# Cisco IOS XE Everest 16.6.x（Catalyst 3650 スイッチ）セキュリティ コンフィギュレーション ガイド

**初版**：2017 年 7 月 31 日

**最終更新**：2017 年 11 月 3 日

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

© 2017 Cisco Systems, Inc. All rights reserved.

# 目 次


第 1 章 不正アクセスの防止 1

機能情報の確認 1

不正アクセスの防止 1

第 2 章 パスワードおよび権限レベルによるスイッチ アクセスの制御 3

パスワードおよび権限によるスイッチ アクセスの制御の制約事項 3

パスワードおよび権限レベルに関する情報 3

デフォルトのパスワードおよび権限レベル設定 3

追加のパスワード セキュリティ 4

パスワードの回復 4

端末回線の Telnet 設定 5

ユーザ名とパスワードのペア 5

権限レベル 5

パスワードおよび権限レベルでスイッチ アクセスを制御する方法 6

スタティック 有効 パスワードの設定または変更 6

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 7

パスワード回復のディセーブル化 10

端末回線に対する Telnet パスワードの設定 11

ユーザ名とパスワードのペアの設定 12

コマンドの特権レベルの設定 14

回線のデフォルト特権レベルの変更 16

権限レベルへのログインおよび終了 17

スイッチ アクセスのモニタリング 18

パスワードおよび権限レベルの設定例 18

例：スタティック イネーブル パスワードの設定または変更 18
例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 18
例：端末回線に対する Telnet パスワードの設定 18
例：コマンドの権限レベルの設定 18
その他の参考資料 19

第 3 章 **TACACS+ の設定** 21
TACACS+ の前提条件 21
TACACS+ によるスイッチ アクセスの制御について 22
TACACS+ およびスイッチ アクセス 22
TACACS+ の概要 22
TACACS+ の動作 24
方式リスト 25
TACACS+ 設定オプション 25
TACACS+ ログイン認証 25
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可 26
TACACS+ Accounting 26
TACACS+ のデフォルト設定 26
TACACS+ とスイッチ アクセスを設定する方法 26
TACACS+ サーバ ホストの指定および認証キーの設定 26
TACACS+ ログイン認証の設定 28
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定 31
TACACS+ アカウンティングの起動 33
AAA サーバが到達不能な場合のルータとのセッションの確立 34
TACACS+ のモニタリング 34
TACACS+ によるスイッチ アクセスの制御に関するその他の参考資料 35
TACACS+ によるスイッチアクセスの機能情報 35

第 4 章 **RADIUS の設定** 37
RADIUS を設定するための前提条件 37
RADIUS の設定に関する制約事項 38

RADIUS について 38
RADIUS およびスイッチ アクセス 38
RADIUS の概要 39
RADIUS の動作 40
RADIUS 許可の変更 41
Change-of-Authorization 要求 42
CoA 要求応答コード 44
CoA 要求コマンド 45
セッション強制終了のスタック構成ガイドライン 48
RADIUS のデフォルト設定 49
RADIUS サーバ ホスト 49
RADIUS ログイン認証 50
AAA サーバグループ 50
AAA 許可 51
RADIUS アカウンティング 51
ベンダー固有の RADIUS 属性 51
ベンダー独自仕様の RADIUS サーバ通信 66
RADIUS の設定方法 67
RADIUS サーバ ホストの識別 67
RADIUS ログイン認証の設定 69
AAA サーバ グループの定義 72
ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定 74
RADIUS アカウンティングの起動 75
すべての RADIUS サーバの設定 76
ベンダー固有の RADIUS 属性を使用するDevice設定 78
ベンダー独自の RADIUS サーバとの通信に関するDeviceの設定 79
次の上での CoA の設定 Device 81
CoA 機能のモニタリング 83

第 5 章 **Kerberos の設定** 85

Kerberos によるスイッチ アクセスの制御の前提条件 85
Kerberos に関する情報 85
Kerberos とスイッチ アクセス 86
Kerberos の概要 86
Kerberos の動作 88
境界スイッチに対する認証の取得 89
KDC からの TGT の取得 89
ネットワーク サービスに対する認証の取得 89
Kerberos を設定する方法 90
Kerberos 設定の監視 90
その他の参考資料 90

第 6 章
**MACsec の暗号化 93**
MACsec 暗号化について 93
Media Access Control Security と MACsec Key Agreement 94
MKA ポリシー 95
仮想ポート 95
MACsec およびスタッキング 96
MACsec、MKA、および 802.1x ホスト モード 96
EAP-TLS を使用した MACsec MKA に関する情報 102
EAP-TLS を使用した MACsec MKA の前提条件 102
EAP-TLS を使用した MACsec MKA の制限事項 102
Cisco TrustSec の概要 102
MACsec 暗号化の設定方法 104
MKA および MACsec の設定 104
MACsec MKA のデフォルト設定 104
MKA ポリシーの設定 105
スイッチからホストへの MACsec の暗号化設定 106
PSK を使用した MACsec MKA の設定 109
PSK を使用した、インターフェイスでの MACsec MKA の設定 110
EAP-TLS を使用した MACsec MKA の設定 111

リモート認証 112
ローカル認証 120
EAP-TLS を使用した MACsec MKA の確認 128
Cisco TrustSec MACsec の設定 130
手動モードでの Cisco TrustSec スイッチ間リンク セキュリティの設定 130
MACsec 暗号化の設定例 132
スイッチからホストへの MACsec の暗号化設定 132
EAP-TLS を使用した MACsec MKA の設定例 135
例: : 証明書の登録 135
例 : 802.1x 認証の有効化と AAA の設定 135
例 : EAP-TLS プロファイルと 802.1x クレデンシャルの設定 135
例 : インターフェイスでの 802.1 X、PKI、および MACsec の設定の適用 136
例 : Cisco TrustSec スイッチ間リンクセキュリティの設定 136

第 7 章 ローカル認証および許可の設定 139
ローカル認証および許可の設定方法 139
スイッチのローカル認証および許可の設定 139
ローカル認証および許可のモニタリング 141
その他の参考資料 142

第 8 章 セキュア シェルの設定 143
セキュア シェルを設定するための前提条件 143
セキュア シェルの設定に関する制約事項 144
セキュア シェルの設定について 144
SSH およびスイッチ アクセス 144
SSH サーバ、統合クライアント、およびサポートされているバージョン 145
SSH 設定時の注意事項 145
セキュア コピー プロトコルの概要 146
セキュア コピー プロトコル 146
セキュア シェルの設定方法 147
SSH を実行するためのデバイスのセットアップ 147

SSH サーバの設定 148
SSH の設定およびステータスのモニタリング 151

第 9 章
SSH 認証の X.509v3 証明書 153
SSH 認証の X.509v3 証明書 153
SSH 認証用のデジタル証明書の前提条件 153
SSH 認証の X.509v3 証明書の制約事項 153
SSH 認証用の X.509v3 証明書に関する情報 154
デジタル証明書 154
X.509v3 を使用したサーバおよびユーザ認証 154
SSH 認証用の X.509v3 証明書の設定方法 155
サーバ認証にデジタル証明書を使用するための IOS SSH サーバの設定 155
ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定 156
デジタル証明書を使用したサーバおよびユーザ認証の設定の確認 158
SSH 認証用の X.509v3 証明書の設定例 159
例：サーバ認証にデジタル証明書を使用するための IOS SSH サーバの設定 159
例：ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定 159
SSH 認証の X.509v3 証明書に関するその他の参考資料 160
SSH 認証の X.509v3 証明書の機能情報 161

第 10 章
Secure Socket Layer HTTP の設定 163
Secure Socket Layer HTTP について 163
セキュア HTTP サーバおよびクライアントの概要 163
CA のトラストポイント 164
CipherSuite 165
SSL のデフォルト設定 166
SSL の設定時の注意事項 167
Secure Socket Layer HTTP の設定方法 167
CA のトラストポイントの設定 167
セキュア HTTP サーバの設定 169

セキュア HTTP クライアントの設定 173
セキュア HTTP サーバおよびクライアントのステータスのモニタリング 175
Secure Socket Layer HTTP に関するその他の参考資料 175
Secure Socket Layer HTTP に関する機能情報 176

第 11 章 **IPv4 ACL** 177
IPv4 アクセス コントロール リストの設定に関する制約事項 177
ACL によるネットワーク セキュリティに関する情報 178
ACL の概要 179
アクセス コントロール エントリ 179
ACL でサポートされるタイプ 179
サポートされる ACL 180
ACL 優先順位 180
ポート ACL 181
ルータ ACL 182
VLAN マップ 183
ACEおよびフラグメント化されたトラフィックとフラグメント化されていないトラフィック 183
ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例 184
ACL とスイッチ スタック 185
アクティブ スイッチおよび ACL の機能 185
スタック メンバおよび ACL の機能 185
アクティブ スイッチの障害および ACL 185
標準 IPv4 ACL および拡張 IPv4 ACL 186
IPv4 ACL スイッチでサポートされていない機能 186
アクセス リスト番号 186
番号付き標準 IPv4 ACL 187
番号付き拡張 IPv4 ACL 188
名前付き IPv4 ACL 189
ACL ロギング 189

ハードウェアおよびソフトウェアによる IP ACL の処理 190
VLAN マップの設定時の注意事項 190
VLAN マップとルータ ACL 191
VLAN マップとルータ ACL の設定時の注意事項 192
ACL の時間範囲 192
IPv4 ACL のインターフェイスに関する注意事項 193
ACL の設定方法 194
IPv4 ACL の設定 194
番号付き標準 ACL の作成（CLI） 194
番号付き拡張 ACL の作成（CLI） 196
名前付き標準 ACL の作成 201
名前付き拡張 ACL の作成 202
ACL の時間範囲の設定 204
端末回線への IPv4 ACL の適用 205
インターフェイスへの IPv4 ACL の適用（CLI） 207
名前付き MAC 拡張 ACL の作成 208
レイヤ 2 インターフェイスへの MAC ACL の適用 210
VLAN マップの設定 211
VLAN マップの作成 213
VLAN への VLAN マップの適用 215
IPv4 ACL のモニタリング 216
ACL の設定例 217
例：ACL での時間範囲を使用 217
例：ACL へのコメントの挿入 218
IPv4 ACL の設定例 218
小規模ネットワークが構築されたオフィス用の ACL 218
例：小規模ネットワークが構築されたオフィスの ACL 219
例：番号付き ACL 220
例：拡張 ACL 220
例：名前付き ACL 221
例：IP ACL に適用される時間範囲 222

例：コメント付き IP ACL エントリの設定 222
例：ACL ロギング 223
ACL および VLAN マップの設定例 224
例：パケットを拒否する ACL および VLAN マップの作成 224
例：パケットを許可する ACL および VLAN マップの作成 225
例：IP パケットのドロップおよび MAC パケットの転送のデフォルト アクション 225
例：MAC パケットのドロップおよび IP パケットの転送のデフォルト アクション 226
例：すべてのパケットをドロップするデフォルト アクション 226
ネットワークでの VLAN マップの使用方法の設定例 226
例：ワイヤリング クローゼットの設定 226
例：別の VLAN にあるサーバへのアクセスの制限 228
例：別の VLAN にあるサーバへのアクセスの拒否 228
VLAN に適用されるルータ ACL と VLAN マップの設定例 229
例：ACL およびスイッチド パケット 229
例：ACL およびブリッジド パケット 230
例：ACL およびルーテッド パケット 230
例：ACL およびマルチキャスト パケット 231

第 12 章 **IPv6 ACL** 233
IPv6 ACL の概要 233
スイッチ スタックおよび IPv6 ACL 234
ACL 優先順位 234
VLAN マップ 235
他の機能およびスイッチとの相互作用 235
IPv6 ACL の制限 236
IPv6 ACL のデフォルト設定 237
IPv6 ACL の設定 237
インターフェイスへの IPv6 ACL の付加 242
VLAN マップの設定 243
VLAN への VLAN マップの適用 245
IPv6 ACL のモニタリング 246

第 13 章 DHCP の設定 249

DHCP に関する情報 249

DHCP サーバ 249

DHCP リレー エージェント 249

DHCP スヌーピング 249

オプション 82 データ挿入 251

Cisco IOS DHCP サーバ データベース 255

DHCP スヌーピング バインディング データベース 255

DHCP スヌーピングおよびスイッチ スタック 257

DHCP 機能の設定方法 257

DHCP スヌーピングのデフォルト設定 257

DHCP スヌーピング設定時の注意事項 258

DHCP サーバの設定 259

DHCP サーバとスイッチ スタック 259

DHCP リレー エージェントの設定 259

パケット転送アドレスの指定 260

DHCP スヌーピングおよびオプション 82 を設定するための前提条件 262

Cisco IOS DHCP サーバ データベースのイネーブル化 264

DHCP スヌーピング情報のモニタリング 264

DHCP サーバ ポートベースのアドレス割り当ての設定 265

DHCP サーバ ポートベースのアドレス割り当ての設定に関する情報 265

ポートベースのアドレス テーブルのデフォルト設定 265

ポートベースのアドレス割り当て設定時の注意事項 266

DHCP スヌーピング バインディング データベース エージェントのイネーブル化 266

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化 268

DHCP サーバ ポートベースのアドレス割り当てのモニタリング 269

第 14 章 Cisco Discovery Protocol バイパスの設定 271

Cisco Discovery Protocol バイパスの制約事項 271

Cisco Discovery Protocol バイパスについて 271

Cisco Discovery Protocol バイパスの設定方法 272
Cisco Discovery Protocol バイパスの設定例 274
例：Cisco Discovery Protocol バイパスの有効化 274
Cisco Discovery Protocol ネイバーの無効化 274
例：Cisco Discovery Protocol バイパスの無効化 274
Cisco Discovery Protocol バイパスの機能情報 275

第 15 章 **IP ソース ガードの設定** 277
IP ソース ガードの概要 277
IP ソース ガード 277
スタティック ホスト用 IP ソース ガード 278
IP ソース ガードの設定時の注意事項 279
IP ソース ガードの設定方法 280
IP ソース ガードのイネーブル化 280
レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定 281
IP ソース ガードのモニタリング 283
その他の参考資料 284

第 16 章 **ダイナミック ARP インスペクションの設定** 285
ダイナミック ARP インスペクションの制約事項 285
ダイナミック ARP インスペクションの概要 287
インターフェイスの信頼状態とネットワーク セキュリティ 289
ARP パケットのレート制限 290
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ 290
廃棄パケットのロギング 291
ダイナミック ARP インスペクションのデフォルト設定 291
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ 292
非 DHCP 環境での ARP ACL の設定 292
DHCP 環境でのダイナミック ARP インスペクションの設定 295
着信 ARP パケットのレート制限 298
ダイナミック ARP インスペクション検証チェックの実行 300

DAI のモニタリング 302
DAI の設定の確認 303
その他の参考資料 304

第 17 章 IPv6 ファースト ホップ セキュリティの設定 305
IPv6 でのファースト ホップ セキュリティの前提条件 305
IPv6 でのファースト ホップ セキュリティの制約事項 305
IPv6 でのファースト ホップ セキュリティに関する情報 306
IPv6 スヌーピング ポリシーの設定方法 308
IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法 310
IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 312
IPv6 スヌーピング ポリシーを VLAN にグローバルにアタッチする方法 313
IPv6 バインディング テーブルの内容を設定する方法 314
IPv6 ネイバー探索インスペクション ポリシーの設定方法 315
IPv6 ネイバー探索インスペクション ポリシーをインターフェイスにアタッチする方法 317
IPv6 ネイバー探索インスペクション ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 318
IPv6 ネイバー探索インスペクション ポリシーを全体的に VLAN にアタッチする方法 319
IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法 320
IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法 323
IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 324
IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法 325
IPv6 DHCP ガード ポリシーの設定方法 326
IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法 328
IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 329
IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法 331

IPv6 ソース ガードの設定方法 331
IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法 333
IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 333
IPv6 プレフィックス ガードの設定方法 334
IPv6 プレフィックス ガード ポリシーをインターフェイスにアタッチする方法 335
IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 336
IPv6 ファースト ホップ セキュリティの設定例 337
例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 337
例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 337

第 18 章 SISF ベースのデバイストラッキングの設定 339
SISF ベースのデバイストラッキングに関する情報 339
SISF ベースのデバイストラッキングの概要 339
SISF ベースのデバイストラッキングを有効にするオプション 340
レガシーコマンドから SISF ベースの Device-Tracking コマンドへの移行 341
レガシー IPDT と IPv6 スヌーピングから SISF ベースのデバイストラッキングへの移行 341
IPDT、IPv6 スヌーピング、および SISF ベースのデバイストラッキング CLI の互換性 343
SISF ベースのデバイストラッキングの設定方法 345
SISF ベースのデバイストラッキングの手動による有効化 345
ターゲットへのデフォルト デバイス トラッキング ポリシーの適用 345
カスタム設定を使用したカスタム デバイス トラッキング ポリシーの作成 346
デバイス トラッキング ポリシーのインターフェイスへの適用 350
デバイス トラッキング ポリシーの VLAN への適用 351
Cisco IOS XE Everest 16.6.x での SISF ベースのデバイストラッキングのプログラムによる有効化 352
トランクポートからのバインディングエントリの作成を停止するためのマルチスイッチネットワークの設定 355

SISF ベースのデバイストラッキングの設定例 356
例：Cisco IOS XE Everest 16.6.x での SISF ベースのデバイストラッキングのプログラムによる有効化 356
例：ターゲットでの IPv6 デバイストラッキングの無効化 357
例：VLAN 上の SVI に対する IPv6 の有効化（重複アドレスの問題を軽減するため） 358
例：IPv4 重複アドレスの問題の緩和 358
例：短いデバイストラッキング バインディング到達可能時間の回避 360
SISF ベースのデバイストラッキングの機能履歴と情報 360

第 19 章
**IEEE 802.1x ポートベースの認証の設定 363**
802.1x ポートベース認証について 363
ポートベース認証プロセス 364
ポートベース認証の開始およびメッセージ交換 366
ポートベース認証の認証マネージャ 368
ポートベース認証方法 368
ユーザ単位 ACL および Filter-Id 369
ポートベース認証マネージャ CLI コマンド 369
許可ステートおよび無許可ステートのポート 371
ポートベース認証とスイッチ スタック 373
802.1X のホスト モード 373
802.1x マルチ認証モード 374
ユーザごとのマルチ認証 VLAN 割り当て 375
MAC 移動 377
MAC 置換 377
802.1x アカウンティング 378
802.1x アカウンティング属性値ペア 378
802.1x 準備状態チェック 379
スイッチと RADIUS サーバ間の通信 380
VLAN 割り当てを使用した 802.1x 認証 380
ユーザ単位 ACL を使用した 802.1x 認証 382
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証 383

Cisco Secure ACS およびリダイレクト URL の属性と値のペア 384
Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア 384
VLAN ID ベース MAC 認証 385
ゲスト VLAN を使用した 802.1x 認証 385
制限付き VLAN を使用した 802.1x 認証 386
アクセス不能認証バイパスを使用した 802.1x 認証 387
複数認証ポートのアクセス不能認証バイパスのサポート 388
アクセス不能認証バイパスの認証結果 388
アクセス不能認証バイパス機能の相互作用 389
802.1x クリティカル音声 VLAN 390
802.1x ユーザ ディストリビューション 391
802.1x ユーザ ディストリビューションの設定時の注意事項 391
音声 VLAN ポートを使用した IEEE 802.1x 認証 391
ポート セキュリティを使用した IEEE 802.1x 認証 392
WoL 機能を使用した IEEE 802.1x 認証 392
MAC 認証バイパスを使用した IEEE 802.1x 認証 393
Network Admission Control レイヤ 2 IEEE 802.1x 検証 394
柔軟な認証の順序設定 395
Open1x 認証 396
マルチドメイン認証 396
Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ 398
音声認識 802.1x セキュリティ 400
コモン セッション ID 400
802.1x ポートベース認証の設定方法 401
802.1x 認証のデフォルト設定 401
802.1x 認証設定時の注意事項 402
802.1X 認証 402
VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス 403
MAC 認証バイパス 405
ポートあたりのデバイスの最大数 405

802.1x 準備状態チェックの設定 405
音声認識 802.1x セキュリティの設定 407
802.1x 違反モードの設定 409
802.1X 認証の設定 411
802.1x ポートベース認証の設定 412
スイッチと RADIUS サーバ間の通信の設定 414
ホスト モードの設定 416
定期的な再認証の設定 418
待機時間の変更 419
スイッチからクライアントへの再送信時間の変更 420
スイッチからクライアントへのフレーム再送信回数の設定 422
再認証回数の設定 423
MAC 移動のイネーブル化 424
MAC 置換のイネーブル化 425
802.1x アカウンティングの設定 426
ゲスト VLAN の設定 428
制限付き VLAN の設定 429
制限付き VLAN の認証試行回数の設定 430
クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定 432
アクセス不能認証バイパスの設定例 435
WoL を使用した 802.1x 認証の設定 435
MAC 認証バイパスの設定 436
802.1x ユーザ ディストリビューションの設定 437
VLAN グループの設定例 438
NAC レイヤ 2 802.1x 検証の設定 439
NEAT を使用したオーセンティケータ スイッチの設定 441
NEAT を使用したサプリカント スイッチの設定 443
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定 445
ダウンロード可能な ACL の設定 446
ダウンロード ポリシーの設定 447
VLAN ID ベース MAC 認証の設定 449

柔軟な認証順序の設定 450
Open1x の設定 451
ポート上での 802.1x 認証のディセーブル化 453
802.1x 認証設定のデフォルト値へのリセット 454
802.1x の統計情報およびステータスのモニタリング 455

第 20 章 **Web ベース認証** 457
Web ベース認証の概要 457
デバイスのロール 458
ホストの検出 459
セッションの作成 460
認証プロセス 460
ローカル Web 認証バナー 461
Web 認証カスタマイズ可能な Web ページ 464
ガイドライン 464
認証プロキシ Web ページの注意事項 465
成功ログインに対するリダイレクト URL の注意事項 466
その他の機能と Web ベース認証の相互作用 466
ポート セキュリティ 466
LAN ポート IP 467
ゲートウェイ IP 467
ACL 467
コンテキストベース アクセス コントロール 467
EtherChannel 467
Web ベース認証の設定方法 468
デフォルトの Web ベース認証の設定 468
Web ベース認証の設定に関する注意事項と制約事項 468
認証ルールとインターフェイスの設定 470
AAA 認証の設定 472
スイッチ/RADIUS サーバ間通信の設定 474
HTTP サーバの設定 475

認証プロキシ Web ページのカスタマイズ 476
成功ログインに対するリダイレクション URL の指定 478
Web ベース認証パラメータの設定 478
Web ベースの認証ローカル バナーの設定 479
Web ベース認証キャッシュ エントリの削除 480
Web ベース認証ステータスの確認 481

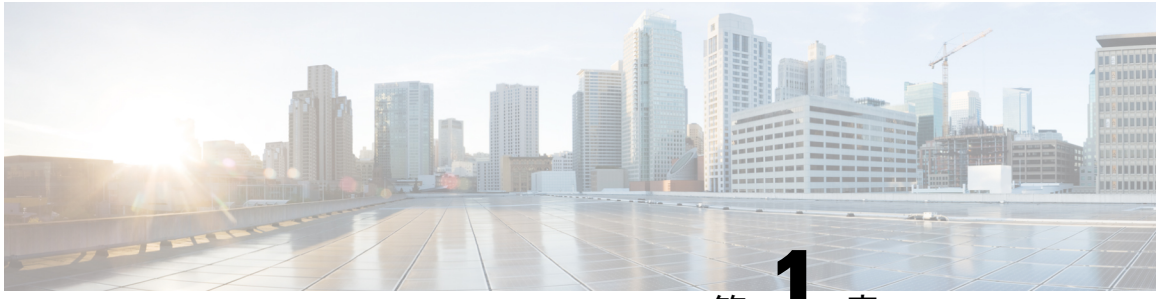
第 21 章
ポート単位のトラフィック制御の設定 483
ポートベースのトラフィック制御の概要 483
ストーム制御に関する情報 483
ストーム制御 483
トラフィック アクティビティの測定方法 484
トラフィック パターン 484
ストーム制御の設定方法 485
ストーム制御およびしきい値レベルの設定 485
保護ポートに関する情報 489
保護ポート 489
保護ポートのデフォルト設定 489
保護ポートのガイドライン 489
保護ポートの設定方法 490
保護ポートの設定 490
保護ポートの監視 491
ポート ブロッキングに関する情報 491
ポート ブロッキング 491
ポート ブロッキングの設定方法 492
インターフェイスでのフラッディング トラフィックのブロッキング 492
ポート ブロッキングの監視 493
ポート セキュリティの前提条件 494
ポート セキュリティの制約事項 494
ポート セキュリティの概要 494
ポート セキュリティ 494

セキュア MAC アドレスのタイプ 494
スティッキ セキュア MAC アドレス 495
セキュリティ違反 495
ポート セキュリティ エージング 497
ポート セキュリティとスイッチ スタック 497
デフォルトのポート セキュリティ設定 497
ポート セキュリティの設定時の注意事項 498
ポートベースのトラフィック制御の概要 499
ポート セキュリティの設定方法 500
ポート セキュリティの設定例 508
プロトコル ストーム プロテクションに関する情報 509
プロトコル ストーム プロテクション 509
デフォルトのプロトコル ストーム プロテクションの設定 510
プロトコル ストーム プロテクションの設定方法 510
プロトコル ストーム プロテクションのイネーブル化 510
プロトコル ストーム プロテクションのモニタリング 511
ポートベースのトラフィック制御に関するその他の関連資料 511

第 22 章 **Cisco TrustSec の設定** 513
Cisco TrustSec の概要 513
Cisco TrustSec の機能 513
Cisco TrustSec の機能情報 517

第 23 章 **コントロール プレーン ポリシングの設定** 519
CoPP の制約事項 519
CoPP の概要 520
CoPP の概要 520
システム定義の CoPP の特徴 521
ユーザ設定可能な CoPP の特徴 522
ソフトウェアバージョンのアップグレードまたはダウングレード 524
ソフトウェアバージョンのアップグレードと CoPP 524

ソフトウェアバージョンのダウングレードと CoPP 525
CoPP の設定方法 525
CPU キューの有効化またはポリサー レートの変更 525
CPU キューの無効化 527
すべての CPU キューに対するデフォルトのポリサー レートの設定 528
ユーザ定義のクラスマップの作成 529
CoPP の設定例 530
例：CPU キューの有効化または CPU キューのポリサー レートの変更 530
例：CPU キューの無効化 531
例：すべての CPU キューに対するデフォルトのポリサー レートの設定 532
例：ユーザ定義のクラスマップの作成 534
CoPP のモニタリング 536
CoPP の機能履歴と情報 536



第 1 章

# 不正アクセスの防止


- 機能情報の確認 （1 ページ）
- 不正アクセスの防止 （1 ページ）


## 機能情報の確認

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

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

## 不正アクセスの防止

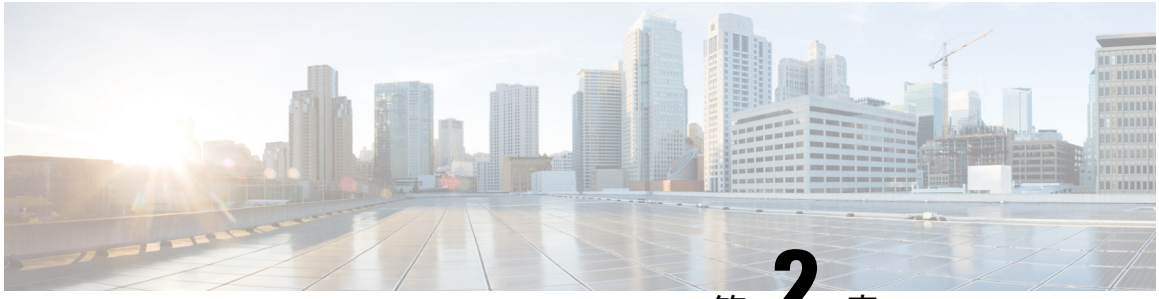
不正ユーザによる、スイッチの再設定や設定情報の閲覧を防止できます。一般的には、ネットワーク管理者からスイッチへのアクセスを許可する一方、非同期ポートを用いてネットワーク外からダイヤルアップ接続するユーザや、シリアル ポートを通じてネットワーク外から接続するユーザ、またはローカル ネットワーク内の端末またはワークステーションから接続するユーザによるアクセスを制限します。

スイッチへの不正アクセスを防止するには、次のセキュリティ機能を 1 つまたは複数設定します。

- 最低限のセキュリティとして、各スイッチ ポートでパスワードおよび権限を設定します。このパスワードは、スイッチにローカルに保存されます。ユーザがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。
- 追加のセキュリティ レイヤとして、ユーザ名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。このペアは回線またはポートに割り当てられ、

各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

- ユーザ名とパスワードのペアを使用したいが、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティ サーバ上のデータベースに保存できます。これにより、複数のネットワーキング デバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。
- また、失敗したログイン試行をログに記録するログイン拡張機能もイネーブルにすることもできます。ログイン拡張は、設定した回数のログインが失敗したあとに、それ以降のログイン試行をブロックするために設定することもできます。詳細については、『Cisco IOS Login Enhancements』マニュアルを参照してください。



第 2 章

# パスワードおよび権限レベルによるスイッチ アクセスの制御


- パスワードおよび権限によるスイッチ アクセスの制御の制約事項 （3 ページ）
- パスワードおよび権限レベルに関する情報 （3 ページ）
- パスワードおよび権限レベルでスイッチ アクセスを制御する方法 （6 ページ）
- スイッチ アクセスのモニタリング （18 ページ）
- パスワードおよび権限レベルの設定例 （18 ページ）
- その他の参考資料 （19 ページ）


## パスワードおよび権限によるスイッチアクセスの制御の制約事項

パスワードおよび権限によるスイッチ アクセスの制御の制約事項は、次のとおりです。

- **boot manual** グローバル コンフィギュレーション コマンドを使用して、スイッチを手動で起動するように設定している場合は、パスワード回復をディセーブルにできません。このコマンドは、スイッチの電源の再投入後、ブートローダ プロンプト（*switch:*）を表示させます。

## パスワードおよび権限レベルに関する情報

### デフォルトのパスワードおよび権限レベル設定

ネットワークで端末のアクセス コントロールを行う簡単な方法は、パスワードを使用して権限レベルを割り当てることです。パスワード保護によって、ネットワークまたはネットワーク デバイスへのアクセスが制限されます。権限レベルによって、ネットワーク デバイスにログイン後、ユーザがどのようなコマンドを使用できるかが定義されます。

次の表に、デフォルトのパスワードおよび権限レベル設定を示します。

表 *1:* デフォルトのパスワードおよび権限レベル設定

| 機能 | デフォルト設定 |
|---|---|
| イネーブルパスワードおよび権限レベル | パスワードは定義されていません。デフォルトはレベル 15 です（特権 EXEC レベル）。パスワードは、コンフィギュレーション ファイル内では暗号化されていない状態です。 |
| イネーブル シークレット パスワードおよび権限レベル | パスワードは定義されていません。デフォルトはレベル 15 です（特権 EXEC レベル）。パスワードは、暗号化されてからコンフィギュレーション ファイルに書き込まれます。 |
| 回線パスワード | パスワードは定義されていません。 |

# 追加のパスワード セキュリティ

セキュリティレベルを強化するために、特にネットワークを超えるパスワードや Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバに保存されたパスワードについて、グローバル コンフィギュレーション コマンド **enable password** または **enable secret** を使用できます。コマンドの作用はどちらも同じです。このコマンドにより、暗号化されたパスワードを設定できます。特権 EXEC モード（デフォルト設定）または特定の権限レベルにアクセスするユーザは、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムが使用されるので、**enable secret** コマンドを使用することを推奨します。

**enable secret** コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

パスワードの暗号化をイネーブルにすると、ユーザ名パスワード、認証キー パスワード、イネーブル コマンド パスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

# パスワードの回復

スイッチに物理的にアクセスできるエンドユーザは、デフォルトで、スイッチの電源投入時にブートプロセスに割り込み、新しいパスワードを入力することによって、失われたパスワードを回復できます。

パスワード回復ディセーブル化機能では、この機能の一部をディセーブルにすることによりスイッチのパスワードへのアクセスを保護できます。この機能がイネーブルの場合、エンドユーザは、システムをデフォルト設定に戻すことに同意した場合に限り、ブートプロセスに割り込むことができます。パスワード回復をディセーブルにしても、ブートプロセスに割り込んでパスワードを変更できますが、コンフィギュレーション ファイル（config.text）および VLAN データベース ファイル（vlan.dat）は削除されます。

パスワード回復をディセーブルにする場合は、エンド ユーザがブート プロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。VTP（VLAN トランキング プロトコル）トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

パスワードの回復を再びイネーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。

# 端末回線の Telnet 設定

初めてスイッチに電源を投入すると、自動セットアップ プログラムが起動して IP 情報を割り当て、この後続けて使用できるようにデフォルト設定を作成します。さらに、セットアップ プログラムは、パスワードによる Telnet アクセス用にスイッチを設定することを要求します。セットアップ プログラムの実行中にこのパスワードを設定しなかった場合は、端末回線に対する Telnet パスワードを設定するときに設定できます。

# ユーザ名とパスワードのペア

ユーザ名とパスワードのペアを設定できます。このペアはスイッチ上でローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

# 権限レベル

シスコデバイスでは、権限レベルを使用して、スイッチ動作の異なるレベルに対してパスワード セキュリティを提供します。デフォルトでは、Cisco IOS ソフトウェアは、パスワード セキュリティの 2 つのモード（権限レベル）で動作します。ユーザ EXEC（レベル 1）および特権 EXEC（レベル 15）です。各モードに、最大 16 個の階層レベルからなるコマンドを設定できます。複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

### 回線の権限レベル

ユーザは、回線にログインし、別の権限レベルを有効に設定することにより、**privilege level** ライン コンフィギュレーション コマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっていれば、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

たとえば、多くのユーザに**clear line**コマンドへのアクセスを許可する場合、レベル2のセキュリティを割り当て、レベル2のパスワードを広範囲のユーザに配布できます。また、**configure**コマンドへのアクセス制限を強化する場合は、レベル3のセキュリティを割り当て、そのパスワードを限られたユーザグループに配布することもできます。

### コマンド権限レベル

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。たとえば、**show ip traffic** コマンドをレベル 15 に設定すると、**show** コマンドと **show ip** コマンドは、異なるレベルに個別に設定しない限り、権限レベルは自動的に 15 に設定されます。

# パスワードおよび権限レベルでスイッチアクセスを制御する方法

## スタティック 有効 パスワードの設定または変更

イネーブルパスワードは、特権EXECモードへのアクセスを制御します。スタティックイネーブル パスワードを設定または変更するには、次の手順を実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **enable password** *password*<br>例：<br>デバイス(config)# **enable password secret321** | 特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。<br>デフォルトでは、パスワードは定義されません。<br>*password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符（?）は、パスワードを作成する場合に、疑問符の前に Ctrl+v を入力すれば使用できます。たとえば、パスワード abc?123 を作成するときは、次のようにします。<br>**1.** **abc** を入力します。<br>**2.** Ctrl+v を入力します。<br>**3.** **?123** を入力します。<br>システムからイネーブル パスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。 |
| ステップ 4 | **end**<br>例：<br>`デバイス(config)# end` | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config**<br>例：<br>`デバイス# show running-config` | 入力を確認します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>`デバイス# copy running-config startup-config` | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# 暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

特権EXECモード（デフォルト）または指定された特権レベルにアクセスするためにユーザが入力する必要がある暗号化パスワードを確立するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | 次のいずれかを使用します。<br>• `enable password [level` *level*`]` {*password encryption-type encrypted-password*}<br>• `enable secret [level` *level*`]` {*password encryption-type encrypted-password*}<br>例：<br>デバイス(config)# **enable password example102**<br>または<br>デバイス(config)# **enable secret level 1 password secret123sample** | • 特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。<br>• シークレット パスワードを定義します。これは非可逆的な暗号化方式を使用して保存されます。<br>• （任意）*level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です（特権 EXEC モード権限）。<br>• *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。<br>• （任意）*encryption-type* には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか使用できません。暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 別のスイッチの設定からコピーします。<br>（注） 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。 |
| ステップ 4 | **service password-encryption**<br>例：<br>デバイス(config)# **service password-encryption** | （任意）パスワードの定義時または設定の書き込み時に、パスワードを暗号化します。<br>暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# パスワード回復のディセーブル化

パスワードの回復をディセーブルにしてスイッチのセキュリティを保護するには、次の手順を実行します。

### 始める前に

パスワード回復をディセーブルにする場合は、エンド ユーザがブート プロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。VTP（VLAN トランキング プロトコル）トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **system disable password recovery switch** {*all* \| <*1-9*>}<br>例：<br>デバイス(config)# **system disable password recovery switch all** | パスワード回復をディセーブルにします。<br>• *all*：スタック内のスイッチで設定を行います。<br>• <*1-9*>：選択したスイッチ番号で設定を行います。<br>この設定は、フラッシュ メモリの中で、ブートローダおよび Cisco IOS イメージがアクセスできる領域に保存されますが、ファイル システムには含まれません。また、ユーザがアクセスすることはできません。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

### 次のタスク

**disable password recovery** を削除するには、**no system disable password recovery switch all** グローバル コンフィギュレーション コマンドを使用します。

## 端末回線に対する Telnet パスワードの設定

接続された端末回線に対する Telnet パスワードを設定するには、ユーザ EXEC モードで次の手順を実行します。

### 始める前に

- エミュレーション ソフトウェアを備えた PC またはワークステーションをスイッチ コンソール ポートに接続するか、または PC をイーサネット管理ポートに接続します。
- コンソール ポートのデフォルトのデータ特性は、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなしです。コマンドラインプロンプトが表示されるまで、Return キーを何回か押す必要があります。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | （注） パスワードが特権 EXEC モードへのアクセスに必要な場合は、その入力が求められます。<br>特権 EXEC モードを開始します。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **line vty 0 15**<br>例：<br>デバイス(config)# **line vty 0 15** | Telnet セッション（回線）の数を設定し、ライン コンフィギュレーション モードを開始します。<br>コマンド対応デバイスでは、最大 16 のセッションが可能です。0 および 15 を指定すると、使用できる 16 の Telnet セッションすべてを設定することになります。 |
| ステップ 4 | **password** *password*<br>例：<br>デバイス(config-line)# **password abcxyz543** | 1 つまたは複数の回線に対応する Telnet パスワードを設定します。<br>*password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config-line)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# ユーザ名とパスワードのペアの設定

ユーザ名とパスワードのペアを設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **username** *name* [ **privilege** *level*] { **password** *encryption-type password*}<br>例：<br>デバイス(config)# **username adamsample privilege 1 password secret456**<br>デバイス(config)# **username 111111111111 mac attribute** | 各ユーザのユーザ名、権限レベル、パスワードを設定します。<br>• *name* には、ユーザ ID を 1 ワードで指定するか、または MAC アドレスを指定します。スペースと引用符は使用できません。<br>• ユーザ名と MAC フィルタの両方に対し、最大 12000 のクライアントを個別に設定できます。<br>• （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。<br>• *encryption-type* には、暗号化されていないパスワードが後ろに続く場合は 0 を入力します。暗号化されたパスワードが後ろに続く場合は 7 を指定します。<br>• *password* には、デバイスへアクセスするためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | 次のいずれかを使用します。<br>• **line console 0**<br>• **line vty 0 15**<br>例：<br>デバイス(config)# **line console 0**<br>または<br>デバイス(config)# **line vty 15** | ライン コンフィギュレーション モードを開始し、コンソールポート（回線0）またはVTY 回線（回線 0 ～ 15）を設定します。 |
| ステップ 5 | **login local**<br>例：<br>デバイス(config-line)# **login local** | ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 3 で指定されたユーザ名に基づきます。 |
| ステップ 6 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 8 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# コマンドの特権レベルの設定

コマンドの権限レベルを設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例： | 特権 EXEC モードを有効にします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス> **enable** | • パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **privilege** *mode* **level** *level command*<br>例：<br>デバイス(config)# **privilege exec level 14 configure** | コマンドの特権レベルを設定します。<br>• *mode* には、グローバル コンフィギュレーション モードの場合は **configure** を、EXEC モードの場合は **exec** を、インターフェイス コンフィギュレーション モードの場合は **interface** を、ライン コンフィギュレーション モードの場合は **line** をそれぞれ入力します。<br>• *level* の範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。<br>• *command* には、アクセスを制限したいコマンドを指定します。 |
| ステップ 4 | **enable password level** *level password*<br>例：<br>デバイス(config)# **enable password level 14 SecretPswd14** | 権限レベルをイネーブルにするためのパスワードを指定します。<br>• *level* の範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。<br>• *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。 |

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

# 回線のデフォルト特権レベルの変更

指定した回線のデフォルトの権限レベルを変更するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **line vty** *line*<br>例：<br>デバイス(config)# **line vty 10** | アクセスを制限する仮想端末回線を選択します。 |
| ステップ 4 | **privilege level** *level*<br>例：<br>デバイス(config)# **privilege level 15** | 回線のデフォルト特権レベルを変更します。<br>*level* の範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。 |

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

### 次のタスク

ユーザは、回線にログインし、別の権限レベルを有効に設定することにより、**privilege level** ライン コンフィギュレーション コマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっていれば、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

## 権限レベルへのログインおよび終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、ユーザ EXEC モードで次の手順を実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable** *level*<br>例：<br>デバイス> **enable 15** | 指定された特権レベルにログインします。<br>この例で、レベル 15 は特権 EXEC モードです。<br>*level* に指定できる範囲は 0 ～ 15 です。 |
| ステップ 2 | **disable** *level*<br>例：<br>デバイス# **disable 1** | 指定した特権レベルを終了します。<br>この例で、レベル 1 はユーザ EXEC モードです。<br>*level* に指定できる範囲は 0 ～ 15 です。 |

# スイッチ アクセスのモニタリング

表 *2: DHCP* 情報を表示するためのコマンド

| | |
|---|---|
| **show privilege** | 権限レベルの設定を表示します。 |

# パスワードおよび権限レベルの設定例

## 例：スタティック イネーブル パスワードの設定または変更

次に、イネーブル パスワードを*l1u2c3k4y5* に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モード アクセス）。

```
デバイス(config)# enable password l1u2c3k4y5
```

## 例：暗号化によるイネーブルおよびイネーブルシークレットパスワードの保護

次に、権限レベル 2 に対して暗号化パスワード *$1$FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

```
デバイス(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

## 例：端末回線に対する Telnet パスワードの設定

次に、Telnet パスワードを *let45me67in89* に設定する例を示します。

```
デバイス(config)# line vty 10
デバイス(config-line)# password let45me67in89
```

## 例：コマンドの権限レベルの設定

ここで、**configure** コマンドを権限レベル 14 に設定する方法、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして *SecretPswd14* を定義する方法を示します。

```
デバイス(config)# privilege exec level 14 configure
デバイス(config)# enable password level 14 SecretPswd14
```

# その他の参考資料

### エラー メッセージ デコーダ

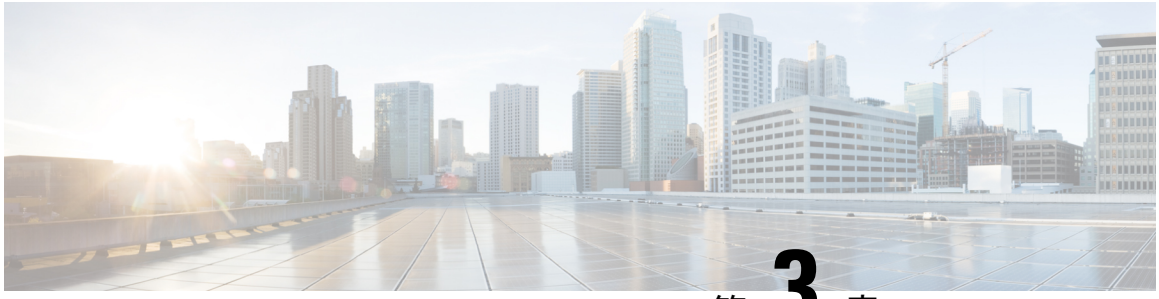
| 説明 | リンク |
|---|---|
| このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。 | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### MIB

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

### シスコのテクニカル サポート

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



第 3 章

# TACACS+ の設定


- TACACS+ の前提条件 （21 ページ）
- TACACS+ によるスイッチ アクセスの制御について （22 ページ）
- TACACS+ とスイッチ アクセスを設定する方法 （26 ページ）
- TACACS+ のモニタリング （34 ページ）
- TACACS+ によるスイッチ アクセスの制御に関するその他の参考資料 （35 ページ）
- TACACS+ によるスイッチアクセスの機能情報 （35 ページ）


## TACACS+ の前提条件

TACACS+によるスイッチアクセスのセットアップと設定の前提条件は、次のとおりです（示されている順序で実行する必要があります）。

1. スイッチに TACACS+ サーバ アドレスとスイッチを設定します。
2. 認証キーを設定します。
3. TACACS+ サーバでステップ 2 からキーを設定します。
4. 認証、許可、アカウンティング（AAA）をイネーブルにする。
5. ログイン認証方式リストを作成します。
6. 端末回線にリストを適用します。
7. 認証およびアカウンティング方式のリストを作成します。

TACACS+ によるスイッチ アクセスの制御の前提条件は、次のとおりです。

- スイッチ上で TACACS+ 機能を設定するには、設定済みの TACACS+ サーバにアクセスする必要があります。また、通常 LINUX または Windows ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されている TACACS+ サービスにもアクセスする必要があります。
- スイッチスタックと TACACS+ サーバとの間に冗長接続を設定することを推奨します。これによって、接続済みのスタック メンバの 1 つがスイッチ スタックから削除された場合でも、TACACS+ サーバにアクセスできます。

- スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼働するシステムが必要です。
- TACACS+ を使用するには、それをイネーブルにする必要があります。
- 許可は、使用するスイッチでイネーブルにする必要があります。
- ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
- このセクションに記載されている AAA コマンドのいずれかを使用するには、まず **aaa new-model** コマンドを使用して AAA をイネーブルにする必要があります。
- 最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウンティングの方式リストを定義できます。
- 方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。
- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。

# TACACS+ によるスイッチ アクセスの制御について

## TACACS+ およびスイッチ アクセス

ここでは、TACACS+ について説明します。TACACS+ は詳細なアカウンティング情報を提供し、認証と許可のプロセスを柔軟に管理します。TACACS+ は、認証、許可、アカウンティング（AAA）機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用する必要があります。

## TACACS+ の概要

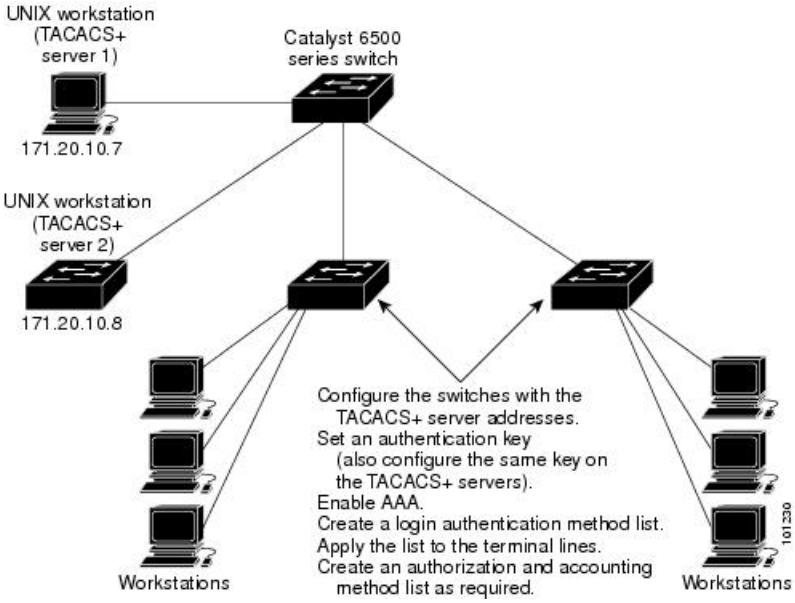
TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）が各サービス（認証、許可、およびアカウンティング）を別個に提供します。各サービスを固有のデータ

ベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ の目的は、1 つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他の Cisco ルータやアクセス サーバとともにネットワーク アクセス サーバにできます。

**図 *1 :* 一般的な *TACACS+* ネットワーク構成**




TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワードダイアログ、チャレンジおよび応答、メッセージサポートによって認証の完全制御を行います。

  認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードが入力された後、自宅の住所、母親の旧姓、サービスタイプ、社会保険番号などのいくつかの質問をすることによりユーザを試します）。TACACS+認証サービスは、ユーザ画面にメッセージを送信することもできます。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。

- 許可：autocommand、アクセス コントロール、セッション期間、プロトコル サポートの設定といった、ユーザ セッション時のユーザ機能についてきめ細かく制御します。また、TACACS+ 許可機能によって、ユーザが実行できるコマンドを制限することもできます。

- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+プロトコルは、スイッチとTACACS+デーモン間の認証を行い、スイッチとTACACS+デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

# TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1. 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これをユーザに表示します。ユーザがユーザ名を入力すると、スイッチはTACACS+デーモンに接続してパスワード プロンプトを取得します。スイッチによってパスワード プロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

   TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。

   - ACCEPT：ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
   - REJECT：ユーザは認証されません。TACACS+デーモンに応じて、ユーザはアクセスを拒否されるか、ログイン シーケンスを再試行するように求められます。
   - ERROR：デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
   - CONTINUE：ユーザは、さらに認証情報の入力を求められます。

   認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛ての属性の形式でデータが含まれています。

   - Telnet、セキュア シェル（SSH）、rlogin、または特権 EXEC サービス
   - 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

# 方式リスト

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティプロトコルを1つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

VTY 回線で方式リストを設定する場合、対応する方式リストを AAA に追加する必要があります。次の例は、VTY 回線の下に方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config)# authorization commands 15 auth1
```

次の例は、AAA で方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 auth1 group tacacs+
```

VTY 回線で方式リストを設定しない場合、デフォルトの方式リストを AAA に追加する必要があります。次の例は、方式リストを使用しない VTY 設定を示しています。

```
Device# configure terminal
Device(config)# line vty 0 4
```

次の例は、デフォルトの方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 default group tacacs+
```

# TACACS+ 設定オプション

認証用に1つのサーバを使用することも、また、既存のサーバ ホストをグループ化するために AAA サーバ グループを使用するように設定することもできます。サーバをグループ化して設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバ グループは、グローバル サーバ ホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストが含まれています。

# TACACS+ ログイン認証

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する1つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功す

るか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

## 特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

## TACACS+ Accounting

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

## TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

（注） TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

# TACACS+ とスイッチ アクセスを設定する方法

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。

## TACACS+ サーバ ホストの指定および認証キーの設定

TACACS+ サーバ ホストを特定し、認証キーを設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **tacacs server** *server-name*<br>例：<br>デバイス(config)# **tacacs server yourserver** | TACACS+ サーバを維持する IP ホストを特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。<br>*server-name* にはサーバ名を指定します。 |
| ステップ 4 | **address** {**ipv4** \| **ipv6**} *ip address*<br>例：<br>デバイス(config-server-tacacs)# **address ipv4 10.0.1.12** | TACACS サーバの IP アドレスを設定します。 |
| ステップ 5 | **exit**<br>例：<br>デバイス(config-server-tacacs)# **exit** | TACACS サーバモードを終了して、グローバル コンフィギュレーション モードを開始します。 |
| ステップ 6 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 7 | **aaa group server tacacs+** *group-name*<br>例：<br>デバイス(config)# **aaa group server tacacs+ your_server_group** | （任意）グループ名で AAA サーバグループを定義します。<br>このコマンドによって、デバイス をサーバ グループ サブコンフィギュレーション モードにします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 8 | **server** *ip-address*<br>例：<br>デバイス(config)# **server 10.1.2.3** | （任意）特定の TACACS+ サーバを定義済みサーバ グループに関連付けます。AAA サーバ グループの TACACS+ サーバごとに、このステップを繰り返します。<br>グループの各サーバは、ステップ 3 で定義済みのものでなければなりません。 |
| ステップ 9 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 10 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 11 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

# TACACS+ ログイン認証の設定

TACACS+ ログイン認証を設定するには、次の手順を実行します。

### 始める前に

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。

（注） AAA 方式を使用して HTTP アクセスに対しのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しのセキュリティは確保しません。

**ip http authentication** コマンドの詳細については、『*Cisco IOS Security Command Reference, Release 12.4*』を参照してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 4 | **aaa authentication login** {**default** \| *list-name*} *method1* [*method2...* ]<br>例：<br>デバイス(config)# **aaa authentication login default tacacs+ local** | ログイン認証方式リストを作成します。<br>• **login authentication** コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。<br>• *list-name* には、作成するリストの名前として使用する文字列を指定します。<br>• *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。<br>次のいずれかの方式を選択します。<br>• *enable*：イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ **enable** |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | *password* グローバル コンフィギュレーション コマンドを使用してイネーブルパスワードを定義しておく必要があります。<br>• *group tacacs+*：TACACS+ 認証を使用します。この認証方式を使用するには、あらかじめ TACACS+ サーバを設定しておく必要があります。<br>• *line*：回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。<br>• *local*：ローカルユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。<br>• *local-case*：大文字と小文字が区別されるローカルユーザ名データベースを認証に使用します。**username** *name* **password** グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。<br>• *none*：ログインに認証を使用しません。 |
| ステップ 5 | **line** [**console** \| **tty** \| **vty**] *line-number* [*ending-line-number*]<br>例：<br>デバイス(config)# **line 2 4** | ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。 |
| ステップ 6 | **login authentication** {**default** \| *list-name*}<br>例： | 1 つの回線または複数回線に認証リストを適用します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-line)# **login authentication default** | • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。<br>• *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。 |
| ステップ 7 | **end**<br>例：<br>デバイス(config-line)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 9 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# 特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

**aaa authorization** グローバル コンフィギュレーション コマンドと **tacacs+** キーワードを使用すると、ユーザのネットワークアクセスを特権EXECモードに制限するパラメータを設定できます。

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa authorization network tacacs+**<br>例：<br>デバイス(config)# **aaa authorization network tacacs+** | ネットワーク関連のすべてのサービス要求に対してユーザ TACACS+認可を行うことを設定します。 |
| ステップ 4 | **aaa authorization exec tacacs+**<br>例：<br>デバイス(config)# **aaa authorization exec tacacs+** | ユーザの特権 EXEC アクセスに対してユーザ TACACS+許可を行うことを設定します。<br>**exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# TACACS+ アカウンティングの起動

TACACS+ アカウンティングを開始するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa accounting network start-stop tacacs+**<br>例：<br>デバイス(config)# **aaa accounting network start-stop tacacs+** | ネットワーク関連のすべてのサービス要求について、TACACS+アカウンティングをイネーブルにします。 |
| ステップ 4 | **aaa accounting exec start-stop tacacs+**<br>例：<br>デバイス(config)# **aaa accounting exec start-stop tacacs+** | TACACS+アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例： | （任意）コンフィギュレーション ファイルに設定を保存します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **copy running-config startup-config** | |

### 次のタスク

AAA サーバが到達不能な場合にルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合に、ルータとのコンソールセッションまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

## AAA サーバが到達不能な場合のルータとのセッションの確立

AAA サーバが到達不能な場合にルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合に、ルータとのコンソールセッションまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

# TACACS+ のモニタリング

表 *3 : TACACS+* 情報を表示するためのコマンド

| コマンド | 目的 |
|---|---|
| **show tacacs** | TACACS+ サーバの統計情報を表示します。 |

# TACACS+によるスイッチアクセスの制御に関するその他の参考資料

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| AAA の設定 | ローカル認証および許可の設定 |

### MIB

| MIB | MIB のリンク |
|---|---|
| | 選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

### シスコのテクニカル サポート

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

# TACACS+ によるスイッチアクセスの機能情報

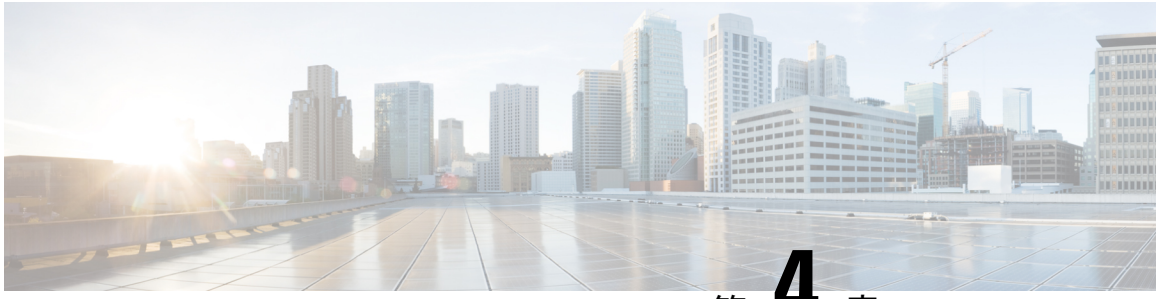
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *4 : TACACS+* によるスイッチアクセスの機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| TACACS+ のスイッチ アクセス | | TACACS+ は、認証および認可プロセスについて詳細なアカウンティング情報と柔軟な管理コントロールを提供します。TACACS+ は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。 |



第 4 章

# RADIUS の設定


- RADIUS を設定するための前提条件 （37 ページ）
- RADIUS の設定に関する制約事項 （38 ページ）
- RADIUS について （38 ページ）
- RADIUS の設定方法 （67 ページ）
- CoA 機能のモニタリング （83 ページ）


## RADIUS を設定するための前提条件

ここでは、RADIUS による デバイス アクセスの制御の前提条件を示します。

全般：

- この章のいずれかのコンフィギュレーション コマンドを使用するには、RADIUS および認証、許可、ならびにアカウンティング（AAA）をイネーブルにする必要があります。
- RADIUS は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。
- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。
- 最低限、RADIUS サーバ ソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS 認証の方式リストを定義する必要があります。また、任意で RADIUS 許可およびアカウンティングの方式リストを定義できます。
- デバイス 上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。
- RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソ

フトウェアが稼働しているマルチユーザ システムです。詳細については、RADIUS サーバのマニュアルを参照してください。

- Change-of-Authorization（CoA）インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。CoA を使用すると、セッションの識別と接続解除要求を実行できます。アップデートは、指定されたセッションにだけ作用します。
- スイッチ スタックと RADIUS サーバとの間に冗長接続を設定することを推奨します。これによって、接続済みのスタック メンバの 1 つがスイッチ スタックから削除された場合でも、RADIUS サーバにアクセスできます。

RADIUS 操作の場合：

- ユーザは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります（イネーブルに設定されている場合）。

# RADIUS の設定に関する制約事項

ここでは、RADIUS による デバイス アクセスの制御の制約事項について説明します。

全般：

- セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。

RADIUS は次のネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は、AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

# RADIUS について

## RADIUS およびスイッチ アクセス

この項では、RADIUS をイネーブルにし、設定する方法について説明します。RADIUS を使用すると、アカウンティングの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます。

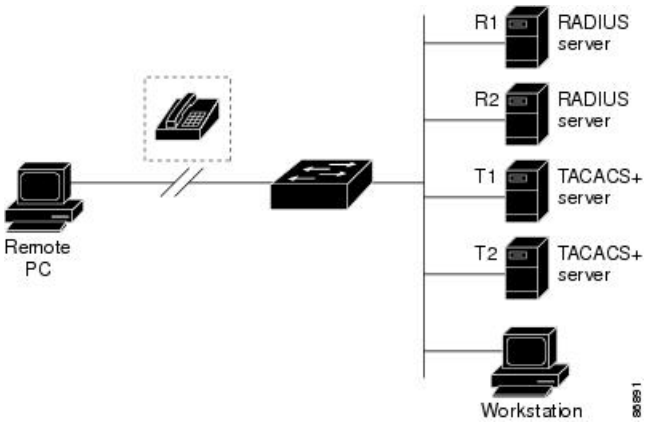
# RADIUS の概要

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。RADIUS クライアントは、サポート対象の Cisco ルータおよびスイッチ上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。

RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベースセキュリティ データベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルインユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カード アクセス コントロール システムを使用するアクセス環境。あるケースでは、RADIUS は Enigma のセキュリティ カードとともに使用してユーザを確認し、ネットワーク リソースのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。RADIUS クライアント装備のシスコ デバイスネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。下の図 「RADIUS サービスから TACACS+ サービスへの移行」を参照してください。
- ユーザが 1 つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1x などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、「*IEEE 802.1x* ポートベースの認証の設定」の章を参照してください。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェアバージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

図 *2 : RADIUS* サービスから *TACACS+* サービスへの移行




# RADIUS の動作

RADIUS サーバによってアクセスコントロールされる デバイス に、ユーザがログインおよび認証を試みると、次のイベントが発生します。

1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由でRADIUSサーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   - ACCEPT：ユーザが認証されたことを表します。
   - REJECT：ユーザの認証が失敗し、ユーザ名およびパスワードの再入力が要求されるか、またはアクセスが拒否されます。
   - CHALLENGE：ユーザに追加データを要求します。
   - CHALLENGE PASSWORD：ユーザは新しいパスワードを選択するように要求されます。

   ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ（ホストまたはクライアントのIPアドレス、アクセスリスト、およびユーザ タイムアウトを含む）

# RADIUS 許可の変更

RADIUS 許可の変更（CoA）は、認証、認可、およびアカウンティング（AAA）セッションの属性を認証された後に変更するためのメカニズムを提供します。AAA でユーザ、またはユーザ グループのポリシーが変更された場合、管理者は、AAA サーバから Cisco Secure Access Control Server（ACS）などの RADIUS CoA パケットを送信し、認証を再初期化して新しいポリシーを適用することができます。このセクションでは、使用可能なプリミティブおよびそれらの CoA での使用方法を含む、RADIUS インターフェイスの概要について説明します。

- Change-of-Authorization 要求
- CoA 要求応答コード
- CoA 要求コマンド
- セッション再認証
- セッション強制終了のスタック構成ガイドライン

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。Catalyst は、RFC 5176 で規定された（通常はプッシュモデルで使用される）RADIUS CoA 拡張機能をサポートし、外部の AAA またはポリシーサーバからのセッションを動的に再設定できるようにします。

は、次のセッション単位の CoA 要求をサポートしています。

- セッション再認証
- セッションの終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了

この機能は、Cisco Secure Access Control Server (ACS) 5.1 に統合されています。

Catalyst で、RADIUS インターフェイスはデフォルトでイネーブルに設定されています。ただし、次の属性については、一部の基本的な設定が必要になります。

- セキュリティおよびパスワード：このガイドの「スイッチへの不正アクセスの防止」を参照してください。
- アカウンティング：このガイドの「スイッチベース認証の設定」の章の「RADIUS アカウンティングの起動」の項を参照してください。

Cisco IOS ソフトウェアは、RFC 5176 で定義されている RADIUS CoA の拡張をサポートします。この拡張は、一般に、外部 AAA またはポリシー サーバからのセッションのダイナミックな再構成を可能にするプッシュ モデルで使用されます。セッションの特定、セッションの終了、ホストの再認証、ポートのシャットダウン、およびポート バウンスでは、セッションごとの CoA 要求がサポートされます。このモデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgement（ACK）[CoA-ACK]
- CoA nonacknowledgement（NAK）[CoA-NAK]

要求は CoA クライアント（通常は AAA またはポリシー サーバ）から開始されて、リスナーとして動作するデバイスに転送されます。

次の表は、Identity-Based Networking Services でサポートされている RADIUS CoA コマンドとベンダー固有属性（VSA）を示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

**表 5 : *Identity-Based Networking Services* でサポートされている *RADIUS CoA* コマンド**

| CoA コマンド | シスコの VSA |
|---|---|
| Activate service | Cisco:Avpair=“subscriber:command=activate-service”<br>Cisco:Avpair=“subscriber:service-name=<*service-name*>”<br>Cisco:Avpair=“subscriber:precedence=<*precedence-number*>”<br>Cisco:Avpair=“subscriber:activation-mode=replace-all” |
| Deactivate service | Cisco:Avpair=“subscriber:command=deactivate-service”<br>Cisco:Avpair=“subscriber:service-name=<*service-name*>” |
| Bounce host port | Cisco:Avpair="subscriber:command=bounce-host-port" |
| Disable host port | Cisco:Avpair="subscriber:command=disable-host-port" |
| Session query | Cisco:Avpair=“subscriber:command=session-query” |
| Session reauthenticate | Cisco:Avpair="subscriber:command=reauthenticate"<br>Cisco:Avpair=“subscriber:reauthenticate-type=last” または<br>Cisco:Avpair=“subscriber:reauthenticate-type=rerun” |
| Session terminate | これは、VSA を必要としない、標準の接続解除要求です。 |
| Interface template | Cisco:AVpair="interface-template-name=<*interfacetemplate*>" |

## Change-of-Authorization 要求

Change of Authorization（CoA）要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。このモデルは、1 つの要求（CoA-Request）と 2 つの可能な応答コードで構成されています。

- CoA acknowledgment（ACK）[CoA-ACK]
- CoA non-acknowledgment（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から発信されて、リスナーとして動作するスイッチに送信されます。

## RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してスイッチでサポートされています。

次の表に、この機能でサポートされている IETF 属性を示します。

**表 *6 :* サポートされている *IETF* 属性**

| 属性番号 | 属性名 |
|---|---|
| 24 | 状態 |
| 31 | Calling-Station-ID |
| 44 | Acct-Session-ID |
| 80 | Message-Authenticator |
| 101 | Error-Cause |

次の表に、Error-Cause 属性で取ることができる値を示します。

**表 *7 : Error-Cause* の値**

| 値 | 説明 |
|---|---|
| 201 | 削除された残留セッション コンテキスト |
| 202 | 無効な EAP パケット（無視） |
| 401 | サポートされていない属性 |
| 402 | 見つからない属性 |
| 403 | NAS 識別情報のミスマッチ |
| 404 | 無効な要求 |
| 405 | サポートされていないサービス |
| 406 | サポートされていない拡張機能 |
| 407 | 無効な属性値 |
| 501 | 管理上の禁止 |
| 502 | ルート不可能な要求（プロキシ） |

| 値 | 説明 |
|---|---|
| 503 | セッション コンテキストが検出されない |
| 504 | セッション コンテキストが削除できない |
| 505 | その他のプロキシ処理エラー |
| 506 | リソースが使用不可能 |
| 507 | 要求が発信された |
| 508 | マルチ セッションの選択がサポートされてない |

## CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。属性フィールドは、シスコのベンダー固有属性（VSA）を送信するために使用します。

### セッションの識別

特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id VSA（シスコの VSA）
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）
- 次のいずれかの IPv6 属性。
  - Framed-IPv6-Prefix（IETF 属性 #97）および Framed-Interface-Id（IETF 属性 #96）。ともに RFC 3162 に従った完全な IPv6 アドレスを作成する
  - Framed-IPv6-Address
- プレーン IP アドレス（IETF 属性 #8）

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、スイッチは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

複数のセッション ID 属性がメッセージ含まれる場合は、すべての属性がセッションと一致しなければなりません。そうでない場合は、スイッチが Disconnect - negative acknowledgement（NAK）または CoA -NAK と、「Invalid Attribute Value」エラー コードを返します。

RFC 5176 で定義されている CoA 要求コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                         Authenticator                         |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

属性フィールドは、シスコのベンダー固有属性（VSA）を送信するために使用します。

特定の適用ポリシーを対象とする CoA 要求の場合、上記のセッション ID 属性のいずれかがメッセージに含まれていると、デバイスはエラー コードが「Invalid Attribute Value」の CoA-NAK を返します。

### CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なり、個々の CoA コマンドで検討されます。

### CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。CoA が成功したかを確認するには、**show** コマンドを使用します。

## CoA 要求コマンド

表 *8 :* でサポートされる *CoA* コマンド

| コマンド [1] | シスコの VSA |
|---|---|
| Reauthenticate host | Cisco:Avpair="subscriber:command=reauthenticate" |
| Terminate session | これは、VSA を要求しない、標準の接続解除要求です。 |
| Bounce host port | Cisco:Avpair="subscriber:command=bounce-host-port" |
| Disable host port | Cisco:Avpair="subscriber:command=disable-host-port" |

[1] すべての CoA コマンドには、と CoA クライアント間のセッション識別情報が含まれている必要があります。

### セッション再認証

不明な ID またはポスチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファイル（たとえば、ゲスト VLAN）に関連付けられると、AAA サーバは通常、セッショ

ン再認証要求を生成します。再認証要求は、クレデンシャルが不明である場合にホストが適切な認証グループに配置されることを許可します。

セッション認証を開始するために、AAA サーバは *Cisco:Avpair="subscriber:command=reauthenticate"* の形式で Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。

現在のセッション ステートは、メッセージに対するスイッチの応答を決定します。セッションが現在、IEEE 802.1x によって認証されている場合、スイッチは EAPOL（LAN 経由の拡張認証プロトコル）RequestId メッセージをサーバに送信することで応答します。

現在、セッションが MAC 認証バイパス（MAB）で認証されている場合は、スイッチはサーバにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

スイッチがコマンドを受信した際にセッション認証が実行中である場合は、スイッチはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションがまだ認証されてない、あるいはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認証されている場合は、再認証メッセージがアクセス コントロール方式を再開し、最初に試行されるように設定された方式で開始します。セッションの現在の許可は、再認証によって異なる認証結果になるまで維持されます。

## スイッチ スタックでのセッションの再認証

スイッチ スタックでセッション再認証メッセージを受信すると、次の動作が発生します。

- 確認応答（ACK）を戻す前に、再認証の必要性がチェックされます。
- 適切なセッションで再認証が開始されます。
- 認証が成功または失敗のいずれかで完了すると、再認証をトリガーする信号がスタック メンバから削除されます。
- 認証の完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、再認証が開始されます。
- ACK の送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再転送コマンドが新しいコマンドとして扱われます。

## セッションの終了

セッションを終了させる 3 種類の CoA 要求があります。CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。このコマンドを使用すると、指定されたホストのオーセンティケータ ステート マシンが再初期化されますが、そのホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA の設定で CoA 要求を使用します。このコマンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であり、そのホストに対してネットワーク アクセスをただちにブロックする必要があります。

ポートへのネットワーク アクセスを復旧する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

プリンタなどのサプリカントを持たないデバイスが新しい IP アドレスを取得する必要がある場合（たとえば、VLAN 変更後）は、ポート バウンスでホスト ポート上のセッションを終了します（ポートを一時的にディセーブルした後、再びイネーブルにする）。

## CoA 接続解除要求

このコマンドは標準の接続解除要求です。セッションが見つからない場合、スイッチは Disconnect-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。セッションがある場合は、スイッチはセッションを終了します。セッションが完全に削除された後、スイッチは接続解除 ACK を返します。

スイッチがクライアントに接続解除 ACK を返す前にスタンバイ スイッチにフェールオーバーする場合は、クライアントから要求が再送信される際に、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。再送信後もセッションが見つからない場合は、Disconnect-ACK と「Session Context Not Found」エラー コード属性が送信されます。

## CoA 要求：ホスト ポートのディセーブル化

RADIUS サーバの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元するには、非RADIUSメカニズムを使用して再びイネーブルにします。このコマンドは、次の新しいベンダー固有属性（VSA）が含まれている標準CoA要求メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチはCoA-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。このセッションがある場合は、スイッチはホスト ポートをディセーブルにし、CoA-ACK メッセージを返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信される際に、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

（注） 再送信コマンドの後に接続解除要求が失敗すると、（接続解除ACKが送信されてない場合に）チェンジオーバー前にセッションが正常終了し、または元のコマンドが実行されてスタンバイ スイッチがアクティブになるまでの間に発生した他の方法（たとえば、リンク障害）によりセッションが終了することがあります。

### CoA 要求：バウンス ポート

RADIUS サーバの CoA bounce port が RADIUS サーバから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチはCoA-NAKメッセージと「Session Context Not Found」エラー コード属性を返します。このセッションがある場合は、スイッチはホストポートを10秒間ディセーブルし、再びイネーブルにし（ポートバウンス）、CoA-ACK を返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信される際に、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

## セッション強制終了のスタック構成ガイドライン

スイッチ スタックでは、CoA 接続解除要求メッセージに必要な特別な処理はありません。

### CoA 要求バウンス ポートのスタック構成ガイドライン

**bounce-port** コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

スタックマスターで Auth Manager コマンドハンドラが有効な **bounce-port** コマンドを受信すると、CoA-ACK メッセージを返す前に次の情報が確認されます。

- ポート バウンスの必要性
- ポート ID（ローカル セッション コンテキストで検出された場合）

スイッチで、ポート バウンスが開始されます（ポートが 10 秒間ディセーブルになり、再びイネーブルにされます）。

ポート バウンスが正常に実行された場合、ポート バウンスをトリガーした信号がスタンバイ スタック マスターから削除されます。

ポート バウンスの完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、ポート バウンスが開始されます。

CoA-ACK メッセージの送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再送信コマンドが新しいコマンドとして扱われます。

### CoA 要求ディセーブル ポートのスタック構成ガイドライン

**disable-port** コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

スタックマスターで Auth Manager コマンドハンドラが有効な **disable-port** コマンドを受信すると、CoA-ACK メッセージを返す前に次の情報が確認されます。

- ポート ディセーブルの必要性
- ポート ID（ローカル セッション コンテキストで検出された場合）

スイッチで、ポートをディセーブルする操作が試行されます。

ポートをディセーブルする操作が正常に実行された場合、ポートをディセーブルする操作をトリガーした信号がスタンバイ スタック マスターから削除されます。

ポートをディセーブルする操作の完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、ポートがディセーブルにされます。

CoA-ACK メッセージの送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再送信コマンドが新しいコマンドとして扱われます。

## RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

## RADIUS サーバ ホスト

スイッチと RADIUS サーバの通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する

RADIUSホストとして個々のポートを定義できます。この一意のIDを使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じRADIUSサーバ上の異なる2つのホストエントリに同じサービス（たとえばアカウンティング）を設定した場合、2番めに設定したホストエントリは、最初に設定したホストエントリのフェールオーバー バックアップとして動作します。この例では、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、スイッチは「%RADIUS-4-RADIUS_DEAD」メッセージを表示し、その後、同じデバイス上で 2 番めに設定されたホスト エントリでアカウンティング サービスを試みます（RADIUS ホスト エントリは、設定した順序に従って試行されます）。

