VTP バージョン 1 および 2 では、VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。 VTP バージョン 3 では、VLAN 情報が消去されることはありません。

スイッチ上で VTP をディセーブルにし、VTP ドメイン内の他のスイッチに影響を与えることなく VLAN 情報を変更するには、**vtp mode transparent** グローバル コンフィギュレーション コマンドを使用します。

手順の概要

1. **enable**
2. **show vtp status**
3. **configureterminal**
4. **vtp domain***domain-name*
5. **end**
6. **show vtp status**
7. **configure terminal**
8. **vtp domain***domain-name*
9. **end**
10. **show vtp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**show vtp status** 例： `Switch# show vtp status`	VTP コンフィギュレーション リビジョン番号をチェックします。 番号が 0 の場合は、スイッチを VTP ドメインに追加します。 番号が 0 より大きい場合は、次の手順に従います。 • ドメイン名を書き留めます。 • コンフィギュレーション リビジョン番号を書き留めます。 • 次のステップに進んで、スイッチのコンフィギュレーション リビジョン番号をリセットします。
ステップ 3	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**vtp domain***domain-name* 例： `Switch(config)# vtp domain`	ドメイン名を、ステップ 1 で表示された元の名前から新しい名前に変更します。

	コマンドまたはアクション	目的
	domain123	
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 スイッチの VLAN 情報が更新され、コンフィギュレーション リビジョン番号が 0 にリセットされます。
ステップ 6	**show vtp status** 例： `Switch# show vtp status`	コンフィギュレーション リビジョン番号が 0 にリセットされていることを確認します。
ステップ 7	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 8	**vtp domain***domain-name* 例： `Switch(config)# vtp domain domain012`	スイッチの元のドメイン名を開始します。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 スイッチの VLAN 情報が更新されます。
ステップ 10	**show vtp status** 例： `Switch# show vtp status`	（任意）ドメイン名がステップ 1 のものと同じであり、コンフィギュレーション リビジョン番号が 0 であることを確認します。

関連トピック

VTP ドメイン，（1949 ページ）

VTP の前提条件

VTP 設定のためのドメイン名，（1955 ページ）

VTP のモニタ

ここでは、VTP の設定を表示およびモニタリングするために使用するコマンドについて説明します。

VTP の設定情報（ドメイン名、現在の VTP バージョン、VLAN 数）を表示することによって、VTP をモニタします。 スイッチで送受信されたアドバタイズに関する統計情報を表示することもできます。

表 *177* : *VTP* モニタ コマンド

コマンド	目的
show vtp counters	送受信された VTP メッセージに関するカウンタを表示します。
show vtp devices [**conflict**]	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。 プライマリ サーバと競合する VTP バージョン 3 の装置が表示されます。 **show vtp devices** コマンドは、スイッチがトランスペアレント モードまたはオフ モードのときは情報を表示しません。
show vtp interface [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。
show vtp password	VTP パスワードを表示します。 表示されるパスワードの形式は、**hidden** キーワードが入力されているか、または、暗号化がスイッチでイネーブル化されているかどうかによって異なります。
show vtp status	VTP スイッチ設定情報を表示します。

VTP の設定例

例：スイッチをプライマリ サーバとして設定する

次に、パスワードが非表示またはシークレットに設定されている場合に、VLAN データベースのプライマリ サーバ（デフォルト）としてスイッチを設定する方法の例を示します。

```
Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain
```

```
VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- -------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

関連トピック

VTP バージョン 3 のパスワードの設定, （1961 ページ）

VTP ドメインのパスワード, （1956 ページ）

例：VTP サーバとしてのスイッチの設定

次に、ドメイン名が *eng_group*、パスワードが *mypassword* という VTP サーバとしてスイッチを設定する例を示します。

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.

Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANS.

Switch(config)# vtp password mypassword
Setting device VLAN database password to mypassword.
Switch(config)# end
```

関連トピック

VTP モードの設定, （1958 ページ）

VTP モード, （1950 ページ）

例：インターフェイスでの VTP のイネーブル化

インターフェイス上で VTP をイネーブルにするには、**vtp** インターフェイス コンフィギュレーション コマンドを使用します。 インターフェイス上で VTP をディセーブルにするには、**no vtp** インターフェイス コンフィギュレーション コマンドを使用します。

```
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# vtp
Switch(config-if)# end
```

例：VTP パスワードの作成

次に、VTP パスワードを作成する例を示します。

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

次の作業

VTP を設定したら、次の項目を設定できます。

- VLANS
- VLAN トランキング
- VLAN メンバーシップ ポリシー サーバ（VMPS）
- 音声 VLAN

第 74 章

VLAN の設定

- 機能情報の確認，1975 ページ
- VLAN の前提条件，1975 ページ
- VLAN の制約事項，1976 ページ
- VLAN について，1976 ページ
- VLAN の設定方法，1983 ページ
- VLAN のモニタリング，1992 ページ
- 設定例，1994 ページ
- 次の作業，1995 ページ

機能情報の確認

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

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

VLAN の前提条件

VLAN 設定時の前提条件と考慮事項を次に示します。

- VLAN を作成する前に、VLAN トランキング プロトコル（VTP）を使用してネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。

- スイッチは、VTP クライアント、サーバ、およびトランスペアレントの各モードで 1000 の VLAN をサポートしています。

（注） LAN Base イメージ使用時は、lanbase のデフォルトのテンプレートだけが 1,000 の VLAN をサポートします。 残りのテンプレート（デフォルトと lanbase-routing）は、255 の VLAN のみをサポートします。 スイッチが LAN Lite イメージを実行中の場合は、最大 64 の VLAN をサポートできます。

VLAN の制約事項

次に、VLAN を設定する際の制約事項を示します。

- 1K VLAN は Lan Base のデフォルト テンプレートが設定された LAN Base イメージを実行しているスイッチ上でのみサポートされます。
- 標準範囲の VLAN 設定の CPU 使用率が高いことを示す警告メッセージを回避するには、使用する VLAN を 256 までにすることを推奨します。 この場合、約10 のアクセス インターフェイス、または 5つのトランク インターフェイスが同時にフラップできます。これによる CPU 使用率への影響はごくわずかです（同時にフラップするインターフェイスが多い場合は、CPU 使用率が非常に高くなる場合があります）。
- プライベート VLAN はスイッチではサポートされません。

VLAN について

論理ネットワーク

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。 VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。 どのようなスイッチポートでも VLAN に属することができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN 内のエンド ステーションだけに転送またはフラッディングされます。 各 VLAN は 1 つの論理ネットワークと見なされ、VLAN に属さないステーション宛のパケットは、ルータまたはフォールバック ブリッジングをサポートするスイッチを経由して伝送しなければなりません。 VLAN はそれぞれが独立した論理ネットワークと見なされるので、VLAN ごとに独自のブリッジ管理情報ベース（MIB）情報があり、スパニングツリーの独自の実装をサポートできます。

VLAN は通常、IP サブネットワークに対応付けられます。 たとえば、特定の IP サブネットに含まれるエンド ステーションはすべて同じ VLAN に属します。 スイッチ上のインターフェイスの VLAN メンバーシップは、インターフェイスごとに手動で割り当てます。 この方法でスイッチイ

ンターフェイスをVLANに割り当てた場合、これをインターフェイス ベース（またはスタティック）VLAN メンバーシップと呼びます。

VLAN 間のトラフィックは、ルーティングする必要があります。

スイッチは、スイッチ仮想インターフェイス（SVI）を使用して、VLAN間でトラフィックをルーティングできます。 VLAN 間でトラフィックをルーティングするには、SVI を明示的に設定して IP アドレスを割り当てる必要があります。

サポートされる VLAN

スイッチは、VTP クライアント、サーバ、およびトランスペアレントの各モードで VLAN をサポートしています。 VLAN は、1 ～ 4094 の番号で識別します。 VLAN ID 1002 ～ 1005 は、トークンリングおよびファイバ分散データ インターフェイス（FDDI）VLAN 専用です。

VTP バージョン 1 およびバージョン 2 は、標準範囲の VLAN（VLAN ID 1 ～ 1005）だけをサポートします。 これらのバージョンで 1006 ～ 4094 の VLAN ID を作成する場合は、スイッチを VTP トランスペアレント モードにする必要があります。 Cisco IOS Release 12.2(52)SE 以降では VTP バージョン 3 をサポートします。 VTP バージョン 3 は、VLAN 範囲全体（VLAN 1 ～ 4094）をサポートします。 拡張範囲 VLAN（VLAN 1006 ～ 4094）は、VTP バージョン 3 でのみサポートされます。 拡張 VLAN がドメインに設定されている場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。

（注） LAN Base イメージ使用時は、lanbase のデフォルトのテンプレートだけが 1,000 の VLAN をサポートします。 残りのテンプレート（デフォルトと lanbase-routing）は、255 の VLAN のみをサポートします。 スイッチが LAN Lite イメージを実行中の場合は、最大 64 の VLAN をサポートできます。

スイッチは、最大 128 のスパニングツリー インスタンスを持つ Per-VLAN Spanning-Tree Plus（PVST+）または Rapid PVST+ をサポートします。 VLAN ごとに 1 つずつスパニングツリー インスタンスを使用できます。 スイッチは、イーサネット ポート経由の VLAN トラフィックの送信方式として IEEE 802.1Q トランキングのみをサポートします。

（注） スイッチが LAN Lite イメージを実行中の場合は、最大 64 のスパニングツリー インスタンスをサポートできます。

VLAN ポート メンバーシップ モード

VLAN に所属するポートは、メンバーシップ モードを割り当てることで設定します。メンバーシップ モードは、各ポートが伝送できるトラフィックの種類、および所属できる VLAN の数を指定します。

ポートが VLAN に所属すると、スイッチは VLAN 単位で、ポートに対応するアドレスを学習して管理します。

表 *178*：ポートのメンバーシップ モードとその特性

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1 つの VLAN だけに所属します。	VTP は必須ではありません。VTP にグローバルに情報を伝播させないようにする場合は、VTP モードをトランスペアレント モードに設定します。 VTP に加入するには、別のスイッチのトランク ポートに接続されているスイッチ少なくとも 1 つのトランク ポートが必要です。
トランク（IEEE 802.1Q）： • IEEE 802.1Q：業界標準のトランキング カプセル化方式です。	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべての VLAN のメンバです。ただし、メンバーシップは許可 VLAN リストを設定して制限できます。 また、プルーニング適格リストを変更して、リストに指定したトランク ポート上の VLAN へのフラッディング トラフィックを阻止することもできます。	VTP を推奨しますが、必須ではありません。 VTP は、ネットワーク全体にわたって VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。 VTP はトランク リンクを通じて他のスイッチと VLAN コンフィギュレーション メッセージを交換します。
ダイナミック アクセス	ダイナミックアクセス ポートは 1 つの VLAN（VLAN ID が 1 ～ 4094）にのみ所属し、VLAN Member Policy Server（VMPS）によって動的に割り当てられます。 VMPS には Catalyst 6500 シリーズのスイッチを使用できますが、Catalyst スイッチなどは使用できません。 Catalyst スイッチは VMPS クライアントです。 同一のスイッチ上でダイナミックアクセス ポートとトランク ポートを使用できますが、ダイナミックアクセス ポートは別のスイッチではなく、エンド ステーションまたはハブに接続する必要があります。	VTP は必須です。 VMPS およびクライアントを同じ VTP ドメイン名で設定してください。 VTP に加入するには、スイッチ上の少なくとも 1 つのトランク ポートが、別のスイッチのトランク ポートに接続されている必要があります。

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
音声 VLAN	音声 VLAN ポートは、Cisco IP Phone に接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データ トラフィックに別の VLAN を使用するように設定されたアクセス ポートです。	VTP は不要です。VTP は音声 VLAN に対して無効です。

VLAN コンフィギュレーション ファイル

VLAN ID 1 ～ 1005 の設定は vlan.dat（VLAN データベース）ファイルに書き込まれます。この設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。 vlan.dat ファイルはフラッシュメモリに格納されます。VTP モードがトランスペアレントモードの場合、それらの設定もスイッチの実行コンフィギュレーション ファイルに保存されます。

さらに、インターフェイスコンフィギュレーションモードを使用して、ポートのメンバーシップモードの定義、VLAN に対するポートの追加および削除を行います。 これらのコマンドの実行結果は、実行コンフィギュレーション ファイルに書き込まれます。このファイルを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

VLAN および VTP 情報（拡張範囲 VLAN 設定情報を含む）をスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントで、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。 VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。
- VTP バージョン 1 および 2 では、VTP モードがサーバである場合、VLAN ID 1 ～ 1005 のドメイン名と VLAN 設定で VLAN データベース情報が使用されます。 VTP バージョン 3 は、VLAN 1006 ～ 4094 もサポートします。

標準範囲 VLAN 設定時の注意事項

標準範囲 VLAN は、ID が 1 ～ 1005 の VLAN です。

VTP 1 および 2 は、標準範囲 VLAN だけをサポートします。

ネットワーク内で標準範囲 VLAN を作成または変更する場合には、次の注意事項に従ってください。

- 標準範囲 VLAN は、1 ～ 1001 の番号で識別します。 VLAN 番号 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 専用です。
- VLAN 1 ～ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。 VTP モードがトランスペアレント モードの場合、VTP と VLAN の設定もスイッチの実行コンフィギュレーション ファイルに保存されます。
- スイッチが VTP サーバ モードまたは VTP トランスペアレント モードにある場合は、VLAN データベース内の VLAN 2 ～ 1001 について設定を追加、変更、または削除できます（VLAN ID 1 および 1002 ～ 1005 は自動作成され、削除できません）。
- VTP バージョン 1 および 2 では、スイッチは VTP トランスペアレント モード（VTP はディセーブル）の場合だけ、VLAN ID 1006 ～ 4094 をサポートします。 これらは拡張範囲 VLAN であり、設定オプションには制限があります。 VTP トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースに保存されず、伝播されません。 VTP バージョン 3 では、VTP サーバ モードでの拡張範囲 VLAN（VLAN 1006～4094）データベース伝播をサポートします。 拡張 VLAN を設定している場合は、VTP バージョン 3 からバージョン 1 または 2 に変換できません。
- VLAN を作成する前に、スイッチを VTP サーバ モードまたは VTP トランスペアレント モードにする必要があります。 スイッチが VTP サーバである場合には、VTP ドメインを定義する必要があります。VTP ドメインを定義しないと、VTP は機能しません。
- スイッチは、トークンリングまたは FDDI メディアをサポートしません。 スイッチは FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを転送するのではなく、VTP を介して VLAN 設定を伝播します。
- スイッチは 128 のスパニングツリー インスタンスをサポートします。 スイッチのアクティブな VLAN 数が、サポートされているスパニングツリー インスタンス数よりも多い場合、スパニングツリーは 128 の VLAN でイネーブルにできます。残りの VLAN で、スパニングツリーはディセーブルになります。 スイッチ上の使用可能なスパニングツリー インスタンスをすべて使い切ってしまった後に、VTP ドメインの中にさらに別の VLAN を追加すると、そのスイッチ上にスパニングツリーが稼働しない VLAN が生成されます。 そのスイッチのトランク ポート上でデフォルトの許可リスト（すべての VLAN を許可するリスト）が設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。 ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチでスパニングツリーインスタンスをすべて使用してしまっている場合には注意が必要です。 スパニングツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。

  スイッチ上の VLAN の数がサポートされているスパニングツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s Multiple STP（MSTP）を設定して、複数の VLAN を単一のスパニングツリー インスタンスにマッピングすることを推奨します。

関連トピック

イーサネット VLAN の作成または変更
VLAN の削除, （1986 ページ）
VLAN へのスタティック アクセス ポートの割り当て
VLAN のモニタリング
イーサネット VLAN の作成または変更
VLAN の削除, （1986 ページ）
VLAN へのスタティック アクセス ポートの割り当て
VLAN のモニタリング
イーサネット VLAN の作成または変更
VLAN の削除, （1986 ページ）
VLAN へのスタティック アクセス ポートの割り当て
VLAN のモニタリング
イーサネット VLAN の作成または変更
VLAN の削除, （1986 ページ）
VLAN へのスタティック アクセス ポートの割り当て
VLAN のモニタリング
イーサネット VLAN の作成または変更
VLAN の削除, （1986 ページ）
VLAN へのスタティック アクセス ポートの割り当て
VLAN のモニタリング
イーサネット VLAN の作成または変更
例：VLAN 名の作成, （1994 ページ）

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN は、ID が 1006 ～ 4094 の VLAN です。

VTP 3 だけが拡張範囲 VLAN をサポートしています。

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- 拡張範囲の VLAN ID は、スイッチが VTP バージョン 3 を実行していない場合は VLAN データベースに保存されず、VTP で認識されません。
- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。
- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで、VTP モードをトランスペアレントに設定できます。 VTP トランスペアレント モードでスイッチが始動するように、この設定をスタートアップ コンフィギュレーションに保存する必要があります。 このようにしないと、スイッチをリセットした場合に、拡張範囲 VLAN 設定が失われます。 VTP バージョン 3 で拡張範囲 VLAN を作成する場合は、VTP バージョン 1 または 2 に変更できません。

- 拡張範囲 VLAN を作成するときに、使用できるハードウェア リソースが不足していると、エラー メッセージが生成され、拡張範囲 VLAN が拒否されます。

関連トピック

拡張範囲 VLAN の作成
内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN のモニタリング
拡張範囲 VLAN の作成
内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN のモニタリング
拡張範囲 VLAN の作成
内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN のモニタリング
拡張範囲 VLAN の作成
内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN のモニタリング
拡張範囲 VLAN の作成
内部 VLAN ID を指定した拡張範囲 VLAN の作成
VLAN のモニタリング
拡張範囲 VLAN の作成, （1990 ページ）
例：拡張範囲 VLAN の作成, （1995 ページ）

VLAN のデフォルト設定

イーサネット VLAN のデフォルト設定

次の表に、イーサネット VLAN のデフォルト設定を記載します。

（注） スイッチがサポートするのは、イーサネットインターフェイスだけです。 FDDIおよびトークンリングVLANは、ローカルではサポートされないので、FDDIおよびトークンリング メディア固有の特性は、他のスイッチに対する VTP グローバル アドバタイズにのみ設定します。

表 *179*：イーサネット *VLAN* のデフォルトおよび範囲

パラメータ	デフォルト	範囲
VLAN ID	1	1 ～ 4094 （注） 拡張範囲 VLAN（VLAN ID 1006 ～ 4094）は、VTP バージョン 3 の VLAN データベースにのみ保存されます。
VLAN 名	VLANxxxx。xxxx は VLAN ID 番号に等しい4桁の数字（先行ゼロを含む）です。	範囲なし
IEEE 802.10 SAID	100001（100000 と VLAN ID の和）	1 ～ 4294967294
IEEE 802.10 SAID	1500	576 ～ 18190
プライベート VLAN	設定なし	2 ～ 1001、1006 ～ 4094

VLAN のデフォルト設定

拡張範囲VLANについてはMTUサイズ、プライベートVLAN、およびリモートSPAN設定ステートしか変更できません。残りのすべての特性はデフォルト状態のままでなければなりません。

（注） リモート SPAN をサポートするには、スイッチが LAN Base イメージを実行している必要があります。

VLAN の設定方法

標準範囲 VLAN の設定方法

VLANデータベースに新しい標準範囲VLANを作成したり、VLANデータベース内の既存のVLANを変更したりする場合、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ

- イーサネット
- Fiber Distributed Data Interface [FDDI]
- FDDI ネットワーク エンティティ タイトル [NET]
- TrBRF または TrCRF
- トークンリング
- トークンリング Net

- VLAN ステート（active または suspended）
- VLAN の最大伝送単位（MTU）
- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN のスパニングツリー プロトコル（STP）タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号

vlan.dat ファイルを手動で削除しようとすると、VLAN データベースに不整合が生じる可能性があります。 VLAN 設定を変更する場合は、この項の手順に従ってください。

イーサネット VLAN の作成または変更

VLAN データベース内の各イーサネット VLAN の ID は 4 桁の一意の数字で、1 ～ 1001 を指定できます。 VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 用に予約されています。標準範囲 VLAN を作成して VLAN データベースに追加するには、VLAN に番号および名前を割り当てます。

（注） VTP バージョン 1 および 2 でスイッチが VTP トランスペアレント モードである場合は、1006 より大きい VLAN ID を割り当てることができますが、それらは VLAN データベースに追加されません。

手順の概要

1. **enable**
2. **configureterminal**
3. **vlan***vlan-id*
4. **name***vlan-name*
5. **mtu***mtu-size*
6. **remote-span**
7. **end**
8. **show vlan** {**name***vlan-name* | **id***vlan-id*}
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan***vlan-id* 例： `Switch(config)# vlan 20`	VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。 新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。 （注） このコマンドで指定できる VLAN ID 範囲は 1 ～ 4094 です。
ステップ 4	**name***vlan-name* 例： `Switch(config-vlan)# name test20`	（任意）VLAN の名前を入力します。 VLAN 名を指定しなかった場合には、デフォルトとして、VLAN という語の後ろに先行ゼロを含めた *vlan-id* 値が付加されます。 たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。
ステップ 5	**mtu***mtu-size* 例： `Switch(config-vlan)# mtu 256`	（任意）MTU サイズ（または他の VLAN 特性）を変更します。

	コマンドまたはアクション	目的
ステップ 6	**remote-span** 例： `Switch(config-vlan)# remote-span`	（任意）リモート スイッチド ポート アナライザ（SPAN）セッションに対する RSPAN VLAN として、VLAN を設定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show vlan** {**name***vlan-name* | **id***vlan-id*} 例： `Switch# show vlan name test20 id 20`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN の削除

VTP サーバ モードのスイッチから VLAN を削除すると、VTP ドメイン内のすべてのスイッチの VLAN データベースから、その VLAN が削除されます。 VTP トランスペアレント モードのスイッチから VLAN を削除した場合、その特定のスイッチスイッチ上に限り VLAN が削除されます。

イーサネット VLAN 1 および FDDI、またはトークンリング VLAN 1002 ～ 1005 の、メディア タイプ別のデフォルト VLAN は削除できません。

注意 VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。 これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に（非アクティブで）対応付けられたままです。

手順の概要

1. **enable**
2. **configureterminal**
3. **no vlan***vlan-id*
4. **end**
5. **show vlan brief**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no vlan***vlan-id* 例： `Switch(config)# no vlan 4`	VLAN ID を入力して、VLAN を削除します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vlan brief** 例： `Switch# show vlan brief`	VLAN が削除されたことを確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

関連トピック

サポートされる VLAN
標準範囲 VLAN 設定時の注意事項, （1979 ページ）

VLAN のモニタリング
サポートされる VLAN
標準範囲 VLAN 設定時の注意事項, （1979 ページ）

VLAN のモニタリング
サポートされる VLAN
標準範囲 VLAN 設定時の注意事項, （1979 ページ）

VLAN のモニタリング
サポートされる VLAN
標準範囲 VLAN 設定時の注意事項, （1979 ページ）

VLAN のモニタリング
サポートされる VLAN
標準範囲 VLAN 設定時の注意事項, （1979 ページ）

VLAN のモニタリング
VLAN のモニタリング

VLAN へのスタティック アクセス ポートの割り当て

VTP をディセーブルにすることによって（VTP トランスペアレント モード）、VTP に VLAN 設定情報をグローバルに伝播させずに、スタティック アクセス ポートを VLAN に割り当てることができます。