RADIUS サーバとスイッチは、共有するシークレット テキスト ストリングを使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUSサーバデーモンが稼働するホストと、そのホストがスイッチと共有するシークレット テキスト（キー）ストリングを指定する必要があります。

タイムアウト、再送信回数、および暗号キーの値は、すべてのRADIUSサーバに対してグローバルに設定することもできますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単位での設定を組み合わせることもできます。

# RADIUS ログイン認証

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外は、デフォルトの方式リストです。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する1つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

# AAA サーバグループ

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意の ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件で

す。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の異なる UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバ上の異なる 2 つのホストエントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エントリがアカウンティング サービスの提供に失敗すると、ネットワーク アクセス サーバは同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように試行します。（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

# AAA 許可

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可をイネーブルにすると、スイッチは（ローカル ユーザ データベースまたはセキュリティ サーバ上に存在する）ユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

# RADIUS アカウンティング

AAA アカウンティング機能は、ユーザが使用したサービスと、消費したネットワーク リソース量を追跡します。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で RADIUS セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。

# ベンダー固有の RADIUS 属性

Internet Engineering Task Force（IETF）ドラフト規格に、ベンダー固有の属性（属性 26）を使用して、スイッチと RADIUS サーバ間でベンダー固有の情報を通信するための方式が定められています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダータイプ 1（名前は *cisco-avpair*）です。この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

*protocol* は、特定の認証タイプに使用するシスコのプロトコル属性の値です。*attribute* および *value* は、シスコの TACACS+ 仕様で定義されている適切な属性値（AV）ペアです。*sep* は、必須の属性の場合は =、任意指定の属性の場合は * です。TACACS+ 認証で使用できるすべての機能は、RADIUS でも使用できます。

たとえば、次の AV ペアにより、IP 認証中（PPP の IPCP アドレス割り当て中）には、シスコの「multiple named IP address pools」機能がアクティブになります。

```
cisco-avpair= ”ip:addr-pool=first“
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」は省略可能になります。任意の AV ペアを省略可能にすることができます。

```
cisco-avpair= ”ip:addr-pool*first“
```

次に、ネットワーク アクセス サーバからユーザがログインしたときに、すぐに EXEC コマンドを実行する方法の例を示します。

```
cisco-avpair= ”shell:priv-lvl=15“
```

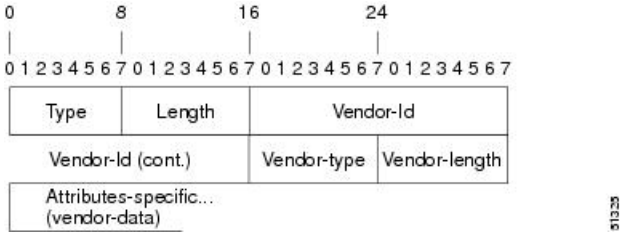
他のベンダーにも、それぞれ独自のベンダー ID、オプション、および対応する VSA があります。ベンダー ID および VSA の詳細については、RFC 2138『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

属性 26 には、次の 3 つの要素が含まれています。

- タイプ
- 長さ
- ストリング（またはデータ）
  - Vendor-Id
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

次の図は、属性 26 の「背後で」カプセル化される VSA のパケット形式を示します。

**図 *3*：属性 *26* の背後でカプセル化される *VSA***




（注） VSA の形式はベンダーが指定します。Attribute-Specific フィールド（Vendor-Data とも呼ばれる）は、ベンダーによるその属性の定義によって異なります。

次の表に、「ベンダー固有 RADIUS IETF 属性テーブル」（次の 2 番目の表）で表示される重要なフィールドを示します。これは、サポート対象のベンダー固有 RADIUS 属性（IETF 属性 26）を表示します。

表 *9*：ベンダー固有属性表のフィールドの説明

| フィールド | 説明 |
|---|---|
| 番号（Number） | 次の表に示されるすべての属性は、IETF 属性 26 の拡張です。 |
| ベンダー固有のコマンドコード | 特定のベンダーの識別に使用する定義されたコード。コード 9 は Cisco VSA、311 は Microsoft VSA、529 は Ascend VSA を定義します。 |
| サブタイプ番号 | 属性 ID 番号。この番号は、属性 26 の背後でカプセル化される「2 番めのレイヤ」の ID 番号であること以外、IETF 属性の ID 番号に似ています。 |
| 属性 | 属性の ASCII ストリング名。 |
| 説明 | 属性の説明。 |

表 *10*：ベンダー固有 *RADIUS IETF* 属性

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| MS-CHAP 属性 | | | | |
| 26 | 311 | 1 | MSCHAP-Response | PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでしか使用されません。この属性は、PPP CHAP ID と同じです（RFC 2548） |
| 26 | 311 | 11 | MSCHAP-Challenge | ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャレンジが含まれます。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。（RFC 2548） |
| VPDN 属性 | | | | |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 1 | l2tp-cm-local-window-size | L2TP 制御メッセージの最大受信ウィンドウ サイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。 |
| 26 | 9 | 1 | l2tp-drop-out-of-order | 正しくない順序で受信したデータ パケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データ パケット上でシーケンス番号が送信されるわけではありません。 |
| 26 | 9 | 1 | l2tp-hello-interval | hello キープアライブ インターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。 |
| 26 | 9 | 1 | l2tp-hidden-avp | イネーブルにすると、L2TP 制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。 |
| 26 | 9 | 1 | l2tp-nosession-timeout | タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。 |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 1 | tunnel-tos-reflect | LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロードパケットの IP ヘッダーからトンネルパケットの IP ヘッダーにコピーします。 |
| 26 | 9 | 1 | l2tp-tunnel-authen | この属性を設定すると、L2TP トンネル認証が実行されます。 |
| 26 | 9 | 1 | l2tp-tunnel-password | L2TP トンネル認証および AVP 隠蔽に使用される共有秘密。 |
| 26 | 9 | 1 | l2tp-udp-checksum | これは認可属性で、L2TP がデータ パケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」と「no」です。デフォルトは「no」です。 |
| Store and Forward Fax 属性 | | | | |
| 26 | 9 | 3 | Fax-Account-Id-Origin | **mmoip aaa receive-id** コマンドまたは **mmoip aaa send-id** コマンドについて、システム管理者によって定義されたものとしてアカウント ID の発信元を示します。 |
| 26 | 9 | 4 | Fax-Msg-Id= | Store and Forward Fax 機能によって割り当てられた一意のファクスメッセージ識別番号を示します。 |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 5 | Fax-Pages | このファクス セッション中に送信または受信したページ数を示します。このページ数には、カバー ページも含まれます。 |
| 26 | 9 | 6 | Fax-Coverpage-Flag | カバー ページがこのファクス セッションのオフランプ ゲートウェイで生成されたかどうかを示します。true はカバー ページが生成されたことを示します。false はカバー ページが生成されなかったことを意味します。 |
| 26 | 9 | 7 | Fax-Modem-Time | モデムがファクス データを送信した時間（x）、およびファクス セッションの合計時間（y）を秒単位で示します。これには、fax-mail および PSTN 時間が x/y の形式で含まれます。たとえば、10/15 は送信時間が 10 秒で、合計ファクス セッションが 15 秒であったことを示します。 |
| 26 | 9 | 8 | Fax-Connect-Speed | この fax-mail が最初に送信または受信された時点のモデム速度を示します。有効値は、1200、4800、9600、および 14400 です。 |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 9 | Fax-Recipient-Count | このファクス送信の受信者数を示します。E メール サーバがセッション モードをサポートするまで、この数字は 1 にする必要があります。 |
| 26 | 9 | 10 | Fax-Process-Abort-Flag | ファクス セッションが中断したこと、または正常に終了したことを示します。true はセッションが中断したことを示します。false はセッションが成功したことを示します。 |
| 26 | 9 | 11 | Fax-Dsn-Address | DSN の送信先のアドレスを示します。 |
| 26 | 9 | 12 | Fax-Dsn-Flag | DSN がイネーブルにされているかどうかを示します。true は DSN がイネーブルにされていることを示します。false は DSN がイネーブルにされていないことを示します。 |
| 26 | 9 | 13 | Fax-Mdn-Address | MDN の送信先のアドレスを示します。 |
| 26 | 9 | 14 | Fax-Mdn-Flag | メッセージ配信通知（MDN）がイネーブルにされているかどうかを示します。true は MDN がイネーブルにされていることを示します。false は MDN がイネーブルにされていないことを示します。 |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 15 | Fax-Auth-Status | このファクス セッションに対する認証が成功したかどうかを示します。このフィールドに対する有効値は、success、failed、bypassed、または unknown です。 |
| 26 | 9 | 16 | Email-Server-Address | オンランプ fax-mail メッセージを処理する E メール サーバの IP アドレスを示します。 |
| 26 | 9 | 17 | Email-Server-Ack-Flag | オンランプ ゲートウェイが fax-mail メッセージを受け入れる E メール サーバから肯定確認応答を受信したことを示します。 |
| 26 | 9 | 18 | Gateway-Id | ファクス セッションを処理したゲートウェイの名前を示します。名前は、hostname.domain-name という形式で表示されます。 |
| 26 | 9 | 19 | Call-Type | ファクスのアクティビティのタイプを、fax receive または fax send のどちらかで記述します。 |
| 26 | 9 | 20 | Port-Used | この fax-mail の送受信いずれかに使用される Cisco AS5300 のスロット/ポート番号を示します。 |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 21 | Abort-Cause | ファクス セッションが中断した場合、中断の信号を送信したシステム コンポーネントを示します。中断する可能性のあるシステム コンポーネントには、FAP（Fax Application Process）、TIFF（TIFF リーダーまたはTIFF ライター）、fax-mail クライアント、fax-mail サーバ、ESMTP クライアント、ESMTP サーバなどがあります。 |
| H323 属性 | | | | |
| 26 | 9 | 23 | Remote-Gateway-ID（h323-remote-address） | リモート ゲートウェイの IP アドレスを示します。 |
| 26 | 9 | 24 | Connection-ID（h323-conf-id） | 会議 ID を識別します。 |
| 26 | 9 | 25 | Setup-Time（h323-setup-time） | 以前、グリニッジ標準時（GMT）およびズール タイムと呼ばれていた協定世界時（UTC）でのこの接続のセットアップ時間を示します。 |
| 26 | 9 | 26 | Call-Origin（h323-call-origin） | ゲートウェイに対するコールの発行元を示します。有効値は、originating および terminating です（回答）。 |
| 26 | 9 | 27 | Call-Type（h323-call-type） | コールのレグ タイプを示します。使用可能な値は **telephony** と **VoIP** です。 |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 28 | Connect-Time（h323-connect-time） | このコール レッグの UTC での接続時間を示します。 |
| 26 | 9 | 29 | Disconnect-Time（h323-disconnect-time） | このコール レッグが UTC で接続解除された時間を示します。 |
| 26 | 9 | 30 | Disconnect-Cause（h323-disconnect-cause） | Q.931 仕様によって、接続がオフラインにされた理由を示します。 |
| 26 | 9 | 31 | Voice-Quality（h323-voice-quality） | コールの音声品質に影響する Impairment Factor（ICPIF）を指定します。 |
| 26 | 9 | 33 | Gateway-ID（h323-gw-id） | 下位のゲートウェイの名前を示します。 |
| 大規模のダイヤルアウト属性 | | | | |
| 26 | 9 | 1 | callback-dialstring | コールバックに使用するダイヤリング文字列を定義します。 |
| 26 | 9 | 1 | data-service | 説明はありません。 |
| 26 | 9 | 1 | dial-number | ダイヤルする番号を定義します。 |
| 26 | 9 | 1 | force-56 | チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。 |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 1 | map-class | ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップ クラスで設定される情報の参照を許可します。 |
| 26 | 9 | 1 | send-auth | CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。 |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 1 | send-name | |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| | | | | PPP 名前認証。PAP に適用する場合、インターフェイスで **ppp pap sent-name password** コマンドは設定しないでください。PAP の場合、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAP の場合、「preauth:send-name」は、アウトバウンド認証だけでなく、インバウンド認証にも使用されます。CHAP インバウンドの場合、NAS は発信元のボックスへのチャレンジ パケットに、「preauth:send-name」で定義された名前を使用します。<br>（注） send-name 属性は時間の経過とともに変わっています。最初は、現在 send-name および remote-name 属性の両方で提供されている機能を実行していました。remote-name |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| | | | | 属性が追加されたため、send-name 属性は現在の動作に制限されています。 |
| 26 | 9 | 1 | send-secret | PPP パスワード認証。ベンダー固有属性（VSA）の場合、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAP アウトバウンドの場合、「preauth:send-name」と「preauth:send-secret」の両方が応答パケットで使用されます。 |
| 26 | 9 | 1 | remote-name | 大規模のダイヤルアウトで使用するリモートホストの名前を提供します。ダイヤラは、大規模のダイヤルアウトのリモート名が認証された名前と一致することを確認し、偶発的なユーザ RADIUS 設定ミスから保護します（有効な電話番号にダイヤルしたが誤ったデバイスに接続されるなどのミスです）。 |
| その他の属性 | | | | |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 2 | Cisco-NAS-Port | NAS-Port アカウンティングに追加的なベンダー固有属性（VSA）を指定します。追加的な NAS-Port 情報を属性値ペア（AVPair）の形式で指定するには、**radius-server vsa send** グローバル コンフィギュレーション コマンドを使用します。<br>（注） この VSA は、通常アカウンティングで使用されますが認証（Access-Request）パケットで使用される場合もあります。 |
| 26 | 9 | 1 | min-links | MLP に対するリンクの最小数を設定します。 |
| 26 | 9 | 1 | proxyacl#<n> | ダウンロード可能なユーザ プロファイル（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。 |

| 番号 | ベンダー固有の企業コード | サブタイプ番号 | 属性 | 説明 |
|---|---|---|---|---|
| 26 | 9 | 1 | spi | 登録中にホーム エージェントがモバイル ノードの認証で必要とする認証情報を伝送します。この情報は、**ip mobile secure host <addr>** コンフィギュレーション コマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーション コマンドはそのまま含まれます。これにはセキュリティ パラメータ インデックス（SPI）、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。 |

# ベンダー独自仕様の RADIUS サーバ通信

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバ間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS 属性セットを独自に機能拡張しているベンダーもあります。Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

前述したように、RADIUS（ベンダーの独自仕様によるものか、IETF ドラフトに準拠するものかを問わず）を設定するには、RADIUS サーバデーモンが稼働しているホストと、そのホストがスイッチと共有するシークレットテキストストリングを指定する必要があります。RADIUS ホストおよび秘密テキスト文字列を指定するには、**radius server** グローバル コンフィギュレーション コマンドを使用します。

# RADIUS の設定方法

## RADIUS サーバ ホストの識別

デバイスと通信するすべてのRADIUSサーバにこのような設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **key** *string* という 3 つの固有なグローバル コンフィギュレーション コマンドを使用します。

認証時用にAAAサーバ グループを使用して既存のサーバ ホストをグループ化するようにデバイスを設定できます。詳細については、次の関連項目を参照してください。

RADIUSサーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、デバイスの IP アドレス、およびサーバとデバイスの双方で共有するキー ストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、次の手順を実行します。

### 始める前に

deviceにグローバルな機能とサーバ単位での機能（タイムアウト、再送信回数、およびキーコマンド）を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、およびキーに関するコマンドは、グローバルに設定したタイムアウト、再送信回数、およびキーに関するコマンドを上書きします。すべての RADIUS サーバに対してこれらの値を設定する方法については、次の関連項目を参照してください。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **radius server** *server name*<br>例：<br>デバイス(config)# **radius server rsim** | |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **address** {**ipv4** \| **ipv6**}*ip address*{ **auth-port** *port number* \| **acct-port** *port number*}<br>例：<br>デバイス(config-radius-server)# **address ipv4 124.2.2.12 auth-port 1612** | （任意）RADIUS サーバのパラメータを指定します。<br>**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは1645 です。指定できる範囲は 0 ～ 65536 です。<br>**acct-port** *port-number* には、認証要求の UDP宛先ポートを指定します。デフォルトは 1646 です。 |
| ステップ 5 | **key** *string*<br>例：<br>デバイス(config-radius-server)# **key rad123** | （任意）**key** *string* には、デバイスと RADIUS サーバで動作する RADIUS デーモンの間で使用される認証と暗号キーを指定します。<br>（注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキストストリングでなければなりません。必ず **radius server** コマンドの最終項目としてキーを設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 |
| ステップ 6 | **retransmit** *value*<br>例：<br>デバイス(config-radius-server)# **retransmit 10** | （任意）サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ～ 100 です。この設定は、**radius-server retransmit** グローバル コンフィギュレーション コマンドによる設定を上書きします。 |
| ステップ 7 | **timeout** *seconds*<br>例：<br>デバイス(config-radius-server)# **timeout 60** | （任意）デバイスが要求を再送信する前に RADIUS サーバからの応答を待機する時間間隔を指定します。指定できる範囲は1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コン |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | フィギュレーションコマンドによる設定を上書きします。 |
| ステップ 8 | **exit**<br>例：<br>デバイス(config-server-tacacs)# **exit** | RADIUS サーバモードを終了して、グローバルコンフィギュレーションモードを開始します。 |
| ステップ 9 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 10 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 11 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

# RADIUS ログイン認証の設定

RADIUS ログイン認証を設定するには、次の手順を実行します。

### 始める前に

AAA 方式を使用して HTTP アクセスに対しdeviceのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでdeviceを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しdeviceのセキュリティは確保しません。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例： | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス> **enable** | |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 4 | **aaa authentication login** {**default** \| *list-name*} *method1* [*method2...* ]<br>例：<br>デバイス(config)# **aaa authentication login default local** | ログイン認証方式リストを作成します。<br>• **login authentication** コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。<br>• *list-name* には、作成するリストの名前として使用する文字列を指定します。<br>• *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。<br>次のいずれかの方式を選択します。<br>  • *enable*：イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ **enable** *password* グローバル コンフィギュレーション コマンドを使用してイネーブルパスワードを定義しておく必要があります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • *group radius*：RADIUS 認証を使用します。この認証方式を使用するには、あらかじめ RADIUS サーバを設定しておく必要があります。<br>• *line*：回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。<br>• *local*：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *name* **password** グローバル コンフィギュレーション コマンドを使用します。<br>• *local-case*：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username** *password* グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。<br>• *none*：ログインに認証を使用しません。 |
| ステップ 5 | **line** [**console** \| **tty** \| **vty**] *line-number* [*ending-line-number*]<br>例：<br>`デバイス(config)# line 1 4` | ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。 |
| ステップ 6 | **login authentication** {**default** \| *list-name*}<br>例： | 1 つの回線または複数回線に認証リストを適用します。<br>• **default** を指定する場合は、**aaa authentication login** コマンドで作成 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config)# **login authentication default** | したデフォルトのリストを使用します。<br>• *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。 |
| ステップ 7 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 9 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# AAA サーバ グループの定義

定義したグループサーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホストインスタンスまたはエントリを特定することもできます。

AAA サーバ グループを定義するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **radius server** *name*<br>例：<br>デバイス(config)# **radius server ISE** | RADIUS サーバの設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。<br>deviceは、IPv6 用の RADIUS もサポートしています。 |
| ステップ 4 | **address** {**ipv4** \| **ipv6**} {*ip-address* \| *hostname*} **auth-port** *port-number* **acct-port** *port-number*<br>例：<br>デバイス(config-radius-server)# **address ipv4 10.1.1.1 auth-port 1645 acct-port 1646** | RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。 |
| ステップ 5 | **end** *string*<br>例：<br>デバイス(config-radius-server)# **key cisco123** | デバイスと RADIUS サーバとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。 |
| ステップ 6 | **end**<br>例：<br>デバイス(config-radius-server)# **end** | RADIUS サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 7 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 8 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | **startup-config** | |

# ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

ユーザ特権アクセスおよびネットワーク サービスに関する RADIUS 許可を設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa authorization network radius**<br>例：<br>デバイス(config)# **aaa authorization network radius** | ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるようにdeviceを設定します。 |
| ステップ 4 | **aaa authorization exec radius**<br>例：<br>デバイス(config)# **aaa authorization exec radius** | ユーザに特権 EXEC のアクセス権限がある場合、ユーザが RADIUS 許可を受けるように device を設定します。<br>**exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

### 次のタスク

**aaa authorization** グローバル コンフィギュレーション コマンドと **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

**aaa authorization exec radius local** コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

# RADIUS アカウンティングの起動

RADIUS アカウンティングを開始するには、次の手順を実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa accounting network start-stop radius**<br>例：<br>デバイス(config)# **aaa accounting network start-stop radius** | ネットワーク関連のあらゆるサービス要求に関して、RADIUS アカウンティングをイネーブルにします。 |
| ステップ 4 | **aaa accounting exec start-stop radius**<br>例：<br>デバイス(config)# **aaa accounting exec start-stop radius** | RADIUS アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# すべての RADIUS サーバの設定

すべての RADIUS サーバを設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **radius-server key** *string*<br>例：<br>デバイス(config)# **radius-server key your_server_key**<br>デバイス(config)# **key your_server_key** | スイッチとすべての RADIUS サーバ間で共有されるシークレット テキスト ストリングを指定します。<br>（注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 |
| ステップ 3 | **radius-server retransmit** *retries*<br>例：<br>デバイス(config)# **radius-server retransmit 5** | スイッチが RADIUS 要求をサーバに再送信する回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ～ 1000 です。 |
| ステップ 4 | **radius-server timeout** *seconds*<br>例：<br>デバイス(config)# **radius-server timeout 3** | スイッチが RADIUS 要求に対する応答を待って、要求を再送信するまでの時間（秒）を指定します。デフォルトは5秒です。指定できる範囲は 1 ～ 1000 です。 |
| ステップ 5 | **radius-server deadtime** *minutes*<br>例：<br>デバイス(config)# **radius-server deadtime 0** | RADIUS サーバが認証要求に応答していない場合、このコマンドはそのサーバに対する要求を停止する時刻を指定します。これにより、要求がタイムアウトするまで待たずとも、次に設定されているサーバを試行することができます。デフォルトは 0 です。指定できる範囲は 0 ～ 1440 分です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 8 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# ベンダー固有の RADIUS 属性を使用するDevice設定

ベンダー固有の RADIUS 属性を使用するようにdeviceを設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **radius-server vsa send** [**accounting** \| **authentication**]<br>例：<br>デバイス(config)# **radius-server vsa send** | deviceが VSA（RADIUS IETF 属性 26 で定義）を認識して使用できるようにします。<br>• （任意）認識されるベンダー固有属性の集合をアカウンティング属性だ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `accounting` | けに限定するには、**accounting** キーワードを使用します。<br>• （任意）認識されるベンダー固有属性の集合を認証属性だけに限定するには、**authentication** キーワードを使用します。<br><br>キーワードを指定せずにこのコマンドを入力すると、アカウンティングおよび認証のベンダー固有属性の両方が使用されます。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# ベンダー独自の RADIUS サーバとの通信に関するDeviceの設定

ベンダー独自仕様の RADIUS サーバ通信を使用するようにdeviceを設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **radius server** *server name*<br>例：<br>デバイス(config)# **radius server rsim** | RADIUS サーバを指定します。 |
| ステップ 4 | **address** { **ipv4** \| **ipv6** } *ip address*<br>例：<br>デバイス(config-radius-server)# **address ipv4 172.24.25.10** | （任意）RADIUS サーバの IP アドレスを指定します。 |
| ステップ 5 | **non-standard**<br>例：<br>デバイス(config-radius-server)# **non-standard** | RADIUS サーバが RADIUS ベンダー独自の実装を使用していることを示します。 |
| ステップ 6 | **key** *string*<br>例：<br>デバイス(config-radius-server)# **key rad123** | deviceとベンダー独自仕様の RADIUS サーバとの間で使用される共有秘密テキスト文字列を指定します。deviceと RADIUS サーバはこのテキスト文字列を使用してパスワードを暗号化し、応答を交換します。 |
| ステップ 7 | **exit**<br>例：<br>デバイス(config-radius-server)# **exit** | RADIUS サーバモードを終了して、グローバル コンフィギュレーション モードを開始します。 |
| ステップ 8 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show running-config**<br>例： | 入力を確認します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **show running-config** | |
| ステップ 10 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

# 次の上での CoA の設定 Device

CoA を device で設定するには、次の手順を実行します。この手順は必須です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 4 | **aaa server radius dynamic-author**<br>例：<br>デバイス(config)# **aaa server radius dynamic-author** | device を認証、許可、アカウンティング（AAA）サーバに設定し、外部ポリシーサーバとの相互作用を実行します。 |
| ステップ 5 | **client** {*ip-address* \| *name*} [ **vrf** *vrfname*] [ **server-key** *string*] | ダイナミック許可ローカルサーバコンフィギュレーションモードを開始し、デバイスがCoAを受け取り、要求を取 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | り外す RADIUS クライアントを指定します。 |
| ステップ 6 | **server-key** [**0** \| **7**] *string*<br>例：<br>デバイス(config-sg-radius)# **server-key your_server_key** | RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。 |
| ステップ 7 | **port** *port-number*<br>例：<br>デバイス(config-sg-radius)# **port 25** | 設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。 |
| ステップ 8 | **auth-type** {**any** \| **all** \| **session-key**}<br>例：<br>デバイス(config-sg-radius)# **auth-type any** | device が RADIUS クライアントに使用する許可のタイプを指定します。<br>クライアントは、許可用に設定されたすべての属性と一致していなければなりません。 |
| ステップ 9 | **ignore session-key** | （任意）セッションキーを無視するように device を設定します。<br>**ignore** コマンドの詳細については、Cisco.com 上の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。 |
| ステップ 10 | **ignore server-key**<br>例：<br>デバイス(config-sg-radius)# **ignore server-key** | （任意）サーバキーを無視するように device を設定します。<br>**ignore** コマンドの詳細については、Cisco.com 上の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。 |
| ステップ 11 | **authentication command bounce-port ignore**<br>例：<br>デバイス(config-sg-radius)# **authentication command bounce-port ignore** | （任意）CoA 要求を無視して、セッションをホスティングするポートを一時的にディセーブルにするように device を設定します。ポートを一時的にディセーブルにする目的は、VLAN の変更が発生しても、その変更を検出するサプリカントがエンドポイント上にない |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 場合に、ホストから DHCP 再ネゴシエーションを行わせることです。 |
| ステップ 12 | **authentication command disable-port ignore**<br>例：<br>デバイス(config-sg-radius)# **authentication command disable-port ignore** | （任意）セッションをホスティングしているポートを管理上のシャットダウン状態にするよう要求する非標準コマンドを無視するように device を設定します。ポートをシャットダウンすると、セッションが終了します。<br>ポートを再びイネーブルにするには、標準の CLI または SNMP コマンドを使用します。 |
| ステップ 13 | **end**<br>例：<br>デバイス(config-sg-radius)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 14 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 15 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

# CoA 機能のモニタリング

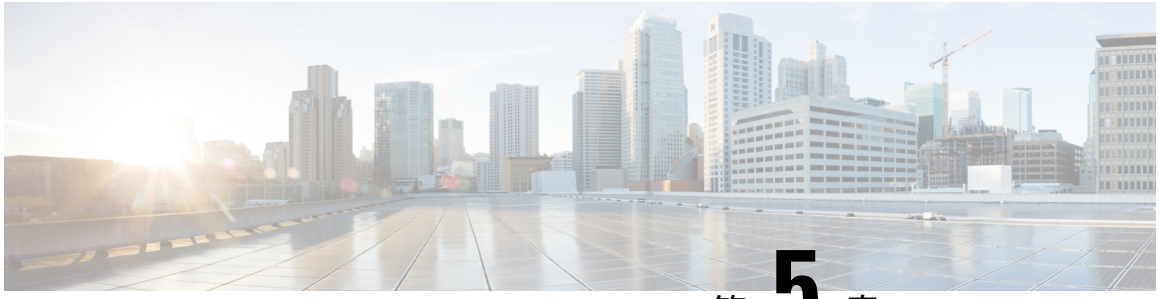
表 *11 :* 特権 *EXEC* 表示コマンド

| コマンド | 目的 |
|---|---|
| **show aaa attributes protocol radius** | RADIUS コマンドの AAA 属性を表示します。 |

表 *12 :* グローバル トラブルシューティング コマンド

| コマンド | 目的 |
|---|---|
| **debug radius** | RADIUS のトラブルシューティングを行うための情報を表示します。 |
| **debug aaa coa** | CoA 処理のトラブルシューティングを行うための情報を表示します。 |
| **debug aaa pod** | POD パケットのトラブルシューティングを行うための情報を表示します。 |
| **debug aaa subsys** | POD パケットのトラブルシューティングを行うための情報を表示します。 |
| **debug cmdhd**[**detail** \|**error** \|**events**] | コマンド ヘッダーのトラブルシューティングを行うための情報を表示します。 |

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。



第 5 章

# Kerberos の設定


- Kerberos によるスイッチ アクセスの制御の前提条件 （85 ページ）
- Kerberos に関する情報 （85 ページ）
- Kerberos を設定する方法 （90 ページ）
- Kerberos 設定の監視 （90 ページ）
- その他の参考資料 （90 ページ）


## Kerberos によるスイッチ アクセスの制御の前提条件

次に、Kerberos を使用してスイッチ アクセスを制御するための前提条件を示します。

- リモート ユーザがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定し、ユーザとネットワーク サービスの両方に通信を行い、相互に認証させる必要があります。これを実現するには、互いの識別が必要です。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。また、KDC データベースにユーザ用のエントリも作成します。

- Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるスイッチを使用できます。

ホストおよびユーザのエントリを追加または作成する場合の注意事項は次のとおりです。

- Kerberos プリンシパル名はすべて小文字でなければなりません。

- Kerberos インスタンス名はすべて小文字でなければなりません。

- Kerberos レルム名はすべて大文字でなければなりません。

## Kerberos に関する情報

ここでは、Kerberos の情報を提供します。

# Kerberos とスイッチ アクセス

ここでは、Kerberos セキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。

（注） Kerberos の設定例では、信頼できるサードパーティを、Kerberos をサポートし、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証するスイッチとすることができます。

# Kerberos の概要

Kerberos はマサチューセッツ工科大学（MIT）が開発した秘密キーによるネットワーク認証プロトコルです。データ暗号規格（DES）という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサードパーティという概念を使ってユーザとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティをキー発行局（KDC）と呼びます。

Kerberos は、ユーザが誰であるか、そのユーザが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC（つまり信頼できる Kerberos サーバ）がユーザにチケットを発行します。これらのチケットには有効期限があり、ユーザ クレデンシャルのキャッシュに保存されます。Kerberos サーバは、ユーザ名やパスワードの代わりにチケットを使ってユーザとネットワーク サービスを認証します。

（注） Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるのであれば、どのスイッチも使用できます。

Kerberos のクレデンシャル発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザを 1 回認証すると、ユーザ クレデンシャルが有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、（UNIX サーバや PC などの）他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh

次の表に、一般的な Kerberos 関連用語とその定義を示します。

**表 *13 : Kerberos* の用語**

| 用語 | 定義 |
|---|---|
| 認証 | ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。 |
| 許可 | ユーザがネットワークやスイッチにおいてどのような権限を有しており、またどのような動作を実行できるかを、スイッチが識別する手段 |
| クレデンシャル | 認証チケット（TSG[2]、サービスクレデンシャルなど）を表す総称。Kerberos クレデンシャルで、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することにした場合、ユーザ名やパスワードを再入力する代わりにこれを使用できます。証明書の有効期限は、8 時間がデフォルトの設定です。 |
| インスタンス | Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、*user@REALM* という形式です（たとえば、smith@EXAMPLE.COM）。Kerberos インスタンスのある Kerberos プリンシパルは、*user/instance@REALM* という形式です（たとえば、smith/admin@EXAMPLE.COM）。Kerberos インスタンスは、認証が成功した場合のユーザの承認レベルを指定するために使用できます。各ネットワーク サービスのサーバは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。<br>（注） Kerberos プリンシパル名およびインスタンス名はすべて小文字でなければなりません。<br>（注） Kerberos レルム名はすべて大文字でなければなりません。 |
| KDC[3] | ネットワーク ホストで稼働する Kerberos サーバおよびデータベース プログラムで構成されるキー発行局 |
| Kerberos 対応 | Kerberos クレデンシャルのインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語 |
| Kerberos レルム | Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク サービスの ID を検証します。<br>（注） Kerberos レルム名はすべて大文字でなければなりません。 |

| 用語 | 定義 |
|---|---|
| Kerberos サーバ | ネットワーク ホストで稼働しているデーモン。ユーザおよびネットワーク サービスはそれぞれKerberosサーバにIDを登録します。ネットワーク サービスはKerberosサーバにクエリーを送信して、他のネットワーク サービスの認証を得ます。 |
| KEYTAB[4] | ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス クレデンシャルを暗号解除して認証します。Kerberos 5 よりも前のバージョンでは、KEYTAB はSRVTAB[5]と呼ばれます。 |
| プリンシパル | Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。<br>（注） Kerberos プリンシパル名はすべて小文字でなければなりません。 |
| サービス クレデンシャル | ネットワーク サービスのクレデンシャル。KDCからクレデンシャルが発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。ユーザ TGT ともパスワードを共有します。 |
| SRVTAB | ネットワーク サービスがKDCと共有するパスワード。SRVTABは、Kerberos 5 以降のバージョンでは KEYTAB と呼ばれています。 |
| TGT | 身分証明書のことで、KDC が認証済みユーザに発行するクレデンシャル。TGT を受け取ったユーザは、KDC が示した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。 |

[2] チケット認可チケット
[3] キー発行局
[4] キー テーブル
[5] サーバ テーブル

# Kerberos の動作

リモートユーザが device を Kerberos サーバとして使用してネットワークサービスで認証されるには、次の手順を実行する必要があります。Kerberosをカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモートユーザは、3つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

リモートユーザが device を Kerberos サーバとして使用してネットワークサービスで認証されるには、次の手順を実行する必要があります。

## 境界スイッチに対する認証の取得

ここでは、リモート ユーザが通過しなければならない最初のセキュリティ レイヤについて説明します。ユーザは、まず境界スイッチに対して認証を得なければなりません。リモートユーザが境界スイッチに対して認証を得る場合、次のプロセスが発生します。

1. ユーザが境界スイッチに対して、Kerberos 未対応の Telnet 接続を開始します。
2. ユーザ名とパスワードの入力を求めるプロンプトをスイッチが表示します。
3. スイッチが、このユーザの TGT を KDC に要求します。
4. KDC がユーザ ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使って TGT の暗号解除を試行します。
   - 暗号解除に成功した場合は、ユーザはスイッチに対して認証を得ます。
   - 暗号解除に成功しない場合は、ユーザ名とパスワードを再入力（Caps Lock または Num Lock のオン/オフに注意）するか、別のユーザ名とパスワードを入力してステップ 2 の手順を繰り返します。

Kerberos 未対応の Telnet セッションを開始し、境界スイッチの認証を得ているリモート ユーザはファイアウォールの内側にいますが、ネットワーク サービスにアクセスするには、KDC から直接認証を得る必要があります。ユーザが KDC から認証を得なければならないのは、KDC が発行する TGT はスイッチに保存されており、ユーザがこのスイッチにログオンしないかぎり、追加の認証に使用できないからです。

## KDC からの TGT の取得

ここでは、リモート ユーザが通過しなければならない 2 番めのセキュリティ レイヤについて説明します。ユーザは、ネットワーク サービスにアクセスするために、このレイヤで KDC の認証を得て、KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章にある「Obtaining a TGT from a KDC」を参照してください。

## ネットワーク サービスに対する認証の取得

ここでは、リモート ユーザが通過しなければならない 3 番めのセキュリティ レイヤについて説明します。TGT を取得したユーザは、このレイヤで Kerberos レルム内のネットワーク サービスに対して認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章の「Authenticating to Network Services」を参照してください。

# Kerberos を設定する方法

Kerberos 認証済みサーバ/クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

# Kerberos 設定の監視

Kerberos 設定を表示するには、次のコマンドを使用します。

- **show running-config**
- **show kerberos creds**：現在のユーザの認定証キャッシュに含まれる認定証を一覧表示します。
- **clear kerberos creds**：転送済みの認定証を含め、現在のユーザの認定証キャッシュに含まれるすべての認定証を破棄します。

# その他の参考資料

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| Kerberos コマンド | 『*Cisco IOS Security Command Reference*』 |

### エラー メッセージ デコーダ

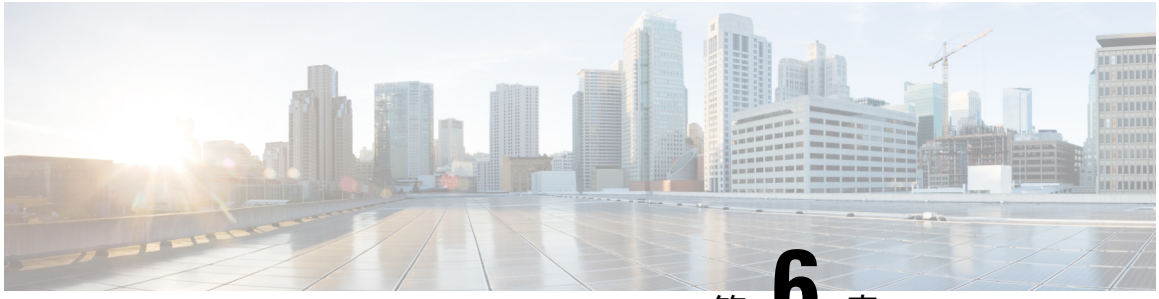
| 説明 | リンク |
|---|---|
| このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。 | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### MIB

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

### シスコのテクニカル サポート

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



第 6 章

# MACsec の暗号化


- MACsec 暗号化について （93 ページ）
- MACsec 暗号化の設定方法 （104 ページ）
- MACsec 暗号化の設定例 （132 ページ）


## MACsec 暗号化について

MACsec は 2 台の MACsec 対応デバイス間のパケットの認証と暗号化の IEEE 802.1AE 規格です。これらの Catalyst スイッチは、スイッチとホスト デバイス間の暗号化に、ダウンリンク ポートでの MACsec Key Agreement（MKA）による 802.1AE 暗号化をサポートします。また、スイッチは、Cisco TrustSec ネットワーク デバイス アドミッション コントロール（NDAC）、Security Association Protocol（SAP）および MKA ベースのキー交換プロトコルを使用して、スイッチ間（ネットワーク間デバイス）セキュリティの MACsec 暗号化をサポートします。

リンク層セキュリティはスイッチ間のパケット認証とスイッチ間のMACsec暗号化の両方を含みます（暗号化は任意です）。

（注） MACsec は NPE ライセンスまたは LAN Base サービス イメージではサポートされません。

表 *14*：スイッチ ポートの *MACsec* サポート

| インターフェイス（Interface） | 接続 | MACsec のサポート |
|---|---|---|
| ダウンリンク ポート | スイッチからホストへ | MACsec MKA の暗号化 |
| アップリンク ポート | スイッチからスイッチへ | MACsec MKA の暗号化<br>Cisco TrustSec NDAC MACsec |

Cisco TrustSec と Cisco SAP はスイッチ間のリンクにのみ使用され、PC や IP フォンなどのエンドホストに接続されたスイッチ ポートではサポートされません。MKA は、スイッチからホストへのリンク（ダウンリンク）とスイッチ間リンク（アップリンク）でサポートされます。ホ

スト側のリンクは、IEEE 802.1x の有無にかかわらず異種デバイスを扱うために、一般に柔軟な認証順序を使用し、オプションで MKA ベースの MACsec 暗号化を使用できます。Cisco NDAC および SAP は、コンパクトなスイッチがワイヤリング クローゼットの外側にセキュリティを拡張するために使用する、ネットワーク エッジ アクセス トポロジ（NEAT）と相互排他的です。

## Media Access Control Security と MACsec Key Agreement

802.1AE で定義された MACsec では、暗号化キー入力のためにアウトオブバンド方式を使用することによって、有線ネットワーク上で MAC レイヤの暗号化を実現します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。MKA と MACsec は、802.1x 拡張認証プロトコル（EAP-TLS）または事前共有キー（PSK）フレームワークを使用した認証に成功した後に実装されます。

MACsec を使用するスイッチでは、MKA ピアに関連付けられたポリシーに応じて、MACsec フレームまたは非 MACsec フレームを許可します。MACsec フレームは暗号化され、整合性チェック値（ICV）で保護されます。スイッチは MKA ピアからフレームを受信すると、MKA によって提供されたセッション キーを使用してこれらのフレームを暗号化し、正しい ICV を計算します。スイッチはこの ICV をフレーム内の ICV と比較します。一致しない場合は、フレームが破棄されます。また、スイッチは現在のセッション キーを使用して、ICV を暗号化し、セキュアなポート（セキュアな MAC サービスを MKA ピアに提供するために使用されるアクセス ポイント）を介して送信されたフレームに追加します。

MKA プロトコルは、基礎となる MACsec プロトコルで使用される暗号キーを管理します。MKA の基本的な要件は 802.1x-REV で定義されています。MKA プロトコルでは 802.1x を拡張し、相互認証の確認によってピアを検出し、MACsec 秘密キーを共有してピアで交換されるデータを保護できます。

EAP フレームワークでは、新しく定義された EAP-over-LAN（EAPOL）パケットとして MKA を実装します。EAP 認証では、データ交換で両方のパートナーで共有されるマスターセッション キー（MSK）を生成します。EAP セッション ID を入力すると、セキュアな接続アソシエーション キー名（CKN）が生成されます。スイッチは、アップリンクおよびダウンリンクの両方のオーセンティケータとして機能します。また、ダウンリンクのキー サーバとして機能します。これによってランダムなセキュア アソシエーション キー（SAK）が生成され、クライアントパートナーに送信されます。クライアントはキー サーバではなく、単一の MKA エンティティであるキー サーバとだけ対話できます。キーの派生と生成の後で、スイッチは定期的にトランスポートをパートナーに送信します。デフォルトの間隔は 2 秒間です。

EAPOL プロトコル データ ユニット（PDU）のパケット本体は、MACsec Key Agreement PDU（MKPDU）と呼ばれます。MKA セッションと参加者は、MKA ライフタイム（6 秒間）が経過しても参加者から MKPDU を受信していない場合に削除されます。たとえば、MKA ピアが接続を解除した場合、スイッチ上の参加者は MKA ピアから最後の MKPDU を受信した後、6 秒間が経過するまで MKA の動作を継続します。

（注） MKPDU の整合性チェック値（ICV）インジケータはオプションです。トラフィックが暗号化されている場合、ICV はオプションではありません。

EAPoL 通知は、キー関連情報のタイプの使用を示します。通知は、サプリカントとオーセンティケータの機能を通知するために使用できます。各側の機能に基づいて、キー関連情報の最大公分母を使用できます。

Cisco IOS XE Fuji 16.8.1a よりも前のリリースでは、MKA と SAP で should-secure がサポートされていました。should-secure を有効にすると、ピアが MACsec に設定されている場合はデータトラフィックが暗号化され、それ以外の場合はクリアテキストで送信されます。Cisco IOS XE Fuji 16.8.1a 以降、入力と出力の両方で must-secure のサポートが有効になります。MKA および SAP では、Must-secure がサポートされています。must-secure を有効にすると、EAPoL トラフィックのみが暗号化されません。他のトラフィックは暗号化されます。暗号化されないパケットはドロップされます。

（注） デフォルトでは、Must-secure モードが有効になっています。

## MKA ポリシー

インターフェイスで MKA を有効にするには、定義された MKA ポリシーをインターフェイスに適用する必要があります。次のオプションを設定可能です。

- 16 ASCII 文字未満のポリシー名。
- 物理インターフェイスごとの 0 バイト、30 バイト、または 50 バイトの機密保持（暗号化）オフセット。

## 仮想ポート

仮想ポートは、1 つの物理ポート上の複数のセキュアな接続アソシエーションに使用します。各接続アソシエーション（ペア）は仮想ポートを表します。アップリンクでは、物理ポートごとに 1 つの仮想ポートのみを指定できます。ダウンリンクでは、物理ポートごとに最大 2 つの仮想ポートを指定でき、一方の仮想ポートはデータ VLAN の一部にできます。もう一方は音声 VLAN に対してパケットを外部的にタグ付けする必要があります。同じポートで同じ VLAN 内のセキュアなセッションとセキュアでないセッションを同時にホストすることはできません。この制限のため、802.1x マルチ認証モードはサポートされません。

この制限の例外は、マルチホスト モードで最初の MACsec サプリカントが正常に認証され、スイッチに接続されたハブに接続される場合です。ハブに接続された非 MACsec ホストでは、マルチホストモードであるため、認証なしでトラフィックを送信できます。最初にクライアントが成功した後、他のクライアントでは認証が必要ないため、マルチホストモードの使用は推奨しません。

仮想ポートは、接続アソシエーションの任意のIDを表し、MKAプロトコル外では意味を持ちません。仮想ポートは個々の論理ポート ID に対応します。仮想ポートの有効なポート ID は 0x0002 ～ 0xFFFF です。各仮想ポートは、16 ビットのポート ID に連結された物理インターフェイスの MAC アドレスに基づいて、一意のセキュア チャネル ID（SCI）を受け取ります。

## MACsec およびスタッキング

MACsec を実行しているスイッチ スタック マスターは、MACsec をサポートしているメンバー スイッチ上のポートを示すコンフィギュレーション ファイルを維持します。スタック マスターは、次に示す機能を実行します。

- セキュアなチャネルとセキュアなアソシエーションの作成および削除を処理します。
- スタック メンバーにセキュアなアソシエーション サービス要求を送信します。
- ローカル ポートまたはリモート ポートからのパケット番号とリプレイ ウィンドウ情報を処理し、キー管理プロトコルを通知します。
- オプションがグローバルに設定されたMACsec初期化要求を、スタックに追加される新しいスイッチに送信します。
- ポート単位の設定をメンバー スイッチに送信します。

メンバー スイッチは、次の機能を実行します。

- スタック マスターからの MACsec 初期化要求を処理します。
- スタック マスターから送信された MACsec サービス要求を処理します。
- スタック マスターにローカル ポートに関する情報を送信します。

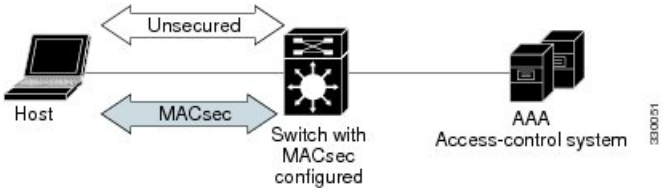
## MACsec、MKA、および 802.1x ホスト モード

MACsec と MKA プロトコルは、802.1x シングルホスト モード、マルチホスト モード、またはマルチドメイン認証（MDA）モードで使用できます。マルチ認証モードはサポートされません。

### シングルホスト モード

次の図に、MKA を使用して、MACsec で 1 つの EAP 認証済みセッションをセキュアにする方法を示します。

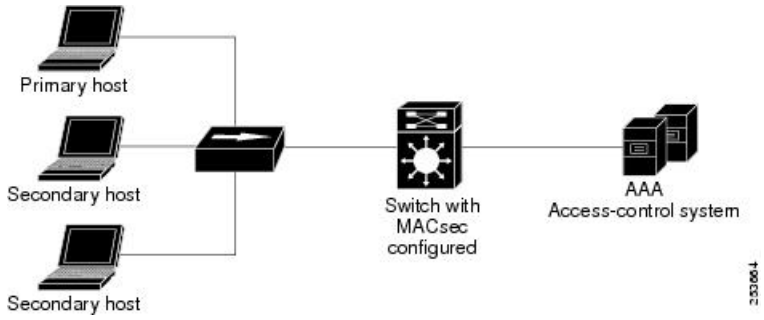
**図 *4:* セキュアなデータ セッションでのシングルホスト モードの *MACsec***



## マルチ ホスト モード

標準の（802.1x REV ではない）802.1x マルチホスト モードでは、1 つの認証に基づいてポートが開いているか、閉じられています。1 人のユーザ（プライマリ セキュア クライアント サービスのクライアントホスト）が認証される場合は、同じポートに接続されているホストに同じレベルのネットワーク アクセスが提供されます。セカンダリ ホストが MACsec サプリカントの場合、認証できず、トラフィック フローは発生しません。非 MACsec ホストであるセカンダリ ホストは、マルチホスト モードであるため、認証なしでネットワークにトラフィックを送信できます。次の図に、標準のマルチホスト非セキュア モードにおける MACsec を示します。

**図 5 : マルチホスト モードの *MACsec*：非セキュア**




（注） マルチホスト モードは推奨されていません。これは最初にクライアントが成功した後、他のクライアントでは認証が必要ないことから、安全性が低いためです。

標準の（802.1x REV ではない）802.1x マルチドメイン モードでは、1 つの認証に基づいてポートが開いているか、閉じられています。プライマリ ユーザ（データ ドメインの PC）が認証されると、同じレベルのネットワーク アクセスが同じポートに接続されているドメインに提供されます。セカンダリ ユーザが MACsec サプリカントの場合、認証できず、トラフィック フローは発生しません。非 MACsec ホストであるセカンダリ ユーザ（音声ドメインの IP フォン）は、マルチドメイン モードであるため、認証なしでネットワークにトラフィックを送信できます。

## MKA 統計情報

一部の MKA カウンタはグローバルに集約され、その他のカウンタはグローバルとセッション単位の両方で更新されます。また、MKA セッションのステータスに関する情報も取得できます。

次に、**show mka sessions** コマンドの出力例を示します。

```
Device# show mka sessions

Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=============================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server
Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN
```

```
==========================================================================================
Gi1/0/1        204c.9e85.ede4/002b p2               NO                YES
43             c800.8459.e764/002a 1                Secured
0100000000000000000000000000000000000000000000000000000000000000

Device# show mka sessions interface G1/0/1

Summary of All Currently Active MKA Sessions on Interface GigabitEthernet1/0/1...

==========================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server
Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN
==========================================================================================
Gi1/0/1        204c.9e85.ede4/002b p2               NO                YES
43             c800.8459.e764/002a 1                Secured
0100000000000000000000000000000000000000000000000000000000000000


Device# show mka sessions interface G1/0/1 de

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier...... 43
Interface Name........... GigabitEthernet1/0/1
Audit Session ID.........
CAK Name (CKN)........... 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)...... 89567
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)

MKA Policy Name.......... p2
Key Server Priority...... 2
Delay Protection......... NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------
```

```
  38046BA37D7DA77E06D006A9  89555       c800.8459.e764/002a   10

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------

Device# show mka sessions detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier...... 43
Interface Name........... GigabitEthernet1/0/1
Audit Session ID.........
CAK Name (CKN)........... 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)...... 89572
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)

MKA Policy Name.......... p2
Key Server Priority...... 2
Delay Protection......... NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------
  38046BA37D7DA77E06D006A9  89560       c800.8459.e764/002a   10

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS Priority
  ----------------------------------------------------------------------
```

```
Device# show mka policy

MKA Policy Summary...

Policy            KS       Delay   Replay  Window Conf   Cipher          Interfaces
Name              Priority Protect Protect Size   Offset Suite(s)        Applied
=================================================================================================
*DEFAULT POLICY*  0        FALSE   TRUE    0      0      GCM-AES-128

p1                1        FALSE   TRUE    0      0      GCM-AES-128

p2                2        FALSE   TRUE    0      0      GCM-AES-128     Gi1/0/1

Device# show mka policy p2 detail

MKA Policy Configuration ("p2")
=======================
MKA Policy Name........ p2
Key Server Priority.... 2
Confidentiality Offset. 0
Send Secure Announcement..DISABLED
Cipher Suite(s)........ GCM-AES-128

Applied Interfaces...
  GigabitEthernet1/0/1
```

次に、**show mka statistics** コマンドの出力例を示します。

```
Device# show mka statistics interface G1/0/1

MKA Statistics for Session
==========================
Reauthentication Attempts.. 0

CA Statistics
   Pairwise CAKs Derived... 0
   Pairwise CAK Rekeys..... 0
   Group CAKs Generated.... 0
   Group CAKs Received..... 0

SA Statistics
   SAKs Generated.......... 1
   SAKs Rekeyed............ 0
   SAKs Received........... 0
   SAK Responses Received.. 1

MKPDU Statistics
   MKPDUs Validated & Rx... 89585
      "Distributed SAK".. 0
      "Distributed CAK".. 0
   MKPDUs Transmitted...... 89596
      "Distributed SAK".. 1
      "Distributed CAK".. 0

Device# show mka summary

Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=================================================================================================
```

```
Interface       Local-TxSCI         Policy-Name      Inherited         Key-Server
Port-ID         Peer-RxSCI          MACsec-Peers     Status            CKN
==========================================================================================
Gi1/0/1         204c.9e85.ede4/002b p2               NO                YES
43              c800.8459.e764/002a 1                Secured
0100000000000000000000000000000000000000000000000000000000000000


MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 1
   Reauthentication Attempts.. 0

   Deleted (Secured)........... 0
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated............. 1
   SAKs Rekeyed............... 0
   SAKs Received.............. 0
   SAK Responses Received..... 1

MKPDU Statistics
   MKPDUs Validated & Rx...... 89589
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 89600
      "Distributed SAK"..... 1
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Session Failures
   Bring-up Failures................ 0
   Reauthentication Failures........ 0
   Duplicate Auth-Mgr Handle........ 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0
   SAK Cipher Mismatch.............. 0

CA Failures
   Group CAK Generation............. 0
   Group CAK Encryption/Wrap........ 0
   Group CAK Decryption/Unwrap...... 0
   Pairwise CAK Derivation.......... 0
   CKN Derivation................... 0
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability... 0
MACsec Failures
   Rx SC Creation................... 0
   Tx SC Creation................... 0
```

```
   Rx SA Installation............... 0
   Tx SA Installation............... 0

MKPDU Failures
   MKPDU Tx......................... 0
   MKPDU Rx Validation.............. 0
   MKPDU Rx Bad Peer MN............. 0
   MKPDU Rx Non-recent Peerlist MN.. 0
```

# EAP-TLS を使用した MACsec MKA に関する情報

MACsec MKA はスイッチ間リンクでサポートされます。Extensible Authentication Protocol（EAP-TLS）による IEE 802.1X ポートベース認証を使用して、デバイスのアップリンク ポート間で MACsec MKA を設定できます。EAP-TLS は相互認証を許可し、MSK（マスター セッションキー）を取得します。そのキーから、MKA 操作用の接続アソシエーションキー（CAK）が取得されます。デバイスの証明書は、AAA サーバへの認証用に、EAP-TLS を使用して伝送されます。

## EAP-TLS を使用した MACsec MKA の前提条件

- 認証局（CA）サーバがネットワークに設定されていることを確認します。
- CA 証明書を生成します。
- Cisco Identity Services Engine（ISE）リリース 2.0 が設定されていることを確認します。
- 両方の参加デバイス（CA サーバと Cisco Identity Services Engine（ISE））が Network Time Protocol（NTP）を使用して同期されていることを確認します。時間がすべてのデバイスで同期されていないと、証明書は検証されません。
- 802.1x 認証と AAA がデバイスに設定されていることを確認します。

## EAP-TLS を使用した MACsec MKA の制限事項

- MKA は、ポート チャネルではサポートされていません。
- MKA は、高可用性とローカル認証ではサポートされていません。
- MKA と EAPTLS は、無差別 PVLAN プライマリポートではサポートされません。
- EAP-TLS を使用して MACsec MKA を設定している間、MACsec セキュアチャネル暗号化カウンタは最初のキー再生成の前に増加しません。

# Cisco TrustSec の概要

次の表に、TrustSec がイネーブルになった Cisco スイッチで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability リリースによって、サポートされるスイッチの数および各スイッチでサポートされる TrustSec 機能の数は増加しています。

| Cisco TrustSec の機能 | 説明 |
|---|---|
| 802.1AE タギング（MACSec） | IEEE 802.1AE に基づくワイヤレート ホップ単位レイヤ 2 暗号化のプロトコル。<br>MACSec 対応デバイス間において、パケットは送信デバイスからの出力で暗号化され、受信デバイスへの入力で復号化されます。デバイス内では平文です。<br>この機能は、TrustSec ハードウェア対応デバイス間だけで利用できます。 |
| エンドポイント アドミッション コントロール（EAC） | EAC は、TrustSec ドメインに接続しているエンドポイント ユーザまたはデバイスの認証プロセスです。通常、EAC はアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可に成功すると、ユーザまたはデバイスに対してセキュリティ グループ タグが割り当てられます。現在、EAC は 802.1X、MAC 認証バイパス（MAB）、および Web 認証プロキシ（WebAuth）とすることができます。 |
| ネットワーク デバイス アドミッション コントロール（NDAC） | NDAC は、TrustSec ドメイン内の各ネットワーク デバイスがピア デバイスのクレデンシャルおよび信頼性を確認できる認証プロセスです。NDAC は、IEEE 802.1X ポート ベースの認証に基づく認証フレームワークを利用し、EAP 方式として EAP-FAST を使用します。NDAC プロセスの認証および許可に成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションとなります。 |
| セキュリティ アソシエーション プロトコル（SAP） | NDAC 認証のあと、セキュリティ アソシエーション プロトコル（SAP）は、その後の TrustSec ピア間の MACSec リンク暗号化のキーおよび暗号スイートについて、自動的にネゴシエーションを行います。SAP は IEEE 802.11i で定義されます。 |
| セキュリティ グループ タグ（SGT） | SGT は、TrustSec ドメイン内の送信元のセキュリティ分類を示す 16 ビットの単一ラベルです。イーサネット フレームまたは IP パケットに追加されます。 |

| Cisco TrustSec の機能 | 説明 |
|---|---|
| SGT 交換プロトコル（SXP） | Security Group Tag Exchange Protocol（SXP）。SXP を使用すると、TrustSec にハードウェアで対応していないデバイスが Cisco Identity Services Engine（ISE）または Cisco Secure アクセス コントロール システム（ACS）から認証されたユーザとデバイスの SGT 属性を受信できます。デバイスは、次にセキュリティ グループ アクセス コントロール リスト（SGACL）強制のために、送信元トラフィックをタグ付けする TrustSec にハードウェアで対応しているデバイスに、sourceIP-to-SGT バインディングを転送できます。 |

リンクの両端で 802.1AE MACsec をサポートしている場合、SAP ネゴシエーションが実行されます。サプリカントとオーセンティケータの間で EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティパラメータの交換、およびキーの管理が実行されます。これらの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョンとライセンスおよびリンク ハードウェア サポートに応じて、SAP ネゴシエーションは次の動作モードの 1 つを使用できます。

- Galois Counter Mode（GCM）：認証と暗号化
- GCM authentication（GMAC）：GCM 認証、暗号化なし
- No Encapsulation：カプセル化なし（クリア テキスト）
- null：カプセル化、認証または暗号化なし

# MACsec 暗号化の設定方法

## MKA および MACsec の設定

### MACsec MKA のデフォルト設定

MACsec はディセーブルです。MKA ポリシーは設定されていません。

# MKA ポリシーの設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **mka policy** *policy name* | MKA ポリシーを指定し、MKA ポリシー コンフィギュレーション モードを開始します。ポリシー名の長さは最大で 16 文字です。<br>（注） MKA ポリシー内のデフォルトの MACsec 暗号スイートは常に「GCM-AES-128」です。デバイスが「GCM-AES-128」および「GCM-AES-256」の両方の暗号方式をサポートしている場合は、ユーザ定義の MKA ポリシーを定義して使用し、必要に応じて、128 および 256 ビット両方の暗号を含めるか、または 256 ビットのみの暗号を含めることを強くお勧めします。 |
| ステップ 3 | **send-secure-announcements** | セキュアなアナウンスを有効にしました。<br>（注） デフォルトでは、セキュアなアナウンスは無効になっています。 |
| ステップ 4 | **key-server** *priority* | MKA キー サーバ オプションを設定し、プライオリティを設定します（0 ～ 255 の間）。<br>（注） キーサーバプライオリティの値を 255 に設定した場合、ピアはキー サーバになることはできません。キーサーバの優先順位の値は MKA PSK に対してのみ有効です。 MKA EAPTLS に対しては有効ではありません。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **include-icv-indicator** | MKPDU の ICV インジケータを有効にします。ICV インジケータを無効にするには、このコマンドの **no** 形式を使用します（**no include-icv-indicator**）。 |
| ステップ 6 | **macsec-cipher-suite** *gcm-aes-128* | 128 ビット暗号により SAK を取得するための暗号スイートを設定します。 |
| ステップ 7 | **confidentiality-offset** オフセット値 | 各物理インターフェイスに機密性（暗号化）オフセットを設定します。<br>（注） オフセット値は、0、30、または50を指定できます。クライアントで Anyconnect を使用している場合は、オフセット 0 を使用することをお勧めします。 |
| ステップ 8 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show mka policy** | 入力内容を確認します。 |

### 例

次に、MKA ポリシーを設定する例を示します。

```
Switch(config)# mka policy mka_policy
Switch(config-mka-policy)# key-server priority 200
Switch(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Switch(config-mka-policy)# confidentiality-offset 30
Switch(config-mka-policy)# end
```

## スイッチからホストへの MACsec の暗号化設定

音声用に 1 つの MACsec セッションとデータ用に 1 つの MACsec セッションが存在するインターフェイスで MACsec を設定するには、次の手順を実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Switch>enable` | 特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configureterminal**<br>例：<br>`Switch>configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface***interface-id* | MACsec インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理インターフェイスでなければなりません。 |
| ステップ 4 | **switchport access vlan***vlan-id* | このポートのアクセス VLAN を設定します。 |
| ステップ 5 | **switchport mode access** | インターフェイスをアクセス ポートとして設定します。 |
| ステップ 6 | **macsec** | インターフェイスで 802.1ae MACsec をイネーブルにします。macsec コマンドを使用すると、スイッチからホストへのリンク（ダウンリンクポート）でのみ MKA MACsec が有効になります。 |
| ステップ 7 | **authentication event linksec fail action authorize vlan** *vlan-id* | （任意）認証の試行に失敗した後で、ポート上の制限付き VLAN を許可することによって、ユーザ証明書が認識されない認証リンク セキュリティの問題をスイッチが処理することを指定します。 |
| ステップ 8 | **authentication host-mode multi-domain** | ホストと音声デバイスの両方が、802.1x で許可されたポート上で認証されるように、ポート上の認証マネージャ モードを設定します。設定されていない場合、デフォルトのホスト モードはシングルです。 |
| ステップ 9 | **authentication linksec policy must-secure** | LinkSec セキュリティ ポリシーを設定して、ピアを利用できる場合に、MACsec でセッションをセキュアにします。設定されていない場合、デフォルト値は *should secure* です。 |
| ステップ 10 | **authentication port-control auto** | ポート上で 802.1x 認証をイネーブルにします。スイッチとクライアント間の認証交換に基づいてポートが許可ス |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | テートまたは無許可ステートに変わります。 |
| ステップ 11 | **authentication periodic** | このポートの再認証を有効または無効にします。 |
| ステップ 12 | **authentication timer reauthenticate** | 1 から 65535 までの値（秒）を入力します。サーバから再認証タイムアウト値を取得します。デフォルトの再認証時間は 3600 秒です。 |
| ステップ 13 | **authentication violation protect** | 新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続されたあとに新しいデバイスがそのポートに接続された場合に、予期しない着信 MAC アドレスを破棄するようポートを設定します。設定されていない場合、デフォルトではポートをシャット ダウンします。 |
| ステップ 14 | **mka policy** *policy name* | 既存の MKA プロトコル ポリシーをインターフェイスに適用し、インターフェイス上で MKA をイネーブルにします。MKA ポリシーを設定しなかった場合（**mka policy** グローバル コンフィギュレーション コマンドの入力による）。 |
| ステップ 15 | **dot1x pae authenticator** | ポートを 802.1x ポート アクセス エンティティ（PAE）オーセンティケータとして設定します。 |
| ステップ 16 | **spanning-tree portfast** | 関連するすべての VLAN 内の特定のインターフェイスで、スパニングツリー Port Fast をイネーブルにします。Port Fast機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。 |
| ステップ 17 | **end**<br>例：<br>`Switch(config)#end` | 特権 EXEC モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 18 | **show authentication session interface** *interface-id* | 許可されたセッションのセキュリティステータスを確認します。 |
| ステップ 19 | **show authentication session interface** *interface-id* details | 承認されたセッションのセキュリティステータスの詳細を確認します。 |
| ステップ 20 | **show macsec interface** *interface-id* | インターフェイスの MacSec ステータスを確認します。 |
| ステップ 21 | **show mka sessions** | 確立された mka セッションを確認します。 |
| ステップ 22 | **copy running-config startup-config**<br>例：<br>`Switch#copy running-config startup-config` | （任意）コンフィギュレーションファイルに設定を保存します。 |

# PSK を使用した MACsec MKA の設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **key chain** *key-chain-name* **macsec** | キー チェーンを設定して、キー チェーン コンフィギュレーション モードを開始します。 |
| ステップ 3 | **key** *hex-string* | キーチェーン内の各キーの固有識別子を設定し、キーチェーンのキー コンフィギュレーション モードを開始します。<br>（注） 128 ビット暗号の場合は、32 文字の 16 進数キー文字列を使用します。256 ビット暗号の場合は、64 文字の 16 進数キー文字列を使用します。 |
| ステップ 4 | **cryptographic-algorithm** *{gcm-aes-128 \| gcm-aes-256}* | 128 ビットまたは 256 ビット暗号による暗号化認証アルゴリズムを設定します。 |
| ステップ 5 | **key-string** *{ [0\|6\|7] pwd-string \| pwd-string}* | キー文字列のパスワードを設定します。16 進数の文字のみを入力する必要があります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **lifetime local** [*start timestamp {hh::mm::ss \| day \| month \| year}*] [ **duration** *seconds* \| *end timestamp {hh::mm::ss \| day \| month \| year}*] | 事前共有キーの有効期間を設定します。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |

例

次に例を示します。

```
Switch(config)# Key chain keychain1 macsec
Switch(config-key-chain)# key 1000
Switch(config-keychain-key)# cryptographic-algorithm gcm-aes-128
Switch(config-keychain-key)# key-string 12345678901234567890123456789012
Switch(config-keychain-key)# lifetime local 12:12:00 July 28 2016 12:19:00
July 28 2016
Switch(config-keychain-key)# end
```

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

（注） セッション間のトラフィックのドロップを回避するには、**mka pre-shared-key key-chain** コマンドの前に **mka policy** コマンドを設定する必要があります。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id* | インターフェイスコンフィギュレーション モードを開始します。 |
| ステップ 3 | **macsec network-link** | インターフェイス上でMACsecをイネーブルにします。<br>（注） **macsec network-link** コマンドは、ダウンリンクポートのMKAセッションをブロックしません。代わりに、**macsec** コマンドを使用してください。 |
| ステップ 4 | **mka policy** *policy-name* | MKA ポリシーを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **mka pre-shared-key key-chain** *key-chain name* | MKA 事前共有キーのキーチェーン名を設定します。<br>（注） MKA 事前共有キーは、物理インターフェイスまたはサブインターフェイスで設定できますが、両方で設定することはできません。 |
| ステップ 6 | **macsec replay-protection window-size** *frame number* | リプレイ保護の MACsec ウィンドウ サイズを設定します。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |

### 例

次に例を示します。

```
Switch(config)# interface GigabitEthernet 0/0/0
Switch(config-if)# mka policy mka_policy
Switch(config-if)# mka pre-shared-key key-chain key-chain-name
Switch(config-if)# macsec replay-protection window-size 10
Switch(config-if)# end
```

### 次のタスク

セッションの実行中に MKA PSK が設定されたインターフェイスで MKA ポリシーを変更することは推奨されません。ただし、変更が必要な場合は、次のようにポリシーを再設定する必要があります。

1. **no macsec network-link** コマンドを使用して、各参加ノードの macsec network-link 設定を削除し、既存のセッションを無効にします。
2. **mka policy policy-name** コマンドを使用して、各参加ノードのインターフェイスで MKA ポリシーを設定します。
3. **macsec network-link**コマンドを使用して、各参加ノードで新しいセッションを有効にします。

# EAP-TLS を使用した MACsec MKA の設定

ポイントツーポイント リンクで MKA による MACsec を設定するには、次のタスクを実行します。

- 証明書登録の設定

- キー ペアの生成
- SCEP 登録の設定
- 証明書の手動設定

- 認証ポリシーの設定
- EAP-TLS プロファイルおよび IEEE 802.1x クレデンシャルの設定
- インターフェイスでの EAP-TLS を使用した MKA MACsec の設定

# リモート認証

## キー ペアの生成

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **crypto key generate rsa label** *label-name* **general-keys modulus** *size* | 署名および暗号化用に RSA キー ペアを作成します。<br>label キーワードを使用すると、各キー ペアにラベルを割り当てることもできます。このラベルは、キー ペアを使用するトラストポイントによって参照されます。ラベルを割り当てなかった場合、キー ペアには <Default-RSA-Key> というラベルが自動的に付けられます。<br>追加のキーワードを使用しない場合、このコマンドは汎用 RSA キー ペアを 1 つ生成します。係数が指定されていない場合は、デフォルトのキー係数である 1024 が使用されます。その他の係数サイズを指定するには、modulus キーワードを使用します。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show authentication session interface** *interface-id* | 許可されたセッションのセキュリティ ステータスを確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

## SCEP による登録の設定

Simple Certificate Enrollment Protocol（SCEP）は、HTTP を使用して認証局（CA）または登録局（RA）と通信する、シスコが開発した登録プロトコルです。SCEP は、要求および証明書の送受信用に最も一般的に使用される方式です。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **crypto pki trustpoint** *server name* | トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。 |
| ステップ 3 | **enrollment url** *url name pem* | デバイスが証明書要求を送信する CA の URL を指定します。<br>URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。<br>pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。 |
| ステップ 4 | **rsakeypair** *label* | 証明書に関連付けるキーペアを指定します。<br>（注） **rsakeypair** 名は、信頼ポイント名と一致している必要があります。 |
| ステップ 5 | **serial-number none** | **none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。 |
| ステップ 6 | **ip-address none** | **none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。 |
| ステップ 7 | **revocation-check crl** | ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。 |
| ステップ 8 | **auto-enroll** *percent* **regenerate** | 自動登録をイネーブルにします。これにより、クライアントは CA から自動 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 的にロールオーバー証明書を要求できます。<br><br>自動登録がイネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。<br><br>デフォルトでは、デバイスのドメインネームシステム（DNS）名だけが証明書に含められます。<br><br>現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、percent 引数を使用します。<br><br>名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、regenerate キーワードを使用します。<br><br>ロールオーバー中のキーペアがエクスポート可能な場合、新しいキーペアもエクスポート可能です。次のコメントがトラストポイントコンフィギュレーションに表示され、キーペアがエクスポート可能かどうかが示されます。「! RSA key pair associated with trustpoint is exportable.」<br><br>新しいキーペアは、セキュリティ上の問題に対処するために生成することを推奨します。 |
| **ステップ 9** | **crypto pki authenticate** *name* | CA 証明書を取得して、認証します。 |
| **ステップ 10** | **exit** | グローバル コンフィギュレーション モードを終了します。 |
| **ステップ 11** | **show crypto pki certificate** *trustpoint name* | 信頼ポイントの証明書に関する情報を表示します。 |

## 登録の手動設定

CA が SCEP をサポートしない場合、またはルータと CA 間のネットワーク接続が不可能な場合。手動での証明書登録を設定するには、次の作業を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **crypto pki trustpoint** *server name* | トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーションモードを開始します。 |
| ステップ 3 | **enrollment url** *url name pem* | デバイスが証明書要求を送信する CA の URL を指定します。<br>URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。<br>pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。 |
| ステップ 4 | **rsakeypair** *label* | 証明書に関連付けるキーペアを指定します。 |
| ステップ 5 | **serial-number none** | **none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。 |
| ステップ 6 | **ip-address none** | **none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。 |
| ステップ 7 | **revocation-check crl** | ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。 |
| ステップ 8 | **exit** | グローバル コンフィギュレーション モードから抜けます。 |
| ステップ 9 | **crypto pki authenticate** *name* | CA 証明書を取得して、認証します。 |
| ステップ 10 | **crypto pki enroll** *name* | 証明書要求を生成し、証明書サーバにコピーおよびペーストするために要求を表示します。<br>プロンプトが表示されたら、登録情報を入力します。たとえば、証明書要求 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | にデバイスの FQDN および IP アドレスを含めるかどうかを指定します。<br><br>コンソール端末に対して証明書要求を表示するかについても選択できます。<br><br>必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。 |
| ステップ 11 | **crypto pki import** *name* **certificate** | 許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。<br><br>デバイスは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場合、拡張子「-sign.crt」および「-encr.crt」が使用されます。<br><br>デバイスは、受信したファイルを解析して証明書を検証し、証明書をスイッチの内部証明書データベースに挿入します。<br><br>（注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキーペアのいずれも使用しません。 |
| ステップ 12 | **exit** | グローバル コンフィギュレーション モードを終了します。 |
| ステップ 13 | **show crypto pki certificate** *trustpoint name* | 信頼ポイントの証明書に関する情報を表示します。 |
| ステップ 14 | **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

## 802.1x 認証の有効化と AAA の設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 4 | **dot1x system-auth-control** | デバイス上で 802.1X を有効にします。 |
| ステップ 5 | **radius server** *name* | RADIUS サーバの設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。 |
| ステップ 6 | **address** *ip-address* **auth-port** *port-number* **acct-port** *port-number* | RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。 |
| ステップ 7 | **automate-tester username** *username* | RADIUS サーバの自動テスト機能を有効にします。<br>このようにすると、デバイスは RADIUS サーバにテスト認証メッセージを定期的に送信し、サーバからの RADIUS 応答を待機します。成功メッセージは必須ではありません。認証失敗であっても、サーバが稼働していることを示しているため問題ありません。 |
| ステップ 8 | **key** *string* | デバイスと RADIUS サーバとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。 |
| ステップ 9 | **radius-server deadtime** *minutes* | いくつかのサーバが使用不能になったときの RADIUS サーバの応答時間を短くし、使用不能になったサーバがすぐにスキップされるようにします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 10 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 11 | **aaa group server radius** *group-name* | 異なる RADIUS サーバホストを別々のリストと方式にグループ化し、サーバグループ コンフィギュレーション モードを開始します。 |
| ステップ 12 | **server** *name* | RADIUS サーバ名を割り当てます。 |
| ステップ 13 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 14 | **aaa authentication dot1x default group** *group-name* | IEEE 802.1x 用にデフォルトの認証サーバ グループを設定します。 |
| ステップ 15 | **aaa authorization network default group** *group-name* | ネットワーク認証のデフォルトグループを設定します。 |

## EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **eap profile** *profile-name* | EAP プロファイルを設定し、EAP プロファイル コンフィギュレーション モードを開始します。 |
| ステップ 4 | **method tls** | デバイスで EAP-TLS 方式を有効にします。 |
| ステップ 5 | **pki-trustpoint** *name* | デフォルトの PKI トラストポイントを設定します。 |
| ステップ 6 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 7 | **dot1x credentials** *profile-name* | 802.1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。 |
| ステップ 8 | **username** *username* | 認証ユーザ ID を設定します。 |
| ステップ 9 | **pki-trustpoint** *name* | デフォルトの PKI トラストポイントを設定します。 |
| ステップ 10 | **end** | 特権 EXEC モードに戻ります。 |

## インターフェイスでの 802.1x MACsec MKA 設定の適用

EAP-TLS を使用して MACsec MKA をインターフェイスに適用するには、次のタスクを実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id* | MACsec インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理インターフェイスでなければなりません。 |
| ステップ 3 | **macsec network-link** | インターフェイス上で MACsec をイネーブルにします。 |
| ステップ 4 | **authentication periodic** | このポートの再認証をイネーブルにします。 |
| ステップ 5 | **authentication timer reauthenticate interval** | 再認証間隔を設定します。 |
| ステップ 6 | **access-session host-mode multi-domain** | ホストにインターフェイスへのアクセスを許可します。 |
| ステップ 7 | **access-session closed** | インターフェイスへの事前認証アクセスを防止します。 |
| ステップ 8 | **access-session port-control auto** | ポートの認可状態を設定します。 |
| ステップ 9 | **dot1x pae both** | ポートを 802.1X ポート アクセス エンティティ（PAE）のサプリカントおよ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | びオーセンティケータとして設定します。 |
| ステップ 10 | **dot1x credentials profile** | 802.1x クレデンシャル プロファイルをインターフェイスに割り当てます。 |
| ステップ 11 | **dot1x supplicant eap profile** *name* | EAP-TLS プロファイルをインターフェイスに割り当てます。 |
| ステップ 12 | **service-policy type control subscriber** *control-policy name* | インターフェイスに加入者制御ポリシーを適用します。 |
| ステップ 13 | **exit** | 特権 EXEC モードに戻ります。 |
| ステップ 14 | **show macsec interface** | インターフェイスの MACsec の詳細を表示します。 |
| ステップ 15 | **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

## ローカル認証

### ローカル認証を使用した EAP クレデンシャルの設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 4 | **aaa local authentication default authorization default** | デフォルトのローカル認証およびデフォルトのローカル認証方法を設定します。 |
| ステップ 5 | **aaa authentication dot1x default local** | IEEE 802.1x 用にデフォルトのローカルユーザ名認証リストを設定します。 |
| ステップ 6 | **aaa authorization network default local** | ローカル ユーザの認可方式リストを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 7 | **aaa authorization credential-download default local** | ローカル クレデンシャルの使用に関する認可方式リストを設定します。 |
| ステップ 8 | **exit** | 特権 EXEC モードに戻ります。 |

## ローカル EAP-TLS 認証と認証プロファイルの設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 4 | **dot1x credentials** *profile-name* | dot1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。 |
| ステップ 5 | **username** *name* **password** *password* | 認証のユーザ ID およびパスワードを設定します。 |
| ステップ 6 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 7 | **aaa attribute list** *list-name* | （任意）AAA 属性リスト定義を設定し、属性リスト コンフィギュレーション モードを開始します。 |
| ステップ 8 | **aaa attribute type linksec-policy must-secure** | （任意）AAA 属性タイプを指定します。 |
| ステップ 9 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 10 | **username** *name* **aaa attribute list** *name* | （任意）ユーザ ID に AAA 属性リストを指定します。 |
| ステップ 11 | **end** | 特権 EXEC モードに戻ります。 |

## SCEP による登録の設定

Simple Certificate Enrollment Protocol（SCEP）は、HTTP を使用して認証局（CA）または登録局（RA）と通信する、シスコが開発した登録プロトコルです。SCEP は、要求および証明書の送受信用に最も一般的に使用される方式です。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **crypto pki trustpoint** *server name* | トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーションモードを開始します。 |
| ステップ 4 | **enrollment url** *url name pem* | デバイスが証明書要求を送信する CA の URL を指定します。<br>URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。<br>pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。 |
| ステップ 5 | **rsakeypair** *label* | 証明書に関連付けるキーペアを指定します。<br>（注） **rsakeypair** 名は、信頼ポイント名と一致している必要があります。 |
| ステップ 6 | **serial-number none** | **none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。 |
| ステップ 7 | **ip-address none** | **none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 8 | **revocation-check crl** | ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。 |
| ステップ 9 | **auto-enroll** *percent* **regenerate** | 自動登録をイネーブルにします。これにより、クライアントは CA から自動的にロールオーバー証明書を要求できます。<br>自動登録がイネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。<br>デフォルトでは、デバイスのドメインネームシステム（DNS）名だけが証明書に含められます。<br>現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、percent 引数を使用します。<br>名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、regenerate キーワードを使用します。<br>ロールオーバー中のキーペアがエクスポート可能な場合、新しいキーペアもエクスポート可能です。次のコメントがトラストポイントコンフィギュレーションに表示され、キーペアがエクスポート可能かどうかが示されます。「! RSA key pair associated with trustpoint is exportable.」<br>新しいキーペアは、セキュリティ上の問題に対処するために生成することを推奨します。 |
| ステップ 10 | **crypto pki authenticate** *name* | CA 証明書を取得して、認証します。 |
| ステップ 11 | **exit** | グローバル コンフィギュレーション モードを終了します。 |
| ステップ 12 | **show crypto pki certificate** *trustpoint name* | 信頼ポイントの証明書に関する情報を表示します。 |

## 登録の手動設定

CA が SCEP をサポートしない場合、またはルータと CA 間のネットワーク接続が不可能な場合。手動での証明書登録を設定するには、次の作業を実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **crypto pki trustpoint** *server name* | トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーションモードを開始します。 |
| ステップ 4 | **enrollment url** *url name pem* | デバイスが証明書要求を送信する CA の URL を指定します。<br>URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。<br>pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。 |
| ステップ 5 | **rsakeypair** *label* | 証明書に関連付けるキーペアを指定します。 |
| ステップ 6 | **serial-number none** | **none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。 |
| ステップ 7 | **ip-address none** | **none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。 |
| ステップ 8 | **revocation-check crl** | ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。 |
| ステップ 9 | **exit** | グローバル コンフィギュレーション モードから抜けます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 10 | **crypto pki authenticate** *name* | CA 証明書を取得して、認証します。 |
| ステップ 11 | **crypto pki enroll** *name* | 証明書要求を生成し、証明書サーバにコピーおよびペーストするために要求を表示します。<br>プロンプトが表示されたら、登録情報を入力します。たとえば、証明書要求にデバイスの FQDN および IP アドレスを含めるかどうかを指定します。<br>コンソール端末に対して証明書要求を表示するかについても選択できます。<br>必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。 |
| ステップ 12 | **crypto pki import** *name* **certificate** | 許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。<br>デバイスは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場合、拡張子「-sign.crt」および「-encr.crt」が使用されます。<br>デバイスは、受信したファイルを解析して証明書を検証し、証明書をスイッチの内部証明書データベースに挿入します。<br>（注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキーペアのいずれも使用しません。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 13 | **exit** | グローバル コンフィギュレーション モードから抜けます。 |
| ステップ 14 | **show crypto pki certificate** *trustpoint name* | 信頼ポイントの証明書に関する情報を表示します。 |
| ステップ 15 | **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

## EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **eap profile** *profile-name* | EAP プロファイルを設定し、EAP プロファイル コンフィギュレーション モードを開始します。 |
| ステップ 4 | **method tls** | デバイスで EAP-TLS 方式を有効にします。 |
| ステップ 5 | **pki-trustpoint** *name* | デフォルトの PKI トラストポイントを設定します。 |
| ステップ 6 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 7 | **dot1x credentials** *profile-name* | 802.1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。 |
| ステップ 8 | **username** *username* | 認証ユーザ ID を設定します。 |
| ステップ 9 | **pki-trustpoint** *name* | デフォルトの PKI トラストポイントを設定します。 |
| ステップ 10 | **end** | 特権 EXEC モードに戻ります。 |

## インターフェイスでの 802.1x MKA MACsec 設定の適用

EAP-TLS を使用して MKA MACsec をインターフェイスに適用するには、次のタスクを実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id* | MACsec インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。インターフェイスは物理インターフェイスでなければなりません。 |
| ステップ 4 | **macsec** | インターフェイス上で MACsec をイネーブルにします。 |
| ステップ 5 | **authentication periodic** | このポートの再認証をイネーブルにします。 |
| ステップ 6 | **authentication timer reauthenticate interval** | 再認証間隔を設定します。 |
| ステップ 7 | **access-session host-mode multi-domain** | ホストにインターフェイスへのアクセスを許可します。 |
| ステップ 8 | **access-session closed** | インターフェイスへの事前認証アクセスを防止します。 |
| ステップ 9 | **access-session port-control auto** | ポートの認可状態を設定します。 |
| ステップ 10 | **dot1x pae both** | ポートを 802.1X ポート アクセス エンティティ（PAE）のサプリカントおよびオーセンティケータとして設定します。 |
| ステップ 11 | **dot1x credentials profile** | 802.1x クレデンシャル プロファイルをインターフェイスに割り当てます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 12 | **dot1x authenticator eap profile** *name* | EAP-TLS オーセンティケータ プロファイルをインターフェイスに割り当てます。 |
| ステップ 13 | **dot1x supplicant eap profile** *name* | EAP-TLS サプリカントプロファイルをインターフェイスに割り当てます。 |
| ステップ 14 | **service-policy type control subscriber** *control-policy name* | インターフェイスに加入者制御ポリシーを適用します。 |
| ステップ 15 | **exit** | 特権 EXEC モードに戻ります。 |
| ステップ 16 | **show macsec interface** | インターフェイスの MACsec の詳細を表示します。 |
| ステップ 17 | **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

## EAP-TLS を使用した MACsec MKA の確認

EAP-TLS を使用して MACsec MKA の設定を確認するには、次のように **show** コマンドを使用します。以下に、**show** コマンドの出力例を示します。

**show mka sessions** コマンドは、アクティブな MACsec Key Agreement（MKA）プロトコルのセッションの概要を表示します。

```
Device# show mka sessions

  Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=========================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server

Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN

=========================================================================================
Te0/1/3        74a2.e625.4413/0013 *DEFAULT POLICY* NO                YES

19             74a2.e625.4c22/0012 1                Secured
1000000000000000000000000000000000000000000000000000000000000000
```

**show macsec status interface** *interface-id* は、指定されたインターフェイスの MACsec ステータス情報を表示します。

```
Device# show macsec status interface te0/1/2

  Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256
  Cipher:                   GCM-AES-128
```

```
  Confidentiality Offset:   0
  Replay Window:            64
  Delay Protect Enable:     FALSE
  Access Control:           must-secure

Transmit SC:
  SCI:                      74A2E6254C220012
  Transmitting:             TRUE
Transmit SA:
  Next PN:                  412
  Delay Protect AN/nextPN:  99/0

Receive SC:
  SCI:                      74A2E62544130013
  Receiving:                TRUE
Receive SA:
  Next PN:                  64
  AN:                       0
  Delay Protect AN/LPN:     0/0
```

**show access-session interface** *interface-id* **details** は、指定されたインターフェイスのアクセス セッションに関する詳細情報を表示します。

```
Device# show access-session interface te1/0/1 details

   Interface:  TenGigabitEthernet1/0/1
             IIF-ID:  0x17298FCD
         MAC Address:  f8a5.c592.13e4
        IPv6 Address:  Unknown
        IPv4 Address:  Unknown
           User-Name:  DOT1XCRED
              Status:  Authorized
              Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  000000000000000BB72E8AFA
      Acct Session ID:  Unknown
              Handle:  0xc3000001
       Current Policy:  MUSTS_1


Local Policies:
 Security Policy:  Must Secure
      Security Status:  Link Secured

Server Policies:


Method status list:
       Method           State
     dot1xSup           Authc Success
        dot1x           Authc Success
```

# Cisco TrustSec MACsec の設定

## 手動モードでの Cisco TrustSec スイッチ間リンク セキュリティの設定

### 始める前に

インターフェイスの Cisco TrustSec を手動で設定する場合は、次のような使用上の注意事項、および制約事項を考慮してください。

- SAP パラメータが定義されていない場合、Cisco TrustSec カプセル化または暗号化は行われません。
- SAP 動作モードとして GCM を選択すると、シスコの MACsec 暗号化ソフトウェア ライセンスが必要です。必要なライセンスなしで GCM を選択した場合、インターフェイスはリンク ダウン状態になります。
- これらの保護レベルは、SAP の Pairwise Master Key（sap pmk）を設定する場合にサポートされます。
  - SAP が設定されていない：保護は行われません。
  - **sap mode-list gcm-encrypt gmac no-encap**：保護が望ましいが必須ではない。
  - **sap mode-list gcm-encrypt gmac**：機密性が推奨され、整合性が必須。保護はサプリカントの設定に応じてサプリカントによって選択されます。
  - **sap mode-list gmac**：整合性のみ。
  - **sap mode-list gcm-encrypt**：機密性が必須。
  - **sap mode-list gmac gcm-encrypt**：整合性が必須であり推奨される。機密性は任意。
- MKA から Cisco TrustSec SAP（またはその逆）に設定を変更する前に、インターフェイスの設定を削除することを推奨します。

別の Cisco TrustSec デバイスへのインターフェイスで Cisco TrustSec を手動で設定するには、特権 EXEC モードで次の手順を実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`Switch# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例： | （注） インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Switch(config)# interface tengigabitethernet 1/1/2` | |
| ステップ 3 | **cts manual**<br>例：<br>`Switch(config-if)# cts manual` | Cisco TrustSec 手動コンフィギュレーション モードを開始します。 |
| ステップ 4 | **sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]]<br>例：<br>`Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap` | （任意）SAP の Pairwise Master Key（PMK）と動作モードを設定します。Cisco TrustSec の手動モードでは、SAP はデフォルトでディセーブルになっています。<br>• *key*：文字数が偶数個で最大 32 文字の 16 進値。<br>SAP 動作モードのオプションは次のとおりです。<br>• **gcm-encrypt**：認証および暗号化<br>（注） ソフトウェア ライセンスが MACsec 暗号化をサポートする場合、MACsec の認証と暗号化にこのモードを選択します。<br>• **gmac**：認証、暗号化なし<br>• **no-encap**：カプセル化なし<br>• **null**：カプセル化、認証または暗号化なし<br>（注） インターフェイスでデータ リンク暗号化を使用できない場合は、デフォルトおよび唯一使用可能な SAP 動作モードは **no-encap** です。SGT はサポートされません。 |
| ステップ 5 | **no propagate sgt**<br>例：<br>`Switch(config-if-cts-manual)# no propagate sgt` | ピアが SGT を処理できない場合、このコマンドの **no** 形式を使用します。**no propagate sgt** コマンドを使用すると、インターフェイスからピアに SGT が送信されなくなります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **exit**<br>例：<br>`Switch(config-if-cts-manual)# exit` | Cisco TrustSec 802.1x インターフェイス コンフィギュレーション モードを終了します。 |
| ステップ 7 | **end**<br>例：<br>`Switch(config-if)# end` | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show cts interface** [*interface-id* \| **brief** \| **summary**] | （任意）TrustSec 関連のインターフェイス特性を表示して、設定を確認します。 |

### 例

次に、インターフェイスにCisco TrustSec認証を手動モードで設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# end
```

# MACsec 暗号化の設定例

## スイッチからホストへの MACsec の暗号化設定

音声用に 1 つの MACsec セッションとデータ用に 1 つの MACsec セッションが存在するインターフェイスで MACsec を設定するには、次の手順を実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Switch>enable` | 特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。 |
| ステップ 2 | **configureterminal**<br>例：<br>`Switch>configure terminal` | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **interface***interface-id* | MACsec インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。インターフェイスは物理インターフェイスでなければなりません。 |
| ステップ 4 | **switchport access vlan***vlan-id* | このポートのアクセス VLAN を設定します。 |
| ステップ 5 | **switchport mode access** | インターフェイスをアクセスポートとして設定します。 |
| ステップ 6 | **macsec** | インターフェイスで 802.1ae MACsec をイネーブルにします。macsec コマンドを使用すると、スイッチからホストへのリンク（ダウンリンクポート）でのみ MKA MACsec が有効になります。 |
| ステップ 7 | **authentication event linksec fail action authorize vlan** *vlan-id* | （任意）認証の試行に失敗した後で、ポート上の制限付き VLAN を許可することによって、ユーザ証明書が認識されない認証リンク セキュリティの問題をスイッチが処理することを指定します。 |
| ステップ 8 | **authentication host-mode multi-domain** | ホストと音声デバイスの両方が、802.1x で許可されたポート上で認証されるように、ポート上の認証マネージャ モードを設定します。設定されていない場合、デフォルトのホストモードはシングルです。 |
| ステップ 9 | **authentication linksec policy must-secure** | LinkSec セキュリティ ポリシーを設定して、ピアを利用できる場合に、MACsec でセッションをセキュアにします。設定されていない場合、デフォルト値は *should secure* です。 |
| ステップ 10 | **authentication port-control auto** | ポート上で 802.1x 認証をイネーブルにします。スイッチとクライアント間の認証交換に基づいてポートが許可ステートまたは無許可ステートに変わります。 |
| ステップ 11 | **authentication periodic** | このポートの再認証を有効または無効にします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 12 | **authentication timer reauthenticate** | 1 から 65535 までの値（秒）を入力します。サーバから再認証タイムアウト値を取得します。デフォルトの再認証時間は 3600 秒です。 |
| ステップ 13 | **authentication violation protect** | 新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続されたあとに新しいデバイスがそのポートに接続された場合に、予期しない着信 MAC アドレスを破棄するようポートを設定します。設定されていない場合、デフォルトではポートをシャット ダウンします。 |
| ステップ 14 | **mka policy** *policy name* | 既存の MKA プロトコル ポリシーをインターフェイスに適用し、インターフェイス上で MKA をイネーブルにします。MKA ポリシーを設定しなかった場合（**mka policy** グローバル コンフィギュレーション コマンドの入力による）。 |
| ステップ 15 | **dot1x pae authenticator** | ポートを 802.1x ポート アクセス エンティティ（PAE）オーセンティケータとして設定します。 |
| ステップ 16 | **spanning-tree portfast** | 関連するすべての VLAN 内の特定のインターフェイスで、スパニングツリー Port Fast をイネーブルにします。Port Fast機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。 |
| ステップ 17 | **end**<br>例：<br>`Switch(config)#end` | 特権 EXEC モードに戻ります。 |
| ステップ 18 | **show authentication session interface** *interface-id* | 許可されたセッションのセキュリティ ステータスを確認します。 |
| ステップ 19 | **show authentication session interface** *interface-id* details | 承認されたセッションのセキュリティ ステータスの詳細を確認します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 20 | **show macsec interface** *interface-id* | インターフェイスの MacSec ステータスを確認します。 |
| ステップ 21 | **show mka sessions** | 確立された mka セッションを確認します。 |
| ステップ 22 | **copy running-config startup-config**<br>例：<br>`Switch#copy running-config startup-config` | （任意）コンフィギュレーションファイルに設定を保存します。 |

# EAP-TLS を使用した MACsec MKA の設定例

## 例:：証明書の登録

```
Configure Crypto PKI Trustpoint:
  crypto pki trustpoint POLESTAR-IOS-CA
   enrollment terminal
   subject-name CN=ASR1000x1@polestar.com, C=IN, ST=KA, OU=ENG,O=Polestar
   revocation-check none
   rsakeypair mkaioscarsa
   storage nvram:
  !
Manual Installation of Root CA certificate:
 crypto pki authenticate POLESTAR-IOS-CA
```

## 例：802.1x 認証の有効化と AAA の設定

```
aaa new-model
dot1x system-auth-control
radius server ISE
 address ipv4 <ISE ipv4 address> auth-port 1645 acct-port 1646
 automate-tester username dummy
 key dummy123
 radius-server deadtime 2
!
aaa group server radius ISEGRP
 server name ISE
!
aaa authentication dot1x default group ISEGRP
aaa authorization network default group ISEGRP
```

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

```
eap profile EAPTLS-PROF-IOSCA
 method tls
 pki-trustpoint POLESTAR-IOS-CA
```

```
!

dot1x credentials EAPTLSCRED-IOSCA
 username asr1000@polestar.company.com
 pki-trustpoint POLESTAR-IOS-CA
!
```

## 例：インターフェイスでの 802.1 X、PKI、および MACsec の設定の適用

```
interface TenGigabitEthernet0/1
 macsec network-link
 authentication periodic
 authentication timer reauthenticate <reauthentication interval>
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 dot1x pae both
 dot1x credentials EAPTLSCRED-IOSCA
 dot1x supplicant eap profile EAPTLS-PROF-IOSCA
 service-policy type control subscriber DOT1X_POLICY_RADIUS
```

# 例：Cisco TrustSec スイッチ間リンクセキュリティの設定

次に、Cisco TrustSec スイッチ間のセキュリティのためにシードおよび非シード デバイスに必要な設定を示します。リンク セキュリティ用に AAA および RADIUS を設定する必要があります。この例では、ACS-1 から ACS-3 は任意のサーバ名、cts-radius は Cisco TrustSec サーバです。

シード デバイスの設定

```
Switch(config)#aaa new-model
Switch(config)#radius server ACS-1
Switch(config-radius-server)#address ipv4 10.5.120.12 auth-port 1812 acct-port
 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#radius server ACS-2
Switch(config-radius-server)#address ipv4 10.5.120.14 auth-port 1812 acct-port
 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#radius server ACS-3
Switch(config-radius-server)#address ipv4 10.5.120.15 auth-port 1812 acct-port
 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#aaa group server radius cts-radius
Switch(config-sg-radius)#server name ACS-1
Switch(config-sg-radius)#server name ACS-2
Switch(config-sg-radius)#server name ACS-3
Switch(config-sg-radius)#exit
```

```
Switch(config)#aaa authentication login default none
Switch(config)#aaa authentication dot1x default group cts-radius
Switch(config)#aaa authorization network cts-radius group cts-radius
Switch(config)#aaa session-id common
Switch(config)#cts authorization list cts-radius
Switch(config)#dot1x system-auth-control

Switch(config)#interface gi1/1/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#cts manual
Switch(config-if-cts-manual)#sap pmk 0 abcd mode-list gcm-encrypt gmac

Switch(config-if-cts-manual)#exit
Switch(config-if)#exit

Switch(config)#interface gi1/1/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#cts manual
Switch(config-if-cts-manual)#sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
 gmac
Switch(config-if-cts-manual)#no propagate sgt
Switch(config-if-cts-manual)#exit
Switch(config-if)#exit

Switch(config)#radius-server vsa send authentication
Switch(config)#end
Switch#cts credentials id cts-36 password trustsec123
```

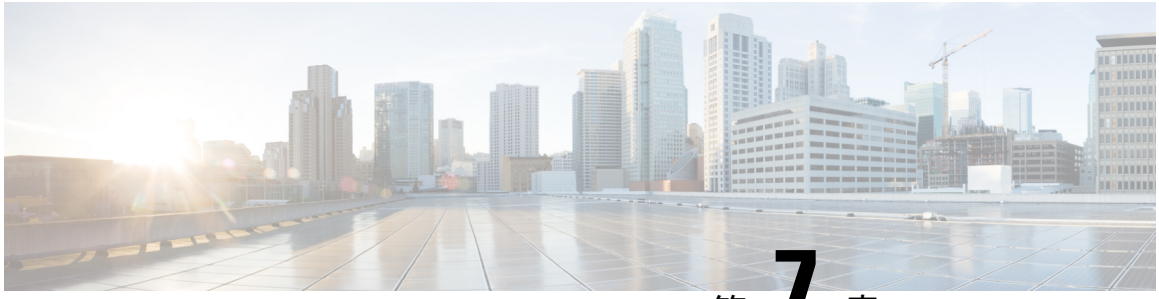
非シード デバイス

```
Switch(config)#aaa new-model
Switch(config)#aaa session-id common
Switch(config)#dot1x system-auth-control

Switch(config)#interface gi1/1/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#shutdown
Switch(config-if)#cts manual
Switch(config-if-cts-manual)#sap pmk 0 abcd mode-list gcm-encrypt gmac
Switch(config-if-cts-manual)#exit
Switch(config-if)#exit

Switch(config)#interface gi1/1/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#shutdown
Switch(config-if)#cts manual
Switch(config-if-cts-manual)#sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
 gmac
Switch(config-if-cts-manual)#no propagate sgt
Switch(config-if-cts-manual)#exit
Switch(config-if)#exit

Switch(config)#radius-server vsa send authentication
Switch(config)#cts credentials id cts-72 password trustsec123
Switch(config)#end
```



第 7 章

# ローカル認証および許可の設定


- ローカル認証および許可の設定方法 （139 ページ）
- ローカル認証および許可のモニタリング （141 ページ）
- その他の参考資料 （142 ページ）


# ローカル認証および許可の設定方法

## スイッチのローカル認証および許可の設定

ローカル モードで AAA を実装するようにスイッチを設定すると、サーバがなくても動作するように AAA を設定できます。この場合、スイッチは認証および許可の処理を行います。この設定ではアカウンティング機能は使用できません。

（注） AAA 方式を使用して HTTP アクセスに対しスイッチ のセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ローカル モードで AAA を実装するようにスイッチを設定して、サーバがなくても動作するように AAA を設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 4 | **aaa authentication login default local**<br>例：<br>デバイス(config)# **aaa authentication login default local** | ローカルユーザ名データベースを使用するログイン認証を設定します。**default** キーワードにより、ローカルユーザデータベース認証がすべてのポートに適用されます。 |
| ステップ 5 | **aaa authorization exec default local**<br>例：<br>デバイス(config)# **aaa authorization exec default local** | ユーザの AAA 許可を設定し、ローカルデータベースを確認して、そのユーザに EXEC シェルの実行を許可します。 |
| ステップ 6 | **aaa authorization network default local**<br>例：<br>デバイス(config)# **aaa authorization network default local** | ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。 |
| ステップ 7 | **username** *name* [ **privilege** *level*] { **password** *encryption-type password*}<br>例：<br>デバイス(config)# **username your_user_name privilege 1 password 7 secret567** | ローカルデータベースを入力し、ユーザ名ベースの認証システムを設定します。<br>ユーザごとにコマンドを繰り返し入力します。<br>• *name* には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。<br>• （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。<br>• *encryption-type* には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。<br>• *password* には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 |
| ステップ 8 | **end**<br>例：<br>`デバイス(config)# end` | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show running-config**<br>例：<br>`デバイス# show running-config` | 入力を確認します。 |
| ステップ 10 | **copy running-config startup-config**<br>例：<br>`デバイス# copy running-config startup-config` | （任意）コンフィギュレーションファイルに設定を保存します。 |

# ローカル認証および許可のモニタリング

ローカル認証および許可の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

# その他の参考資料

### エラー メッセージ デコーダ

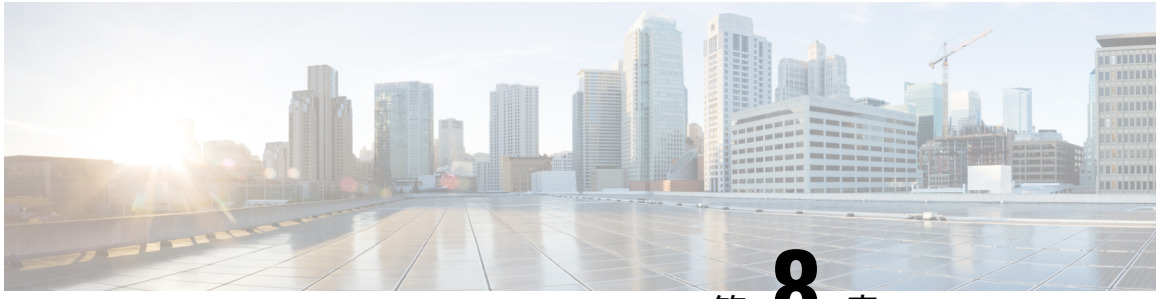
| 説明 | リンク |
|---|---|
| このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。 | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### MIB

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

### シスコのテクニカル サポート

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



第 8 章

# セキュア シェルの設定


- セキュア シェルを設定するための前提条件 （143 ページ）
- セキュア シェルの設定に関する制約事項 （144 ページ）
- セキュア シェルの設定について （144 ページ）
- セキュア シェルの設定方法 （147 ページ）
- SSH の設定およびステータスのモニタリング （151 ページ）


## セキュア シェルを設定するための前提条件

セキュア シェル（SSH）用にスイッチを設定するための前提条件は、次のとおりです。

- SSH を動作させるには、スイッチに Rivest、Shamir、および Adleman（RSA）の公開キーと秘密キーのペアが必要です。これは SSH が必要なセキュア コピー プロトコル（SCP）も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。
- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。
- SCP はセキュリティについて SSH に依存します。
- SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。
- ユーザが SCP を使用するには適切な許可が必要です。
- 適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System（IFS）のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには **copy** コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。
- セキュア シェル（SSH）サーバは、IPsec（データ暗号規格（DES）または 3DES）の暗号化ソフトウェアイメージを必要とします。SSH クライアントは、IPsec（DES または 3DES）の暗号化ソフトウェア イメージが必要です。

- グローバル コンフィギュレーション モードで **hostname** および **ip domain-name** コマンドを使用して、デバイスのホスト名とホスト ドメインを設定します。

# セキュア シェルの設定に関する制約事項

セキュア シェル用に device を設定するための制約事項は、次のとおりです。

- スイッチは、Rivest, Shamir, and Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、データ暗号規格（DES）（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアでのみサポートされます。DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。
- device は、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES）暗号化アルゴリズムをサポートします。ただし、キーを暗号化する対称暗号化 AES はサポートされません。
- SCP を使用する場合、**copy** コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。
- ログイン バナーはセキュア シェル バージョン 1 ではサポートされません。セキュア シェル バージョン 2 ではサポートされています。
- リバース SSH の代替手段をコンソール アクセス用に設定する場合、-l キーワード、userid :{number} {ip-address} デリミタ、および引数が必須です。
- FreeRADIUS over RADSEC でクライアントを認証するには、1024 ビットよりも長い RSA キーを生成する必要があります。その場合は、**crypto key generate rsa general-keys exportable label** *label-name* コマンドを使用します。

# セキュア シェルの設定について

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 2（SSHv2）をサポートします。

## SSH およびスイッチ アクセス

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 2（SSHv2）をサポートします。

IPv6 の SSH 機能は IPv4 における機能と同じです。IPv6 の場合、SSH は IPv6 アドレスをサポートし、IPv6 トランスポート上において、リモート IPv6 ノードとのセキュリティ保護および暗号化された接続を有効化します。

# SSH サーバ、統合クライアント、およびサポートされているバージョン

セキュア シェル（SSH）統合クライアント機能は、SSH プロトコル上で動作し、デバイスの認証および暗号化を実現するアプリケーションです。SSH クライアントによって、シスコ デバイスは別のシスコ デバイスなど SSH サーバを実行するデバイスに対して、セキュアで暗号化された接続を実行できます。この接続は、接続が暗号化される点を除いて Telnet のアウトバウンド接続と同様の機能を提供します。SSH クライアントは、認証および暗号化により、保護されていないネットワーク上でもセキュアな通信ができます。

SSH サーバおよび SSH 統合クライアントは、スイッチ上で実行されるアプリケーションです。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。SSH クライアントは、市販の一般的な SSH サーバと連動します。SSH クライアントは、Data Encryption Standard（DES）、3DES、およびパスワード認証の暗号をサポートします。

（注） SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

ユーザ認証は、デバイスに対する Telnet セッションの認証と同様に実行されます。SSH は、次のユーザ認証方式もサポートします。

- TACACS+
- RADIUS
- ローカル認証および許可

# SSH 設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できます（逆の場合も同様です）。
- スタック マスターで SSH サーバが実行されている場合で、スタック マスターに障害が発生した場合、新しいスタック マスターでは、前のスタック マスターによって生成された RSA キー ペアが使用されます。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力した後、CLI エラー メッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。

- RSA キーのペアを生成する場合に、メッセージ「No host name specified」が表示されることがあります。このメッセージが表示された場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

# セキュア コピー プロトコルの概要

Secure Copy Protocol（SCP）機能は、スイッチの設定やイメージ ファイルのコピーにセキュアな認証方式を提供します。SCP にはセキュア シェル（SSH）が必要です（Berkeley の r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルです）。

SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

また、SSH には AAA 認証が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。

（注） SCP を使用する場合、copy コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

# セキュア コピー プロトコル

セキュア コピー プロトコル（SCP）機能は、deviceの設定やスイッチ イメージ ファイルのコピーにセキュアな認証方式を提供します。SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol（RCP）と類似しています。また、SCP では認証、許可、およびアカウンティング（AAA）の設定が必要なため、deviceはユーザが正しい権限レベルを保有しているかどうかを特定できます。セキュア コピー機能を設定するには、SCP の概念を理解する必要があります。

# セキュア シェルの設定方法

## SSH を実行するためのデバイスのセットアップ

SSH を実行するようにデバイスをセットアップするには、次の手順を実行します。

### 始める前に

ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。この手順は必須です。詳細については、次の関連項目を参照してください。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **hostname** *hostname*<br>例：<br>デバイス(config)# **hostname your_hostname** | デバイスのホスト名および IP ドメイン名を設定します。<br>（注） この手順を実行するのは、デバイスを SSH サーバとして設定する場合だけです。 |
| ステップ 4 | **ip domain-name** *domain_name*<br>例：<br>デバイス(config)# **ip domain-name your_domain** | デバイスのホスト ドメインを設定します。 |
| ステップ 5 | **crypto key generate rsa**<br>例：<br>デバイス(config)# **crypto key generate** | デバイス上でローカルおよびリモート認証用に SSH サーバを有効にし、RSA キー ペアを生成します。デバイスの RSA キー ペアを生成すると、SSH が自動的に有効になります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | **rsa** | 最小モジュラス サイズは、1024 ビットにすることを推奨します。<br>RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。<br>（注） この手順を実行するのは、デバイスを SSH サーバとして設定する場合だけです。 |
| ステップ 6 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 8 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# SSH サーバの設定

SSH サーバを設定するには、次の手順を実行します。

（注） デバイスを SSH サーバとして設定する場合にのみ、この手順が必要です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例： | 特権 EXEC モードを有効にします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス> **enable** | • パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip ssh version** [**2**]<br>例：<br>デバイス(config)# **ip ssh version 2** | （任意）SSH バージョン 2 を実行するように デバイス を設定します。<br>このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。 |
| ステップ 4 | **ip ssh** {**timeout** *seconds* \| **authentication-retries** *number*}<br>例：<br>デバイス(config)# **ip ssh timeout 90 authentication-retries 2** | SSH 制御パラメータを設定します。<br>• タイムアウト値は秒単位で指定します（デフォルト値は120秒）。指定できる範囲は0～120秒です。このパラメータは、SSHネゴシエーション フェーズに適用されます。接続が確立されると、デバイスは CLI ベース セッションのデフォルトのタイムアウト値を使用します。<br>デフォルトでは、ネットワーク上の複数の CLI ベース セッション（セッション 0 ～ 4）に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。<br>• クライアントをサーバへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ～ 5 です。<br>両方のパラメータを設定する場合はこの手順を繰り返します。 |

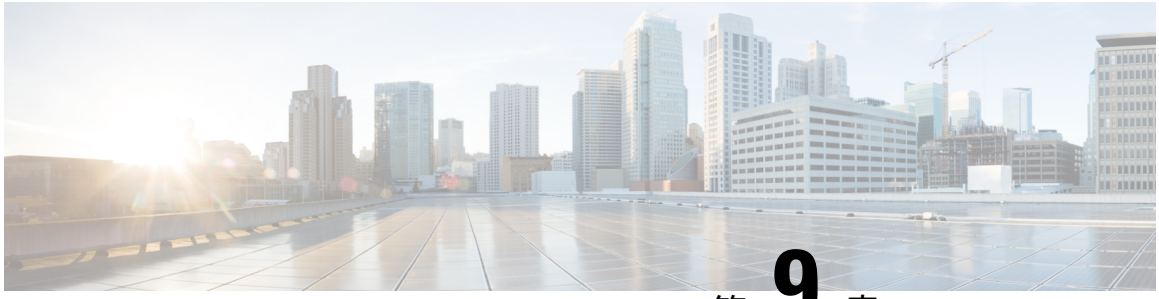
| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | 次のいずれかまたは両方を使用します。<br>• `line vty` *line_number*[*ending_line_number*]<br>• **transport input ssh**<br>例：<br>デバイス(config)# **line vty 1 10**<br>または<br>デバイス(config-line)# **transport input ssh** | （任意）仮想端末回線設定を設定します。<br>• ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。*line_number* 引数と *ending_line_number* 引数の有効な範囲は 0 ～ 15 です。<br>• デバイス で SSH 以外の Telnet 接続を防ぎ、デバイスを SSH 接続のみに限定するように指定します。 |
| ステップ 6 | **end**<br>例：<br>デバイス(config-line)# **end** | 回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。 |
| ステップ 7 | 次のいずれかを使用します。<br>• **show ip ssh**<br>• **show ssh**<br>例：<br>デバイス# **show ip ssh**<br>または<br>デバイス# **show ssh** | • SSH サーバのバージョンおよび設定情報を表示します。<br>• デバイス上の SSH サーバの接続ステータスを表示します。 |
| ステップ 8 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 9 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# SSH の設定およびステータスのモニタリング

次の表に、SSH サーバの設定およびステータスを示します。

表 *15 : SSH* サーバの設定およびステータスを表示するコマンド

| コマンド | 目的 |
|---|---|
| **show ip ssh** | SSH サーバのバージョンおよび設定情報を表示します。 |
| **show ssh** | SSH サーバのステータスを表示します。 |



第 9 章

# SSH 認証の X.509v3 証明書


- SSH 認証の X.509v3 証明書 （153 ページ）
- SSH 認証用の X.509v3 証明書に関する情報 （154 ページ）
- SSH 認証用の X.509v3 証明書の設定方法 （155 ページ）
- SSH 認証用の X.509v3 証明書の設定例 （159 ページ）
- SSH 認証の X.509v3 証明書に関するその他の参考資料 （160 ページ）
- SSH 認証の X.509v3 証明書の機能情報 （161 ページ）


## SSH 認証の X.509v3 証明書

セキュアシェル（SSH）認証用の X.509v3 証明書機能は、サーバ内で X.509v3 デジタル証明書を使用し、SSH サーバ側でユーザ認証を使用します。

## SSH 認証用のデジタル証明書の前提条件

SSH 認証用のデジタル証明書機能では、**ip ssh server authenticate user** コマンドの代わりに **ip ssh server algorithm authentication** コマンドが導入されます。**ip ssh server authenticate user** コマンドを使用すると、次の警告メッセージが表示されます。

```
Warning: SSH command accepted but this CLI will be deprecated soon. Please move to new
CLI "ip ssh server algorithm authentication". Please configure "default ip ssh server
authenticate user" to make CLI ineffective.
```

**default ip ssh server authenticate user** コマンドを使用して、**ip ssh server authenticate user** コマンドを無効にします。その後、IOS セキュア シェル（SSH）サーバは **ip ssh server algorithm authentication** コマンドを使用して起動します。

## SSH 認証の X.509v3 証明書の制約事項

SSH 認証用の X.509v3 証明書には、次の制限事項が適用されます。

- SSH 認証の X.509v3 証明書機能の実装は、IOS セキュア シェル（SSH）サーバ側にのみ適用できます。

- IOS SSH サーバは、IOS SSH サーバ側のサーバおよびユーザ認証について、x509v3-ssh-rsa アルゴリズム ベースの証明書のみをサポートします。

SSH 認証用の X.509v3 証明書は、次の条件で失敗します。

- ルート認証機関がデバイスのトラストポイントとして設定されている場合。
- クライアントが、クライアント証明書、サブ CA 証明書、自己署名ルート認証局を含む自己署名ルート認証局につながる証明書チェーンを渡す場合。
- サブ CA 証明書がデバイスのトラストポイントとして設定されているが、ユーザ証明書のトラストポイントとして含まれていない場合。

# SSH 認証用の X.509v3 証明書に関する情報

次の項では、デジタル証明書、サーバおよびユーザ認証について説明します。

## デジタル証明書

認証の有効性は、公開署名キーとその署名者のアイデンティティとの関連の強さに依存します。X.509v3 形式（RFC5280）のデジタル証明書は、アイデンティティの管理を実行するために使用されます。信頼できるルート証明機関とその中間証明機関による署名の連鎖によって、指定の公開署名キーと指定のデジタル アイデンティティがバインドされます。

公開キーインフラストラクチャ（PKI）のトラストポイントは、デジタル証明書の管理に役立ちます。証明書とトラストポイントを関連付けることによって、証明書を追跡できます。トラストポイントには、認証局（CA）、さまざまなアイデンティティ パラメータ、およびデジタル証明書に関する情報が含まれています。複数のトラストポイントを作成して、異なる証明書に関連付けることができます。

## X.509v3 を使用したサーバおよびユーザ認証

サーバ認証の場合、IOS セキュア シェル（SSH）が確認のためにそれ自体の証明書を SSH クライアントに送信します。このサーバ証明書は、サーバ証明書プロファイル（ssh-server-cert-profile-server コンフィギュレーション モード）で設定されたトラストポイントに関連付けられます。

ユーザ認証の場合、SSH クライアントが確認のためにユーザの証明書を IOS SSH サーバに送信します。SSH サーバは、サーバ証明書プロファイル（ssh-server-cert-profile-user コンフィギュレーション モード）で設定された公開キーインフラストラクチャ（PKI）トラストポイントを使用して、受信したユーザ証明書を確認します。

デフォルトでは、証明書ベースの認証が、IOS SSH サーバ端末でサーバおよびユーザに対して有効になっています。

# SSH 認証用の X.509v3 証明書の設定方法

次の項では、SSH 認証用の X.509v3 証明書の設定方法について説明します。

## サーバ認証にデジタル証明書を使用するための IOS SSH サーバの設定

次の項では、IOS SSH サーバがサーバ認証用にデジタル証明書を使用するための設定について説明します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip ssh server algorithm hostkey {x509v3-ssh-rsa [ssh-rsa] \| ssh-rsa [x509v3-ssh-rsa]}**<br>例：<br>デバイス(config)# **ip ssh server algorithm hostkey x509v3-ssh-rsa** | ホスト キー アルゴリズムの順序を定義します。セキュア シェル（SSH）クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。<br>（注） IOS SSH サーバには、1 つ以上の設定済みホスト キー アルゴリズムが必要です。<br>• ssh-rsa：公開キーベース認証<br>• x509v3-ssh-rsa：証明書ベース認証 |
| ステップ 4 | **ip ssh server certificate profile**<br>例：<br>デバイス(config)# **ip ssh server certificate profile** | サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイル コンフィギュレーション モードを開始します。 |
| ステップ 5 | **server**<br>例： | サーバ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユー |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(ssh-server-cert-profile)# **server** | ザ コンフィギュレーション モードを開始します。 |
| ステップ 6 | **trustpoint sign** *PKI-trustpoint-name*<br>例：<br>デバイス(ssh-server-cert-profile-server)# **trustpoint sign trust1** | 公開キーインフラストラクチャ（PKI）トラストポイントをサーバ証明書プロファイルにアタッチします。SSH サーバは、この PKI トラストポイントに関連付けられた証明書をサーバ認証に使用します。 |
| ステップ 7 | **ocsp-response include**<br>例：<br>デバイス(ssh-server-cert-profile-server)# **ocsp-response include** | （任意）Online Certificate Status Protocol（OCSP）の応答または OCSP ステープリングをサーバ証明書と一緒に送信します。<br>（注） デフォルトではこのコマンドの「no」形式が設定されており、OCSP応答はサーバ証明書と一緒には送信されません。 |
| ステップ 8 | **end**<br>例：<br>デバイス(ssh-server-cert-profile-server)# **end** | SSH サーバ証明書プロファイルのサーバ コンフィギュレーション モードを終了し、特権EXECモードを開始します。 |

# ユーザ認証用のユーザのデジタル証明書を確認するためのIOSSSHサーバの設定

次の項では、IOS SSH サーバがユーザ認証用にユーザのデジタル証明書を確認するための設定について説明します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例： | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **configure terminal** | |
| ステップ 3 | **ip ssh server algorithm authentication** {**publickey** \| **keyboard** \| **password**}<br>例：<br>デバイス(config)# **ip ssh server algorithm authentication publickey** | ユーザ認証アルゴリズムの順序を定義します。セキュア シェル（SSH）クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。<br>（注）<br>• IOS SSH サーバには、1 つ以上の設定済みユーザ認証アルゴリズムが必要です。<br>• ユーザ認証に証明書方式を使用するには、**publickey** キーワードを設定する必要があります。<br>• **ip ssh server algorithm authentication** コマンドは **ip ssh server authenticate user** コマンドの代わりに使用します。 |
| ステップ 4 | **ip ssh server algorithm publickey** {**x509v3-ssh-rsa** [**ssh-rsa**] \| **ssh-rsa** [**x509v3-ssh-rsa**]}<br>例：<br>デバイス(config)# **ip ssh server algorithm publickey x509v3-ssh-rsa** | 公開キー アルゴリズムの順序を定義します。SSH クライアントによってユーザ認証に許可されるのは、設定済みのアルゴリズムのみです。<br>（注） IOS SSH クライアントには、1 つ以上の設定済み公開キー アルゴリズムが必要です。<br>• ssh-rsa：公開キーベース認証<br>• x509v3-ssh-rsa：証明書ベース認証 |
| ステップ 5 | **ip ssh server certificate profile**<br>例：<br>デバイス(config)#**ip ssh server certificate profile** | サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **user**<br>例：<br>デバイス(ssh-server-cert-profile)# **user** | ユーザ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユーザ コンフィギュレーション モードを開始します。 |
| ステップ 7 | **trustpoint verify** *PKI-trustpoint-name*<br>例：<br>デバイス(ssh-server-cert-profile-user)#**trustpoint verify trust2** | 受信したユーザ証明書の確認に使用される公開キー インフラストラクチャ（PKI）トラストポイントを設定します。<br>（注） 同じコマンドを複数回実行することで、複数のトラストポイントを設定します。最大 10 のトラストポイントを設定できます。 |
| ステップ 8 | **ocsp-response required**<br>例：<br>デバイス(ssh-server-cert-profile-user)# **ocsp-response required** | （任意）受信したユーザ証明書による Online Certificate Status Protocol（OCSP）の応答の有無を要求します。<br>（注） デフォルトではこのコマンドの「no」形式が設定されており、ユーザ証明書は OCSP 応答なしで受け入れられます。 |
| ステップ 9 | **end**<br>例：<br>デバイス(ssh-server-cert-profile-user)#**end** | SSH サーバ証明書プロファイルのユーザ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。 |

# デジタル証明書を使用したサーバおよびユーザ認証の設定の確認

次の項では、デジタル証明書を使用したサーバおよびユーザ認証の設定の確認について説明します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>Device> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **show ip ssh**<br>例：<br>`Device# show ip ssh`<br>`SSH Enabled - version 1.99`<br>`Authentication methods:publickey,keyboard-interactive,password`<br>`Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa`<br>`Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa`<br>`Authentication timeout: 120 secs;`<br>`Authentication retries: 3`<br>`Minimum expected Diffie Hellman key size : 1024 bits` | 現在設定されている認証方式を表示します。証明書ベース認証の使用を確認するには、x509v3-ssh-rsa アルゴリズムが設定済みのホスト キー アルゴリズムであることを確認します。 |

# SSH 認証用の X.509v3 証明書の設定例

次の項では、デジタル証明書を使用したユーザおよびサーバ認証の例を示します。

## 例：サーバ認証にデジタル証明書を使用するための IOS SSH サーバの設定

この例では、サーバ認証用のデジタル証明書を使用するための IOS SSH サーバの設定方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# server
Device(ssh-server-cert-profile-server)# trustpoint sign trust1
Device(ssh-server-cert-profile-server)# exit
```

## 例：ユーザ認証用のユーザのデジタル証明書を確認するためのIOSSSH サーバの設定

この例では、ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定方法を示します。

```
Device> enable
Device# configure terminal
```

```
Device(config)# ip ssh server algorithm authentication publickey
Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# user
Device(ssh-server-cert-profile-user)# trustpoint verify trust2
Device(ssh-server-cert-profile-user)# end
```

# SSH 認証の X.509v3 証明書に関するその他の参考資料

関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| Cisco IOS コマンド | Cisco IOS Master Command List, All Releases |
| セキュリティ コマンド | • 『Cisco IOS Security Command Reference: Commands A to C』<br>• 『Cisco IOS Security Command Reference: Commands D to L』<br>• 『Cisco IOS Security Command Reference: Commands M to R』<br>• 『Cisco IOS Security Command Reference: Commands S to Z』 |
| SSH 認証 | 『セキュア シェル コンフィギュレーション ガイド』の「セキュア シェル：ユーザ認証方式の設定」の章 |
| 公開キー インフラストラクチャ（PKI）のトラストポイント | 『*Public Key Infrastructure Configuration Guide*』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章 |

### シスコのテクニカル サポート

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

# SSH 認証の X.509v3 証明書の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

**表 *16 : SSH* 認証用の *X.509v3* 証明書の機能情報**

| 機能情報 | リリース | 変更内容 |
|---|---|---|
| SSH 認証の X.509v3 証明書 | Cisco IOS XE Denali 16.1.x | SSH 認証用の X.509v3 証明書機能は、サーバ内で X.509v3 デジタル証明書を使用し、セキュアシェル（SSH）サーバ側でユーザ認証を使用します。 |

第 10 章

# Secure Socket Layer HTTP の設定


- Secure Socket Layer HTTP について （163 ページ）
- Secure Socket Layer HTTP の設定方法 （167 ページ）
- セキュア HTTP サーバおよびクライアントのステータスのモニタリング （175 ページ）
- Secure Socket Layer HTTP に関するその他の参考資料 （175 ページ）
- Secure Socket Layer HTTP に関する機能情報 （176 ページ）


## Secure Socket Layer HTTP について

### セキュア HTTP サーバおよびクライアントの概要

セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。シスコが実装するセキュア HTTP サーバおよび HTTP クライアントでは、アプリケーション層の暗号化に SSL バージョン 3.0 を使用します。HTTP over SSL は、HTTPS と省略されます（セキュアな接続の場合、URL が http://の代わりに https://で始まります）。

（注） SSL は 1999 年に Transport Layer Security（TLS）に発展しましたが、このような特定のコンテキストでまだ使用されています。

セキュア HTTP サーバ（スイッチ）の主な役割は、指定のポート（デフォルトの HTTPS ポートは 443）で HTTPS 要求を待ち受けて、HTTP 1.1 Web サーバへその要求を渡すことです。HTTP 1.1 サーバはその要求を処理して、セキュア HTTP サーバへ応答（呼び出す）します。セキュア HTTP サーバは HTTP 1.1 サーバの代わりに、元の要求に応えます。

セキュア HTTP クライアント（Web ブラウザ）の主な役割は、Cisco IOS アプリケーション要求に応答して、そのアプリケーションが要求した HTTPS User Agent サービスを実行し、応答を（そのアプリケーションに）返すことです。

（注） Cisco IOS XE Denali 16.3.1 以降では、HTTP サーバへの IPv6 ACL の接続に対するサポートが有効になっています。Cisco IOS XE Denali 16.3.1 より前は、IPv4 ACL のサポートのみがセキュアな HTTP サーバの設定に有効でした。セキュアな HTTP サーバ用の設定 CLI を使用して、事前設定された IPv6 および IPv4 ACL を HTTP サーバに接続できます。

# CA のトラストポイント

認証局（CA）は、要求を認可して参加するネットワーク デバイスに証明書を発行します。これらのサービスは、参加するデバイスに対する中央集中的なセキュリティ キーおよび証明書の管理を提供します。特定の CA サーバはトラストポイントと呼ばれます。

接続が実行されると、HTTPS サーバは、トラストポイントとなる特定の CA から得た X.509v3 の証明書を発行することで、セキュアな接続をクライアントに提供します。クライアント（通常、Web ブラウザ）は、その証明書の認証に必要な公開キーを保有しています。

セキュア HTTP 接続には、CA のトラストポイントを設定することを強く推奨します。HTTPS サーバを実行しているデバイスに CA のトラストポイントが設定されていないと、サーバは自身を認証して必要な RSA のキーのペアを生成します。自身で認証した（自己署名）証明書は適切なセキュリティではないので、接続するクライアントはその証明書が自己証明書であることを通知し、ユーザに接続の選択（確立または拒否）をさせる必要があります。この選択肢は内部ネットワーク トポロジ（テスト用など）に役立ちます。

CA のトラストポイントを設定していないと、セキュア HTTP 接続を有効にした場合、そのセキュア HTTP サーバ（またはクライアント）に対する一時的または永続的な自己署名証明書が自動的に生成されます。

- スイッチにホスト名とドメイン名が設定されてない場合、生成される自己署名証明書は一時的なものです。スイッチを再起動すると、この一時的な自己署名証明書は失われ、新たに自己署名証明書（一時的に）が割り当てられます。
- スイッチにホスト名とドメイン名が設定されている場合、生成される自己署名証明書は永続的なものです。この証明書は、スイッチを再起動しても、セキュア HTTP サーバを無効にしても有効のままです。そのため、再度セキュア HTTP 接続を有効にしたときに使用できます。

（注） 認証局およびトラストポイントは、個々のデバイスで設定する必要があります。他のデバイスからコピーすると、それらはスイッチ上で無効になります。

新しい証明書を登録した場合、新しい設定の変更は、サーバが再起動するまで HTTPS サーバに適用されません。CLI を使用するか、または物理的な再起動によって、サーバを再起動できます。サーバを再起動すると、スイッチは新しい証明書の使用を開始します。

自己署名証明書が生成された場合、その情報は **show running-config** 特権 EXEC コマンドで出力できます。自己署名証明書を表示するコマンドの出力（show running-config コマンド）を例として一部示します。

```
デバイス# show running-config
Building configuration...

<output truncated>

crypto pki trustpoint TP-self-signed-3080755072
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3080755072
 revocation-check none
 rsakeypair TP-self-signed-3080755072
!
!
crypto ca certificate chain TP-self-signed-3080755072
 certificate self-signed 01
  3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109
  02161743 45322D33 3535302D 31332E73 756D6D30 342D3335 3530301E 170D3933
  30333031 30303030 35395A17 0D323030 31303130 30303030 305A3059 312F302D

<output truncated>
```

自己署名証明書は、セキュア HTTP サーバを無効にして、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで削除できます。その後、セキュア HTTP サーバを再度有効にすると、自己署名証明書が新たに生成されます。

（注） *TP self-signed* の後ろに表示されている値は、デバイスのシリアル番号によって異なります。

オプションのコマンド（**ip http secure-client-auth**）を使用すると、HTTPS サーバがクライアントからの X.509v3 証明書を要求します。クライアントの認証は、サーバ自身の認証よりも高いセキュリティを提供します。

# CipherSuite

CipherSuite は暗号化アルゴリズムおよびダイジェストアルゴリズムを指定して、SSL 接続に使用します。HTTPS サーバに接続すると、クライアントの Web ブラウザは、サポート対象の CipherSuite のリストを提供します。その後クライアントとサーバは、両方でサポートされている暗号化アルゴリズムで最適なものをリストから選択してネゴシエートします。たとえば、Netscape Communicator 4.76 は、米国のセキュリティ（RSA 公開キー暗号 MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC）をサポートしています。

最適な暗号化には、128 ビット暗号化をサポートするクライアントブラウザ（Microsoft Internet Explorer バージョン 5.5 以降または Netscape Communicator バージョン 4.76 以降など）が必要です。SSL_RSA_WITH_DES_CBC_SHA CipherSuite は、128 ビット暗号化を提供しないため、他の CipherSuite よりもセキュリティが低くなります。

CipherSuite は、よりセキュリティが高く、複雑になればなるほど、わずかですが処理時間が必要になります。次に、スイッチでサポートされる CipherSuite およびルータの処理負荷（速さ）による CipherSuite のランク（速い順）を定義します。

1. SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化に DES-CBC、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換（RSA 公開キー暗号化）
2. SSL_RSA_WITH_NULL_SHA：メッセージの暗号化に NULL、およびメッセージ ダイジェストに SHA を使用したキー交換（SSL 3.0 専用）。
3. SSL_RSA_WITH_NULL_MD5：メッセージの暗号化に NULL、およびメッセージ ダイジェストに MD5 を使用したキー交換（SSL 3.0 専用）。
4. SSL_RSA_WITH_RC4_128_MD5：RC4 128 ビット暗号化、およびメッセージ ダイジェストに MD5 を使用した RSA のキー交換
5. SSL_RSA_WITH_RC4_128_SHA：RC4 128 ビット暗号化、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換
6. SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージ ダイジェストに SHA を使用した RSA のキー交換（RSA 公開キー暗号化）
7. SSL_RSA_WITH_AES_128_CBC_SHA：AES 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。
8. SSL_RSA_WITH_AES_256_CBC_SHA：AES 256 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。
9. SSL_RSA_WITH_AES_128_CBC_SHA：AES 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。
10. SSL_RSA_WITH_AES_256_CBC_SHA：AES 256 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換（SSL 3.0 専用）。

（注） Chrome の最新バージョンは 4 つの元の暗号スイートをサポートしません。そのため、Web GUI とゲスト ポータル両方へのアクセスが拒否されます。

（暗号化およびダイジェスト アルゴリズムをそれぞれ指定して組み合わせた）RSA は、SSL 接続においてキーの生成および認証の両方に使用されます。これは、CA のトラストポイントが設定されているかどうかにかかわりません。

# SSL のデフォルト設定

標準の HTTP サーバはイネーブルに設定されています。

SSL はイネーブルに設定されています。

CA のトラストポイントは設定されていません。

自己署名証明書は生成されていません。

## SSL の設定時の注意事項

SSL をスイッチ クラスタで使用すると、SSL セッションがクラスタ コマンダで終了します。クラスタ メンバのスイッチは標準の HTTP で動作させる必要があります。

CA のトラストポイントを設定する前に、システム クロックが設定されていることを確認してください。クロックが設定されていないと、不正な日付により証明書が拒否されます。

スイッチ スタック内のスタック マスターで、SSL セッションが強制終了されます。

# Secure Socket Layer HTTP の設定方法

## CA のトラストポイントの設定

セキュア HTTP 接続には、CA のトラストポイントを正式に設定することを推奨します。CA のトラストポイントは、自己署名証明書より高いセキュリティがあります。

CA のトラストポイントを設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`デバイス# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **hostname** *hostname*<br>例：<br>`デバイス(config)# hostname your_hostname` | スイッチのホスト名を指定します（以前ホスト名を設定していない場合のみ必須）。ホスト名はセキュリティ キーと証明書に必要です。 |
| ステップ 3 | **ip domain-name** *domain-name*<br>例：<br>`デバイス(config)# ip domain-name your_domain` | スイッチの IP ドメイン名を指定します（以前 IP ドメイン名を設定していない場合のみ必須）。IP ドメイン名はセキュリティ キーと証明書に必要です。 |
| ステップ 4 | **crypto key generate rsa**<br>例： | （任意）RSA キーペアを生成します。RSA キーのペアは、スイッチの証明書 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config)# **crypto key generate rsa** | を入手する前に必要です。RSA キーのペアは自動的に生成されます。必要であれば、このコマンドを使用してキーを再生成できます。 |
| ステップ 5 | **crypto ca trustpoint** *name*<br>例：<br>デバイス(config)# **crypto ca trustpoint your_trustpoint** | CA のトラストポイントにローカルの設定名を指定して、CA トラストポイントコンフィギュレーションモードを開始します。 |
| ステップ 6 | **enrollment url** *url*<br>例：<br>デバイス(ca-trustpoint)# **enrollment url http://your_server:80** | スイッチによる証明書要求の送信先の URL を指定します。 |
| ステップ 7 | **enrollment http-proxy** *host-name port-number*<br>例：<br>デバイス(ca-trustpoint)# **enrollment http-proxy your_host 49** | （任意）HTTP プロキシ サーバを経由して CA から証明書を入手するようにスイッチを設定します。<br>• *host-name* には、CA を取得するために使用するプロキシサーバを指定します。<br>• *port-number* には、CA にアクセスするために使用するポート番号を指定します。 |
| ステップ 8 | **crl query** *url*<br>例：<br>デバイス(ca-trustpoint)# **crl query ldap://your_host:49** | ピアの証明書が取り消されていないかを確認するために、証明書失効リスト（CRL）を要求するようにスイッチを設定します。 |
| ステップ 9 | **primary** *name*<br>例：<br>デバイス(ca-trustpoint)# **primary your_trustpoint** | （任意）トラストポイントが CA 要求に対してプライマリ（デフォルト）トラストポイントとして使用されるように指定します。<br>• *name* には、設定したトラストポイントを指定します。 |
| ステップ 10 | **exit**<br>例： | CA トラストポイントコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(ca-trustpoint)# **exit** | |
| ステップ 11 | **crypto ca authentication** *name*<br>例：<br>デバイス(config)# **crypto ca authentication your_trustpoint** | CA の公開キーを取得して CA を認証します。ステップ 5 で使用した名前と同じものを使用します。 |
| ステップ 12 | **crypto ca enroll** *name*<br>例：<br>デバイス(config)# **crypto ca enroll your_trustpoint** | 指定した CA トラストポイントから証明書を取得します。このコマンドは、各 RSA キーのペアに対して 1 つの署名入りの証明書を要求します。 |
| ステップ 13 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

# セキュア HTTP サーバの設定

セキュア HTTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

### 始める前に

証明に証明書の認証を使用する場合、前の手順を使用してスイッチの CA トラストポイントを設定してから、HTTP サーバを有効にする必要があります。CA のトラストポイントを設定していない場合、セキュア HTTP サーバを最初に有効にした時点で、自己署名証明書が生成されます。サーバを設定した後、標準およびセキュア HTTP サーバ両方に適用するオプション（パス、適用するアクセス リスト、最大接続数、またはタイムアウト ポリシー）を設定できます。

Web ブラウザを使用してセキュア HTTP 接続を確認するには、https://*URL* を入力します（URL は IP アドレス、またはサーバ スイッチのホスト名）。デフォルト ポート以外のポートを設定している場合、URL の後ろにポート番号も指定する必要があります。次に例を示します。

（注） AES256_SHA2 はサポートされません。

```
https://209.165.129:1026
```

または

```
https://host.domain.com:1026
```

アクセスリスト（IPv4 ACL のみ）を指定するための従来の **ip http access-class** *access-list-number* コマンドは廃止予定です。引き続きこのコマンドを使用して、HTTP サーバへのアクセスを許可するアクセス リストを指定できます。2 つの新しいコマンドは、IPv4 および IPv6 ACL を指定するためのサポートを有効にするために導入されました。これらは、IPv4 ACL を指定するための **ip http access-class ipv4** *access-list-name* | *access-list-number* と、IPv6 ACL を指定するための **ip http access-class ipv6** *access-list-name* です。警告メッセージの受信を防ぐために、新しい CLI の使用をお勧めします。

アクセス リストを指定する際は、次の考慮事項があります。

- 存在しないアクセスリストを指定すると、設定は実行されますが、次の警告メッセージを受信します。

  ```
  ACL being attached does not exist, please configure it
  ```

- HTTP サーバにアクセスリストを指定するために **ip http access-class** コマンドを使用すると、次の警告メッセージが表示されます。

  ```
  This CLI will be deprecated soon, Please use new CLI ip http
  access-class ipv4/ipv6 <access-list-name>| <access-list-number>
  ```

- **ip http access-class ipv4** *access-list-name* | *access-list-number* または **ip http access-class ipv6** *access-list-name* を使用した場合に、アクセスリストがすでに **ip http access-class** を使用して設定されていた場合は、次の警告メッセージが表示されます。

  ```
  Removing ip http access-class <access-list-number>
  ```

**ip http access-class** *access-list-number* と **ip http access-class ipv4** *access-list-name* | *access-list-number* は同じ機能を共有しています。コマンドを実行するごとに、その前のコマンドのコンフィギュレーションは上書きされます。2 つのコマンドの設定間の次の組み合わせによって、実行コンフィギュレーションへの影響が説明されます。

- **ip http access-class** *access-list-number* がすでに設定されている場合に、**ip http access-class ipv4** *access-list-number* コマンドを使用して設定を行おうとした場合、**ip http access-class** *access-list-number* の設定は削除され、**ip http access-class ipv4** *access-list-number* の設定が実行コンフィギュレーションに追加されます。

- **ip http access-class** *access-list-number* がすでに設定されている場合に、**ip http access-class ipv4** *access-list-name* コマンドを使用して設定を行おうとした場合、**ip http access-class** *access-list-number* の設定は削除され、**ip http access-class ipv4** *access-list-name* の設定が実行コンフィギュレーションに追加されます。

- **ip http access-class ipv4** *access-list-number* がすでに設定されている場合に、**ip http access-class** *access-list-name* を使用して設定を行おうとした場合、**ip http access-class ipv4** *access-list-number* の設定は削除され、**ip http access-class** *access-list-name* の設定が実行コンフィギュレーションに追加されます。

- **ip http access-class ipv4** *access-list-name* がすでに設定されている場合に、**ip http access-class** *access-list-number* を使用して設定を行おうとした場合、**ip http access-class ipv4**

*access-list-name* の設定は削除され、**ip http access-class** *access-list-number* の設定が実行コンフィギュレーションに追加されます。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **show ip http server status**<br>例：<br>デバイス# **show ip http server status** | （任意）HTTP サーバのステータスを表示して、セキュア HTTP サーバの機能がソフトウェアでサポートされているかどうかを判断します。出力で、次のラインのどちらかを確認してください。<br>`HTTP secure server capability: Present`<br>または<br>`HTTP secure server capability: Not present` |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip http secure-server**<br>例：<br>デバイス(config)# **ip http secure-server** | HTTPS サーバがディセーブルの場合、イネーブルにします。HTTPS サーバは、デフォルトでイネーブルに設定されています。 |
| ステップ 4 | **ip http secure-port** *port-number*<br>例：<br>デバイス(config)# **ip http secure-port 443** | （任意）HTTPS サーバに使用するポート番号を指定します。デフォルトのポート番号は 443 です。443 または 1025 ～ 65535 の範囲で指定できます。 |
| ステップ 5 | **ip http secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}<br>例：<br>デバイス(config)# **ip http** | （任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `secure-ciphersuite rc4-128-md5` | CipherSuite でネゴシエートするように設定します。これがデフォルトです。 |
| ステップ 6 | **ip http secure-client-auth**<br>例：<br>デバイス(config)# **ip http secure-client-auth** | （任意）HTTP サーバを設定して、接続処理の間、認証のために、クライアントからの X.509v3 証明書を要求します。デフォルトでは、クライアントがサーバからの証明書を要求する設定になっていますが、サーバはクライアントを認証しないようになっています。 |
| ステップ 7 | **ip http secure-trustpoint** *name*<br>例：<br>デバイス(config)# **ip http secure-trustpoint your_trustpoint** | X.509v3 セキュリティ証明書の取得およびクライアントの証明書接続の認証に使用する CA のトラストポイントを指定します。<br>（注） このコマンドの使用は、前の手順に従って CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。 |
| ステップ 8 | **ip http path** *path-name*<br>例：<br>デバイス(config)# **ip http path /your_server:80** | （任意）HTML ファイルのベースとなる HTTP パスを設定します。パスは、ローカル システムにある HTTP サーバファイルの場所を指定します（通常、システムのフラッシュ メモリを指定します）。 |
| ステップ 9 | **ip http access-class** *access-list-number*<br>例：<br>デバイス(config)# **ip http access-class 2** | （任意）HTTP サーバへのアクセスの許可に使用するアクセスリストを指定します。 |
| ステップ 10 | **ip http access-class** { **ipv4** {*access-list-number* \| *access-list-name*} \| **ipv6** {*access-list-name*} }<br>例：<br>デバイス(config)# **ip http access-class ipv4 4** | （任意）HTTP サーバへのアクセスの許可に使用するアクセスリストを指定します。 |
| ステップ 11 | **ip http max-connections** *value*<br>例： | （任意）HTTP サーバへの同時最大接続数を指定します。値は10以上にすることを推奨します。これは、UI が想定 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config)# **ip http max-connections 4** | どおりに機能するために必要な値です。 |
| ステップ 12 | **ip http timeout-policy idle** *seconds* **life** *seconds* **requests** *value*<br>例：<br>デバイス(config)# **ip http timeout-policy idle 120 life 240 requests 1** | （任意）指定の状況下における、HTTP サーバへの接続最大時間を指定します。<br>• **idle**：データの受信がないか、応答データが送信できない場合の最大時間。指定できる範囲は 1 ～ 600 秒です。デフォルト値は180秒（3分）です。<br>• **life**：接続を確立している最大時間。指定できる範囲は 1 ～ 86400 秒（24時間）です。デフォルト値は 180 秒です。<br>• **requests**：永続的な接続で処理される要求の最大数。最大値は 86400 です。デフォルトは 1 です。 |
| ステップ 13 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

# セキュア HTTP クライアントの設定

セキュア HTTP クライアントを設定するには、特権 EXEC モードで次の手順を実行します。

### 始める前に

標準の HTTP クライアントおよびセキュア HTTP クライアントは常にイネーブルです。証明書の認証にはセキュア HTTP クライアントの証明書が必要です。次の手順では、前の手順で CA のトラストポイントをスイッチに設定していることを前提にしています。CA のトラストポイントが設定されておらず、リモートの HTTPS サーバがクライアントの認証を要求した場合、セキュア HTTP クライアントへの接続は失敗します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **ip http client secure-trustpoint** *name*<br>例：<br>デバイス(config)# **ip http client secure-trustpoint your_trustpoint** | （任意）リモートの HTTP サーバがクライアント認証を要求した場合に使用する、CA のトラストポイントを指定します。このコマンドの使用は、前の手順を使用して CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。クライアント認証が必要ない場合、またはプライマリのトラストポイントがすでに設定されている場合は、このコマンドは任意です。 |
| ステップ 3 | **ip http client secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}<br>例：<br>デバイス(config)# **ip http client secure-ciphersuite rc4-128-md5** | （任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これがデフォルトです。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

# セキュア HTTP サーバおよびクライアントのステータスのモニタリング

SSL セキュア サーバおよびクライアントのステータスをモニタするには、次の表の特権 EXEC コマンドを使用します。

表 *17 : SSL* セキュア サーバおよびクライアントのステータスを表示するコマンド

| コマンド | 目的 |
|---|---|
| **show ip http client secure status** | セキュア HTTP クライアントの設定を表示します。 |
| **show ip http server secure status** | セキュア HTTP サーバの設定を表示します。 |
| **show running-config** | セキュア HTTP 接続に対して生成された自己署名証明書を表示します。 |

# Secure Socket Layer HTTP に関するその他の参考資料

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| 証明機関 | 「Configuring Certification Authority Interoperability」 |

### MIB

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

### シスコのテクニカル サポート

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

# Secure Socket Layer HTTP に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

**表 *18 : Secure Socket Layer HTTP* に関する機能情報**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| Secure Socket Layer HTTP | | シスコが導入するセキュア HTTP サーバおよび HTTP クライアントでは、アプリケーション層の暗号化に SSL バージョン 3.0 を使用します。セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。 |

第 11 章

# IPv4 ACL


- IPv4 アクセス コントロール リストの設定に関する制約事項 （177 ページ）
- ACL によるネットワーク セキュリティに関する情報 （178 ページ）
- ACL の設定方法 （194 ページ）
- IPv4 ACL のモニタリング （216 ページ）
- ACL の設定例 （217 ページ）


## IPv4アクセスコントロールリストの設定に関する制約事項

### 一般的なネットワーク セキュリティ

次は、ACL によるネットワーク セキュリティの設定の制約事項です。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。インターフェイスのパケット フィルタおよびルート フィルタ用の ACL では、名前を使用できます。また、VLAN マップでも名前を指定できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- **appletalk** は、コマンドラインのヘルプ ストリングに表示されますが、**deny** および **permit** MAC アクセスリスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。
- ACL ワイルドカードは、ダウンストリーム クライアント ポリシーではサポートされていません。

### IPv4 ACL ネットワーク インターフェイス

次の制限事項が、ネットワーク インターフェイスへの IPv4 ACL に適用されます。

- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。

- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2（ポート）ACL はVLANインターフェイスに適用された入力方向のレイヤ3ACL、またはVLANに適用された VLAN マップよりも優先します。
- レイヤ 3 インターフェイスに ACL が適用され、スイッチ上でルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。
- パケットをフィルタリングするために **preauth_ipv4_acl** ACL が設定されている場合、ACL は認証後に削除されます。
- レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。

### レイヤ 2 インターフェイスの MAC ACL

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に留意してください。

- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

（注） **mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用される場合のみ有効です。このコマンドは、EtherChannel ポート チャネルでは使用できません。

### IP アクセス リスト エントリ シーケンス番号

- この機能は、ダイナミック アクセス リスト、再帰アクセス リスト、またはファイアウォール アクセス リストをサポートしていません。

# ACL によるネットワーク セキュリティに関する情報

この章では、アクセス コントロール リスト（ACL）を使用して、スイッチのネットワーク セキュリティを設定する方法について説明します。コマンドや表では、ACL をアクセス リストと呼ぶこともあります。

# ACL の概要

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACLはルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスまたは VLAN を通過するパケットを許可または拒否します。ACLは、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。パケットがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用されるACLと比較し、アクセスリストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセスリスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。スイッチは、VLAN内でブリッジングされるパケットを含めて、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ3スイッチにアクセス リストを設定します。ACL を設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータインターフェイスで転送またはブロックされるトラフィックの種類を決定したりできます。たとえば、電子メールトラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。ACL を着信トラフィック、発信トラフィック、またはその両方をブロックするように設定することもできます。

## アクセス コントロール エントリ

ACL には、アクセス コントロール エントリ（ACE）の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

## ACL でサポートされるタイプ

スイッチは、IP ACL とイーサネット（MAC）ACL をサポートしています。

- IP ACL は、TCP、ユーザ データグラム プロトコル（UDP）、インターネット グループ管理プロトコル（IGMP）、およびインターネット制御メッセージプロトコル（ICMP）などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

このスイッチは、Quality of Service（QoS）分類 ACL もサポートしています。

# サポートされる ACL

スイッチでは、トラフィックをフィルタリングするために、次に示す 3 種類の ACL がサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。IPv4 と MAC どちらのアクセス リスト タイプのどの方向に対してでも、レイヤ 2 インターフェイスにポート ACL を適応できます。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御し、レイヤ 3 インターフェイスで特定の方向（着信または発信）に適用されます。
- VLAN ACL または VLAN マップは、すべてのパケット（ブリッジド パケットおよびルーテッド パケット）のアクセスを制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。VLAN マップは、IPv4 のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されています。イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプロトコルがアクセス コントロールされます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケット（ルーテッド パケットまたはブリッジド パケット）が VLAN マップと照合されます。パケットは、スイッチ ポートを介して、または、ルーティングされたパケットの場合、ルーテッド ポートを介して、VLAN に入ることができます。

## ACL 優先順位

VLAN マップ、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、入力トラフィックの場合のフィルタの優先順位は上からポート ACL、VLAN マップ、およびルータ ACL です。出力トラフィックの場合、フィルタの優先順位は、ルータ ACL、VLAN マップ、ポート ACL です。

次の例で、簡単な使用例を説明します。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- スイッチ仮想インターフェイス（SVI）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。他のポートで受信した着信のルーティン

グ IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

## ポート ACL

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL を使用できるのは、物理インターフェイスだけです。EtherChannel インターフェイスでは使用できません。ポート ACL は、アウトバウンドおよびインバウンド方向のインターフェイスに適用できます。次のアクセス リストがサポートされています。

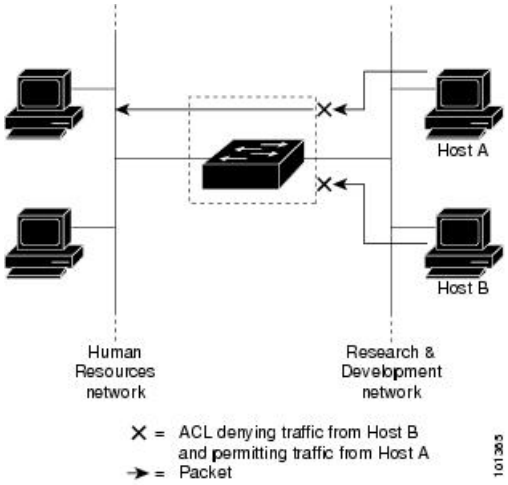
- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイス上の ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。

**図 *6 : ACL* によるネットワーク内のトラフィックの制御**

次に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマン リソース ネットワークにアクセスすることを許可しますが、ホスト B が

同一のネットワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2




インターフェイスだけに適用できます。

ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。

（注） レイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

## ルータ ACL

VLAN へのレイヤ 3 インターフェイスであるスイッチ仮想インターフェイス（SVI）、物理層 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

スイッチは、IPv4 トラフィックの次のアクセス リストをサポートしています。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチはインターフェイスに設定されている機能に関連付けられている ACL が照合されます。パケットがスイッチのインターフェイスに着信すると、その

インターフェイスに設定されているすべての着信機能に対応するACLが照合されます。パケットがルーティングされてからネクストホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACLを使用すると、ネットワーク全体またはネットワークの一部に対するアクセス コントロールが行えます。

## VLAN マップ

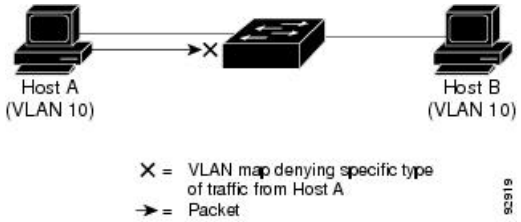
VLAN ACL または VLAN マップは、VLAN 内のネットワーク トラフィックを制御するために使用されます。スイッチまたはスイッチ スタックの VLAN 内でブリッジングされるすべてのパケットに VLAN マップを適用できます。VACL は、セキュリティ パケット フィルタリングおよび特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向（入力または出力）で定義されることはありません。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます（IP トラフィックは、MAC VACL マップではアクセス制御されません）。VLANマップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

VLANマップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

**図 7: *VLAN* マップによるトラフィックの制御**

次の図に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用できます。




# ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック

IPパケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

アクセス コントロール エントリ（ACE）には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化されたIPパケットのほとんどのフラグメントに標準的な方法では適用できません。

フラグメントにレイヤ4情報が含まれておらず、ACEが一部のレイヤ4情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報（TCP や UDP などのプロトコル タイプを含む）をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。

（注） L4 Ops をともなう ACE の TCP では、フラグメント化パケットは RFC 1858 ごとにドロップします。

- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

## ACEおよびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例

次のコマンドで構成され、フラグメント化された3つのパケットに適用されるアクセス リスト 102 を例に取って説明します。