存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます

手順の概要

1. **configureterminal**
2. **interface***interface-id*
3. **switchport mode access**
4. **switchport access vlan***vlan-id*
5. **end**
6. **show running-config interface***interface-id*
7. **show interfaces***interface-id***switchport**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	VLAN に追加するインターフェイスを入力します。
ステップ 3	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	ポート（レイヤ 2 アクセス ポート）の VLAN メンバーシップ モードを定義します。
ステップ 4	**switchport access vlan***vlan-id* 例： `Switch(config-if)# switchport access vlan 2`	VLAN にポートを割り当てます。 指定できる VLAN ID の範囲は 1 ～ 4094 です。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface***interface-id* 例： `Switch# show running-config interface gigabitethernet2/0/1`	インターフェイスの VLAN メンバーシップ モードを確認します。
ステップ 7	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet2/0/1 switchport`	表示された *Administrative Mode* および *Access Mode VLAN* フィールドの設定を確認します。

関連トピック

例：アクセス ポートとしてのポートの設定, （1995 ページ）

拡張範囲 VLAN の設定方法

VTP バージョン 1 およびバージョン 2 でスイッチが VTP トランスペアレント モード（VTP がディセーブル）の場合、拡張範囲 VLAN（1006 ～ 4094）を作成できます。 VTP バージョンは、拡張範囲 VLAN をサーバ モードおよびトランスペアレント モードでサポートします。 サービス プロバイダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応できます。 拡張範囲 VLAN ID は、VLAN ID を許可するどの **switchport** コマンドでも許可されます。

VTP バージョン 1 または 2 での拡張範囲 VLAN の設定は VLAN データベースに格納されません。ただし、VTP モードがトランスペアレントであるため、スイッチの実行コンフィギュレーション ファイルにストアされます。設定をスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。 VTP バージョン 3 で作成された拡張範囲 VLAN は、VLAN データベースに保存されます。

拡張範囲 VLAN の作成

グローバル コンフィギュレーション モードで拡張範囲 VLAN を作成するには、**vlan** グローバル コンフィギュレーション コマンドを入力し、1006 ～ 4094 の VLAN ID を指定します。 拡張範囲 VLAN にはデフォルトのイーサネット VLAN 特性が適用されます。変更できるパラメータは MTU サイズおよび RSPAN 設定のみです。 すべてのパラメータのデフォルト値については、コマンド リファレンスに記載された **vlan** グローバル コンフィギュレーション コマンドの説明を参照してください。 VTP バージョン 1 または 2 で、スイッチが VTP トランスペアレント モードでない場合に拡張範囲 VLAN ID を入力すると、VLAN コンフィギュレーション モードの終了時にエラー メッセージが生成され、拡張範囲 VLAN が作成されません。

VTP バージョン 1 および 2 では、拡張範囲 VLAN は VLAN データベースに保存されず、スイッチの実行コンフィギュレーション ファイルに保存されます。 拡張範囲 VLAN 設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用できます。 VTP バージョン 3 は、拡張範囲 VLAN を VLAN データベースに保存します。

手順の概要

1. **configureterminal**
2. **vtp mode transparent**
3. **vlan***vlan-id*
4. **mtu** *mtu size*
5. **remote-span**
6. **end**
7. **show vlan id***vlan-id*
8. **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp mode transparent** 例： `Switch(config)# vtp mode transparent`	スイッチを VTP トランスペアレント モードで設定し、VTP をディセーブルにします。 （注） この手順は、VTP バージョン 3 では不要です。

ステップ 3	**vlan***vlan-id*
	
	例：
	
	`Switch(config)# vlan 2000`
	`Switch(config-vlan)#`
		拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。 指定できる範囲は 1006 ～ 4094 です。

ステップ 4	**mtu** *mtu size* 例： `Switch(config-vlan)# mtu 1024`	MTU サイズを変更して、VLAN を変更します。
ステップ 5	**remote-span** 例： `Switch(config-vlan)# remote-span`	（任意）RSPAN VLAN として VLAN を設定します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show vlan id***vlan-id* 例： `Switch# show vlan id 2000`	VLAN が作成されたことを確認します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup config** 例： `Switch# copy running-config startup-config`	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。 拡張範囲VLAN設定を保存するには、スイッチのスタートアップ コンフィギュレーション ファイルに VTP トランスペアレント モード設定と拡張範囲 VLAN 設定を保存する必要があります。 これらを保存しないと、スイッチをリセットした場合に、スイッチがデフォルトで VTP サーバ モードになり、拡張範囲 VLAN ID は保存されません。 （注） VTP バージョン 3 では、VLAN が VLAN データベースに保存されるため、この手順は必要ありません。

関連トピック

拡張範囲 VLAN 設定時の注意事項, （1981 ページ）

例：拡張範囲 VLAN の作成, （1995 ページ）

VLAN のモニタリング

表 *180*：特権 *EXEC* 表示コマンド

コマンド	目的
show interfaces [**vlan***vlan-id*]	スイッチ上に設定されたすべてのインターフェイスまたは特定の VLAN の特性を表示します。

コマンド	目的
show vlan [**brief** | **group** [**group-name** *name*] |**id***vlan-id* | **ifindex** | **internal** | **mtu** | **name** *name* |**remote-span** | **summary**]]	スイッチ上のすべての VLAN または指定した VLAN のパラメータを表示します。 次のコマンド オプションが使用可能です。 • **brief**：VTP VLAN のステータス概要を表示します。 • **group**：VLAN グループをグループ名と使用可能な接続済みの VLAN と一緒に表示します。 • **id**：識別番号別に VTP VLAN ステータスを表示します。 • **ifindex**：SNMP ifIndex を表示します。 • **mtu**：VLAN MTU 情報を表示します。 • **name**：指定された名前の VTP VLAN 情報を表示します。 • **remote-span**：リモート SPAN VLAN を表示します。 • **summary**：VLAN 情報の要約を表示します。

コマンド	目的
show vlan [**access-log** {**config** | **flow** | **statistics**} | **access-map** *name* | **brief** | **dot1q** { **tag native** } | **filter** [**access-map** | **vlan**] | **group** [**group-name** *name*] | **id***vlan-id* | **ifindex** | **internal usage** | **mtu** | **name** *name* | **private-vlan type** | **remote-span** | **summary**]	スイッチ上のすべての VLAN または指定した VLAN のパラメータを表示します。 次のコマンド オプションが使用可能です。 • **access-log**：VACL ロギングを表示します。 • **access-map**：VLAN アクセスマップを表示します。 • **brief**：VTP VLAN のステータス概要を表示します。 • **dot1q**：dot1q パラメータを表示します。 • **filter**：VLAN フィルタ情報を表示します。 • **group**：VLAN グループをグループ名と使用可能な接続済みの VLAN と一緒に表示します。 • **id**：識別番号別に VTP VLAN ステータスを表示します。 • **ifindex**：SNMP ifIndex を表示します。 • **mtu**：VLAN MTU 情報を表示します。 • **name**：指定された名前の VTP VLAN 情報を表示します。 • **private-vlan**：プライベート VLAN 情報を表示します。 • **remote-span**：リモート SPAN VLAN を表示します。 • **summary**：VLAN 情報の要約を表示します。

設定例

例：VLAN 名の作成

次に、イーサネット VLAN 20 を作成し、test20 という名前を付け、VLAN データベースに追加する例を示します。

```
Switch# configure terminal
```

```
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

関連トピック

イーサネット VLAN の作成または変更
標準範囲 VLAN 設定時の注意事項, （1979 ページ）

例：アクセス ポートとしてのポートの設定

次に、VLAN 2 のアクセス ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

関連トピック

VLAN へのスタティック アクセス ポートの割り当て, （1988 ページ）

例：拡張範囲 VLAN の作成

次に、すべてデフォルトの特性で拡張範囲 VLAN を新規作成し、VLAN コンフィギュレーション モードを開始して、新規 VLAN をスイッチのスタートアップ コンフィギュレーション ファイルに保存する例を示します。

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

関連トピック

拡張範囲 VLAN の作成, （1990 ページ）
拡張範囲 VLAN 設定時の注意事項, （1981 ページ）

次の作業

VLAN を設定したら、次の項目を設定できます。

- VLAN トランキング プロトコル（VTP）
- VLAN トランク
- プライベート VLAN
- VLAN メンバーシップ ポリシー サーバ（VMPS）

第 75 章

VLAN トランクの設定

- 機能情報の確認，1997 ページ
- VLAN トランクの前提条件，1997 ページ
- VLAN トランクについて，1998 ページ
- VLAN トランクの設定方法，2003 ページ
- VLAN トランキングの設定例，2019 ページ
- 次の作業，2019 ページ

機能情報の確認

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

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

VLAN トランクの前提条件

IEEE 802.1Q トランクは、ネットワークのトランキング方式について次の制約があります。

- IEEE 802.1Q トランクを使用して接続している Cisco スイッチのネットワークでは、スイッチはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。 他社製のデバイスは、すべての VLAN でスパニングツリー インスタンスを 1 つサポートする場合があります。

IEEE 802.1Q トランクを使用して Cisco スイッチを他社製のデバイスに接続する場合、Cisco スイッチは、トランクの VLAN のスパニングツリー インスタンスを、他社製の IEEE 802.1Q スイッチのスパニングツリー インスタンスと結合します。 ただし、各 VLAN のスパニングツリー情報は、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離された Cisco スイッチによって維持されます。 Cisco スイッチと分離された他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

- IEEE 802.1Qトランクに対応するネイティブVLANが、トランク リンクの両側で一致していなければなりません。 トランクの片側のネイティブ VLAN と反対側のネイティブ VLAN が異なっていると、スパニングツリー ループが発生する可能性があります。
- ネットワーク上のすべてのネイティブVLANについてスパニングツリーをディセーブルにせずに、IEEE 802.1Q トランクのネイティブ VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。 IEEE 802.1Q トランクのネイティブVLAN上でスパニングツリーをイネーブルのままにしておくか、またはネットワーク上のすべての VLAN でスパニングツリーをディセーブルにすることを推奨します。 また、ネットワークにループがないことを確認してから、スパニングツリーをディセーブルにしてください。

VLAN トランクについて

トランキングの概要

トランクとは、1 つまたは複数のイーサネット スイッチ インターフェイスと他のネットワーキング デバイス（ルータ、スイッチなど）の間のポイントツーポイント リンクです。 イーサネット トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張できます。

（注） トランクを設定できるのは、1 つのイーサネット インターフェイスまたは EtherChannel バンドルに対してです。

トランキング モード

イーサネット トランク インターフェイスは、さまざまなトランキング モードをサポートします。インターフェイスをトランキングまたは非トランキングとして設定したり、ネイバー インターフェイスとトランキングのネゴシエーションを行ったりするように設定できます。 トランキングを自動ネゴシエーションするには、インターフェイスが同じ VTP ドメインに存在する必要があります。

トランク ネゴシエーションは、ポイントツーポイント プロトコル（PPP）であるダイナミック トランキング プロトコル（DTP）によって管理されます。 ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。

関連トピック

トランク ポートの設定, （2003 ページ）
レイヤ 2 インターフェイス モード, （1999 ページ）

レイヤ 2 インターフェイス モード

表 *181*：レイヤ *2* インターフェイス モード

モード	機能
switchport mode access	インターフェイス（アクセス ポート）を永続的な非トランキング モードにして、リンクの非トランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバーインターフェイスがトランク インターフェイスかどうかに関係なく、非トランク インターフェイスになります。
switchport mode dynamic auto	インターフェイスがリンクをトランク リンクに変換できるようにします。 インターフェイスは、ネイバーインターフェイスが **trunk** または **desirable** モードに設定されている場合、トランク インターフェイスになります。 すべてのイーサネット インターフェイスのデフォルトのスイッチポート モードは、**dynamic auto** です。
switchport mode dynamic desirable	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、ネイバーインターフェイスが **trunk**、**desirable**、または **auto** モードに設定されている場合、トランク インターフェイスになります。
switchport mode trunk	インターフェイスを永続的なトランキング モードにして、ネイバー リンクのトランク リンクへの変換をネゴシエートします。 インターフェイスは、ネイバーインターフェイスがトランク インターフェイスでない場合でも、トランク インターフェイスになります。

モード	機能
switchport nonegotiate	インターフェイスが DTP フレームを生成しないようにします。 このコマンドは、インターフェイス スイッチポート モードが **access** または **trunk** の場合だけ使用できます。 トランク リンクを確立するには、手動でネイバー インターフェイスをトランク インターフェイスとして設定する必要があります。
switchport mode private-vlan	プライベート VLAN モードを設定します。 （注） **switchport mode private-vlan** コマンドのオプションはサポートされていません。

関連トピック

トランク ポートの設定, （2003 ページ）

トランキング モード, （1998 ページ）

トランクでの許可 VLAN

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。 各トランクですべての VLAN ID（1 ～ 4094）が許可されます。 ただし、許可リストから VLAN を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。

スパニングツリー ループまたはストームのリスクを減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにできます。 トランク ポートから VLAN 1 を削除した場合、インターフェイスは引き続き VLAN 1 内で Cisco Discovery Protocol（CDP）、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、DTP、および VTP などの管理トラフィックを送受信します。

VLAN 1 をディセーブルにしたトランク ポートが非トランク ポートになると、そのポートはアクセス VLAN に追加されます。 アクセス VLAN が 1 に設定されると、**switchport trunk allowed** の設定には関係なく、ポートは VLAN 1 に追加されます。 ポート上でディセーブルになっている任意の VLAN について同様のことが当てはまります。

トランク ポートは、VLAN がイネーブルになっており、VTP が VLAN を認識し、なおかつポートの許可リストにその VLAN が登録されている場合に、VLAN のメンバになることができます。 VTP が新しくイネーブルにされた VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバになります。 VTP が新しい VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されていない場合には、トランク ポートはその VLAN のメンバにはなりません。

関連トピック

トランクでの許可 VLAN の定義, （2005 ページ）

トランク ポートでの負荷分散

負荷分散により、スイッチに接続しているパラレル トランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、スイッチ間で 1 つのパラレル リンク以外のすべてのリンクをブロックします。 負荷分散を行うと、トラフィックの所属する VLAN に基づいて、リンク間でトラフィックが分散されます。

トランク ポートで負荷分散を設定するには、STP ポート プライオリティまたは STP パス コストを使用します。 STP ポート プライオリティを使用して負荷分散を設定する場合には、両方の負荷分散リンクを同じスイッチに接続する必要があります。 STP パス コストを使用して負荷分散を設定する場合には、それぞれの負荷分散リンクを同一のスイッチに接続することも、2 台の異なるスイッチに接続することもできます。

STP プライオリティによるネットワーク負荷分散

同一のスイッチ上の 2 つのポートがループを形成すると、スイッチは STP ポート プライオリティを使用して、どのポートをイネーブルとし、どのポートをブロッキング ステートとするかを判断します。 パラレル トランク ポートにプライオリティを設定することにより、そのポートに、特定の VLAN のすべてのトラフィックを伝送させることができます。 VLAN に対するプライオリティの高い（値の小さい）トランク ポートがその VLAN のトラフィックを転送します。 同じ VLAN に対してプライオリティの低い（値の大きい）トランク ポートは、その VLAN に対してブロッキング ステートのままです。 1 つのトランク ポートが特定の VLAN に関するすべてのトラフィックを送受信することになります。

関連トピック

STP ポート プライオリティによる負荷分散の設定, （2011 ページ）

STP パス コストによるネットワーク負荷分散

トランクにそれぞれ異なるパス コストを設定し、各パス コストをそれぞれ異なる VLAN 群に対応付け、各 VLAN でポートをブロックすることによって、VLAN トラフィックを分散するパラレル トランクを設定できます。 VLAN はトラフィックを分離し、リンクが失われた場合に備えて冗長性を維持します。

関連トピック

STP パス コストによる負荷分散の設定, （2016 ページ）

機能の相互作用

トランキングは他の機能と次のように相互作用します。

- トランク ポートをセキュア ポートにすることはできません。

- トランク ポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内のすべてのトランクに同じ設定をする必要があります。 グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。 次に示すパラメータのいずれかの設定を変更すると、スイッチは、入力された設定をグループ内のすべてのポートに伝播します。
  - 許可 VLAN リスト。
  - 各 VLAN の STP ポート プライオリティ。
  - STP PortFast の設定値。
  - トランク ステータス：

    ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- Per VLAN Spanning Tree（PVST）モードでは最大 24 までのトランク ポート、マルチ スパニング ツリー（MST）モードでは最大 40 までのトランク ポートを設定することを推奨します。
- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。 IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。 ダイナミック ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。 IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。

レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

次の表に、レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定を記載します。

表 *182*：レイヤ *2* イーサネット インターフェイス *VLAN* のデフォルト設定

機能	デフォルト設定
インターフェイス モード	**switchport mode dynamic auto**
VLAN 許容範囲	VLAN 1 ～ 4094
プルーニングに適格な VLAN 範囲	VLAN 2 ～ 1001
デフォルト VLAN（アクセス ポート用）	VLAN 1
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1

VLAN トランクの設定方法

トランクの誤設定を避けるために、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように（つまり DTP をオフにするように）設定してください。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

トランク ポートとしてのイーサネット インターフェイスの設定

トランク ポートの設定

トランク ポートは VTP アドバタイズを送受信するので、VTP を使用する場合は、スイッチ上で少なくとも 1 つのトランク ポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。

はじめる前に

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}
5. **switchport access vlan***vlan-id*
6. **switchport trunk native vlan***vlan-id*
7. **end**
8. **show interfaces***interface-id***switchport**
9. **show interfaces***interface-id***trunk**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	トランクに設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**} 例： `Switch(config-if)# switchport mode dynamic desirable`	インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートであり、トランキング モードを設定する場合に限り必要となります）。 • **dynamic auto**：ネイバー インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 これはデフォルトです。 • **dynamic desirable**：ネイバー インターフェイスが trunk、desirable、または auto モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 • **trunk**：ネイバー インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リンクに変換するようにネゴシエートします。
ステップ 5	**switchport access vlan***vlan-id* 例： `Switch(config-if)# switchport access vlan 200`	（任意）インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。

	コマンドまたはアクション	目的
ステップ 6	**switchport trunk native vlan***vlan-id* 例： `Switch(config-if)# switchport trunk native vlan 200`	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/2 switchport`	インターフェイスのスイッチ ポート設定を表示します。[Administrative Mode] および [Administrative Trunking Encapsulation] フィールドに表示されます。
ステップ 9	**show interfaces***interface-id***trunk** 例： `Switch# show interfaces gigabitethernet1/0/2 trunk`	インターフェイスのトランクの設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

トランキング モード, （1998 ページ）

レイヤ 2 インターフェイス モード, （1999 ページ）

トランクでの許可 VLAN の定義

VLAN 1 は、すべての Cisco スイッチのすべてのトランク ポートのデフォルト VLAN です。以前は、すべてのトランク リンクで VLAN 1 を必ずイネーブルにする必要がありました。 VLAN 1 の最小化機能を使用して、個々の VLAN トランク リンクで VLAN 1 をディセーブルに設定できま

す。これにより、ユーザ トラフィック（スパニングツリー アドバタイズなど）は VLAN 1 で送受信されなくなります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode trunk**
5. **switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list*
6. **end**
7. **show interfaces***interface-id***switchport**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk** 例： `Switch(config-if)# switchport mode trunk`	インターフェイスを VLAN トランク ポートとして設定します。

	コマンドまたはアクション	目的
ステップ 5	**switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list* 例： `Switch(config-if)# switchport trunk allowed vlan remove 2`	（任意）トランク上で許容される VLAN のリストを設定します。 *vlan-list* パラメータは、1 ～ 4094 の単一の VLAN 番号、または 2 つの VLAN 番号（小さい方が先、ハイフンで区切る）で指定された VLAN 範囲です。カンマで区切った VLAN パラメータの間、またはハイフンで指定した範囲の間には、スペースを入れないでください。 デフォルトでは、すべての VLAN が許可されます。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/1 switchport`	表示された [Trunking VLANs Enabled] フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

関連トピック

トランクでの許可 VLAN, （2000 ページ）

プルーニング適格リストの変更

プルーニング適格リストは、トランク ポートだけに適用されます。 トランク ポートごとに独自の適格リストがあります。 この手順を有効にするには、VTP プルーニングがイネーブルに設定されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**}*vlan-list* [,*vlan* [,*vlan* [,,,]]
5. **end**
6. **show interfaces***interface-id***switchport**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	VLAN プルーニングを適用するトランク ポートを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**}*vlan-list* [,*vlan* [,*vlan* [,,,]]	トランクからのプルーニングを許可する VLAN のリストを設定します。 **add**、**except**、**none**、および **remove** キーワードの使用方法については、このリリースに対応するコマンド リファレンスを参照してください。 連続していない VLAN ID は、カンマ（スペースなし）で区切ります。ID の範囲はハイフンで指定します。 有効な ID 範囲は 2 ～ 1001 です。 拡張範囲 VLAN（VLAN ID 1006 ～ 4094）はプルーニングできません。 プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。

	コマンドまたはアクション	目的
		デフォルトでは、プルーニングが許可される VLAN のリストには、VLAN 2 ～ 1001 が含まれます。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet2/0/1 switchport`	表示された [Pruning VLANs Enabled] フィールドの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

タグなしトラフィック用ネイティブ VLAN の設定

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、スイッチはタグなしトラフィックを、ポートに設定されたネイティブ VLAN に転送します。 ネイティブ VLAN は、デフォルトでは VLAN 1 です。

ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

パケットの VLAN ID が出力ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport trunk native vlan***vlan-id*
5. **end**
6. **show interfaces***interface-id***switchport**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	IEEE 802.1Q トランクとして設定するインターフェイスを定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport trunk native vlan***vlan-id* 例： `Switch(config-if)# switchport trunk native vlan 12`	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。 *vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/2 switchport`	[Trunking Native Mode VLAN] フィールドの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

トランク ポートの負荷分散の設定

STP ポート プライオリティによる負荷分散の設定

次の手順では、STP ポート プライオリティを使用した負荷分散を指定してネットワークを設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vtp domain***domain-name*
4. **vtp mode server**
5. **end**
6. **show vtp status**
7. **show vlan**
8. **configure terminal**
9. **interface***interface-id*
10. **switchport mode trunk**
11. **end**
12. **show interfaces***interface-id***switchport**
13. スイッチ A で、スイッチ の 2 番目のポートに対して前述の手順を繰り返します。
14. スイッチ B で前述の手順を繰り返し、スイッチ A で設定したトランク ポートに接続するトランク ポートを設定します。
15. **show vlan**
16. **configure terminal**
17. **interface***interface-id*
18. **spanning-tree vlan***vlan-range***port-priority***priority-value*
19. **exit**
20. **interface***interface-id*
21. **spanning-tree vlan***vlan-range***port-priority***priority-value*
22. **end**
23. **show running-config**
24. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**vtp domain***domain-name* 例： `Switch(config)# vtp domain workdomain`	VTP 管理ドメインを設定します。 1 ～ 32 文字のドメイン名を使用できます。
ステップ 4	**vtp mode server** 例： `Switch(config)# vtp mode server`	スイッチ A を VTP サーバとして設定します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show vtp status** 例： `Switch# show vtp status`	スイッチ A およびスイッチ B の両方で、VTP 設定を確認します。 表示された *VTP Operating Mode* および *VTP Domain Name* フィールドをチェックします。
ステップ 7	**show vlan** 例： `Switch# show vlan`	スイッチ A のデータベースに VLAN が存在していることを確認します。
ステップ 8	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 9	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**switchport mode trunk** 例： `Switch(config-if)# switchport mode trunk`	ポートをトランク ポートとして設定します。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/1 switchport`	VLAN の設定を確認します。
ステップ 13	スイッチ A で、スイッチ の 2 番目のポートに対して前述の手順を繰り返します。	
ステップ 14	スイッチ B で前述の手順を繰り返し、スイッチ A で設定したトランク ポートに接続するトランク ポートを設定します。	
ステップ 15	**show vlan** 例： `Switch# show vlan`	トランク リンクがアクティブになると、VTP がスイッチ B に VTP および VLAN 情報を渡します。このコマンドは、スイッチ B が VLAN 設定を学習したことを確認します。
ステップ 16	**configure terminal** 例： `Switch# configure terminal`	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 17	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 18	**spanning-tree vlan***vlan-range***port-priority***priority-value* 例： `Switch(config-if)# spanning-tree vlan 8-10 port-priority 16`	指定された VLAN 範囲にポート プライオリティを割り当てます。 0 ～ 240 のポート プライオリティ値を入力します。 ポート プライオリティ値は 16 ずつ増分します。

	コマンドまたはアクション	目的
ステップ 19	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 20	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	STPのポートプライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 21	**spanning-tree vlan***vlan-range***port-priority***priority-value* 例： `Switch(config-if)# spanning-tree vlan 3-6 port-priority 16`	指定された VLAN 範囲にポート プライオリティを割り当てます。 0 ～ 240 のポート プライオリティ値を入力します。 ポート プライオリティ値は 16 ずつ増分します。
ステップ 22	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 23	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 24	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

STP プライオリティによるネットワーク負荷分散, （2001 ページ）

STP パス コストによる負荷分散の設定

次の手順では、STP パス コストを使用した負荷分散を指定してネットワークを設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **switchport mode trunk**
5. **exit**
6. スイッチ A 内の別のインターフェイスでステップ 2 ～ 4 を繰り返します。
7. **end**
8. **show running-config**
9. **show vlan**
10. **configure terminal**
11. **interface***interface-id*
12. **spanning-tree vlan***vlan-range***cost***cost-value*
13. **end**
14. スイッチ A に設定したもう一方のトランク インターフェイスでステップ 9 ～ 13 を繰り返し、VLAN 8、9、および 10 のスパニングツリー パス コストを 30 に設定します。
15. **exit**
16. **show running-config**
17. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk** 例： `Switch(config-if)# switchport mode trunk`	ポートをトランク ポートとして設定します。
ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	スイッチ A 内の別のインターフェイスでステップ 2 ～ 4 を繰り返します。	
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。 画面で、インターフェイスがトランク ポートとして設定されていることを確認してください。
ステップ 9	**show vlan** 例： `Switch# show vlan`	トランク リンクがアクティブになると、スイッチ A がもう一方のスイッチから VTP 情報を受信します。このコマンドは、スイッチ A が VLAN コンフィギュレーションを学習したことを確認します。
ステップ 10	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	STP コストを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**spanning-tree vlan***vlan-range***cost***cost-value* 例： `Switch(config-if)# spanning-tree vlan 2-4 cost 30`	VLAN 2 ～ 4 のスパニングツリー パス コストを 30 に設定します。
ステップ 13	**end** 例： `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	スイッチ A に設定したもう一方のトランク インターフェイスでステップ 9 ～ 13 を繰り返し、VLAN 8、9、および 10 のスパニングツリー パス コストを 30 に設定します。	
ステップ 15	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 16	**show running-config** 例： `Switch# show running-config`	入力を確認します。 両方のトランク インターフェイスに対してパス コストが正しく設定されていることを表示で確認します。
ステップ 17	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

STP パス コストによるネットワーク負荷分散, （2001 ページ）

VLAN トランキングの設定例

例：トランク ポートの設定

次に、IEEE 802.1Q トランクとしてポートを設定する例を示します。 この例では、ネイバー インターフェイスが IEEE 802.1Q トランキングをサポートするように設定されていることを前提としています。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
```

例：ポートからの VLAN の削除

次に、ポートの許可 VLAN リストから VLAN 2 を削除する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

次の作業

VLAN トランクを設定したら、次の項目を設定できます。

- VLANs
- プライベート VLAN

第 76 章

VMPS の設定

- 機能情報の確認，2021 ページ
- VMPS の前提条件，2021 ページ
- VMPS の制約事項，2022 ページ
- VMPS について，2022 ページ
- VMPS の設定方法，2025 ページ
- VMPS のモニタリング，2032 ページ
- VMPS の設定例，2033 ページ
- 次の作業，2034 ページ

機能情報の確認

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

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

VMPS の前提条件

ダイナミックアクセスポートとしてポートを設定する前に、VLAN メンバーシップポリシーサーバ（VMPS）を設定する必要があります。

ポートをダイナミックアクセス ポートとして設定すると、そのポートに対してスパニングツリーの PortFast 機能が自動的にイネーブルになります。 PortFast モードにより、ポートをフォワーディング ステートに移行させるプロセスが短縮されます。

VMPS クライアントと VMPS サーバの VTP 管理ドメインは、同じでなければなりません。

VMPS の制約事項

次に、VMPS を設定する際の制約事項を示します。

- IEEE 802.1x ポートをダイナミックアクセス ポートとして設定することはできません。 ダイナミックアクセス（VQP）ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。 IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
- トランク ポートをダイナミック アクセス ポートにすることはできませんが、トランク ポートに対して **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドを入力することは可能です。 その場合、スイッチの設定は維持され、後にアクセス ポートとして設定された場合には、その設定が適用されます。 ダイナミックアクセス設定を有効にするには、ポート上でトランキングをオフにしておく必要があります。
- ダイナミックアクセス ポートをモニタ ポートにすることはできません。
- セキュア ポートをダイナミックアクセス ポートにすることはできません。 ポートをダイナミックにするには、ポート上でポート セキュリティをディセーブルにしておく必要があります。
- プライベート VLAN ポートは、ダイナミックアクセス ポートにできません。
- ダイナミックアクセス ポートを EtherChannel グループのメンバにすることはできません。
- ポート チャネルをダイナミックアクセス ポートとして設定することはできません。
- VMPS サーバ上に設定された VLAN を音声 VLAN にしないでください。
- 1K VLAN は Lan Base のデフォルト テンプレートが設定されている LAN Base イメージ上で実行するスイッチのみでサポートされます。

VMPS について

ダイナミック VLAN 割り当て

VLAN Query Protocol（VQP）は、ダイナミックアクセス ポートをサポートする場合に使用します。ダイナミックアクセス ポートは VLAN に永続的に割り当てられるのではなく、ポートで認識された MAC（メディア アクセス コントロール）送信元アドレスに基づいて VLAN を割り当てます。 未知の MAC アドレスが検出されるたびに、スイッチはリモート VLAN メンバーシップ ポリシー サーバ（VMPS）に VQP クエリーを送信します。そのクエリーには、新たに検出された MAC

アドレスおよび検出場所のポートが含まれます。 VMPS はそのポートの VLAN 割り当てで応答します。 このスイッチを VMPS サーバにすることはできませんが、VMPS のクライアントとして機能させ、VQP を介して通信することができます。

クライアント スイッチは新しいホストの MAC アドレスを受信するたびに、VMPS に VQP クエリーを送信します。 このクエリーを受信した VMPS は、データベースで MAC アドレスと VLAN のマッピングを検索します。 サーバの応答は、このマッピングと、サーバがオープンモードかセキュア モードかに基づいて行われます。 セキュア モードの場合、サーバは不正なホストが検出されると、ポートをシャットダウンします。 オープンモードでは、サーバはホストに対してポート アクセスを拒否します。

ポートが未割り当ての場合（つまり、VLAN 割り当てがまだ設定されていない場合）、VMPS は次のいずれかの応答を行います。

- そのポートでホストが許可されている場合、VMPS は割り当てられた VLAN 名を指定し、ホストへのアクセスを許可する VLAN 割り当て応答をクライアントに送信します。
- そのポートでホストが許可されておらず、なおかつ VMPS がオープン モードの場合、VMPS はアクセス拒否応答を送信します。
- そのポートで VLAN が許可されておらず、なおかつ VMPS がセキュア モードの場合、VMPS はポートシャットダウン応答を送信します。

ポートに VLAN 割り当てがすでに設定されている場合、VMPS は次のいずれかの応答を行います。

- データベース内の VLAN がポート上の現在の VLAN と一致した場合、VMPS は成功応答を送信し、ホストへのアクセスを許可します。
- データベース内の VLAN がポート上の現在の VLAN と一致せず、なおかつポート上にアクティブ ホストが存在する場合、VMPS は VMPS のセキュア モードに応じて、アクセス拒否またはポートシャットダウン応答を送信します。

VMPS からアクセス拒否応答を受け取った場合、スイッチはそのホスト MAC アドレスとの間のトラフィックを引き続きブロックします。 スイッチはポート宛てのパケットを引き続きモニタし、新しいホストアドレスを検出すると VMPS にクエリーを送信します。 VMPS からポートシャットダウン応答を受信した場合、スイッチはそのポートをディセーブルにします。 Network Assistant、CLI（コマンドライン インターフェイス）、または SNMP（簡易ネットワーク管理プロトコル）を使用して、ポートを手動で再びイネーブルにする必要があります。

関連トピック

VMPS クライアント上のダイナミックアクセス ポートの設定, （2026 ページ）

例：VMPS の設定, （2033 ページ）

ダイナミックアクセス ポート VLAN メンバーシップ

ダイナミックアクセス ポートが所属できるのは、VLAN ID が 1 ～ 4094 の 1 つの VLAN だけです。 リンクがアクティブになっても、VMPS によって VLAN が割り当てられるまで、スイッチは

このポートとの間のトラフィック転送を行いません。 VMPS は、ダイナミックアクセス ポートに接続した新しいホストの最初のパケットから送信元 MAC アドレスを受信し、VMPS データベースの VLAN とその MAC アドレスを照合します。

一致した場合、VMPS はそのポートの VLAN 番号を送信します。 クライアント スイッチがまだ設定されていない場合、VMPS からトランク ポートで受信した最初の VTP パケットからのドメイン名を使用します。 クライアント スイッチがすでに設定されている場合は、クエリ パケットにスイッチのドメイン名を含めて VMPS に送信し、VLAN 番号を取得します。 VMPS はパケット内のドメイン名が自身のドメイン名と一致することを確認した後、要求を受け入れ、クライアントに割り当てられた VLAN 番号を応答します。 一致しない場合、（VMPS セキュア モードの設定に応じて）VMPS は要求を拒否するか、ポートをシャットダウンします。

ダイナミックアクセス ポート上で複数のホスト（MAC アドレス）をアクティブにできますが、それらのホストはすべて同じ VLAN に存在する必要があります。ただし、ポート上でアクティブなホスト数が 20 を超えると、VMPS はダイナミックアクセス ポートをシャットダウンします。

ダイナミックアクセス ポート上でリンクがダウンになると、ポートは切り離された状態に戻り、VLAN の所属から外れます。 ポート経由でオンラインになるホストは VMPS によって VQP 経由で再チェックされてから、ポートが VLAN に割り当てられます。

ダイナミックアクセス ポートは、直接ホスト接続に使用したり、ネットワークに接続したりできます。 スイッチ上のポートごとに、最大 20 個の MAC アドレスを使用できます。 ダイナミックアクセス ポートが一度に所属できる VLAN は 1 つだけですが、VLAN は検出された MAC アドレスに基づいて後で変更されることがあります。

関連トピック

VMPS クライアント上のダイナミックアクセス ポートの設定, （2026 ページ）

例：VMPS の設定, （2033 ページ）

デフォルトの VMPS クライアント設定

次の表に、クライアント スイッチ上のデフォルトの VMPS およびダイナミックアクセス ポートの設定を記載します。

表 *183*：*VMPS* クライアントおよびダイナミックアクセス ポートのデフォルト設定

機能	デフォルト設定
VMPS ドメイン サーバ	なし
VMPS 再確認インターバル	60 分
VMPS サーバ再試行回数	3
ダイナミックアクセス ポート	未設定

VMPS の設定方法

VMPS の IP アドレスの入力

（注） スイッチ クラスタに対して VMPS を定義する場合は、コマンド スイッチにこのアドレスを入力する必要があります。

はじめる前に

スイッチをクライアントとして設定するには、サーバの IP アドレスを最初に入力する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **vmps server***ipaddress***primary**
4. **vmps server***ipaddress*
5. **end**
6. **show vmps**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vmps server***ipaddress***primary** 例： `Switch(config)# vmps server 10.1.2.3 primary`	プライマリ VMPS サーバとして機能するスイッチの IP アドレスを入力します。

	コマンドまたはアクション	目的
ステップ 4	**vmps server***ipaddress* 例： `Switch(config)# vmps server 10.3.4.5`	（任意）セカンダリ VMPS サーバとして機能するスイッチの IP アドレスを入力します。 セカンダリ サーバのアドレスは、3 つまで入力できます。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show vmps** 例： `Switch# show vmps`	表示された [VMPS Domain Server] フィールドの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

VMPS クライアント上のダイナミックアクセス ポートの設定

注意 ダイナミックアクセス ポート VLAN メンバーシップはエンド ステーション用、またはエンド ステーションに接続されたハブ用です。 他のスイッチにダイナミックアクセス ポートを接続すると、接続が切断されることがあります。

クラスタ メンバ スイッチのポートをダイナミックアクセス ポートとして設定する場合には、最初に **rcommand** 特権 EXEC コマンドを使用して、そのクラスタ メンバ スイッチにログインします。

はじめる前に

ダイナミックアクセス ポートを動作させるには、VMPS に IP 接続できなければなりません。 IP 接続が可能かどうかをテストするには、VMPS の IP アドレスに ping を実行し、応答が得られるかどうかを確認します。

（注） インターフェイスをデフォルト設定に戻すには、**default interface***interface-id* インターフェイス コンフィギュレーション コマンドを使用します。 インターフェイスをデフォルトのスイッチ ポート モード（dynamic auto）に戻すには、**no switchport mode** インターフェイス コンフィギュレーション コマンドを使用します。 アクセス モードをスイッチのデフォルト VLAN にリセットするには、**no switchport access vlan** インターフェイス コンフィギュレーション コマンドを使用します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode access**
5. **switchport access vlan dynamic**
6. **end**
7. **show interfaces***interface-id***switchport**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**switchport mode access** 例： `Switch(config-if)# switchport mode access`	ポートをアクセス モードに設定します。
ステップ 5	**switchport access vlan dynamic** 例： `Switch(config-if)# switchport access vlan dynamic`	ポートをダイナミック VLAN メンバーシップ適格として設定します。 ダイナミックアクセス ポートは、エンド ステーションに接続されている必要があります。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet 1/0/1 switchport`	表示された [Operational Mode] フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ダイナミック VLAN 割り当て，（2022 ページ）

ダイナミックアクセス ポート VLAN メンバーシップ，（2023 ページ）

例：VMPS の設定，（2033 ページ）

VLAN メンバーシップの再確認

このタスクでは、スイッチが VMPS から受信したダイナミックアクセス ポート VLAN メンバーシップの割り当てを確認します。

手順の概要

1. **enable**
2. **vmpsreconfirm**
3. **showvmps**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**vmpsreconfirm** 例： `Switch# vmps reconfirm`	ダイナミックアクセス ポート VLAN メンバーシップを再確認します。
ステップ 3	**showvmps** 例： `Switch# show vmps`	ダイナミック VLAN 再確認ステータスを確認します。

再確認インターバルの変更

VMPS クライアントは、VMPS から受信した VLAN メンバーシップ情報を定期的に再確認します。 この再確認を行う間隔を分単位で設定できます。

（注） クラスタのメンバ スイッチを設定する場合、このパラメータはコマンド スイッチの再確認インターバルの設定値以上でなければなりません。 また、メンバスイッチにログインするには、最初に **rcommand** 特権 EXEC コマンドを使用する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **vmps reconfirm***minutes*
4. **end**
5. **show vmps**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vmps reconfirm***minutes* 例： `Switch(config)# vmps reconfirm 90`	ダイナミック VLAN メンバーシップの再確認を行う間隔（分）を設定します。 指定できる範囲は 1 ～ 120 です。 デフォルトは 60 分です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vmps** 例： `Switch# show vmps`	表示された [Reconfirm Interval] フィールドのダイナミック VLAN の再確認ステータスを確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	startup-config	

再試行回数の変更

スイッチが次のサーバにクエリーを送信する前に VMPS への接続を試行する回数を変更するには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **vmps retry***count*
4. **end**
5. **show vmps**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vmps retry***count* 例： `Switch(config)# vmps retry 5`	再試行の回数を変更します。 指定できる再試行回数の範囲は 1 ～ 10 です。デフォルトは 3 です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vmps** 例： `Switch# show vmps`	表示された [Server Retry Count] フィールドの設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

ダイナミックアクセス ポート VLAN メンバーシップのトラブルシューティング

問題　VMPS は次の状況でダイナミックアクセス ポートをシャットダウンします。

- **問題** VMPS がセキュアモードであり、なおかつホストのポートへの接続を許可しない場合。VMPS はポートをシャットダウンして、ホストがネットワークに接続できないようにします。
- **問題**　ダイナミックアクセス ポート上のアクティブ ホストが 20 を超えた場合。

解決法　ディセーブルになっているダイナミックアクセス ポートを再びイネーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドに続けて、**no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

VMPS のモニタリング

show vmps 特権 EXEC コマンドを使用して、VMPS に関する情報を表示できます。 スイッチは VMPS に関する次の情報を表示します。

- VMPS VQP バージョン：VMPS との通信に使用する VQP のバージョン。 スイッチは VQP バージョン 1 を使用する VMPS にクエリーを送信します。
- 再確認インターバル：スイッチが VLAN と MAC アドレスの割り当てを再確認する間隔（分）。

- サーバ再試行回数：VQP が VMPS にクエリーを再送信する回数。 この回数試行しても応答が得られない場合、スイッチはセカンダリ VMPS へのクエリーを開始します。
- VMPS ドメイン サーバ：設定されている VLAN メンバーシップ ポリシー サーバの IP アドレス。 スイッチスイッチは *current* と表示されているサーバにクエリーを送信します。 *primary* と表示されているサーバは、プライマリ サーバです。
- VMPS 動作：最近の再確認の結果。 再確認は、再確認インターバルが経過したときに自動的に行われますが、**vmps reconfirm** 特権 EXEC コマンドを入力するか、Network Assistant あるいは SNMP で同等の操作を行うことによって、強制的に再確認することもできます。

次に、**show vmps** 特権 EXEC コマンドの出力例を示します。

```
Switch# show vmps
VQP Client Status:
---------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:         other
```

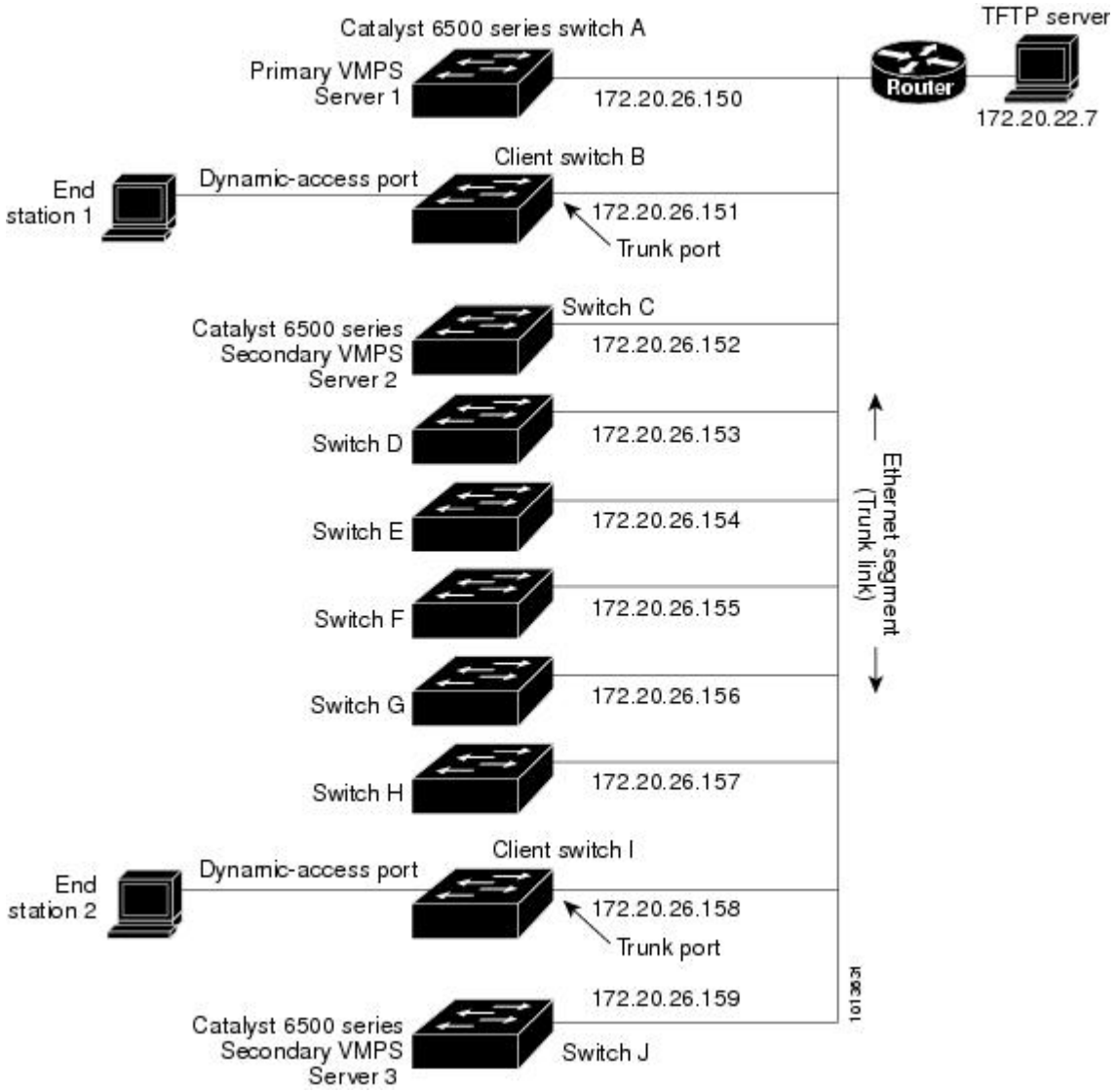
VMPS の設定例

例：VMPS の設定

VMPS サーバ スイッチと VMPS クライアント スイッチでダイナミックアクセス ポートを使用するこのネットワークは、次のように設定されます。

- VMPS サーバと VMPS クライアントは、それぞれ別のスイッチです。
- Catalyst 6500 シリーズのスイッチ A が、プライマリ VMPS サーバです。
- Catalyst 6500 シリーズのスイッチ C およびスイッチ J が、セカンダリ VMPS サーバです。
- エンド ステーションはクライアント（スイッチ B、スイッチ I）に接続されています。
- データベース コンフィギュレーション ファイルは、IP アドレス 172.20.22.7 の TFTP サーバに保存されています。

図 *128*：ダイナミック ポート *VLAN* メンバーシップの構成例



関連トピック

VMPS クライアント上のダイナミックアクセス ポートの設定，（2026 ページ）
ダイナミック VLAN 割り当て，（2022 ページ）
ダイナミックアクセス ポート VLAN メンバーシップ，（2023 ページ）