```
デバイス(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
デバイス(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
デバイス(config)# access-list 102 permit tcp any host 10.1.1.2
デバイス(config)# access-list 102 deny tcp any any
```

（注） 最初の 2 つの ACE には宛先アドレスの後に *eq* キーワードがありますが、これは既知の TCP 宛先ポート番号がそれぞれシンプル メール転送プロトコル（SMTP）および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE（permit）と一致します。残りのフラグメントも最初の ACE と一致します。これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ3情報だけをチェックするからです。この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです。

- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて揃っているため、最初のフラグメントが2つめのACE（deny）と一致します。残りのフラグメントは、レイヤ4情報が含まれていないため、2つめのACEと一致しません。残りのフラグメントは 3 つめの ACE（permit）と一致します。

最初のフラグメントが拒否されたため、ホスト10.1.1.2は完全なパケットを再構成できず、その結果、パケットBは拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。

- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE（deny）と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

# ACL とスイッチ スタック

スイッチ スタックの ACL サポートは、スタンドアロン スイッチと同じです。ACL の構成情報は、スタック内のすべてのスイッチに送信されます。アクティブ スイッチを含むスタック内のすべてのスイッチでは、情報が処理され、ハードウェアがプログラムされます。

## アクティブ スイッチおよび ACL の機能

アクティブ スイッチにより、次の ACL 機能が実行されます。

- ACL 構成情報が処理され、情報がすべてのスタック メンバに送信されます。
- ACL 情報は、スタックに加入しているすべてのスイッチに配信されます。
- （たとえば、十分なハードウェア リソースがないなど）何らかの理由で、ソフトウェアによってパケットが送信される必要がある場合、ACL をパケットに適用後にのみ、アクティブ スイッチによってパケットが転送されます。
- そのハードウェアは、処理する ACL 情報でプログラムされます。

## スタック メンバおよび ACL の機能

スタック メンバにより、次の ACL 機能が実行されます。

- スタック メンバでは、アクティブ スイッチから ACL 情報を受信し、ハードウェアがプログラムされます。
- スタンバイ スイッチとして設定されたスタック メンバがアクティブ スイッチが失敗したイベント内のアクティブ スイッチ機能を実行します。

## アクティブ スイッチの障害および ACL

アクティブとスタンバイの両方のスイッチに ACL 情報があります。アクティブ スイッチに障害が発生すると、スタンバイが役割を引き継ぎます。新しいアクティブ スイッチにより、すべてのスタック メンバーに ACL 情報が配信されます。

# 標準 IPv4 ACL および拡張 IPv4 ACL

ここでは、IP ACL について説明します。

ACL は、許可条件と拒否条件の順序付けられた集まりです。スイッチは、アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致する最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、IPv4 について次の ACL（アクセス リスト）をサポートします。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることもできます。

## IPv4 ACL スイッチでサポートされていない機能

このスイッチで IPv4 ACL を設定する手順は、他の Cisco スイッチやルータで IPv4 ACL を設定する手順と同じです。

以下の ACL 関連の機能はサポートされていません。

- 非 IP プロトコル ACL または
- IP アカウンティング
- 再帰 ACL およびダイナミック ACL はサポートされていません。

## アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。

次の一覧に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト（1 ～ 199 および 1300 ～ 2699）をサポートします。

**表 *19*：アクセス リスト番号**

| アクセス リスト番号 | タイプ | サポートあり |
|---|---|---|
| 1 ～ 99 | IP 標準アクセス リスト | あり |
| 100 ～ 199 | IP 拡張アクセス リスト | あり |
| 200 ～ 299 | プロトコルタイプコードアクセス リスト | なし |
| 300 ～ 399 | DECnet アクセス リスト | なし |

| アクセス リスト番号 | タイプ | サポートあり |
|---|---|---|
| 400 ～ 499 | XNS 標準アクセス リスト | なし |
| 500 ～ 599 | XNS 拡張アクセス リスト | なし |
| 600 ～ 699 | AppleTalk アクセス リスト | なし |
| 700 ～ 799 | 48 ビット MAC アドレス アクセス リスト | なし |
| 800 ～ 899 | IPX 標準アクセス リスト | なし |
| 900 ～ 999 | IPX 拡張アクセス リスト | なし |
| 1000 ～ 1099 | IPX SAP アクセス リスト | なし |
| 1100 ～ 1199 | 拡張 48 ビット MAC サマリー アドレス アクセス リスト | なし |
| 1200 ～ 1299 | IPX サマリー アドレス アクセス リスト | なし |
| 1300 ～ 1999 | IP 標準アクセス リスト（拡張範囲） | あり |
| 2000 ～ 2699 | IP 拡張アクセス リスト（拡張範囲） | あり |

番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

## 番号付き標準 IPv4 ACL

ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

スイッチは、**host** 一致条件があるエントリと *don't care* マスク 0.0.0.0 を含む一致条件があるエントリがリストの先頭に移動し、0 以外の *don't care* マスクを含むエントリよりも前に位置するように、標準アクセス リストの順序を書き換えます。そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号付き標準 IPv4 ACL を VLAN、端末回線、またはインターフェイスに適用できます。

# 番号付き拡張 IPv4 ACL

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコルタイプ情報を使用して制御のきめ細かさを高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

このスイッチは、ダイナミックまたはリフレクシブアクセスリストをサポートしていません。また、タイプ オブ サービス（ToS）の minimize-monetary-cost ビットに基づくフィルタリングもサポートしていません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

拡張 TCP、UDP、ICMP、IGMP、またはその他の IP ACL を定義できます。また、このスイッチはこれらの IP プロトコルをサポートします。

（注） ICMP エコー応答はフィルタリングできません。他の ICMP コードまたはタイプは、すべてフィルタリングできます。

これらの IP プロトコルがサポートされます。

- 認証ヘッダー プロトコル（**ahp**）
- Encapsulation Security Payload（**esp**）
- Enhanced Interior Gateway Routing Protocol（**eigrp**）
- 総称ルーティング カプセル化（**gre**）
- インターネット制御メッセージ プロトコル（**icmp**）
- インターネット グループ管理プロトコル（**igmp**）
- すべての内部プロトコル（**ip**）
- IP-in-IP トンネリング（**ipinip**）
- KA9Q NOS 互換 IP over IP トンネリング（**nos**）
- Open Shortest Path First ルーティング（**ospf**）
- ペイロード圧縮プロトコル（**pcp**）
- プロトコル独立マルチキャスト（**pim**）
- 伝送制御プロトコル（**tcp**）
- ユーザ データグラム プロトコル（**udp**）

## 名前付き IPv4 ACL

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング（名前）を使用できます。名前付き ACL を使用すると、ルータ上で番号付きアクセス リストの場合より多くの IPv4 アクセス リストを設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付きアクセス リストで使用できるわけではありません。

（注） 標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。標準 IP ACL の名前は 1 ～ 99 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定するときには、次の注意事項に留意してください。

- また、番号付き ACL も使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。

## ACL ロギング

標準 IP アクセス リストによって許可または拒否されたパケットに関するログ メッセージが、スイッチのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、syslog メッセージを管理する **logging console** コマンドで管理されます。

（注） ACL ロギングは、RACL でのみサポートされます。

（注） ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可（*permit*）または拒否（*deny*）ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

（注） ロギング メッセージが多すぎて処理できない場合、または1秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作によって、ロギング パケットが多すぎてルータがクラッシュすることを回避します。そのため、課金ツールや、アクセス リストと一致する数の正確な情報源としてロギング設備をを使用しないでください。

# ハードウェアおよびソフトウェアによる IP ACL の処理

ACL 処理はハードウェアで実行されます。ハードウェアで ACL の設定を保存する領域が不足すると、そのインターフェイス上のすべてのパケットがドロップします。

（注） デバイスまたはスタックメンバのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受けるのは、デバイスに着信した該当 VLAN 内のトラフィックだけです。

ルータ ACL の場合は、次の場合にパケットが CPU に送信されることがあります。

- **log** キーワードの使用
- ICMP 到達不能メッセージを生成する。

**show ip access-lists** 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。スイッチドパケットおよびルーテッドパケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、**show platform software fed switch** { *switch_num* | **active** | **standby** } **acl counters hardware** 特権 EXEC コマンドを使用します。

ルータ ACL の機能は、次のとおりです。

- 標準 ACL および拡張 ACL（入力および出力）の許可アクションや拒否アクションをハードウェアで制御し、アクセス コントロールのセキュリティを強化します。
- *ip unreachables* が無効の場合、**log**を指定しないと、セキュリティ ACL の *deny* ステートメントと一致するフローがハードウェアによってドロップされます。許可ステートメントと一致するフローは、ハードウェアでスイッチングされます。
- ルータ ACL の ACE に **log** キーワードを追加すると、パケットのコピーが CPU に送信され、ロギングだけが行われます。ACE が許可ステートメントの場合も、パケットはハードウェアでスイッチングおよびルーティングされます。

# VLAN マップの設定時の注意事項

VLANマップは、VLAN内でフィルタリングを制御する唯一の方法です。VLANマップには方向の指定がありません。VLANマップを使用して、特定の方向のトラフィックをフィルタリン

グするには、特定の送信元または宛先アドレスが指定されたACLを追加する必要があります。VLAN マップ内に該当パケット タイプ（IP または MAC）に対する match 句がある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットはドロップされます。該当パケット タイプに対する match コマンドがない場合、デフォルトでは、パケットが転送されます。

次は、VLAN マップ設定の注意事項です。

- インターフェイスでトラフィックを拒否するように設定された ACL がなく、VLAN マップが設定されていない場合、すべてのトラフィックが許可されます。
- 各 VLAN マップは一連のエントリで構成されます。VLAN マップのエントリの順序は重要です。スイッチに着信したパケットは、VLANマップの最初のエントリに対してテストされます。一致した場合は、VLANマップのその部分に指定されたアクションが実行されます。一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。
- 該当パケット タイプ（IP または MAC）に対する match 句が VLAN マップに 1 つまたは複数ある場合でも、パケットがそれらの match 句に一致しない場合、デフォルトではパケットがドロップされます。該当パケット タイプに対する match 句が VLAN マップ内にない場合、デフォルトではパケットが転送されます。
- VLAN マップのロギングはサポートされていません。
- レイヤ 2 インターフェイスに適用された IP アクセス リストまたは MAC アクセス リストがスイッチにあって、ポートが属する VLAN に VLAN マップを適用する場合、ポート ACL が VLAN マップに優先します。
- ハードウェアに VLAN マップの設定を適用できない場合は、その VLAN 内のすべてのパケットがドロップします。

# VLAN マップとルータ ACL

ブリッジングされたトラフィックおよびルーティングされたトラフィックの両方に対してアクセス コントロールを行うには、VLANマップを単独で使用するか、またはルータ ACL と VLAN マップを組み合わせて使用します。入力と出力両方のルーテッド VLAN インターフェイスでルータ ACL を定義したり、ブリッジングされたトラフィックのアクセスをコントロールする VLAN マップを定義したりできます。

パケット フローが ACL 内 VLAN マップの deny ステートメントと一致した場合、ルータ ACL の設定に関係なく、パケット フローは拒否されます。

（注） ルータ ACL を VLAN マップと組み合わせて使用し、ルータ ACL でのロギングを必要とするパケットが VLAN マップで拒否された場合、これらのパケットはロギングされません。

該当パケット タイプ（IP または MAC）に対する match 句が VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトではパケットがドロップされます。VLAN

マップ内に match 句がなく、アクションが指定されていない場合、どの VLAN マップ エントリとも一致しないパケットは転送されます。

## VLAN マップとルータ ACL の設定時の注意事項

ここに記載された注意事項は、ルータ ACL および VLAN マップを同じ VLAN 上で使用する必要がある設定に適用されます。ルータ ACL および VLAN マップを異なる VLAN に割り当てる設定には、これらの注意事項は適用されません。

ルータ ACL および VLAN マップを同じ VLAN に設定する必要がある場合は、ルータ ACL と VLAN マップの両方の設定に関し、ここで説明する注意事項に従ってください。

- VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつに限り設定できます。
- 可能な限り、すべてのエントリのアクションが同一で、末尾のデフォルトアクションだけが反対のタイプとなるように ACL を記述します。次のいずれかの形式を使用して、ACL を記述します。

  permit... permit... permit... deny ip any any

  または

  deny... deny... deny... permit ip any any
- ACL 内で複数のアクション（許可、拒否）を定義する場合は、それぞれのアクション タイプをまとめて、エントリ数を削減します。
- ACL 内にレイヤ 4 情報を指定しないでください。レイヤ 4 情報を追加すると、統合プロセスが複雑になります。ACL のフィルタリングが、full-flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）でなく、IP アドレス（送信元および宛先）に基づいて行われる場合に、最適な統合結果が得られます。可能な限り、IP アドレスには *don't care* ビットを使用してください。

  IP ACE とレイヤ 4 情報を含む TCP/UDP/ICMP ACE が両方とも ACL 内に存在し、full-flow モードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

# ACL の時間範囲

**time-range** グローバル コンフィギュレーション コマンドを使用することによって、時刻および曜日に基づいて拡張 ACL を選択的に適用できます。まず、時間範囲の名前を定義し、その時間範囲内の時刻および日付または曜日を設定します。次に、ACL を適用してアクセス リストに制限を設定するときに時間範囲を入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間（指定期間内や指定曜日など）を定義できます。**time-range** キーワードおよび引数については、名前付きおよび番号付き拡張 ACL タスクの表を参照してください。

時間範囲を使用するいくつかの利点を次に示します。

- アプリケーションなどのリソース（IP アドレスとマスクのペア、およびポート番号で識別）へのユーザ アクセスをより厳密に許可または拒否できます。
- ログ メッセージを制御できます。ACL エントリを使用して特定の時刻に関してのみトラフィックをロギングできるため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセス リストを使用すると、CPU に負荷が生じます。これは、アクセス リストの新規設定を他の機能や、ハードウェア メモリにロードされた結合済みの設定とマージする必要があるためです。そのため、複数のアクセス リストが短期間に連続して（互いに数分以内に）有効となるような設定とならないように注意する必要があります。

（注） 時間範囲は、スイッチのシステム クロックに基づきます。したがって、信頼できるクロック ソースが必要です。ネットワーク タイム プロトコル（NTP）を使用してスイッチ クロックを同期させることを推奨します。

# IPv4 ACL のインターフェイスに関する注意事項

**ip access-group** インターフェイス コンフィギュレーション コマンドをレイヤ 3 インターフェイス（SVI、レイヤ 3 EtherChannel、またはルーテッド ポート）に適用するには、そのインターフェイスに IP アドレスが設定されている必要があります。レイヤ 3 アクセス グループは、CPU のレイヤ 3 プロセスによってルーティングまたは受信されるパケットをフィルタリングします。このグループは、VLAN 内でブリッジングされるパケットに影響を与えません。

着信 ACL の場合、パケットの受信後スイッチはパケットを ACL と照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

発信 ACL の場合、パケットを受信し制御対象インターフェイスにルーティングしたあと、スイッチはパケットを ACL と照合します。ACL がパケットを許可した場合は、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスの ACL または発信インターフェイスの ACL のいずれであっても、常に入力インターフェイスから ICMP 到達不能メッセージが送信されます。ICMP 到達不能メッセージは通常、入力インターフェイス 1 つにつき、0.5 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

# ACL の設定方法

## IPv4 ACL の設定

スイッチで IP ACL を使用するには、次の手順に従います。

手順

**ステップ 1** アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。

**ステップ 2** その ACL をインターフェイスまたは端末回線に適用します。標準および拡張 IP ACL を VLAN マップに適用することもできます。

## 番号付き標準 ACL の作成（CLI）

番号付き標準 ACL を作成するには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **access-list** *access-list-number* {**deny** \| **permit**} *source source-wildcard* ]<br>例：<br>デバイス(config)# **access-list 2 deny your_host** | 送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。<br>*access-list-number* には、1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。<br>条件が一致した場合にアクセスを拒否する場合は **deny** を指定し、許可する場合は **permit** を指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | *source* には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。<br>• ドット付き 10 進表記による 32 ビット長の値。<br>• キーワード **any** は 0.0.0.0 255.255.255.255 という *source* および *source-wildcard* の省略形です。source-wildcard を入力する必要はありません。<br>• キーワード **host** は送信元および *source* 0.0.0.0 の *source-wildcard* の省略形です。<br>（任意）*source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。<br>（注） ロギングは、レイヤ 3 インターフェイスに割り当てられた ACL でだけサポートされます。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# 番号付き拡張 ACL の作成（CLI）

番号付き拡張 ACL を作成するには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **access-list** *access-list-number* {**deny** \| **permit**} *protocol source source-wildcard destination destination-wildcard* [ **precedence** *precedence*] [**tos** tos] [**fragments**] [**log** [**log-input**] [ **time-range** *time-range-name*] [ **dscp** *dscp*]<br>例：<br>デバイス(config)# **access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log** | 拡張 IPv4 アクセス リストおよびアクセス条件を定義します。<br>*access-list-number* には、100 ～ 199 または 2000 ～ 2699 の 10 進数を指定します。<br>条件が一致した場合にパケットを拒否する場合は **deny** を指定し、許可する場合は **permit** を指定します。<br>*protocol* には、インターネット プロトコルの名前または番号を入力します。**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、**udp**、または IP プロトコル番号を表す 0 ～ 255 の整数を使用できます。一致条件としてインターネット プロトコル（ICMP、TCP、UDP など）を指定するには、キーワード **ip** を使用します。<br>（注） この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加の特定パラメータについては、次のステップを参照してください。<br>*source* には、パラメータの送信元であるネットワークまたはホストの番号を指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | *source-wildcard* は、ワイルドカードビットを送信元アドレスに適用します。<br><br>*destination* には、パラメータの宛先であるネットワークまたはホストの番号を指定します。<br><br>*destination-wildcard* は、ワイルドカードビットを宛先アドレスに適用します。<br><br>source、source-wildcard、destination、および destination-wildcard の値は、次の形式で指定します。<br><br>• ドット付き 10 進表記による 32 ビット長の値。<br><br>• 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード **any**。<br><br>• 単一のホスト 0.0.0.0 を表すキーワード **host**。<br><br>その他のキーワードはオプションであり、次の意味を持ちます。<br><br>• **precedence**：パケットを 0 ～ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、**routine**（0）、**priority**（1）、**immediate**（2）、**flash**（3）、**flash-override**（4）、**critical**（5）、**internet**（6）、**network**（7）です。<br><br>• **fragments**：2 つ目以降のフラグメントをチェックする場合に入力します。<br><br>• **tos**：パケットを 0 ～ 15 の番号または名前で指定するサービス タイプ レベルと一致させる場合に入力します。指定できる値は、**normal**（0）、**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）です。<br><br>• **log**：エントリと一致するパケットに関するログ通知メッセージを作成 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | し、コンソールに送信します。<br>**log-input** を指定すると、ログ エントリに入力インターフェイスが追加されます。<br>• **time-range**：時間範囲の名前を指定します。<br>• **dscp**：パケットを 0 ～ 63 の番号で指定する DSCP 値と一致させる場合に入力します。または、指定できる値のリストを表示するには、疑問符（?）を使用します。<br>（注） コントローラは次の機能をサポートしている必要があります。<br>• DCSP のマーク<br>• UP のマーク<br>• DSCP と UP のマッピング<br>「DSCP から UP へのマッピング」の詳細については、次を参照してください。<br>https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-01<br>（注） **dscp** 値を入力する場合は、**tos** または **precedence** を入力できません。**dscp** を入力せずに **tos** と **precedence** の両方の値を入力できます。 |
| ステップ 3 | **access-list** *access-list-number* {**deny** \| **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] **[established]** [ **precedence** *precedence*] [ **tos** *tos*] [**fragments**] [**log** [**log-input**] [ **time-range** *time-range-name*] [ **dscp** *dscp*] [*flag*] | 拡張 TCP アクセス リストおよびアクセス条件を定義します。<br>次に示す例外を除き、拡張 IPv4 ACL に対して説明するパラメータと同じパラメータを使用します。<br>（任意）*operator* および *port* を入力すると、送信元ポート（*source* |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | 例：<br><br>デバイス(config)# **access-list 101 permit tcp any any eq 500** | *source-wildcard* の後に入力した場合）または宛先ポート（*destination destination-wildcard* の後に入力した場合）が比較されます。演算子の候補には、**eq**（次の値に等しい）、**gt**（次の値より大きい）、**lt**（次の値より小さい）、**neq**（次の値に等しくない）、および**range**（次の範囲）があります。演算子にはポート番号を指定する必要があります（range の場合は 2 つのポート番号をスペースで区切って指定する必要があります）。<br><br>*port* には、10 進数（0 ～ 65535）のポート番号または TCP ポート名を入力します。TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。<br><br>他のオプションのキーワードの意味は次のとおりです。<br><br>• **established**：確立された接続と照合する場合に入力します。このキーワードは、**ack** または **rst** フラグでの照合と同じ機能を果たします。<br><br>• *flag*：指定された TCP ヘッダー ビットを基準にして照合します。入力できるフラグは、**ack**（確認応答）、**fin**（終了）、**psh**（プッシュ）、**rst**（リセット）、**syn**（同期）、または **urg**（緊急）です。 |
| ステップ 4 | **access-list** *access-list-number* {**deny** \| **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [ **precedence** *precedence*] [ **tos** *tos*] [**fragments**] [**log** [**log-input**] [ **time-range** *time-range-name*] [ **dscp** *dscp*]<br><br>例：<br><br>デバイス(config)# **access-list 101 permit udp any any eq 100** | （任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。<br><br>UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[operator [port]] ポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP では、**flag**と **established** キーワードは無効です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **access-list** *access-list-number* {**deny** \| **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* \| [[*icmp-type icmp-code*] \| [*icmp-message*]] [ **precedence** *precedence*] [ **tos** *tos*] [**fragments**] [ **time-range** *time-range-name*] [ **dscp** *dscp*]<br>例：<br>デバイス(config)# **access-list 101 permit icmp any any 200** | 拡張 ICMP アクセス リストおよびアクセス条件を定義します。<br>ICMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。<br>• *icmp-type*：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。<br>• *icmp-code*：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。<br>• *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。 |
| ステップ 6 | **access-list** *access-list-number* {**deny** \| **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [ **precedence** *precedence*] [ **tos** *tos*] [**fragments**] [**log** [**log-input**] [ **time-range** *time-range-name*] [ **dscp** *dscp*]<br>例：<br>デバイス(config)# **access-list 101 permit igmp any any 14** | （任意）拡張 IGMP アクセス リストおよびアクセス条件を定義します。<br>IGMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。<br>*igmp-type*IGMP メッセージタイプと比較するには、0 ～ 15 の番号またはメッセージ名（**dvmrp**、**host-query**、**host-report**、**pim**、または **trace**）を入力します。 |
| ステップ 7 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

# 名前付き標準 ACL の作成

名前を使用して標準 ACL を作成するには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip access-list standard** *name*<br>例：<br>デバイス(config)# **ip access-list standard 20** | 名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。<br>名前には、1 ～ 99 の番号を使用できます。 |
| ステップ 4 | 次のいずれかを使用します。<br>• **deny** {*source* [*source-wildcard*] \| **host** *source* \| **any**} [**log**]<br>• **permit** {*source* [*source-wildcard*] \| **host** *source* \| **any**} [**log**]<br>例：<br>デバイス(config-std-nacl)# **deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255**<br>または<br>デバイス(config-std-nacl)# **permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0** | アクセス リスト コンフィギュレーション モードで、パケットを転送するのかドロップするのかを決定する 1 つ以上の拒否条件または許可条件を指定します。<br>• **host** *source*：送信元および送信元ワイルドカードの値である *source* 0.0.0.0。<br>• **any**：送信元および送信元ワイルドカードの値である 0.0.0.0 255.255.255.255 |
| ステップ 5 | **end**<br>例： | 特権 EXEC モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-std-nacl)# **end** | |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# 名前付き拡張 ACL の作成

名前を使用して拡張 ACL を作成するには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip access-list extended** *name*<br>例：<br>デバイス(config)# **ip access-list extended 150** | 名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。<br>名前には、100 ～ 199 の番号を使用できます。 |
| ステップ 4 | {**deny** \| **permit**} *protocol* {*source* [*source-wildcard*] \| **host** *source* \| **any**} {*destination* [*destination-wildcard*] \| host | アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。**log** キーワードを使用す |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | *destination* \| **any**} [ **precedence** *precedence*] [ **tos** *tos*] **[established]** [**log**] [ **time-range** *time-range-name*]<br>例：<br>デバイス(config-ext-nacl)# **permit 0 any any** | ると、違反を含むアクセス リストのログ メッセージを取得できます。<br>• **host** *source*：送信元および送信元ワイルドカードの値である *source* 0.0.0.0。<br>• **host** *destination*：接続先および接続先ワイルドカードの値である *destination* 0.0.0.0。<br>• **any**：source および source wildcard の値または destination および destination wildcard の値である 0.0.0.0 255.255.255.255 |
| ステップ 5 | **end**<br>例：<br>デバイス(config-ext-nacl)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、関連付けられた IP ホスト アドレス アクセス リストの指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に選択的に追加できません。ただし、**no permit** および **no deny** アクセスリスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

### 次のタスク

作成した名前付き ACL は、インターフェイスまたは VLAN に適用できます。

## ACL の時間範囲の設定

ACL の時間範囲パラメータを設定するには、次の手順に従ってください。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`デバイス(config)# enable` | 特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`デバイス# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **time-range** *time-range-name*<br>例：<br>`デバイス(config)# time-range workhours` | 作成する時間範囲には意味のある名前（*workhours* など）を割り当て、時間範囲コンフィギュレーション モードを開始します。名前にスペースや疑問符を含めることはできません。また、文字から始める必要があります。 |
| ステップ 4 | 次のいずれかを使用します。<br>• **absolute** [ **start** *time date*] [**end** *time date*]<br>• **periodic** *day-of-the-week hh:mm to* [*day-of-the-week*] *hh:mm*<br>• **periodic** {**weekdays** \| **weekend** \| **daily**} *hh:mm to hh:mm*<br>例：<br>`デバイス(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006`<br>または<br>`デバイス(config-time-range)# periodic` | 適用対象の機能がいつ動作可能になるかを指定します。<br>• 時間範囲には、**absolute** ステートメントを 1 つだけ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。<br>• 複数の **periodic** ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。<br>設定例を参照してください。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `weekdays 8:00 to 12:00` | |
| ステップ 5 | **end**<br>例：<br>`デバイス(config)# end` | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>`デバイス# show running-config` | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>`デバイス# copy running-config startup-config` | （任意）コンフィギュレーション ファイルに設定を保存します。 |

### 次のタスク

複数の項目をそれぞれ異なる時間に有効にする場合は、上記の手順を繰り返してください。

## 端末回線への IPv4 ACL の適用

番号付き ACL を使用して、1 つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

仮想端末回線と ACL に指定されたアドレス間の着信接続および発信接続を制限するには、次の手順を実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`デバイス(config)# enable` | 特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例： | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **configure terminal** | |
| ステップ 3 | **line** [**console** \| **vty**] *line-number*<br>例：<br>デバイス(config)# **line console 0** | 設定する回線を指定し、インライン コンフィギュレーション モードを開始します。<br>• **console**：コンソール端末回線を指定します。コンソール ポートは DCE です。<br>• **vty**：リモート コンソール アクセス用の仮想端末を指定します。<br>*line-number* は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。指定できる範囲は0～16です。 |
| ステップ 4 | **access-class** *access-list-number* {**in** \| **out**}<br>例：<br>デバイス(config-line)# **access-class 10 in** | （デバイスへの）特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信接続および発信接続を制限します。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config-line)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# インターフェイスへの IPv4 ACL の適用（CLI）

ここでは、IPv4 ACL をネットワーク インターフェイスへ適用する方法について説明します。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`デバイス# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>`デバイス(config)# interface gigabitethernet1/0/1` | 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。<br>インターフェイスには、レイヤ 2 インターフェイス（ポート ACL）またはレイヤ3インターフェイス（ルータ ACL）を指定できます。 |
| ステップ 3 | **ip access-group** {*access-list-number* \| *name*} {**in** \| **out**}<br>例：<br>`デバイス(config-if)# ip access-group 2 in` | 指定されたインターフェイスへのアクセスを制御します。 |
| ステップ 4 | **end**<br>例：<br>`デバイス(config-if)# end` | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config**<br>例：<br>`デバイス# show running-config` | アクセス リストの設定を表示します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>`デバイス# copy running-config` | （任意）コンフィギュレーション ファイルに設定を保存します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | **startup-config** | |

# 名前付き MAC 拡張 ACL の作成

VLAN またはレイヤ 2 インターフェイスで非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。その手順は、他の名前付き拡張 ACL を設定する場合と同様です。

名前付き MAC 拡張 ACL を作成するには、次の手順に従ってください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **mac access-list extended** *name*<br>例：<br>デバイス(config)# **mac access-list extended mac1** | 名前を使用して MAC 拡張アクセス リストを定義します。 |
| ステップ 4 | {**deny** \| **permit**} {**any** \| **host** *source MAC address* \| *source MAC address mask*} {**any** \| **host** *destination MAC address* \| *destination MAC address mask*} [*type mask* \| **lsap** *lsap mask* \| **aarp** \| **amber** \| **dec-spanning** \| **decnet-iv** \| **diagnostic** \| **dsm** \| **etype-6000** \| **etype-8042** \| **lat** \| **lavc-sca** \| **mop-console** \| **mop-dump** \| **msdos** \| **mumps** \| **netbios** \| **vines-echo** \| **vines-ip** \| **xns-idp** \| 0-*65535*] [**cos** *cos*]<br>例：<br>デバイス(config-ext-macl)# **deny any any** | 拡張MACアクセス リスト コンフィギュレーション モードでは、すべての送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定の**host**の送信元MACアドレスと、**any**の宛先MACアドレス、マスク付き宛先MACアドレス、または特定の宛先 MAC アドレスに、**permit** または **deny** を指定します。<br>（任意）次のオプションを入力することもできます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | **decnet-iv**<br><br>または<br><br>デバイス(config-ext-macl)# **permit any any** | • *type mask*：Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号。10 進数、16 進数、または8進数で表記できます。一致検査の前に、任意で指定できる *don't care* ビットのマスクが EtherType に適用されます。<br><br>• **lsap** *lsap mask*：IEEE 802.2 でカプセル化されたパケットのLSAP番号。10 進数、16 進数、または 8 進数で表記できます。任意で *don't care* ビットのマスクを指定できます。<br><br>• **aarp** \| **amber** \| **dec-spanning** \| **decnet-iv** \| **diagnostic** \| **dsm** \| **etype-6000** \| **etype-8042** \| **lat** \| **lavc-sca** \| **mop-console** \| **mop-dump** \| **msdos** \| **mumps** \| **netbios** \| **vines-echo** \| **vines-ip** \| **xns-idp**：非 IP プロトコル。<br><br>• **cos** *cos*：プライオリティを設定する 0 ～ 7 の IEEE 802.1Q CoS 番号。 |
| ステップ 5 | **end**<br>例：<br><br>デバイス(config-ext-macl)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br><br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br><br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# レイヤ 2 インターフェイスへの MAC ACL の適用

レイヤ 2 インターフェイスへのアクセスを制御するために MAC アクセス リストを適用するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet1/0/2** | 特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。指定するインターフェイスは物理レイヤ 2 インターフェイス（ポート ACL）でなければなりません。 |
| ステップ 4 | **mac access-group** {*name*} {**in** \| **out** } | MAC アクセス リストを使用して、指定されたインターフェイスへのアクセスを制御します。<br>ポート ACL は発信および着信方向サポートされます。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show mac access-group** [ **interface** *interface-id*]<br>例：<br>デバイス# **show mac access-group interface gigabitethernet1/0/2** | そのインターフェイスまたはすべてのレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 7 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 8 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |

スイッチは、パケットを受信すると、着信 ACL とパケットを照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

# VLAN マップの設定

VLAN マップを作成して 1 つまたは複数の VLAN に適用するには、次の手順に従います。

### 始める前に

VLAN に適用する標準 IPv4 ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **vlan access-map** *name* [**number**]<br>例：<br>デバイス(config)# **vlan access-map map_1 20** | VLANマップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。<br>同じ名前のVLANマップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。<br>VLAN マップでは、特定の permit または deny キーワードを使用しません。VLANマップを使用してパケットを拒否するには、パケットを照合する ACL を |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 作成して、アクションをドロップに設定します。ACL 内の permit は、一致するという意味です。ACL 内の deny は、一致しないという意味です。<br>このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。 |
| **ステップ 2** | **match** {**ip** \| **mac**} **address** {*name* \| *number*} [*name* \| *number*]<br>例：<br>`デバイス(config-access-map)# match ip address ip2` | 1 つまたは複数の標準または拡張アクセス リストに対してパケットを照合します（IP または MAC アドレスを使用）。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ照合されます。<br>（注） パケット タイプ（IP または MAC）に対する match 句が VLAN マップに設定されている場合で、そのマップ アクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。match 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。 |
| **ステップ 3** | IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1 つ以上の ACL（標準または拡張）とそのパケットを照合するには、次のコマンドのいずれかを入力します。<br>• **action** { **forward**}<br>`デバイス(config-access-map)# action forward`<br>• **action** { **drop**} | マップ エントリに対するアクションを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-access-map)# **action drop** | |
| ステップ 4 | **vlan filter** *mapname* **vlan-list** *list*<br>例：<br>デバイス(config)# **vlan filter map 1 vlan-list 20-22** | VLANマップを1つまたは複数のVLANに適用します。<br>listには単一のVLAN ID（22）、連続した範囲（10 ～ 22）、またはVLAN IDのストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。 |

# VLAN マップの作成

各 VLAN マップは順番に並べられた一連のエントリで構成されます。VLAN マップ エントリを作成、追加、または削除するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **vlan access-map** *name* [**number**]<br>例：<br>デバイス(config)# **vlan access-map map_1 20** | VLANマップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。<br>同じ名前のVLANマップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。<br>VLAN マップでは、特定の permit または deny キーワードを使用しません。VLANマップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致する |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | という意味です。ACL 内の deny は、一致しないという意味です。<br>このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。 |
| ステップ 3 | **match** {**ip** \| **mac**} **address** {*name* \| *number*} [*name* \| *number*]<br>例：<br>`デバイス(config-access-map)# match ip address ip2` | 1 つまたは複数の標準または拡張アクセス リストに対してパケットを照合します（IP または MAC アドレスを使用）。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ照合されます。 |
| ステップ 4 | **action** {**drop** \| **forward**}<br>例：<br>`デバイス(config-access-map)# action forward` | （任意）マップ エントリに対するアクションを設定します。デフォルトは転送（forward）です。 |
| ステップ 5 | **end**<br>例：<br>`デバイス(config-access-map)# end` | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>`デバイス# show running-config` | アクセス リストの設定を表示します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>`デバイス# copy running-config startup-config` | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# VLAN への VLAN マップの適用

VLAN マップを 1 つまたは複数の VLAN に適用するには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | | |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **vlan filter** *mapname* **vlan-list** *list*<br>例：<br>デバイス(config)# **vlan filter map 1 vlan-list 20-22** | VLAN マップを 1 つまたは複数の VLAN に適用します。<br>list には単一の VLAN ID（22）、連続した範囲（10 ～ 22）、または VLAN ID のストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config**<br>例：<br>デバイス# **show running-config** | アクセス リストの設定を表示します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# IPv4 ACL のモニタリング

スイッチに設定されている ACL、およびインターフェイスと VLAN に適用された ACL を表示して IPv4 ACL をモニタできます。

**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 またはレイヤ 3 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセス グループを表示できます。また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、次の表に記載された特権 EXEC コマンドを使用します。

表 *20*：アクセス リストおよびアクセス グループを表示するコマンド

| コマンド | 目的 |
|---|---|
| **show access-lists** [*number* \| *name*] | 最新の IP および MAC アドレス アクセス リストの全体やその一部、または特定のアクセス リスト（番号付きまたは名前付き）の内容を表示します。 |
| **show ip access-lists** [*number* \| *name*] | 最新の IP アクセス リスト全体、または特定の IP アクセス リスト（番号付きまたは名前付き）を表示します。 |
| **show ip interface** *interface-id* | インターフェイスの詳細設定およびステータスを表示します。IP がイネーブルになっているインターフェイスに、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示に含まれます。 |
| **show running-config** [ **interface** *interface-id*] | スイッチまたは指定されたインターフェイスのコンフィギュレーションファイルの内容（設定されたすべての MAC および IP アクセス リストや、どのアクセスグループがインターフェイスに適用されたかなど）を表示します。 |
| **show mac access-group** [ **interface** *interface-id*] | すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リスト<br>を表示します。 |

# ACL の設定例

## 例：ACL での時間範囲を使用

次の例に、*workhours*（営業時間）の時間範囲および会社の休日（2006 年 1 月 1 日）を設定し、設定を確認する例を示します。

```
デバイス# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に時間範囲名を入力します。次に、拡張アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての TCP トラフィックを許可します。

```
デバイス(config)# access-list 188 deny tcp any any time-range new_year_day_2006
デバイス(config)# access-list 188 permit tcp any any time-range workhours
デバイス(config)# end
デバイス# show access-lists
Extended IP access list 188
   10 deny tcp any any time-range new_year_day_2006 (inactive)
   20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
デバイス(config)# ip access-list extended deny_access
デバイス(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
デバイス(config-ext-nacl)# exit
デバイス(config)# ip access-list extended may_access
デバイス(config-ext-nacl)# permit tcp any any time-range workhours
デバイス(config-ext-nacl)# end
デバイス# show ip access-lists
Extended IP access list lpip_default
    10 permit ip any any
Extended IP access list deny_access
    10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
    10 permit tcp any any time-range workhours (inactive)
```

# 例：ACL へのコメントの挿入

**remark** キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント（注釈）を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、permit ステートメントまたは deny ステートメントの前後どちらにでも配置できます。コメントがどの permit ステートメントまたは deny ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する permit または deny ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list** *access-list number* **remark** *remark* グローバル コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
デバイス(config)# access-list 1 remark Permit only Jones workstation through
デバイス(config)# access-list 1 permit 171.69.2.88
デバイス(config)# access-list 1 remark Do not allow Smith through
デバイス(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリには、**remark** アクセスリスト コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

```
デバイス(config)# ip access-list extended telnetting
デバイス(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
デバイス(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

# IPv4 ACL の設定例

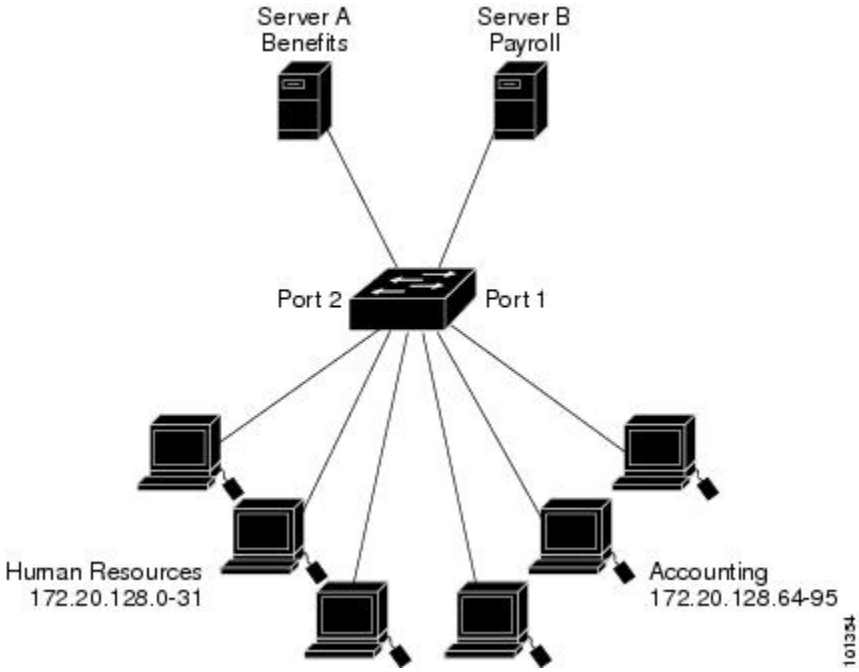
ここでは、IPv4 ACL を設定および適用する例を示します。ACL のコンパイルに関する詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』および『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Adderssing and Services」の章にある「Configuring IP Services」の項を参照してください。

## 小規模ネットワークが構築されたオフィス用の ACL

**図 *8*：ルータ *ACL* によるトラフィックの制御**

次に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッド ポート 2 に接続されたサーバ A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されて

います。サーバAにはすべてのユーザがアクセスできますが、サーバBにアクセスできるユーザは制限されています。




ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバに着信するトラフィックをフィルタリングします。
- 拡張 ACL を作成し、サーバからポート 1 に着信するトラフィックをフィルタリングします。

## 例：小規模ネットワークが構築されたオフィスの ACL

次に、標準ACLを使用してポートからサーバBに着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ～ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッド ポート 1 から送信されるトラフィックに適用されます。

```
デバイス(config)# access-list 6 permit 172.20.128.64 0.0.0.31
デバイス(config)# end
デバイス# how access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 6 out
```

次に、拡張ACLを使用してサーバBからポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバ B）から経理部の宛先アドレス 172.20.128.64 ～ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。このACLは、ルーテッドポート1に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィッ

クだけを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前に、プロトコル（IP）を入力する必要があります。

```
デバイス(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
デバイス(config)# end
デバイス# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 106 in
```

## 例：番号付き ACL

次の例のネットワーク 10.0.0.0 は、2 番目のオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネットマスクは255.255.0.0です。ネットワーク 10.0.0.0アドレスの3番目および4番目のオクテットで特定のホストを指定します。アクセス リスト2を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセス リストの最終行は、ネットワーク 10.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。この ACL は、ポートに着信するパケットに適用されます。

```
デバイス(config)# access-list 2 permit 10.48.0.3
デバイス(config)# access-list 2 deny 10.48.0.0 0.0.255.255
デバイス(config)# access-list 2 permit 10.0.0.0 0.255.255.255
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# ip access-group 2 in
```

## 例：拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番めの行は、ホスト 128.88.1.2 の SMTP ポートへの着信 TCP 接続を許可します。3 番めの行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
デバイス(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
デバイス(config)# access-list 102 permit icmp any any
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。ただし、IP ホストからは、専用メール ホストのメール（SMTP）ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。発信パケットのポート番号は予約されています。安全なネッ

トワーク システムでは常にポート 25 でのメール接続が使用されているため、着信サービスと発信サービスを個別に制御できます。ACL は発信インターフェイスの入力 ACL および着信インターフェイスの出力 ACL として設定される必要があります。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 102 in
```

次の例では、ネットワークはアドレスが 128.88.0.0 のクラス B ネットワークで、メール ホストのアドレスは 128.88.1.2 です。**established** キーワードは、確立された接続を表示する TCP 専用のキーワードです。TCP データグラムに ACK または RST ビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。スタック メンバー 1 のギガビット イーサネット インターフェイス 1 は、ルータをインターネットに接続するインターフェイスです。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
デバイス(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 102 in
```

## 例：名前付き ACL

### 名前付き標準 ACL および名前付き拡張 ACL の作成

次に、*Internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。*Internet_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
デバイス(config)# ip access-list standard Internet_filter
デバイス(config-ext-nacl)# permit 1.2.3.4
デバイス(config-ext-nacl)# exit
```

*marketing_group* ACL は、宛先アドレスとワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ～ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
デバイス(config)# ip access-list extended marketing_group
デバイス(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
デバイス(config-ext-nacl)# deny tcp any any
デバイス(config-ext-nacl)# permit icmp any any
デバイス(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
デバイス(config-ext-nacl)# deny ip any any log
デバイス(config-ext-nacl)# exit
```

*Internet_filter* ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
デバイス(config)# interface gigabitethernet3/0/1
デバイス(config-if)# no switchport
デバイス(config-if)# ip address 2.0.5.1 255.255.255.0
デバイス(config-if)# ip access-group Internet_filter out
デバイス(config-if)# ip access-group marketing_group in
```

### 名前付き ACL からの個別 ACE の削除

次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```
デバイス(config)# ip access-list extended border-list
デバイス(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

## 例：IP ACL に適用される時間範囲

次に、月曜日から金曜日の午前 8 時 〜午後 6 時（18 時）の間、IP の HTTP トラフィックを拒否する例を示します。UDP トラフィックは、土曜日および日曜日の正午〜午後 8 時（20 時）の間だけ許可されます。

```
デバイス(config)# time-range no-http
デバイス(config)# periodic weekdays 8:00 to 18:00
!
デバイス(config)# time-range udp-yes
デバイス(config)# periodic weekend 12:00 to 20:00
!
デバイス(config)# ip access-list extended strict
デバイス(config-ext-nacl)# deny tcp any any eq www time-range no-http
デバイス(config-ext-nacl)# permit udp any any time-range udp-yes
!
デバイス(config-ext-nacl)# exit
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# ip access-group strict in
```

## 例：コメント付き IP ACL エントリの設定

次に示す番号付き ACL の例では、Jones が所有するワークステーションにはアクセスを許可し、Smith が所有するワークステーションにはアクセスを許可しません。

```
デバイス(config)# access-list 1 remark Permit only Jones workstation through
デバイス(config)# access-list 1 permit 171.69.2.88
デバイス(config)# access-list 1 remark Do not allow Smith workstation through
デバイス(config)# access-list 1 deny 171.69.3.13
```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しません。

```
デバイス(config)# access-list 100 remark Do not allow Winter to browse the web
デバイス(config)# access-list 100 deny host 171.69.3.85 any eq www
デバイス(config)# access-list 100 remark Do not allow Smith to browse the web
デバイス(config)# access-list 100 deny host 171.69.3.13 any eq www
```

次に示す名前付き ACL の例では、Jones のサブネットにアクセスを許可しません。

```
デバイス(config)# ip access-list standard prevention
デバイス(config-std-nacl)# remark Do not allow Jones subnet through
デバイス(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次に示す名前付き ACL の例では、Jones のサブネットに発信 Telnet の使用を許可しません。

```
デバイス(config)# ip access-list extended telnetting
デバイス(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
デバイス(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

## 例：ACL ロギング

ACL では 2 種類のロギングがサポートされています。**log** キーワードを指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。**log-input** キーワードを指定すると、ログ エントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセス リスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。**log** キーワードも指定されています。

```
デバイス(config)# ip access-list standard stan1
デバイス(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
デバイス(config-std-nacl)# permit any log
デバイス(config-std-nacl)# exit
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group stan1 in
デバイス(config-if)# end
デバイス# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 37 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 37 messages logged
    File logging: disabled
    Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems

<output truncated>
```

```
00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次に、名前付き拡張アクセス リスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```
デバイス(config)# ip access-list extended ext1
デバイス(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
デバイス(config-ext-nacl)# deny udp any any log
デバイス(config-std-nacl)# exit
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# ip access-group ext1 in
```

次に、拡張 ACL のログの例を示します。

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
01:26:12:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1
packet
01:31:33:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8
packets
```

IP ACL のすべてのロギング エントリは %SEC-6-IPACCESSLOG で開始します。エントリの形式は、一致した ACL やアクセス エントリの種類に応じて若干異なります。

次に、**log-input** キーワードを指定した場合の出力メッセージの例を示します。

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400)
 ->
10.1.1.61 (0/0), 1 packet
```

**log** キーワードを指定した場合、同様のパケットに関するログ メッセージには入力インターフェイス情報が含まれません。

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0),
 1 packet
```

# ACL および VLAN マップの設定例

## 例：パケットを拒否する ACL および VLAN マップの作成

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、*ip1* ACL（TCP パケット）に一致するすべてのパケットがドロップされます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する *ip1* ACL を作成します。VLAN マップには IP パケットに対する match 句が存在するため、デフォルトのアクションでは、どの match 句とも一致しない IP パケットがすべてドロップされます。

```
デバイス(config)# ip access-list extended ip1
デバイス(config-ext-nacl)# permit tcp any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map map_1 10
デバイス(config-access-map)# match ip address ip1
デバイス(config-access-map)# action drop
```

## 例：パケットを許可する ACL および VLAN マップの作成

次に、パケットを許可する VLAN マップを作成する例を示します。ACL *ip2* は UDP パケットを許可し、*ip2* ACL と一致するすべてのパケットが転送されます。このマップでは、これ以前のどの ACL とも一致しないすべての IP パケット（TCP でも UDP でもないパケット）がドロップされます。

```
デバイス(config)# ip access-list extended ip2
デバイス(config-ext-nacl)# permit udp any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map map_1 20
デバイス(config-access-map)# match ip address ip2
デバイス(config-access-map)# action forward
```

## 例：IP パケットのドロップおよび MAC パケットの転送のデフォルト アクション

次の例の VLAN マップでは、デフォルトで IP パケットがドロップされ、MAC パケットが転送されます。標準の ACL 101 および名前付き拡張アクセス リスト **igmp-match** および **tcp-match** をこのマップと組み合わせて使用すると、次のようになります。

- すべての UDP パケットが転送されます。
- すべての IGMP パケットがドロップされます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- すべての非 IP パケットが転送されます。

```
デバイス(config)# access-list 101 permit udp any any
デバイス(config)# ip access-list extended igmp-match
デバイス(config-ext-nacl)# permit igmp any any
```

```
デバイス(config-ext-nacl)# permit tcp any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map drop-ip-default 10
デバイス(config-access-map)# match ip address 101
デバイス(config-access-map)# action forward
デバイス(config-access-map)# exit
デバイス(config)# vlan access-map drop-ip-default 20
デバイス(config-access-map)# match ip address igmp-match
デバイス(config-access-map)# action drop
```

```
デバイス(config-access-map)# exit
デバイス(config)# vlan access-map drop-ip-default 30
デバイス(config-access-map)# match ip address tcp-match
デバイス(config-access-map)# action forward
```

## 例：MAC パケットのドロップおよび IP パケットの転送のデフォルト アクション

次の例の VLAN マップでは、デフォルトで MAC パケットがドロップされ、IP パケットが転送されます。MAC 拡張アクセス リスト **good-hosts** および **good-protocols** をこのマップと組み合わせて使用すると、次のようになります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- decnet-iv または vines-ip プロトコルを使用する MAC パケットが転送されます。
- その他のすべての非 IP パケットがドロップされます。
- すべての IP パケットが転送されます。

## 例：すべてのパケットをドロップするデフォルト アクション

次の例の VLAN マップでは、デフォルトですべてのパケット（IP および非 IP）がドロップされます。例 2 および例 3 のアクセス リスト **tcp-match** および **good-hosts** をこのマップと組み合わせて使用すると、次のようになります。

- すべての TCP パケットが転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- その他のすべての MAC パケットがドロップされます。

```
デバイス(config)# vlan access-map drop-all-default 10
デバイス(config-access-map)# match ip address tcp-match
デバイス(config-access-map)# action forward
デバイス(config-access-map)# exit
デバイス(config)# vlan access-map drop-all-default 20
デバイス(config-access-map)# match mac address good-hosts
デバイス(config-access-map)# action forward
```

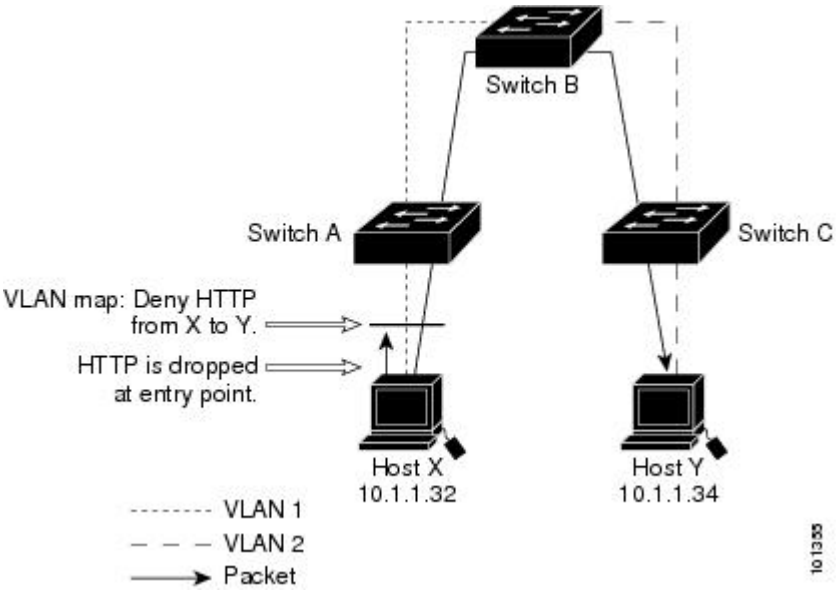
# ネットワークでの VLAN マップの使用方法の設定例

## 例：ワイヤリング クローゼットの設定

**図 *9*: ワイヤリング クローゼットの設定**

ワイヤリング クローゼット構成では、ルーティングがスイッチ上で有効にされていない場合があります。ただし、この設定でも VLAN マップおよび QoS 分類 ACL はサポートされています。ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリング クローゼット スイッチ

A およびスイッチ C に接続されていると想定します。ホスト X からホスト Y へのトラフィックは、ルーティングが有効に設定されたレイヤ 3 スイッチであるスイッチ B によって最終的にルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックのエントリ ポイントであるスイッチ A でアクセス コントロールできます。




HTTP トラフィックをホスト X からホスト Y へスイッチングしない場合は、ホスト X（IP アドレス 10.1.1.32）からホスト Y（IP アドレス 10.1.1.34）に向かうすべての HTTP トラフィックがスイッチ A でドロップされ、スイッチ B にブリッジングされないように、スイッチ A の VLAN マップを設定できます。

最初に、HTTP ポート上ですべての TCP トラフィックを許可（一致）する IP アクセス リスト *http* を定義します。

```
デバイス(config)# ip access-list extended http
デバイス(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
デバイス(config-ext-nacl)# exit
```

次に、*http* アクセス リストと一致するトラフィックがドロップされ、その他のすべての IP トラフィックが転送されるように、VLAN アクセス マップ *map2* を作成します。

```
デバイス(config)# vlan access-map map2 10
デバイス(config-access-map)# match ip address http
デバイス(config-access-map)# action drop
デバイス(config-access-map)# exit
デバイス(config)# ip access-list extended match_all
デバイス(config-ext-nacl)# permit ip any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map map2 20
デバイス(config-access-map)# match ip address match_all
デバイス(config-access-map)# action forward
```

次に、VLAN アクセス マップ *map2* を VLAN 1 に適用します。

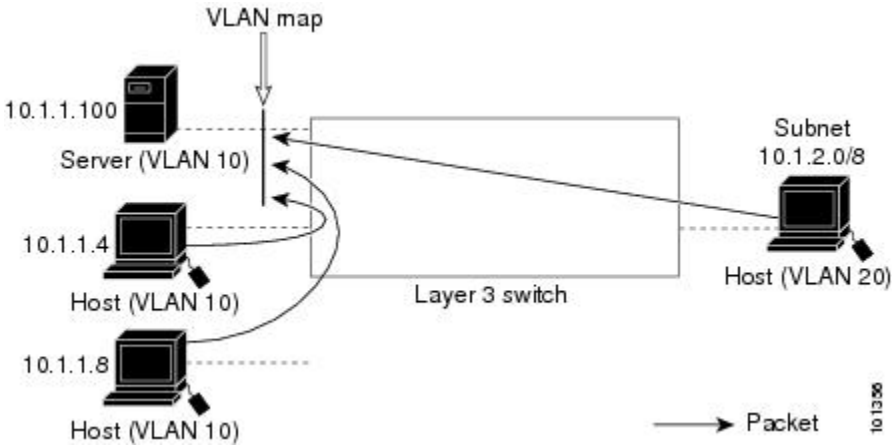
```
デバイス(config)# vlan filter map2 vlan 1
```

## 例：別の VLAN にあるサーバへのアクセスの制限

**図 *10*：別の *VLAN* 上のサーバへのアクセスの制限**

別の VLAN にあるサーバへのアクセスを制限できます。たとえば、VLAN 10 内のサーバ 10.1.1.100 では、次のホストへのアクセスを拒否する必要があります。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスを禁止します。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスを禁止します。




## 例：別の VLAN にあるサーバへのアクセスの拒否

次に、サブネット 10.1.2.0.8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 のアクセスを拒否し、その他の IP トラフィックを許可する VLAN マップ SERVER1-ACL を作成して、別の VLAN内のサーバへのアクセスを拒否する例を示します。最後のステップでは、マップSERVER1 を VLAN 10 に適用します。

正しいパケットと一致する IP ACL を定義します。

```
デバイス(config)# ip access-list extended SERVER1_ACL
デバイス(config-ext-nacl))# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
デバイス(config-ext-nacl))# permit ip host 10.1.1.4 host 10.1.1.100
デバイス(config-ext-nacl))# permit ip host 10.1.1.8 host 10.1.1.100
デバイス(config-ext-nacl))# exit
```

SERVER1_ACL と一致する IP パケットをドロップして、この ACL と一致しない IP パケットを転送する ACL を使用して、VLAN マップを定義します。

```
デバイス(config)# vlan access-map SERVER1_MAP
```

```
デバイス(config-access-map)# match ip address SERVER1_ACL
デバイス(config-access-map)# action drop
デバイス(config)# vlan access-map SERVER1_MAP 20
デバイス(config-access-map)# action forward
デバイス(config-access-map)# exit
```

VLAN 10 に VLAN マップを適用します。

```
デバイス(config)# vlan filter SERVER1_MAP vlan-list 10
```

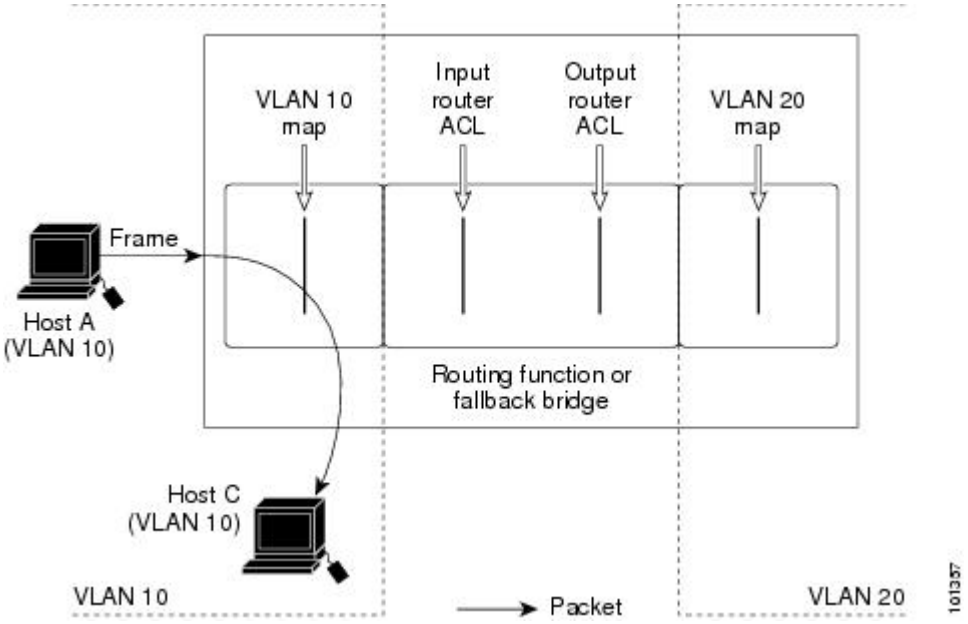
# VLAN に適用されるルータ ACL と VLAN マップの設定例

ここでは、ルータ ACL および VLAN マップを VLAN に適用し、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットを処理する例を示します。次の図ではそれぞれの宛先に転送されるパケットを示します。パケットのパスが VLAN マップや ACL を示す線と交差するポイントで、パケットを転送せずにドロップする可能性もあります。

## 例：ACL およびスイッチド パケット

**図 *11 :* スイッチド パケットへの *ACL* の適用**

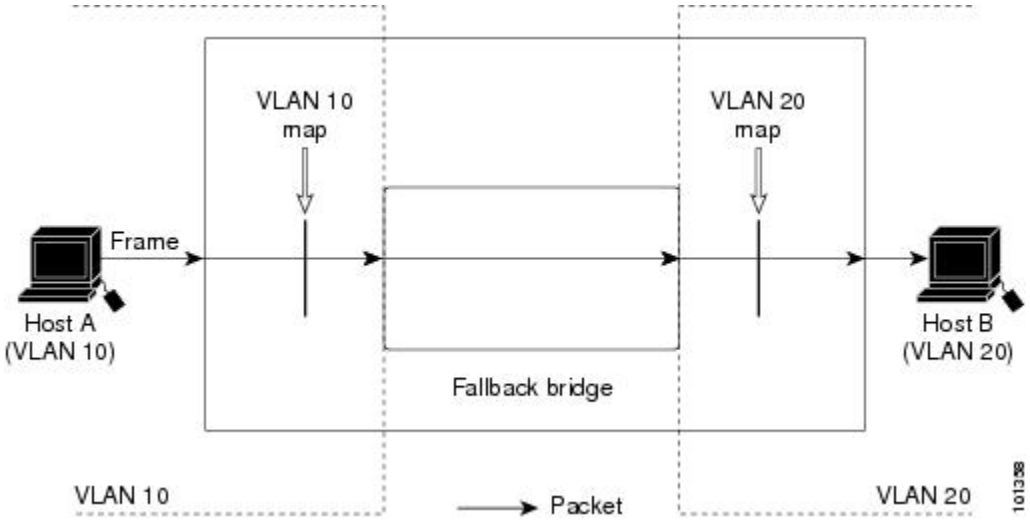
次の例に、VLAN 内でスイッチングされるパケットに ACL を適用する方法を示します。フォールバック ブリッジングによってルーティングまたは転送されず、VLAN 内でスイッチングされるパケットには、入力 VLAN の VLAN マップだけが適用されます。



## 例：ACL およびブリッジド パケット

図 *12*：ブリッジド パケットへの *ACL* の適用

次の例に、フォールバック ブリッジド パケットに ACL を適用する方法を示します。ブリッジド パケットの場合は、入力 VLAN にレイヤ 2 ACL だけが適用されます。また、非 IP および非 ARP パケットだけがフォールバック ブリッジド パケットとなります。

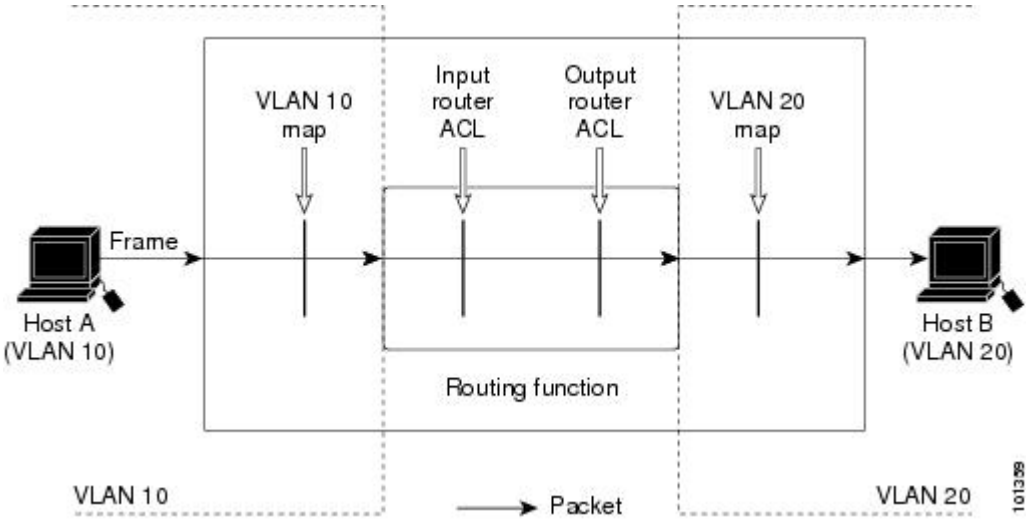



## 例：ACL およびルーテッド パケット

図 *13*：ルーテッド パケットへの *ACL* の適用

次の例に、ルーテッド パケットに ACL を適用する方法を示します。ACL は次の順番で適用されます。

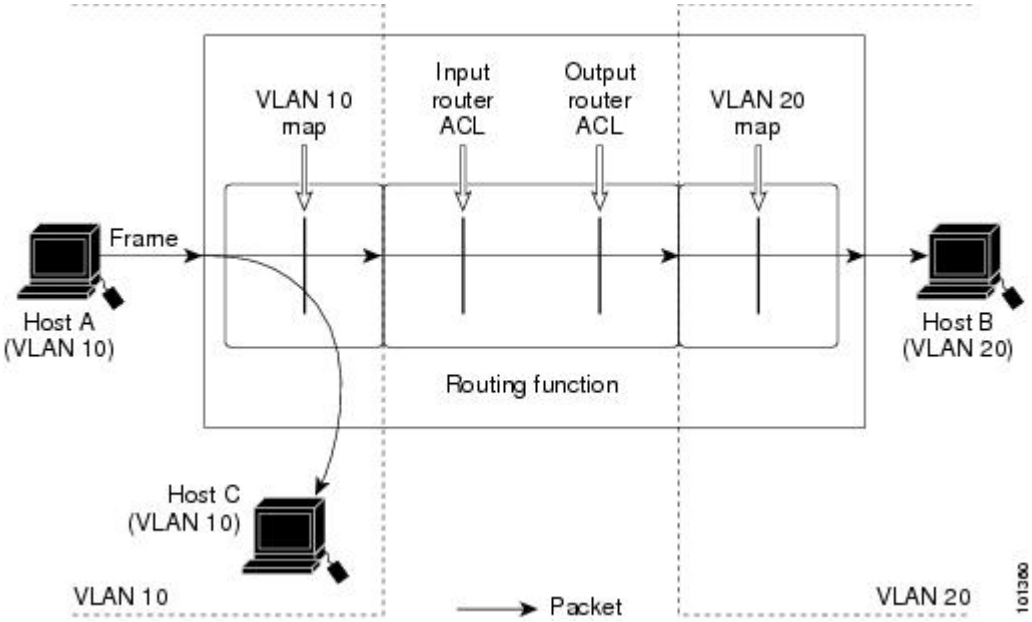
1. 入力 VLAN の VLAN マップ
2. 入力ルータ ACL
3. 出力ルータ ACL
4. 出力 VLAN の VLAN マップ




## 例：ACL およびマルチキャスト パケット

図 *14*：マルチキャスト パケットへの *ACL* の適用

次の例に、IPマルチキャスト用に複製されたパケットにACLを適用する方法を示します。ルーティングされるマルチキャストパケットには、2つの異なるフィルタが適用されます。1つは、宛先が入力VLAN内の他のポートである場合に使用され、もう1つは、宛先がパケットのルーティング先である別の VLAN 内にある場合に使用されます。パケットは複数の出力 VLAN にルーティングされる場合がありますが、この場合は宛先 VLAN ごとに異なるルータ出力 ACL およびVLANマップが適用されます。最終的に、パケットは一部の出力VLAN内で許可され、それ以外の VLAN で拒否されます。パケットのコピーが、許可された宛先に転送されます。ただし、入力 VLAN マップによってパケットがドロップされる場合、パケットのコピーは宛先に送信されません。



第 12 章

# IPv6 ACL


- IPv6 ACL の概要 （233 ページ）
- IPv6 ACL の制限 （236 ページ）
- IPv6 ACL のデフォルト設定 （237 ページ）
- IPv6 ACL の設定 （237 ページ）
- インターフェイスへの IPv6 ACL の付加 （242 ページ）
- VLAN マップの設定 （243 ページ）
- VLAN への VLAN マップの適用 （245 ページ）
- IPv6 ACL のモニタリング （246 ページ）


## IPv6 ACL の概要

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。また、スイッチで IP ベースおよび LAN ベース フィーチャ セットが稼働している場合、入力ルータ ACL を作成し、それを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

スイッチは、次の 3 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンド トラフィックまたはインバウンド トラフィックでサポートされます。IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。

- IPv6 ポート ACL は、アウトバウンドおよびインバウンドのレイヤ 2 インターフェイスでサポートされます。IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。

- VLAN ACL または VLAN マップは、VLAN 内のすべてのパケットのアクセスを制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。ACL VLAN マップは、L2 VLAN に適用されます。VLAN マップは、IPv6 のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されています。イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプ

ロトコルがアクセスコントロールされます。VLANマップをVLANに適用すると、VLANに入るすべてのパケットが VLAN マップと照合されます。

スイッチは、IPv6 トラフィックの VLAN ACL（VLAN マップ）をサポートします。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

# スイッチ スタックおよび IPv6 ACL

アクティブ スイッチは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバに配信します。

スタンバイ スイッチがアクティブ スイッチを引き継ぐと、ACL 設定がすべてのスタック メンバに配信されます。メンバ スイッチは、新しいアクティブ スイッチによって配信された設定を同期し、不要なエントリを消去します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、アクティブ スイッチは変更内容をすべてのスタック メンバーに配信します。

# ACL 優先順位

VLAN マップ、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、入力トラフィックの場合のフィルタの優先順位は上からポート ACL、VLAN マップ、およびルータ ACL です。出力トラフィックの場合、フィルタの優先順位は、ルータ ACL、VLAN マップ、ポート ACL です。

次の例で、簡単な使用例を説明します。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- スイッチ仮想インターフェイス（SVI）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

# VLAN マップ

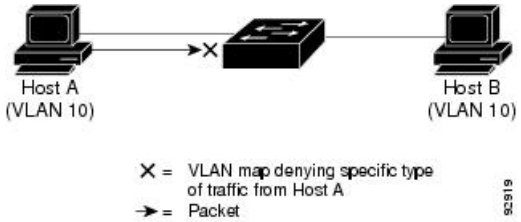
VLAN ACL または VLAN マップは、VLAN 内のネットワーク トラフィックを制御するために使用されます。スイッチまたはスイッチ スタックの VLAN 内でブリッジングされるすべてのパケットに VLAN マップを適用できます。VACL は、セキュリティ パケット フィルタリングおよび特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向（入力または出力）で定義されることはありません。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます（IP トラフィックは、MAC VACL マップではアクセス制御されません）。VLANマップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

VLANマップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

**図 *15 : VLAN* マップによるトラフィックの制御**

次の図に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用できます。




# 他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージ プロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチスタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリに空きがない場合、パケットはインターフェイスでドロップされ、アンロードのエラー メッセージが記録されます。

# IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは再起 ACL（**reflect** キーワード）をサポートしません。
- このリリースは、IPv6 のポート ACL、ルータ ACL および VLAN ACL（VLAN マップ）をサポートしています。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうか判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ（ACE）を追加しようとする場合、スイッチは現在インターフェイスに適用されている ACL に ACE が追加されるのを許可しません。

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム（IPv4 では **fragments** キーワード）がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。
- スイッチのハードウェア スペースがなくなった場合、ACL に関連付けられたパケットはインターフェイスでドロップされます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。

- スイッチは、プレフィックス長の最大範囲の IPv6 アドレス一致をサポートしません。

# IPv6 ACL のデフォルト設定

デフォルトの IPv6 ACL 設定は次のとおりです。