次の作業

次の設定を行えます。

- VTP

- VLANs
- VLAN トランキング
- プライベート VLAN
- 音声 VLAN

第 77 章

音声 VLAN の設定

- 機能情報の確認，2037 ページ
- 音声 VLAN の前提条件，2037 ページ
- 音声 VLAN の制約事項，2038 ページ
- 音声 VLAN に関する情報，2038 ページ
- 音声 VLAN の設定方法，2041 ページ
- 音声 VLAN のモニタリング，2046 ページ
- 設定例，2046 ページ
- 次の作業，2047 ページ

機能情報の確認

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

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

音声 VLAN の前提条件

音声 VLAN の前提条件は、次のとおりです。

- 音声 VLAN 設定はスイッチのアクセス ポートだけでサポートされており、トランク ポートではサポートされていません。

（注） トランク ポートは、標準 VLAN と同様に、任意の数の音声 VLAN を伝送できます。 トランク ポートでは、音声 VLAN の設定がサポートされません。

- 音声 VLAN をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチ上で QoS をイネーブルに設定し、さらに **mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力してポートの信頼状態を trust に設定しておくことを推奨します。 Auto-QoS 機能を使用すると、これらは自動的に設定されます。
- IP Phone にコンフィギュレーションを送信するために、Cisco IP Phone に接続するスイッチ ポート上で CDP をイネーブルにする必要があります （デフォルト設定では、CDP がすべてのスイッチ インターフェイスでグローバルにイネーブルになっています）。

音声 VLAN の制約事項

音声 VLAN には、スタティック セキュア MAC アドレスを設定できません。

音声 VLAN に関する情報

音声 VLAN

音声 VLAN 機能を使用すると、アクセス ポートで IP Phone からの IP 音声トラフィックを伝送できます。 スイッチを Cisco 7960 IP Phone に接続すると、IP Phone はレイヤ 3 IP 値およびレイヤ 2 サービス クラス（CoS）値を使用して、音声トラフィックを送信します。どちらの値もデフォルトでは 5 に設定されます。 データ送信が均質性に欠ける場合、IP Phone の音質が低下することがあります。そのため、このスイッチは IEEE 802.1p CoS に基づく Quality of Service（QoS）をサポートしています。 QoS は、分類およびスケジューリングを使用して、スイッチからのネットワーク トラフィックを予測可能な方法で送信します。

Cisco7960 IP Phone は設定可能なデバイスであり、IEEE 802.1p プライオリティに基づいてトラフィックを転送するように設定できます。 Cisco IP Phone によって割り当てられたトラフィック プライオリティを信頼したり、オーバーライドしたりするようにスイッチを設定できます。

Cisco IP Phone の音声トラフィック

Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。 Cisco Discovery Protocol（CDP）パケットを送信するよう、スイッチ上のアクセス ポートを設定できます。CDP パケットは、接続する IP Phone に対して、次のいずれかの方法で音声トラフィックをスイッチに送信するよう指示します。

- レイヤ 2 CoS プライオリティ値のタグ付き音声 VLAN による送信

- レイヤ 2 CoS プライオリティ値のタグ付きアクセス VLAN による送信
- タグなし（レイヤ 2 CoS プライオリティ値なし）のアクセス VLAN による送信

（注） いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（音声トラフィックはデフォルトで 5、音声制御トラフィックは 3）を伝送します。

関連トピック

Cisco IP Phone の音声トラフィックの設定

例：Cisco IP Phone の音声トラフィックの設定, （2046 ページ）

Cisco IP Phone のデータ トラフィック

スイッチは、Cisco IP Phone のアクセス ポートに接続されたデバイスから送られる、タグ付きデータ トラフィック（IEEE 802.1Q または IEEE 802.1p フレーム タイプのトラフィック）を処理することもできます。 CDP パケットを送信するよう、スイッチ上のレイヤ 2 アクセス ポートを設定できます。CDP パケットは、接続する IP Phone に対して、次のいずれかのモードで IP Phone アクセス ポートを設定するよう指示します。

- trusted（信頼性がある）モードでは、Cisco IP Phone のアクセス ポート経由で受信したすべてのトラフィックがそのまま IP Phone を通過します。
- untrusted（信頼性がない）モードでは、Cisco IP Phone のアクセス ポート経由で受信した IEEE 802.1Q および IEEE 802.1p フレームのすべてのトラフィックに、設定されたレイヤ 2 CoS 値を与えます。 デフォルトのレイヤ 2 CoS 値は 0 です。 信頼できないモードがデフォルト設定です。

（注） Cisco IP Phone に接続されたデバイスからのタグなしトラフィックは、IP Phone のアクセス ポートの信頼状態に関係なく、そのまま IP Phone を通過します。

関連トピック

着信データ フレームのプライオリティ設定, （2044 ページ）

例：着信データ フレームのプライオリティの設定, （2046 ページ）

音声 VLAN 設定時の注意事項

- Cisco7960 IP Phone は、PC やその他のデバイスとの接続もサポートしているので、スイッチを Cisco IP Phone に接続するポートは、さまざまな種類のトラフィックを伝送できます。 ポートを設定することによって、Cisco IP Phone による音声トラフィックおよびデータ トラフィックの伝送方法を決定できます。

- IP Phone で音声 VLAN 通信が適切に行われるには、スイッチ上に音声 VLAN が存在し、アクティブになっている必要があります。 VLAN が存在しているかどうかを確認するには、**show vlan** 特権 EXEC コマンドを使用します（リストで表示されます）。 VLAN がリストされていない場合は、音声 VLAN を作成します。
- Power Over Ethernet（PoE）スイッチは、シスコ先行標準の受電デバイスまたは IEEE 802.3af 準拠の受電デバイスが AC 電源から電力を供給されてない場合に、それらの受電デバイスに自動的に電力を供給できます。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。 音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。
- Cisco IP Phone とその IP Phone に接続されたデバイスが同じ VLAN 上にある場合、両方とも同じ IP サブネットに属していなければなりません。 次の条件が満たされている場合は、同じ VLAN 上にあります。
  - 両方とも IEEE 802.1p またはタグなしフレームを使用する。
  - Cisco IP Phone が IEEE 802.1p フレームを使用し、デバイスがタグなしフレームを使用する。
  - Cisco IP Phone がタグなしフレームを使用し、デバイスが IEEE 802.1p フレームを使用する。
  - Cisco IP Phone が IEEE 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである。
- Cisco IP Phone と IP Phone に接続されたデバイスは、同一 VLAN、同一サブネット上にあっても、使用するフレーム タイプが異なる場合は通信できません。トラフィックは同一サブネット上でルーティングされないからです（ルーティングによってフレーム タイプの相違が排除されます）。
- 音声 VLAN ポートには次のポート タイプがあります。
  - ダイナミック アクセス ポート。
  - IEEE 802.1x 認証ポート。

    （注） 音声 VLAN が設定され Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x をイネーブルにした場合、その IP Phone からスイッチへの接続が最大 30 秒間失われます。

  - 保護ポート。
  - SPAN または RSPAN セッションの送信元ポートまたは宛先ポート。
  - セキュア ポート。

（注） 音声 VLAN も設定しているインターフェイス上でポート セキュリティをイネーブルにする場合、ポートで許容されるセキュア アドレスの最大数を、アクセス VLAN におけるセキュア アドレスの最大数に 2 を足した数に設定する必要があります。 ポートを Cisco IP Phone に接続している場合、IP Phone に最大で 2 つの MAC アドレスが必要になります。 IP Phone のアドレスは、音声 VLAN で学習され、アクセス VLAN でも学習される場合があります。 PC を IP Phone に接続する場合、追加の MAC アドレスが必要になります。

音声 VLAN のデフォルト設定

音声 VLAN 機能は、デフォルトではディセーブルに設定されています。

音声 VLAN 機能がイネーブルの場合、すべてのタグなしトラフィックはポートのデフォルトの CoS プライオリティに従って送信されます。

IEEE 802.1p または IEEE 802.1Q のタグ付きトラフィックでは、CoS 値が信頼されません。

音声 VLAN の設定方法

Cisco IP Phone の音声トラフィックの設定

Cisco IP Phone に CDP パケットを送信して IP Phone による音声トラフィックの送信方法を設定するように、IP Phone に接続するポートを設定できます。 IP Phone は指定された音声 VLAN に、レイヤ 2 CoS 値を使用して、IEEE 802.1Q フレームの音声トラフィックを伝送できます。 IEEE 802.1p のプライオリティ タグを使用すると、音声トラフィックにさらに高いプライオリティを与え、すべての音声トラフィックをネイティブ（アクセス）VLAN 経由で転送できます。 Cisco IP Phone はタグなしの音声トラフィックを送信する、または独自の設定を使用してアクセス VLAN で音声トラフィックを送信することもできます。 いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（デフォルトは 5）を伝送します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **mls qos trust cos**
5. **switchport voice**{**vlan**{*vlan-id* | **dot1p** | **none** | **untagged**}}
6. **end**
7. 次のいずれかを使用します。
   - **show interfaces***interface-id***switchport**
   - **show running-config interface***interface-id*
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**mls qos trust cos** 例： `Switch(config-if)# mls qos trust cos`	パケットの CoS 値を使用して着信トラフィック パケットを分類するよう、インターフェイスを設定します。 タグなしパケットの場合、ポートのデフォルト CoS 値が使用されます。 （注） ポートの信頼状態を設定する前に、**mls qos** グローバル コンフィギュレーション コマンドを使用することによって、QoS をグローバルでイネーブルに設定しておく必要があります。

	コマンドまたはアクション	目的
ステップ 5	**switchport voice**{**vlan**{*vlan-id* | **dot1p** | **none** | **untagged**}} 例： `Switch(config-if)# switchport voice vlan dot1p`	音声 VLAN を設定します。 • *vlan-id*：すべての音声トラフィックが特定の VLAN を経由して転送されるように IP Phone を設定します。 デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。 指定できる VLAN ID の範囲は 1 ～ 4094 です。 • **dot1p**：VLAN ID 0（ネイティブ VLAN）のタグが付けられた音声およびデータ IEEE 802.1p プライオリティ フレームを受け入れるよう、スイッチを設定します。 デフォルトでは、スイッチは VLAN 0 のタグが付いたすべての音声およびデータ トラフィックをドロップします。 802.1p に対応するよう設定されると、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用してトラフィックを転送します。 • **none**：IP Phone で独自の設定を使ってタグなし音声トラフィックを送信できるようにします。 • **untagged**：タグなし音声トラフィックを送信するように IP Phone を設定します。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

ステップ 7	次のいずれかを使用します。
	
	• **show interfaces***interface-id***switchport**
	
	• **show running-config interface***interface-id*
	
	例：
	
	`Switch# show interfaces gigabitethernet1/0/1 switchport`
	
	または
	
	`Switch# show running-config interface gigabitethernet1/0/1`
		音声 VLAN の設定、または QoS および音声 VLAN の設定を確認します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

着信データ フレームのプライオリティ設定

PC またはその他のデータ デバイスを Cisco IP Phone ポートに接続できます。 タグ付きデータ トラフィック（IEEE 802.1Q または IEEE 802.1p フレーム）を処理するために、CDP パケットを送信するようスイッチを設定できます。CDP パケットは Cisco IP Phone に対して、IP Phone 上のアクセス ポートに接続されたデバイスからのデータ パケット送信方法を指示します。 PC は、CoS 値が割り当てられたパケットを生成できます。 接続デバイスから IP Phone のポートに届いたフレームのプライオリティを変更しない（信頼する）または変更する（信頼しない）ように、IP Phone を設定できます。

Cisco IP Phone で非音声ポートから受信するデータ トラフィックのプライオリティを設定するには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport priority extend** {**cos***value* | **trust**}
5. **end**
6. **show interfaces***interface-id***switchport**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	Cisco IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport priority extend** {**cos***value* | **trust**} 例： `Switch(config-if)# switchport priority extend trust`	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプライオリティを次のように設定します。 • **cos***value*：PC または接続しているデバイスから受信したプライオリティを、指定の CoS 値にオーバーライドするよう、IP Phone を設定します。 値は 0 ～ 7 です。 7 が最高のプライオリティです。 デフォルトのプライオリティは **cos** 0 です。 • **trust**：PC または接続しているデバイスから受信したプライオリティを信頼するよう IP Phone アクセス ポートを設定します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces***interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

Cisco IP Phone のデータ トラフィック，（2039 ページ）
例：着信データ フレームのプライオリティの設定，（2046 ページ）

音声 VLAN のモニタリング

インターフェイスの音声 VLAN 設定を表示するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを使用します。

設定例

例：Cisco IP Phone の音声トラフィックの設定

次の例では、CoS 値を使用して着信トラフィックを分類し、VLAN ID 0 のタグが付いた音声およびデータ プライオリティ トラフィックを受け付けるよう、Cisco IP Phone に接続しているポートを設定する方法について示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