```
Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

# IPv6 ACL の設定

IPv6 トラフィックをフィルタリングするには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | [**no**]{**ipv6 access-list** *list-name*\| **client permit-control-packets**\| **log-update threshold**\| **role-based** *list-name*}<br>例：<br>デバイス(config)# **ipv6 access-list example_acl_list** | IPv6 ACL 名を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。 |
| ステップ 4 | [**no**]{**deny** \| **permit**} protocol {*source-ipv6-prefix/* \|*prefix-length* \|**any threshold**\| **host** *source-ipv6-address*} [ | 条件が一致した場合にパケットを拒否する場合は deny、許可する場合は |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | operator [ *port-number* ]] { *destination-ipv6-prefix/ prefix-length* \| **any** \| **host** *destination-ipv6-address*} [operator [*port-number*]][ **dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [ **sequence** *value*] [ **time-range** *name*] | permit を指定します。次に、条件について説明します。<br>• protocol には、IP の名前または番号を入力します。 **ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、**udp** または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。<br>• *source-ipv6-prefix/prefix-length* または *destination-ipv6-prefix/ prefix-length* は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。<br>• IPv6 プレフィックス ::/0 の短縮形として、**any** を入力します。<br>• **host** *source-ipv6-address* または *destination-ipv6-address* には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホストアドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。<br>• （任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、および **range**（包含範囲）があります。<br>*source-ipv6-prefix/prefix-length* 引数のあとの operator は、送信元ポートに一致する必要があります。*destination-ipv6- prefix/prefix-length* 引数のあとの operator は、宛先ポートに一致する必要があります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • （任意）**port-number** は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。<br>• （任意）**dscp** value を入力して、各 IPv6 パケットヘッダーの Traffic Class フィールド内のトラフィッククラス値と DiffServ コードポイント値を照合します。指定できる範囲は 0 ～ 63 です。<br>• （任意）**fragments** を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。<br>• （任意）**log** を指定すると、エントリと一致するパケットに関するログメッセージがコンソールに送信されます。**log-input** を指定すると、ログエントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。<br>• （任意）**routing** を入力して、IPv6 パケットのルーティングを指定します。<br>• （任意）**sequence** *value* を入力して、アクセスリストステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4,294,967,295 です。<br>• （任意）**time-range** name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | {**deny** \| **permit**} **tcp** {*source-ipv6-prefix/prefix-length* \| **any** \| **host** *source-ipv6-address*} [**operator** [**port-number**]] {*destination-ipv6-prefix/prefix-length* \| **any** \| **host** *destination-ipv6-address*} [operator [*port-number*]] [**ack**] [ **dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {**port** \| protocol}] [**psh**] [**range** {**port** \| protocol}] [**rst**] [**routing**] [ **sequence** *value*] [**syn**] [ **time-range** *name*] [**urg**] | （任意）TCP アクセスリストおよびアクセス条件を定義します。<br>TCP の場合は **tcp** を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。<br>• **ack**：確認応答（ACK）ビットセット。<br>• **established**：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。<br>• **fin**：終了ビットセット。送信者からのデータはそれ以上ありません。<br>• **neq** {*port* \|**protocol**}：所定のポート番号上にないパケットだけを照合します。<br>• **psh**：プッシュ機能ビットセット<br>• **range** {*port* \|**protocol**}：ポート番号の範囲内のパケットだけを照合します。<br>• **rst**：リセットビットセット<br>• **syn**：同期ビットセット<br>• **urg**：緊急ポインタビットセット |
| ステップ 6 | {**deny** \| **permit**} **udp** {*source-ipv6-prefix/prefix-length* \| **any** \| **host** *source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* \| **any** \| **host** *destination-ipv6-address*} [operator [*port-number*]] [ **dscp** *value*] [**log**] [**log-input**] [**neq** {*port* \| *protocol*}] [**range** {*port* \| *protocol*}] [**routing**] [ **sequence** *value*] [ **time-range** *name*]] | （任意）UDP アクセスリストおよびアクセス条件を定義します。<br>ユーザデータグラムプロトコルの場合は、**udp** を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [*port*]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 7 | {**deny** \| **permit**} **icmp** {*source-ipv6-prefix/prefix-length* \| **any** \| **host** *source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* \| **any** \| **host** *destination-ipv6-address*} [operator [*port-number*]] [*icmp-type* [*icmp-code*] \| icmp-message] [ **dscp** *value*] [**log**] [**log-input**] [**routing**] [ **sequence** *value*] [ **time-range** *name*] | （任意）ICMP アクセス リストおよびアクセス条件を定義します。<br>インターネット制御メッセージプロトコルの場合は、**icmp** を入力します。ICMP パラメータはステップ 1 の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。<br>• *icmp-type*：ICMP メッセージタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。<br>• *icmp-code*：ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。<br>• *icmp-message*：ICMP パケットを ICMP メッセージタイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、? キーを使用するか、またはこのリリースのコマンドリファレンスを参照してください。 |
| ステップ 8 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show ipv6 access-list** | アクセスリストの設定を確認します。 |
| ステップ 10 | **show running-config**<br>例：<br>デバイス# `show running-config` | 入力を確認します。 |
| ステップ 11 | **copy running-config startup-config**<br>例： | （任意）コンフィギュレーションファイルに設定を保存します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **copy running-config startup-config** | |

# インターフェイスへの IPv6 ACL の付加

レイヤ 3 インターフェイスで発信または着信トラフィックに ACL を、あるいはレイヤ 2 インターフェイスで着信トラフィックに を適用できます。レイヤ 3 インターフェイスで着信トラフィックにだけ ACL を適用できます。

インターフェイスへのアクセスを制御するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id* | アクセスリストを適用するレイヤ2インターフェイス（ポート ACL 用）またはレイヤ3インターフェイス（ルータ ACL 用）を特定して、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **no switchport** | ルータ ACL を適用する場合は、これによってインターフェイスがレイヤ2モード（デフォルト）からレイヤ3モードに変化します。 |
| ステップ 5 | **ipv6 address** *ipv6-address* | レイヤ3インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **ipv6 traffic-filter** *access-list-name* {**in** \| **out**} | インターフェイスの着信トラフィックまたは発信トラフィックにアクセスリストを適用します。 |
| ステップ 7 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 9 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# VLAN マップの設定

VLAN マップを作成して、1 つまたは複数の VLAN に適用するには、次のステップを実行します。

### 始める前に

VLAN に適用する IPv6 ACL を作成します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例： | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **configure terminal** | |
| ステップ 3 | **vlan access-map** *name* [**number**]<br>例：<br>デバイス(config)# **vlan access-map map_1 20** | VLANマップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。<br>同じ名前のVLANマップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。<br>VLAN マップでは、特定の permit または deny キーワードを使用しません。VLANマップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致するという意味です。ACL 内の deny は、一致しないという意味です。<br>このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。 |
| ステップ 4 | **match** {**ip** \| **ipv6** \| **mac**} **address** {*name* \| *number*} [*name* \| *number*]<br>例：<br>デバイス(config-access-map)# **match ipv6 address ip_net** | パケットを 1 つまたは複数のアクセス リストに対して照合します。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC アクセス リストに対してだけ照合されます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | （注） パケット タイプ（IP または MAC）に対する match 句が VLAN マップに設定されている場合で、そのマップ アクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。match 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。 |
| **ステップ 5** | IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1 つ以上の ACL とそのパケットを照合するには、次のコマンドのいずれかを入力します。<br>• **action** { **forward**}<br>`デバイス(config-access-map)# action forward`<br>• **action** { **drop**}<br>`デバイス(config-access-map)# action drop` | マップ エントリに対するアクションを設定します。 |
| **ステップ 6** | **vlan filter** *mapname* **vlan-list** *list*<br>例：<br>`デバイス(config)# vlan filter map 1 vlan-list 20-22` | VLAN マップを 1 つまたは複数の VLAN に適用します。<br>list には単一の VLAN ID（22）、連続した範囲（10 ～ 22）、または VLAN ID のストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。 |

# VLAN への VLAN マップの適用

VLAN マップを 1 つまたは複数の VLAN に適用するには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | | |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **vlan filter** *mapname* **vlan-list** *list*<br>例：<br>デバイス(config)# **vlan filter map 1 vlan-list 20-22** | VLAN マップを 1 つまたは複数の VLAN に適用します。<br>list には単一の VLAN ID（22）、連続した範囲（10 ～ 22）、または VLAN ID のストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config**<br>例：<br>デバイス# **show running-config** | アクセス リストの設定を表示します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# IPv6 ACL のモニタリング

次の表に示された 1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

表 *21 : show ACL commands*

| コマンド | 目的 |
|---|---|
| **show access-lists** | スイッチに設定されたすべてのアクセス リストを表示します。 |
| **show ipv6 access-list** [*access-list-name*] | 設定済みのすべての IPv6 アクセス リストまたは名前で指定されたアクセス リストを表示します。 |
| **show vlan access-map** [*map-name*] | VLAN アクセス マップ設定を表示します。 |
| **show vlan filter** [**access-map** *access-map* \| **vlan** *vlan-id*] | VACL と VLAN 間のマッピングを表示します。 |

次に、show access-lists 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Switch # show access-lists
Extended IP access list hello
    10 permit ip any any
IPv6 access list ipv6
    permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet (15 matches) sequence 20
    permit udp any any sequence 30
IPv6 access list outbound
    deny udp any any sequence 10
    deny tcp any any eq telnet sequence 20
```

次に、show vlan access-map 特権 EXEC コマンドの出力例を示します。出力には、VLAN アクセス マップ情報が表示されます。

```
Switch# show vlan access-map
Vlan access-map "m1"  10
  Match clauses:
    ipv6 address: ip2
  Action: drop
```

第 13 章

# DHCP の設定


- DHCP に関する情報 （249 ページ）
- DHCP 機能の設定方法 （257 ページ）
- DHCP サーバ ポートベースのアドレス割り当ての設定 （265 ページ）


## DHCP に関する情報

### DHCP サーバ

DHCP サーバは、スイッチまたはルータ上の指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、それらのアドレスを管理します。DHCP サーバがそのデータベースから要求された設定パラメータを取得して DHCP クライアントに渡すことができない場合は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに要求を転送します。スイッチは、DHCP サーバとして機能できます。

### DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送するレイヤ 3 デバイスです。リレーエージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは、DHCP メッセージを受け取ると、新しい DHCP メッセージを生成して、出力インターフェイス上で送信します。

### DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと DHCP スヌーピング バインディング データベース（DHCP スヌーピング バインディング テーブルとも呼ばれる）の作成および管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。DHCP スヌーピングを使用することにより、エンドユーザに接続された信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。

（注） DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。

信頼できない DHCP メッセージとは、信頼できないインターフェイス経由で送信されたメッセージのことです。デフォルトでは、スイッチはすべてのインターフェイスを信頼できないものと見なします。そのため、スイッチはいくつかのインターフェイスを信頼して DHCP スヌーピングを使用するように設定する必要があります。サービス プロバイダー環境で DHCP スヌーピングを使用する場合は、カスタマーのスイッチなど、サービス プロバイダー ネットワーク内には存在しないデバイスから送信されたメッセージが信頼できないメッセージとなります。不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカルインターフェイスのインターフェイス情報が含まれています。このデータベースには、信頼できるインターフェイスに接続されたホストの情報はありません。

サービス プロバイダー ネットワークでは、信頼できるインターフェイスとして設定できるものの例として、同じネットワーク内のデバイスのポートに接続されたインターフェイスがあります。信頼できないインターフェイスには、ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスがあります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。アドレスが一致した場合（デフォルト）、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットをドロップします。

- DHCPOFFER パケット、DHCPACK パケット、DHCPNAK パケット、DHCPLEASEQUERY パケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスが一致しない。
- スイッチが DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バインディングデータベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。

- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。
- DHCP スヌーピングがイネーブルになっている場合に、最大スヌーピングキューサイズの 1000 を超える。

（注） これは、リリース Cisco IOS XE Denali 16.1.x 以降に適用されます。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP オプション 82 情報を挿入するエッジ スイッチに接続されているスイッチは、オプション 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットをドロップします。DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジスイッチに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジスイッチによって挿入されたオプション 82 情報を含むパケットを受け入れます。集約スイッチは、信頼できないスイッチインターフェイスを介して接続されたホストのバインディングを認識します。集約スイッチで、ダイナミック ARP インスペクションや IP ソース ガードなど、DHCP セキュリティ機能をイネーブルに設定することもできますが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない入力インターフェイスで受信します。集約スイッチ上のエッジスイッチとの接続ポートは、信頼できるインターフェイスとして設定する必要があります。

通常、ワイヤレス クライアントにパケットをブロードキャストするのは望ましくありません。したがって、DHCP スヌーピングは、宛先ブロードキャスト MAC アドレス（ffff.ffff.ffff）をサーバからワイヤレス クライアントに送信される DHCP パケットのユニキャスト MAC アドレスに置き換えます。ユニキャスト MAC アドレスは DHCP ペイロード内の CHADDR フィールドから取得されます。この処理は、DHCP OFFER、DHCP ACK および DHCP NACK メッセージなどのクライアント パケットにサーバ用に適用されます。**ip dhcp snooping wireless bootp-broadcast enable**を使用して、この動作を元に戻すことができます。ワイヤレス BOOTP ブロードキャストがイネーブルの場合、サーバからのブロードキャスト DHCP パケットは、宛先 MAC アドレスを変更せずにワイヤレス クライアントに転送されます。

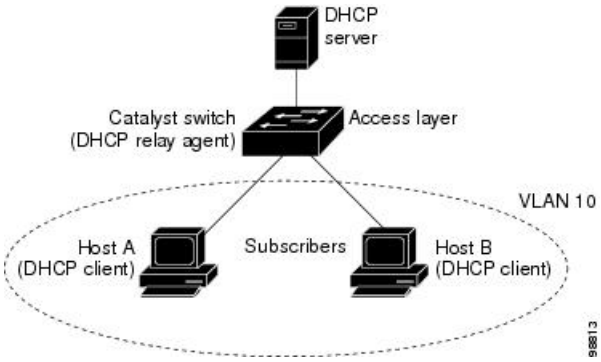
# オプション 82 データ挿入

住宅地域にあるメトロポリタン イーサネット アクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチ ポートによっても識別されます。サブスクライバ LAN 上の複数のホストをアクセス スイッチの同じポートに接続できます。これらのホストは一意に識別されます。

（注） DHCP オプション 82 機能は、DHCP スヌーピングがグローバルに有効であり、オプション 82 を使用する加入者装置が割り当てられた VLAN で有効である場合に限りサポートされます。

次の図に、一元的な DHCP サーバがアクセス レイヤのスイッチに接続された加入者に IP アドレスを割り当てるメトロポリタン イーサネット ネットワークを示します。DHCP クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレー エージェント（Catalyst スイッチ）にヘルパー アドレスを設定することにより、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

**図 *16 :* メトロポリタン イーサネット ネットワークにおける *DHCP* リレー エージェント**




スイッチで DHCP スヌーピング情報 オプション 82 を有効にすると、次のイベントがこの順序で発生します。

- ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。デフォルトでは、リモート ID サブオプションがスイッチの MAC アドレスで、回線 ID サブオプションはパケットを受信するポート ID（**vlan-mod-port**）です。リモート ID および回線 ID は設定できます。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するようなポリシーを実装したりできます。次に DHCP サーバは、DHCP 応答内にオプション 82 フィールドをエコーします。
- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィー

ルドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

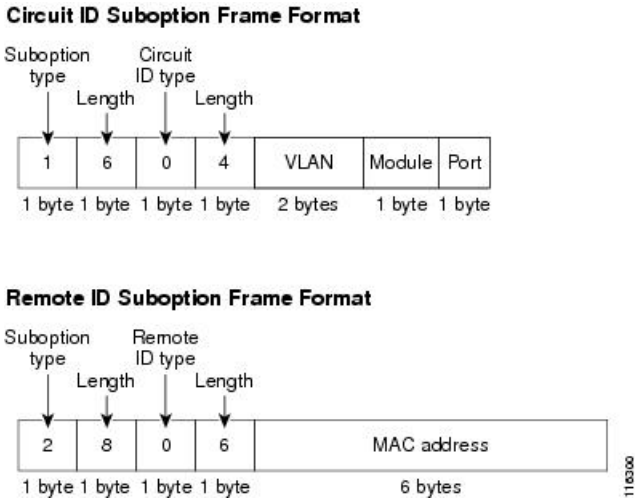
デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、次のフィールドの値は変化しません（図「サブオプションのパケット形式」を参照）。

- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号が 3 から始まります。たとえば、24 個の 10/100/1000 ポートおよび 4 つの Small Form-Factor Pluggable（SFP）モジュール スロットを搭載するスイッチでは、ポート 3 がギガビット イーサネット 1/0/1 ポート、ポート 4 がギガビット イーサネット 1/0/2 ポートとなり、以降同様に続きます。ポート 27 は SFP モジュール スロットのギガビット イーサネット 1/0/25 となり、以降同様に続きます。

図「サブオプションのパケット形式」に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。回線 ID サブオプションでは、モジュール番号は、スタックにあるスイッチ番号に対応します。スイッチがこれらのパケット形式を使用するのは、DHCP スヌーピングをグローバルに有効にし、ip dhcp snooping information option グローバル コンフィギュレーション コマンドを入力した場合です。

図 *17*: サブオプションのパケット形式

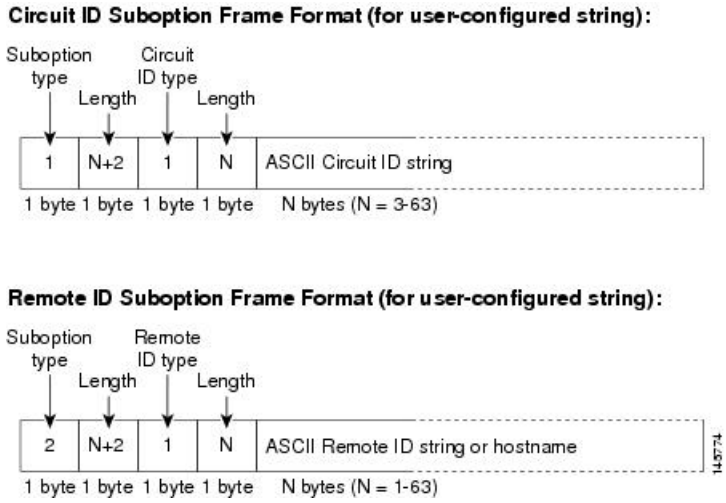



図「ユーザ設定のサブオプションのパケット形式」は、ユーザ設定のリモート ID サブオプション、および回線 ID サブオプションのパケット形式を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力した場合に、これらのパケット形式が使用されます。

パケットでは、リモート ID および回線 ID サブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

- 回線 ID サブオプション フィールド
  - 回線 ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
  - リモート ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。

図 *18 :* ユーザ設定のサブオプションのパケット形式




# Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。これには IP アドレス、アドレス バインディング、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てること、または、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てることが可能です。手動および自動アドレス バインディングの詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章を参照してください。

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

# DHCP スヌーピング バインディング データベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピング バインディング データベースに保存します。データベースには、64,000 のバインディングを含めることができます。

各データベース エントリ（バインディング）は、IP アドレス、それに関連付けられた MAC アドレス、リース期間（16 進形式）、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。データベース エージェントは、設定された場所のファイルにバインディングを保存します。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、まず 72 バイトのデータがあり、その後に 1 つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP インスペクションまたは IP ソース ガードがイネーブルにされ、DHCP スヌーピング バインディングデータベースがダイナミックバインディングされている場合、スイッチは接続を切断されます。このエージェントがディセーブルで、DHCPスヌーピングだけがイネーブルである場合、スイッチの接続は切断されませんが、DHCPスヌーピングはDHCPスプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディングデータベースを作成します。スイッチは、データベースに変更が加えられたときにはバインディング ファイルを更新します。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、ただちにデータベース内のエントリを更新します。スイッチはバインディング ファイル内のエントリも更新します。バインディング ファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイルが指定された時間内（書き込み遅延および中断タイムアウトの値によって設定される）に更新されない場合、更新は停止します。

バインディングが含まれるファイルの形式は次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の initial-checksum エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Gi1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 584a38f0
END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを DHCP スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スイッチがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している（スイッチはリース期間の終了時にバインディング エントリを削除しないことがある）。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- インターフェイスがルーテッド インターフェイスまたは DHCP スヌーピングにおける信頼できるインターフェイスである。

## DHCP スヌーピングおよびスイッチ スタック

DHCP スヌーピングは、スタック マスターで管理されます。新しいスイッチがスタックに加入すると、スイッチでは、スタック マスターから DHCP スヌーピング設定を受信します。メンバがスタックから除外されると、スイッチに関連付けられているすべての DHCP スヌーピング アドレス バインディングがエージング アウトします。

すべてのスヌーピング統計情報は、スタック マスター上で生成されます。新しいスタック マスターが選出された場合、統計カウンタはリセットされます。

スタックのマージが発生し、スタック マスターではなくなった場合、スタック マスターにあったすべての DHCP スヌーピング バインディングが失われます。スタック パーティションでは、既存のスタック マスターに変更はなく、パーティション化スイッチに属しているバインディングは、エージング アウトします。パーティション化スイッチの新しいマスターでは、新たな着信 DHCP パケットの処理が開始されます。

# DHCP 機能の設定方法

## DHCP スヌーピングのデフォルト設定

表 *22 : DHCP* のデフォルト設定

| 機能 | デフォルト設定 |
|---|---|
| DHCP サーバ | Cisco IOS ソフトウェアではイネーブル、設定が必要[6] |
| DHCP リレー エージェント | イネーブル[7] |
| DHCP パケット転送アドレス | 未設定 |
| リレー エージェント情報の確認 | イネーブル（無効なメッセージは廃棄） |
| DHCP リレー エージェント転送ポリシー | 既存のリレー エージェント情報を置換。 |

| 機能 | デフォルト設定 |
|---|---|
| DHCP スヌーピングをグローバルにイネーブル | ディセーブル |
| DHCP スヌーピング情報オプション | イネーブル |
| パケットを信頼できない入力インターフェイスで受け取る DHCP スヌーピング オプション[8] | ディセーブル |
| DHCP スヌーピング レート制限 | 未設定 |
| DHCP スヌーピング信頼状態 | 信頼できない |
| DHCP スヌーピング VLAN | ディセーブル |
| DHCP スヌーピングの MAC アドレス検証 | イネーブル |
| Cisco IOS DHCP サーバ バインディング データベース | Cisco IOS ソフトウェアではイネーブル、設定が必要。<br>（注） スイッチは、DHCP サーバとして設定されているデバイスからだけ、ネットワーク アドレスおよび設定パラメータを取得します。 |
| DHCP スヌーピング バインディング データベース エージェント | Cisco IOS ソフトウェアではイネーブル、設定が必要。この機能は宛先が設定されている場合に限り有効。 |

[6] スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。
[7] スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。
[8] この機能は、スイッチがエッジスイッチによってオプション 82 情報が挿入されたパケットを受信する集約スイッチである場合に使用します。

# DHCP スヌーピング設定時の注意事項

- スイッチポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust interface** コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。

- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報を表示したり、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報をクリアしたりできるようになりました。

# DHCP サーバの設定

スイッチは、DHCP サーバとして機能できます。管理ポートを備えた DHCP クライアント用に IOS ベースの DHCP サーバを使用する場合は、管理 VRF を使用して DHCP プールと対応するインターフェイスの両方を設定する必要があります。

スイッチを DHCP サーバとして設定するときの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の項の「Configuring DHCP」を参照してください。

# DHCP サーバとスイッチ スタック

DHCP バインディング データベースは、スタック マスターで管理されます。新しいスタック マスターが割り当てられると、新しいマスターでは、TFTP サーバから保存されているバインディングデータベースがダウンロードされます。スイッチオーバーが発生した場合、アクティブな新しいスタック マスターは SSO 機能を使用して以前のアクティブ スタック マスターから同期されたデータベース ファイルを使用します。失われたバインディングに関連付けられていた IP アドレスは、解放されます。自動バックアップは、**ip dhcp database** *url* [ **timeout** *seconds* | **write-delay** *seconds*] グローバル コンフィギュレーション コマンドを使用して設定する必要があります。

# DHCP リレー エージェントの設定

スイッチ上で DHCP リレー エージェントをイネーブルにするには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **service dhcp**<br>例：<br>デバイス(config)# **service dhcp** | スイッチ上でDHCPサーバおよびDHCPリレー エージェントをイネーブルにします。デフォルトでは、この機能はイネーブルです。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

次のタスク

- リレー エージェント情報のチェック（検証）
- リレー エージェント転送ポリシーの設定

# パケット転送アドレスの指定

DHCPサーバおよびDHCPクライアントが異なるネットワークまたはサブネットにある場合、スイッチを **ip helper-address** *address* インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的なルールは、クライアントに最も近いレイヤ3インターフェイス上にコマンドを設定することです。**ip helper-address** コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワークセグメントにある場合はネットワークアドレスにすることができます。ネットワーク アドレスを使用することで、どの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface vlan** *vlan-id*<br>例：<br>デバイス(config)# interface vlan 1 | VLAN ID を入力してスイッチ仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ip address** *ip-address subnet-mask*<br>例：<br>デバイス(config-if)# ip address 192.108.1.27 255.255.255.0 | インターフェイスに IP アドレスおよび IP サブネットを設定します。 |
| ステップ 5 | **ip helper-address** *address*<br>例：<br>デバイス(config-if)# ip helper-address 172.16.1.2 | DHCP パケット転送アドレスを指定します。<br>ヘルパー アドレスは特定の DHCP サーバ アドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。<br>複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。 |
| ステップ 6 | **end**<br>例：<br>デバイス(config-if)# end | グローバル コンフィギュレーション モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 7 | 次のいずれかを使用します。<br>• **interface range** *port-range*<br>• **interface** *interface-id*<br>例：<br>`デバイス(config)# interface gigabitethernet1/0/2` | DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス範囲コンフィギュレーションモードを開始します。<br>または<br>DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイスコンフィギュレーションモードを開始します。 |
| ステップ 8 | **switchport mode access**<br>例：<br>`デバイス(config-if)# switchport mode access` | ポートの VLAN メンバーシップモードを定義します。 |
| ステップ 9 | **switchport access vlan** *vlan-id*<br>例：<br>`デバイス(config-if)# switchport access vlan 1` | ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。 |
| ステップ 10 | **end**<br>例：<br>`デバイス(config-if)# end` | 特権 EXEC モードに戻ります。 |
| ステップ 11 | **show running-config**<br>例：<br>`デバイス# show running-config` | 入力を確認します。 |
| ステップ 12 | **copy running-config startup-config**<br>例：<br>`デバイス# copy running-config startup-config` | （任意）コンフィギュレーションファイルに設定を保存します。 |

# DHCP スヌーピングおよびオプション 82 を設定するための前提条件

DHCP スヌーピングおよびオプション 82 の前提条件は次のとおりです。

- DHCP スヌーピングは、スイッチ上でグローバルにイネーブルにする必要があります。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレー エージェントとして機能するデバイスが設定され、イネーブルになっていることを確認してください。
- スイッチを DHCP 要求に応答するようにする場合は、DHCP サーバとして設定する必要があります。
- スイッチで DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能するデバイスを設定してください。DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。サービス プロバイダー ネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。
- DHCP スヌーピングで Cisco IOS DHCP サーバ バインディング データベースを使用するには、Cisco IOS DHCP サーバ バインディング データベースを使用するようにスイッチを設定する必要があります。
- 信頼できない入力でパケットを受け入れる DHCP スヌーピング オプションを使用するには、スイッチがエッジ スイッチからオプション 82 情報を含むパケットを受信する集約スイッチである必要があります。
- 次の前提条件が DHCP スヌーピング バインディング データベースの設定に適用されます。
  - DHCP スヌーピング用にスイッチを使用するには、DHCP スヌーピング バインディング データベースで宛先を設定する必要があります。
  - NVRAM とフラッシュ メモリは、いずれも記憶容量が限られているため、バインディング ファイルを TFTP サーバに保存することを推奨します。
  - ネットワーク ベースの URL（TFTP や FTP など）については、スイッチがバインディングをその URL のバインディング ファイルに初めて書き込む前に、設定された URL に空のファイルを作成する必要があります。空のファイルをサーバ上に作成する必要があるかどうかについては、TFTP サーバのマニュアルを参照してください。TFTP サーバによっては、そのように設定できないことがあります。
  - データベースに正しいリース期間が記録されるように、ネットワーク タイム プロトコル（NTP）をイネーブルにし、設定することを推奨します。
  - NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディング ファイルに書き込みます。
- スイッチで DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスを設定してください。DHCP サーバが割り当てたり除外したりできる IP アドレス

を指定するか、デバイスの DHCP オプションを設定するか、または DHCP データベースエージェントをセットアップする必要があります。

- スイッチが DHCP パケットをリレーするようにする場合は、DHCP サーバの IP アドレスは DHCP クライアントのスイッチ仮想インターフェイス（SVI）に設定する必要があります。
- スイッチポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust interface** コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。

# Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『Cisco IOS IP Configuration Guide, Release 12.4』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

# DHCP スヌーピング情報のモニタリング

表 *23 : DHCP* 情報を表示するためのコマンド

| | |
|---|---|
| **show ip dhcp snooping** | スイッチの DHCP スヌーピングの設定を表示します。 |
| **show ip dhcp snooping binding** | DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングだけを表示します。このようなバインディングは、バインディング テーブルとも呼ばれます。 |
| **show ip dhcp snooping database** | DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。 |
| **show ip dhcp snooping statistics** | DHCP スヌーピングの統計情報を要約または詳細形式で表示します。 |
| **show ip source binding** | 動的および静的に設定されたバインディングを表示します。 |

（注） DHCP スヌーピングがイネーブルでインターフェイスがダウン ステートに変更された場合、静的に設定されたバインディングは削除されません。

# DHCP サーバ ポートベースのアドレス割り当ての設定

## DHCP サーバ ポートベースのアドレス割り当ての設定に関する情報

DHCP サーバ ポートベースのアドレス割り当ては、接続されたデバイス クライアントの ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポートで同じ IP アドレスを維持できるようにする機能です。

ネットワークに導入されたイーサネット スイッチは、直接接続されたデバイスに接続を提供します。工場の作業場など、一部の環境では、あるデバイスで不具合が発生した場合は、それと同時に、そのネットワークで代わりのデバイスが動作を開始しなければなりません。現在の DHCP 実装では、この代わりのデバイスに、DHCP が同じ IP アドレスを提供する保証はありません。コントロールやモニタリングなどを行うソフトウェアは、各デバイスに関連付けられた IP アドレスが一定であることを期待しています。デバイスを交換した場合、DHCP クライアントが変更された場合でも、アドレスの割り当ては一定のままでなければなりません。

DHCP サーバ ポートベースのアドレス割り当て機能が設定されている場合、この機能により、ある接続ポートで受信された DHCP メッセージでクライアント ID やクライアント ハードウェア アドレスが変更されたとしても、同じ接続ポートには常に同じ IP アドレスが提供されることが保証されます。DHCP プロトコルは、DHCP パケットのクライアント ID オプションにより、DHCP クライアントを識別します。クライアント ID オプションを含まないクライアントは、クライアント ハードウェア アドレスにより識別されます。この機能を設定すると、インターフェイスのポート名が、クライアント ID またはハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアント ID になります。

すべてのケースで、同じポートにイーサネット ケーブルを接続することにより、接続されたデバイスに、DHCP 経由で同じ IP アドレスが割り当てられます。

DHCP サーバ ポートベースのアドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけです。サードパーティ製のサーバではサポートされていません。

## ポートベースのアドレス テーブルのデフォルト設定

デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。

# ポートベースのアドレス割り当て設定時の注意事項

- デフォルトでは、DHCP サーバポートベースのアドレス割り当てはディセーブルにされています。
- DHCP プールから事前に設定された予約への割り当てを制限する（予約されていないアドレスはクライアントに提供されず、その他のクライアントはプールによるサービスを受けない）ために、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力することができます。

# DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチ上で DHCP スヌーピング バインディング データベース エージェントをイネーブルにし、設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip dhcp snooping database** {**flash**[*number*]**:**/*filename* \| **ftp:**//*user***:***password***@***host*/*filename* \| **http:**//[[*username***:***password*]**@**]{*hostname* \| *host-ip*}[/*directory*] /*image-name***.tar** \| **rcp:**//*user***@***host*/*filename*}\| **tftp:**//*host*/*filename*<br>例：<br>デバイス(config)# **ip dhcp snooping database tftp://10.90.90.90/snooping-rp2** | 次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイルの URL を指定します。<br>• **flash**[*number*]**:**/*filename*<br>（任意）スタック マスターのスタック メンバ番号を指定するには、*number* パラメータを使用します。*number* の指定できる範囲は 1 ～ 9 です。<br>• **ftp:**//*user***:***password***@***host*/*filename* |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • **http:**//[[*username*:*password*]@]{*hostname* \| *host-ip*}[/*directory*] /*image-name*.**tar**<br>• **rcp:**//*user*@*host*/*filename*<br>• **tftp:**//*host*/*filename* |
| ステップ 4 | **ip dhcp snooping database timeout** *seconds*<br>例：<br>デバイス(config)# **ip dhcp snooping database timeout 300** | データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間（秒数）を指定します。<br>デフォルトは 300 秒です。指定できる範囲は 0 ～ 86400 です。無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。 |
| ステップ 5 | **ip dhcp snooping database write-delay** *seconds*<br>例：<br>デバイス(config)# **ip dhcp snooping database write-delay 15** | バインディングデータベースが変更されてから転送を開始するまでの遅延時間を指定します。指定できる範囲は15 ～ 86400 秒です。デフォルトは 300 秒（5 分）です。 |
| ステップ 6 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*<br>例：<br>デバイス# **ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000** | （任意）DHCP スヌーピング バインディングデータベースにバインディングエントリを追加します。*vlan-id* に指定できる範囲は 1 ～ 4904 です。*seconds* の範囲は 1 ～ 4294967295 です。<br>このコマンドは、追加するエントリごとに入力します。<br>このコマンドは、スイッチをテストまたはデバッグするときに使用します。 |
| ステップ 8 | **show ip dhcp snooping database** [**detail**]<br>例：<br>デバイス# show ip dhcp snooping database detail | DHCP スヌーピング バインディングデータベースエージェントのステータスおよび統計情報を表示します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 9 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 10 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

# DHCP サーバ ポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルにイネーブル化し、インターフェイス上で加入者 ID を自動的に生成するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip dhcp use subscriber-id client-id**<br>例：<br>デバイス(config)# **ip dhcp use subscriber-id client-id** | すべての着信 DHCP メッセージで、加入者 ID がクライアント ID としてグローバルに使用されるように DHCP サーバを設定します。 |
| ステップ 4 | **ip dhcp subscriber-id interface-name**<br>例：<br>デバイス(config)# **ip dhcp subscriber-id interface-name** | インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。<br>特定のインターフェイスで設定された加入者 ID は、このコマンドで優先されます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet1/0/1** | 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 6 | **ip dhcp server use subscriber-id client-id**<br>例：<br>デバイス(config-if)# **ip dhcp server use subscriber-id client-id** | インターフェイス上ですべての着信 DHCP メッセージで、加入者 ID がクライアント ID として使用されるように DHCP サーバを設定します。 |
| ステップ 7 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 9 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

### 次のタスク

スイッチ上での DHCP ポートベースのアドレス割り当てをイネーブルにした後で、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用して、IP アドレスの事前割り当てと、クライアントへの関連付けを行います。

## DHCP サーバ ポートベースのアドレス割り当てのモニタリング

表 *24 : DHCP* ポートベースのアドレス割り当て情報を表示するためのコマンド

| コマンド | 目的 |
|---|---|
| **show interface** *interface id* | 特定のインターフェイスのステータスおよび設定を表示します。 |

| コマンド | 目的 |
| --- | --- |
| **show ip dhcp pool** | DHCP アドレス プールを表示します。 |
| **show ip dhcp binding** | Cisco IOS DHCP サーバのアドレス バインディングを表示します。 |

第 14 章

# Cisco Discovery Protocol バイパスの設定

Cisco Discovery Protocol バイパス モードでは、Cisco Discovery Protocol パケットを受け取り、そのまま送信します。受信パケットは処理されません。パケットは生成されません。このモードでは、Bump-In-The-Wire（BITW）動作が Cisco Discovery Protocol パケットに適用されます。これは Cisco Discovery Protocol のサポートがない場合に等しい下位互換モードです。


- Cisco Discovery Protocol バイパスの制約事項 （271 ページ）
- Cisco Discovery Protocol バイパスについて （271 ページ）
- Cisco Discovery Protocol バイパスの設定方法 （272 ページ）
- Cisco Discovery Protocol バイパスの設定例 （274 ページ）
- Cisco Discovery Protocol バイパスの機能情報 （275 ページ）


## Cisco Discovery Protocol バイパスの制約事項

Cisco Discovery Protocol バイパスは、スイッチ ポート上の標準 ACL をサポートしていません。

## Cisco Discovery Protocol バイパスについて

Cisco IP Phone が音声 VLAN とシングルホスト モードで設定されたポートに接続されている電話機は、Cisco Discovery Protocol バイパス機能によりネットワークに暗黙的に許可されます。Cisco Discovery Protocol メッセージで適切な TLV（Type Length Value）を送信する電話機（またはデバイス）が音声 VLAN へのアクセスを許可されます。

Cisco Discovery Protocol バイパス モードでは、Cisco Discovery Protocol パケットを受け取り、そのまま送信します。受信パケットは処理されません。パケットは生成されません。このモードでは、Bump-In-The-Wire（BITW）動作が Cisco Discovery Protocol パケットに適用されます。これは Cisco Discovery Protocol のサポートがない場合に等しい下位互換モードです。

Cisco Discovery Protocol バイパス モードでは、認証セッションが IP フォンのシングルホスト モードとマルチポスト モードで確立されます。ただし、インターフェイス ポートの音声 VLAN と 802.1 x が有効になっている場合は、ホスト モードがシングルホスト モードまたはマルチポスト モードに設定されているときに Cisco Discovery Protocol バイパスが有効になります。

Cisco Discovery Protocol バイパス機能の代わりに、より優れたアクセス制御、可視性、および許可を提供する Multi-Domain Authentication（MDA）機能を使用できます。

（注） デフォルトでは、ホスト モードはレガシー モードの場合はシングル モード、エッジ モードの場合はマルチ認証に設定されます。

2 番目のポートの切断の場合の Cisco Discovery Protocol の機能拡張：電話機の背後からプラグが抜かれホストが切断されたときに Cisco IP Phone は Cisco Discovery Protocol メッセージをスイッチに送信できます。ホストが直接接続され、リンク ダウン イベントを検出した場合と同様に、スイッチは間接的に接続されたホストの認証済みセッションをクリアできます。これは最新の IP 電話機でサポートされています。

Cisco Discovery Protocol バイパスは、サードパーティ製の電話機ではサポートされていません。Cisco Discovery Protocol バイパスが動作するのはシスコ製の電話機に限られます。

# Cisco Discovery Protocol バイパスの設定方法

Cisco Discovery Protocol バイパスを有効にするには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface GigabitEthernet1/0/12** | 物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。<br>• 指定できるインターフェイスは、物理ポートです。 |
| ステップ 4 | **switchport mode access**<br>例：<br>デバイス(config-if)# **switchport mode access** | インターフェイスがアクセス モードになるように指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **switchport access vlan** *vlan id*<br>例：<br>デバイス(config-if)# **switchport access vlan 10** | 同じ VLAN 内のすべてのポートをスタティック アクセス ポートとして割り当てます。<br>• ポートをスタティックアクセスポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。指定できる範囲は 1 ～ 4094 です。 |
| ステップ 6 | **switchport voice vlan** *vlan-id*<br>例：<br>デバイス(config-if)# **switchport voice vlan 3** | 指定された VLAN 経由ですべての音声トラフィックを転送するように、Cisco IP Phone に指示します。デフォルトでは、Cisco IP Phone は 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。<br>有効な VLAN ID の範囲は、拡張ソフトウェア イメージ（EI）がインストールされている場合は 1 ～ 4094 で、標準ソフトウェアイメージ（SI）がインストールされている場合は 1 ～ 1001 です。先行ゼロは入力しないでください。 |
| ステップ 7 | **authentication port-control auto**<br>例：<br>デバイス(config-if)# **authentication port-control auto** | ポートでの 802.1x 認証をイネーブルにします。 |
| ステップ 8 | **authentication host-mode** {**single-host** \| **multi-host**}<br>例：<br>デバイス(config-if)# **authentication host-mode single \| multi-host** | キーワードにより、次のものが許可されます。<br>• single-host：IEEE 802.1X 認可ポートの単一ホスト（クライアント）が許可されます。<br>• multi-host：単一ホストの認証後に 802.1X 認可ポートの複数ホストが許可されます。 |
| ステップ 9 | **dot1x pae authenticator**<br>例：<br>デバイス(config-if)# **dot1x pae authenticator** | ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 |

# Cisco Discovery Protocol バイパスの設定例

## 例：Cisco Discovery Protocol バイパスの有効化

「Authentication port-control auto」が dotx1 または MAB で設定されるか、または音声 VLAN がシングル/マルチポストモードとともにインターフェイスに設定されている場合、Cisco Discovery Protocol バイパスがデフォルトで有効になります。

次に、認証で MAB を使用している場合の Cisco Discovery Protocol バイパスの設定例を示します。

```
デバイス(config)# interface GigabitEthernet1/0/12
デバイス(config-if)# switchport mode access
デバイス(config-if)# switchport access vlan 10
デバイス(config-if)# switchport voice vlan 3
デバイス(config-if)# authentication port-control auto
デバイス(config-if)# mab
```

## Cisco Discovery Protocol ネイバーの無効化

次に、Cisco Discovery Protocol ネイバーを表示する設定例を示します。

```
デバイス# show cdp neighbors g1/0/37 detail
Device ID: SEP24B657B038DF
Entry address(es):
Platform: Cisco IP Phone 9971,  Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/37,  Port ID (outgoing port): Port 1
Holdtime : 157 sec
Second Port Status: Down <<<<<<<<<<
Version :
sip9971.9-1-1SR1
advertisement version: 2
Duplex: full
Power drawn: 12.804 Watts
Power request id: 57146, Power management id: 4
Power request levels are:12804 0 0 0 0
Total cdp entries displayed : 1
```

## 例：Cisco Discovery Protocol バイパスの無効化

Cisco Discovery Protocol バイパスを無効にするには、インターフェイスから「Authentication port-control auto」を削除する必要があります。

# Cisco Discovery Protocol バイパスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *25 : Cisco Discovery Protocol* バイパスの機能情報

| リリース | 機能情報 |
|---|---|
| | この機能が導入されました。 |

第 15 章

# IP ソース ガードの設定


- IP ソース ガードの概要 （277 ページ）
- IP ソース ガードの設定方法 （280 ページ）
- IP ソース ガードのモニタリング （283 ページ）
- その他の参考資料 （284 ページ）


# IP ソース ガードの概要

## IP ソース ガード

ネイバーの IP アドレスを使用する場合に、トラフィック攻撃を防ぐために IP ソース ガードを使用でき、そして信頼できないインターフェイスで DHCP スヌーピングがイネーブルの場合に、IP アドレスを使用しようとすると、IP ソース ガードをイネーブルにできます。

インターフェイス上で IPSG をイネーブルにすると、スイッチは、DHCP スヌーピングにより許可された DHCP パケットを除き、このインターフェイスで受信したすべての IP トラフィックをブロックします。

スイッチは IP アドレスをポートにバインドするためにハードウェアの発信元 IP 検索テーブルを使用します。IP および MAC のフィルタリングでは、送信元 IP 検索および送信元 MAC 検索の組み合わせが使用されます。バインディングテーブル内の送信元 IP アドレスを使用する IP トラフィックは許可され、他のすべてのトラフィックは拒否されます。

IP ソース バインディング テーブルには、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング（スタティック IP 送信元バインディング）があります。このテーブルのエントリには IP アドレスと、関連 MAC アドレス、および関連 VLAN 番号があります。スイッチは、IP ソース ガードがイネーブルにされている場合だけ、IP ソース バインディング テーブルを使用します。

IPSG は、アクセス ポートおよびトランク ポートを含むレイヤ 2 ポートだけでサポートされます。送信元 IP アドレスと送信元 IP および MAC アドレス フィルタリングで IPSG を設定できます。

# スタティック ホスト用 IP ソース ガード

（注） アップリンク ポート、またはトランク ポートで、スタティック ホスト用 IP ソース ガード（IPSG）を使用しないでください。

スタティック ホスト用 IPSG は、IPSG の機能を DHCP ではない、スタティックな環境に拡張するものです。これまでの IPSG は、DHCP スヌーピングにより作成されたエントリを使用して、スイッチに接続されたホストを検証していました。ホストから受信したトラフィックのうち、有効な DHCP を持たないものはすべてドロップされます。このセキュリティ機能によって、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックが制限されます。この機能は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソースバインディングに基づいてトラフィックをフィルタリングします。前バージョンの IPSG では、IPSG を動作させるために DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしで IPSG を動作させることができます。スタティック ホスト用 IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブルエントリに依存しています。このスイッチは、指定されたポートで有効なホストのリストを維持するために、ARP リクエスト、またはその他の IP パケットに基づいてスタティックエントリを作成します。また、指定されたポートにトラフィックを送信できるホストの数を指定することもできます。これはレイヤ 3 でのポート セキュリティと同じです。

スタティック ホスト用 IPSG はダイナミック ホストもサポートしています。ダイナミック ホストが、IP DHCP スヌーピング テーブルに存在する DHCP が割り当てられた IP アドレスを受信すると、IP デバイス トラッキング テーブルは同じエントリを学習します。スタック化環境では、マスターのフェールオーバーが発生すると、メンバ ポートに接続されたスタティック ホストの IP ソース ガード エントリは、そのまま残ります。 **show device-tracking database** 特権 EXEC コマンドを入力すると、IP デバイス トラッキング テーブルには、これらのエントリが ACTIVE であると表示されます。

（注） 複数のネットワーク インターフェイスを持つ IP ホストの一部は、ネットワーク インターフェイスに無効なパケットを注入することができます。この無効なパケットには、ソースアドレスとして、別のホスト ネットワーク インターフェイスの IP アドレス、または MAC アドレスが含まれます。この無効パケットは、スタティック ホスト用 IPSG がホストに接続され、無効な IP アドレス バインディングまたは MAC アドレス バインディングが学習されて、有効なバインディングが拒否される原因となります。ホストによる無効なパケットの注入を回避する方法については、対応するオペレーティング システムとネットワーク インターフェイスのベンダーにお問い合わせください。

最初、スタティック ホスト用 IPSG は ACL ベースのスヌーピング メカニズムを通じて、動的に IP バインディング、または MAC バインディングを学習します。IP バインディング、または MAC バインディングは、ARP パケット、および IP パケットにより、スタティック ホストから学習されます。これらはデバイス トラッキング データベースに保存されます。指定されたポートで動的に学習、または静的に設定された IP アドレスの数が最大値に達した場合、新

しい IP アドレスを持つパケットはすべて、ハードウェアによりドロップされます。何らかの理由で移動された、またはなくなったホストを解決するために、スタティック ホスト用 IPSG は IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングをエージング アウトします。この機能は、DHCP スヌーピングとともに使用できます。複数バインディングは、DHCP ホストとスタティック ホストの両方に接続されたポートに確立されます。たとえば、バインディングは、デバイス トラッキング データベースと DHCP スヌーピング バインディング データベースの両方に保存されます。

# IP ソース ガードの設定時の注意事項

- スタティック IP バインディングは、非ルーテッド ポートだけで設定できます。ルーテッドインターフェイスで **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを入力すると、次のエラーメッセージが表示されます。