ポートをデフォルト設定に戻すには、**no switchport voice vlan** インターフェイス コンフィギュレーション コマンドを使用します。

関連トピック

Cisco IP Phone の音声トラフィックの設定
Cisco IP Phone の音声トラフィック，（2038 ページ）

例：着信データ フレームのプライオリティの設定

次に、Cisco IP Phone に接続しているポートを設定して、PC または接続しているデバイスから受信するフレームのプライオリティを変更しないようにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport priority extend trust
Switch(config-if)# end
```

ポートをデフォルト設定に戻すには、**no switchport priority extend** インターフェイス コンフィギュレーション コマンドを使用します。

関連トピック

着信データ フレームのプライオリティ設定，（2044 ページ）

Cisco IP Phone のデータ トラフィック，（2039 ページ）

次の作業

音声 VLAN を設定した後は、次の設定を行うことができます。

- VLANs
- VLAN トランキング
- VTP
- プライベート VLAN

第 78 章

プライベート VLAN の設定

- 機能情報の確認，2049 ページ
- プライベート VLAN の前提条件，2049 ページ
- プライベート VLAN の制約事項，2050 ページ
- プライベート VLAN について，2051 ページ
- プライベート VLAN の設定方法，2060 ページ
- プライベート VLAN のモニタ，2071 ページ
- プライベート VLAN の設定例，2071 ページ
- 次の作業，2073 ページ
- その他の参考資料，2073 ページ

機能情報の確認

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

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

プライベート VLAN の前提条件

プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は、VTP 3 のサーバ モードでもサポートされます。

プライベート VLAN をスイッチに設定するときに、ユニキャスト ルートとレイヤ 2 エントリとの間のシステム リソースのバランスを取るために、常にデフォルトの Switch Database Management（SDM）テンプレートを使用してください。 別の SDM テンプレートが設定されている場合、デフォルト テンプレートを設定するのに **sdm prefer default** グローバル コンフィギュレーション コマンドを使用します。

プライベート VLAN の制約事項

プライベート VLAN はLAN Base イメージを実行しているスイッチではサポートされません。

（注） 一部の状況では、エラー メッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

- プライベート VLAN が設定されているスイッチでは、フォールバック ブリッジングを設定しないでください。
- リモート SPAN（RSPAN）をプライベート VLAN のプライマリまたはセカンダリ VLAN として設定しないでください。
- 次のような機能が設定されているインターフェイスにプライベート VLAN ポートを設定しないでください。
  - ダイナミック アクセス ポート VLAN メンバーシップ
  - ダイナミック トランキング プロトコル（DTP）
  - IPv6 Security Group（SG）
  - ポート集約プロトコル（PAgP）
  - リンク集約制御プロトコル（LACP）
  - マルチキャスト VLAN レジストレーション（MVR）
  - 音声 VLAN
  - Web Cache Communication Protocol（WCCP）
- IEEE 802.1x ポートベース認証をプライベート VLAN ポートに設定できますが、802.1x とポート セキュリティ、音声 VLAN、またはポート単位のユーザ ACL は、プライベート VLAN ポートに設定できません。
- プライベート VLAN ホストまたは無差別ポートは SPAN 宛先ポートにはできません。 SPAN 宛先ポートをプライベート VLAN ポートに設定した場合、ポートは非アクティブになります。
- プライマリ VLAN の無差別ポートでスタティック MAC アドレスを設定する場合は、すべての関連セカンダリ VLAN に同じスタティック アドレスを追加する必要はありません。 同様に、セカンダリ VLAN のホスト ポートでスタティック MAC アドレスを設定する場合は、関

連プライマリ VLAN に同じスタティック MAC アドレスを追加する必要はありません。 さらに、スタティック MAC アドレスをプライベート VLAN ポートから削除する際に、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要はありません。

（注） プライベート VLAN のセカンダリ VLAN で学習したダイナミック MAC アドレスは、関連プライマリ VLAN で複製されます。 プライマリ VLAN からトラフィックが入力される場合でも、すべての MAC エントリはセカンダリ VLAN で学習されます。 MAC アドレスがプライマリ VLAN で動的に学習される場合は、関連セカンダリ VLAN では複製されません。

- レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。

プライベート VLAN について

プライベート VLAN ドメイン

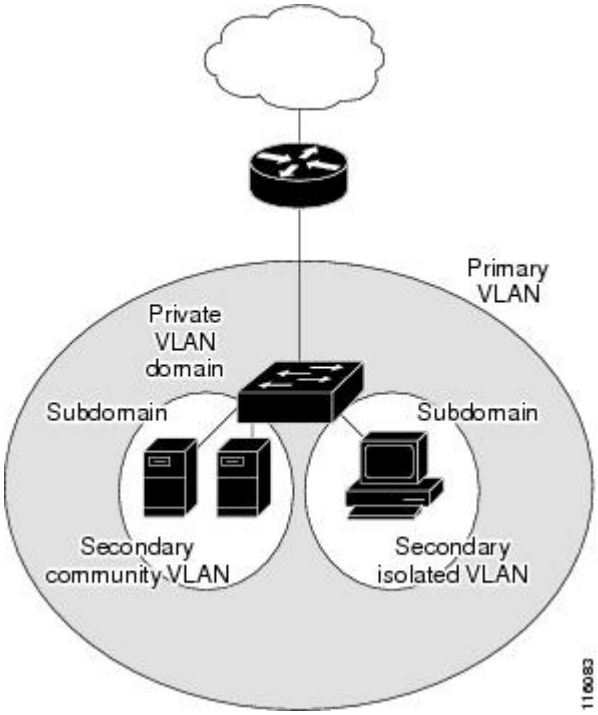
PVLAN 機能を使用すると、サービス プロバイダーが VLAN を使用したときに直面する 2 つの問題に対処できます。

- IP Base イメージまたは IP Services イメージを実行している場合、最大で 個のアクティブ VLAN がスイッチでサポートされます。 サービス プロバイダーが 1 カスタマーあたり 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数はこれに制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てますが、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。

プライベート VLAN を使用することでスケーラビリティの問題に対処でき、サービス プロバイダーにとっては IP アドレス管理上の利得がもたらされ、カスタマーに対してはレイヤ 2 セキュリティを提供できます。 プライベート VLAN では、通常の VLAN ドメインをサブドメインに分割します。 サブドメインは、プライマリ VLAN とセカンダリ VLAN のペアで表されます。 プライベート VLAN には複数の VLAN ペアを設定可能で、各サブドメインにつき 1 ペアになります。

プライベート VLAN 内のすべての VLAN ペアは同じプライマリ VLAN を共有します。 セカンダリ VLAN ID は、各サブドメインの区別に使用されます。

図 *129*：プライベート *VLAN* ドメイン



セカンダリ VLAN

セカンダリ VLAN には、次の 2 種類があります。

- 独立 VLAN：独立 VLAN 内のポートは、レイヤ 2 レベルでは相互に通信できません。
- コミュニティ VLAN：コミュニティ VLAN 内のポートは互いに通信できますが、レイヤ 2 レベルにある他のコミュニティ内のポートとは通信できません。

関連トピック

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング，（2068 ページ）

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする，（2072 ページ）

プライベート VLAN ポート

プライベート VLAN では、同じプライベート VLAN 内のポート間をレイヤ 2 で分離します。 プライベート VLAN ポートは、次のいずれかの種類に属するアクセス ポートです。

- 無差別：無差別ポートは、プライベート VLAN に属し、プライマリ VLAN と関連しているセカンダリ VLAN に属するコミュニティ ポートや独立ホスト ポートなどの、すべてのインターフェイスと通信できます。
- 独立：独立ポートは、独立セカンダリ VLAN に属しているホスト ポートです。 これは、無差別ポートを除く、同じプライベート VLAN 内の他のポートからレイヤ 2 で完全に分離されています。 プライベート VLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。 独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。
- コミュニティ：コミュニティ ポートは、1 つのコミュニティ セカンダリ VLAN に属しているホスト ポートです。 コミュニティ ポートは、同一コミュニティ VLAN のその他のポート、および無差別ポートと通信します。 これらのインターフェイスは、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN 内の独立ポートとレイヤ 2 で分離されます。

（注） トランク ポートは、通常の VLAN からのトラフィックを伝送し、またプライマリ、独立、およびコミュニティ VLAN からのトラフィックも伝送します。

プライマリおよびセカンダリ VLAN には次のような特性があります。

- プライマリ VLAN：プライベート VLAN には、プライマリ VLAN を 1 つだけ設定できます。 プライベート VLAN 内のすべてのポートは、プライマリ VLAN のメンバーです。 プライマリ VLAN は、無差別ポートからの単一方向トラフィックのダウンストリームを、（独立およびコミュニティ）ホスト ポートおよび他の無差別ポートへ伝送します。
- 独立 VLAN：プライベート VLAN の独立 VLAN は 1 つだけです。 独立 VLAN はセカンダリ VLAN であり、ホストから無差別ポートおよびゲートウェイに向かう単一方向トラフィックアップストリームを搬送します。
- コミュニティ VLAN：コミュニティ VLAN は、アップストリーム トラフィックをコミュニティ ポートから無差別ポート ゲートウェイおよび同じコミュニティ内の他のホスト ポートに伝送するセカンダリ VLAN です。 複数のコミュニティ VLAN を 1 つのプライベート VLAN に設定できます。

無差別ポートは、1 つのプライマリ VLAN、1 つの独立 VLAN、複数のコミュニティ VLAN だけで動作できます。 レイヤ 3 ゲートウェイは通常、無差別ポートを介してスイッチに接続されます。 無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。 たとえば、すべてのプライベート VLAN サーバを管理ワークステーションから監視したりバックアップしたりするのに、無差別ポートを使用できます。

関連トピック

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定, （2064 ページ）
プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定, （2066 ページ）
例：ホスト ポートとしてのインターフェイスの設定, （2071 ページ）

例：インターフェイスをプライベート VLAN 無差別ポートとして設定する，（2072 ページ）

ネットワーク内のプライベート VLAN

スイッチング環境では、個々のエンドステーションに、または共通グループのエンドステーションに、個別のプライベート VLAN や、関連する IP サブネットを割り当てることができます。 エンド ステーションはデフォルト ゲートウェイとの通信を行うだけで、プライベート VLAN の外部と通信することができます。

プライベート VLAN を使用し、次の方法でエンド ステーションへのアクセスを制御できます。

- エンド ステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ 2 の通信をしないようにします。 たとえば、エンド ステーションがサーバの場合、この設定によりサーバ間のレイヤ 2 通信ができなくなります。
- デフォルト ゲートウェイおよび選択したエンド ステーション（バックアップ サーバなど）に接続されているインターフェイスを無差別ポートとして設定し、すべてのエンド ステーションがデフォルト ゲートウェイにアクセスできるようにします。

複数のデバイスにわたるようにプライベート VLAN を拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他のデバイスにトランキングします。 使用するプライベート VLAN 設定のセキュリティを確保して、プライベート VLAN として設定された VLAN が他の目的に使用されないようにするには、プライベート VLAN ポートがないデバイスを含めて、すべての中間デバイスでプライベート VLAN を設定します。

プライベート VLAN での IP アドレッシング方式

各カスタマーに個別の VLAN を割り当てると、次のように IP アドレッシング方式が非効率的になります。

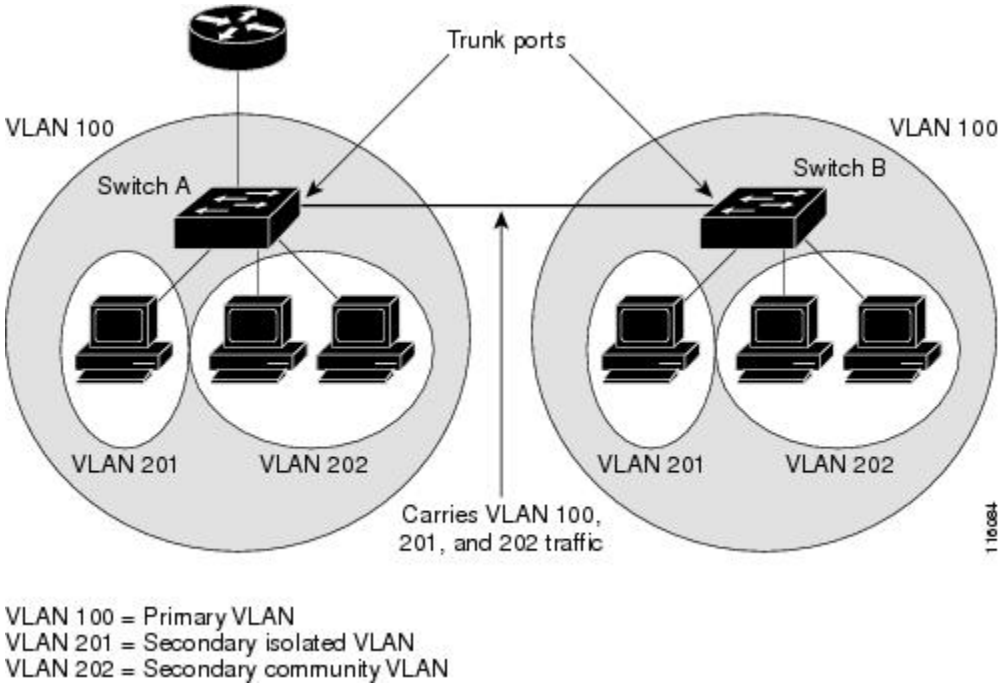
- カスタマー VLAN にアドレスのブロックを割り当てると、未使用 IP アドレスが発生することがあります。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベート VLAN のすべてのメンバーが、プライマリ VLAN に割り当てられている共通アドレス空間を共有するためです。 ホストはセカンダリ VLAN に接続され、プライマリ VLAN に割り当てられているアドレスのブロックから IP アドレスが DHCP サーバによってホストに割り当てられますが、同一プライマリ VLAN 内のセカンダリ VLAN には割り当てられません。 さまざまなセカンダリ VLAN のカスタマー デバイスには後続 IP アドレスが割り当てられます。 新しいデバイスを追加すると、サブネット アドレスの巨大プールから次に使用できるアドレスが、DHCP サーバによって割り当てられます。

複数のスイッチにまたがるプライベート VLAN

通常の VLAN と同様に、プライベート VLAN を複数のスイッチにまたがるように設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN を隣接スイッチに伝送します。 トランク ポートはプライベート VLAN を他の VLAN として扱います。 複数のスイッチにまたがるプライベート VLAN の機能の特徴として、スイッチ A にある独立ポートからのトラフィックはスイッチ B に到達しません。

図 *130*：複数のスイッチにまたがるプライベート *VLAN*



プライベート VLAN は VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は VTP 3 のサーバ モードでもサポートされます。 VTP 3 を使用して設定したサーバクライアントがある場合、サーバに設定されているプライベート VLAN をクライアント上に反映させる必要があります。

プライベート VLAN の他機能との相互作用

プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック

通常の VLAN では、同じ VLAN にあるデバイスはレイヤ 2 レベルで互いに通信しますが、別の VLAN にあるインターフェイスに接続されたデバイスとはレイヤ 3 レベルで通信する必要があります。 プライベート VLAN の場合、無差別ポートはプライマリ VLAN のメンバーであり、ホスト ポートはセカンダリ VLAN に属します。 セカンダリ VLAN はプライマリ VLAN に対応付けられているため、これらの VLAN のメンバーはレイヤ 2 レベルで互いに通信できます。

通常の VLAN の場合、ブロードキャストはその VLAN のすべてのポートに転送されます。 プライベート VLAN のブロードキャストの転送は、次のようにブロードキャストを送信するポートによって決まります。

- 独立ポートは、無差別ポートまたはトランク ポートだけにブロードキャストを送信します。
- コミュニティ ポートは、すべての無差別ポート、トランク ポート、同一コミュニティ VLAN のポートにブロードキャストを送信します。
- 無差別ポートは、プライベート VLAN のすべてのポート（その他の無差別ポート、トランク ポート、独立ポート、コミュニティ ポート）にブロードキャストを送信します。

マルチキャスト トラフィックのルーティングとブリッジングは、プライベート VLAN 境界を横断して行われ、単一コミュニティ VLAN 内でも行われます。 マルチキャスト トラフィックは、同一独立 VLAN のポート間、または別々のセカンダリ VLAN のポート間で転送されません。

プライベート VLAN のマルチキャスト転送は次の状況をサポートします。

- 送信側が VLAN 外に存在する可能性があり、受信側が VLAN ドメイン内に存在している可能性がある。
- 送信側が VLAN 内に存在する可能性があり、受信側が VLAN ドメイン外に存在している可能性がある。
- 送信側と受信側が同一のコミュニティ VLAN に存在している可能性がある。

プライベート VLAN と SVI

レイヤ 3 スイッチスイッチでは、スイッチ仮想インターフェイス（SVI）が VLAN のレイヤ 3 インターフェイスを表します。 レイヤ3デバイスは、セカンダリ VLAN ではなく、プライマリ VLAN だけを介してプライベート VLAN と通信します。 レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。 レイヤ 3 VLAN インターフェイスをセカンダリ VLAN 用に設定できません。 VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI はアクティブになりません。

- SVI がアクティブである VLAN をセカンダリ VLAN として設定する場合、SVI をディセーブルにしないと、この設定は許可されません。
- セカンダリ VLAN として設定されている VLAN に SVI を作成しようとしてセカンダリ VLAN がすでにレイヤ 3 にマッピングされている場合、SVI は作成されず、エラーが返されます。 SVI がレイヤ 3 にマッピングされていない場合、SVI は作成されますが、自動的にシャットダウンされます。

プライマリ VLAN をセカンダリ VLAN と関連付けてマッピングすると、プライマリ VLAN の設定がセカンダリ VLAN の SVI に伝播されます。 たとえば、プライマリ VLAN の SVI に IP サブネットを割り当てると、このサブネットは、プライベート VLAN 全体の IP サブネット アドレスになります。

プライベート VLAN 設定時の注意事項

セカンダリ VLAN およびプライマリ VLAN の設定

プライベート VLAN の設定時は、次の注意事項に従ってください。

- プライベート VLAN は VTP 1、2、および 3 のトランスペアレント モードでサポートされます。 スイッチで VTP バージョン 1 または 2 が稼働している場合は、VTP をトランスペアレント モードに設定する必要があります。 プライベート VLAN を設定した後で、VTP モードをクライアントまたはサーバに変更できません。 VTP バージョン 3 は、すべてのモードでプライベート VLAN をサポートします。
- VTP バージョン 1 または 2 でプライベート VLAN を設定した後、**copy running-config startup config** 特権 EXEC コマンドを使用して、VTP トランスペアレント モード設定とプライベート VLAN 設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存します。 保存しないと、スイッチをリセットした場合、デフォルトの VTP サーバ モードになり、プライベート VLAN をサポートしなくなります。 VTP バージョン 3 ではプライベート VLAN をサポートします。
- VTP バージョン 1 および 2 では、プライベート VLAN 設定の伝播は行われません。 プライベート VLAN ポートが必要なデバイスで VTP バージョン 3 が実行されていない場合は、VTP3 はプライベート VLAN を伝播するため、そのデバイス上でプライベート VLAN を設定する必要があります。
- VLAN 1 または VLAN 1002 ～ 1005 をプライマリ VLAN またはセカンダリ VLAN として設定できません。 拡張 VLAN（VLAN ID 1006 ～ 4094）はプライベート VLAN に属することができます。
- プライマリ VLAN には、1 つの独立 VLAN および複数のコミュニティ VLAN を関連付けることができます。 独立 VLAN またはコミュニティ VLAN には、1 つのプライマリ VLAN だけを関連付けることができます。
- プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行可能なスパニングツリー プロトコル（STP）インスタンスは 1 つだけです。 セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。
- TFTP サーバから PVLAN 設定をコピーし、それを実行中の設定に適用しても、PVLAN の関連付けは形成されません。 プライマリ VLAN がすべてのセカンダリ VLAN に確実に関連付けられていることを確認する必要があります。

  また、**copy flash:config_file running-config** の代わりに **configure replace flash:config_file force** も使用できます。
- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。 プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、DHCP スヌーピングはセカンダリ VLAN に伝播されます。 セカンダリ VLAN で DHCP を設定しても、プライマリ VLAN をすでに設定している場合、DHCP 設定は有効になりません。

- プライベート VLAN ポートで IP ソース ガードをイネーブルにする場合は、プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。
- プライベート VLAN でトラフィックを伝送しないデバイスのトランクから、プライベート VLAN をプルーニングすることを推奨します。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の Quality of Service（QoS）設定を適用できます
- sticky ARP には、次の考慮事項があります。
  - sticky ARP エントリとは、SVI およびレイヤ 3 インターフェイス上で学習されるエントリです。 これらのエントリは、期限切れになることはありません。
  - **ip sticky-arp** グローバル コンフィギュレーション コマンドは、プライベート VLAN に属する SVI でだけサポートされます。
  - **ip sticky-arp** インターフェイス コンフィギュレーション コマンドは、以下でのみサポートされます。
    - レイヤ 3 インターフェイス
    - 標準 VLAN に属する SVI
    - プライベート VLAN に属する SVI

    ip sticky-arp グローバル コンフィギュレーション コマンドおよび **ip sticky-arp インターフェイス** コンフィギュレーション コマンドの使用の詳細については、このリリースのコマンド リファレンスを参照してください。
- プライマリ VLAN およびセカンダリ VLAN で VLAN マップを設定できます。 ただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- PVLAN は双方向です。 これらは、入力側と出力側の両方に適用されます。

  レイヤ 2 のフレームがプライベート VLAN 内で転送されると、入力側と出力側で VLAN マップが適用されます。 フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。 同様に、フレームが外部ポートからプライベート VLAN にルーティングされると、プライベート VLAN は出力側に適用されます。

  ブリッジング

  - セカンダリ VLAN からプライマリ VLAN へのアップストリーム トラフィックの場合、セカンダリ VLAN の MAP は入力側に適用され、プライマリ VLAN の MAP は出力側に適用されます。
  - プライマリ VLAN からセカンダリ VLAN へのダウンストリーム トラフィックの場合は、プライマリ VLAN の MAP は入力方向で適用され、セカンダリ VLAN のMAP は出力方向で適用されます。

  Routing

プライベート VLAN ドメインが 2 つ（PV1（sec1、prim1）および PV2（sec2、prim2））ある場合を想定します。 PV1 から PV2 にルーティングされるフレームについては次のようになります。

- sec1 の MAP および prim1 の L3 ACL は入力ポートに適用されます。
- sec1 の MAP および prim2 の L3 ACL は出力ポートに適用されます。
- 分離されたホスト ポートから無差別ポートへのアップストリームまたはダウンストリームに従うパケットの場合、分離された VLAN の VACL は入力方向に適用され、プライマリ VLAN の VACL は出力方向に適用されます。 これにより、ユーザは同じプライマリ VLAN ドメインの別のセカンダリ VLAN に異なる VACL を設定することができます。

プライベート VLAN の特定 IP トラフィックをフィルタリングするには、プライマリ VLAN およびセカンダリ VLAN の両方に VLAN マップを適用する必要があります。

- プライマリ VLAN SVI にだけルータ ACL を適用できます。 ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。
- プライベート VLAN がレイヤ 2 でホストを分離していても、ホストはレイヤ 3 で互いに通信できます。
- プライベート VLAN では、次のスイッチド ポート アナライザ（SPAN）機能がサポートされます。
  - プライベート VLAN を SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN ベースの SPAN（VSPAN）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別に監視することができます。

プライベート VLAN ポートの設定

プライベート VLAN ポートの設定時は、次の注意事項に従ってください。

- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てるには、プライベート VLAN コンフィギュレーション コマンドだけを使用します。 プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定する VLAN に割り当てられているレイヤ 2 アクセス ポートは、この VLAN がプライベート VLAN の設定に含まれている場合、非アクティブです。 レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。
- PAgP または LACP EtherChannel に属するポートを、プライベート VLAN ポートとして設定しないでください。 ポートがプライベート VLAN の設定に含まれている間は、そのポートの EtherChannel 設定はいずれも非アクティブです。
- 設定ミスによる STP ループの発生を防ぎ、STP コンバージェンスを高速化するには、独立ホスト ポートおよびコミュニティ ホスト ポート上で PortFast および BPDU ガードをイネーブルにします イネーブルの場合、STP はすべての PortFast が設定されたレイヤ 2 LAN ポートに

BPDU ガード機能を適用します。 PortFast および BPDU ガードを無差別ポートでイネーブルにしないでください。

- プライベート VLAN の設定で使用される VLAN を削除すると、この VLAN に関連付けられたプライベート VLAN ポートが非アクティブになります。
- ネットワーク デバイスをトランク接続し、プライマリ VLAN およびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートはさまざまなネットワーク デバイス上で使用できます。

プライベート VLAN の設定タスク

プライベート VLAN を設定するには、次の手順を実行します。

1. VTP モードをトランスペアレントに設定します。
2. プライマリおよびセカンダリ VLAN を作成してこれらを対応付けします。

（注） VLANがまだ作成されていない場合、プライベートVLAN設定プロセスでこれを作成します。

3. インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバーシップを割り当てます。
4. インターフェイスを無差別ポートとして設定し、無差別ポートをプライマリおよびセカンダリ VLAN のペアにマッピングします。
5. VLAN 間ルーティングを使用する場合は、プライマリ SVI を設定し、セカンダリ VLAN をプライマリにマッピングします。
6. プライベート VLAN の設定を確認します。

プライベート VLAN の設定方法

プライベート VLAN 内の VLAN の設定および対応付け

private-vlan コマンドは VLAN コンフィギュレーション モードを終了するまで機能しません。

プライベート VLAN 内で VLAN を設定し、関連付けるには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vtp mode transparent**
4. **vlan***vlan-id*
5. **private-vlan primary**
6. **exit**
7. **vlan***vlan-id*
8. **private-vlan isolated**
9. **exit**
10. **vlan***vlan-id*
11. **private-vlan community**
12. **exit**
13. **vlan***vlan-id*
14. **private-vlan community**
15. **exit**
16. **vlan***vlan-id*
17. **private-vlan association** [**add** | **remove**] *secondary_vlan_list*
18. **end**
19. **show vlan private-vlan** [**type**] または **show interfaces status**
20. **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp mode transparent** 例： `Switch(config)# vtp mode transport`	VTP モードをトランスペアレントに設定します（VTP をディセーブルにします）。 （注） VTP3 の場合、サーバまたはトランスペアレントモードのいずれにもモードを設定できます。

	コマンドまたはアクション	目的
ステップ 4	**vlan***vlan-id* 例： `Switch(config)# vlan 20`	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定または作成します。 VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 5	**private-vlan primary** 例： `Switch(config-vlan)# private-vlan primary`	VLAN をプライマリ VLAN として指定します。
ステップ 6	**exit** 例： `Switch(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**vlan***vlan-id* 例： `Switch(config)# vlan 501`	（任意）VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定または作成します。 VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 8	**private-vlan isolated** 例： `Switch(config-vlan)# private-vlan isolated`	VLAN を独立 VLAN として指定します。
ステップ 9	**exit** 例： `Switch(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**vlan***vlan-id* 例： `Switch(config)# vlan 502`	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。 VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。

	コマンドまたはアクション	目的
ステップ 11	**private-vlan community** 例： `Switch(config-vlan)# private-vlan community`	VLAN をコミュニティ VLAN として指定します。
ステップ 12	**exit** 例： `Switch(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**vlan***vlan-id* 例： `Switch(config)# vlan 503`	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 14	**private-vlan community** 例： `Switch(config-vlan)# private-vlan community`	VLAN をコミュニティ VLAN として指定します。
ステップ 15	**exit** 例： `Switch(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**vlan***vlan-id* 例： `Switch(config)# vlan 20`	ステップ 4 で指定したプライマリ VLAN に関して VLAN コンフィギュレーション モードを開始します。
ステップ 17	**private-vlan association** [**add** | **remove**] *secondary_vlan_list* 例： `Switch(config-vlan)# private-vlan association 501-503`	セカンダリ VLAN をプライマリ VLAN に関連付けます。 単一のプライベート VLAN ID でも、またはハイフンで連結したプライベート VLAN ID でもかまいません。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。 カンマで区切った複数の項目を含めることができます。 各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。

	コマンドまたはアクション	目的
		• *secondary_vlan_list* パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。 • *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN を関連付けます。 • セカンダリ VLAN とプライマリ VLAN 間の関連付けをクリアするには、*secondary_vlan_list* に **remove** キーワードを使用します。 • このコマンドは、VLAN コンフィギュレーション モードを終了するまで機能しません。
ステップ 18	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 19	**show vlan private-vlan** [**type**] または **show interfaces status** 例： `Switch# show vlan private-vlan`	設定を確認します。
ステップ 20	**copy running-config startup config** 例： `Switch# copy running-config startup-config`	スイッチ スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN ホスト ポートとして設定し、これをプライマリおよびセカンダリ VLAN に関連付けるには、次の手順を実行します。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode private-vlan host**
5. **switchport private-vlan host-association***primary_vlan_id secondary_vlan_id*
6. **end**
7. **show interfaces** [*interface-id*] **switchport**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/22`	設定するレイヤ 2 インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode private-vlan host** 例： `Switch(config-if)# switchport mode private-vlan host`	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 5	**switchport private-vlan host-association***primary_vlan_id secondary_vlan_id* 例： `Switch(config-if)# switchport private-vlan`	レイヤ 2 ポートをプライベート VLAN と関連付けます。 （注） これは、レイヤ 2 インターフェイスに PVLAN を関連付けるために必要な手順です。

	コマンドまたはアクション	目的
	`host-association 20 501`	
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `Switch# show interfaces gigabitethernet1/0/22 switchport`	設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

プライベート VLAN ポート，（2052 ページ）
例：ホスト ポートとしてのインターフェイスの設定，（2071 ページ）
例：インターフェイスをプライベート VLAN 無差別ポートとして設定する，（2072 ページ）

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN 無差別ポートとして設定し、これをプライマリおよびセカンダリ VLAN にマッピングするには、次の手順を実行します。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-id*
4. **switchport mode private-vlan promiscuous**
5. **switchport private-vlan mapping***primary_vlan_id* {**add** | **remove**} *secondary_vlan_list*
6. **end**
7. **show interfaces** [*interface-id*] **switchport**
8. **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	設定するレイヤ2インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode private-vlan promiscuous** 例： `Switch(config-if)# switchport mode private-vlan promiscuous`	レイヤ 2 ポートをプライベート VLAN 無差別ポートとして設定します。
ステップ 5	**switchport private-vlan mapping***primary_vlan_id* {**add** | **remove**} *secondary_vlan_list* 例： `Switch(config-if)# switchport`	プライベート VLAN 無差別ポートをプライマリ VLAN、および選択したセカンダリ VLAN にマッピングします。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。 カンマで区切った複数の項目を含めることができます。 各項目として入力できるのは、単一

	コマンドまたはアクション	目的
	`private-vlan mapping 20 add 501-503`	のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。 • セカンダリ VLAN とプライマリ VLAN をプライベート VLAN 無差別ポートにマッピングするには、*secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用します。 • セカンダリ VLAN とプライベート VLAN 無差別ポートのマッピングを解除するには、**remove** キーワードを指定した *secondary_vlan_list* を使用します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `Switch# show interfaces gigabitethernet1/0/2 switchport`	設定を確認します。
ステップ 8	**copy running-config startup config** 例： `Switch# copy running-config startup-config`	スイッチ スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

関連トピック

プライベート VLAN ポート，（2052 ページ）
例：ホスト ポートとしてのインターフェイスの設定，（2071 ページ）
例：インターフェイスをプライベート VLAN 無差別ポートとして設定する，（2072 ページ）

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング

プライベート VLAN が VLAN 間ルーティングに使用される場合、SVI をプライマリ VLAN に設定してセカンダリ VLAN を SVI にマッピングできます。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

セカンダリ VLAN をプライマリ VLAN の SVI にマッピングしてプライベート VLAN トラフィックのレイヤ 3 スイッチングを可能にするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface vlan***primary_vlan_id*
4. **private-vlan mapping** [**add** | **remove**] *secondary_vlan_list*
5. **end**
6. **show interface private-vlan mapping**
7. **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface vlan***primary_vlan_id* 例： `Switch(config)# interface vlan 20`	プライマリ VLAN でインターフェイス コンフィギュレーション モードを開始して、VLAN を SVI として設定します。 VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 4	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list* 例： `Switch(config-if)# private-vlan`	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。 （注） **private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされているプライベート VLAN トラフィックにだけ影響を与えます。

	コマンドまたはアクション	目的
	`mapping 501-503`	• *secondary_vlan_list* パラメータには、スペースを含めないでください。 カンマで区切った複数の項目を含めることができます。 各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。 • *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN をプライマリ VLAN にマッピングします。 • **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN のマッピングを解除します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interface private-vlan mapping** 例： `Switch# show interfaces private-vlan mapping`	設定を確認します。
ステップ 7	**copy running-config startup config** 例： `Switch# copy running-config startup-config`	スイッチ スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

関連トピック

VTP ドメイン，（1949 ページ）

セカンダリ VLAN，（2052 ページ）

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする，（2072 ページ）

プライベート VLAN のモニタ

次の表に、プライベート VLAN をモニタするために使用するコマンドを記載します。

表 *184*：プライベート *VLAN* モニタリング コマンド

コマンド	目的
show interfaces status	所属する VLAN を含む、インターフェイスのステータスを表示します。
show vlan private-vlan [**type**]	Switchのプライベート VLAN 情報を表示します。
show interface switchport	インターフェイス上のプライベート VLAN 設定を表示します。
show interface private-vlan mapping	VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。
show platform vlan pvlan	FED 側の PVLAN 情報を表示します。
show platform vlan pvlan hardware	FED 側の PVLAN で保持されているすべてのハードウェア リソースを表示します。

プライベート VLAN の設定例

例：ホスト ポートとしてのインターフェイスの設定

次に、インターフェイスをプライベート VLAN ホスト ポートとして設定し、それをプライベート VLAN ペアに関連付けて、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/22
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
Switch# show interfaces gigabitethernet1/0/22 switchport
Name: Gi1/0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 501
```

```
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 501

<output truncated>
```

関連トピック

プライベート VLAN ポート，（2052 ページ）

プライベート VLAN ホストポートとしてのレイヤ 2 インターフェイスの設定，（2064 ページ）

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定，（2066 ページ）

例：インターフェイスをプライベート VLAN 無差別ポートとして設定する

次の例では、インターフェイスをプライベート VLAN 無差別ポートとして設定し、それをプライベート VLAN にマッピングする方法を示します。 インターフェイスは、プライマリ VLAN 20 のメンバで、セカンダリ VLAN 501 ～ 503 がマッピングされます。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport mode private-vlan promiscous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

show vlan private-vlan または **show interface status** 特権 EXEC コマンドを使用してプライマリおよびセカンダリ VLAN とSwitch上のプライベート VLAN ポートを表示します。

関連トピック

プライベート VLAN ポート，（2052 ページ）

プライベート VLAN ホストポートとしてのレイヤ 2 インターフェイスの設定，（2064 ページ）

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定，（2066 ページ）

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする

次に、VLAN 501 および 502 のインターフェイスをプライマリ VLAN 10 にマッピングする例を示します。これにより、プライベート VLAN 501 および 502 からのセカンダリ VLAN 入力トラフィックのルーティングが可能になります。

```
Switch# configure terminal
Switch(config)# interface vlan 20
Switch(config-if)# private-vlan mapping 501-503
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan20    501            isolated
vlan20    502            community
```

```
vlan20    503            community
```

関連トピック

VTP ドメイン, （1949 ページ）

セカンダリ VLAN, （2052 ページ）

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング, （2068 ページ）

例：プライベート VLAN のモニタリング

次に、**show vlan private-vlan** コマンドの出力例を示します。

```
Switch# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated          Gi1/0/22, Gi1/0/2
20      502       community         Gi1/0/2
20      503       community         Gi1/0/2
```

次の作業

次の設定を行えます。

- VTP
- VLANs
- VLAN トランキング
- VLAN メンバーシップ ポリシー サーバ（VMPS）
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CLI コマンド	LAN Switching Command Reference, Cisco IOS Release

標準および RFC

標準/RFC	Title
RFC 1573	
RFC 1757	
RFC 2021	

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB • BRIDGE-MIB（RFC1493） • CISCO-BRIDGE-EXT-MIB • CISCO-CDP-MIB • CISCO-PAGP-MIB • CISCO-PRIVATE-VLAN-MIB • CISCO-LAG-MIB • CISCO-L2L3-INTERFACE-CONFIG-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • IEEE8023-LAG-MIB • IF-MIB（RFC 1573） • RMON-MIB（RFC 1757） • RMON2-MIB（RFC 2021）	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

付 録 A

重要な通知

- 免責事項，2077 ページ
- ステートメント 361：電源障害が発生した場合に VoIP および緊急コール サービスは機能しない，2078 ページ
- ステートメント 1071：警告の定義，2078 ページ

免責事項

Cisco EnergyWise の利用により、使用していないデバイスの電源を切ることでネットワーク内のエネルギー消費を減らすことができます。 IP Phone がネットワークの一部であれば、EnergyWise を介して IP Phone の電源を切り、コールの発信や受信をできないようにすることもできます。電話機の電源投入は、ネットワーク管理者が行うか、ネットワーク管理者が EnergyWise で設定したルールに従って行う必要があります。 ネットワークの場所における法律によって、緊急用に使用できる電話機の確保が義務付けられている場合があります。 ユーザは、適用される法律を特定し、その法律を遵守する責任があります。 法律で定められていない場合でも、一部の電話機を常時使用可能にして、緊急コールの発信や受信ができるようにしておくことを強く推奨します。 これらの電話機を明確に識別し、すべての従業員や、コールを発信または受信するための緊急アクセスを必要とするユーザにこれらの電話機が使用可能であることを通知してください。

ステートメント 361：電源障害が発生した場合に VoIP および緊急コール サービスは機能しない

Warning	**Voice over IP（VoIP）サービスおよび緊急コールサービスは、電源障害や停電が発生している場合は機能しません。電源が復旧した後、VoIP および緊急コールサービスへ再びアクセスできるように機器のリセットまたは再設定をする必要がある場合があります。米国では、この緊急番号は 911 です。国内の緊急番号を確認しておく必要があります。**

ステートメント 1071：警告の定義

Warning	**IMPORTANT SAFETY INSTRUCTIONS** **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071** **SAVE THESE INSTRUCTIONS**

索 引

数字

128 ビット **118**
802.1x **1535**

A

AAA サーバ グループの定義 **1386**
AAA でのローカル モード **1413**
ABR **910**
ACE **1442**
　IP **1442**
　イーサネット **1442**
ACL **732, 741, 778, 779, 781, 784, 1442, 1443, 1447, 1448, 1449, 1451, 1452, 1453, 1454, 1455, 1456, 1458, 1465, 1467, 1469, 1474, 1479, 1482, 1493, 1494, 1495**
　ACL **778**
　　IPv4 **778**
　interface **1455**
　IP **732, 1447, 1449, 1455, 1465**
　　undefined **1455**
　　フラグメントと QoS のガイドライン **732**
　　マッチング基準 **1447**
　　暗黙のマスク **1449**
　　暗黙的な拒否 **1465**
　IP 拡張 **779**
　IP 標準 **778**
　IPv4 **779, 1447, 1448, 1455, 1467, 1469**
　　インターフェイス **1455**
　　インターフェイスへの適用 **1469**
　　サポートされていない機能 **1448**
　　マッチング基準 **1447**
　　作成 **1447**
　　数値 **1448**
　　端末回線、設定する **1467**
　IPv6 **781**
　port **1442**
　QoS **741, 778**
ACL *(続き)*
　QoS クラス マップごとの数 **732**
　QoS のトラフィックの分類 **778**
　VLAN マップ **1452, 1474**
　　設定 **1474**
　　設定時の注意事項 **1452**
　VLAN マップを ACL ルータと共に使用 **1453**
　ガイドライン **732**
　コンパイル **1482**
　サポートされていない機能 **1448**
　　IPv4 **1448**
　サポートされるタイプ **1442**
　の例 **778, 1482**
　ハードウェアでのサポート **1451**
　へのコメント **1482**
　マッチング **1455**
　モニタリング **1479**
　ルータ **1442**
　ルータ ACL と VLAN マップの設定時の注意事項 **1453**
　レイヤ 2 MAC **784**
　レイヤ 4 情報 **1453**
　ロギング メッセージ **1451**
　拡張 IPv4 **1447, 1458**
　　マッチング基準 **1447**
　　作成 **1458**
　時間範囲 **1454**
　定義 **1447**
　適用 **741, 1465, 1469, 1493, 1494, 1495**
　　ルーテッド パケットの **1494**
　　QoS に適応 **741**
　　インターフェイスへの **1469**
　　スイッチド パケットの **1493**
　　ブリッジド パケット上の **1493**
　　マルチキャスト パケット上の **1495**
　　時間範囲 **1465**
　標準 IPv4 **1447, 1456**
　　マッチング基準 **1447**

ACL *(続き)*
標準 IPv4 *(続き)*
作成 **1456**
優先順位 **1443**
alternate **254**
port **254**
ARP **881, 883, 1787, 1914**
table **1787**
アドレス解決 **1787**
カプセル化 **883**
スタティック キャッシュの設定 **881**
定義 **1787**
AS パス フィルタ、BGP **956**
auto モード **80**
Auto-MDIX **49**
設定 **49**
説明 **49**
Auto-MDIX コマンドの設定例 **50**
Auto-MDIX、設定する **49**
Auto-QoS **847, 855, 861, 862**
enhanced **847**
VoIP デバイス用に生成される設定 **861**
グローバル設定 **855**
拡張されたビデオ、信頼、および分類デバイス用に生成される設定 **862**
設定の移行 **847**
Auto-RP **1130**
automatic **1534**

B

BackboneFast **332, 345**
イネーブル化 **345**
説明 **332**
Berkeley r-tool の置換 **1420**
BGP **941, 945, 946, 949, 951, 952, 955, 959, 962, 967, 969, 970**
マルチパス サポート **952**
CIDR **967**
イネーブル化 **946**
コミュニティ フィルタリング **962**
デフォルト設定 **941**
ネイバー、タイプ **945**
バージョン 4 **941**
パスの選択 **951**
プレフィックス フィルタリング **959**
リセット セッション **949**
ルーティング ドメイン コンフェデレーション **969**
ルート マップ **955**
BGP *(続き)*
ルート リフレクタ **970**
集約アドレス **967**
説明 **941**
bindings **1513, 1534**
IP ソース ガード **1534**
アドレス、Cisco IOS DHCP サーバ **1513**
BIP マルチキャスト ルーティング **1186**
Bootstrap Router：ブートストラップ ルータ **1117**
BPDU **255, 300, 329**
RSTP 形式 **300**
フィルタリング **329**
内容 **255**
BSR **1148**
候補 **1148**

C

CA トラストポイント **1428, 1430**
設定 **1430**
定義 **1428**
CDP **51, 78, 771, 1914**
LLDP での定義 **51**
および信頼境界 **771**
電力ネゴシエーションの拡張機能 **78**
CDP に対する電力ネゴシエーションの拡張機能 **78**
CEF **143, 1020**
distributed **1020**
IPv6 **143**
CEFv6 **143**
CGMP **1100**
サーバ サポートのイネーブル化 **1100**
サーバ サポートのみ **1100**
CipherSuite **1429**
Cisco 7960 IP フォン **2038**
Cisco Discovery Protocol（CDP） **575**
Cisco Express Forwarding; シスコ エクスプレス フォワーディング **1019**
「CEF」を参照 **1019**
Cisco IOS DHCP サーバ **1513**
DHCP、Cisco IOS DHCP サーバを参照 **1513**
Cisco IOS IP SLA **502**
Cisco IP Phone のデータ トラフィック **2039**
Cisco IP Phone の音声トラフィック **2038**
Cisco Networking Service **554**
Cisco インテリジェント電力管理 **78**
CIST リージョナル ルート **289, 290**
「MSTP」を参照 **289, 290**

CIST ルート 290
「MSTP」を参照 290
CLNS 976
ISO CLNS を参照 976
clock 1779
システム クロックを参照 1779
CNS 554
CoA 要求コマンド 1374
collect パラメータ 691
CoS 735, 2044
プライオリティのオーバーライド 2044
レイヤ 2 フレーム 735
CoS 出力キューしきい値マップ、QoS の 754
CoS/DSCP マップ、QoS での 762, 799

D

debug コマンドを使用 1917
debugging 1917, 1933, 1944
エラー メッセージ出力のリダイレクト 1933
コマンドを使用 1917
すべてのシステム診断のイネーブル 1944
DHCP 121, 1507, 1516
DHCP for IPv6 121
「DHCPv6」を参照 121
イネーブル化 1507, 1516
サーバ 1507
リレー エージェント 1516
DHCP for IPv6 121
「DHCPv6」を参照 121
DHCP Option 82 1510, 1518
ヘルパー アドレス 1518
概要 1510
転送アドレス、指定 1518
DHCP オプション 82 1525
表示 1525
DHCP サーバ ポート ベースのアドレス割り当て 1527, 1530
イネーブル化 1530
デフォルト設定 1527
DHCP スヌーピング 1508, 1509, 1510, 1534
Option 82 データ挿入 1510
信頼できないメッセージ 1508
信頼できるインターフェイス 1508
非信頼パケット形式エッジ スイッチの受信 1509
DHCP スヌーピング バインディング データベース 1513, 1514, 1521, 1527
イネーブル化 1527
DHCP スヌーピング バインディング データベース *(続き)*
バインディング ファイル 1514
形式 1514
場所 1514
バインディングの追加 1527
設定 1527
設定時の注意事項 1521
説明 1513
DHCPv6 121, 171, 174
クライアント機能のイネーブル化 174
設定時の注意事項 171
DHCPv6 サーバ機能のイネーブル化 171
デフォルト設定 171
説明 121
DHCPv6 クライアント機能のイネーブル化：コマンド例 177
DHCPv6 サーバ機能のイネーブル化 171
DHCPv6 サーバ機能のイネーブル化：コマンド例 177
Differentiated Services（Diff-Serv）アーキテクチャ 734
DiffServ コード ポイント 736
disabled 260
state 260
distribute-list コマンド 1040
DNS 119, 1784, 1785, 1795
IPv6 119
セットアップ 1795
デフォルト設定 1785
概要 1784
Domain Name System; ドメイン ネーム システム 1784
DNS を参照 1784
DRP 120, 140
IPv6 120
説明 120
設定 140
DSCP 736
DSCP マップ 762
DSCP/CoS マップ、QoS での 763
DSCP/DSCP 変換マップ、QoS での 805
DUAL 有限状態マシン、EIGRP 929
DVMRP（ディスタンス ベクター マルチキャスト ルーティング プロトコル） 1068
IP マルチキャスト ルーティング、DVMRP を参照 1068

E

EIGRP 927, 928, 934, 936, 938, 939
インターフェイス パラメータ、設定 934
コンポーネント 928
スタブ ルーティング 938

EIGRP *(続き)*
モニタリング 939
定義 927
認証 936
EIGRP IPv6 123
EIGRP IPv6 コマンド 122
ELIN ロケーション 54
enable secret 1334
Enhanced Interior Gateway Routing Protocol（EIGRP）
IPv6 122, 123
EIGRP IPv6 コマンド 122
ルータ ID 123
EtherChannel 386, 389, 391, 393, 394, 395, 396, 397, 399, 401, 404, 407, 408, 409, 410, 411, 872, 1535
IEEE:802.3ad、説明 395
LACP 395, 396, 409, 410, 411
システム プライオリティ 410
ポート プライオリティ 411
ホット スタンバイ ポート 409
モード 395
他の機能との相互作用 396
PAgP 391, 393, 394, 395, 408
デュアル アクション検出を使用 394
モード 391
仮想スイッチとの相互作用 394
学習方式およびプライオリティについて 393
学習方式とプライオリティの設定 408
集約ポート ラーナー 408
集約ポート ラーナーについて 393
説明 391
他の機能との相互作用 395
チャネル グループ 389
番号 389
物理および論理インターフェイスのバインド 389
デフォルト設定 399
ポートチャネル インターフェイス 389
番号 389
レイヤ 3 インターフェイス 872
ロード バランシング 397, 407
自動作成の 391, 395
設定 404
レイヤ 2 インターフェイス 404
設定時の注意事項 401
相互作用 401
STP を使用 401
転送方式 397, 407
論理インターフェイス、説明 389
EtherChannel | 相互作用 401
VLAN を使用 401
EtherChannel ガード 335, 346
イネーブル化 346
説明 335
EtherChannel コマンドの設定例 414
EtherChannel フェールオーバー 389
EUI 119
Extended Universal Identifier 119
「EUI」を参照 119

F

Flex Link 444, 446, 450, 451, 452, 454, 458, 459, 460
VLAN ロード バランシングの設定 454
VLAN ロード バランシングの例 460
スイッチポート バックアップの例 459
強制プリエンプション モードの例 459
デフォルト設定 450
プリエンプション方式 452
モニタリング 458
リンクのロード バランシング 446
設定 451, 452
説明 444
優先 VLAN の例 460
Flex Link の VLAN ロード バランシング 446, 450
設定時の注意事項 450
説明 446
Flex Link フェールオーバー 446
flow record 697

G

GLOP アドレス 1071

H

hello タイム 277, 315
MSTP 315
STP 277
HSRP for IPv6 153, 154
設定 154
ガイドライン 153
HTTP over SSL 1427
「HTTPS」を参照 1427
HTTP セキュア サーバ 1427

HTTPS 1427, 1428, 1433
自己署名証明書 1428
設定 1433
説明 1427

I

IBPG 940
ICMP 119, 1440, 1451, 1915
IPv6 119
traceroute 1915
時間超過メッセージ 1915
到達不能および ACL 1451
到達不能メッセージ 1440
ICMP PING 1913, 1931
概要 1913
実行 1931
ICMP Router Discovery Protocol 887
「IRDP」を参照 887
ICMP Router Discovery Protocol（IRDP） 887
設定 887
定義 887
ICMP エコー動作 519
IP SLAs 519
設定 519
ICMPv6 119
IEEE 395
802.3ad、説明 395
IEEE 802.1Q 224
protocol 224
IEEE 802.1Q タギング 2009
IEEE 802.1Q トンネリング 225, 230
デフォルト 230
IEEE 802.1s 285
「MSTP」を参照 285
IEEE 802.3ad 395
「EtherChannel」を参照 395
IEEE 電力分類レベル 78
IGMP 109, 112, 113, 1076, 1077, 1078, 1079, 1081, 1082, 1083, 1089, 1091, 1093, 1094, 1231, 1232, 1234, 1235, 1236, 1251, 1253, 1254, 1255, 1260
マルチキャスト アドレス 1077
設定可能 Leave タイマー 1235
説明 1235
join メッセージ 1232
role 1076
Version 1 1078
Version 2 1078
クエリー 1232

IGMP *(続き)*
クエリー タイムアウト 1091
クエリー タイムアウト 1091
サポートされているバージョン 1077, 1231
スイッチの設定 1083, 1094
グループのメンバとして 1083
静的に接続されたメンバ 1094
スヌーピング 113
デフォルト設定 1083
バージョン 3 1078
バージョンの違い 1079
フラッディングされたマルチキャスト トラフィック 1253, 1254, 1255
インターフェイスにおけるディセーブル化 1255
グローバルな脱退 1254
フラッディング モードからの回復 1254
時間の長さの制御 1253
プルーニング グループ 1093
ホストクエリー インターバル、変更 1089
マルチキャスト グループからの脱退 1234
マルチキャストの到達可能性 1083
レポート抑制 112, 1235, 1260
ディセーブル化 112, 1260
説明 1235
加入処理 1081
最大クエリー応答時間値 1093
設定可能な脱退タイマー 1251
イネーブル化 1251
脱退処理 1082
脱退処理、イネーブル化 109
IGMP グループ 1271, 1272
フィルタリングの設定 1272
最大数の設定 1271
IGMP スヌーピング 104, 105, 113, 1077, 1227, 1230, 1231, 1234, 1235, 1241, 1243, 1257
querier 1227, 1257
設定 1257
設定時の注意事項 1227
VLAN コンフィギュレーション 1243
イネーブル化またはディセーブル化 105, 1241
およびアドレスのエイリアス 1231
グローバル コンフィギュレーション 1241
サポートされているバージョン 1077, 1231
デフォルト設定 104, 105, 1235
モニタリング 113
即時脱退 1234
定義 1230

IGMP スロットリング 1240, 1241, 1272, 1277
アクションの表示 1277
デフォルト設定 1241
設定 1272
説明 1240
IGMP スロットリング アクション 1229
設定時の注意事項 1229
IGMP のバージョン 1088
IGMP フィルタリング 1240, 1241
デフォルト設定 1241
説明 1240
IGMP プロファイル 1267, 1269
コンフィギュレーション モード 1267
適用 1269
IGMP ヘルパー 1114
IGMP レポートの生成 447
IGMP レポート抑制 1229
IGMP 即時脱退 1229, 1249
イネーブル化 1249
IGMPv3 1078
Inter-Switch Link; スイッチ間リンク 620
「ISL」を参照 620
interface 91
Interior Gateway Protocol 910
「IGP」を参照 910
IP 1068
PIM 1068
IP マルチキャスト ルーティング、PIM を参照 1068
IP ACL 741, 1450
QoS 分類 741
ネームド 1450
IP precedence 736
IP precedence/DSCP マップ、QoS での 763, 801
IP SLA 504, 506, 508, 509, 522
しきい値監視 506
モニタリング 522
レスポンダ 504, 509
イネーブル化 509
説明 504
設定時の注意事項 508
IP SLAs 502, 503, 505, 506, 507, 508, 515, 519
ICMP エコー動作 519
SNMP のサポート 503
UDP ジッター動作 507, 515
サポートされるメトリック 502
ネットワーク パフォーマンスの測定 503
応答時間 505
設定 508
IP SLAs *(続き)*
複数動作のスケジューリング 506
利点 503
IP traceroute 1915, 1933
概要 1915
実行 1933
IP アドレス 118, 872, 874, 898, 1787
128 ビット 118
IP ルーティング 872
IPv6 118
クラス 874
モニタリング 898
検出する 1787
IP アドレスおよびサブネット 1914
IP ソース ガード 1534, 1535, 1537, 1538
802.1x 1535
DHCP スヌーピング 1534
EtherChannel 1535
TCAM エントリ 1535
VRF 1535
イネーブル化 1537, 1538
スタティック バインディング 1537, 1538
追加 1537, 1538
スタティック ホスト 1538
トランク インターフェイス 1535
バインディング コンフィギュレーション 1534
automatic 1534
manual 1534
バインディング テーブル 1534
ポート セキュリティ 1535
ルーテッド ポート 1535
設定時の注意事項 1535
説明 1534
IP ダイレクト ブロードキャスト 890
IP ブロードキャスト アドレス 894
IP ホスト ping コマンド例 1942
IP ホストに対する traceroute 実行コマンド例 1943
IP マルチキャスト 1067, 1071, 1074
グループ アドレッシング 1071
情報配信における役割 1067
配信 modesany 送信元マルチキャスト 1074
IP マルチキャスト ルーティング 1068, 1106, 1144, 1165, 1187, 1188, 1189, 1197
DVMRP 1068
定義 1068
IGMP 1068
目的 1068

IP マルチキャスト ルーティング *(続き)*
MBONE 1068, 1187, 1188
会議セッション アナウンスの SAP パケット 1188
説明 1187
PIMv1 および PIMv2 の相互運用性 1106
RP 1144, 1165
PIMv2 BSR の設定 1144
マッピング情報のモニタリング 1165
イネーブル化 1189
PIM モード 1189
統計情報、システムおよびネットワークの表示 1197
IP マルチキャスト境界 1146, 1190
IP ユニキャスト ルーティング 118, 870, 871, 872, 874, 876, 877, 880, 886, 887, 890, 894, 895, 899, 1018, 1023, 1026, 1027, 1039, 1042, 1043
unicast Reverse Path Forwarding 1018
broadcast 890, 894, 895
address 894
ストーム 890
パケット 890
フラッディング 895
directed ブロードキャスト 890
EtherChannel レイヤ 3 インターフェイス 872
ICMP Router Discovery Protocol（IRDP） 887
IP アドレッシング 872, 874
classes 874
設定 872
IPv6 118
MAC アドレスと IP アドレス 880
SVI を使用 872
VLAN 間 870
アドミニストレーティブ ディスタンス 1042
イネーブル化 899
クラスレス ルーティング 877
サブネット ゼロ 876
サブネット マスク 874
スタティック ルートの設定 1023
デフォルト 886, 1026
ゲートウェイ 886
ネットワーク 1026
ルート 1026
プロキシ ARP 880
ルーテッド ポート 871
レイヤ 3 インターフェイス 871
再配布 1027
受動インターフェイス 1039
設定手順 872
認証キー 1043
IP ルーティング 899
イネーブル化 899
IP 電話 770
信頼される境界、QoS の 770
IPv4 ACL 1455, 1456, 1458, 1462, 1469
インターフェイス 1455
インターフェイスへの適用 1469
ネームド 1462
拡張、作成 1458
標準、作成 1456
IPv6 99, 117, 118, 119, 120, 121, 122, 123, 124, 125, 143, 170
CEFv6 143
Enhanced Interior Gateway Routing Protocol（EIGRP） IPv6 122, 123
EIGRP IPv6 コマンド 122
ルータ ID 123
ICMP 119
OSPF 121
SDM テンプレート 99
アドレス 118
アドレスの割り当て 125
アドレス形式 118
アプリケーション 120
サポートされない機能 124
サポートされる機能 118
スイッチの制限 125
スタティック ルートの概要 121
ステートレス自動設定 120
デフォルト ルータ プリファレンス（DRP） 120
デフォルト設定 125
ネイバー探索 120
パス MTU 検出 119
フォワーディング 125
モニタリング 170
機能の制限 125
自動設定 120
定義 117
IPv6 ICMP レート制限の設定：コマンド例 178
IPv6 アドレスの割り当て 125
IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化：コマンド例 175
IPv6 による HTTP（S） 124
IPv6 の HSRP グループのイネーブル化：コマンド例 176
IPv6 の RIP の設定：コマンド例 178
IPv6 のスタティック ルーティングの設定：コマンド例 178
IPv6 の場合 121
IPv6 の表示：コマンド例 178