```
Static IP source binding can only be configured on switch port.
```

- 送信元 IP フィルタリング機能を持つ IP ソース ガードがインターフェイスでイネーブルにされている場合、このインターフェイスのアクセス VLAN で、DHCP スヌーピングをイネーブルにしておく必要があります。
- 複数の VLAN を持つトランク インターフェイス上で IP ソース ガードをイネーブルにし、これらすべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。

（注） IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切にトラフィックをフィルタリングできない可能性があります。

- この機能は、802.1x ポートベースの認証がイネーブルにされている場合にイネーブルにできます。

# IP ソース ガードの設定方法

## IP ソース ガードのイネーブル化

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/0/1** | 設定するインターフェイスを指定して、インターフェイスコンフィギュレーション モードを開始します。 |
| ステップ 4 | **ip verify source**［**mac-check** ］<br>例：<br>デバイス(config-if)# **ip verify source** | 送信元 IP アドレス フィルタリングによる IP ソース ガードを有効にします。<br>（任意）**mac-check**：送信元 IP アドレスによる IP ソース ガードおよび MAC アドレス フィルタリングをイネーブルにします。 |
| ステップ 5 | **exit**<br>例：<br>デバイス(config-if)# **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*<br>例：<br>デバイス(config)# **ip source binding** | スタティック IP ソース バインディングを追加します。<br>スタティック バインディングごとにこのコマンドを入力します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1` | |
| ステップ 7 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 9 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定

スタティックホスト用 IPSG を動作させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルに有効にしていない、または IP device tracking maximum をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例： | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **configure terminal** | |
| ステップ 3 | **ip device tracking**<br>例：<br>デバイス(config)# **ip device tracking** | IP ホスト テーブルをオンにし、IP デバイス トラッキングをグローバルに有効にします。 |
| ステップ 4 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/0/1** | インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 5 | **switchport mode access**<br>例：<br>デバイス(config-if)# **switchport mode access** | アクセスとしてポートを設定します。 |
| ステップ 6 | **switchport access vlan** *vlan-id*<br>例：<br>デバイス(config-if)# **switchport access vlan 10** | このポートに VLAN を設定します。 |
| ステップ 7 | **ip verify source**[**tracking**] [**mac-check** ]<br>例：<br>デバイス(config-if)# **ip verify source tracking mac-check** | 送信元 IP アドレス フィルタリングによる IP ソース ガードを有効にします。<br>（任意）**tracking**：スタティック ホスト用 IP ソース ガードを有効にします。<br>（任意）**mac-check**：MAC アドレス フィルタリングを有効にします。<br>**ip verify source tracking mac-check** コマンドは、MAC アドレス フィルタリングのあるスタティック ホストに対して IP ソース ガードを有効にします。 |
| ステップ 8 | **ip device tracking maximum** *number*<br>例：<br>デバイス(config-if)# **ip device tracking** | そのポートで、IP デバイス トラッキング テーブルにより許可されるスタティック IP 数の上限を設定します。指定でき |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `maximum 8` | る範囲は 1 ～ 10 です。最大値は 10 です。<br>（注） **ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。 |
| ステップ 9 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

# IP ソース ガードのモニタリング

表 *26 :* 特権 *EXEC* 表示コマンド

| コマンド | 目的 |
|---|---|
| **show ip verify source** [ **interface** *interface-id* ] | スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。 |
| **show ip device tracking** { **all** \| **interface** *interface-id* \| **ip** *ip-address* \| **mac** *mac-address*} | IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。 |

表 *27 :* インターフェイス コンフィギュレーション コマンド

| コマンド | 目的 |
|---|---|
| **ip verify source tracking** | データ ソースを確認します。 |

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

# その他の参考資料

### エラー メッセージ デコーダ

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

### MIB

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

### シスコのテクニカル サポート

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

第 16 章

# ダイナミック ARP インスペクションの設定


- ダイナミック ARP インスペクションの制約事項 （285 ページ）
- ダイナミック ARP インスペクションの概要 （287 ページ）
- ダイナミック ARP インスペクションのデフォルト設定 （291 ページ）
- ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ （292 ページ）
- 非 DHCP 環境での ARP ACL の設定 （292 ページ）
- DHCP 環境でのダイナミック ARP インスペクションの設定 （295 ページ）
- 着信 ARP パケットのレート制限 （298 ページ）
- ダイナミック ARP インスペクション検証チェックの実行 （300 ページ）
- DAI のモニタリング （302 ページ）
- DAI の設定の確認 （303 ページ）
- その他の参考資料 （304 ページ）


## ダイナミック ARP インスペクションの制約事項

ここでは、スイッチにダイナミック ARP インスペクションを設定するときの制約事項および注意事項を示します。

- ダイナミック ARP インスペクションは入力セキュリティ機能です。出力チェックはまったく行いません。
- ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションをサポートしていないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されるホストに対しては有効ではありません。中間者攻撃は単一のレイヤ2ブロードキャストドメインに制限されているため、チェックされないドメインと、ダイナミック ARP インスペクションによりチェックされるドメインは区別します。このアクションは、ダイナミック ARP インスペクションのためにイネーブルにされているドメインでホストの ARP キャッシュを保護します。
- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インスペクション DHCP スヌーピング バインディング データベースの

エントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可または拒否を行います。

- ダイナミック ARP インスペクションは、アクセス ポート、トランク ポート、および EtherChannel ポートでサポートされます。

（注） RSPAN VLAN では、ダイナミック ARP インスペクションをイネーブルにしないでください。RSPAN VLAN でダイナミック ARP インスペクションをイネーブルにすると、ダイナミック ARP インスペクション パケットが RSPAN 宛先ポートに届かない可能性があります。

- 物理ポートを EtherChannel ポート チャネルに結合するには、この物理ポートとチャネル ポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポートチャネル内で中断状態のままとなります。ポート チャネルは、チャネルと結合された最初の物理ポートの信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態と一致する必要はありません。

  逆に、ポートチャネルで信頼状態を変更すると、スイッチは、チャネルを構成するすべての物理ポートで新しい信頼状態を設定します。

- レート制限は、スイッチ スタックの各スイッチで別々に算出されます。クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも高い可能性があることを意味します。たとえば、レート制限が 30 pps に設定された EtherChannel で、スイッチ 1 に 1 つのポート、およびスイッチ 2 に 1 つのポートがある場合、EtherChannel が errdisable にならずに、各ポートは 29 pps でパケットを受信できます。

- ポートチャネルの動作レートは、チャネル内のすべての物理ポートによる累積値です。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定すると、このチャネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャネル メンバーからの受信パケット レートの合計となります。EtherChannel ポートのレート制限は、各チャネル ポート メンバーが受信する ARP パケットのレートを確認してから設定してください。

  物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポートチャネルの設定に照合して検査されます。ポートチャネルのレート制限設定は、物理ポートの設定には依存しません。

  EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャネル（すべての物理ポートを含む）は errdisable ステートとなります。

- 着信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートの集約を反映し、複数のダイナミック ARP インスペクションがイネーブルにされた VLAN にわたってパケットを処理するために、トランク ポートのレートをより高く設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コ

マンドを使用して、レートを無制限に設定することもできます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。

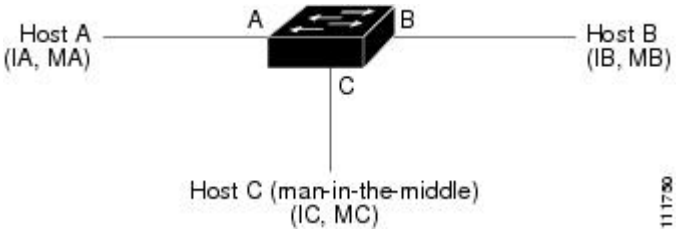
- スイッチで、ダイナミック ARP インスペクションをイネーブルにすると、ARP トラフィックをポリシングするように設定されたポリサーの有効性は失われます。この結果、すべての ARP トラフィックは CPU に送信されます。

# ダイナミック ARP インスペクションの概要

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B はホスト A に情報を送信する必要がありますが、ARP キャッシュにホスト A の MAC アドレスを持っていないとします。ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャスト ドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロードキャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。しかし、ARP は、ARP 要求が受信されなった場合でも、ホストからの余分な応答を許可するため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生することがあります。攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイヤ 2 ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。図 26-1 に、ARP キャッシュ ポイズニングの例を示します。

**図 *19 : ARP* キャッシュ ポイズニング**




ホスト A、B、および C は、インターフェイス A、B、および C 上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。カッコ内に示されているのは、これらの IP アドレス、および MAC アドレスです。たとえば、ホスト A が使用する IP アドレスは IA、MAC アドレスは MA です。ホスト A が IP レイヤにあるホスト B と通信する必要がある場合、ホスト A は IP アドレス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。スイッチとホスト B は、この ARP 要求を受信すると、IP アドレスが IA で、MAC アドレスが MA のホストに対する ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は、MAC アドレス MA にバインドされています。ホスト B が応答すると、スイッチ、およびホスト A は、IP アドレスが IB で、MAC アドレスが MB のホストに対するバインディングを ARP に読み込みます。

ホスト C は、IP アドレスが IA（または IB）で、MAC アドレスが MC のホストに対するバインディングを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングすることができます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は自身をホスト A からホスト B へのトラフィック ストリームに挿入します。従来の中間者攻撃です。

ダイナミック ARP インスペクションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。この機能により、ネットワークをある種の中間者攻撃から保護することができます。

ダイナミック ARP インスペクションにより、有効な ARP 要求と応答だけが確実にリレーされるようになります。スイッチが実行する機能は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

ダイナミック ARP インスペクションは、信頼できるデータベースである DHCP スヌーピング バインディング データベースに格納されている有効な IP/MAC アドレス バインディングに基づいて、ARP パケットの正当性を判断します。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングが有効になっている場合に、DHCP スヌーピングにより構築されます。信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、このパケットを転送します。信頼できないインターフェイスでは、スイッチはこのパケットが有効である場合だけ、このパケットを転送します。

**ip arp inspection vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用して、VLAN ごとにダイナミック ARP インスペクションを有効にすることができます。

非 DHCP 環境では、ダイナミック ARP インスペクションは、静的に設定された IP アドレスを持つホストに対するユーザ設定の ARP アクセス コントロール リスト（ACL）と照らし合わせて、ARP パケットの正当性を確認することができます。ARP ACL を定義するには、**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用します。

パケットの IP アドレスが無効である場合、または ARP パケットの本文にある MAC アドレスが、イーサネット ヘッダーで指定されたアドレスと一致しない場合、ARP パケットをドロップするようにダイナミック ARP インスペクションを設定することができます。このためには、**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} グローバル コンフィギュレーション コマンドを使用します。

# インターフェイスの信頼状態とネットワーク セキュリティ

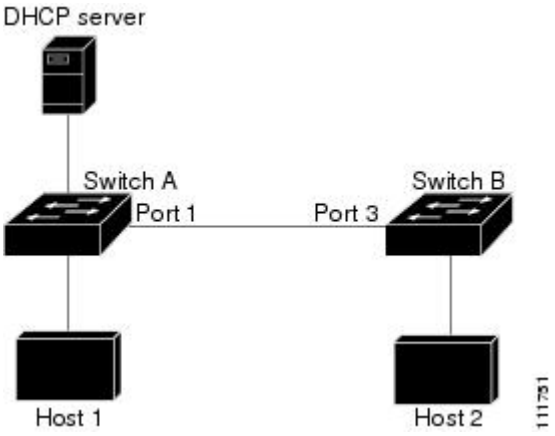
ダイナミック ARP インスペクションは、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイスに到着するパケットは、ダイナミック ARP インスペクションの確認検査をすべてバイパスし、信頼できないインターフェイスに到着するパケットには、ダイナミック ARP インスペクションの検証プロセスを受けます。

一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチポートすべてを信頼できるものに設定します。この構成では、指定されたスイッチからネットワークに入ってくるARPパケットはすべて、セキュリティ チェックをバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、ip arp inspection trust インターフェイス コンフィギュレーション コマンドを使用します。

**注意** 信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

次の図では、スイッチ A とスイッチ B の両方が、ホスト 1 とホスト 2 を含む VLAN でダイナミック ARP インスペクションを実行しているとします。ホスト 1 とホスト 2 が、スイッチ A に接続している DHCP サーバから IP アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。したがって、スイッチ A とスイッチ B 間のインターフェイスが信頼できない場合は、ホスト 1 からの ARP パケットはスイッチ B ではドロップされ、ホスト 1 およびホスト 2 の間の接続は切断されます。

**図 *20*：ダイナミック *ARP* インスペクションのために有効にされた *VLAN* 上の *ARP* パケット検証**




実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティ ホールが生じます。スイッチ A でダイナミック ARP インスペクションが実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの間のリンクが信頼できるものとして設定されている場合はホスト 2）。この状況は、スイッチ B がダイナミック ARP インスペクションを実行している場合でも発生します。

ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションを実行しているスイッチに接続された（信頼できないインターフェイス上の）ホストが、そのネットワークにあるその他のホストのARPキャッシュをポイズニングしていないことを保証します。しかし、ダイナミック ARP インスペクションにより、ネットワークの他の部分にあるホストが、ダイナミック ARPインスペクションを実行しているスイッチに接続されているホストのキャッシュをポイズニングできないようにすることはできません。

VLAN のスイッチの一部がダイナミック ARP インスペクションを実行し、残りのスイッチは実行していない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定します。ただし、非ダイナミック ARP インスペクションスイッチからパケットのバインディングを検証するには、ARP ACL を使用して、ダイナミック ARP インスペクションを実行するスイッチを設定します。このようなバインディングが判断できない場合は、レイヤ 3 で、ダイナミック ARP インスペクション スイッチを実行していないスイッチから、ダイナミック ARP インスペクションを実行しているスイッチを分離します。

（注） DHCP サーバとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

# ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。デフォルトでは、信頼できないインターフェイスのレートは 15 パケット/秒（pps）です。信頼できるインターフェイスはレート制限されません。この設定を変更するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。ユーザが介入するまで、ポートはこの状態を維持します。**errdisable recovery** グローバル コンフィギュレーション コマンドを使用すると、errdisable ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。

（注） EtherChannel のレート制限は、スタックにある各スイッチに個別に適用されます。たとえば、EtherChannel で 20 pps の制限が設定されている場合、EtherChannel にあるポートの各スイッチでは、最大 20 pps まで実行できます。スイッチが制限を超過した場合、EtherChannel 全体が errdisable ステートになります。

# ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのは、ACL が **ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

## 廃棄パケットのロギング

スイッチがパケットをドロップすると、ログ バッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。各ログエントリには、受信側の VLAN、ポート番号、送信元 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

**ip arp inspection log-buffer** グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定します。記録されるパケットの種類を指定するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。

# ダイナミック ARP インスペクションのデフォルト設定

| 機能 | デフォルト設定 |
|---|---|
| ダイナミック ARP インスペクション | すべての VLAN でディセーブル。 |
| インターフェイスの信頼状態 | すべてのインターフェイスは untrusted。 |
| 着信 ARP パケットのレート制限 | 1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチドネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。<br>信頼できるすべてのインターフェイスでは、レート制限は行われません。<br>バースト インターバルは 1 秒です。 |
| 非 DHCP 環境に対する ARP ACL | ARP ACL は定義されません。 |
| 有効性検査 | 検査は実行されません。 |

| 機能 | デフォルト設定 |
|---|---|
| ログ バッファ | ダイナミック ARP インスペクションがイネーブル化されると、拒否またはドロップされた ARP パケットはすべてが記録されます。<br>ログ内のエントリ数は 32 です。<br>システム メッセージ数は、毎秒 5 つに制限されます。<br>ロギング レート インターバルは 1 秒です。 |
| VLAN 単位のロギング | 拒否または廃棄されたすべての ARP パケットが記録されます。 |

# ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのは、ACL が ip arp inspection filter vlan グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

# 非 DHCP 環境での ARP ACL の設定

この手順は、図 2 に示すスイッチ B がダイナミック ARP インスペクション、または DHCP スヌーピングをサポートしていないときにダイナミック ARP インスペクションを設定する方法を示しています。

スイッチ A のポート 1 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、スイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが作り出されます。これを阻止するには、スイッチ A のポート 1 を信頼できないものとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない（スイッチ A で ACL 設定を適用することは不可能である）場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを使用してパケットをルートする必要があります。

スイッチ A で ARP ACL を設定するには、次の手順を実行します。この手順は、非 DHCP 環境では必須です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **arp access-list** *acl-name* | ARP ACL を定義し、ARP アクセス リストコンフィギュレーションモードを開始します。デフォルトでは、ARP アクセス リストは定義されません。<br>（注） ARPアクセスリストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。 |
| ステップ 4 | **permit ip host** *sender-ip* **mac host** *sender-mac* | 指定されたホスト（ホスト 2）からの ARP パケットを許可します。<br>• *sender-ip* には、ホスト 2 の IP アドレスを入力します。<br>• *sender-mac* には、ホスト 2 の MAC アドレスを入力します。 |
| ステップ 5 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**] | VLAN に ARP ACL を適用します。デフォルトでは、定義済みの ARP ACL は、どのような VLAN にも適用されません。<br>• *arp-acl-name* には、ステップ 2 で作成した ACL の名前を指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • *vlan-range* では、スイッチとホストが存在する VLAN を指定します。VLAN ID 番号により識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。<br>• （任意）**static** を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットは廃棄されます。DHCP バインディングは使用されません。<br>このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。<br>IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセスリストで許可された場合だけに許可されます。 |
| ステップ 7 | **interface** *interface-id* | スイッチ B に接続されたスイッチ A のインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。 |
| ステップ 8 | **no ip arp inspection trust** | スイッチ B に接続されたスイッチ A のインターフェイスを untrusted として設定します。<br>デフォルトでは、すべてのインターフェイスは信頼できません。<br>信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | アドレスとの有効なバインディングを持つことを確認してから、ローカルキャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバルコンフィギュレーションコマンドで指定されたロギング設定に従ってログバッファに記録します。 |
| ステップ 9 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 10 | 次の show コマンドを使用します。<br>• **show arp access-list** acl-name<br>• **show ip arp inspection vlan** *vlan-range*<br>• **show ip arp inspection interfaces** | 入力を確認します。 |
| ステップ 11 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 12 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

# DHCP 環境でのダイナミック ARP インスペクションの設定

### 始める前に

この手順では、2つのスイッチがダイナミック ARP インスペクションをサポートしているときに、この機能を設定する方法を示します。ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B にそれぞれ接続されています。スイッチは両方とも、ホストが配置されている VLAN 1 でダイナミック ARP インスペクションを実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。したがって、

スイッチ A はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。

（注） 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

ダイナミック ARP インスペクションを設定するには、次の手順を実行します。この処理は、両方のスイッチで行う必要があります。この手順は必須です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **show cdp neighbors**<br>例：<br>デバイス(config-if)#**show cdp neighbors** | スイッチ間の接続を確認します。 |
| ステップ 3 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ip arp inspection vlan** *vlan-range*<br>例：<br>デバイス(config)# **ip arp inspection vlan 1** | VLAN 単位で、ダイナミック ARP インスペクションをイネーブルにします。デフォルトでは、すべての VLAN 上でダイナミック ARP インスペクションはディセーブルになっています。<br>vlan-range には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。両方のスイッチに同じ VLAN ID を指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **Interface***interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet1/0/1** | 他のスイッチに接続されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 6 | **ip arp inspection trust**<br>例：<br>デバイス(config-if)#**ip arp inspection trust** | スイッチ間の接続を trusted に設定します。デフォルトでは、すべてのインターフェイスは信頼できません。<br>スイッチは、信頼できるインターフェイスにあるもう 1 つのスイッチから受信した ARP パケットは確認しません。この場合、パケットはそのまま転送されます。<br>信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。 |
| ステップ 7 | **end**<br>例：<br>デバイス(config-if)#**end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show ip arp inspection interfaces**<br>例： | インターフェイスでダイナミック ARP インスペクションの設定を検証します。 |
| ステップ 9 | **show ip arp inspection vlan** *vlan-range*<br>例：<br>デバイス(config-if)#**show ip arp inspection vlan 1** | VLAN でダイナミック ARP インスペクションの設定を検証します。 |
| ステップ 10 | **show ip dhcp snooping binding**<br>例： | DHCP バインディングを確認します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if)#**show ip dhcp snooping binding** | |
| ステップ 11 | **show ip arp inspection statistics vlan** *vlan-range*<br>例：<br>デバイス(config-if)#**show ip arp inspection statistics vlan 1** | VLAN でダイナミック ARP インスペクションの統計情報を確認します。 |
| ステップ 12 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 13 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |

# 着信 ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。errordisable 回復をイネーブルにして、指定されたタイムアウト時間の後にポートがこのステートから自動的に抜け出すようにするまで、ポートはこのステートのままです。

（注） インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、レート制限をその信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

着信 ARP パケットのレートを制限するには、次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id* | レート制限されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ip arp inspection limit {rate pps [burst interval seconds] \| none}** | インターフェイス上の着信 ARP 要求および ARP 応答のレートを制限します。デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。バースト インターバルは 1 秒です。<br>キーワードの意味は次のとおりです。<br>• **rate***pps* には、1 秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ～ 2048 pps です。<br>• （任意）**burst interval***seconds* は、レートの高い ARP パケットの有無についてインターフェイスがモニタリングされる間隔（秒）を指定します。指定できる範囲は 1 ～ 15 です。<br>• **rate none** には、処理可能な着信 ARP パケットのレートに上限を指定しません。 |
| ステップ 5 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | 次のコマンドを使用します。<br>• **errdisable detect cause arp-inspection**<br>• **errdisable recovery cause arp-inspection**<br>• **errdisable recovery interval** *interval* | （任意）ダイナミック ARP インスペクションの errdisable ステートからのエラー回復をイネーブルにし、ダイナミック ARP インスペクションの回復メカニズムで使用する変数を設定します。<br>デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。<br>**interval** *interval* には、error-disabled ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。 |
| ステップ 7 | **exit** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | 次の show コマンドを使用します。<br>• **show ip arp inspection interfaces**<br>• **show errdisable recovery** | 設定を確認します。 |
| ステップ 9 | **show running-config**<br>例：<br>デバイス# `show running-config` | 入力を確認します。 |
| ステップ 10 | **copy running-config startup-config**<br>例：<br>デバイス# `copy running-config startup-config` | （任意）コンフィギュレーションファイルに設定を保存します。 |

# ダイナミック ARP インスペクション検証チェックの実行

ダイナミック ARP インスペクションは、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。宛先 MAC アドレス、送信側および宛先の IP アドレス、および送信元 MAC アドレスで追加検証を実行するように、スイッチを設定できます。

着信 ARP パケットで特定のチェックを実行するには、次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip arp inspection validate {[src-mac] [dst-mac] [ip]}** | 着信 ARP パケットで特定の検査を実行します。デフォルトでは、検証は実行されません。<br>キーワードの意味は次のとおりです。<br>• **src-mac** では、イーサネットヘッダーの送信元MACアドレスと ARP 本文の送信元 MAC アドレスが比較されます。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。<br>• **dst-mac** では、イーサネットヘッダーの宛先 MAC アドレスと ARP 本文の宛先 MAC アドレスが比較されます。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。<br>• **ip** では、ARP 本文から、無効な IP アドレスや予期しない IP アドレスがないかを確認します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | スは ARP 応答内だけで検査されます。<br><br>少なくとも 1 つのキーワードを指定する必要があります。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが src および dst mac の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番めのコマンドによって src および dst mac の検証がディセーブルになります。 |
| ステップ 4 | **exit** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show ip arp inspection vlan** *vlan-range* | 設定を確認します。 |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# `show running-config` | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>デバイス# `copy running-config startup-config` | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# DAI のモニタリング

DAI をモニタするには、次のコマンドを使用します。

| コマンド | 説明 |
|---|---|
| **clear ip arp inspection statistics** | ダイナミック ARP インスペクション統計情報をクリアします。 |

| コマンド | 説明 |
|---|---|
| **show ip arp inspection statistics** [**vlan** *vlan-range*] | 指定のVLANにおいて、転送されたパケット、廃棄されたパケット、MAC検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。 |
| **clear ip arp inspection log** | ダイナミック ARP インスペクション ログ バッファをクリアします。 |
| **show ip arp inspection log** | ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。 |

**show ip arp inspection statistics** コマンドでは、スイッチは信頼されたダイナミック ARP インスペクション ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

# DAI の設定の確認

DAI の設定を表示して確認するには、次のコマンドを使用します。

| コマンド | 説明 |
|---|---|
| **show arp access-list** [*acl-name*] | ARP ACL についての詳細情報を表示します。 |
| **show ip arp inspection interfaces** [interface-id] | 指定されたインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。 |
| **show ip arp inspection vlan** *vlan-range* | 指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。 |

# その他の参考資料

### エラー メッセージ デコーダ

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

### MIB

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

### シスコのテクニカル サポート

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

第 17 章

# IPv6 ファースト ホップ セキュリティの設定


- IPv6 でのファースト ホップ セキュリティの前提条件 （305 ページ）
- IPv6 でのファースト ホップ セキュリティの制約事項 （305 ページ）
- IPv6 でのファースト ホップ セキュリティに関する情報 （306 ページ）
- IPv6 スヌーピング ポリシーの設定方法 （308 ページ）
- IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法 （310 ページ）
- IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 （312 ページ）
- IPv6 スヌーピング ポリシーを VLAN にグローバルにアタッチする方法 （313 ページ）
- **IPv6 バインディング テーブルの内容を設定する方法** （314 ページ）
- IPv6 ネイバー探索インスペクション ポリシーの設定方法 （315 ページ）
- IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法 （320 ページ）
- **IPv6 DHCP ガード ポリシーの設定方法** （326 ページ）
- IPv6 ソース ガードの設定方法 （331 ページ）
- IPv6 プレフィックス ガードの設定方法 （334 ページ）
- IPv6 ファースト ホップ セキュリティの設定例 （337 ページ）


## IPv6 でのファースト ホップ セキュリティの前提条件

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

## IPv6 でのファースト ホップ セキュリティの制約事項

- 次の制限は、FHS ポリシーを EtherChannel インターフェイスに適用する場合に該当します（ポート チャネル）。

- FHS ポリシーがアタッチされた物理ポートは EtherChannel グループに参加することができません。
- FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。

- デフォルトでは、スヌーピング ポリシーにはセキュリティ レベルのガードがあります。そのようなスヌーピングポリシーがアクセススイッチに設定されると、ルータまたはDHCPサーバ/リレーに対応するアップリンクポートが信頼できるポートとして設定されていても、外部 IPv6 ルータアドバタイズメント（RA）または Dynamic Host Configuration Protocol のサーバパケットはブロックされます。IPv6 RA または DHCPv6 サーバ メッセージを許可するには、次の手順を実行します。
  - IPv6 RA ガード ポリシー（RA の場合）または IPv6 DHCP ガード ポリシー（DHCP サーバ メッセージの場合）をアップリンク ポートに適用します。
  - 低いセキュリティ レベルでスヌーピング ポリシーを設定します（たとえば、glean や inspect など）。しかし、ファースト ホップ セキュリティ機能の利点が有効でないため、このようなスヌーピング ポリシーでは、低いセキュリティ レベルを設定することはお勧めしません。

# IPv6 でのファースト ホップ セキュリティに関する情報

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

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

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

（注） 有効な Cisco IOS XE Release 16.3.1、ND インスペクション機能、IPv6 スヌーピングポリシー、IPv6 FHS バインディング テーブル コンテンツは、スイッチ統合セキュリティ機能（SISF）ベースのデバイストラッキングによってサポートされます。詳細については、『Software Configuration Guide』の「*Configuring SISF based device tracking*」の項を参照してください。

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

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

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

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

- IPv6 宛先ガード：IPv6 宛先ガード機能は、IPv6 ネイバー探索で動作し、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決します。アドレス グリーニング機能に依存して、リンク上でアクティブなすべての宛先をバイ

ンディング テーブルに挿入してから、バインディング テーブルで宛先が見つからなかったときに実行される解決をブロックします。

（注） IPv6 宛先ガードは、設定された SVI のレイヤ2 VLANに適用することをお勧めします。

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

# IPv6 スヌーピング ポリシーの設定方法

IPv6 スヌーピングポリシー機能は、Cisco IOS XE Denali 16.3.1 以降では廃止されています。コマンドはCLIに表示され、設定できますが、代わりにスイッチ統合セキュリティ機能（SISF）ベースのデバイストラッキング機能を使用することを推奨します。

IPv6 スヌーピング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **ipv6 snooping policy** *policy-name*<br>例：<br>デバイス(config)# **ipv6 snooping policy example_policy** | スヌーピング ポリシーを作成し、IPv6 スヌーピング ポリシー コンフィギュレーション モードに移行します。 |
| ステップ 3 | {[**default** ] \| [**device-role** {**node** \| **switch**}] \| [ **limit address-count** *value*] \| [**no**] \| [**protocol** {**dhcp** \| **ndp**} ] \| [**security-level** {**glean** \| **guard** \| **inspect**} ] \| [**tracking** {**disable** [**stale-lifetime** [*seconds* \| **infinite**] \| **enable** [**reachable-lifetime** [*seconds* \| **infinite**] } ] \| [**trusted-port** ] }<br>例：<br>デバイス**(config-ipv6-snooping)#** **security-level inspect**<br>例：<br>デバイス**(config-ipv6-snooping)#** **trusted-port** | データ アドレス グリーニングをイネーブルにし、さまざまな条件に対してメッセージを検証し、メッセージのセキュリティ レベルを指定します。<br>• （任意）**default**：すべてをデフォルト オプションに設定します。<br>• （任意）**device-role**{**node**] \| **switch**}：ポートに接続されたデバイスの役割を指定します。デフォルトは **node** です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • （任意）**limit address-count** *value*：ターゲットごとに許可されるアドレス数を制限します。<br>• （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。<br>• （任意）**protocol**{**dhcp**\|**ndp**}：分析のために、スヌーピング機能にどのプロトコルをリダイレクトするかを指定します。デフォルトは、**dhcp** および **ndp** です。デフォルトを変更するには、**no protocol** コマンドを使用します。<br>• （任意）**security-level**{**glean**\|**guard**\|**inspect**}：この機能によって適用されるセキュリティのレベルを指定します。デフォルトは **guard** です。<br>**glean**：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。<br>**guard**：アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバ メッセージを拒否します。これがデフォルトのオプションです。<br>**inspect**：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。<br>• （任意）**tracking** {**disable**\|**enable**}：デフォルトのトラッキング動作を上書きし、トラッキング オプションを指定します。<br>• （任意）**trusted-port**：信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | インディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config-ipv6-snooping)# **exit** | コンフィギュレーション モードから特権 EXEC モードに戻ります。 |
| ステップ 5 | **show ipv6 snooping policy** *policy-name*<br>例：<br>デバイス#**show ipv6 snooping policy example_policy** | スヌーピング ポリシー設定を表示します。 |

### 次のタスク

IPv6 スヌーピング ポリシーをインターフェイスまたは VLAN にアタッチします。

# IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはVLANにIPv6スヌーピング ポリシーをアタッチするには、特権EXECモードで次の手順を実行してください。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** Interface_type *stack/module/port*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/1/4** | インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **switchport**<br>例： | switchport モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if)# **switchport** | （注） インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに switchport インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。switchport コンフィギュレーション モードではコマンドプロンプトは（config-if）# と表示されます。 |
| ステップ 4 | **ipv6 snooping** [ **attach-policy** *policy_name* [ **vlan** {*vlan_id* \| **add** *vlan_ids* \| **except***vlan_ids* \| **none** \| **remove** *vlan_ids*}] \| **vlan** {*vlan_id* \| **add** *vlan_ids* \| **except***vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ]<br>例：<br>デバイス(config-if)# **ipv6 snooping**<br>or<br>デバイス(config-if)# **ipv6 snooping attach-policy example_policy**<br>or<br>デバイス(config-if)# **ipv6 snooping vlan 111,112**<br>or | インターフェイスまたはそのインターフェイス上の特定の VLAN にカスタム IPv6 スヌーピング ポリシーをアタッチします。デフォルトポリシーをインターフェイスにアタッチするには、**attach-policy** キーワードを指定せずに **ipv6 snooping** コマンドを使用します。デフォルト ポリシーをインターフェイス上の VLAN にアタッチするには、**ipv6 snooping vlan** コマンドを使用します。デフォルト ポリシーは、セキュリティ レベル **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if)# **ipv6 snooping attach-policy example_policy vlan 111,112** | |
| ステップ 5 | **do show running-config**<br>例：<br>デバイス#(config-if)# **do show running-config** | インターフェイスコンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。 |

# IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface range** *Interface_name*<br>例：<br>デバイス(config)# **interface range Po11** | EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。<br>ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。 |
| ステップ 3 | **ipv6 snooping** [ **attach-policy** *policy_name* [ **vlan** {*vlan_ids* \| **add** *vlan_ids* \| **except** *vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ] \| **vlan** [ {*vlan_ids* \| **add** *vlan_ids* \| **except***vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ]<br>例： | IPv6 スヌーピング ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if-range)# **ipv6 snooping attach-policy example_policy**<br><br>or<br><br>デバイス(config-if-range)# **ipv6 snooping attach-policy example_policy vlan 222,223,224**<br><br>**or**<br><br>デバイス(config-if-range)#**ipv6 snooping vlan 222, 223,224** | |
| ステップ 4 | **do show running-config interface***portchannel_interface_name*<br><br>例：<br><br>デバイス#(config-if-range)# **do show running-config int po11** | コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。 |

# IPv6スヌーピングポリシーをVLANにグローバルにアタッチする方法

複数のインターフェイス上の VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br><br>例：<br><br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **vlan configuration** *vlan_list*<br><br>例：<br><br>デバイス(config)# **vlan configuration 333** | VLANインターフェイスのコンフィギュレーションモードを開始し、IPv6スヌーピング ポリシーをアタッチする VLAN を指定します。 |
| ステップ 3 | **ipv6 snooping** [ **attach-policy** *policy_name*]<br><br>例：<br><br>デバイス(config-vlan-config)#**ipv6 snooping attach-policy example_policy** | すべてのスイッチおよびスタック インターフェイスで、IPv6 スヌーピング ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルトポリシーがアタッ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | チされます。デフォルト ポリシーは、セキュリティ レベル **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。 |
| ステップ 4 | **do show running-config**<br>例：<br>デバイス#(config-if)# **do show running-config** | インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。 |

# IPv6 バインディング テーブルの内容を設定する方法

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | [**no**] **ipv6 neighbor binding** [ **vlan** *vlan-id* {*ipv6-address* **interface** interface_type *stack/module/port hw_address* [**reachable-lifetimevalue** [*seconds* \| **default** \| **infinite**] \| [**tracking**{ [default \| disable] [ **reachable-lifetimevalue** [*seconds* \| **default** \| **infinite**] \| [**enable** [**reachable-lifetimevalue** [*seconds* \| **default** \| **infinite**] \| [**retry-interval** {*seconds*\| **default** [**reachable-lifetimevalue** [*seconds* \| **default** \| **infinite**] } ]<br>例：<br>デバイス(config)# **ipv6 neighbor binding** | バインディング テーブル データベースにスタティック エントリを追加します。<br>（注） スイッチは、バインディング エントリのタイマーの有効期限切れ時のシステムの安定性を向上させるために、設定された到達可能時間値に小さいバリアンスを追加します。 |
| ステップ 3 | [**no**] **ipv6 neighbor binding max-entries** *number* [ **mac-limit** *number* \| **port-limit** *number* [ **mac-limit** *number*] \| **vlan-limit** *number* [ [ **mac-limit** *number*] \| [ **port-limit** *number* [**mac-limit***number*] ] ] ]<br>例： | バインディング テーブル キャッシュに挿入できるエントリの最大数を指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config)# **ipv6 neighbor binding max-entries 30000** | |
| ステップ 4 | **ipv6 neighbor binding logging**<br>例：<br>デバイス(config)# **ipv6 neighbor binding logging** | バインディング テーブル メイン イベントのロギングをイネーブルにします。 |
| ステップ 5 | **exit**<br>例：<br>デバイス(config)# **exit** | グローバル コンフィギュレーション モードを終了して、ルータを特権EXEC モードにします。 |
| ステップ 6 | **show ipv6 neighbor binding**<br>例：<br>デバイス# **show ipv6 neighbor binding** | バインディング テーブルの内容を表示します。 |

# IPv6 ネイバー探索インスペクション ポリシーの設定方法

特権 EXEC モードから、IPv6 ND インスペクション ポリシーを設定するには、次の手順に従ってください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | [**no**]**ipv6 nd inspection policy** *policy-name*<br>例：<br>デバイス(config)# **ipv6 nd inspection policy example_policy** | ND インスペクション ポリシー名を指定し、ND インスペクション ポリシー コンフィギュレーション モードを開始します。 |
| ステップ 3 | **device-role** {**host** \| **switch**}<br>例：<br>デバイス(config-nd-inspection)# **device-role switch** | ポートに接続されているデバイスの役割を指定します。デフォルトは **host** です。 |
| ステップ 4 | **limit address-count** *value*<br>例： | 1 ～ 10,000 を入力します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-nd-inspection)# **limit address-count 1000** | |
| ステップ 5 | **tracking** {**enable** [**reachable-lifetime** {*value* \| **infinite**}] \| **disable** [**stale-lifetime** {*value* \| **infinite**}]}<br>例：<br>デバイス(config-nd-inspection)# **tracking disable stale-lifetime infinite** | ポートでデフォルトのトラッキングポリシーを上書きします。 |
| ステップ 6 | **trusted-port**<br>例：<br>デバイス(config-nd-inspection)# **trusted-port** | 信頼できるポートにするポートを設定します。 |
| ステップ 7 | **validate source-mac**<br>例：<br>デバイス(config-nd-inspection)# **validate source-mac** | 送信元 Media Access Control（MAC）アドレスをリンク層アドレスと照合します。 |
| ステップ 8 | **no** {**device-role** \| **limit address-count** \| **tracking** \| **trusted-port** \| **validate source-mac**}<br>例：<br>デバイス(config-nd-inspection)# **no validate source-mac** | このコマンドの **no** 形式を使用してパラメータの現在の設定を削除します。 |
| ステップ 9 | **default** {**device-role** \| **limit address-count** \| **tracking** \| **trusted-port** \| **validate source-mac**}<br>例：<br>デバイス(config-nd-inspection)# **default limit address-count** | 設定をデフォルト値に戻します。 |
| ステップ 10 | **do show ipv6 nd inspection policy** *policy_name*<br>例：<br>デバイス(config-nd-inspection)# **do show ipv6 nd inspection policy example_policy** | ND インスペクション コンフィギュレーション モードを終了しないで ND インスペクションの設定を確認します。 |

# IPv6ネイバー探索インスペクションポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェース上の VLAN に IPv6 ND 検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** Interface_type *stack/module/port*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/1/4** | インターフェイスのタイプおよび ID を指定し、インターフェイスコンフィギュレーション モードを開始します。 |
| ステップ 3 | **ipv6 nd inspection** [ **attach-policy** *policy_name* [ **vlan** {*vlan_ids* \| **add** *vlan_ids* \| **except** *vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ] \| **vlan** [ {*vlan_ids* \| **add** *vlan_ids* \| **except***vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ]<br>例：<br>デバイス(config-if)# **ipv6 nd inspection attach-policy example_policy**<br>or<br>デバイス(config-if)# **ipv6 nd inspection attach-policy example_policy vlan 222,223,224**<br>**or**<br>デバイス(config-if)# **ipv6 nd inspection vlan 222, 223,224** | ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |
| ステップ 4 | **do show running-config**<br>例：<br>デバイス#(config-if)# **do show running-config** | インターフェイスコンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。 |

# IPv6 ネイバー探索インスペクション ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ネイバー探索検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface range** *Interface_name*<br>例：<br>デバイス(config)# **interface Po11** | EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。<br>ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。 |
| ステップ 3 | **ipv6 nd inspection** [ **attach-policy** *policy_name* [ **vlan** {*vlan_ids* \| **add** *vlan_ids* \| **except** *vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ] \| **vlan** [ {*vlan_ids* \| **add** *vlan_ids* \| **except***vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ]<br>例：<br>デバイス(config-if-range)# **ipv6 nd inspection attach-policy example_policy**<br>or<br>デバイス(config-if-range)# **ipv6 nd inspection attach-policy example_policy vlan 222,223,224**<br>**or**<br>デバイス(config-if-range)#**ipv6 nd inspection vlan 222, 223,224** | ND インスペクション ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **do show running-config interface***portchannel_interface_name*<br>例：<br>デバイス#(config-if-range)# **do show running-config int po11** | コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。 |

# IPv6ネイバー探索インスペクションポリシーを全体的にVLANにアタッチする方法

複数のインターフェイス上の VLAN に IPv6 ND 探索ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **vlan configuration** *vlan_list*<br>例：<br>デバイス(config)# **vlan configuration 334** | VLANインターフェイスのコンフィギュレーション モードを開始し、IPv6スヌーピング ポリシーをアタッチする VLAN を指定します。 |
| ステップ 3 | **ipv6 nd inspection** [ **attach-policy** *policy_name*]<br>例：<br>デバイス(config-vlan-config)#**ipv6 nd inspection attach-policy example_policy** | すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルトポリシーがアタッチされます。<br>デフォルトのポリシーは、device-role **host**、no drop-unsecure、limit address-count disabled、sec-level minimum is disabled、tracking is disabled、no trusted-port、no validate source-mac です。 |
| ステップ 4 | **do show running-config**<br>例：<br>デバイス#(config-if)# **do show running-config** | コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。 |

# IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法

IPv6 ルータ アドバタイズメント ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | [**no**]**ipv6 nd raguard policy** *policy-name*<br>例：<br>デバイス(config)# **ipv6 nd raguard policy example_policy** | RA ガード ポリシー名を指定し、RA ガードポリシーコンフィギュレーション モードを開始します。 |
| ステップ 3 | [**no**]**device-role** {**host** \| **monitor** \| **router** \| **switch**}<br>例：<br>デバイス(config-nd-raguard)# **device-role switch** | ポートに接続されているデバイスの役割を指定します。デフォルトは **host** です。<br>（注） ホスト側ポートとルータ側ポートの両方を備えたネットワークでは、ホスト側ポートまたは VLAN で **device-role host** を設定した RA ガードポリシーとともに、RA ガード機能が適切に動作できるように、ルータ側のポートで **device-role router** を設定した RA ガードポリシーを設定することが必須です。 |
| ステップ 4 | [**no**]**hop-limit** {**maximum** \| **minimum**} *value*<br>例：<br>デバイス(config-nd-raguard)# **hop-limit maximum 33** | （1 ～ 255）最大および最小のホップ制限値の範囲。<br>ホップ制限値によるルータアドバタイズメントメッセージのフィルタリングをイネーブルにします。不正 RA メッセージは低いホップ制限値（IPv4 の Time to Live と同じ）を持つ可能性があるため、ホストによって受け入れられ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | ると、ホストが不正 RA メッセージジェネレータを超えて宛先にトラフィックを生成することができなくなります。指定されていないホップ制限値を持つ RA メッセージはブロックされます。<br>設定されていない場合、このフィルタはディセーブルになります。<br>「**minimum**」を設定して、指定する値より低いホップ制限値を持つ RA メッセージをブロックします。<br>「**maximum**」を設定して、指定する値より高いホップ制限値を持つ RA メッセージをブロックします。 |
| ステップ 5 | [**no**]**managed-config-flag** {**off** \| **on**}<br>例：<br>デバイス(config-nd-raguard)# **managed-config-flag on** | 管理アドレス設定（「M」フラグ）フィールドに基づいてルータ アドバタイズメント メッセージのフィルタリングをイネーブルにします。「M」フィールドが 1 の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバを使用する場合があります。設定されていない場合、このフィルタはディセーブルになります。<br>**On**：「M」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。<br>**Off**：「M」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。 |
| ステップ 6 | [**no**]**match** {**ipv6 access-list** *list* \| **ra prefix-list** *list*}<br>例：<br>デバイス(config-nd-raguard)# **match ipv6 access-list example_list** | 指定したプレフィックス リストまたはアクセス リストと照合します。 |
| ステップ 7 | [**no**]**other-config-flag** {**on** \| **off**}<br>例：<br>デバイス(config-nd-raguard)# **other-config-flag on** | その他の設定（「O」フラグ）フィールドに基づくルータ アドバタイズメント メッセージのフィルタリングをイネーブルにします。「O」フィールドが 1 の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバを使用 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | する場合があります。設定されていない場合、このフィルタはディセーブルになります。<br>**On**：「O」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。<br>**Off**：「O」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。 |
| ステップ 8 | **[no]router-preference maximum {high \| medium \| low}**<br>例：<br>デバイス(config-nd-raguard)# **router-preference maximum high** | 「Router Preference」フラグを使用したルータアドバタイズメントメッセージのフィルタリングをイネーブルにします。設定されていない場合、このフィルタはディセーブルになります。<br>• **high**：「Router Preference」が「high」、「medium」、または「low」に設定された RA メッセージを受け入れます。<br>• **medium**：「Router Preference」が「high」に設定された RA メッセージをブロックします。<br>• **low**：「Router Preference」が「medium」または「high」に設定された RA メッセージをブロックします。 |
| ステップ 9 | **[no]trusted-port**<br>例：<br>デバイス(config-nd-raguard)# **trusted-port** | 信頼できるポートとして設定すると、すべての接続デバイスが信頼され、より詳細なメッセージ検証は実行されません。 |
| ステップ 10 | **default {device-role \| hop-limit {maximum \| minimum} \| managed-config-flag \| match {ipv6 access-list \| ra prefix-list } \| other-config-flag \| router-preference maximum\| trusted-port}**<br>例：<br>デバイス(config-nd-raguard)# **default hop-limit** | コマンドをデフォルト値に戻します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 11 | **do show ipv6 nd raguard policy** *policy_name*<br>例：<br>デバイス(config-nd-raguard)# **do show ipv6 nd raguard policy example_policy** | （任意）：RA ガード ポリシー コンフィギュレーションモードを終了しないで ND ガード ポリシー設定を表示します。 |

# IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェース上の VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** Interface_type *stack/module/port*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/1/4** | インターフェイスのタイプおよび ID を指定し、インターフェイスコンフィギュレーション モードを開始します。 |
| ステップ 3 | **ipv6 nd raguard** [ **attach-policy** *policy_name* [ **vlan** {*vlan_ids* \| **add** *vlan_ids* \| **except** *vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ] \| **vlan** [ {*vlan_ids* \| **add** *vlan_ids* \| **except***vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ]<br>例：<br>デバイス(config-if)# **ipv6 nd raguard attach-policy example_policy**<br>or<br>デバイス(config-if)# **ipv6 nd raguard attach-policy example_policy vlan 222,223,224**<br>**or**<br>デバイス(config-if)# **ipv6 nd raguard vlan 222, 223,224** | ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | |
| ステップ 4 | **do show running-config**<br>例：<br>デバイス#(config-if)# **do show running-config** | コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。 |

# IPv6ルータアドバタイズメントガードポリシーをレイヤ2EtherChannelインターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ルータ アドバタイズメント ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface range** *Interface_name*<br>例：<br>デバイス(config)# **interface Po11** | EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。<br>ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。 |
| ステップ 3 | **ipv6 nd raguard** [ **attach-policy** *policy_name* [ **vlan** {*vlan_ids* \| **add** *vlan_ids* \| **except** *vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ] \| **vlan** [ {*vlan_ids* \| **add** *vlan_ids* \| **except***vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ]<br>例：<br>デバイス(config-if-range)# **ipv6 nd raguard attach-policy example_policy**<br>or | RA ガードポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if-range)# **ipv6 nd raguard attach-policy example_policy vlan 222,223,224**<br><br>**or**<br><br>デバイス(config-if-range)#**ipv6 nd raguard vlan 222, 223,224** | |
| ステップ 4 | **do show running-config interface***portchannel_interface_name*<br><br>例：<br><br>デバイス#(config-if-range)# **do show running-config int po11** | コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。 |

# IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法

インターフェイスに関係なく VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br><br>例：<br><br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **vlan configuration** *vlan_list*<br><br>例：<br><br>デバイス(config)# **vlan configuration 335** | VLANインターフェイスのコンフィギュレーション モードを開始し、IPv6 RA ガード ポリシーをアタッチする VLAN を指定します。 |
| ステップ 3 | **ipv6 dhcp guard** [ **attach-policy** *policy_name*]<br><br>例：<br><br>デバイス(config-vlan-config)#**ipv6 nd raguard attach-policy example_policy** | すべてのスイッチおよびスタック インターフェイスで、IPv6 RA ガード ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **do show running-config**<br>例：<br>デバイス#(config-if)# **do show running-config** | コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。 |

# IPv6 DHCP ガードポリシーの設定方法

IPv6 DHCP（DHCPv6）ガードポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | [**no**]**ipv6 dhcp guard policy** *policy-name*<br>例：<br>デバイス(config)# **ipv6 dhcp guard policy example_policy** | DHCPv6 ガードポリシー名を指定し、DHCPv6 ガードポリシー コンフィギュレーション モードを開始します。 |
| ステップ 3 | [**no**]**device-role** {**client** \| **server**}<br>例：<br>デバイス(config-dhcp-guard)# **device-role server** | （任意）特定の役割のデバイスからのものではないポート上の DHCPv6 応答および DHCPv6 アドバタイズメントをフィルタします。デフォルトは **client** です。<br>• **client**：デフォルト値。アタッチされたデバイスがクライアントであることを指定します。サーバメッセージにはこのポートでドロップされます。<br>• **server**：適用されたデバイスが DHCPv6 サーバであることを指定します。このポートでは、サーバメッセージが許可されます。 |
| ステップ 4 | [**no**] **match server access-list** *ipv6-access-list-name*<br>例： | （任意）。アドバタイズされた DHCPv6 サーバまたはリレー アドレスが認証されたサーバのアクセス リストからのものであることの確認をイネーブルにしま |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | ;;Assume a preconfigured IPv6 Access List as follows:<br>デバイス(config)# **ipv6 access-list my_acls**<br>デバイス(config-ipv6-acl)# **permit host FE80::A8BB:CCFF:FE01:F700 any**<br><br>;;configure DCHPv6 Guard to match approved access list.<br>デバイス(config-dhcp-guard)# **match server access-list my_acls** | す（アクセス リストの宛先アドレスは「any」です）。設定されていない場合、このチェックは回避されます。空のアクセス リストは、permit all として処理されます。 |
| ステップ 5 | [**no**] **match reply prefix-list** *ipv6-prefix-list-name*<br>例：<br><br>;;Assume a preconfigured IPv6 prefix list as follows:<br>デバイス(config)# **ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128**<br><br>;; Configure DCHPv6 Guard to match prefix<br>デバイス(config-dhcp-guard)# **match reply prefix-list my_prefix** | （任意）DHCPv6応答メッセージ内のアドバタイズされたプレフィクスが設定された承認プレフィクス リストからのものであることの確認をイネーブルにします。設定されていない場合、このチェックは回避されます。空のプレフィクス リストは、permit として処理されます。 |
| ステップ 6 | [**no**]**preference**{ **max** *limit* \| **min** *limit* }<br>例：<br>デバイス(config-dhcp-guard)# **preference max 250**<br>デバイス(config-dhcp-guard)#**preference min 150** | **device-role** が **server** である場合に **max** および **min** を設定して、DHCPv6 サーバ アドバタイズメント値をサーバ優先度値に基づいてフィルタします。デフォルトではすべてのアドバタイズメントが許可されます。<br><br>**max** *limit*：（0 ～ 255）（任意）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限未満であるかどうかの検証をイネーブルにします。デフォルトは255です。設定されていない場合、このチェックは回避されます。<br><br>**min** *limit*：（0 ～ 255）（任意）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限を超過しているかどうかの検証をイネーブルにします。デフォルトは0です。設定されていない場合、このチェックは回避されます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 7 | [no] **trusted-port**<br>例：<br>デバイス(config-dhcp-guard)# **trusted-port** | （任意）**trusted-port**：ポートを信頼モードに設定します。このポートでは、これ以上のポリシングは実行されません。<br>（注） 信頼できるポートを設定した場合、device-role オプションは使用できません。 |
| ステップ 8 | **default** {**device-role** \| **trusted-port**}<br>例：<br>デバイス(config-dhcp-guard)# **default device-role** | （任意）**default**：コマンドをデフォルトに設定します。 |
| ステップ 9 | **do show ipv6 dhcp guard policy** *policy_name*<br>例：<br>デバイス(config-dhcp-guard)# **do show ipv6 dhcp guard policy example_policy** | （任意）コンフィギュレーション サブモードを終了せずに IPv6 DHCP のガード ポリシーの設定を表示します。*policy_name* 変数を省略すると、すべての DHCPv6 ポリシーが表示されます。 |

### DHCPv6 ガード設定の例

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

# IPv6 DHCP ガードポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** Interface_type *stack/module/port*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/1/4** | インターフェイスのタイプおよび ID を指定し、インターフェイスコンフィギュレーション モードを開始します。 |
| ステップ 3 | **ipv6 dhcp guard** [ **attach-policy** *policy_name* [ **vlan** {*vlan_ids* \| **add** *vlan_ids* \| **except** *vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ] \| **vlan** [ {*vlan_ids* \| **add** *vlan_ids* \| **except***vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ]<br>例：<br>デバイス(config-if)# **ipv6 dhcp guard attach-policy example_policy**<br>or<br>デバイス(config-if)# **ipv6 dhcp guard attach-policy example_policy vlan 222,223,224**<br>**or**<br>デバイス(config-if)# **ipv6 dhcp guard vlan 222, 223,224** | DHCP ガード ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。<br>**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |
| ステップ 4 | **do show running-config interface** Interface_type *stack/module/port*<br>例：<br>デバイス#(config-if)# **do show running-config gig 1/1/4** | コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。 |

# IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 DHCP ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface range** *Interface_name*<br>例：<br>デバイス(config)# **interface Po11** | EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。<br>ヒント　インターフェイス名やタイプを簡単に参照するには **do show interfaces summary** コマンドを使用します。 |
| ステップ 3 | **ipv6 dhcp guard** [ **attach-policy** *policy_name* [ **vlan** {*vlan_ids* \| **add** *vlan_ids* \| **except** *vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ] \| **vlan** [ {*vlan_ids* \| **add** *vlan_ids* \| **except***vlan_ids* \| **none** \| **remove** *vlan_ids* \| **all**} ]<br>例：<br>デバイス(config-if-range)# **ipv6 dhcp guard attach-policy example_policy**<br>or<br>デバイス(config-if-range)# **ipv6 dhcp guard attach-policy example_policy vlan 222,223,224**<br>**or**<br>デバイス(config-if-range)#**ipv6 dhcp guard vlan 222, 223,224** | DHCP ガード ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |
| ステップ 4 | **do show running-config interface***portchannel_interface_name*<br>例：<br>デバイス#(config-if-range)# **do show running-config int po11** | コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。 |

# IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法

複数のインターフェイス上の VLAN に IPv6 DHCP のガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **vlan configuration** *vlan_list*<br>例：<br>デバイス(config)# **vlan configuration 334** | VLANインターフェイスのコンフィギュレーションモードを開始し、IPv6スヌーピング ポリシーをアタッチする VLAN を指定します。 |
| ステップ 3 | **ipv6 dhcp guard** [ **attach-policy** *policy_name*]<br>例：<br>デバイス(config-vlan-config)#**ipv6 dhcp guard attach-policy example_policy** | すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルトポリシーがアタッチされます。デフォルト ポリシーは、device-role **client**、**no** trusted-port です。 |
| ステップ 4 | **do show running-config**<br>例：<br>デバイス#(config-if)# **do show running-config** | コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。 |

# IPv6 ソース ガードの設定方法

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | [**no**] **ipv6 source-guard policy** *policy_name*<br>例：<br>デバイス(config)# **ipv6 source-guard policy example_policy** | IPv6 ソース ガード ポリシー名を指定し、IPv6 ソース ガード ポリシー コンフィギュレーション モードを開始します。 |
| ステップ 4 | [**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }]<br>例：<br>デバイス(config-sisf-sourceguard)# **deny global-autoconf** | （任意）IPv6 ソース ガード ポリシーを定義します。<br>• **deny global-autoconf**：自動設定されたグローバル アドレスからのデータ トラフィックを拒否します。これは、リンク上のすべてのグローバル アドレスが DHCP によって割り当てられている際に、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。<br>• **permit link-local**：リンクローカル アドレスから送信されたすべてのデータ トラフィックを許可します。<br>（注） ソース ガード ポリシーに基づく信頼できるオプションはサポートされません。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config-sisf-sourceguard)# **end** | IPv6 ソース ガード ポリシー コンフィギュレーション モードを終了します。 |
| ステップ 6 | **show ipv6 source-guard policy** *policy_name*<br>例：<br>デバイス# **show ipv6 source-guard policy example_policy** | ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。 |

### 次のタスク

インターフェイスに IPv6 ソース ガード ポリシーを適用します。

# IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** Interface_type *stack/module/port*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/1/4** | インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ipv6 source-guard** [**attach-policy** <*policy_name*> ]<br>例：<br>デバイス(config-if)# **ipv6 source-guard attach-policy example_policy** | インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。<br>**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |
| ステップ 5 | **show ipv6 source-guard policy** *policy_name*<br>例：<br>デバイス#(config-if)# **show ipv6 source-guard policy example_policy** | ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。 |

# IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface port-channel** *port-channel-number*<br>例：<br>デバイス (config)# **interface Po4** | インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。 |
| ステップ 4 | **ipv6 source-guard** [**attach-policy** <*policy_name*> ]<br>例：<br>デバイス(config-if) # **ipv6 source-guard attach-policy example_policy** | インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。<br>**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |
| ステップ 5 | **show ipv6 source-guard policy** *policy_name*<br>例：<br>デバイス(config-if) #**show ipv6 source-guard policy example_policy** | ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。 |

# IPv6 プレフィックス ガードの設定方法

（注） プレフィックス ガードが適用されている場合にリンクローカル アドレスから送信されたルーティング プロトコル制御パケットを許可するには、ソースガード ポリシー コンフィギュレーション モードで permit link-local コマンドをイネーブルにします。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | ［**no**］**ipv6 source-guard policy** *source-guard-policy*<br>例：<br>デバイス (config)# **ipv6 source-guard policy my_snooping_policy** | IPv6 ソースガード ポリシー名を定義して、スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを開始します。 |
| ステップ 4 | ［ **no** ］**validate address**<br>例：<br>デバイス (config-sisf-sourceguard)# **no validate address** | アドレス検証機能をディセーブルにし、IPv6 プレフィックス ガード機能を設定できるようにします。 |
| ステップ 5 | **validate prefix**<br>例：<br>デバイス (config-sisf-sourceguard)# **validate prefix** | IPv6 ソース ガードをイネーブルにし、IPv6 プレフィックスガード動作を実行します。 |
| ステップ 6 | **exit**<br>例：<br>デバイス (config-sisf-sourceguard)# **exit** | スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 7 | **show ipv6 source-guard policy** ［*source-guard-policy*］<br>例：<br>デバイス # **show ipv6 source-guard policy policy1** | IPv6 ソースガード ポリシー設定を表示します。 |

# IPv6プレフィックスガードポリシーをインターフェイスにアタッチする方法

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **interface** Interface_type *stack/module/port*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/1/4** | インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ipv6 source-guard attach-policy** *policy_name*<br>例：<br>デバイス(config-if)# **ipv6 source-guard attach-policy example_policy** | インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。<br>**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。 |
| ステップ 5 | **show ipv6 source-guard policy** *policy_name*<br>例：<br>デバイス(config-if)# **show ipv6 source-guard policy example_policy** | ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。 |

# IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface port-channel** *port-channel-number*<br>例：<br>デバイス (config)# **interface Po4** | インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。 |
| ステップ 4 | **ipv6 source-guard** [**attach-policy** <*policy_name*> ]<br>例： | インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。<br>**attach-policy** オプションを使用しない場 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if)# **ipv6 source-guard attach-policy example_policy** | 合、デフォルト ポリシーがアタッチされます。 |
| ステップ 5 | **show ipv6 source-guard policy** *policy_name*<br>例：<br>デバイス(config-if)# **show ipv6 source-guard policy example_policy** | ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。 |

# IPv6 ファースト ホップ セキュリティの設定例

## 例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

次の例は、IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch(config-sisf-sourceguard) # validate address
switch(config-sisf-sourceguard)# exit
Switch(config)# interface Po4
Switch(config)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
Switch(config-if)# exit
switch(config)#
```

## 例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

次の例は、IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch (config-sisf-sourceguard)# no validate address
Switch((config-sisf-sourceguard)# validate prefix
Switch(config)# interface Po4
Switch(config-if)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
```

第 18 章

# SISF ベースのデバイストラッキングの設定


- SISF ベースのデバイストラッキングに関する情報 （339 ページ）
- SISF ベースのデバイストラッキングの設定方法 （345 ページ）
- SISF ベースのデバイストラッキングの設定例 （356 ページ）
- SISF ベースのデバイストラッキングの機能履歴と情報 （360 ページ）


## SISF ベースのデバイストラッキングに関する情報

### SISF ベースのデバイストラッキングの概要

スイッチ統合セキュリティ機能ベース（SISF ベース）のデバイストラッキング機能は、一連のファーストホップセキュリティ機能の一部です。

この機能の主な役割は、ネットワーク内のエンドノードの存在、ロケーション、移動を追跡することです。SISF は、スイッチが受信したトラフィックをスヌーピングし、デバイスアイデンティティ（MAC と IP アドレス）を抽出して、バインディングテーブルに保存します。IEEE 802.1X、web 認証、Cisco TrustSec、LISP などの多くの機能は、この情報の正確性に依存して正常に動作します。

SISF ベースのデバイストラッキングは、IPv4 と IPv6 の両方をサポートします。

SISF ベースのデバイストラッキングが導入されても、レガシーデバイストラッキング CLI（IP デバイストラッキング（IPDT）および IPv6 スヌーピング CLI）は引き続き使用できます。スイッチをブートアップすると、使用可能なコマンドのセットは既存の設定によって異なり、次のいずれかのみが使用可能です。

- SISF ベースのデバイストラッキング CLI、または
- IPDT および IPv6 スヌーピング CLI

（注） IPDT および IPv6 スヌーピングコマンドは廃止されましたが、引き続き使用できます。SISF ベースのデバイストラッキングにアップグレードすることを推奨します。

IPDT および IPv6 スヌーピング CLI を使用していて、SISF ベースのデバイストラッキングに移行する場合、詳細については「*レガシー IPDT と IPv6 スヌーピングから SISF ベースのデバイストラッキングへの移行*」を参照してください。

SISF ベースのデバイストラッキングは、手動で（**device-tracking** コマンドを使用して）、またはプログラムで（デバイス トラッキング サービスを他の機能に提供する場合に）有効にできます。

# SISF ベースのデバイストラッキングを有効にするオプション

デフォルトでは、SISF ベースのデバイストラッキングは無効になっています。

デバイス トラッキング ポリシーを定義し、そのポリシーを特定のターゲットに適用することで、有効にできます。

（注） ターゲットは、インターフェイスまたは VLAN です。

### SISF ベースのデバイストラッキングの手動による有効化

- オプション 1：**default** デバイス トラッキング ポリシーをターゲットに適用します。

  インターフェイス コンフィギュレーション モードまたは VLAN コンフィギュレーション モードで、**device-tracking** コマンドを入力します。次に、システムは**default**ポリシーをインターフェイスまたは VLAN に対応付けます。

  （注） **default**ポリシーは、デフォルト設定の組み込みポリシーです。**default**ポリシーの属性は変更できません。デバイストラッキングポリシーの属性を設定できるようにするには、カスタムポリシーを作成する必要があります。「*オプション 2：カスタム設定でカスタムポリシーを作成します*」を参照してください。

- オプション 2：カスタム設定でカスタムポリシーを作成します。

  グローバル コンフィギュレーション モードで device-tracking policy コマンドを入力し、続けてカスタムポリシー名を入力します。システムにより、指定した名前のポリシーが作成されます。その後、デバイス トラッキング コンフィギュレーション モード（config-device-tracking）で使用可能な設定を行い、指定したターゲットにポリシーをアタッチできます。

### プログラムによる SISF ベースのデバイストラッキングの有効化

一部の機能はデバイストラッキングに依存し、SISF ベースのデバイストラッキングが構築および維持するバインディングエントリの信頼性のあるデータベースを利用します。これらの機能

は、デバイス トラッキング クライアントとも呼ばれ、プログラムによりデバイストラッキングを有効にします（デバイス トラッキング ポリシーを作成して対応付けします）。

（注） ここでの例外は、IEEE 802.1X、web 認証、Cisco TrustSec、IP ソースガード（IPSG）です。これらはデバイストラッキングにも依存しますが、有効にはなりません。これらのデバイス トラッキング クライアントでは、**ip dhcp snooping vlan** *vlan* コマンドを入力して、プログラムにより特定のターゲットでデバイストラッキングを有効にする必要があります。

プログラムによる SISF ベースのデバイストラッキングの有効化については、次の点に注意してください。

- デバイス トラッキング クライアントでは、デバイストラッキングを有効にする必要があります。

  複数のデバイス トラッキング クライアントが存在するため、複数のプログラムポリシーを作成できます。各ポリシーの設定は、ポリシーを作成するデバイス トラッキング クライアントによって異なります。

- 作成されるポリシーとその設定はシステム定義です。

  設定可能なポリシー属性は、デバイス トラッキング コンフィギュレーション モード（config-device-tracking）で使用でき、リリースごとに異なります。設定不可能な属性を変更しようとすると、設定変更は拒否され、エラーメッセージが表示されます。

プログラムによって作成されたポリシーのリリース固有の情報については、マニュアルの必要なバージョンの『*Cisco IOS XE <release name> <release number>*』の「Programmatically Enabling SISF-Based Device Tracking」を参照してください。

# レガシーコマンドから SISF ベースの Device-Tracking コマンドへの移行

## レガシー IPDT と IPv6 スヌーピングから SISF ベースのデバイストラッキングへの移行

Cisco IOS XE Denali 16.1.1 以降では、既存の IPv6 スヌーピングおよび IP デバイストラッキング（IPDT）に、対応する SISF ベースの device-tracking コマンドが用意され、IPv4 と IPv6 の両方のアドレスファミリに設定を適用できるようになりました。

Cisco IOS XE 3.xx リリースから Cisco IOS XE 16.xx リリースにアップグレードした後、**device-tracking upgrade-cli** を入力してレガシー IPDT および IPv6 スヌーピングコマンドを SISF ベースのデバイス トラッキング コマンドに変換します。このコマンドを実行した後は、新しい device-tracking コマンドのみがデバイスで使用でき、レガシーコマンドはサポートされません。

デバイスにあるレガシー設定に基づいて、**device-tracking upgrade-cli** コマンドは CLI を異なる方法でアップグレードします。既存の設定を移行する前に、次の設定シナリオ、および対応する移行結果を検討します。

（注） 古い IPDT IPv6 スヌーピング CLI と新しい SISF ベースデバイストラッキング CLI の両方を設定することはできません。

### IPDT 設定のみが存在する

デバイスに IPDT 設定のみがある場合は、**device-tracking upgrade-cli** コマンドを実行すると、設定が変換され、新しく作成されてインターフェイスで適用される SISF ポリシーが使用されます。これにより、この SISF ポリシーを更新できます。

引き続きレガシーコマンドを使用する場合、レガシーモードでの操作が制限されます。このモードでは、レガシー IPDT と IPv6 スヌーピングコマンドのみがデバイスで使用可能になります。

### IPv6 スヌーピング設定のみが存在する

既存の IPv6 スヌーピング設定があるデバイスで、古い IPv6 スヌーピングコマンドを以降の設定に使用できます。次のオプションを使用できます。

- （推奨）**device-tracking upgrade-cli** コマンドを使用して、レガシー設定をすべて、新しい SISF ベースの device-tracking コマンドに変換します。変換後は、新しいデバイス トラッキング コマンドのみがデバイスで動作します。
- レガシー IPv6 スヌーピングコマンドを今後の設定に使用し、**device-tracking upgrade-cli** コマンドは実行しません。このオプションでは、デバイスで使用可能なのはレガシー IPv6 スヌーピングコマンドのみであり、新しい SISF ベースの device-tracking CLI コマンドは使用できません。

### IPDT と IPv6 スヌーピングの両方の設定が存在する

レガシー IPDT 設定と IPv6 スヌーピング設定の両方が存在するデバイスでは、レガシーコマンドを SISF ベースのデバイストラッキング CLI に変換できます。ただし、インターフェイスに適用することができるスヌーピングポリシーは 1 つだけであり、IPv6 スヌーピング ポリシーパラメータは IPDT 設定よりも優先される、ということに注意してください。

（注） 新しい SISF ベースのコマンドに移行しておらず、レガシー IPv6 スヌーピングや IPDT コマンドを使用し続けている場合、IPv4 デバイストラッキング設定情報が IPv6 スヌーピングコマンドに表示される可能性があります。SISF ベースのデバイストラッキング機能では、IPv4 と IPv6 の両方の設定を扱うためです。これを回避するには、レガシー設定を SISF ベースのデバイストラッキング コマンドに変換することを推奨します。

### IPDT または IPv6 スヌーピング設定が存在しない

デバイスにレガシー IP デバイストラッキング設定も IPv6 スヌーピング設定もない場合は、今後の設定に使用できるのは新しい SISF ベースの device-tracking コマンドのみです。レガシー IPDT コマンドと IPv6 スヌーピングコマンドは使用できません。

（注） Cisco IOS XE Denali 16.3.1 以降、**ip dhcp snooping vlan** *vlan* コマンドは、IEEE 802.1X、web 認証、Cisco TrustSec、IPSG 機能をサポートするために、プログラムによってデバイス トラッキング ポリシーを作成します。プログラムによって作成されたポリシーは、IPv4 および IPv6 クライアントの両方を追跡します。前述の機能のいずれかを使用している場合、このコマンドが設定されていることを確認します。

## IPDT、IPv6 スヌーピング、および SISF ベースのデバイストラッキング CLI の互換性

表 28 : IPDT → IPv6 スヌーピングコマンド （343 ページ） に、**device-tracking upgrade-cli** コマンド（グローバル コンフィギュレーション モード）が実行されていない場合に、レガシー IPDT と、それらが変換される IPv6 スヌーピングコマンドを示します。

表 表 29 : IPDT → SISF コマンド （344 ページ） に、**device-tracking upgrade-cli** コマンドを実行した場合に、レガシー IPDT と、それをシステムが変換する SISF ベースの device-tracking コマンドを示します。

**表 *28 : IPDT → IPv6* スヌーピングコマンド**

| レガシー IP デバイストラッキング（IPDT） | IPv6 スヌーピングコマンド<br>（Cisco IOS XE Denali 16.3.7 以降のすべての Cisco IOS XE 16.xx リリース）。 |
|---|---|
| **ip device tracking probe count** | デフォルト値に設定されており、変更できません。 |
| **ip device tracking probe delay** | デフォルト値に設定されており、変更できません。[9]。 |
| **ip device tracking probe interval** | **ipv6 neighbor binding reachable-lifetime**[10] |
| **ip device tracking probe use-svi** | デフォルトの動作に設定されており、変更できません。 |
| **ip device tracking probe auto-source** [ **fallback** *host-ip-address subnet-mask*] [**override**] | **ipv6 neighbor tracking auto-source** [ **fallback** *host-ip-address subnet-mask*] [**override**] |
| **ip device tracking trace-buffer** | サポート対象外 |
| **ip device tracking maximum n** | **ipv6 snooping policy** *IPDT_MAX_n* [**limit** *address-count*] |
| **ip device tracking maximum 0** | サポート対象外 |
| **clear ip device tracking all** | サポート対象外 |

[9] Cisco IOS XE Denali 16.3.6 まで、および Cisco IOS XE Everest 16.5.1a では、システムは **ip device tracking probe delay** コマンドを誤って **ipv6 neighbor binding reachable-lifetime** に変換します。Cisco IOS XE Denali 16.3.7 以降（Cisco IOS XE Everest 16.5.x を除く）では、デフォルト値に設定されており、変更できません。

[10] Cisco IOS XE Denali 16.3.6 まで、および Cisco IOS XE Everest 16.5.1a では、システムが **ip device tracking probe interval** コマンドを誤って **ipv6 snooping tracking retry-interval** に変換します。Cisco IOS XE Denali 16.3.7 以降（Cisco IOS XE Everest 16.5.x を除く）では、**ipv6 neighbor binding reachable-lifetime** に正しく変換されます。

表 *29 : IPDT → SISF* コマンド

| レガシー IP デバイストラッキング（IPDT） | SISF 変換後の SISF ベースのデバイストラッキング（Cisco IOS XE Denali 16.3.7 以降のすべての Cisco IOS XE 16.xx リリース）。 |
|---|---|
| **ip device tracking probe count** | デフォルト値に設定されており、変更できません。 |
| **ip device tracking probe delay** | デフォルト値に設定されており、変更できません。[11]。 |
| **ip device tracking probe interval** | **device-tracking binding reachable-lifetime**[12] |
| **ip device tracking probe use-svi** | デフォルトの動作に設定されており、変更できません。 |
| **ip device tracking probe auto-source** [ **fallback** *host-ip-address subnet-mask*] [**override**] | **device-tracking tracking auto-source** [ **fallback** *host-ip-address subnet-mask*] [**override**] |
| **ip device tracking trace-buffer** | 未サポート |
| **ip device tracking maximum n** | **device-tracking snooping policy** *IPDT_MAX_n* [**limit** *address-count*] |
| **ip device tracking maximum 0** | 未サポート |
| **clear ip device tracking all** | 未サポート |

[11] Cisco IOS XE Denali 16.3.6 まで、および Cisco IOS XE Everest 16.5.1a では、システムは **ip device tracking probe delay** コマンドを誤って **device-tracking binding reachable-lifetime** に変換します。Cisco IOS XE Denali 16.3.7 以降（Cisco IOS XE Everest 16.5.x を除く）では、デフォルト値に設定されており、変更できません。

[12] Cisco IOS XE Denali 16.3.6 まで、および Cisco IOS XE Everest 16.5.1a では、システムが **ip device tracking probe interval** コマンドを誤って **device-tracking tracking retry-interval** に変換します。Cisco IOS XE Denali 16.3.7 以降（Cisco IOS XE Everest 16.5.1a を除く）では、**device-tracking binding reachable-lifetime** に正しく変換されます。

# SISF ベースのデバイストラッキングの設定方法

## SISF ベースのデバイストラッキングの手動による有効化

### ターゲットへのデフォルト デバイス トラッキング ポリシーの適用

デフォルトのデバイス トラッキング ポリシーをインターフェイスまたは VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | インターフェイスまたは VLAN を指定します。<br>• **interface** *interface*<br>• **vlan configuration** *vlan_list*<br>例：<br>`Device(config)# interface gigabitethernet 1/1/4`<br>OR<br>`Device(config)# vlan configuration 333` | **interface** *type number*—Specifies the interface and enters the interface configuration mode. デバイス トラッキング ポリシーは、指定されたインターフェイスに適用されます。<br>**vlan configuration** *vlan_list*：VLAN を指定し、VLAN機能コンフィギュレーション モードを開始します。デバイス トラッキング ポリシーは、指定された VLAN に適用されます。 |
| ステップ 3 | **device-tracking**<br>例：<br>`Device(config-if)# device-tracking`<br>OR<br>`Device(config-vlan-config)# device-tracking` | SISF ベースのデバイストラッキングを有効にし、デフォルトポリシーをインターフェイスまたは VLAN に適用します。<br>デフォルトポリシーは、デフォルト設定の組み込みポリシーです。デフォルトポリシーの属性は変更できません。 |
| ステップ 4 | **exit**<br>例：<br>`Device(config-if)# exit`<br>OR<br>`Device(config-vlan-config)# exit` | 設定モードを終了します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **show device-tracking policy** *policy-name*<br>例：<br>`Device# show device-tracking policy default` | デバイストラッキング ポリシーの設定と、それが適用されるすべてのターゲットを表示します。 |

## カスタム設定を使用したカスタム デバイス トラッキング ポリシーの作成

デバイス トラッキング ポリシーを作成して設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | [**no**] **device-tracking policy** *policy-name*<br>例：<br>`Device(config)# device-tracking policy example_policy` | ポリシーを作成し、デバイストラッキング コンフィギュレーション モードを開始します。 |
| ステップ 3 | [**data-glean** \| **default** \| **destination-glean** \| **device-role** \| **distribution-switch** \| **exit** \| **limit** \| **no** \| **prefix-glean** \| **protocol** \| **security-level** \| **tracking** \| **trusted-port** \| **vpc**]<br>例：<br>`Device (config-device-tracking)# destination-glean log-only` | システムプロンプトに疑問符（?）を入力すると、このモードで使用できるオプションのリストが表示されます。IPv4 と IPv6 の両方に対して以下を設定できます。<br>• （任意）**data-glean**：ネットワーク内の送信元からスヌーピングされたデータパケットからのアドレスの学習を有効にし、データトラフィックの送信元アドレスとともにバインディングテーブルを読み込みます。次のいずれかのオプションを入力します。<br>  • log-only：データパケット通知時に syslog メッセージを生成します。<br>  • recovery：プロトコルを使用してバインディングテーブルの回復を有効にします。**NDP**または**DHCP**の入力。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • （任意）**default**：ポリシー属性をデフォルト値に設定します。次のポリシー属性をデフォルト値に設定できます。**data-glean**、**destination-glean**、**device-role**、**limit**、**prefix-glean**、**protocol**、**security-level**、**tracking**、**trusted-port**。<br>• （任意）**destination-glean**：データトラフィックの宛先アドレスを収集して、バインディングテーブルを読み込みます。次のいずれかのオプションを入力します。<br>  • log-only：データパケット通知時に syslog メッセージを生成します。<br>  • recovery：プロトコルを使用してバインディングテーブルの回復を有効にします。**DHCP** を入力します。<br>• （任意）**device-role**；ポートに接続されているデバイスのロールを設定します。ノードまたはスイッチを指定できます。次のいずれかのオプションを入力します。<br>  • node：接続されているデバイスをノードとして設定します。これがデフォルトのオプションです。<br>  • switch：接続されているデバイスをスイッチとして設定します。<br>• （任意）**distribution-switch**：このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • **exit**：デバイストラッキング ポリシー コンフィギュレーション モードを終了します。<br>• **limit** address-count：ポートごとのアドレスカウント制限を指定します。有効な範囲は1～32000です。<br>• **no**：コマンドを無効にするか、デフォルト値を設定します。<br>• （任意）**prefix-glean**：IPv6 ルータアドバタイズメントまたはDHCP-PD のどちらかからのプレフィックスの学習を有効にします。次のオプションがあります。<br>　• （任意）**only**：プレフィックスのみを収集し、ホストアドレスは収集しません。<br>• （任意）**protocol**：収集するプロトコルを設定します。デフォルトでは、すべて収集されます。次のいずれかのオプションを入力します。<br>　• **arp** ［**prefix-list** *name*］：ARP パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。<br>　• **dhcp4** ［**prefix-list** *name*］：DHCPv4 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。<br>　• **dhcp6** ［**prefix-list** *name*］：DHCPv6 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。<br>　• **ndp** ［**prefix-list** *name*］：NDP パケットのアドレスを収集します。必要に応じて、照合するプ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | レフィックスリストの名前を入力します。<br>• **udp** ［**prefix-list** *name*］：このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。<br>• （任意）**security-level**：この機能によって適用されるセキュリティのレベルを指定します。次のいずれかのオプションを入力します。<br>• **glean** ：アドレスをパッシブに収集します。<br>• **guard** ：不正なメッセージを検査してドロップします。これはデフォルトです。<br>• **inspect** ：メッセージを収集して検証します。<br>• （オプション）**tracking**：トラッキングオプションを指定します。次のいずれかのオプションを入力します。<br>• **disable** ［**stale-lifetime** ［*1* ー *86400* 秒 \| **infinite**］］：デバイストラッキングをオフにします。<br>必要に応じて、エントリを削除するまで非アクティブにする期間を入力することも、永続的に非アクティブにすることもできます。<br>• **enable** ［**reachable-lifetime** ［*1* ー *86400* 秒 \| **infinite**］］：デバイストラッキングをオンにします。<br>必要に応じて、エントリを到達可能にする期間を入力すること |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | も、永続的に到達可能にすることもできます。<br>• （任意）**trusted-port**：信頼できるポートを設定します。該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。<br>• （任意）**vpc**：このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。 |
| ステップ 4 | **end**<br>例：<br>`Device(config-device-tracking)# exit` | 設定モードを終了します。 |
| ステップ 5 | **show device-tracking policy** *policy-name*<br>例：<br>`Device# show device-tracking policy example_policy` | デバイス トラッキング ポリシー設定を表示します。 |

### 次のタスク

ポリシーをインターフェイスまたは VLAN に適用します。

## デバイス トラッキング ポリシーのインターフェイスへの適用

デバイス トラッキング ポリシーをインターフェイスにアタッチするには、特権 EXEC モードで次の手順を実行します。

### 手順

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

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **interface** *interface*<br>例：<br>`Device(config)# interface gigabitethernet 1/1/4` | インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | [**no**] **device-tracking attach-policy** *policy name*<br>例：<br>`Device(config-if)# device-tracking attach-policy example_policy` | デバイス トラッキング ポリシーをインターフェイスに適用します。<br>（注） SISF ベースのデバイス トラッキング ポリシーは、カスタム ポリシーである場合にのみ無効にできます。プログラムによって作成されたポリシーは、対応するデバイストラッキング クライアント機能の設定が削除された場合にのみ削除できます。 |
| ステップ 4 | **end**<br>例：<br>`Device# end` | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show device-tracking policies** [**interface** *interface*]<br>例：<br>`Device# show device-tracking policies interface gigabitethernet 1/1/4` | 指定されたインターフェイスの種類と番号に一致するポリシーを表示します。 |

## デバイス トラッキング ポリシーの VLAN への適用

複数のインターフェイスでデバイス トラッキング ポリシーを VLAN にアタッチするには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **vlan configuration** *vlan_list*<br>例：<br>`Device(config)# vlan configuration 333` | デバイス トラッキング ポリシーを適用する VLAN を指定し、その VLAN インターフェイスのコンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | [**no**] **device-tracking attach-policy** *policy_name*<br>例：<br>`Device(config-vlan-config)# device-tracking attach-policy example_policy` | すべてのスイッチインターフェイスで、デバイス トラッキング ポリシーを指定された VLAN にアタッチします。<br>（注） SISF ベースのデバイス トラッキング ポリシーは、カスタム ポリシーである場合にのみ無効にできます。プログラムによって作成されたポリシーは、対応するデバイストラッキング クライアント機能の設定が削除された場合にのみ削除できます。 |
| ステップ 4 | **do show device-tracking policies vlan** *vlan-ID*<br>例：<br>`Device(config-vlan-config)# do show device-tracking policies vlan 333` | VLAN インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが指定された VLAN に割り当てられていることを確認します。 |

# Cisco IOS XE Everest 16.6.x での SISF ベースのデバイストラッキングのプログラムによる有効化

表 *30 : Cisco IOS XE Everest 16.6.x* での *SISF* ベースのデバイストラッキングのプログラムによる有効化

| | |
|---|---|
| SISF ベースのデバイストラッキングを有効にできるデバイス トラッキング クライアント機能 | このリリースでは、次の機能に対して SISF ベースのデバイストラッキングをプログラムで有効にできます。<br>• IEEE 802.1X、web 認証、Cisco TrustSec、IPSG 機能：**ip dhcp snooping vlan** *vlan* コマンドを入力します。<br>• Cisco Locator/ID Separation Protocol（LISP）。<br>（注） プログラムによって作成されたポリシーが複数ある場合、LISP 設定は有効です。これは、他のデバイス トラッキング クライアント機能の動作に悪影響を与えることはありません。たとえば、IEEE 802.1X の **ip dhcp snooping vlan** *vlan* コマンドを設定し、LISP を設定して SISF ベースのデバイストラッキングを有効にした場合も、IEEE 802.1X 機能は予期どおりに動作し続けます。 |

| | |
|---|---|
| [Policy Name] | DT-PROGRAMMATIC<br>複数のデバイス トラッキング クライアント機能がありますが、システムによって生成されたポリシーは同一です。設定のリストは、プログラムによって作成されたポリシーにより異なる場合があります。詳細については、例を参照してください。 |

| | |
|---|---|
| ユーザ オプション | • 同じインターフェイスまたは VLAN に適用することができるのは、1 つのポリシーだけです。<br>• ポリシーを別のポリシーに置き換えることはできません。<br>• デバイス トラッキング クライアント機能の設定が削除されない限り、ポリシーは削除できません。<br>• プログラムによって作成されたポリシーの次の設定を変更できます（デバイス トラッキング コンフィギュレーション モード（config-device-tracking）での **device-tracking policy** コマンド）。<br>  • **data-glean**<br>  • **default**<br>  • **device-role**<br>  • **destination-glean**<br>  • **exit**<br>  • **limit**<br>  • **no**<br>  • **prefix-glean**<br>  • **protocol**<br>  • **security-level**<br>  • **tracking**<br>  • trusted-port<br>  • **distribution-switch** および **vpc** は CLI に表示されますが、設定の変更は有効になりません。<br>• MAC設定ごとのアドレスカウント制限は変更できません（これは**limit address-count for IPv4 per mac** および **limit address-count for IPv6 per mac** コマンドを参照）が、ポートまたはインターフェイスごとのアドレスカウント制限は変更できます。<br>• デバイストラッキング ポリシーが VLAN のインターフェイスに適用されると、インターフェイスのポリシー設定がVLANのポリシー設定よりも優先されます。ここでの例外は、**limit address-count for IPv4 per mac** と **limit address-count for IPv6 per mac** の値で、インターフェイスと VLAN の両方のポリシーから集約されます。 |

# トランクポートからのバインディングエントリの作成を停止するためのマルチスイッチネットワークの設定

マルチスイッチネットワークでは、SISF ベースのデバイストラッキングにより、機能を実行しているスイッチ間でバインディング テーブル エントリを分散できます。バインディングエントリは、ホストがアクセスポートに表示されるスイッチでのみ作成されます。トランクポート経由で表示されるホストのエントリは作成されません。これは、**trusted-port** および **device-role switch** オプションを使用してポリシーを設定し、トランクポートに適用することで実現されます。

**重要** ポリシーで、**trusted-port** および **device-role switch** オプションの両方を設定する必要があります。

さらに、SISF ベースのデバイストラッキングが有効になっているデバイス側のポートに、このようなポリシーを適用することを推奨します。

次の手順を実行します。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| **ステップ 2** | **device-tracking policy** *policy-name*<br>例：<br>`Device(config)# device-tracking policy example_trusted_policy` | 指定されたポリシーのデバイストラッキング ポリシー コンフィギュレーション モードを開始します。 |
| **ステップ 3** | **device-role switch**<br>例：<br>`Device(config-device-tracking)# device-role switch` | ポートに接続されているデバイスのロールを指定します。デフォルトは node です。ポートのバインディングエントリの作成を停止する **device-role switch** オプションを入力します。 |
| **ステップ 4** | **trusted-port**<br>例：<br>`Device(config-device-tracking)# trusted-port` | 信頼できるポートを設定します。該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 突が発生した場合、信頼できるポートが優先されます。 |
| ステップ 5 | **end**<br>例：<br>`Device(config-device-tracking)# end` | デバイストラッキング ポリシー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードを開始します。 |
| ステップ 6 | **interface** *interface*<br>例：<br>`Device(config)# interface gigabitethernet 1/0/25` | インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 7 | **device-tracking attach-policy** *policy-name*<br>例：<br>`Device(config-if)# device-tracking attach-policy example_trusted_policy` | デバイス トラッキング ポリシーをインターフェイスまたはそのインターフェイス上で指定された VLAN にアタッチします。 |

# SISF ベースのデバイストラッキングの設定例

次の例は、デバイストラッキングの設定例と、特定の状況で推奨される、または関連するその他の設定を示しています。

## 例：Cisco IOS XE Everest 16.6.x での SISF ベースのデバイストラッキングのプログラムによる有効化

例の出力例は、プログラムによって作成されたポリシーのさまざまな設定を示しています。

### デバイス トラッキング クライアント：LISP

ここでの LISP の設定は、あくまでも一例です。

LISP を設定した後、特権 EXEC モードで **show device-tracking policy** コマンドを入力して、作成された `DT-PROGRAMMATIC` ポリシーと対応する設定を表示します。

```
Device(config)# router lisp
<output truncated>
Device(config-router-lisp)# instance-id 3
Device(config-router-lisp-instance)# service ethernet
Device(config-router-lisp-instance-service)# eid-table vlan 10
Device(config-router-lisp-instance-dynamic-eid)# database-mapping 10.1.1.0/24 locator-set
 set1
Device(config-router-lisp-instance-service)# exit-service-ethernet
Device(config-router-lisp-instance)# exit-instance-id
Device(config-router-lisp)# exit-router-lisp
```

```
Device# show device-tracking policy DT-PROGRAMMATIC
Policy DT-PROGRAMMATIC configuration:
  security-level guard (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1 (*)
  limit address-count for IPv6 per mac 8 (*)
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target      Type  Policy             Feature            Target range
vlan 10     VLAN  DT-PROGRAMMATIC    Device-tracking    vlan all
 note:
 Binding entry Down timer: 10 minutes (*)
 Binding entry Stale timer:   30 minutes (*)
```

### デバイス トラッキング クライアント：IEEE 802.1X、web 認証、Cisco TrustSec、IPSG

グローバル コンフィギュレーション モードで **ip dhcp snooping vlan** *vlan* コマンドを設定して、IEEE 802.1X、web 認証、Cisco TrustSec、IPSG 機能のデバイストラッキングを有効にします。特権 EXEC モードで **show device-tracking policy** コマンドを入力し、作成された `DT-PROGRMMATIC` ポリシーとポリシーに応じて行った設定を表示します。

```
Device# configure terminal
Device(config)# ip dhcp snooping vlan 10
Device(config)# end

Device# show device-tracking policy DT-PROGRAMMATIC
Policy DT-PROGRAMMATIC configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1 (*)

  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target   Type    Policy             Feature          Target range
vlan 10  VLAN    DT-PROGRAMMATIC    Device-tracking  vlan all
  note:
  Binding entry Down timer: 24 hours (*)
  Binding entry Stale timer:   24 hours (*)
```

## 例：ターゲットでの IPv6 デバイストラッキングの無効化

デフォルトでは、SISF ベースのデバイストラッキングは IPv4 と IPv6 の両方をサポートします。次の設定例は、必要な場合に IPv6 デバイストラッキングを無効にする方法を示しています。

ターゲットがカスタムポリシーに適用されている場合の**IPv6**デバイストラッキングの無効化：

```
Device(config)# device-tracking policy example-policy
 Device(config-device-tracking)# no protocol ndp
 Device(config-device-tracking)# no protocol dhcp6
 Device(config-device-tracking)# end
```

ターゲットがプログラムによるポリシーに適用されている場合の**IPv6**デバイストラッキングの無効化：

（注） Cisco IOS XE Denali 16.3.x および Cisco IOS XE Everest 16.5.x のリリースで IPv6 デバイストラッキングを無効にすることはできません。

Cisco IOS XE Everest 16.6.x では、プログラムによるポリシーを変更することで、IPv6 デバイストラッキングを無効にできます。

```
Device(config)# device-tracking policy DT-PROGRAMMATIC
Device(config-device-tracking)# no protocol ndp
Device(config-device-tracking)# no protocol dhcp6
Device(config-device-tracking)# end
```

# 例：VLAN 上の SVI に対する IPv6 の有効化（重複アドレスの問題を軽減するため）

ネットワークで IPv6 が有効になっており、VLAN 上でスイッチ仮想インターフェイス（SVI）が設定されている場合は、SVI 設定に次の内容を追加することを推奨します。これにより、SVI はリンクローカルアドレスを自動的に取得できます。このアドレスは SISF プローブの送信元 IP アドレスとして使用されるため、重複 IP アドレスの問題を防止できます。

```
Device(config)# interface vlan 10
Device(config-if)# ipv6 enable
Device(config-if)# end
```

# 例：IPv4 重複アドレスの問題の緩和

次に、Microsoft Windows を実行しているクライアントによって発生した`重複 IP アドレス 0.0.0.0 エラーメッセージ`の問題に対応する例を示します。

**device-tracking tracking auto-source** コマンドを設定します。このコマンドは、デバイストラッキングテーブル内のエントリを維持するために、スイッチがクライアントをプローブするよう送信するアドレス解決パケット（ARP）要求で使用される送信元 IP および MAC アドレスを決定します。その目的は、送信元 IP アドレスとして 0.0.0.0 を使用しないようにすることです。

（注） スイッチ仮想インターフェイス（SVI）が設定されていない場合にのみ、**device-tracking tracking auto-source** コマンドを設定します。SVI が VLAN で IPv4 アドレスを使用して設定されている場合は、設定する必要はありません。

| コマンド | Action<br>（デバイストラッキング ARP プローブの送信元 IP および MAC アドレスを選択するため） | 注記 |
|---|---|---|
| **device-tracking tracking auto-source** | • 存在する場合、VLAN SVI に送信元を設定します。<br>• 同じサブネットからデバイストラッキング テーブルで IP および MAC バインディングを検索します。<br>• 0.0.0.0 を使用します。 | MAC フラッピングを回避するために、すべてのトランクポートでデバイストラッキングを無効にすることを推奨します。 |
| **device-tracking tracking auto-source override** | • 存在する場合、VLAN SVI に送信元を設定します。<br>• 0.0.0.0 を使用します。 | SVI がない場合は推奨しません。 |
| **device-tracking tracking auto-source fallback 0.0.0.X 255.255.255.0** | • 存在する場合、VLAN SVI に送信元を設定します。<br>• 同じサブネットからデバイストラッキング テーブルで IP および MAC バインディングを検索します。<br>• 提供されたホストビットとマスクを使用して、クライアント IP から送信元 IP を計算します。送信元 MAC は、クライアント側のスイッチポートの MAC アドレスから取得されます*。 | MAC フラッピングを回避するために、すべてのトランクポートでデバイストラッキングを無効にすることを推奨します。<br>計算された IPv4 アドレスは、クライアントまたはネットワークデバイスに割り当てることはできません。 |

| コマンド | Action<br>（デバイストラッキング ARP プローブの送信元 IP および MAC アドレスを選択するため） | 注記 |
|---|---|---|
| **device-tracking tracking auto-source fallback 0.0.0.X 255.255.255.0 override** | • 存在する場合、VLAN SVI に送信元を設定します。<br>提供されたホストビットとマスクを使用して、クライアント IP から送信元 IP を計算します*。送信元 MAC は、クライアント側のスイッチポートの MAC アドレスから取得されます*。 | |

* クライアント IP アドレスによっては、IPv4 アドレスを送信元 IP 用に予約する必要があります。

予約済み送信元 IPv4 アドレス = (client-ip and mask) | host-ip

- クライアント IP = 192.0.2.25
- 送信元 IP = (192.0.2.25 and 255.255.255.0) | (0.0.0.1) = 192.0.2.1

IP アドレス 192.0.2.1 をクライアントまたはネットワークデバイスに割り当てないでください。

## 例：短いデバイストラッキング バインディング到達可能時間の回避

以前のリリースから移行する場合、次の設定が存在している可能性があります。