IS-IS 976
エリア ルーティング 976
システム ルーティング 976
ISL 118
および IPv6 118
ISO CLNS 976
OSI 標準 976
ダイナミック ルーティング プロトコル 976

J

join メッセージ、IGMP 1232

K

KDC 1406, 1410
「Kerberos」も参照 1406
zzz] 1406
説明 1406
Kerberos 1406, 1409, 1410, 1411
KDC 1406
TGT 1406
クレデンシャル 1406
ご利用条件 1406
サーバ 1406
チケット 1406
レルム 1406
信頼済みサード パーティとしてのスイッチ 1406
設定 1411
設定例 1406
説明 1406
動作 1409
認証 1410
KDC 1410
ネットワーク サービス 1410
境界スイッチ 1410

L

LACP 387, 395, 396, 404, 409, 410, 411
システム プライオリティ 410
ポート プライオリティ 411
ホット スタンバイ ポート 409
モード 395
他の機能との相互作用 396
LLDP 51, 55, 56, 58
送信タイマーとホールドタイム、設定 58
イネーブル化 56
スイッチ スタックの考慮事項 51
概要 51
設定 55
デフォルト設定 55
LLDP-MED 52, 60
サポートされている TLV 52
概要 52
設定 60
TLV 60
login 1358, 1383

M

MAC アドレス 880, 1786, 1787, 1800, 1809
dynamic 1786
ラーニング 1786
IP アドレス アソシエーション 880
VLAN の関連付け 1786
アドレス テーブルの構築 1786
エージング時間 1800
デフォルト設定 1786
検出する 1787
静的 1809
特性 1809
MAC アドレスおよび VLAN 1914
MAC アドレステーブル移動更新 448, 450, 451, 456, 457
デフォルト設定 451
メッセージの取得および処理 457
設定 456
設定時の注意事項 450
説明 448
MAC 拡張アクセス リスト 1440, 1472
レイヤ 2 インターフェイスに適用 1440, 1472
MAC/PHY コンフィギュレーション ステータス TLV 51
manual 1534
match パラメータ 689
maximum-paths コマンド 1022
MBONE 1187
MBONE（マルチキャスト バックボーン） 1068
MLD クエリー 101
MLD スヌーピング 100
MLD スヌーピング クエリー コマンドの設定例 114
MLD スヌーピング クエリーの設定：コマンド例 115
MLD メッセージ 101

MLD レポート 102
MLD 即時脱退のイネーブル化：コマンド例 115
MLDv1 Done メッセージ 103
mrouter ポート 447
MSDP コマンドの設定例 1318
MSDP ピアからの送信元情報の要求：コマンド例 1319, 1320
MST モード 2001
MSTP 264, 284, 286, 287, 288, 289, 290, 292, 293, 294, 296, 303, 304, 305, 307, 308, 309, 312, 313, 315, 316, 318, 319, 320, 321, 323, 324, 328, 329, 335, 336, 337, 338, 340, 346, 347, 349
設定 304, 307, 308, 309, 312, 313, 315, 316, 318, 319, 320, 321
ネイバー タイプ 321
BPDU ガード 328, 338
イネーブル化 338
説明 328
BPDU フィルタリング 329, 340
イネーブル化 340
説明 329
CIST リージョナル ルート 289, 290
CIST ルート 290
CIST、説明 289
CST 290
領域間の動作 290
EtherChannel ガード 335, 346
イネーブル化 346
説明 335
IEEE 802.1D との相互運用性 296, 323
移行プロセスの再開 323
説明 296
IEEE 802.1s 290, 294
ポートの役割名の変更 294
実装 294
用語 290
IST 289
領域内の動作 289
MST 領域 288, 289, 292, 304
CIST 289
IST 288
サポートされるスパニングツリーインスタンス 288
ホップ カウント メカニズム 292
設定 304
説明 288
PortFast 328, 337
イネーブル化 337
説明 328
PortFast 対応ポートのシャットダウン 329
VLAN から MST インスタンスへのマッピング 305
MSTP *(続き)*
インターフェイス ステート、ブロッキングからフォワーディングへ 328
サポートされるインスタンス 264
ステータス、表示 324
ステータスの表示 324
デフォルト設定 303
モードのイネーブル化 304
モード間の相互運用性と互換性 264, 284
ルート ガード 335, 347
イネーブル化 347
説明 335
ルート スイッチ選択の防止 335
ルート デバイス 287
拡張システム ID の影響 287
設定 287
予期しない動作 287
ループ ガード 336, 349
イネーブル化 349
説明 336
拡張システム ID 287, 308
セカンダリ ルート デバイスに対する効果 308
ルート デバイスに対する効果 287
予期しない動作 287
境界ポート 284, 293
設定時の注意事項 284
説明 293
設定 304, 307, 308, 309, 312, 313, 315, 316, 318, 319, 320, 321
hello タイム 315
MST 領域 304
セカンダリ ルート デバイス 308
デバイス プライオリティ 313
パス コスト 312
ポート プライオリティ 309
ルート デバイス 307
高速コンバージェンスのリンク タイプ 320
最大エージング タイム 318
最大ホップ カウント 319
転送遅延時間 316
設定時の注意事項 286
MTU 73
system 73
MVR 1236, 1239
デフォルト設定 1239
説明 1236
MVR インターフェイス 1264
MVR パラメータ 1261

N

NSAP、ISO IGRP アドレスとして 976
NSF 認識 979
IS-IS 979
NTP 1780, 1782
time 1782
services 1782
アソシエーション 1782
定義 1782
概要 1780
NVRAM バッファ サイズ設定コマンドの例 1847

O

OBFL 1917, 1934, 1935
設定 1934
説明 1917
表示 1935
OSPF 121, 914, 918, 920, 921, 924, 925, 926
LSA グループ ペーシング 924
IPv6 の場合 121
エリア パラメータ、設定 918
デフォルト設定 921
メトリック 921
ルート 921
モニタリング 926
ルータ ID 925
ルート集約 920
仮想リンク 921
設定 914

P

PaGP 387
PAgP 391, 394, 395, 404, 408
「EtherChannel」を参照 391
デュアル アクション検出を使用 394
モード 391
仮想スイッチとの相互作用 394
学習方式とプライオリティの設定 408
集約ポート ラーナー 408
説明 391
他の機能との相互作用 395
password 1956
PBR 1034, 1038
ローカル ポリシーベース ルーティング 1038
PBR *(続き)*
高速スイッチングされたポリシーベース ルーティング 1038
定義 1034
PIM 1106, 1112, 1124, 1152, 1154, 1165, 1166, 1189
デフォルト設定 1124
バージョン 1106, 1112, 1166
v2 の改善点 1112
相互運用性 1106
相互運用性の問題のトラブルシューティング 1166
モードのイネーブル化 1189
モニタリング 1165
ルータクエリー メッセージ間隔、変更 1154
最短パスツリー、使用の延期 1152
PIM スタブ ルーティング 1107, 1113, 1125
PIM ソース ツリー 1120
PIM デンス モード 1109
PIM ドメイン境界 1117, 1144
PIM 共有ツリー 1120
PIM-SSM 1201
ping 1913, 1931, 1942
概要 1913
実行 1931
文字出力の説明 1942
ping を使用 1913
PoE 21, 77, 78, 80, 81, 89
auto モード 80
CDP に対する電力ネゴシエーションの拡張機能 78
Cisco インテリジェント電力管理 78
IEEE 電力分類レベル 78
サポートされているデバイス 21, 77
サポートされる標準 78
サポートしているポート単位のワット数 21, 77
スタティック モード 80
モニタリング 81
受電装置の検出および初期電力割り当て 78
消費電力のポリシング 81
低電力モードで動作する高電力装置 78
電力ネゴシエーションを伴う CDP、説明 78
電力のモニタ 89
電力管理モード 80
電力消費のポリシング 89
電力消費を伴う CDP、説明 78
PoE コマンドの設定例 92
PoE ポート 1912
port 255
priority 255

priority 2044
CoS の無効化 2044
Protocol Independent Multicast 1109
PVST モード 2001
PVST+ 263, 264, 265
IEEE 802.1Q トランキングの相互運用性 265
サポートされるインスタンス 264
説明 263

Q

QoS 736, 738, 739, 741, 742, 743, 744, 746, 747, 751, 754, 755, 756, 762, 763, 764, 766, 768, 773, 775, 778, 786, 789, 791, 795, 796, 799, 801, 802, 804, 805, 807, 809, 810, 812, 813, 815, 820, 822, 824, 826, 828, 837, 838, 844, 845, 848, 849, 850, 854
QoS 738, 812
入力キュー 812
SRR 共有重みの設定 812
classification 736, 738, 739, 741, 742, 773
DSCP 透過性、説明 773
IP ACL、説明 741, 742
IP トラフィックのオプション 739
MAC ACL、説明 738, 742
信頼 CoS、説明 738
転送処理 736
IP 電話 844
自動分類とキューイング 844
QoS 738, 812
classification 738
DSCP の信頼、説明 738
IP precedence の信頼、説明 738
SRR 812
設定 812
入力キューの共有重み 812
キュー 747, 755, 826
WTD、説明 747
ハイ プライオリティ（緊急） 755, 826
ロケーション 747
クラス マップ 786, 789
設定 786, 789
グローバルなイネーブル化 764
デフォルト自動設定 845
デフォルト設定 756
パケットの変更 756
ポリサー 744, 795
のタイプ 744
設定 795
ポリシング、説明 743
QoS *(続き)*
マーキング:説明 743
マークされたアクション 795
マッピング テーブル 746, 762, 763, 799, 801, 802, 804, 805
CoS/DSCP 762, 799
DSCP-CoS 804
DSCP/CoS 763
DSCP/DSCP 変換 805
IP precedence/DSCP 763, 801
policed-DSCP 802
のタイプ 746
暗黙的な拒否 742
基本モデル 736
自動 QoS 845, 849, 854
ディセーブル化 854
トラフィックの分類 845
実行コンフィギュレーションでの影響 849
出力インターフェイスで帯域幅を制限する 828
出力キュー 754, 820, 822, 824
DSCP または CoS 値のマッピング 820
SRR シェーピング重みの設定 822
SRR 共有重みの設定 824
WTD、説明 754
しきい値マップの表示 822
書き換え 756
設定 766, 768, 775, 778, 791, 796, 799, 807, 815, 837, 838, 850
DSCP マップ 799
IP 標準 ACL 778
デフォルトのポート CoS 値 768
ドメイン内のポートの信頼状態 766
自動 QoS 850
集約ポリシング機能 796, 837, 838
出力キューの特性 815
入力キューの特性 807
物理ポートのポリシー マップ 791
別のドメインとの境界での DSCP 信頼状態 775
設定時の注意事項 848
自動 QoS 848
入力キュー 751, 809, 810, 812, 813
WTD、説明 751
しきい値マップの表示 809
バッファおよび帯域幅の割り当て、説明 751
バッファの割り当て 810
プライオリティ キュー、説明 751
プライオリティ キューの設定 813
帯域幅の割り当て 812
QoS の CoS 入力キューしきい値マップ 750

QoS のクラス マップ 786, 789
設定 786, 789
QoS のポリシー マップ 791
物理ポートの非階層型 791
設定 791
QoS のマッピング テーブル 746, 762, 763, 799, 801, 802, 805
設定 762, 763, 799, 801, 802, 805
CoS/DSCP 762, 799
DSCP 799
DSCP/CoS 763
DSCP/DSCP 変換 805
IP precedence/DSCP 763, 801
policed-DSCP 802
説明 746
QoS ポリシー 777
queueing 749, 752

R

RADIUS 1369, 1370, 1377, 1380, 1383, 1386, 1389, 1391, 1393, 1394, 1396, 1403
AAA サーバ グループの定義 1386
login 1383
キー 1380
サーバの指定 1380
デフォルト設定 1377
ネットワーク環境の提案 1369
ユーザによってアクセスされるサービスのトラッキング 1391
ユーザに対するサービスの制限 1389
概要 1369
設定 1380, 1383, 1389, 1391, 1393
アカウンティング 1391
許可 1389
通信、グローバル 1380, 1393
通信、サーバ単位 1380
認証 1383
複数の UDP ポート 1380
属性 1394, 1396, 1403
ベンダー固有 1394
ベンダー独自仕様 1396, 1403
動作 1370
RADIUS サーバ ホストの識別：コマンド例 1401
RADIUS によるスイッチ アクセスの制御の例 1401
RADIUS 許可の変更 1371
references 865
自動 QoS 865
Remote SPAN 625
RFC 900, 910, 940, 1230, 1780
1058、RIP 900
1112、IP マルチキャストおよび IGMP 1230
1163、BGP 940
1267、BGP 940
1305、NTP 1780
1587、NSSAs 910
1771、BGP 940
RFC 5176 規定 1372
Right-To-Use 1849, 1850, 1851, 1852, 1854
AP-Count のアクティブ化 1854
イメージ ベースのライセンス 1851
ベース イメージのアクティブ化 1852
ライセンスの概要 1850
ライセンスの状態 1851
永久ライセンス 1850
制約事項 1849
評価ライセンス 1850
RIP 121, 900, 901, 902, 905, 906
IPv6 の場合 121
サマリー アドレス 906
スプリット ホライズン 906
ホップ カウント 901
設定 902
説明 900
認証 905
role 254
port 254
root 254, 256
port 254
switch 254
スイッチ 256
route-map コマンド 1037
RP 1127, 1134, 1150
スパース モード クラウド 1134
候補 1150
RP アナウンスメント メッセージ 1142
RPF 1122
RPF チェックの失敗（図） 1123
RPF チェックの成功（図） 1123
RSPAN 620, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 635, 645, 646, 649, 654
sessions 626, 645, 646, 649, 654
イネーブルにされた入力トラフィック 654
監視対象ポートの指定 645, 646
作成 645, 646
定義 626
特定の VLAN への送信元トラフィックの制限 649
VLAN ベース 629

RSPAN *(続き)*
セッションの制限 620
デバイス スタック内 624
デフォルト設定 635
ポートのモニタリング 630
宛先ポート 630
概要 623
監視対象ポート 629
受信トラフィック 627
設定時の注意事項 635
送信トラフィック 628
送信元ポート 629
他の機能との相互作用 632
特性 631
RSTP 296, 297, 298, 299, 300, 301, 320, 323
BPDU 300, 301
形式 300
処理 301
IEEE 802.1D との相互運用性 296, 301, 323
トポロジの変更 301
移行プロセスの再開 323
説明 296
アクティブなトポロジ 297
ポートのロール 296, 299
synchronized 299
説明 296
ルート ポート、定義済み 296
概要 296
高速コンバージェンス 297, 298, 320
エッジ ポートと PortFast 297
クロススタック高速コンバージェンス 298
ポイントツーポイント リンク 298, 320
ルート ポート 298
説明 297
指定スイッチ、定義済み 296
指定ポート、定義済み 296
RTC 1780
定義 1780
利点 1780

S

SA ステートのキャッシング：コマンド例 1319
sampler 705
SAP リスナー 1195
SCP 1420, 1421
および SSH 1420
SCP *(続き)*
設定 1421
SDM 1880
テンプレート 1880
設定 1880
SDM テンプレート 99
SDM テンプレート コマンドの設定例 1881
SDMテンプレートの設定：コマンド例 1882
sdr 1187
Secure Copy Protocol
services 554
ネットワーキング 554
SFP 1931
ステータス、表示 1931
ステータスのモニタリング 1931
セキュリティおよび識別 1931
SFP ステータス 1931
SFP セキュリティおよび識別 1931
show access-lists hw-summary コマンド 1451
show forward コマンド 1934
show interfaces switchport 462
show platform forward コマンド 1934
SNMP 503, 1801, 1804, 1807
および IP SLA 503
トラップ 1801, 1804, 1807
MAC アドレス通知のイネーブル 1801, 1804, 1807
SNMP と Syslog、IPv6 による 123
Source Specific Multicast 1074
SPAN 620, 623, 626, 627, 628, 629, 630, 632, 635, 637, 640, 642, 657
sessions 626, 635, 637, 640, 642, 657
イネーブルにされた入力トラフィック 640
宛先（モニタリング）ポートの削除 635
監視対象ポートの指定 637, 657
作成 637, 657
定義 626
特定の VLAN への送信元トラフィックの制限 642
VLAN ベース 629
セッションの制限 620
デフォルト設定 635
ポートのモニタリング 630
宛先ポート 630
概要 623
監視対象ポート 629
受信トラフィック 627
設定時の注意事項 635
送信トラフィック 628
送信元ポート 629
他の機能との相互作用 632

SPAN トラフィック 627
Spanning Tree 258
状態 258
spanning-tree 255
ポート プライオリティ 255
SRR 748, 749
シェーピング モード 748
共有モード 749
説明 748
SSH 1418, 1419
暗号化方式 1419
ユーザ認証方式、サポートされる 1419
SSH サーバ 1423
SSL 1430, 1433, 1436, 1437
セキュア HTTP クライアントの設定 1436
セキュア HTTP サーバの設定 1433
モニタリング 1437
設定時の注意事項 1430
SSM 1071, 1201, 1203, 1209
アドレス 1071
IGMPv3 ホスト シグナリング 1203
概要 1201
設定 1209
SSM マッピング 1205, 1206, 1211, 1213, 1215, 1217, 1219
DNS ベースの SSM マッピング 1206
DNS ベースの SSM マッピングの設定 1213
スタティック SSM マッピング 1206
スタティック トラフィック転送 1215
モニタリング 1219
概要 1205
設定と動作の確認 1217
SSM、ISM および IGMPv3 1203
SSM（Source Specific Multicast） 1202, 1203
ISM との違い 1202
operations 1203
STP 253, 254, 255, 256, 257, 258, 259, 260, 262, 263, 264, 265, 266, 267, 268, 269, 271, 273, 274, 276, 277, 278, 279, 280, 281, 284, 330, 332, 335, 342, 344, 345, 346
BackboneFast 332, 345
イネーブル化 345
説明 332
BPDU メッセージ交換 255
EtherChannel ガード 335, 346
イネーブル化 346
説明 335
IEEE 802.1D とブリッジ ID 256
IEEE 802.1D とマルチキャスト アドレス 262
IEEE 802.1Q トランクでの制限 265
STP *(続き)*
IEEE 802.1t と VLAN 識別子 256
root 253
switch 253
予期しない動作 253
UplinkFast 330, 342, 344
イネーブル化 342
ディセーブル化 344
説明 330
VLAN ブリッジ 265
インターフェイス ステート 258, 259, 260
disabled 260
フォワーディング 259, 260
ブロック 259
ラーニング 260
リスニング 260
キープアライブ メッセージ 255
サポートされるインスタンス 264
サポートされるプロトコル 263
サポートされるモード 263
ステータス、表示 281
ステータスの表示 281
ディセーブル化 268
デフォルト設定 266
モード間の相互運用性と互換性 264, 284
ルート 256
スイッチ 256
選定 256
ルート デバイス 256, 257, 269
拡張システム ID の影響 256, 269
設定 257
ルート ポート、定義済み 256
ルート ポート選択の高速化 330
概要 254
拡張システム ID 253, 256, 269, 271
セカンダリ ルート デバイスに対する効果 271
ルート デバイスに対する効果 269
概要 256
予期しない動作 253
間接リンク障害の検出 332
指定ポート、定義済み 256
指定定義 256
スイッチ 256
冗長接続 262
設定 267, 269, 271, 273, 274, 276, 277, 278, 279, 280
hello タイム 277
スパニングツリー モード 267
セカンダリ ルート デバイス 271

STP *(続き)*
設定 *(続き)*
デバイス プライオリティ 276
パス コスト 274
ポート プライオリティ 273
ルート デバイス 269
最大エージング タイム 279
転送遅延時間 278
転送保留カウント 280
STP パス コスト 2016
STP ポート プライオリティ 2011
STP を使用 401
SVI 872, 1445
および IP ユニキャスト ルーティング、 872
およびルータ ACL 1445
switchport backup interface 463
system 73

T

TACACS+ 1351, 1353, 1355, 1356, 1358, 1361, 1363, 1365
login 1358
アカウンティング、定義 1351
キー 1356
サーバの指定 1356
デフォルト設定 1355
ユーザによってアクセスされるサービスのトラッキング 1363
ユーザに対するサービスの制限 1361
概要 1351
許可、定義 1351
設定 1356, 1358, 1361, 1363
アカウンティング 1363
ログイン認証 1358
許可 1361
認証キー 1356
定義 1351
動作 1353
認証、定義 1351
表示 1365
TCAM エントリ 1535
TCN 処理 103
Telnet 1338
パスワードの設定 1338
Terminal Access Controller Access Control System Plus 1351
「TACACS+」を参照 1351
TGT 1406
time 1779
「NTP」および「システム クロック」を参照してください 1779
time-range コマンド 1454
TLV 51
定義 51
traceroute 1915
traceroute コマンド 1915
「IP traceroute」も参照 1915
traceroute の使用 1915
traceroute、レイヤ 2 1914
ARP 1914
CDP 1914
IP アドレスおよびサブネット 1914
MAC アドレスおよび VLAN 1914
ブロードキャスト トラフィック 1914
ポートへの複数のデバイスの設定 1914
マルチキャスト トラフィック 1914
ユニキャスト トラフィック 1914
使用上のガイドライン 1914
説明 1914

U

UDLD 465, 466, 467, 468, 469, 471
aggressive 466, 467
normal 466
アグレッシブ モード 469
メッセージ タイム 469
イネーブル化 469, 471
インターフェイスごと 471
グローバル 469
エコー検出メカニズム 467, 468
ツイスト ペア リンク 467
ディセーブル化 471
インターフェイスごと 471
デフォルト設定 469
ネイバー データベース 467
ネイバー データベース メンテナンス 468
概要 466
光ファイバ リンク 467
制約事項 465
通常モード 466
UDP ジッタ、設定する 515
UDP ジッタ動作、IP SLA 507, 515
UplinkFast 330, 342, 344
イネーブル化 342
ディセーブル化 344

UplinkFast *(続き)*
説明 330
User Datagram Protocol 892
「UDP」を参照 892

V

Virtual Private Network（バーチャル プライベート ネットワーク） 157, 993
VPN を参照 157, 993
VLAN 1976
定義 1976
VLAN ACL 1442
VLAN マップを参照 1442
VLAN ID、検出する 1787
VLAN のデフォルト設定 1983
VLAN のモニタリング コマンド 1992
VLAN フィルタリングと SPAN 630
VLAN ポート メンバーシップ モード 1977
VLAN マップ 1442, 1452, 1474, 1475, 1477, 1478, 1480, 1490, 1492
サーバに対するアクセス拒否の例 1492
パケットの拒否と許可 1475, 1477
一般的な使用方法 1490
作成 1477
設定 1474
設定時の注意事項 1452
定義 1442
適用 1478
表示 1480
VLAN マップ エントリ、順序 1452
VLAN メンバーシップ 2028
確認 2028
VLAN 間ルーティング 870
VLANs 263, 265, 642, 649
RSPAN での送信元トラフィックの制限 649
SPAN での送信元トラフィックの制限 642
STP および IEEE 802.1Q トランク 265
VLAN ブリッジ STP 265
ダイナミック アドレスのエージング 263
VMPS 2022, 2023, 2025, 2028, 2029, 2031, 2032
サーバ アドレスの入力 2025
ダイナミック ポート メンバーシップ 2023, 2029, 2032
トラブルシューティング 2032
再確認 2029
説明 2023
メンバーシップの再確認 2028
再確認インターバル、変更 2029
VMPS *(続き)*
再試行回数、変更 2031
VMPS クライアント設定 2024
デフォルト 2024
VMPS コンフィギュレーション コマンドの例 2033
VoIP デバイスの詳細 845
VPN 163, 1011
ルーティングの設定 163, 1011
VRF 1535
VRF 認識サービス 159, 160, 161, 162, 1001, 1002, 1004, 1005, 1006, 1007, 1008
RADIUS 1006
ARP 160, 161, 1002
HSRP 1004
ping 1002
SNMP 1002
syslog 1006
tftp 162, 1008
traceroute 1007
uRPF 1005
設定 159, 1001
VRF、マルチキャストの設定 1009, 1192
VTP 1948, 1955, 1956
version 1956
設定の要件 1955
VTP アドバタイズ 1951
VTP ドメイン（VTP domain） 1949, 1968
VTP の設定 1955
VTP バージョン 1963
VTP バージョン 2 1952
VTP バージョン 3 1953
VTP パスワード 1961
VTP プライマリ 1962
VTP プルーニング 1954, 1965
VTP モード 1950, 1958

W

Web ベース認証 1665, 1671
カスタマイズ可能な Web ページ 1671
説明 1665
Web ベース認証、他の機能との相互作用 1674
WTD 808, 816
しきい値の設定 808, 816
出力キュー セット 816
入力キュー 808

Z

zzz] 1406

あ

アカウンティング 1351, 1363, 1391
RADIUS 1391
TACACS+ 1351, 1363
アカウンティング、定義 1351
アクセス グループ 1455
レイヤ 3 1455
アクセス グループ、IPv4 ACL をインターフェイスに対して適用する 1469
アクセス コントロール エントリ 1442
ACE を参照 1442
アクセス リスト 1447
「ACL」を参照 1447
アクセスの制限 1327, 1351, 1369
RADIUS 1369
TACACS+ 1351
概要 1327
アクティブ リンク 445, 447, 463
アクティブ化、AP-Count 1854
アクティブ化、ベース 1852
アドミニストレーティブ ディスタンス 921, 1042
OSPF 921
定義 1042
アドレス 118, 262, 1071, 1073, 1785, 1786, 1787, 1809
dynamic 262, 1785, 1786
デフォルト エージング 262
ラーニング 1786
迅速なエージング 262
定義 1785
GLOP 1071
IP マルチキャスト クラス D 1071
IPv6 118
MAC、検出する 1787
multicast 262, 1071
STP アドレス管理 262
SSM 1071
グローバル スコープ 1071
レイヤ 2 マルチキャスト 1073
限定スコープ 1071
静的 1809
追加と削除 1809
予約済みリンクローカル 1071
アドレスのエイリアス 1231
アドレスの割り当て 125
アドレス解決 1787
アドレス解決プロトコル 880
「ARP」を参照 880
アドレス形式 118
アプリケーション 120

い

イーサネット VLAN 1984
イーサネット VLAN のデフォルト設定 1982
イネーブル シークレット パスワード 1334
イネーブル パスワード 1334
イネーブル化 109, 1333, 1537, 1538, 1934
イネーブル化またはディセーブル化 105
イベント サービス 554
インターネット プロトコル バージョン 6 117
「IPv6」を参照 117
インターフェイス 49
Auto-MDIX、設定する 49
インターフェイス コンフィギュレーション 707
インベントリ管理 TLV 53

え

エージング時間 278, 316, 1800
MAC アドレス テーブル 1800
短縮 278, 316
MSTP 用 316
STP 用 278
エラー メッセージ出力のリダイレクト 1933
エリア ルーティング 976
IS-IS 976
エリア境界ルータ 910
「ABRs」を参照 910

お

および IPv6 118
および SSH 1420
オンボード障害ロギング 1917
オンライン診断 1899
概要 1899
説明 1899

か

ガイドライン 153
カスタマー エッジ デバイス 993
カスタマー エッジ デバイスでの複数 VPN ルーティング/転送 157, 993
　マルチ VRF CE を参照 157, 993
カスタマイズ可能な Web ページ、Web ベース認証 1671

き

キー 1356, 1380
キープアライブ メッセージ 255
キー発行局 1406
　「KDC」を参照 1406

く

クエリー、IGMP 1232
クライアント機能のイネーブル化 174
クラス D アドレス 1071
クラスレス ルーティング 877
クリア 1196
　databases 1196
　キャッシュ 1196
　テーブル 1196
クレデンシャル 1406
グローバル スコープ アドレス 1071
グローバルな脱退、IGMP 1254
クロススタック EtherChannel 386, 388, 401, 404
　図 386
　設定 404
　　レイヤ 2 インターフェイス上 404
　説明 386

こ

コマンド、権限レベルを設定する 1342
コマンドの権限レベルの設定：コマンド例 1347
コマンドの設定 1342
コマンドを使用 1917
コンフィギュレーション コマンド例 175
コンフィギュレーション ファイル 1337, 1979
　パスワード回復のディセーブル時の考慮事項 1337
ご利用条件 1406

さ

サーバ 1406
サーバ アドレスの入力 2025
サーバの指定 1356, 1380
サービス プロバイダー ネットワーク、MSTP および RSTP 285
サービス プロバイダー ネットワーク内 157, 993
サブネット ゼロ 876
サブネット マスク 874
サブネットワーク アクセス プロトコル（SNAP） 575
サポートされているデバイス 21, 77
サポートされない機能 124
サポートされる機能 118
サポートされる標準 78
サポートしているポート単位のワット数 21, 77

し

シェーピング モード 755
しきい値監視、IP SLA 506
システム MTU 229, 983
　および IS-IS LSP 983
システム MTU コマンドの設定例 75
システム クロック 1779, 1787, 1788, 1790
　概要 1779
　設定 1787, 1788, 1790
　　タイム ゾーン 1788
　　夏時間 1790
　　手動 1787
システム プライオリティ 410
システム プロンプト、デフォルト設定 1784
システム ルーティング 976
　IS-IS 976
システム機能 TLV 51
システム記述 TLV 51
システム名 1784, 1793
　デフォルト設定 1784
　手動設定 1793
システム名 TLV 51

す

スイッチ アクセス 1346
　表示 1346
スイッチ スタック 1934

スイッチから転送される送信元情報の制御：コマンド例 1319
スイッチから発信される送信元情報の制御：コマンド例 1319
スイッチで受信される送信元情報の制御：コマンド例 1320
スイッチド パケット、ACL 1493
スイッチの制限 125
スケジューリング 749, 752
スタック 255, 264
STP 255
ブリッジ ID 255
switch 264
サポートされる MSTP インスタンス 264
スタックの変更、影響 401
クロススタック EtherChannel 401
スタティック アクセス ポート 1988
スタティック アドレス 1785
「アドレス」を参照 1785
スタティック イネーブル パスワードの設定または変更：コマンド例 1347
スタティック バインディング 1537, 1538
追加 1537, 1538
スタティック ホスト 1538
スタティック モード 80
スタティック ルート 121, 1023
設定 1023
説明 121
スタティック ルートの概要 121
スタティックなマルチキャスト グループの設定：コマンド例 114
スタティック結合 107
スタブ ルーティング、EIGRP 938
ステータス、表示 1931
ステータスのモニタリング 1931
ステートレス自動設定 120
スヌーピング 113
スパース モード 1110, 1138
スタティック RP を使用 1138
スパース-デンス モード 1111
スプリット ホライズン、RIP 906
すべてのシステム診断のイネーブル 1944

せ

セカンダリ VLAN 2052
セカンダリ VLAN の設定 2057
セキュア HTTP クライアント 1436, 1437
設定 1436
表示 1437
セキュア HTTP クライアントの設定 1436
セキュア HTTP サーバ 1433, 1437
設定 1433
表示 1437
セキュア HTTP サーバの設定 1433
セキュア シェル 1419
セキュリティおよび識別 1931

そ

ソース ツリー 1120
利点 1120

た

ダイナミック VLAN 割り当て 2022
ダイナミック アドレス 262
「アドレス」を参照 262
ダイナミック ポート VLAN メンバーシップ 2023, 2026, 2028, 2029, 2032
トラブルシューティング 2032
再確認 2028, 2029
接続のタイプ 2026
説明 2023
ダイナミック ポート メンバーシップ 2023, 2029, 2032
トラブルシューティング 2032
再確認 2029
説明 2023
ダイナミック モード 1237
ダイナミックアクセス ポート 2026
設定 2026
タイム ゾーン 1788

ち

チケット 1406
チャネル グループ 389
番号 389
物理および論理インターフェイスのバインド 389

つ

ツイスト ペア、単方向リンクの検出 466

て

ディセーブル化 112
デバイス 261
　ルート 261
デバイス プライオリティ 276, 313
　MSTP 313
　STP 276
デフォルト MSDP ピアの設定：コマンド例 1318
デフォルト ゲートウェイ 886
デフォルト ネットワーク 1026
デフォルト ルータ プリファレンス 120
　「DRP」を参照 120
デフォルト ルータ プリファレンス（DRP） 120
デフォルトルータ プリファレンスの設定：コマンド例 176
デフォルト ルート 1026
デフォルトの Web ベース認証の設定 1676
　802.1X 1676
デフォルト設定 55, 104, 105, 125, 157, 171, 266, 303, 399, 450, 451, 469, 635, 697, 758, 845, 941, 996, 1083, 1124, 1235, 1239, 1241, 1330, 1355, 1377, 1430, 1785, 1786
　BGP 941
　DNS 1785
　EtherChannel 399
　Flex Link 450
　IGMP 1083
　IGMP スヌーピング 104, 105, 1235
　IGMP スロットリング 1241
　IGMP フィルタリング 1241
　IPv6 125
　LLDP 55
　MAC アドレス テーブル 1786
　MAC アドレステーブル移動更新 451
　MSTP 303
　MVR 1239
　PIM 1124
　RADIUS 1377
　RSPAN 635
　SPAN 635
　SSL 1430
　STP 266
　TACACS+ 1355
　UDLD 469
　パスワードおよび権限レベル 1330
　バナー 1785
デフォルト設定 *(続き)*
　マルチ VRF CE 157, 996
　自動 QoS 845
デュアル アクション検出を使用 394
デュアルアクション検出 394
デンス モード 1109
テンプレート 1880
　設定 1880

と

トークン リング 1963
ドメイン、ISO IGRP ルーティング 976
ドメイン名 1784, 1955
　DNS 1784
トラストポイント、CA 1428
トラップ 1801, 1804, 1807
　MAC アドレス通知設定 1801, 1804, 1807
　イネーブル化 1801, 1804, 1807
トラフィック 1446
　フラグメント化 1446
トラブルシューティング 854, 1166, 1913, 1915, 1917, 1931, 1934, 2032
　debug コマンドを使用 1917
　PIMv1 および PIMv2 の相互運用性の問題 1166
　ping を使用 1913
　SFP セキュリティおよび識別 1931
　show forward コマンド 1934
　traceroute の使用 1915
　パケット転送の設定 1934
　自動 QoS 854
トラブルシューティング コマンド例 1942
トランキング 1998
トランキング モード 1998
トランク 2000, 2003, 2005
　許可 VLAN 2000
　設定 2003
トランク インターフェイス 1535
トランク ポート 2003
トランクのフェールオーバー 416

ね

ネイティブ VLAN 228, 2009
ネイバー探索 120
ネイバー探索、IPv6 120

ネイバー探索および回復、EIGRP 928
ネットワーク サービス 1410
ネットワーク パフォーマンス、IP SLA で測定する 503
ネットワーク ポリシー TLV 53
ネットワーク環境の提案 1369
ネットワーク負荷分散 2001
STP パス コスト 2001
STP プライオリティ 2001

は

バインディング コンフィギュレーション 1534
automatic 1534
manual 1534
バインディング データベース 1513
アドレス、DHCP サーバ 1513
DHCP、Cisco IOS サーバ データベースを参照 1513
バインディング テーブル 1534
パケットの変更、QoS での 756
パケット転送の設定 1934
パス MTU 検出 119
パス コスト 274, 312
MSTP 312
STP 274
パスワード 1327, 1330, 1333, 1334, 1337, 1338, 1340, 1912
デフォルト設定 1330
暗号化 1334
回復 1912
回復のディセーブル化 1337
概要 1327
設定 1333, 1334, 1338, 1340
enable secret 1334
Telnet 1338
イネーブル化 1333
ユーザ名 1340
パスワードおよび権限レベル 1330
パスワードおよび権限レベル コマンドの設定例 1347
パスワードの設定 1338
パスワード回復のディセーブル時の考慮事項 1337
バックアップ 254
port 254
バックアップ インターフェイス 444
「Flex Link」 を参照 444
バッファ割り当て 753, 754
バナー 1785, 1797, 1798
デフォルト設定 1785
バナー *(続き)*
設定 1797, 1798
login 1798
Message-of-The-Day ログイン 1797
パラレル パス、ルーティング テーブル内 1022
パワー バジェット：コマンド例 92

ふ

フィルタ、IP 1441
ACL、IP フィルタを参照 1441
IP 1441
zzz] 1441
フィルタリング 1470
非 IP トラフィック。 1470
フォールバック ブリッジング 255, 265
STP 255
キープアライブ メッセージ 255
VLAN ブリッジ STP 265
フォワーディング 125, 260, 995
ステート 260
プライベート VLAN 2049, 2055, 2059, 2060, 2064, 2066, 2068
broadcast 2055
multicast 2055
unicast 2055
セカンダリ VLAN のマッピング 2068
ポート設定 2059
レイヤ 2 インターフェイスの設定 2064
設定 2060
複数のスイッチ 2055
無差別ポートの設定 2066
プライベート VLAN ドメイン 2051
プライベート VLAN のモニタ 2073
プライマリ VLAN の設定 2057
フラッシュ メモリ 1917
ブリッジ プロトコル データ ユニット 254
ブリッジド パケット、ACL 1493
ブリッジ型 NetFlow 708
ブリッジ識別子（ブリッジID） 256
プルーニング適格リスト 2007
プレフィックス リスト、BGP 959
フロー エクスポータ 700
フロー モニタ 703
フロー レコード 688
ブロードキャスト ストーム 890
ブロードキャスト トラフィック 1914

ブロードキャスト パケット 890
directed 890
フラッディング 890
ブロードキャストのフラッディング 895
プロキシ ARP 880, 885
ディセーブルにした IP ルーティング 885
定義 880
プロキシ レポート 447
ブロック 259
state 259
プロトコル依存モジュール、EIGRP 929
プロバイダー エッジ デバイス 994

へ

ベンダー固有 1394
ベンダー固有の RADIUS 属性を使用するスイッチ設定：コマンド例 1402
ベンダー独自仕様 1396
ベンダー独自仕様の RADIUS サーバとの通信に関するスイッチ設定：コマンド例 1403

ほ

ポート 261, 2052
community 2052
isolated 2052
ルート 261
無差別 2052
ポート ACL 1442, 1443
のタイプ 1443
定義 1442
ポート VLAN ID TLV 51
ポート セキュリティ 1535
ポート プライオリティ 273, 309, 411
MSTP 309
STP 273
ポート ベース認証 1666, 1676, 1678, 1682, 1691
switch 1666
プロキシとして 1666
イネーブル化 1682
802.1X 認証 1682
デバイスの役割 1666
デフォルト設定 1676
設定 1678, 1682
RADIUS サーバ 1678
ポート ベース認証 *(続き)*
設定 *(続き)*
スイッチ上の RADIUS サーバ パラメータ 1682
設定時の注意事項 1676
統計情報の表示 1691
ポートチャネル インターフェイス 389
番号 389
ポートの信頼状態 738
分類オプション 738
ポートへの複数のデバイスの設定 1914
ポート記述 TLV 51
ポート集約プロトコル 391
「EtherChannel」を参照 391
ホスト シグナリング 1078
ホスト、ダイナミック ポートでの制限 2032
ホット スタンバイ ポート 409
ポリサー 744, 796
のタイプ 744
設定 796
複数のトラフィック クラス 796
ポリシーベース ルーティング 1034
「PBR」を参照 1034
ポリシング 744
トークンバケット アルゴリズム 744
ポリシング済み DSCP マップ、QoS での 802

ま

マーキング 791, 796, 837, 838
ポリシー マップのアクション 791
集約ポリシング機能でのアクション 796, 837, 838
マッピング テーブル 761
デフォルト設定 761
マッピング、VLAN の 2072
マルチ VRF CE 157, 166, 993, 995, 996, 997, 1014
デフォルト設定 157, 996
ネットワーク コンポーネント 995
パケット転送処理 995
設定時の注意事項 997
設定例 166, 1014
定義 157, 993
マルチキャスト ping 1163, 1164
ルータ の設定 1163
ルータへの ping 1164
マルチキャスト TV アプリケーション 1237
マルチキャスト VRF の設定 1009, 1192

マルチキャスト クライアント エージングの堅牢性 102
マルチキャスト グループ 107, 1232, 1234, 1248
スタティック結合 107, 1248
参加 1232
脱退 1234
マルチキャスト グループ伝送方式 1068
マルチキャスト トラフィック 1914
マルチキャスト パケット 1495
への ACL 1495
マルチキャスト マルチメディア セッション、アドバタイジング 1195
マルチキャスト ルータ インターフェイス、モニタリング 1276
マルチキャスト ルータ ポート、追加する 1246
マルチキャスト ルータ ポートの設定：コマンド例 114
マルチキャスト ルータ検出 102
マルチキャスト高速コンバージェンス 446, 462
マルチキャスト転送 1117
マルチキャスト動作の確認 1156, 1157, 1159
SPT 上のルータ 1156, 1157
ラスト ホップ ルータ 1159
モニタリング *(続き)*
IGMP 113, 1096
スヌーピング 113
IP 898, 1196
アドレス テーブル 898
マルチキャスト ルーティング 1196
IP SLA の動作 522
IPv4 ACL コンフィギュレーション 1479
IPv6 170
OSPF 926
RP マッピング情報 1165
SFP ステータス 1931
SSM マッピング 1219
VLAN 1480
maps 1480
フィルタ 1480
VTP 1971
アクセス グループ 1480
トンネリング ステータス 250
プライベート VLAN 2071
プローブでの分析用のネットワーク トラフィック 623
音声 VLAN 2046

み

ミラーリング トラフィック、分析用の 623

め

メッセージ、ユーザに対するバナーを使用した 1785
メトリック、BGP 内 952
メトリック変換、ルーティング プロトコル間 1033
メモリ割り当て 754
メンバーシップの再確認 2028

も

モード 391, 395
モニタリング 81, 113, 170, 250, 458, 522, 623, 711, 830, 898, 926, 939, 1020, 1096, 1165, 1196, 1219, 1276, 1437, 1479, 1480, 1931, 1971, 2046, 2071
マルチキャスト ルータ インターフェイス 1276
BSR 情報 1165
CEF 1020
EIGRP 939
Flex Link 458

ゆ

ユーザによってアクセスされるサービスのトラッキング 1363, 1391
ユーザに対するサービスの制限 1361, 1389
ユーザ認証方式、サポートされる 1419
ユーザ名 1340
ユーザ名ベース認証 1340
ユニキャスト MAC アドレス フィルタリング 1810
設定 1810
ユニキャスト トラフィック 1914

ら

ライセンス AP-Count のアクティブ化 1854
ライセンス ベースのイメージのアクティブ化 1852
ランデブー ポイント 1126

り

リークする、IGMP レポートを 447
リスニング 260
state 260

リセット、BGP 内 949
リトライ回数、VMPS、変更する 2031
リファレンス 294
リモート認証ダイヤルイン ユーザ サービス 1369
「RADIUS」を参照 1369
リンク ローカル ユニキャスト アドレス 119
リンクステート トラッキング 416
説明 416
リンクステート トラッキングの設定：例 421
リンクの失敗、単一方向の検出 295
リンクの冗長性 444
「Flex Link」 を参照 444

る

ルータ ACL 1442, 1445
のタイプ 1445
定義 1442
ルータ ID 123
ルータ ID、OSPF 925
ルーティング 1027
情報の再配信 1027
ルーティング ドメイン連合、BGP 969
ルーテッド パケット、ACL 1494
ルーテッド ポート 871, 872, 1535
IP アドレス 872
設定 871
ルート ターゲット、VPN 995
ルート デバイス 269, 307
MSTP 307
STP 269
ルート マップ 955, 1034
BGP 955
ポリシーベース ルーティング 1034
ルート リフレクタ、BGP 970
ルート計算タイマー、OSPF 921
ルート選択、BGP 951

れ

レイヤ 2 224
protocol 224
レイヤ 2 EtherChannel の設定：例のコマンド 414
レイヤ 2 EtherChannel 設定時の注意事項 403
レイヤ 2 NetFlow 709
レイヤ 2 インターフェイス 404
レイヤ 2 インターフェイス モード 1999
レイヤ 2 インターフェイス上 404
レイヤ 2 トンネリング 224
EtherChannel 224
レイヤ 2 の traceroute 1914
ARP 1914
CDP 1914
IP アドレスおよびサブネット 1914
MAC アドレスおよび VLAN 1914
ブロードキャスト トラフィック 1914
ポートへの複数のデバイスの設定 1914
マルチキャスト トラフィック 1914
ユニキャスト トラフィック 1914
使用上のガイドライン 1914
説明 1914
レイヤ 2 プロトコル トンネリング 230, 233, 234
デフォルト 234
レイヤ 3 インターフェイス 125, 871, 1004
IPv6 アドレスの割り当て 125
のタイプ 871
レイヤ 2 モードからの変更 1004
レイヤ 3 パケット、分類方式 736
レスポンダ、IP SLA 504, 509
イネーブル化 509
説明 504
レポート抑制 112
ディセーブル化 112
レポート抑制、IGMP 112, 1235, 1260
ディセーブル化 112, 1260
説明 1235
レルム 1406

ろ

ローカル SPAN 623
ロード バランシング 397, 407
ロードバランシングの利点 398
ロギング メッセージ、ACL 1451
ログイン 1346
ログイン バナー 1785
ログイン認証 1358, 1383
RADIUS 1383
TACACS+ 1358
ロケーション TLV 53

わ

ワイヤード ロケーション サービス **53, 54, 65**
ロケーション TLV **53**
ワイヤード ロケーション サービス *(続き)*
設定 **65**
説明 **54**