```
device-tracking binding reachable-time 10
```

コマンドの **no** バージョンを入力して、これを削除します。

# SISF ベースのデバイストラッキングの機能履歴と情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

| リリース | 変更内容 |
|---|---|
| Cisco IOS XE Denali 16.1.1 | この機能が導入されました。 |

| リリース | 変更内容 |
|---|---|
| Cisco IOS XE Denali 16.3.7 | IPv6 スヌーピングコマンドおよび SISF ベースのデバイストラッキング コマンドのシステム変換を修正。<br><br>IPDT → IPv6 スヌーピング変換の修正：<br><br>• Cisco IOS XE Denali 16.3.6 までは、システムは **ip device tracking probe delay** コマンドを誤って **ipv6 neighbor tracking retry-interval** に変換します。Cisco IOS XE Denali 16.3.7 以降では、デフォルト値に設定されており、変更できません。<br><br>• Cisco IOS XE Denali 16.3.6 までは、システムは **ip device tracking probe interval** コマンドを誤って **ipv6 neighbor tracking retry-interval** に変換します。Cisco IOS XE Denali 16.3.7 以降では、に正しく変換されます。 **ipv6 snooping tracking retry-interval**<br><br>IPDT → SISF 変換の修正：<br><br>• Cisco IOS XE Denali 16.3.6 までは、システムは **ip device tracking probe delay** コマンドを誤って **device-tracking binding reachable-lifetime** に変換します。指定のリリースでは、このコマンドを引き続き使用できますが、エントリの reachable-lifetime のみを設定できます。Cisco IOS XE Denali 16.3.7 以降では、デフォルト値に設定されており、変更できません。<br><br>• Cisco IOS XE Denali 16.3.6 までは、システムは **ip device tracking probe interval** コマンドを誤って **device-tracking tracking retry-interval** に変換します。Cisco IOS XE Denali 16.3.7 以降では、**device-tracking binding reachable-lifetime** に正しく変換されます。 |
| Cisco IOS XE Everest 16.5.1a | LISP を設定することで、この機能をプログラムで有効にできるようになりました。<br><br>システムによって生成されたポリシー名が DT-PROGRAMMATIC に変更されます。イネーブラは複数ありますが、システムによって生成されたポリシーは同一です。設定のリストは各イネーブラによって異なります。<br><br>カスタムポリシーを作成して、インターフェイスまたは VLAN に付加することもできます。<br><br>（注） IPDT → IPv6 および IPDT → SISF のシステム変換の修正は、Cisco IOS XE Denali 16.3.7 から導入されましたが、これらの修正は Cisco IOS XE Everest 16.5.1a では利用できません。 |
| Cisco IOS XE Everest 16.6.1 | このリリース以降、DT_PROGRAMMATIC の特定の設定を変更できます（デバイス トラッキング コンフィギュレーション モード（config-device-tracking）で **device-tracking policy** コマンドを使用）。 |

第 19 章

# IEEE 802.1x ポートベースの認証の設定

この章では、IEEE 802.1x ポート ベース認証を設定する方法について説明します。IEEE 802.1x 認証は、不正なデバイス（クライアント）によるネットワーク アクセスを防止します。別途記載のないかぎり、スイッチという用語はスタンドアロンスイッチまたはスイッチスタックを意味します。


- 802.1x ポートベース認証について （363 ページ）
- 802.1x ポートベース認証の設定方法 （401 ページ）
- 802.1x の統計情報およびステータスのモニタリング （455 ページ）


## 802.1x ポートベース認証について

802.1x 規格では、一般の人がアクセス可能なポートから不正なクライアントが LAN に接続しないように規制する（適切に認証されている場合を除く）、クライアント/サーバ型のアクセス コントロールおよび認証プロトコルを定めています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN が提供するサービスを利用できるようにします。

（注） TACACS は、802.1x 認証ではサポートされていません。

802.1x アクセス コントロールでは、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、およびスパニングツリー プロトコル（STP）トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

次の表に、Catalyst 3850 および Catalyst 3650 スイッチでサポートされる各クライアント セッションの最大数を示します。

| クライアント セッション | サポートされる最大セッション数 |
|---|---|
| dot1x または MAB クライアント セッションの最大数 | 2000 |

| クライアント セッション | サポートされる最大セッション数 |
|---|---|
| Web ベース認証セッションの最大数 | 2000 |
| クリティカル認証 VLAN を有効にしてサーバを再初期化した dot1x セッションの最大数 | 2000 |
| さまざまなセッション機能が適用される MAB セッションの最大数 | 2000 |
| サービス テンプレートまたはセッション機能が適用される dot1x セッションの最大数 | 2000 |

# ポートベース認証プロセス

IEEE 802.1X ポートベース認証を設定するには、認証、認可、およびアカウンティング（AAA）を有効にし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

AAA プロセスは認証から始まります。802.1x ポートベース認証がイネーブルであり、クライアントが 802.1x 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

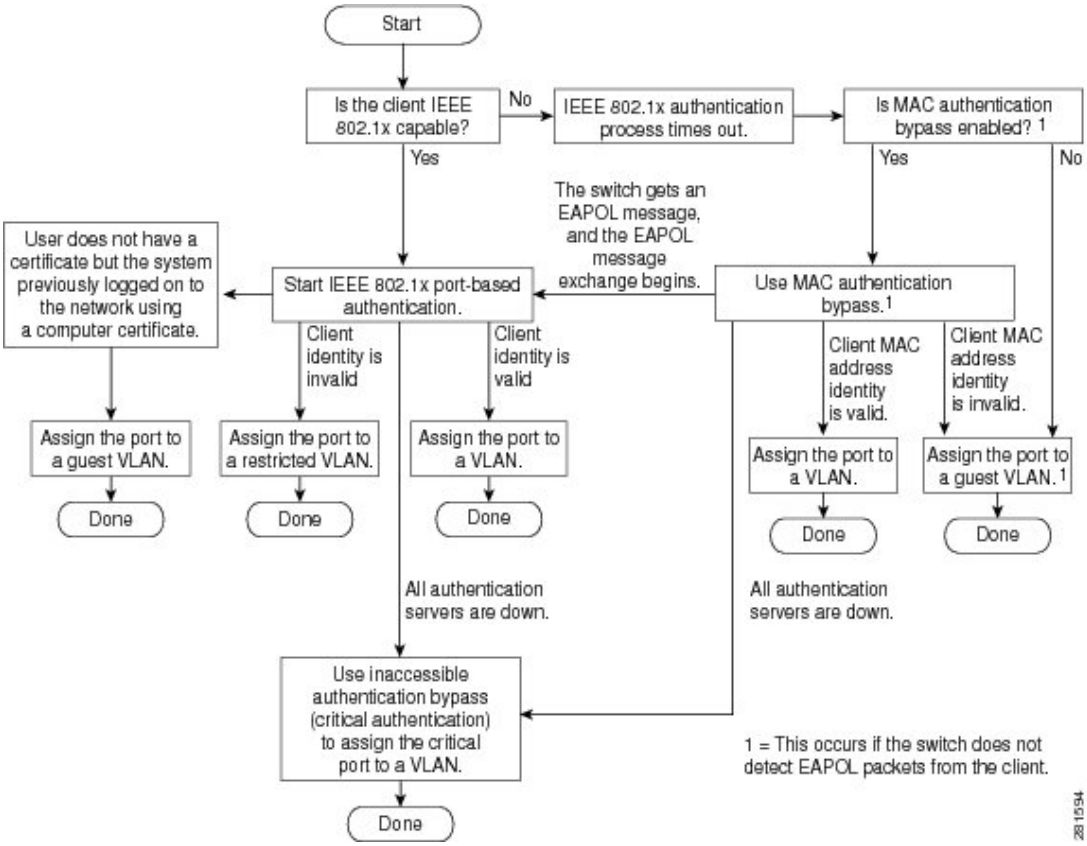
- クライアント ID が有効で 802.1x 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。

（注） アクセスできない認証バイパスは、クリティカル認証、または AAA 失敗ポリシーとも呼ばれます。

ポートで Multi Domain Authentication（MDA）が有効になっている場合、音声許可に該当する例外をいくつか伴ったフローを使用できます。

**図 *21 :* 認証フローチャート**

次の図は認証プロセスを示します。




次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

  スイッチ固有の値を使用するか、RADIUS サーバからの値に基づいて再認証タイマーを設定できます。

  RADIUS サーバを使用した 802.1x 認証の後で、スイッチは Session-Timeout RADIUS 属性（Attribute[27]）、および Termination-Action RADIUS 属性（Attribute[29]）に基づいてタイマーを使用します。

  Session-Timeout RADIUS 属性（Attribute[27]）には再認証が行われるまでの時間を指定します。指定できる範囲は 1 ～ 65535 秒です。

  Termination-Action RADIUS 属性（Attribute[29]）には、再認証中に行われるアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。アクションに *Initialize*（属性値は *DEFAULT*）を設定した場合、802.1x セッションは終了し、認証中、接続は失われます。アクションに *ReAuthenticate*（属性値は RADIUS-Request）を設定した場合、セッションは再認証による影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを入力します。

# ポートベース認証の開始およびメッセージ交換

802.1x認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにすると、スイッチは、リンクステートがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

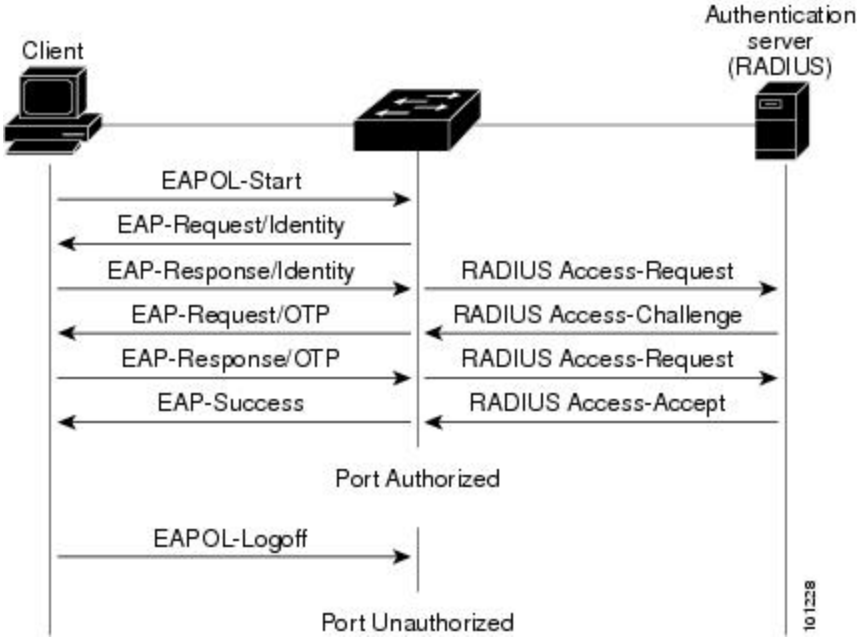
（注） ネットワーク アクセスデバイスで802.1x認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。

図 *22 :* メッセージ交換

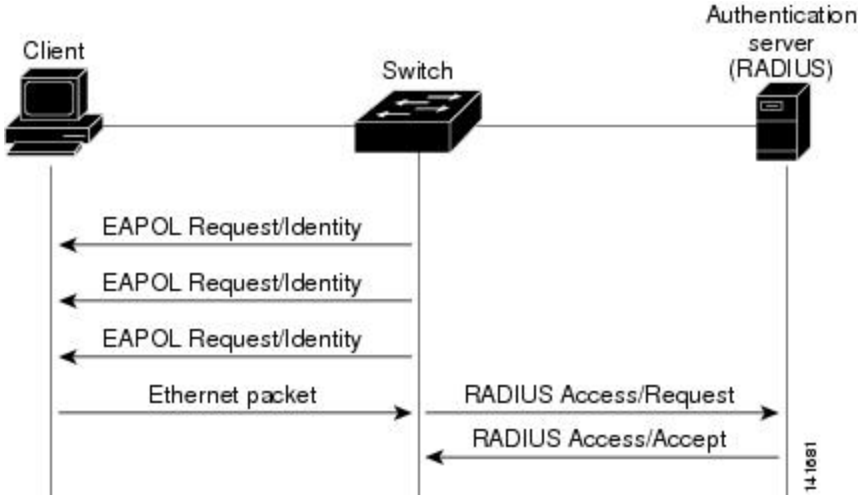
次の図に、クライアントが RADIUS サーバとの間で OTP（ワンタイム パスワード）認証方式を使用する際に行われるメッセージ交換を示します。




EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネットパケットを検出するとそのクライアントを認証できます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS Access/Request フレームにこの情報を保存します。サーバがスイッチに RADIUS Access/Accept フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネット パケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、802.1x 認証を開始します。

図 *23 : MAC* 認証バイパス中のメッセージ交換

次の図に、MAC 認証バイパス中のメッセージ交換を示します。




# ポートベース認証の認証マネージャ

## ポートベース認証方法

表 *31 : 802.1x* 機能

| 認証方法 | モード | | | |
|---|---|---|---|---|
| | シングル ホスト | マルチ ホスト | **MDA** | 複数認証 |
| 802.1x | VLAN 割り当て<br>ユーザ単位 ACL<br>Filter-ID 属性<br>ダウンロード可能 ACL<br>リダイレクト URL | VLAN 割り当て | VLAN 割り当て<br>ユーザ単位 ACL<br>Filter-ID 属性<br>ダウンロード可能 ACL<br>リダイレクト URL | VLAN 割り当て<br>ユーザ単位 ACL<br>Filter-ID 属性<br>ダウンロード可能 ACL<br>リダイレクト URL |
| MAC 認証バイパス | VLAN 割り当て<br>ユーザ単位 ACL<br>Filter-ID 属性<br>ダウンロード可能 ACL<br>リダイレクト URL | VLAN 割り当て | VLAN 割り当て<br>ユーザ単位 ACL<br>Filter-ID 属性<br>ダウンロード可能 ACL<br>リダイレクト URL | VLAN 割り当て<br>ユーザ単位 ACL<br>Filter-ID 属性<br>ダウンロード可能 ACL<br>リダイレクト URL |

| 認証方法 | モード | | | |
|---|---|---|---|---|
| | シングル ホスト | マルチ ホスト | MDA | 複数認証 |
| スタンドアロン Web 認証 | プロキシ ACL、Filter-ID 属性、ダウンロード可能な ACL | | | |
| NAC レイヤ 2 IP 検証 | Filter-ID 属性<br>ダウンロード可能 ACL<br>リダイレクト URL | Filter-ID 属性<br>ダウンロード可能 ACL<br>リダイレクト URL | Filter-ID 属性<br>ダウンロード可能 ACL<br>リダイレクト URL | Filter-ID 属性<br>ダウンロード可能 ACL<br>リダイレクト URL |
| フォールバック方式としての Web 認証 | プロキシ ACL<br>Filter-ID 属性<br>ダウンロード可能 ACL | プロキシ ACL<br>Filter-ID 属性<br>ダウンロード可能 ACL | プロキシ ACL<br>Filter-ID 属性<br>ダウンロード可能 ACL | プロキシ ACL<br>Filter-ID 属性<br>ダウンロード可能 ACL |

[13] Cisco IOS リリース 12.2(50)SE 以降でサポートされています。
[14] 802.1x 認証をサポートしないクライアント用。

## ユーザ単位 ACL および Filter-Id

（注） Filter-Id としてロールベース ACL を使用することは推奨されません。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。ホストに適用される ACL ポリシーは、別のホストのトラフィックには影響を与えません。マルチ ホスト ポートで認証されるホストが 1 つだけで、他のホストが認証なしでネットワーク アクセスを取得する場合、発信元アドレスに any を指定することで、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

## ポートベース認証マネージャ CLI コマンド

認証マネージャ インターフェイス コンフィギュレーション コマンドは、802.1x、MAC 認証バイパスおよび Web 認証など、すべての認証方法を制御します。認証マネージャ コマンドは、接続ホストに適用される認証方法のプライオリティと順序を決定します。

認証マネージャ コマンドは、ホスト モード、違反モードおよび認証タイマーなど、一般的な認証機能を制御します。一般的な認証コマンドには、**authentication host-mode**、**authentication violation**、および **authentication timer** インターフェイス コンフィギュレーション コマンドが含まれます。

802.1x 専用コマンドは、先頭に **dot1x** キーワードが付きます。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにします。

スイッチでの dot1x を無効にするには、**no dot1x system-auth-control** コマンドを使用して、設定をグローバルに削除し、設定されているすべてのインターフェイスからも削除します。

（注） 802.1x 認証がグローバルにディセーブル化されても、Web 認証など他の認証方法はそのポートでイネーブルのままです。

スイッチで dot1x を再度有効にするには、dot1x グローバル設定とインターフェイス設定の両方を設定する必要があります。設定が不完全な場合、CPU 使用率が高くなる可能性があります。

**authentication manager** コマンドは、以前の 802.1x コマンドと同じ機能を提供します。

認証マネージャが生成する冗長なシステムメッセージをフィルタリングすると、通常は、フィルタリングされた内容が認証の成功に結びつきます。802.1x 認証および MAB 認証の冗長なメッセージをフィルタリングすることもできます。認証方式ごとに異なるコマンドが用意されています。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの詳細メッセージをフィルタリングします。
- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1x 認証の詳細メッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC 認証バイパス（MAB）の詳細メッセージをフィルタリングします。

表 *32 :* 認証マネージャ コマンドおよび以前の *802.1x* コマンド

| Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド | Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド | 説明 |
|---|---|---|
| **authentication control-direction** {**both** \| **in**} | **dot1x control-direction** {**both** \| **in**} | Wake-on-LAN（WoL）機能を使用して 802.1x 認証をイネーブルにし、ポート制御を単一方向または双方向に設定します。 |
| **authentication event** | **dot1x auth-fail vlan**<br>**dot1x critical (interface configuration)**<br>**dot1x guest-vlan6** | ポート上で制限付き VLAN をイネーブルにします。<br>アクセス不能認証バイパス機能をイネーブルにします。<br>アクティブ VLAN を 802.1x ゲスト VLAN として指定します。 |

| Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド | Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド | 説明 |
|---|---|---|
| **authentication fallback** *fallback-profile* | **dot1x fallback** *fallback-profile* | 802.1x 認証をサポートしていないクライアント用に、Web 認証をフォールバック方式として使用するようにポートを設定します。 |
| **authentication host-mode**[**multi-auth** \|**multi-domain** \|**multi-host** \|**single-host**] | **dot1x host-mode** {**single-host** \| **multi-host** \| **multi-domain**} | 802.1x 許可ポートで単一のホスト（クライアント）または複数のホストの接続を許可します。 |
| **authentication order** | **mab** | 使用される認証方法の順序を柔軟に定義できるようにします。 |
| **authentication periodic** | **dot1x reauthentication** | クライアントの定期的再認証をイネーブルにします。 |
| **authentication port-control** {**auto** \| **force-authorized** \| **force-un authorized**} | **dot1x port-control** {**auto** \| **force-authorized** \| **force-unauthorized**} | ポートの許可ステートの手動制御をイネーブルにします。 |
| **authentication timer** | **dot1x timeout** | 802.1x タイマーを設定します。 |
| **authentication violation** {**protect** \| **restrict** \| **shutdown**} | **dot1x violation-mode** {**shutdown** \| **restrict** \| **protect**} | 新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続された後に新しいデバイスがそのポートに接続された場合に発生する違反モードを設定します。 |

# 許可ステートおよび無許可ステートのポート

802.1x 認証中に、スイッチのポートステートによって、スイッチはネットワークへのクライアント アクセスを許可します。ポートは最初、無許可ステートです。このステートでは、音声 VLAN（仮想 LAN）ポートとして設定されていないポートは 802.1x 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは許可ステートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN ポートとして設定されている場合、VoIP トラフィックおよび 802.1x プロトコル パケットが許可された後クライアントが正常に認証されます。

（注） CDP バイパスはサポートされていないため、ポートが error-disabled ステートになる場合があります。

802.1x をサポートしていないクライアントが、無許可ステートの 802.1x ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x 対応のクライアントが、802.1x 標準が稼働していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

**authentication port-control** インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized**：802.1x 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized**：ポートが無許可ステートのままになり、クライアントからの認証の試みをすべて無視します。スイッチはポートを介してクライアントに認証サービスを提供できません。
- **auto**：802.1x 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更した際、または EAPOL-Start フレームを受信した際に、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、スイッチは要求を再送信します。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

ポートのリンク ステートがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信した場合に、ポートは無許可ステートに戻ります。

# ポートベース認証とスイッチ スタック

スイッチが、スイッチ スタックに追加されるか、スイッチ スタックから削除される場合、RADIUS サーバとスタックとの間の IP 接続が正常な場合、802.1x 認証は影響を受けません。これは、スタック マスターがスイッチスタックから削除される場合も、適用されます。スタック マスターに障害が発生した場合、スタック メンバは、選択プロセスを使用することによって新しいスタック マスターになり、802.1x 認証プロセスは通常どおり続行されます。

サーバに接続されていたスイッチが削除されたか、そのスイッチに障害が発生したために、RADIUS サーバへの IP 接続が中断された場合、これらのイベントが発生します。

- すでに認証済みで、定期的な再認証がイネーブルではないポートは、認証ステートのままです。RADIUS サーバとの通信は、必要ではありません。
- すでに認証済みで、（**dot1x re-authentication** グローバル コンフィギュレーション コマンドを使用）定期的な再認証がイネーブルにされているポートは、再認証の発生時に、認証プロセスに失敗します。ポートは、再認証プロセス中に、非認証ステートに戻ります。RADIUS サーバとの通信が必要です。

  進行中の認証については、サーバ接続が行われていないため、認証はただちに失敗します。

障害が発生したスイッチが実行状態になり、スイッチスタックに再加入した場合、ブートアップの時刻と、認証の試行時までにRADIUSサーバへの接続が再確立されたかどうかによって、認証は失敗する場合と、失敗しない場合があります。

RADIUSサーバへの接続を失うことを避けるには、冗長接続を設定する必要があります。たとえば、スタック マスターへの冗長接続と、スタック メンバへの別の接続を設定できます。スタック マスターに障害が発生した場合でも、スイッチ スタックは、RADIUS サーバに接続されたままです。

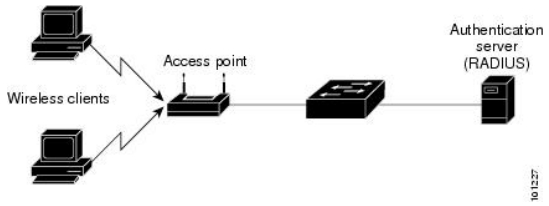
# 802.1X のホスト モード

802.1x ポートは、シングル ホスト モードまたはマルチ ホスト モードで設定できます。シングル ホスト モードでは、802.1x 対応のスイッチ ポートに接続できるのはクライアント 1 つだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチホストモードでは、複数のホストを単一の802.1x対応ポートに接続できます。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。

このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

図 *24 :* マルチ ホスト モードの例




（注） すべてのホスト モードで、ポートベース認証が設定されている場合、ライン プロトコルは許可の前にアップのままです。

スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチ ポートに接続できます。

# 802.1x マルチ認証モード

マルチ認証（multiauth）モードでは、データ VLAN および音声 VLAN で複数のクライアントを認証できます。各ホストは個別に認証されます。マルチ認証ポートで認証できるデータデバイスまたは音声デバイスの数には制限はありません。

ハブまたはアクセス ポイントが 802.1x 対応ポートに接続されている場合、接続されている各クライアントを認証する必要があります。802.1x 以外のデバイスでは、MAC 認証バイパスまたは Web 認証をホスト単位認証フォールバック メソッドとして使用し、単一のポートで異なる方法で異なるホストを認証できます。

（注） ポートがマルチ認証モードの場合、認証失敗 VLAN 機能はアクティブになりません。

次の条件で、RADIUS サーバから提供された VLAN をマルチ認証モードで割り当てることができます。

- ホストがポートで最初に許可されたホストであり、RADIUS サーバが VLAN 情報を提供している。
- 後続のホストが、動作 VLAN に一致する VLAN を使用して許可される。
- ホストは VLAN が割り当てられていないポートで許可され、後続のホストでは VLAN 割り当てが設定されていないか、VLAN 情報が動作 VLAN と一致している。
- ポートで最初に許可されたホストにはグループ VLAN が割り当てられ、後続のホストでは VLAN 割り当てが設定されていないか、グループ VLAN がポート上のグループ VLAN と一致している。後続のホストが、最初のホストと同じ VLAN グループの VLAN を使用する必要がある。VLAN リストが使用されている場合、すべてのホストは VLAN リストで指定された条件に従う。

- VLAN がポート上のホストに割り当てられると、後続のホストは一致する VLAN 情報を持つ必要があり、この情報がなければポートへのアクセスを拒否される。
- ゲスト VLAN または認証失敗 VLAN をマルチ認証モードに設定できない。
- クリティカル認証 VLAN の動作が、マルチ認証モード用に変更されない。ホストが認証を試みたときにサーバに到達できない場合、許可されたすべてのホストは、設定された VLAN で再初期化される。

## ユーザごとのマルチ認証 VLAN 割り当て

ユーザごとのマルチ認証 VLAN 割り当て機能を使用すると、単一の設定済みアクセス VLAN を持つポート上のクライアントに割り当てられた VLAN に基づいて複数の運用アクセス VLAN を作成することができます。データ ドメインに関連付けられたすべての VLAN に対するトラフィックが dot1q とタグ付けされていないアクセス ポートとして設定されているポートおよびこれらの VLAN は、ネイティブ VLAN として処理されます。

マルチ認証ポート 1 つあたりのホストの数は 8 ですが、さらに多くのホストが存在する場合があります。

次のシナリオは、ユーザごとのマルチ認証 VLAN 割り当てに関連しています。

**シナリオ 1**

ハブがアクセス ポートに接続されている場合、およびポートがアクセス VLAN（V0）で設定されている場合。

ホスト（H1）は、ハブを介して VLAN（V1）に割り当てられます。ポートの運用 VLAN は V1 に変更されます。この動作は、単一ホスト ポートまたはマルチ ドメイン認証ポートで同様です。

2 番目のホスト（H2）が接続され、VLAN（V2）に割り当てられる場合、ポートには 2 つの運用 VLAN があります（V1 および V2）。H1 と H2 がタグなし入力トラフィックを送信すると、H1 トラフィックは VLAN（V1）に、H2 トラフィックは VLAN（V2）にマッピングされ、VLAN（V1）および VLAN（V2）のポートからの出トラフィックはすべてタグなしになります。

両方のホスト H1 と H2 がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN（V1）と VLAN（V2）がポートから削除され、設定された VLAN（V0）がポートに復元されます。

**シナリオ 2**

ハブがアクセス ポートに接続されている場合、およびポートがアクセス VLAN（V0）で設定されている場合。ホスト（H1）は、ハブを介して VLAN（V1）に割り当てられます。ポートの運用 VLAN は V1 に変更されます。

2 番目のホスト（H2）が接続され明示的な VLAN ポリシーなしで承認されると、H2 はポート上で復元される設定済み VLAN（V0）を使用することを予期されます。2 つの運用 VLAN、VLAN（V0）および VLAN（V1）からの出トラフィックはすべてタグなしになります。

ホスト（H2）がログアウトするか、またはセッションがなんらかの理由で削除されると、設定されたVLAN（V0）がポートから削除され、VLAN（V1）がそのポートでの唯一の運用VLANになります。

**シナリオ 3**

ハブがオープン モードでアクセス ポートに接続されている場合、およびポートがアクセス VLAN（V0）で設定されている場合。

ホスト（H1）は、ハブを介してVLAN（V1）に割り当てられます。ポートの運用VLANはV1に変更されます。2 番目のホスト（H2）が接続され無許可のままだと、オープン モードにより、運用 VLAN（V1）に引き続きアクセスできます。

ホスト H1 がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN（V1）はポートから削除され、ホスト（H2）は VLAN（V0）に割り当てられます。

（注） オープン モードと VLAN 割り当ての組み合わせは、ホスト（H2）に悪影響を与えます。そのホストは VLAN（V1）に対応するサブネット内に IP アドレスを含んでいるからです。

## ユーザごとのマルチ認証 VLAN 割り当ての制限

ユーザごとのマルチ認証 VLAN 割り当て機能では、複数の VLAN からの出トラフィックは、ホストが自分宛てではないトラフィックを受信するポート上ではタグなしになります。これは、ブロードキャストおよびマルチキャスト トラフィックで問題になる可能性があります。

- **IPv4 ARP**：ホストは他のサブネットからの ARP パケットを受信します。これは、IP アドレス範囲が重複する異なる仮想ルーティングおよび転送（VRF）テーブルの 2 個のサブネットがポート上でアクティブな場合に問題となります。ホスト ARP キャッシュのエントリが無効になる可能性があります。

- **IPv6 制御パケット**：IPv6 の導入環境では、ルータ アドバタイズメント（RA）は、その受信を想定されていないホストによって処理されます。ある VLAN からのホストが別の VLAN からの RA を受信すると、ホストはそれ自身に間違った IPv6 アドレスを割り当てます。このようなホストは、ネットワークにアクセスできません。

  回避策は、IPv6 ファースト ホップ セキュリティをイネーブルにして、ブロードキャスト ICMPv6 パケットがユニキャストに変換され、マルチ認証がイネーブルのポートから送信されるようにすることです。パケットは VLAN に属するマルチ認証ポートの各クライアント用に複製され、宛先 MAC が個々のクライアントに設定されます。1 つの VLAN を持つポートで、ICMPv6 パケットは正常にブロードキャストされます。

- **IP マルチキャスト**：送信先のマルチキャスト グループへのマルチキャスト トラフィックは、異なる VLAN 上のホストがそのマルチキャスト グループに参加している場合それらの VLAN 用に複製されます。異なる VLAN の 2 つのホストが（同じマルチ認証ポート上の）マルチキャスト グループに参加している場合、各マルチキャスト パケットのコピー 2 部がそのポートから送信されます。

# MAC 移動

あるスイッチ ポートでMACアドレスが認証されると、そのアドレスは同じスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じ MAC アドレスを別の認証マネージャ対応ポートで検出すると、そのアドレスは許可されなくなります。

場合によっては、MAC アドレスを同じスイッチ上のポート間で移動する必要があります。たとえば、認証ホストとスイッチ ポート間に別のデバイス（ハブまたは IP Phone など）がある場合、ホストをデバイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC 移動をグローバルにイネーブルにできます。ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再認証されます。MAC 移動はすべてのホスト モードでサポートされます（認証ホストは、ポートでイネーブルにされているホストモードに関係なく、スイッチの任意のポートに移動できます）。MAC アドレスがあるポートから別のポートに移動すると、スイッチは元のポートで認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。MAC 移動の機能は、音声およびデータ ホストの両方に適用されます。

（注） オープン認証モードでは、MACアドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

# MAC 置換

MAC 置換機能は、ホストが、別のホストがすでに認証済みであるポートに接続しようとすると発生する違反に対処するように設定できます。

（注） 違反はマルチ認証モードでは発生しないため、マルチ認証モードのポートにこの機能は適用されません。マルチホストモードで認証が必要なのは最初のホストだけなので、この機能はこのモードのポートには適用されません。

**replace** キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、マルチドメインモードのポートでの認証プロセスは、次のようになります。

- 既存の認証済みMACアドレスを使用するポートで新しいMACアドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータ ホストの MAC アドレスを、新しい MAC アドレスで置き換えます。
- 認証マネージャは、新しい MAC アドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MACアドレスはただちにMACアドレステーブルに追加されます。

# 802.1x アカウンティング

802.1x標準では、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1xアカウンティングは、デフォルトでディセーブルです。802.1xアカウンティングをイネーブルにすると、次の処理を 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。
- 再認証が失敗します。

スイッチは802.1xアカウンティング情報を記録しません。その代わり、スイッチはこの情報をRADIUSサーバに送信します。RADIUSサーバは、アカウンティング メッセージを記録するように設定する必要があります。

# 802.1x アカウンティング属性値ペア

RADIUS サーバに送信された情報は、属性値（AV）ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます（たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性の情報が必要です）。

AV ペアは、802.1x アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START：新規ユーザ セッションが始まると送信されます。
- INTERIM：既存のセッションが更新されると送信されます。
- STOP：セッションが終了すると送信されます。

（注） RADIUS および AAA のデバッグのログを表示するには、**show platform software trace message smd** コマンドを使用します。詳細については、『*Command Reference Guide, Cisco IOS XE Denali 16.1.1*』のセクション「Tracing Commands」を参照してください。

次の表に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 *33*：アカウンティング *AV* ペア

| 属性番号 | AV ペア名 | START | INTERIM | STOP |
|---|---|---|---|---|
| 属性 [1] | User-Name | 常に（Always） | 常に（Always） | 常に（Always） |
| 属性 [4] | NAS-IP-Address | 常に（Always） | 常に（Always） | 常に（Always） |
| 属性 [5] | NAS-Port | 常に（Always） | 常に（Always） | 常に（Always） |
| 属性 [8] | Framed-IP-Address | 非送信 | 条件に応じて送信[15] | 条件に応じて送信 |
| 属性 [30] | Called-Station-ID | 常に（Always） | 常に（Always） | 常に（Always） |
| 属性 [31] | Calling-Station-ID | 常に（Always） | 常に（Always） | 常に（Always） |
| 属性 [40] | Acct-Status-Type | 常に（Always） | 常に（Always） | 常に（Always） |
| 属性 [41] | Acct-Delay-Time | 常に（Always） | 常に（Always） | 常に（Always） |
| 属性 [42] | Acct-Input-Octets | 非送信 | 常に（Always） | 常に（Always） |
| 属性 [43] | Acct-Output-Octets | 非送信 | 常に（Always） | 常に（Always） |
| 属性 [47] | Acct-Input-Packets | 非送信 | 常に（Always） | 常に（Always） |
| 属性 [48] | Acct-Output-Packets | 非送信 | 常に（Always） | 常に（Always） |
| 属性 [44] | Acct-Session-ID | 常に（Always） | 常に（Always） | 常に（Always） |
| 属性 [45] | Acct-Authentic | 常に（Always） | 常に（Always） | 常に（Always） |
| 属性 [46] | Acct-Session-Time | 非送信 | 常に（Always） | 常に（Always） |
| 属性 [49] | Acct-Terminate-Cause | 非送信 | 非送信 | 送信 |
| 属性 [61] | NAS-Port-Type | 常に（Always） | 常に（Always） | 常に（Always） |

[15] 有効な静的 IP アドレスが設定されているか、ホストに対する Dynamic Host Control Protocol（DHCP）バインディングが DHCP スヌーピング バインディング テーブルに存在している場合に、Framed-IP-Address の AV ペアが送信されます。

# 802.1x 準備状態チェック

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判

別できます。802.1x 機能をサポートしていないデバイスでは、MAC 認証バイパスまたは Web 認証などの代替認証を使用します。

この機能が有用なのは、クライアントのサプリカントで NOTIFY EAP 通知パケットでのクエリーがサポートされている場合だけです。クライアントは、802.1x タイムアウト値内に応答しなければなりません。

# スイッチと RADIUS サーバ間の通信

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

# VLAN 割り当てを使用した 802.1x 認証

スイッチは、VLAN 割り当てを使用した 802.1x 認証をサポートしています。ポートの 802.1x 認証が成功すると、RADIUS サーバは VLAN 割り当てを送信し、スイッチ ポートを設定します。RADIUS サーバデータベースは、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに接続するクライアントのユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

音声デバイス認証は、Cisco IOS Release 12.2(37)SE のマルチドメイン ホスト モードでサポートされています。Cisco IOS Release 12.2(40)SE 以降、音声デバイスが許可されており、RADIUS サーバが許可された VLAN を返した場合、割り当てられた音声 VLAN 上でパケットを送受信するようにポート上の音声 VLAN が設定されます。音声 VLAN 割り当ては、マルチドメイン認証（MDA）対応のポートでのデータ VLAN 割り当てと同じように機能します。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 802.1x 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1x 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN とは、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべて、この VLAN に所属します。

- 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

  設定エラーには、ルーテッド ポートの VLAN、間違った VLAN ID、存在しないまたは内部（ルーテッド ポート）の VLAN ID、RSPAN VLAN、シャットダウンしている VLAN、あるいは一時停止している VLAN ID の指定などがあります。マルチドメイン ホスト ポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行（またはその逆）のために発生するものもあります。

- 802.1x 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。
- 802.1x ポートでマルチ ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN（RADIUS サーバにより指定）に配置されます。
- ポート セキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
  - あるデバイスでVLAN設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みのVLANと一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みのVLANが一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
  - 音声デバイスが許可されて、ダウンロードされた音声VLANを使用している場合、音声VLAN設定を削除したり設定値をdot1pまたはuntaggedに修正したりすると、音声デバイスが未許可になり、マルチドメインホストモードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウンステートの場合、ポートは設定済みのアクセスVLANに配置されます。

802.1xポートが認証され、RADIUSサーバによって割り当てられたVLANに配置されると、そのポートのアクセスVLAN設定への変更は有効になりません。マルチドメインホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。

- あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済または割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
- 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウンステートの場合、ポートは設定済みのアクセスVLANに配置されます。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。（アクセスポートで 802.1x 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN 名または VLAN ID
  - [83] Tunnel-Preference

  属性 [64] は、値 *VLAN*（タイプ 13）でなければなりません。属性 [65] は、値*802*（タイプ 6）でなければなりません。属性 [81] は、IEEE 802.1x 認証ユーザに割り当てられた *VLAN* 名または *VLAN ID* を指定します。

# ユーザ単位 ACL を使用した 802.1x 認証

ユーザ単位アクセス コントロール リスト（ACL）をイネーブルにして、異なるレベルのネットワーク アクセスおよびサービスを 802.1x 認証ユーザに提供できます。RADIUS サーバは、802.1x ポートに接続されるユーザを認証する場合、ユーザ ID に基づいて ACL 属性を受け取り、これらをスイッチに送信します。スイッチは、ユーザ セッションの期間中、その属性を 802.1x ポートに適用します。セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザ単位 ACL 設定が削除されます。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションには保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

ユーザは同一のスイッチ上で、ルータ ACL および入力ポート ACL を使用できます。ただし、ポートの ACL はルータ ACL より優先されます。入力ポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力ルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド パケットは、ルータ ACL によってフィルタリングされます。発信するルーテッド パケットには、ルータ ACL のフィルタが適用されます。コンフィギュレーションの矛盾を回避するには、RADIUS サーバに保存するユーザ プロファイルを慎重に計画しなければなりません。

RADIUS は、ベンダー固有属性などのユーザ単位属性をサポートします。ベンダー固有属性（VSA）は、オクテット ストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では inacl#<*n*> で、出力方向では outacl#<*n*> です。MAC ACL は、入力方向に限りサポートされます。VSA は入力方向に限りサポートされます。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザ単位コンフィギュレーションを定義します。RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。属性には、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す *.in* または *.out* が含まれています。RADIUS サーバが *.in* または *.out* 構文を許可しない場合、アクセス リストはデフォルトで発信 ACL に適用されます。RADIUS サーバから送信された Filter-Id がデバイスで設定されていない場合、ユーザは未承認としてマークされます。スイッチでの Cisco IOS のアクセスリストに関するサポートが制限されているため、Filter-ID 属性は 1 ～ 199（IP 標準 ACL）および 1300 ～ 2699（IP 拡張 ACL）の範囲の IP ACL に対してだけサポートされます。

ユーザ単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズにより制限されます。

ユーザ単位の ACL を設定するには、次の前提条件を満たす必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- 802.1x ポートをシングル ホスト モードに設定します。

（注） ユーザ単位 ACL がサポートされるのはシングル ホスト モードだけです。

# ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証

ACL およびリダイレクト URL は、ホストの 802.1x 認証または MAC 認証バイパス中に、RADIUS サーバからスイッチにダウンロードできます。また、Web 認証中に ACL をダウンロードすることもできます。

（注） ダウンロード可能な ACL は *dACL* とも呼ばれます。

複数のホストが認証され、それらのホストがシングル ホスト モード、MDA モード、またはマルチ認証モードである場合、スイッチは ACL の送信元アドレスをホスト IP アドレスに変更します。

ACL およびリダイレクト URL は、802.1x 対応のポートに接続されるすべてのデバイスに適用できます。

ACL が 802.1x 認証中にダウンロードされない場合、スイッチは、ポートのスタティック デフォルト ACL をホストに適用します。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、スイッチは ACL を認証ポリシーの一部として電話にだけ適用します。

URL リダイレクト ACL の場合：

- 許可アクセス制御エントリ （ACE）ルールに一致するパケットは、AAA サーバに転送するために CPU に送信されます。
- 拒否 ACE ルールに一致するパケットは、スイッチを介して転送されます。
- 許可 ACE ルールにも拒否 ACE ルールにも一致しないパケットは、次の dACL によって処理されます。dACL がない場合、パケットは暗黙的拒否 ACL にヒットしてドロップされます。

## Cisco Secure ACS およびリダイレクト URL の属性と値のペア

スイッチはこれらの *cisco-av-pair* VSA を使用します。

- url-redirect は HTTP URL または HTTPS URL です。
- url-redirect-acl はスイッチ ACL 名または番号です。

スイッチは、CiscoSecure-defined-ACL 属性値ペアを使用して、エンド ポイントからの HTTP または HTTPS リクエストを代行受信します。スイッチは、クライアント Web ブラウザを指定されたリダイレクト アドレスに転送します。Cisco Secure ACS 上の url-redirect AV ペアには、Web ブラウザがリダイレクトされる URL が格納されます。url-redirect-acl 属性値ペアには、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号が含まれます。

（注）

- ACL の permit ACE と一致するトラフィックがリダイレクトされます。
- スイッチの URL リダイレクト ACL およびデフォルト ポート ACL を定義します。

リダイレクト URL が認証サーバのクライアントに設定される場合、接続されるクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

## Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア

Cisco Secure ACS で、RADIUS cisco-av-pair ベンダー固有属性（VSA）を使用して、CiscoSecure-Defined-ACL 属性と値（AV）ペアを設定できます。このペアは、#ACL#-IP-name-number 属性を使って、Cisco Secure ACS でダウンロード可能な ACL の名前を指定します。

- *name* は ACL の名前です。

- *number* はバージョン番号（たとえば 3f783768）です。

ダウンロード可能な ACL が認証サーバのクライアントに設定される場合、接続されるクライアント スイッチ ポートのデフォルト ポート ACL も設定する必要があります。

デフォルト ACL がスイッチで設定されている場合、Cisco Secure ACS がホスト アクセス ポリシーをスイッチに送信すると、スイッチは、スイッチ ポートに接続されるホストからのトラフィックにこのポリシーを適用します。ポリシーが適用されない場合、デフォルト ACL が適用されます。Cisco Secure ACS がダウンロード可能な ACL をスイッチに送信する場合、この ACL は、スイッチ ポートに設定されているデフォルト ACL より優先されます。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信し、デフォルト ACL が設定されていない場合、許可失敗が宣言されます。

# VLAN ID ベース MAC 認証

ダウンロード可能な VLAN ではなくスタティック VLAN ID に基づいてホストを認証する場合、VLAN ID ベース MAC 認証を使用できます。スタティック VLAN ポリシーがスイッチで設定されている場合、認証用の各ホストの MAC アドレスとともに、VLAN 情報が IAS（Microsoft）RADIUS サーバに送信されます。接続ポートに設定されている VLAN ID は MAC 認証に使用されます。VLAN ID ベース MAC 認証を IAS サーバで使用することで、ネットワークで一定数の VLAN を使用できます。

機能は、STP によってモニタおよび処理される VLAN の数も制限します。ネットワークは固定 VLAN として管理できます。

# ゲスト VLAN を使用した 802.1x 認証

スイッチ上の各 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます（802.1x クライアントのダウンロードなど）。これらのクライアントは 802.1x 認証用にシステムをアップグレードできる場合がありますが、一部のホスト（Windows 98 システムなど）は IEEE 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチはEAPOLパケット履歴を保持します。EAPOLパケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが IEEE 802.1x 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

スイッチが 802.1x 対応の音声デバイスを許可しようとしたが、AAA サーバが使用できない場合、許可は失敗します。ただし、EAPOLパケットの検出はEAPOL履歴に保存されます。この音声デバイスは、AAA サーバが使用可能になると許可されます。ただし、他のデバイスによ

るゲスト VLAN へのアクセスは許可されなくなります。この状況を防ぐには、次のいずれかのコマンド シーケンスを使用します。

- **authentication event no-response action authorize vlan** *vlan-id* インターフェイス コンフィギュレーション コマンドを入力し、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。

（注） インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1x 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに 802.1x 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、単一のホスト、複数のホスト、複数認証、またはマルチドメイン モードにおける 802.1x ポートでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

スイッチは *MAC* 認証バイパス をサポートします。MAC 認証バイパスが 802.1x ポートでイネーブルの場合、スイッチは、IEEE 802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。スイッチは、802.1x ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。

# 制限付き VLAN を使用した 802.1x 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチスタックまたはスイッチの各 IEEE 802.1x ポートに対して制限付き VLAN（認証失敗 *VLAN* と呼ばれることもあります）を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1x 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効なクレデンシャルを持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。

（注） 両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチポートがスパニングツリーのブロッキングステートから変わることができなくなります。制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。VLAN 内のポートは設定された間隔に従って再認証を試みます（デフォルトは 60 秒）。再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルにすることもできますが、ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しない限り、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の疑似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントによっては（Windows XP が稼働しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、すべてのホスト モードでの 802.1x ポート上、およびレイヤ 2 ポート上でサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

ダイナミック ARP インスペクション、DHCP スヌーピング、IP 送信元ガードなどの他のセキュリティ ポート機能は、制限付き VLAN に対して個別に設定できます。

# アクセス不能認証バイパスを使用した 802.1x 認証

スイッチが設定された RADIUS サーバに到達できず、新しいホストを認証できない場合、アクセス不能認証バイパス機能を使用します。この機能は、クリティカル認証または *AAA* 失敗ポリシーとも呼ばれます。これらのホストをクリティカルポートに接続するようにスイッチを設定できます。

新しいホストがクリティカルポートに接続しようとすると、そのホストはユーザ指定のアクセス VLAN、クリティカル *VLAN* に移動されます。管理者はこれらのホストに制限付き認証を付与します。

スイッチは、クリティカルポートに接続されているホストを認証しようとする場合、設定されている RADIUS サーバのステータスをチェックします。利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワークアクセスを許可して、ポートを認証ステートの特別なケースであるクリティカル認証ステートにします。

（注） クリティカル認証をインターフェイスで設定する場合は、クリティカル承認（クリティカル *vlan*）に使用する vlan をスイッチでアクティブにする必要があります。クリティカル *vlan* が非アクティブまたはダウンしていると、クリティカル認証セッションは非アクティブな vlan の有効化を試行し続け、繰り返し失敗します。これは大量のメモリ保持の原因となる可能性があります。

## 複数認証ポートのアクセス不能認証バイパスのサポート

ポートが任意のホスト モードで設定されていて、AAA サーバを使用できない場合、ポートはマルチホストモードに設定され、クリティカル VLAN に移動されます。マルチ認証（multiauth）ポートで、このアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan** *vlan-id* コマンドを使用します。新しいホストがクリティカル ポートに接続しようとすると、そのポートは再初期化され、接続されているすべてのホストがユーザ指定のアクセス VLAN に移動されます。

このコマンドは、すべてのホスト モードでサポートされます。

## アクセス不能認証バイパスの認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカルポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカルポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイム アウトとなり、スイッチは次の認証試行の間にクリティカルポートをクリティカル認証ステートとします。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、クリティカル VLAN から移動するように、クリティカルポートを設定できます。このように設定した場合、クリティカル認証ステートのすべてのクリティカル ポートは自動的に再認証されます。

## アクセス不能認証バイパス機能の相互作用

アクセス不能認証バイパスは、次の機能と相互に作用します。

- ゲスト VLAN：アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 8021.x ポートでイネーブルの場合、この機能は次のように相互に作用します。
  - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカルポートをRADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲストVLANが設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲストVLANが割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- 制限付き VLAN：ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- 802.1x アカウンティング：RADIUS サーバが使用できない場合、アカウンティングは影響を受けません。
- プライベート VLAN：プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声VLAN：アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer（RSPAN）：アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

スイッチ スタックで、次の動作が発生します。

- キープアライブ パケットを送信することによって、スタック マスターにより、RADIUS サーバのステータスがチェックされます。RADIUS サーバのステータスが変更されると、スタック マスターからスタック メンバへ、情報が送信されます。クリティカル ポートの再認証時に、スタック メンバにより、RADIUS サーバのステータスがチェックされます。
- 新しいスタック マスターが選択されると、スイッチ スタックと RADIUS サーバとの間のリンクが変更される可能性があり、新しいスタックにより、キープアライブ パケットがただちに送信され、RADIUS サーバのステータスがアップデートされます。サーバのステー

タスが *dead* から *alive* に変化すると、スイッチはクリティカル認証ステートの状態にあるすべてのスイッチ ポートを再認証します。

メンバがスタックに追加されると、スタック マスターからメンバへサーバ ステータスが送信されます。

# 802.1x クリティカル音声 VLAN

ポートに接続されている IP フォンが Cisco Identity Services Engine（ISE）によって認証される際、そのIPフォンは音声ドメインに参加します。ISEが到達不能である場合、スイッチはデバイスが音声デバイスなのかどうかを判断できません。サーバが使用できない場合、電話機は音声ネットワークにアクセスできないため、動作できません。

データ トラフィックの場合、アクセス不能認証バイパス（クリティカル認証）を設定し、サーバが使用できない場合にトラフィックがネイティブ VLAN を通過できるようにすることができます。RADIUS認証サーバが使用できず（ダウンしていて）、アクセスできない認証バイパスがイネーブルの場合、スイッチは、クライアントにネットワークのアクセスを許可し、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN でポートをクリティカル認証ステートにします。設定されたRADIUSサーバにスイッチが到達できず、新しいホストを認証できない場合、スイッチはこれらのホストをクリティカル ポートに接続します。クリティカル ポートに接続を試行している新しいホストは、ユーザ指定のアクセスVLAN（クリティカルVLAN）に移動され、制限付き認証を許可されます。

（注） クリティカル音声 VLAN のダイナミック割り当ては、ネストされたサービステンプレートではサポートされません。それによって、デバイスはループ内で VLAN を連続的に切り替えます。

**authentication event server dead action authorize voice** インターフェイス コンフィギュレーション コマンドを使用して、クリティカル音声 VLAN 機能を設定できます。ISE が応答しない場合、ポートはクリティカル認証モードになります。ホストからのトラフィックが音声 VLAN でタグ付けされると、接続デバイス（電話機）は、ポートに対して設定された音声 VLAN に配置されます。IP フォンは Cisco Discovery Protocol（シスコデバイス）や LLDP または DHCP を介して音声 VLAN ID を学習します。

**switchport voice vlan** *vlan-id* インターフェイス コンフィギュレーション コマンドを入力して、ポートの音声 VLAN を設定できます。

この機能は、マルチドメイン モードおよびマルチ認証ホスト モードでサポートされます。スイッチがシングルホスト モードまたはマルチホスト モードの場合にコマンドを入力できますが、デバイスがマルチドメインまたはマルチ認証ホストモードに変わらない限りコマンドは有効になりません。

# 802.1x ユーザ ディストリビューション

802.1x ユーザ ディストリビューションを設定すると、複数の異なる VLAN で同じグループ名のユーザのロード バランシングを行うことができます。

VLAN は、RADIUS サーバにより提供されるか、VLAN グループ名でスイッチ CLI を介して設定します。

- RADIUS サーバを設定して、ユーザの複数の VLAN 名を送信します。複数の VLAN 名は、ユーザへの応答の一部として送信できます。802.1x ユーザ ディストリビューションは、特定の VLAN のすべてのユーザを追跡し、許可されたユーザをユーザ数が最も少ない VLAN に移動することでロード バランシングを行います。
- RADIUS サーバを設定してユーザの VLAN グループ名を送信します。VLAN グループ名は、ユーザへの応答の一部として送信できます。スイッチ CLI を使用して設定した VLAN グループ名で、選択された VLAN グループ名を検索できます。VLAN グループ名が検出されると、この VLAN グループ名で対応する VLAN を検索して、ユーザ数が最も少ない VLAN が検出されます。ロード バランシングは、対応する許可済みユーザをその VLAN に移動することで行われます。

（注） RADIUS サーバは、VLAN-ID、VLAN 名または VLAN グループを任意に組み合わせて VLAN 情報を送信できます。

## 802.1x ユーザ ディストリビューションの設定時の注意事項

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされることを確認してください。
- 複数の VLAN を VLAN グループにマッピングできます。
- VLAN を追加または削除することで、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアする場合、VLAN の認証済みポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブ VLAN がグループにマッピングされても VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内で任意の VLAN の認証ステートであるポートまたはユーザはクリアされませんが、VLAN の VLAN グループへのマッピングはクリアされます。

# 音声 VLAN ポートを使用した IEEE 802.1x 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の 2 つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータ トラフィックを伝送する PVID。PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、IP Phone は IEEE 802.1x 認証とは独立して動作できます。

シングル ホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチ ホスト モードでは、サプリカントが PVID で認証された後、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチ ホスト モードがイネーブルの場合、サプリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで IEEE 802.1x 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

IEEE 802.1x 認証をスイッチ ポート上でイネーブルにすると、音声 VLAN でもあるアクセス ポート VLAN を設定できます。

IP 電話がシングル ホスト モードで 802.1x 対応のスイッチ ポートに接続されている場合、スイッチは認証を行わずに電話ネットワーク アクセスを承認します。ポートで Multidomain Authentication（MDA）を使用して、データ デバイスと IP フォンなどの音声デバイスの両方を認証することを推奨します。

（注） 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

# ポート セキュリティを使用した IEEE 802.1x 認証

通常、IEEE 802.1x がイネーブルの場合に、ポート セキュリティをイネーブルにすることは推奨されません。IEEE 802.1x ではポート単位（IP テレフォニーに MDA が設定されている場合は VLAN 単位）で単一の MAC アドレスが適用されるため、ポート セキュリティは冗長であり、場合によっては期待される IEEE 802.1x の動作と干渉することがあります。

# WoL 機能を使用した IEEE 802.1x 認証

IEEE 802.1x 認証の Wake-on-LAN（WoL）機能を使用すると、スイッチにマジック パケットと呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが IEEE 802.1x ポートを通じて接続され、ホストの電源がオフになると、IEEE 802.1x ポートは無許可になります。無許可になったポートはEAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした IEEE 802.1x 認証を使用している場合、スイッチはマジックパケットを含むトラフィックを無許可の IEEE 802.1x ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。

（注） PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

**authentication control-direction in** インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向として設定すると、ポートはスパニングツリーフォワーディングステートに変更されます。ポートは、ホストにパケットを送信できますが、受信はできません。

**authentication control-direction both** インターフェイス コンフィギュレーション コマンドを使用してポートを双方向として設定すると、ポートは、両方向でアクセスコントロールされます。ポートは、ホストとの間でパケットを送受信しません。

# MAC 認証バイパスを使用した IEEE 802.1x 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレスに基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された IEEE 802.1x ポートでこの機能をイネーブルにできます。

クライアントからのEAPOL応答の待機中にIEEE 802.1x認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が IEEE 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアントMACアドレスのデータベースがあります。スイッチは、IEEE 802.1x ポート上のクライアントを検出した後で、クライアントからのイーサネットパケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲストVLANが設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。このプロセスは、ほとんどのクライアントデバイスで動作します。ただし、代替のMACアドレス形式を使用しているクライアントでは動作しません。標準の形式とは異なる MAC アドレスを持つクライアントに対して MAB 認証をどのように実行するかや、RADIUS の設定のどこでユーザ名とパスワードが異なることが要求されるかを設定できます。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが 802.1x 対応サプリカントであることを確認し、（MAC 認証バイパス機能ではなく）802.1x 認証を使用してインターフェイスを認

証します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでにMAC認証バイパスを使用してポートを許可し、IEEE 802.1xサプリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生するときに、Termination-Action RADIUS 属性値が DEFAULT であるために前のセッションが終了した場合、スイッチはポートに設定されている認証または再認証手法を使用します。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、IEEE 802.1x を使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てられた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS 属性（Attribute[27]）、および Termination-Action RADIUS 属性（Attribute[29]）に基づいて行われるときに、Termination-Action RADIUS 属性（Attribute[29]）のアクションが *Initialize*（属性値は *DEFAULT*）である場合、MAC 認証バイパス セッションは終了し、再認証の間の接続は失われます。MAC 認証バイパス機能が IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。これらの AV ペアの詳細については、RFC 3580『IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- IEEE 802.1x 認証：802.1x 認証がポートでイネーブルの場合にのみ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：IEEE 802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ
- 音声 VLAN
- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。
- Network Edge Access Topology（NEAT）：MAB と NEAT は相互に排他的です。インターフェイス上で NEAT が有効の場合は、MAB を有効にすることはできません。また、インターフェイス上で MAB が有効の場合は、NEAT を有効にすることはできません。

Cisco IOS Release 12.2(55)SE 以降では、冗長 MAB システム メッセージのフィルタリングをサポートします。

# Network Admission Control レイヤ 2 IEEE 802.1x 検証

スイッチは、デバイスのネットワーク アクセスを許可する前にエンドポイント システムやクライアントのウイルス対策の状態またはポスチャを調べる Network Admission Control（NAC）

レイヤ 2 IEEE 802.1x 検証をサポートしています。NAC レイヤ 2 IEEE 802.1x 検証を使用すると、以下の作業を実行できます。

- Session-Timeout RADIUS 属性（属性 [27]）と Termination-Action RADIUS 属性（属性 [29]）を認証サーバからダウンロードします。
- Session-Timeout RADIUS 属性（属性 [27]）の値として再認証試行間の秒数を指定し、RADIUS サーバからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS 属性（属性[29]）を使用してクライアントを再認証する際のアクションを設定します。値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- VLAN の番号や名前、または VLAN グループ名のリストを Tunnel Group Private ID（属性 [81]）の値として設定し、VLAN の番号や名前、または VLAN グループ名のプリファレンスを Tunnel Preference（属性 [83]）の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID（属性 [81]）属性がリストから選択されます。
- NAC ポスチャトークンを表示します。これは、**show authentication** 特権 EXEC コマンドを使用して、クライアントのポスチャを示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 IEEE 802.1x 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があることを除いて、IEEE 802.1x ポートベース認証と似ています。

# 柔軟な認証の順序設定

柔軟な認証の順序設定を使用して、ポートが新しいホストを認証するときに使用する方法の順序を設定できます。The IEEE 802.1X の柔軟な認証機能では、以下の 3 つの認証方法をサポートしています。

- dot1X：IEEE 802.1X 認証はレイヤ 2 の認証方式です。
- mab：MAC 認証バイパスはレイヤ 2 の認証方式です。
- webauth：Web 認証はレイヤ 3 の認証方式です。

この機能を使用すると、各ポートでどの認証方式を使用するかを制御できます。また、そのポートの方式についてフェールオーバー順も制御できます。たとえば、MAC 認証バイパスおよび 802.1x は、プライマリまたはセカンダリ認証方法として使用し、Web 認証は、これらの認証のいずれか、または両方が失敗した場合のフォールバック方法として使用できます。

The IEEE 802.1X の柔軟な認証機能では、以下のホスト モードをサポートしています。

- multi-auth：マルチ認証では、音声 VLAN に 1 つの認証、データ VLAN に複数の認証を使用できます。
- multi-domain：マルチドメイン認証では、音声 VLAN に 1 つ、データ VLAN に 1 つ、計 2 つの認証を使用できます。

# Open1x 認証

Open1x 認証によって、デバイスが認証される前に、そのデバイスがポートにアクセスできるようになります。オープン認証が設定されている場合、新しいホストはポートに定義されているアクセス コントロール リスト（ACL）に基づいてトラフィックを渡します。ホストが認証されると、RADIUS サーバに設定されているポリシーがそのホストに適用されます。

オープン認証を次の状況で設定できます。

- シングル ホスト モードでのオープン認証：1 人のユーザだけが認証の前後にネットワークにアクセスできます。
- MDA モードでのオープン認証：音声ドメインの 1 人のユーザだけ、およびデータ ドメインの 1 人のユーザだけが許可されます。
- マルチ ホスト モードでのオープン認証：任意のホストがネットワークにアクセスできます。
- 複数認証モードでのオープン認証：MDA の場合と似ていますが、複数のホストを認証できます。

（注） オープン認証が設定されている場合は、他の認証制御よりも優先されます。これは、**authentication open** インターフェイス コンフィギュレーション コマンドを使用した場合、**authentication port-control** インターフェイス コンフィギュレーション コマンドに関係なく、ポートがホストにアクセス権を付与することを意味します。

# マルチドメイン認証

スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチ ポート上で認証できます。ポートはデータ ドメインと音声ドメインに分割されます。

（注） すべてのホスト モードで、ポートベース認証が設定されている場合、ライン プロトコルは許可の前にアップのままです。

MDA では、デバイス認証の順序が指定されません。ただし、最適な結果を得るには、MDA 対応のポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA のスイッチ ポートを設定する必要があります。

- ホスト モードがマルチドメインに設定されている場合、IP Phone の音声 VLAN を設定する必要があります。
- MDA 対応ポートでの音声 VLAN 割り当ては、Cisco IOS Release 12.2(40)SE 以降でサポートされています。
- 音声デバイスを認可するには、値を *device-traffic-class=voice* に設定した Cisco 属性値（AV）ペア属性を送信するように AAA サーバを設定する必要があります。この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応のポートのデータ デバイスだけに適用されます。許可に失敗した音声デバイスは、データ デバイスとして扱われます。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、errordisable になります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。他社製 IP Phone または音声デバイスはデータおよび音声 VLAN の両方に許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。音声デバイスが 音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポート セキュリティ MAC アドレス制限にカウントされません。
- MDA では、IEEE 802.1x 認証をサポートしていないデバイスへのスイッチ ポートの接続を許可するフォールバック メカニズムとして、MAC 認証バイパスを使用できます。
- データまたは音声デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスがデータ VLAN で検出された場合や、複数の音声デバイスが音声 VLAN で検出された場合、ポートは errdisable になります。
- ポートのホスト モードをシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変更すると、ポートでは許可されたデータ デバイスは許可されたままになります。ただし、ポートの音声 VLAN で許可されている Cisco IP Phone は自動的に削除されるので、そのポートでは再認証を行う必要があります。
- ゲスト VLAN や制限付き VLAN などのアクティブ フォールバック メカニズムは、ポートをシングル モードまたはマルチホスト モードからマルチドメイン モードに変更したあとでも設定されたままになります。
- ポートのホスト モードをマルチドメイン モードからシングル モードまたはマルチホスト モードに変更すると、許可されているすべてのデバイスがポートから削除されます。
- まずデータ ドメインを許可してゲスト VLAN に参加させる場合、IEEE 802.1x 非対応の音声デバイスは、音声 VLAN のパケットをタグ付けして、認証を開始する必要があります。

- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーを備えた、許可されたデバイスは、ポートの音声 VLAN とデータ VLAN の両方のトラフィックに影響を与えることがあります。このようなデバイスを使用する場合は、ポートでユーザ単位 ACL を適用するデバイスは 1 台だけにしてください。

## Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ

Network Edge Access Topology（NEAT）機能は、ワイヤリング クローゼット（会議室など）外の領域まで識別を拡張します。これにより、任意のタイプのデバイスをポートで認証できます。

- 802.1x スイッチ サプリカント：802.1x サプリカント機能を使用することで、別のスイッチのサプリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼット外にあり、トランク ポートを介してアップストリーム スイッチに接続される場合に役に立ちます。802.1x スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチで認証します。サプリカント スイッチが認証に成功すると、オーセンティケータ スイッチでポート モードがアクセスからトランクに変更されます。サプリカント スイッチでは、CISP を有効にするときに手動でトランクを設定する必要があります。
- アクセス VLAN は、オーセンティケータ スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

デフォルトでは、BPDU ガードが有効にされたオーセンティケータ スイッチにサプリカントのスイッチを接続する場合、オーセンティケータのポートはサプリカント スイッチが認証する前にスパニングツリー プロトコル（STP）のブリッジ プロトコル データ ユニット（BPDU）を受信した場合、errdisable 状態になる可能性があります。Cisco IOS Release 15.0(1) SE 以降では、認証中にサプリカントのポートから送信されるトラフィックを制御できます。**dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証が完了する前にオーセンティケータ ポートがシャットダウンすることがないように、認証中に一時的にサプリカントのポートをブロックします。認証に失敗すると、サプリカントのポートが開きます。**no dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証期間中にサプリカント ポートが開きます。これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドによりオーセンティケータのスイッチ ポートで有効になっている場合、サプリカント スイッチで **dot1x supplicant controlled transient** コマンドを使用することを強く推奨します。

（注） **spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用して、グローバルにオーセンティケータ スイッチで BPDU ガードを有効にした場合、**dot1x supplicant controlled transient** コマンドを入力すると、BPDU の違反が避けられなくなります。

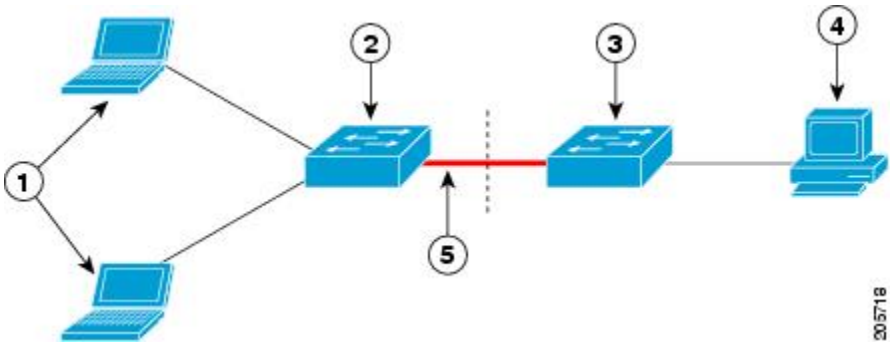
1 つ以上のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスでMDAまたはmultiauthモードをイネーブルにできます。マルチホストモードはオーセンティケータ スイッチ インターフェイスではサポートされていません。

インターフェイスで有効になっているシングルホスト モードでオーセンティケータ スイッチをリブートすると、インターフェイスが認証前にerr-disabled状態に移行する場合があります。err-disabled 状態から回復するには、オーセンティケータ ポートをフラップしてインターフェイスを再度アクティブにし、認証を開始します。

すべてのホストモードで機能するように **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを Network Edge Access Topology（NEAT）のサプリカントスイッチで使用します。

- ホスト許可：許可済み（サプリカントでスイッチに接続する）ホストからのトラフィックだけがネットワークで許可されます。これらのスイッチは、Client Information Signalling Protocol（CISP）を使用して、サプリカント スイッチに接続する MAC アドレスをオーセンティケータ スイッチに送信します。
- 自動有効化：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的に有効化します。これにより、サプリカントスイッチから着信する複数のVLANのユーザ トラフィックが許可されます。ISE で cisco-av-pair を *device-traffic-class=switch* として設定します（この設定は *group* または *user* 設定で行うことができます）。

**図 *25 : CISP* を使用したオーセンティケータまたはサプリカント スイッチ**




| | | | |
|---|---|---|---|
| 1 | ワークステーション（クライアント） | 2 | サプリカントスイッチ（ワイヤリングクローゼット外） |
| 3 | オーセンティケータ スイッチ | 4 | Cisco ISE |
| 5 | トランク ポート | | |

（注） **switchport nonegotiate** コマンドは、NEAT を使用したサプリカントおよびオーセンティケータスイッチではサポートされません。このコマンドは、トポロジのサプリカント側で設定しないでください。オーセンティケータ サーバ側で設定した場合は、内部マクロによってポートからこのコマンドが自動的に削除されます。

# 音声認識 802.1x セキュリティ

（注） 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにするようにスイッチを設定します。以前のリリースでは、セキュリティ違反の原因であるデータ クライアントを認証しようとすると、ポート全体がシャットダウンし、接続が完全に切断されます。

この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

# コモン セッション ID

認証マネージャは、使用された認証方式が何であれ、クライアントの単一のセッション ID（共通セッション ID）を使用します。この ID は、表示コマンドや MIB などのすべてのレポートに使用されます。セッション ID は、セッション単位のすべての Syslog メッセージに表示されます。

セッション ID には、次の情報が含まれます。

- ネットワーク アクセス デバイス（NAD）の IP アドレス
- 一意の 32 ビット整数（機械的に増加します）
- セッション開始タイム スタンプ（32 ビット整数）

次に、show authentication コマンドの出力に表示されたセッション ID の例を示します。この例では、セッション ID は 160000050000000B288508E5 です。

```
デバイス# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

次に、Syslog 出力にセッション ID が表示される例を示します。この例でも、セッション ID は 160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

セッションIDは、NAD、AAAサーバ、その他のレポート分析アプリケーションでクライアントを識別するために使用されます。ID は自動的に表示されます。設定は必要ありません。

# 802.1x ポートベース認証の設定方法

## 802.1x 認証のデフォルト設定

表 *34 : 802.1x* 認証のデフォルト設定

| 機能 | デフォルト設定 |
|---|---|
| スイッチの 802.1x イネーブル ステート | ディセーブル |
| ポート単位の 802.1x イネーブル ステート | ディセーブル（force-authorized）<br>ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。 |
| AAA | ディセーブル |
| RADIUS サーバ<br>• IP アドレス<br>• UDP 認証ポート<br>• デフォルトのアカウンティング ポート<br>• キー | • 指定なし<br>• 1645<br>• 1646<br>• 指定なし |
| ホスト モード | シングル ホスト モード |
| 制御方向 | 双方向制御 |
| 定期的な再認証 | ディセーブル |
| 再認証の間隔（秒） | 3600 秒 |
| 再認証回数 | 2回（ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数） |

| 機能 | デフォルト設定 |
|---|---|
| 待機時間 | 60 秒（スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数） |
| 再送信時間 | 30 秒（スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数） |
| 最大再送信回数 | 2 回（スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数） |
| クライアント タイムアウト時間 | 30 秒（認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間） |
| 認証サーバ タイムアウト時間 | 30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間）<br>dot1x timeout server-timeout インターフェイス コンフィギュレーションコマンドを使用して、このタイムアウト時間を変更できます。 |
| 無活動タイムアウト | ディセーブル |
| ゲスト VLAN | 指定なし |
| アクセス不能認証バイパス | ディセーブル |
| 制限付き VLAN | 指定なし |
| オーセンティケータ（スイッチ）モード | 指定なし |
| MAC 認証バイパス | ディセーブル |
| 音声認識セキュリティ | ディセーブル |

# 802.1x 認証設定時の注意事項

## 802.1X 認証

802.1x 認証を設定する場合の注意事項は、次のとおりです。

- 802.1x 認証を使用するには、SISF ベースのデバイストラッキングを有効にする必要があります。デフォルトでは、SISF ベースのデバイス トラッキングはスイッチで無効になっています。

- 802.1x 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当ててられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

  802.1x ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除された後、ポートは無許可になります。
- 802.1x プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポート タイプではサポートされません。
  - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。
  - スイッチド ポート アナライザ（SPAN）およびリモート SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートの 802.1x 認証をイネーブルにすることができます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1x 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは 802.1x 認証をイネーブルにすることができます。
- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x 認証をグローバルにイネーブルにする前に、802.1x 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- Cisco IOS Release 12.2(55)SE 以降のリリースでは、802.1x 認証に関連するシステム メッセージのフィルタリングがサポートされています。

## VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、およびアクセス不能認証バイパス設定時の注意事項は、次のとおりです。

- 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。

- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。
- DHCP クライアントが接続されている 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1x 認証プロセスを再起動する設定を変更できます。802.1x 認証プロセスの設定を減らします（**authentication timer inactivity** および **authentication timer reauthentication** インターフェイス コンフィギュレーション コマンド）。設定の減少量は、接続された 802.1x クライアントのタイプによって異なります。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
  - この機能はシングル ホスト モードおよびマルチホスト モードの 802.1x ポートでサポートされます。
  - Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステートの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
  - Windows XP クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。
  - アクセス不能認証バイパス機能および制限 VLAN を 802.1x ポート上に設定できます。スイッチが制限付き VLAN 内でクリティカル ポートを再認証しようとし、すべての RADIUS サーバが利用不可能な場合、スイッチはポート ステートをクリティカル認証ステートに変更し、制限付き VLAN に残ります。
  - CTS リンクがクリティカル認証モードである場合にマスターがリロードすると、SGT をデバイスに設定したポリシーは新しいマスターでは使用できません。これは、内部バインドが 3750-X スイッチ スタックのスタンバイ スイッチと同期しないためです。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。
- ワイヤレス ゲスト クライアントが固定クライアント VLAN の代わりに外部クライアント VLAN から IP を取得する際には、クライアントに新しい DHCP 要求の発行を求めるために、WLAN 設定で **ip dhcp required** コマンドを使用する必要があります。これは、クライアントがアンカーで正しくない IP を取得することを防止します。
- Cisco WLC（外部の）のリロード後に、有線ゲスト クライアントが IP アドレスの取得に失敗した場合は、クライアントによって使用されているポートで shut/no shut を実行して再接続します。

## MAC 認証バイパス

MAC 認証バイパス設定時の注意事項は次のとおりです。

- 特に明記していないかぎり、MAC 認証バイパスの注意事項は 802.1x 認証のものと同じです。
- ポートが MAC アドレスで許可された後に、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバデータベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。
- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を設定できます。指定できる範囲は 1 ～ 65535 秒です。

## ポートあたりのデバイスの最大数

802.1x 対応のポートに接続できるデバイスの最大数です。

- シングル ホスト モードの場合、アクセス VLAN で接続できるデバイスは 1 台だけです。ポートが音声 VLAN でも設定されている場合、音声 VLAN を介して送受信できる Cisco IP Phone の数には制限はありません。
- マルチドメイン認証（MDA）モードの場合、アクセス VLAN で 1 台のデバイス、音声 VLAN で 1 台の IP Phone が許可されます。
- マルチホストモードでは、1 つの 802.1x サプリカントだけがポートで許可されますが、非 802.1x ホストは数に制限なく、アクセス VLAN で許可されます。音声 VLAN で許可されるデバイスの数には制限はありません。

# 802.1x 準備状態チェックの設定

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。

802.1x 準備状態チェックは、802.1x で設定できるすべてのポートで使用できます。準備状態チェックは、**dot1x force-unauthorized** として設定されるポートでは使用できません。

802.1x 準備状態チェックをスイッチでイネーブルにする場合には、次の手順に従ってください。

### 始める前に

準備状態チェックをスイッチでイネーブルにする場合、次の注意事項に従ってください。

- 準備状態チェックは通常、802.1x がスイッチでイネーブルにされる前に使用されます。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用すると、スイッチ スタックのすべてのポートがテストされます。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x 対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。Syslog メッセージは生成されません。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x 対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。Syslog メッセージは生成されません。
- 準備状態チェックは、複数のホスト（たとえば、IP Phone に接続される PC）を扱うポートに送信できます。Syslog メッセージは、タイマー時間内に準備状態チェックに応答する各クライアントに生成されます。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **dot1x test eapol-capable** [ **interface** *interface-id*]<br>例：<br>デバイス# **dot1x test eapol-capable interface gigabitethernet1/0/13**<br>DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on | スイッチ上で 802.1x 準備状態チェックをイネーブルにします。<br>（任意）*interface-id* では、IEEE 802.1x の準備状態をチェックするポートを指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `gigabitethernet1/0/13 is EAPOL capable` | （注） オプションの **interface** キーワードを省略した場合、スイッチのすべてのインターフェイスがテストされます。 |
| ステップ 4 | **dot1x test timeout** *timeout* | （任意）EAPOL 応答の待機に使用するタイムアウトを設定します。範囲は1～65535秒です。デフォルトは10秒です。 |
| ステップ 5 | **end**<br>例：<br>`デバイス(config)# end` | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config**<br>例：<br>`デバイス# show running-config` | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>`デバイス# copy running-config startup-config` | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# 音声認識 802.1x セキュリティの設定

（注） 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能をスイッチで使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにします。この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

スイッチで音声認識 802.1x 音声セキュリティを設定する場合、次の注意事項に従ってください。

- 音声認識 802.1x セキュリティをイネーブルにするには、**errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力します。音声認識 802.1x セキュリティをディセーブルにするには、このコマンドの **no** バージョンを入力します。このコマンドは、スイッチの 802.1x 設定ポートのすべてに適用されます。

（注） **shutdown vlan** キーワードを指定しない場合、error-disabled ステートになった際にポート全体がシャットダウンされます。

- **errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して、error-disabled リカバリを設定すると、ポートは自動的に再びイネーブルにされます。error-disabled リカバリがポートで設定されていない場合、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。
- 個々の VLAN を再びイネーブルにするには、**clear errdisable interface** *interface-id* **vlan** [*vlan-list*] 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルにされます。

音声認識 802.1x セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| **ステップ 2** | **errdisable detect cause security-violation shutdown vlan** | セキュリティ違反エラーが発生したすべての VLAN をシャットダウンします。<br>（注） **shutdown vlan** キーワードを指定しない場合、すべてのポートが errdisable ステートになり、シャットダウンされます。 |
| **ステップ 3** | **errdisable recovery cause security-violation** | グローバル コンフィギュレーション モードを開始します。 |
| **ステップ 4** | **clear errdisable interface***interface-id* **vlan** *[vlan-list]* | （任意）errordisable になっている個々の VLAN を再びイネーブルにします。<br>• interface-id の場合、個々の VLAN を再びイネーブルにするポートを指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • （任意）vlan-list の場合、再びイネーブルにする VLAN のリストを指定します。vlan-list を指定しない場合は、すべての VLAN が再びイネーブルになります。 |
| ステップ 5 | 次を入力します。<br>• **shutdown**<br>• **no shutdown** | （任意）errordisable の VLAN を再びイネーブルにして、すべての errordisable 指示をクリアします。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show errdisable detect** | 入力内容を確認します。 |

例

次に、セキュリティ違反エラーが発生した任意の VLAN をシャットダウンするようにスイッチを設定する例を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次に、ポート ギガビット イーサネット 40/2 で errdisable ステートであったすべての VLAN を再度イネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet40/2
vlan
```

**show errdisable detect** 特権 EXEC コマンドを入力すると、設定を確認できます。

# 802.1x 違反モードの設定

次に示す状況で、シャットダウン、Syslog エラーを生成、または新しいデバイスからのパケットを廃棄するように 802.1x ポートを設定できます。

- デバイスが 802.1x 対応のポートに接続した
- ポートで認証されるデバイスの最大数に達した

スイッチ上にセキュリティ違反アクションを設定するには、特権 EXEC モードで次の手順を実行します。

手順

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

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **configure terminal** | |
| ステップ 2 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 3 | **aaa authentication dot1x**{ **default** } *method1*<br>例：<br>デバイス(config)# **aaa authentication dot1x default group radius** | 802.1x 認証方式リストを作成します。<br>**authentication** コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。<br>*method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。 |
| ステップ 4 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet1/0/4** | IEEE 802.1x 認証を有効にするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 5 | **switchport mode access**<br>例：<br>デバイス(config-if)# **switchport mode access** | ポートをアクセスモードに設定します。 |
| ステップ 6 | **authentication violation** {**shutdown** \| **restrict** \| **protect** \| **replace**}<br>例：<br>デバイス(config-if)# **authentication violation restrict** | 違反モードを設定します。キーワードの意味は次のとおりです。<br>• **shutdown**：エラーによってポートがディセーブルになります。<br>• **restrict**：Syslog エラーを生成します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • **protect**：トラフィックをポートに送信するすべての新しいデバイスからパケットをドロップします。<br>• **replace**：現在のセッションを削除し、新しいホストで認証します。 |
| ステップ 7 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |

# 802.1X 認証の設定

ユーザ単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1x の AAA プロセスを示します。

### 始める前に

802.1x ポートベース認証を設定するには、認証、許可、アカウンティング（AAA）をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | ユーザがスイッチのポートに接続します。 | |
| ステップ 2 | 認証が実行されます。 | |
| ステップ 3 | RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。 | |
| ステップ 4 | スイッチが開始メッセージをアカウンティング サーバに送信します。 | |
| ステップ 5 | 必要に応じて、再認証が実行されます。 | |
| ステップ 6 | スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバに送信します。 | |
| ステップ 7 | ユーザがポートから切断します。 | |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 8 | スイッチが停止メッセージをアカウンティング サーバに送信します。 | |

# 802.1x ポートベース認証の設定

802.1x ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 3 | **aaa authentication dot1x**{ **default** } *method1*<br>例：<br>デバイス(config)# **aaa authentication dot1x default group radius** | 802.1x 認証方式リストを作成します。<br>**authentication** コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。<br>*method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。<br>（注） コマンドラインのヘルプストリングには他のキーワードも表示されますが、サポートされるのは **group radius** キーワードのみです。 |
| ステップ 4 | **dot1x system-auth-control**<br>例： | スイッチで 802.1x 認証をグローバルに有効にします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config)# **dot1x system-auth-control** | |
| ステップ 5 | **aaa authorization network** {**default**} **group radius**<br>例：<br>デバイス(config)# **aaa authorization network default group radius** | （任意）ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。 |
| ステップ 6 | **radius server** *server name*<br>例：<br>デバイス(config)# **radius server rsim address ipv4 124.2.2.12** | （任意）RADIUS サーバの IP アドレスを指定します。 |
| ステップ 7 | **address** {**ipv4** \| **ipv6**} *ip address*<br>例：<br>デバイス(config-radius-server)# **address ipv4 10.0.1.12** | RADIUS サーバの IP アドレスを設定します。 |
| ステップ 8 | **key** *string*<br>例：<br>デバイス(config-radius-server)# **key rad123** | （任意）RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 |
| ステップ 9 | **exit**<br>例：<br>デバイス(config-radius-server)# **exit** | RADIUS サーバモードを終了して、グローバル コンフィギュレーション モードを開始します。 |
| ステップ 10 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet1/0/2** | IEEE 802.1x 認証を有効にするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 11 | **switchport mode access**<br>例： | （任意）ステップ 6 および 7 で RADIUS サーバを設定した場合のみ、 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if)# **switchport mode access** | ポートをアクセス モードに設定します。 |
| ステップ 12 | **authentication port-control auto**<br>例：<br>デバイス(config-if)# **authentication port-control auto** | ポートでの 802.1x 認証を有効にします。 |
| ステップ 13 | **dot1x pae authenticator**<br>例：<br>デバイス(config-if)# **dot1x pae authenticator** | インターフェイスのポートアクセスエンティティを、オーセンティケータとしてのみ動作し、サプリカント用のメッセージは無視するように設定します。 |
| ステップ 14 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |

# スイッチと RADIUS サーバ間の通信の設定

すべてのRADIUSサーバについて、タイムアウト、再送信回数、および暗号キー値をグローバルに設定するには、**radius server** グローバル コンフィギュレーション コマンドを使用します。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **key** *string* グローバル コンフィギュレーション コマンドを使用します。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

スイッチでRADIUSサーバのパラメータを設定するには、次の手順を実行します。この手順は必須です。

### 始める前に

認証、許可、およびアカウンティング（AAA）をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **radius server** *server name*<br>例：<br>デバイス(config)# **radius server rsim** | RADIUS サーバの名前を指定し、RADIUS サーバ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **address** {**ipv4** \| **ipv6**} *ip address* **auth-port** *port number* **acct-port** *port number*<br>例：<br>デバイス(config-radius-server)# **address ipv4 124.2.2.12** | RADIUS サーバの IP アドレスを指定します。<br>**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1645 です。指定できる範囲は 0 ～ 65536 です。<br>**acct-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1646 です。 |
| ステップ 5 | **key** *string*<br>例：<br>デバイス(config-radius-server)# **key rad123** | デバイスと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。必ず **radius server** コマンドの最終項目としてキーを設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 |
| ステップ 6 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

# ホスト モードの設定

**authentication port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されている IEEE 802.1x 許可ポート上で、複数のホスト（クライアント）を許可するには、特権 EXEC モードで次の手順を実行します。マルチドメイン認証（MDA）を設定してイネーブルにするには、**multi-domain** キーワードを使用します。これにより、ホストデバイス、および IP Phone（シスコ製または他社製）など音声デバイスの両方が同じスイッチポートで許可されます。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface** | 複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `gigabitethernet2/0/1` | |
| ステップ 3 | **authentication host-mode**[**multi-auth** \|**multi-domain** \|**multi-host** \|**single-host**]<br>例：<br>デバイス(config-if)# **authentication host-mode multi-host** | 単一の 802.1x 許可ポートで複数のホスト（クライアント）を許可することができます。<br>キーワードの意味は次のとおりです。<br>• **multi-auth**：音声 VLAN とデータ VLAN の両方で複数の認証クライアントを許可します。<br>（注） **multi-auth** キーワードは、**authentication host-mode** コマンドでのみ使用できます。<br>• **multi-host**：シングル ホストの認証後に 802.1x 許可ポートで複数のホスト（クライアント）の接続を許可します。<br>• **multi-domain**：ホスト デバイスと IP Phone（シスコ製または他社製）など音声デバイスの両方が、IEEE 802.1x 許可ポートで認証されるようにします。<br>（注） ホストモードが **multi-domain** に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。<br>指定のインターフェイスに対し **authentication port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |

# 定期的な再認証の設定

802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証を行う間隔（秒）を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet2/0/1** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **authentication periodic**<br>例：<br>デバイス(config-if)# **authentication periodic** | クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。<br>（注） デフォルト値は3600秒です。再認証タイマーの値を変更するか、スイッチに RADIUS-provided セッション タイムアウトを使用させるには、**authentication timer reauthenticate** コマンドを入力します。 |
| ステップ 4 | **authentication timer** {{[**inactivity** \| **reauthenticate** \| **restart** \| **unauthorized**]} {*value*}}<br>例：<br>デバイス(config-if)# **authentication timer reauthenticate 180** | 再認証の試行の間隔（秒）を設定します。<br>**authentication timer** キーワードの意味は次のとおりです。<br>• **inactivity**：クライアントからのアクティビティがなくなり無許可になるまでの間隔（秒） |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • **reauthenticate**：自動再認証試行が開始されるまでの時間（秒）<br>• **restart** *value*：無許可ポートの認証の試行が行われるまでの間隔（秒）<br>• **unauthorized** *value*：不正セッションが削除されるまでの間隔（秒）<br><br>このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。 |
| ステップ 5 | **end**<br>例：<br>`デバイス(config-if)# end` | 特権 EXEC モードに戻ります。 |

# 待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。**authentication timer restart** インターフェイス コンフィギュレーション コマンドは、アイドル状態の期間を制御します。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、特権EXECモードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`デバイス# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>`デバイス(config)# interface gigabitethernet2/0/1` | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **authentication timer restart** *seconds*<br>例：<br>デバイス(config-if)# **authentication timer restart 30** | クライアントとの認証のやり取りに失敗した場合に、スイッチが待機状態のままでいる秒数を設定します。<br>指定できる範囲は1～65535秒です。デフォルトは60秒です。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show authentication sessions interface** *interface-id*<br>例：<br>デバイス# **show authentication sessions interface gigabitethernet2/0/1** | 入力を確認します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。スイッチがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、その後フレームを再送信します。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチがクライアントからの通知を待機する時間を変更するには、特権EXECモードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet2/0/1** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **authentication timer reauthenticate** *seconds*<br>例：<br>デバイス(config-if)# **authentication timer reauthenticate 60** | スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。<br>指定できる範囲は 1 ～ 65535 秒です。デフォルトは 5 秒です。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show authentication sessions interface** *interface-id*<br>例：<br>デバイス# **show authentication sessions interface gigabitethernet2/0/1** | 入力を確認します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# スイッチからクライアントへのフレーム再送信回数の設定

スイッチからクライアントへの再送信時間を変更できるだけでなく、（クライアントから応答が得られなかった場合に）スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチからクライアントへのフレーム再送信回数を設定するには、特権EXECモードで次の手順を実行します。この手順は任意です。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **configure terminal**<br>例：<br>`デバイス# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| **ステップ 2** | **interface** *interface-id*<br>例：<br>`デバイス(config)# interface gigabitethernet2/0/1` | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| **ステップ 3** | **dot1x max-reauth-req** *count*<br>例：<br>`デバイス(config-if)# dot1x max-reauth-req 5` | スイッチが認証処理を再開するまでに、クライアントへ EAP 要求/アイデンティティ フレームを送信する回数を変更できます。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。 |
| **ステップ 4** | **end**<br>例：<br>`デバイス(config-if)# end` | 特権 EXEC モードに戻ります。 |

# 再認証回数の設定

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス# **interface gigabitethernet2/0/1** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **switchport mode access**<br>例：<br>デバイス(config-if)# **switchport mode access** | RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。 |
| ステップ 4 | **dot1x max-req** *count*<br>例：<br>デバイス(config-if)# **dot1x max-req 4** | ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ～ 10 です。デフォルトは 2 です。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |

# MAC 移動のイネーブル化

MAC 移動を使用すると、認証されたホストをスイッチのポート間で移動できます。

スイッチで MAC 移動をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **authentication mac-move permit**<br>例：<br>デバイス(config)# **authentication mac-move permit** | スイッチでMAC移動をイネーブルにします。デフォルトは deny です。<br>セッション認識型ネットワーク モードでは、デフォルト CLI は **access-session mac-move deny** です。セッション認識型ネットワークでMAC移動をイネーブルにするには、**no access-session mac-move** グローバル コンフィギュレーション コマンドを使用します。<br>**mac-move** のデフォルト値は、レガシーモード（IBNS 1.0）の場合は **deny** で、C3PL モード（IBNS 2.0）の場合は **permit**です。 |
| ステップ 3 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 5 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | **startup-config** | |

# MAC 置換のイネーブル化

MAC 置換を使用すると、ホストはポート上の認証ホストを置換できます。

インターフェイス上で MAC 置換をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet2/0/2** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **authentication violation** {**protect** \| **replace** \| **restrict** \| **shutdown**}<br>例：<br>デバイス(config-if)# **authentication violation replace** | インターフェイス上で MAC 置換をイネーブルにするには、**replace** キーワードを使用します。ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。<br>他のキーワードは、次のような機能があります。<br>• **protect**：ポートは、システム メッセージを生成せずに、予期しない MAC を使用するパケットをドロップします。<br>• **restrict**：違反パケットが CPU によってドロップされ、システムメッセージが生成されます。<br>• **shutdown**：ポートは、予期しない MAC アドレスを受信すると error disabled になります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# 802.1x アカウンティングの設定

802.1xアカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、ロギングのためにシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバは、アクティブな 802.1x セッションすべてが終了したものと判断します。

（注） Cisco IOS XE Denali 16.3.x および Cisco IOS XE Everest 16.6.x では、定期的な AAA アカウンティングのアップデートはサポートされていません。スイッチは、定期的中間アカウンティングレコードをアカウンティングサーバに送信しません。定期的な AAA アカウンティングのアップデートは、Cisco IOS XE Fuji 16.9.x 以降のリリースで利用できます。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップ メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

（注） ロギングの開始、停止、仮のアップデート メッセージ、タイム スタンプなどのアカウンティング タスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになった後、802.1x アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet1/0/3** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa accounting dot1x default start-stop group radius**<br>例：<br>デバイス(config-if)# **aaa accounting dot1x default start-stop group radius** | すべての RADIUS サーバのリストを使用して 802.1x アカウンティングをイネーブルにします。 |
| ステップ 4 | **aaa accounting system default start-stop group radius**<br>例：<br>デバイス(config-if)# **aaa accounting system default start-stop group radius** | （任意）システム アカウンティングをイネーブルにし（すべての RADIUS サーバのリストを使用）、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。 |
| ステップ 5 | **end**<br>例： | 特権 EXEC モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if)# **end** | |
| ステップ 6 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 7 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1x 対応でないクライアントはゲスト VLAN に配置されます。802.1x 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングル ホスト モードまたはマルチ ホスト モードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 2/0/2** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | 次のいずれかを使用します。<br>• **switchport mode access**<br>• **switchport mode private-vlan host** | • ポートをアクセス モードに設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | 例：<br>デバイス(config-if)# **switchport mode private-vlan host** | • レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。 |
| ステップ 4 | **authentication event no-response action authorize vlan** *vlan-id*<br>例：<br>デバイス(config-if)# **authentication event no-response action authorize vlan 2** | アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。<br>内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |

# 制限付き VLAN の設定

スイッチスタックまたはスイッチ上に制限付き VLAN を設定している場合、認証サーバが有効なユーザ名またはパスワードを受信できないと、IEEE 802.1x に準拠しているクライアントは制限付き VLAN に移されます。スイッチは、シングル ホスト モードでのみ制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 2/0/2** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | 次のいずれかを使用します。<br>• **switchport mode access**<br>• **switchport mode private-vlan host**<br>例：<br>`デバイス(config-if)# switchport mode access` | • ポートをアクセス モードに設定します。<br>• レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。 |
| ステップ 4 | **authentication port-control auto**<br>例：<br>`デバイス(config-if)# authentication port-control auto` | ポートでの 802.1x 認証をイネーブルにします。 |
| ステップ 5 | **authentication event fail action authorize vlan** *vlan-id*<br>例：<br>`デバイス(config-if)# authentication event fail action authorize vlan 2` | アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。<br>内部 VLAN（ルーテッド ポート）、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。 |
| ステップ 6 | **end**<br>例：<br>`デバイス(config-if)# end` | 特権 EXEC モードに戻ります。 |

## 制限付き VLAN の認証試行回数の設定

ユーザに制限付き VLAN を割り当てる前に、**authentication event retry** *retry count* インターフェイス コンフィギュレーション コマンドを使用して、認証試行回数を最大に設定できます。指定できる試行回数は 1 ～ 3 です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、特権EXECモードで次の手順を実行します。この手順は任意です。

### 手順

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

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **configure terminal** | |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 2/0/3** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | 次のいずれかを使用します。<br>• **switchport mode access**<br>• **switchport mode private-vlan host**<br>例：<br>または<br>デバイス(config-if)# **switchport mode access** | • ポートをアクセス モードに設定します。<br>• レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。 |
| ステップ 4 | **authentication port-control auto**<br>例：<br>デバイス(config-if)# **authentication port-control auto** | ポートでの 802.1x 認証をイネーブルにします。 |
| ステップ 5 | **authentication event fail action authorize vlan** *vlan-id*<br>例：<br>デバイス(config-if)# **authentication event fail action authorize vlan 8** | アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。<br>内部 VLAN（ルーテッド ポート）、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。 |
| ステップ 6 | **authentication event retry** 再試行回数<br>例：<br>デバイス(config-if)# **authentication event retry 2** | ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は 1 ～ 3 秒です。デフォルトは 3 回に設定されています。 |
| ステップ 7 | **end**<br>例： | 特権 EXEC モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if)# **end** | |

# クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定

ポートにクリティカル音声 VLAN を設定し、アクセス不能認証バイパス機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 3 | **radius-server dead-criteria** {**time** *seconds*} [**tries** *number*]<br>例：<br>デバイス(config)# **radius-server dead-criteria time 20 tries 10** | RADIUS サーバが使用不可またはダウン（切断）と見なされる条件を設定します。<br>• **time**：1 ～ 120 秒。スイッチは、デフォルトの *seconds* 値を 10 ～ 60 の間で動的に決定します。<br>• **number**：1 ～ 100 の試行回数。スイッチは、デフォルトの **tries***number* を 10 ～ 100 の間で動的に決定します。 |
| ステップ 4 | **radius-serverdeadtime**分<br>例：<br>デバイス(config)# **radius-server deadtime 60** | （任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分（24 時間）です。デフォルト値は 0 分です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **radius server** *server name*<br>例：<br>デバイス(config)# **radius server rsim address ipv4 124.2.2.12** | （任意）RADIUS サーバの IP アドレスを指定します。 |
| ステップ 6 | **address** {**ipv4** \| **ipv6**} *ip address* **auth-port** *port_number* **acct-port** *port_number*<br>例：<br>デバイス(config-radius-server)# **address ipv4 10.0.1.2 auth-port 1550 acct-port 1560** | RADIUS サーバの IP アドレスを設定します。 |
| ステップ 7 | **key** *string*<br>例：<br>デバイス(config-radius-server)# **key rad123** | （任意）RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 |
| ステップ 8 | **exit**<br>例：<br>デバイス(config-radius-server)# **exit** | RADIUS サーバモードを終了して、グローバルコンフィギュレーションモードを開始します。 |
| ステップ 9 | **dot1x critical** {**eapol** \| **recovery delay** *milliseconds*}<br>例：<br>デバイス(config)# **dot1x critical eapol**<br>(config)# **dot1x critical recovery delay 2000** | （任意）アクセス不能認証バイパスのパラメータを設定します。<br>• **eapol**：スイッチがクリティカルポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。<br>• **recovery delay***milliseconds*：使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカルポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です（ポートは毎秒再初期化できます）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 10 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/0/1** | 設定するポートを指定し、インターフェイスコンフィギュレーションモードを開始します。 |
| ステップ 11 | **authentication event server dead action** {**authorize** \| **reinitialize**} **vlan** *vlan-id*]<br>例：<br>デバイス(config-if)# **authentication event server dead action reinitialicze vlan 20** | これらのキーワードを使用して、RADIUS サーバが到達不能な場合にポートでホストを移動します。<br>• **authorize**：認証しようとする新しいホストをユーザ指定のクリティカル VLAN に移動します。<br>• **reinitialize**：ポートのすべての許可済みホストをユーザ指定のクリティカル VLAN に移動します。 |
| ステップ 12 | **switchport voice vlan** *vlan-id*<br>例：<br>デバイス(config-if)# **switchport voice vlan** | ポートの音声 VLAN を指定します。音声 VLAN はステップ 6 で設定されたクリティカルデータ VLAN と同じにはできません。 |
| ステップ 13 | **authentication event server dead action authorize voice**<br>例：<br>デバイス(config-if)# **authentication event server dead action authorize voice** | RADIUS サーバが到達不能な場合、ポートのデータ トラフィックを音声 VLAN に移動するために、クリティカル音声 VLAN を設定します。 |
| ステップ 14 | **show authentication interface** *interface-id*<br>例：<br>デバイス(config-if)# **do show authentication interface gigabit 1/0/1** | （任意）設定を確認します。 |
| ステップ 15 | **copy running-config startup-config**<br>例：<br>デバイス(config-if)# **do copy running-config startup-config** | （任意）設定を確認します。 |

### 例

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server** グローバル コンフィギュレーション コマンドを使用します。アクセス不能な認証バイパスをディセーブルにするには、**no authentication event server dead action** インターフェイス コンフィギュレーション コマンドを使用します。クリティカル音声VLANをディセーブルにするには、**authentication event server dead action authorize voice** インターフェイス コンフィギュレーション コマンドを使用します。

## アクセス不能認証バイパスの設定例

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
デバイス(config)# radius-server dead-criteria time 30 tries 20
デバイス(config)# radius-server deadtime 60
デバイス(config)# radius server server1
デバイス(config-radius-server)# address ipv4 172.29.36.49 acct-port 1618 auth-port 1612
デバイス(config-radius-server)# key abc1234
デバイス(config-radius-server)# exit
デバイス(config)# dot1x critical eapol
デバイス(config)# dot1x critical recovery delay 2000
デバイス(config)# interface gigabitethernet 1/0/1
デバイス(config-if)# dot1x critical
デバイス(config-if)# dot1x critical recovery action reinitialize
デバイス(config-if)# dot1x critical vlan 20
デバイス(config-if)# end
```

# WoL を使用した 802.1x 認証の設定

WoL を使用した 802.1x 認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順

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

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet2/0/3** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **authentication control-direction** {**both** \| **in**}<br>例：<br>デバイス(config-if)# **authentication control-direction both** | ポートで WoL を使用して 802.1x 認証をイネーブルにし、次のキーワードを使用してポートを双方向または単方向に設定します。<br>• **both**：ポートを双方向に設定します。ポートは、ホストにパケットを送受信できません。デフォルトでは、ポートは双方向です。<br>• **in**：ポートを単方向に設定します。ポートは、ホストにパケットを送信できますが、受信はできません。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show authentication sessions interface** *interface-id*<br>例：<br>デバイス# **show authentication sessions interface gigabitethernet2/0/3** | 入力を確認します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 2/0/1** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **authentication port-control auto**<br>例：<br>デバイス(config-if)# **authentication port-control auto** | ポートでの 802.1x 認証をイネーブルにします。 |
| ステップ 4 | **mab** [**eap**]<br>例：<br>デバイス(config-if)# **mab** | MAC 認証バイパスをイネーブルにします。<br>（任意）**eap** キーワードを使用して、認可用に EAP を使用できるようにスイッチを設定します。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |

# 802.1x ユーザ ディストリビューションの設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、特権 EXEC モードで次の手順を実行します。

手順

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

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **configure terminal** | |
| ステップ 2 | **vlan group** *vlan-group-name* **vlan-list** *vlan-list*<br>例：<br>デバイス(config)# **vlan group eng-dept vlan-list 10** | VLAN グループを設定し、単一の VLAN または VLAN の範囲をそのグループにマッピングします。 |
| ステップ 3 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **no vlan group** *vlan-group-name* **vlan-list** *vlan-list*<br>例：<br>デバイス(config)# **no vlan group eng-dept vlan-list 10** | VLAN グループ コンフィギュレーションまたは VLAN グループ コンフィギュレーションの要素をクリアします。 |

## VLAN グループの設定例

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ コンフィギュレーションおよび指定 VLAN とのマッピングを確認する例を示します。

```
デバイス(config)# vlan group eng-dept vlan-list 10

デバイス(config)# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10

デバイス(config)# show dot1x vlan-group all
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10
hr-dept                         20
```

次に、VLAN を既存の VLAN グループに追加し、VLAN が追加されたことを確認する例を示します。

```
デバイス(config)# vlan group eng-dept vlan-list 30
デバイス(config)# show vlan group eng-dept
Group Name                      Vlans Mapped
```

```
-------------                    --------------
eng-dept                         10,30
```

次に、VLAN を VLAN グループから削除する例を示します。

```
デバイス# no vlan group eng-dept vlan-list 10
```

次に、すべての VLAN が VLAN グループからクリアされたときに、その VLAN グループもクリアされる例を示します。

```
デバイス(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

デバイス(config)# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループをクリアする方法を示します。

```
デバイス(config)# no vlan group end-dept vlan-list all
デバイス(config)# show vlan-group all
```

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

# NAC レイヤ 2 802.1x 検証の設定

NAC レイヤ 2 802.1x 検証を設定できます。これは、RADIUS サーバを使用した 802.1x 認証とも呼ばれます。

NAC レイヤ 2 802.1x 検証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| **ステップ 2** | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet2/0/3** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **switchport mode access**<br>例：<br>デバイス(config-if)# **switchport mode access** | RADIUS サーバを設定した場合に限り、ポートをアクセスモードに設定します。 |
| ステップ 4 | **authentication event no-response action authorize vlan** *vlan-id*<br>例：<br>デバイス(config-if)# **authentication event no-response action authorize vlan 8** | アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。<br>内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。 |
| ステップ 5 | **authentication periodic**<br>例：<br>デバイス(config-if)# **authentication periodic** | クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。 |
| ステップ 6 | **authentication timer reauthenticate**<br>例：<br>デバイス(config-if)# **authentication timer reauthenticate** | クライアントに対する再認証試行を設定します（1 時間に設定）。<br>このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。 |
| ステップ 7 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show authentication sessions interface** *interface-id*<br>例：<br>デバイス# **show authentication sessions interface gigabitethernet2/0/3** | 入力を確認します。 |
| ステップ 9 | **copy running-config startup-config**<br>例： | （任意）コンフィギュレーション ファイルに設定を保存します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **copy running-config startup-config** | |

# NEAT を使用したオーセンティケータ スイッチの設定

この機能を設定するには、ワイヤリング クローゼット外の 1 つのスイッチがサプリカントとして設定され、オーセンティケータ スイッチに接続されている必要があります。

（注）

- CISP または NEAT セッションがアクティブなときにラインカードを取り外してシャーシに挿入する場合は、オーセンティケータ スイッチ インターフェイスの設定を明示的にフラッピングすることによって、アクセスモードに復元する必要があります。
- *cisco-av-pairs* は、ISE で *device-traffic-class=switch* として設定されている必要があります。これにより、サプリカントが正常に認証された後でトランクとしてインターフェイスが設定されます。

スイッチをオーセンティケータに設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **cisp enable**<br>例：<br>デバイス(config)# **cisp enable** | CISP をイネーブルにします。 |
| ステップ 3 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 2/0/1** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **switchport mode access**<br>例：<br>`デバイス(config-if)# switchport mode access` | ポートモードを **access** に設定します。 |
| ステップ 5 | **authentication port-control auto**<br>例：<br>`デバイス(config-if)# authentication port-control auto` | ポート認証モードを auto に設定します。 |
| ステップ 6 | **dot1x pae authenticator**<br>例：<br>`デバイス(config-if)# dot1x pae authenticator` | インターフェイスをポートアクセスエンティティ（PAE）オーセンティケータとして設定します。 |
| ステップ 7 | **spanning-tree portfast**<br>例：<br>`デバイス(config-if)# spanning-tree portfast trunk` | 単一ワークステーションまたはサーバに接続されたアクセス ポート上で Port Fast をイネーブルにします。 |
| ステップ 8 | **end**<br>例：<br>`デバイス(config-if)# end` | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show running-config interface** *interface-id*<br>例：<br>`デバイス# show running-config interface gigabitethernet 2/0/1` | 設定を確認します。 |
| ステップ 10 | **copy running-config startup-config**<br>例： | （任意）コンフィギュレーションファイルに設定を保存します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **copy running-config startup-config** | （注） 変更をコンフィギュレーション ファイルに保存すると、オーセンティケータインターフェイスがリロード後も引き続きトランクモードになることを意味します。 オーセンティケータインターフェイスをアクセスポートとして維持する場合は、コンフィギュレーションファイルに変更を保存しないでください。 |

# NEAT を使用したサプリカント スイッチの設定

スイッチをサプリカントに設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **cisp enable**<br>例：<br>デバイス(config)# **cisp enable** | CISP をイネーブルにします。 |
| ステップ 3 | **dot1x credentials** *profile*<br>例：<br>デバイス(config)# **dot1x credentials test** | 802.1x クレデンシャル プロファイルを作成します。これは、サプリカントとして設定されるポートに接続する必要があります。 |
| ステップ 4 | **username** *suppswitch*<br>例：<br>デバイス(config)# **username suppswitch** | ユーザ名を作成します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **password** *password*<br>例：<br>デバイス(config)# **password myswitch** | 新しいユーザ名のパスワードを作成します。 |
| ステップ 6 | **dot1x supplicant force-multicast**<br>例：<br>デバイス(config)# **dot1x supplicant force-multicast** | ユニキャストまたはマルチキャストパケットのいずれかを受信した場合にスイッチに強制的にマルチキャスト EAPOL だけを送信させます。<br>これにより、NEAT がすべてのホストモードでのサプリカントスイッチで機能できるようにもなります。 |
| ステップ 7 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet1/0/1** | 設定するポートを指定し、インターフェイスコンフィギュレーションモードを開始します。 |
| ステップ 8 | **switchport trunk encapsulation dot1q**<br>例：<br>デバイス(config-if)# **switchport trunk encapsulation dot1q** | ポートをトランク モードに設定します。 |
| ステップ 9 | **switchport mode trunk**<br>例：<br>デバイス(config-if)# **switchport mode trunk** | インターフェイスを VLAN トランクポートとして設定します。 |
| ステップ 10 | **dot1x pae supplicant**<br>例：<br>デバイス(config-if)# **dot1x pae supplicant** | インターフェイスをポートアクセスエンティティ（PAE）サプリカントとして設定します。 |
| ステップ 11 | **dot1x credentials** *profile-name*<br>例：<br>デバイス(config-if)# **dot1x credentials** | 802.1x クレデンシャル プロファイルをインターフェイスに対応付けます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `test` | |
| ステップ 12 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 13 | **show running-config interface** *interface-id*<br>例：<br>デバイス# **show running-config interface gigabitethernet1/0/1** | 設定を確認します。 |
| ステップ 14 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |
| ステップ 15 | Auto Smartport マクロを使用した NEAT の設定 | スイッチ VSA ではなく Auto Smartport ユーザ定義マクロを使用して、オーセンティケータスイッチを設定することもできます。詳細については、このリリースに対応する『*Auto Smartports Configuration Guide*』を参照してください。 |

# ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定

（注） スイッチにダウンロードする前に、ダウンロード可能な ACL を ACS で設定する必要があります。

ポートでの認証後、**show ip access-list** 特権 EXEC コマンドを使用して、ポートにダウンロードした ACL を表示できます。

# ダウンロード可能な ACL の設定

これらのポリシーは、クライアントが認証され、クライアント IP アドレスが IP デバイス トラッキングテーブルに追加された後で有効になります。その後スイッチがダウンロード可能な ACL をポートに適用します。

特権 EXEC モードで次の手順を実行します。

### 始める前に

SISF ベースのデバイストラッキングは、802.1x 認証を設定するための前提条件です。デバイストラッキングをプログラムまたは手動で有効にしていることを確認します。詳細については、「*SISF* ベースのトラッキングの設定」の章を参照してください。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 3 | **aaa authorization network default local group radius**<br>例：<br>デバイス(config)# **aaa authorization network default local group radius** | 許可の方法をローカルに設定します。認可方式を削除するには、**no aaa authorization network default local group radius** コマンドを使用します。 |
| ステップ 4 | **radius-server vsa send authentication**<br>例：<br>デバイス(config)# **radius-server vsa send authentication** | RADIUS VSA 送信認証を設定します。 |
| ステップ 5 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | **gigabitethernet2/0/4** | |
| ステップ 6 | **ip access-group** *acl-id* **in**<br>例：<br>デバイス(config-if)# **ip access-group default_acl in** | ポートの入力方向のデフォルト ACL を設定します。<br>（注） *acl-id* はアクセス リストの名前または番号です。 |
| ステップ 7 | **show running-config interface** *interface-id*<br>例：<br>デバイス(config-if)# **show running-config interface gigabitethernet2/0/4** | 設定を確認します。 |
| ステップ 8 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

## ダウンロード ポリシーの設定

特権 EXEC モードで次の手順を実行します。

### 始める前に

SISF ベースのデバイストラッキングは、802.1x 認証を設定するための前提条件です。デバイストラッキングをプログラムまたは手動で有効にしていることを確認します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **access-list** *access-list-number* **{ deny \| permit } { hostname \| any \| host } log**<br>例：<br>デバイス(config)# **access-list 1 deny any log** | デフォルト ポート ACL を定義します。<br>access-list-number には、1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 条件が一致した場合にアクセスを拒否する場合は **deny** を指定し、許可する場合は **permit** を指定します。<br>source は、次のようなパケットを送信するネットワークまたはホストの送信元アドレスです。<br>• **hostname**：ドット付き 10 進表記による 32 ビット長の値。<br>• **any**：source および source-wildcard の値 0.0.0.0 255.255.255.255 の省略形を意味するキーワード any。source-wildcard 値を入力する必要はありません。<br>• **host**：source および source-wildcard の値 source 0.0.0.0 の省略形を意味するキーワード host。<br>（任意）source-wildcard ビットを送信元アドレスに適用します。<br>（任意）ログを入力して、エントリと一致するパケットに関する情報ロギングメッセージをコンソールに送信します。 |
| **ステップ 3** | **interface** *interface-id*<br>例：<br>`デバイス(config)# interface gigabitethernet2/0/2` | インターフェイスコンフィギュレーション モードを開始します。 |
| **ステップ 4** | **ip access-group** *acl-id* **in**<br>例：<br>`デバイス(config-if)# ip access-group default_acl in` | ポートの入力方向のデフォルト ACL を設定します。<br>（注） acl-id はアクセス リストの名前または番号です。 |
| **ステップ 5** | **exit**<br>例：<br>`デバイス(config-if)# exit` | グローバル コンフィギュレーション モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 7 | **aaa authorization network default group radius**<br>例：<br>デバイス(config)# **aaa authorization network default group radius** | 許可の方法をローカルに設定します。認可方式を削除するには、**no aaa authorization network default group radius** コマンドを使用します。 |
| ステップ 8 | **radius-server vsa send authentication**<br>例：<br>デバイス(config)# **radius-server vsa send authentication** | ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。<br>（注） ダウンロード可能な ACL が機能する必要があります。 |
| ステップ 9 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

# VLAN ID ベース MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **mab request format attribute 32 vlan access-vlan**<br>例： | VLAN ID ベース MAC 認証をイネーブルにします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config)# **mab request format attribute 32 vlan access-vlan** | |
| ステップ 3 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# 柔軟な認証順序の設定

下の手順で使用される例は、MAB が IEEE 802.1x 認証（dot1x）の前に試行されるように柔軟な認証の順序設定の順序を変更します。MAB は最初の認証方式として設定されているため、MAB は他のすべての認証方式よりも優先されます。

（注） これらの認証方式のデフォルトの順序とプライオリティを変更する前に、これらの変更による潜在的な結果を理解する必要があります。詳細について、http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/application_note_c27-573287_ps6638_Products_White_Paper.html を参照してください。

特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/0/1** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **switchport mode access**<br>例：<br>`デバイス(config-if)# switchport mode access` | RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。 |
| ステップ 4 | **authentication order [ dot1x \| mab ] \| {webauth}**<br>例：<br>`デバイス(config-if)# authentication order mab dot1x` | （任意）ポート上で使用される認証方式の順序を設定します。 |
| ステップ 5 | **authentication priority [ dot1x \| mab ] \| {webauth}**<br>例：<br>`デバイス(config-if)# authentication priority mab dot1x` | （任意）認証方式をポート プライオリティ リストに追加します。 |
| ステップ 6 | **end**<br>例：<br>`デバイス(config-if)# end` | 特権 EXEC モードに戻ります。 |

# Open1x の設定

ポートの許可ステートの手動制御をイネーブルにするには、特権EXECモードで次の手順を実行します。

手順

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

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **interface** *interface-id*<br>例：<br>`デバイス(config)# interface gigabitethernet 1/0/1` | 設定するポートを指定し、インターフェイスコンフィギュレーションモードを開始します。 |
| ステップ 3 | **switchport mode access**<br>例：<br>`デバイス(config-if)# switchport mode access` | RADIUS サーバを設定した場合に限り、ポートをアクセスモードに設定します。 |
| ステップ 4 | **authentication control-direction** {**both** \| **in**}<br>例：<br>`デバイス(config-if)# authentication control-direction both` | （任意）ポート制御を単一方向モードまたは双方向モードに設定します。 |
| ステップ 5 | **authentication fallback** *name*<br>例：<br>`デバイス(config-if)# authentication fallback profile1` | （任意）802.1x 認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。 |
| ステップ 6 | **authentication host-mode**[**multi-auth** \|**multi-domain** \|**multi-host** \|**single-host**]<br>例：<br>`デバイス(config-if)# authentication host-mode multi-auth` | （任意）ポート上で認証マネージャモードを設定します。 |
| ステップ 7 | **authentication open**<br>例：<br>`デバイス(config-if)# authentication open` | （任意）ポート上でオープンアクセスをイネーブルまたはディセーブルにします。 |
| ステップ 8 | **authentication order** [ **dot1x** \| **mab** ] \| {**webauth**}<br>例： | （任意）ポート上で使用される認証方式の順序を設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if)# **authentication order dot1x webauth** | |
| ステップ 9 | **authentication periodic**<br>例：<br>デバイス(config-if)# **authentication periodic** | （任意）ポート上で再認証をイネーブルまたはディセーブルにします。 |
| ステップ 10 | **authentication port-control {auto \| force-authorized \| force-un authorized}**<br>例：<br>デバイス(config-if)# **authentication port-control auto** | （任意）ポートの許可ステートの手動制御をイネーブルにします。 |
| ステップ 11 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |

# ポート上での 802.1x 認証のディセーブル化

802.1x 認証をポートでディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで 802.1x 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

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

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 2/0/1** | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **switchport mode access**<br>例：<br>デバイス(config-if)# **switchport mode access** | （任意）RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。 |
| ステップ 4 | **no dot1x pae authenticator**<br>例：<br>デバイス(config-if)# **no dot1x pae authenticator** | ポートでの 802.1x 認証をディセーブルにします。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |

# 802.1x 認証設定のデフォルト値へのリセット

802.1x 認証設定をデフォルト値に戻すには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface** | インターフェイスコンフィギュレーション モードを開始し、設定するポートを指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `gigabitethernet 1/0/2` | |
| ステップ 3 | **dot1x default**<br>例：<br>`デバイス(config-if)# dot1x default` | 設定可能な 802.1x のパラメータをデフォルト値へ戻します。 |
| ステップ 4 | **end**<br>例：<br>`デバイス(config-if)# end` | 特権 EXEC モードに戻ります。 |

# 802.1x の統計情報およびステータスのモニタリング

表 *35 :* 特権 *EXEC* 表示コマンド

| コマンド | 目的 |
|---|---|
| **show dot1x all statistics** | すべてのポートの 802.1x 統計情報を表示します。 |
| **show dot1x interface** *interface-id* **statistics** | 指定されたポートの 802.1x 統計情報を表示します。 |
| **show dot1x all**[**count** \|**details** \|**statistics** \|**summary**] | スイッチの 802.1x 管理ステータスおよび動作ステータスを表示します。 |
| **show dot1x interface** *interface-id* | 指定されたポートの 802.1x 管理ステータスおよび動作ステータスを表示します。 |

表 *36 :* グローバル コンフィギュレーション コマンド

| コマンド | 目的 |
|---|---|
| **no dot1x logging verbose** | 冗長な 802.1x 認証メッセージをフィルタに掛けます（Cisco IOS Release 12.2(55) SE 以降） |

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

第 20 章

# Web ベース認証

この章では、デバイスで Web ベース認証を設定する方法について説明します。この章の内容は、次のとおりです。


- Web ベース認証の概要 （457 ページ）
- Web ベース認証の設定方法 （468 ページ）
- Web ベース認証ステータスの確認 （481 ページ）


## Web ベース認証の概要

IEEE 802.1x サプリカントが実行されていないホストシステムでエンドユーザを認証するには、Web 認証プロキシとして知られている Web ベース認証機能を使用します。

HTTP セッションを開始すると、Web ベース認証は、ホストからの入力 HTTP パケットを代行受信し、ユーザに HTML ログイン ページを送信します。ユーザはクレデンシャルを入力します。このクレデンシャルは、Web ベース認証機能により、認証のために認証、許可、アカウンティング（AAA）サーバに送信されます。

認証が成功すると、Web ベース認証はログイン成功 HTML ページをホストに送信し、AAA サーバから返されたアクセス ポリシーを適用します。

認証に失敗した場合、Web ベース認証は、ログインの失敗を示す HTML ページをユーザに転送し、ログインを再試行するように、ユーザにプロンプトを表示します。最大試行回数を超過した場合、Web ベース認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザは待機期間中、ウォッチ リストに載せられます。

（注） 中央 Web 認証リダイレクト用の HTTPS トラフィック インターセプションはサポートされていません。

（注） グローバル パラメータ マップ（method-type、custom、redirect）は、すべてのクライアントおよび SSID で同じ Web 認証方式（consent、web consent、webauth など）を使用するときにのみ使用する必要があります。これにより、すべてのクライアントが同じ Web 認証方式になります。

要件により、1 つの SSID に consent、別の SSID に webauth を使用する場合、名前付きパラメータ マップを 2 つ使用する必要があります。1 番目のパラメータ マップには consent を設定し、2 番目のパラメータ マップには webauth を設定する必要があります。

（注） Webauth クライアントの認証試行時に受信する traceback には、パフォーマンスや行動への影響はありません。これは、ACL アプリケーションの EPM に FFM が返信したコンテキストがすでにキュー解除済み（タイマーの有効期限切れの可能性あり）で、セッションが「未承認」になった場合にまれに発生します。

Web ページがホストされている場所に基づいて、ローカル Web 認証は次のように分類できます。

- 内部：ローカル Web 認証時に、コントローラの内部デフォルト HTML ページ（ログイン、成功、失敗、および期限切れ）が使用されます。
- カスタマイズ：ローカル Web 認証時に、カスタマイズされた Web ページ（ログイン、成功、失敗、および期限切れ）がコントローラにダウンロードされ、使用されます。
- 外部：組み込みまたはカスタム Web ページを使用する代わりに、外部 Web サーバ上でカスタマイズされた Web ページがホストされます。

さまざまな Web 認証ページに基づき、Web 認証のタイプは次のように分類できます。

- *Webauth*：これが基本的な Web 認証です。この場合、コントローラはユーザ名とパスワードの入力が必要なポリシー ページを提示します。ネットワークにアクセスするには、ユーザは正しいクレデンシャルを入力する必要があります。
- *Consent* または *web-passthrough*：この場合、コントローラは [Accept] ボタンまたは [Deny] ボタンが表示されたポリシー ページを提示します。ネットワークにアクセスするには、ユーザは [Accept] ボタンをクリックする必要があります。
- *Webconsent*：これは webauth と consent の Web 認証タイプの組み合わせです。この場合、コントローラは [Accept] ボタンまたは [Deny] ボタンがあり、ユーザ名とパスワードの入力が必要なポリシーページを提示します。ネットワークにアクセスするには、ユーザは正しいクレデンシャルを入力して [Accept] ボタンをクリックする必要があります。

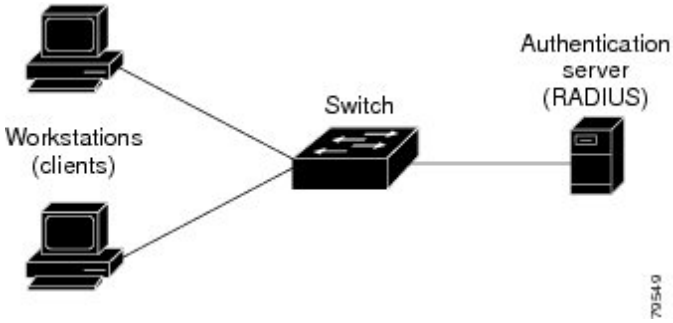
# デバイスのロール

Web ベース認証では、ネットワーク上のデバイスに次のような固有の役割があります。

- クライアント：LAN およびサービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。このワークステーションでは、Java Script がイネーブルに設定された HTML ブラウザが実行されている必要があります。
- 認証サーバ：クライアントを認証します。認証サーバはクライアントの識別情報を確認し、そのクライアントが LAN およびスイッチのサービスへのアクセスを許可されたか、あるいはクライアントが拒否されたのかをスイッチに通知します。
- スイッチ：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。

**図 *26 : Web* ベース認証デバイスの役割**

次の図は、ネットワーク上でのこれらのデバイスの役割を示します。




# ホストの検出

スイッチは、検出されたホストに関する情報を格納するために、IP デバイストラッキングテーブルを維持します。

（注） デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

レイヤ 2 インターフェイスでは、Web ベース認証は、これらのメカニズムを使用して、IP ホストを検出します。

- ARP ベースのトリガー：ARP リダイレクト ACL により、Web ベース認証は、スタティック IP アドレス、またはダイナミック IP アドレスを持つホストを検出できます。
- ダイナミック ARP インスペクション
- DHCP スヌーピング：スイッチがホストの DHCP バインディング エントリを作成するときに Web ベース認証が通知されます。

# セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストをレビューします。

  ホスト IP が例外リストに含まれている場合、この例外リスト エントリからポリシーが適用され、セッションが確立されます。

- 認証バイパスをレビューします。

  ホストIPが例外リストに含まれていない場合、Webベース認証は応答しないホスト（NRH）要求をサーバに送信します。

  サーバの応答が access accepted であった場合、認証はこのホストにバイパスされます。セッションが確立されます。

- HTTP インターセプト ACL を設定します。

  NRH 要求に対するサーバの応答が access rejected であった場合、HTTP インターセプト ACLがアクティブ化され、セッションはホストからのHTTP トラフィックを待機します。

# 認証プロセス

Web ベース認証をイネーブルにすると、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTP トラフィックが代行受信され、認証が開始されます。スイッチは、ユーザにログインページを送信します。ユーザはユーザ名とパスワードを入力します。スイッチはこのエントリを認証サーバに送信します。
- 認証に成功した場合、スイッチは認証サーバからこのユーザのアクセス ポリシーをダウンロードし、アクティブ化します。ログインの成功ページがユーザに送信されます
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザはログインを再試行します。失敗の回数が試行回数の最大値に達した場合、スイッチはログイン期限切れページを送信します。このホストはウォッチ リストに入れられます。ウォッチ リストのタイム アウト後、ユーザは認証プロセスを再試行することができます。
- 認証サーバがスイッチに応答せず、AAA 失敗ポリシーが設定されている場合、スイッチはホストに失敗アクセス ポリシーを適用します。ログインの成功ページがユーザに送信されます
- ホストがレイヤ 2 インターフェイス上の ARP プローブに応答しなかった場合、またはホストがレイヤ 3 インターフェイスでアイドル タイムアウト内にトラフィックを送信しなかった場合、スイッチはクライアントを再認証します。
- ホストがレイヤ 2 インターフェイス上の ARP プローブに応答しない場合、スイッチはクライアントを再認証します。

- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッションタイムアウトを適用します。
- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信します。Termination-Action は、サーバからの応答に含まれます。
- Termination-Action がデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除されます。

# ローカル Web 認証バナー

Web 認証を使用して、デフォルトのカスタマイズ済み Web ブラウザ バナーを作成して、スイッチにログインしたときに表示するようにできます。

このバナーは、ログイン ページと認証結果ポップアップ ページの両方に表示されます。デフォルトのバナー メッセージは次のとおりです。

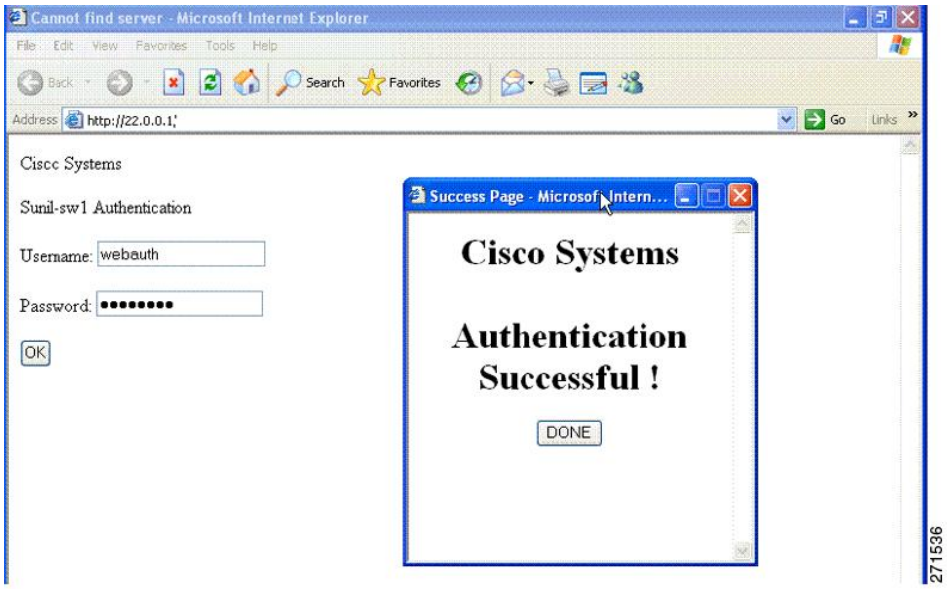
- 認証成功
- 認証失敗
- 認証期限切れ

ローカル ネットワーク認証バナーは、レガシーおよび新スタイル（セッション アウェア）の CLI で次のように設定できます。

- レガシー モード：**ip admission auth-proxy-banner http** グローバル コンフィギュレーション コマンドを使用します。
- 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。

ログイン ページには、デフォルトのバナー、*Cisco Systems*、および *Switch host-name Authentication* が表示されます。*Cisco Systems* は認証結果ポップアップ ページに表示されます。

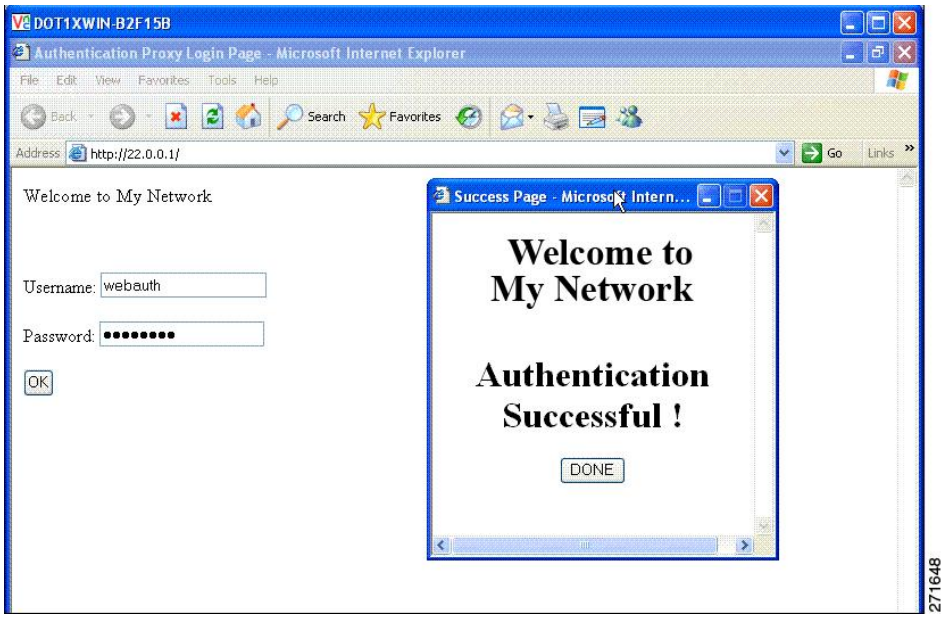
図 *27*：認証成功バナー




バナーは次のようにカスタマイズ可能です。

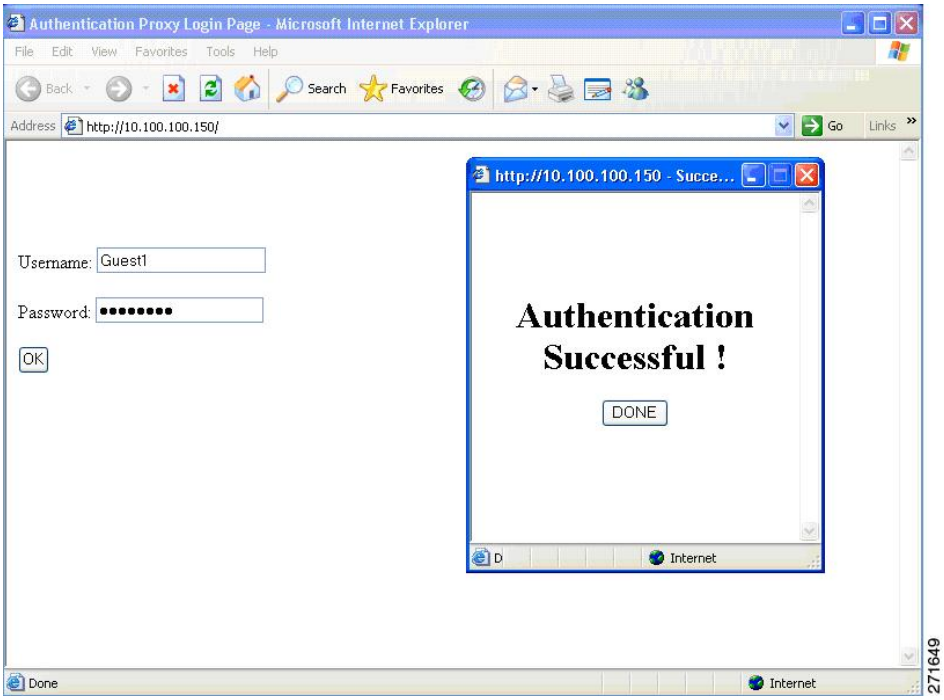
- スイッチ名、ルータ名、または会社名などのメッセージをバナーに追加する。
  - レガシーモード： **ip admission auth-proxy-banner http** *banner-text* グローバル コンフィギュレーション コマンドを使用します。
  - 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。
- ロゴまたはテキスト ファイルをバナーに追加する。
  - レガシーモード：**ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用します。
  - 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。

図 *28 :* カスタマイズされた *Web* バナー




バナーがイネーブルにされていない場合、Web認証ログイン画面にはユーザ名とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはバナーは表示されません。

図 *29 :* バナーが表示されていないログイン画面



# Web 認証カスタマイズ可能な Web ページ

Web ベース認証プロセスでは、スイッチ内部の HTTP サーバは、認証中のクライアントに配信される 4 種類の HTML ページをホストします。サーバはこれらのページを使用して、ユーザに次の 4 種類の認証プロセス ステートを通知します。

- ログイン：資格情報が要求されています。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：ログインの失敗回数が多すぎて、ログイン セッションが期限切れになりました。

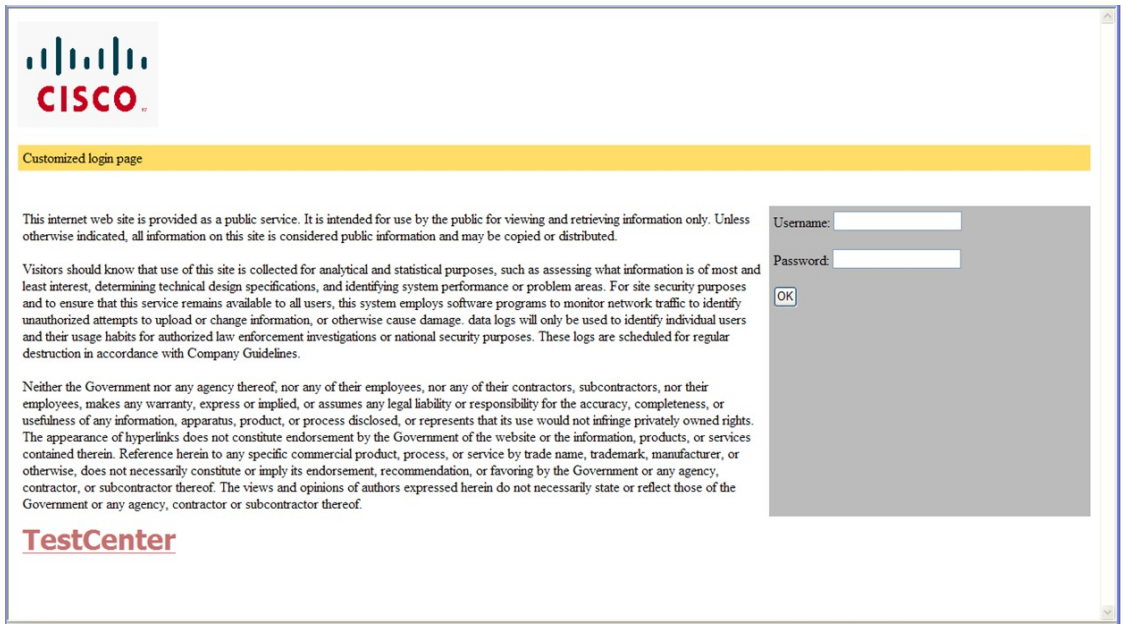
## ガイドライン

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。
- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。
- バナー ページで、ログイン ページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。
- この URL 文字列は有効な URL（例：http://www.cisco.com）でなければなりません。不完全な URL は、Web ブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド（例：ページのタイムアウトを設定、暗号化されたパスワードの設定、同じページが 2 回送信されていないことの確認など）を記入する必要があります.
- 設定されたログイン フォームがイネーブルにされている場合、特定の URL にユーザをリダイレクトする CLI コマンドは使用できません。管理者は、Web ページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定の URL にユーザをリダイレクトする CLI コマンドを入力してから、Web ページを設定するコマンドを入力した場合、特定の URL にユーザをリダイレクトする CLI コマンドは効力を持ちません。
- 設定された Web ページは、スイッチのブート フラッシュ、またはフラッシュにコピーできます。
- ログイン ページを 1 つのフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、スタック マスター、またはメンバのフラッシュ）にすることができます。

- 4 ページすべてを設定する必要があります。
- Web ページを使ってバナー ページを設定した場合、このバナー ページには効果はありません。
- システムディレクトリ（たとえば、flash、disk0、disk）に保存されていて、ログイン ページに表示する必要のあるロゴ ファイル（イメージ、フラッシュ、オーディオ、ビデオなど）すべてには、必ず、*web_auth_<filename>* の形式で名前をつけてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

デフォルトの内部HTMLページの代わりに、自分のHTMLページを使用することができます。認証後のユーザのリダイレクト先で、内部成功ページの代わりとなる URL を指定することもできます。

**図 *30* : カスタマイズ可能な認証ページ**




## 認証プロキシ Web ページの注意事項

カスタマイズされた認証プロキシ Web ページを設定する際には、次の注意事項に従ってください。

- カスタム Web ページ機能をイネーブルにするには、カスタム HTML ファイルを 4 個すべて指定します。指定したファイルの数が 4 個未満の場合、内部デフォルト HTML ページが使用されます。
- これら 4 個のカスタム HTML ファイルは、スイッチのフラッシュ メモリ内に存在しなければなりません。各 HTML ファイルの最大サイズは 8 KB です。
- カスタムページ上のイメージはすべて、アクセス可能はHTTPサーバ上に存在しなければなりません。インターセプト ACL は、管理ルール内で設定します。

- カスタム ページからの外部リンクはすべて、管理ルール内でのインターセプト ACL の設定を必要とします。
- 有効なDNSサーバにアクセスするには、外部リンクまたはイメージに必要な名前解決で、管理ルール内にインターセプト ACL を設定する必要があります。
- カスタムWebページ機能がイネーブルに設定されている場合、設定されたauth-proxy-bannerは使用されません。
- カスタム Web ページ機能がイネーブルに設定されている場合、ログインの成功に対するリダイレクション URL は使用できません。
- カスタム ファイルの指定を解除するには、このコマンドの **no** 形式を使用します。

カスタム ログイン ページはパブリック Web フォームであるため、このページについては、次の注意事項に従ってください。

- ログイン フォームは、ユーザによるユーザ名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

## 成功ログインに対するリダイレクト URL の注意事項

成功ログインに対するリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルに設定されている場合、リダイレクションURL機能はディセーブルにされ、CLIでは使用できません。リダイレクションは、カスタム ログイン成功ページで実行できます。
- リダイレクション URL 機能が有効に設定されている場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの **no** 形式を使用します。
- Web ベースの認証クライアントが正常に認証された後にリダイレクション URL が必要な場合、URL 文字列は有効な URL（たとえば http://）で開始し、その後に URL 情報が続く必要があります。http://を含まないURLが指定されると、正常に認証が行われても、そのリダイレクション URL によって Web ブラウザでページが見つからないまたは同様のエラーが生じる場合があります。

# その他の機能と Web ベース認証の相互作用

## ポート セキュリティ

Webベース認証とポートセキュリティは、同じポートに設定できます。Webベース認証はポートを認証し、ポート セキュリティは、クライアントの MAC アドレスを含むすべての MAC ア

ドレスに対するネットワーク アクセスを管理します。この場合、このポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

## LAN ポート IP

LAN ポート IP（LPIP）とレイヤ 2 Web ベース認証は、同じポートに設定できます。ホストは、まず Web ベース認証、次に LPIP ポスチャ検証を使用して認証されます。LPIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

Web ベース認証のアイドル時間が満了すると、NAC ポリシーは削除されます。ホストが認証され、ポスチャが再度検証されます。

## ゲートウェイ IP

VLAN のいずれかのスイッチ ポートで Web ベース認証が設定されている場合、レイヤ 3 VLAN インターフェイス上にゲートウェイ IP（GWIP）を設定することはできません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェアで、両方の機能のホスト ポリシーが適用されます。GWIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

## ACL

インターフェイスで VLAN ACL、または Cisco IOS ACL を設定した場合、ACL は、Web ベース認証のホスト ポリシーが適用された後だけ、ホスト トラフィックに適用されます。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの入力トラフィックについて、ポート ACL（PACL）をデフォルトのアクセス ポリシーとして設定することが必須ではないものの、より安全です。認証後、Web ベース認証のホスト ポリシーは、PACL に優先されます。ポートに設定された ACL がなくても、ポリシー ACL はセッションに適用されます。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN が VACL キャプチャ用に設定されているポートには Web ベース認証は設定できません。

## コンテキストベース アクセス コントロール

コンテキストベース アクセス コントロール（CBAC）が、ポート VLAN のレイヤ 3 VLAN インターフェイスで設定されている場合、レイヤ 2 ポートで Web ベース認証は設定できません。

## EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。Web ベース認証設定は、すべてのメンバ チャネルに適用されます。

# Web ベース認証の設定方法

## デフォルトの Web ベース認証の設定

次の表に、デフォルトの Web ベース認証の設定を示しています。

表 *37 :* デフォルトの *Web* ベース認証の設定

| 機能 | デフォルト設定 |
|---|---|
| AAA | 無効 |
| RADIUS サーバ<br>• IP アドレス<br>• UDP 認証ポート<br>• キー | • 指定なし<br>• 1645<br>• 指定なし |
| 無活動タイムアウトのデフォルト値 | 3600 秒 |
| 無活動タイムアウト | イネーブル |

## Web ベース認証の設定に関する注意事項と制約事項

- Web ベース認証は入力だけの機能です。
- Web ベース認証は、アクセス ポートだけで設定できます。Web ベース認証は、トランク ポート、EtherChannel メンバ ポート、またはダイナミック トランク ポートではサポートされていません。
- スイッチが特定のホストまたは Web サーバにクライアントをリダイレクトしてログインメッセージを表示する場合、外部 Web 認証はサポートされません。
- スタティックな ARP キャッシュが割り当てられているレイヤ 2 インターフェイス上のホストは認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能では検出されません。
- デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。
- Web ベース認証を使用するには、SISF ベースのデバイス トラッキングを有効にする必要があります。デフォルトでは、SISF ベースのデバイス トラッキングはスイッチで無効になっています。

- スイッチ HTTP サーバを実行するには、IP アドレスを少なくとも 1 つ設定する必要があります。また、各ホスト IP アドレスに到達するようにルートを設定する必要もあります。HTTP サーバは、ホストに HTTP ログイン ページを送信します。
- 2 ホップ以上離れたところにあるホストでは、STP トポロジの変更により、ホスト トラフィックの到着するポートが変わってしまった場合、トラフィックが停止する可能性があります。これは、レイヤ 2（STP）トポロジの変更後に、ARP および DHCP の更新が送信されていない場合に発生します。
- Webベース認証は、ダウンロード可能なホストポリシーとして、VLAN割り当てをサポートしていません。
- Web ベース認証はセッション認識型ポリシー モードで IPv6 をサポートします。IPv6 Web 認証には、スイッチで設定された少なくても 1 つの IPv6 アドレスおよびスイッチ ポートに設定設定された IPv6 スヌーピングが必要です。
- Web ベース認証および Network Edge Access Topology（NEAT）は、相互に排他的です。インターフェイス上で NEAT がイネーブルの場合、Web ベース認証を使用できず、インターフェイス上で Web ベース認証が実行されている場合は、NEAT を使用できません。
- スイッチから RADIUS サーバへの通信の設定に使用される次の RADIUS セキュリティ サーバ設定を確認します。
  - ホスト名
  - ホスト IP アドレス
  - ホスト名と特定の UDP ポート番号
  - IP アドレスと特定の UDP ポート番号

  IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホストエントリは、最初に設定されたホストエントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って選択されます。
- RADIUS サーバ パラメータを設定する場合は、次の点に注意してください。
  - 別のコマンドラインに、**key** *string* を指定します。
  - **key** *string* には、スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する、認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。
  - **key** *string* を指定する場合、キーの中間、および末尾にスペースを使用します。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。

- すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号キー値をグローバルに設定するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、radius-server transmit、および radius-server key グローバル コンフィギュレーション コマンドを使用します。

（注） RADIUS サーバでは、スイッチの IP アドレス、サーバとスイッチで共有される key string、およびダウンロード可能な ACL（DACL）などの設定を行う必要があります。詳細については、RADIUS サーバのマニュアルを参照してください。

- URL リダイレクト ACL の場合：
  - 許可アクセス制御エントリ （ACE）ルールに一致するパケットは、AAA サーバに転送するために CPU に送信されます。
  - 拒否 ACE ルールに一致するパケットは、スイッチを介して転送されます。
  - 許可 ACE ルールにも拒否 ACE ルールにも一致しないパケットは、次の dACL によって処理されます。dACL がない場合、パケットは暗黙的拒否 ACL にヒットしてドロップされます。

# 認証ルールとインターフェイスの設定

認証ルールおよびインターフェイスを設定するには、次の手順を実行します。

### 始める前に

SISF ベースのデバイストラッキングは、web 認証の前提条件です。デバイストラッキングをプログラムまたは手動で有効にしていることを確認します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例： | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **configure terminal** | |
| ステップ 3 | **ip admission name** *name* **proxy http**<br>例：<br>デバイス(config)# **ip admission name webauth1 proxy http** | Web ベース許可の認証ルールを設定します。 |
| ステップ 4 | **interface** *type slot/port*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/0/1** | インターフェイスコンフィギュレーション モードを開始し、Web ベース認証をイネーブルにする入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。<br>*type* には、fastethernet、gigabit ethernet、または tengigabitethernet を指定できます。 |
| ステップ 5 | **ip access-group** *name*<br>例：<br>デバイス(config-if)# **ip access-group webauthag** | デフォルト ACL を適用します。 |
| ステップ 6 | **ip admission name**<br>例：<br>デバイス(config)# **ip admission name** | インターフェイスの Web ベース認可の認証ルールを設定します。 |
| ステップ 7 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show ip admission**<br>例：<br>デバイス# **show ip admission** | 設定を表示します。 |
| ステップ 9 | **copy running-config startup-config**<br>例： | （任意）コンフィギュレーション ファイルに設定を保存します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **copy running-config startup-config** | |

# AAA 認証の設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa new-model**<br>例：<br>デバイス(config)# **aaa new-model** | AAA 機能をイネーブルにします。 |
| ステップ 4 | **aaa authentication login default group {tacacs+ \| radius}**<br>例：<br>デバイス(config)# **aaa authentication login default group tacacs+** | ログイン時の認証方法のリストを定義します。<br>**named_authentication_list** は、31 文字未満の名前を示します。<br>**AAA_group_name** はサーバ グループ名を示します。サーバグループ **server_name** をその先頭で定義する必要があります。 |
| ステップ 5 | **aaa authorization auth-proxy default group {tacacs+ \| radius}**<br>例：<br>デバイス(config)# **aaa authorization auth-proxy default group tacacs+** | Web ベース許可の許可方式リストを作成します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **tacacs server** *server-name*<br>例：<br>デバイス(config)# **tacacs server yourserver** | AAA サーバを指定します。 |
| ステップ 7 | **address** {**ipv4** \| **ipv6**} *ip address*<br>例：<br>デバイス(config-server-tacacs)# **address ipv4 10.0.1.12** | TACACS サーバの IP アドレスを設定します。 |
| ステップ 8 | **key** 文字列<br>例：<br>デバイス(config-server-tacacs)# **key cisco123** | スイッチと TACACS サーバとの間で使用される許可および暗号キーを設定します。 |
| ステップ 9 | **exit**<br>例：<br>デバイス(config-server-tacacs)# **exit** | TACACS サーバモードを終了して、グローバルコンフィギュレーションモードを開始します。 |
| ステップ 10 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 11 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 12 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

# スイッチ/RADIUS サーバ間通信の設定

RADIUS サーバのパラメータを設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip radius source-interface vlan** *vlan interface number*<br>例：<br>デバイス(config)# **ip radius source-interface vlan 80** | RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。 |
| ステップ 4 | **radius server** *server name*<br>例：<br>デバイス(config)# **radius server rsim address ipv4 124.2.2.12** | （任意）RADIUS サーバの IP アドレスを指定します。 |
| ステップ 5 | **address** {**ipv4** \| **ipv6**} *ip address*<br>例：<br>デバイス(config-radius-server)# **address ipv4 10.0.1.2 auth-port 1550 acct-port 1560** | RADIUS サーバの IP アドレスを設定します。 |
| ステップ 6 | **key** *string*<br>例：<br>デバイス(config-radius-server)# **key rad123** | （任意）RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 7 | **exit**<br>例：<br>デバイス(config-radius-server)# **exit** | RADIUS サーバモードを終了して、グローバル コンフィギュレーション モードを開始します。 |
| ステップ 8 | **radius-server dead-criteria tries** *num-tries*<br>例：<br>デバイス(config)# **radius-server dead-criteria tries 30** | RADIUS サーバに送信されたメッセージへの応答がない場合に、このサーバが非アクティブであると見なすまでの送信回数を指定します。指定できる *num-tries* の範囲は 1 ～ 100 です。 |
| ステップ 9 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

# HTTP サーバの設定

Web ベース認証を使用するには、デバイスで HTTP サーバをイネーブルにする必要があります。このサーバは HTTP または HTTPS のいずれかについてイネーブルにできます。

（注） Apple の疑似ブラウザは、**ip http secure-server** コマンドを設定するだけでは開きません。**ip http server** コマンドも設定する必要があります。

HTTP または HTTPS のいずれかについてサーバをイネーブルにするには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例： | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **configure terminal** | |
| ステップ 3 | **ip http server**<br>例：<br>デバイス(config)# **ip http server** | HTTP サーバをイネーブルにします。Web ベース認証機能は、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。 |
| ステップ 4 | **ip http secure-server**<br>例：<br>デバイス(config)# **ip http secure-server** | HTTPS をイネーブルにします。<br>カスタム認証プロキシ Web ページを設定するか、成功ログインのリダイレクション URL を指定します。<br>（注） **ip http secure-server** コマンドを入力したときに、セキュア認証が確実に行われるようにするには、ユーザが HTTP 要求を送信した場合でも、ログインページは必ず HTTPS（セキュア HTTP）形式になるようにします。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

## 認証プロキシ Web ページのカスタマイズ

Web ベースの認証中、デバイスのデフォルト HTML ページではなく、代わりの HTML ページがユーザに表示されるように、Web 認証を設定できます。

カスタム認証プロキシ Web ページの使用を指定するには、次の手順を実行してください。

### 始める前に

デバイスのフラッシュ メモリにカスタム HTML ファイルを保存します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例： | 特権 EXEC モードを有効にします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス> **enable** | • パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip admission proxy http login page file** *device:login-filename*<br>例：<br>デバイス(config)# **ip admission proxy http login page file disk1:login.htm** | デバイスのメモリ ファイル システム内で、デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの場所を指定します。*device:* はフラッシュ メモリです。 |
| ステップ 4 | **ip admission proxy http success page file** *device:success-filename*<br>例：<br>デバイス(config)# **ip admission proxy http success page file disk1:success.htm** | デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。 |
| ステップ 5 | **ip admission proxy http failure page file** *device:fail-filename*<br>例：<br>デバイス(config)# **ip admission proxy http fail page file disk1:fail.htm** | デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。 |
| ステップ 6 | **ip admission proxy http login expired page file** *device:expired-filename*<br>例：<br>デバイス(config)# **ip admission proxy http login expired page file disk1:expired.htm** | デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。 |
| ステップ 7 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

## 成功ログインに対するリダイレクション URL の指定

認証後に内部成功 HTML ページを効果的に置き換えユーザのリダイレクト先となる URL を指定するためには、次の手順を実行してください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip admission proxy http success redirect** *url-string*<br>例：<br>デバイス(config)# **ip admission proxy http success redirect www.example.com** | デフォルトのログイン成功ページの代わりにユーザをリダイレクトする URL を指定します。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

# Web ベース認証パラメータの設定

クライアントが待機時間中にウォッチリストに掲載されるまで許容される失敗ログイン試行の最大回数を設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例： | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device> enable` | |
| ステップ 2 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip admission max-login-attempts** *number*<br>例：<br>`Device(config)# ip admission max-login-attempts 10` | 失敗ログイン試行の最大回数を設定します。指定できる範囲は 1 ～ 2147483647 回です。デフォルトは 5 分です。 |
| ステップ 4 | **exit**<br>例：<br>`Device# exit` | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

# Web ベースの認証ローカル バナーの設定

Web 認証が設定されているスイッチにローカル バナーを設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`デバイス> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`デバイス# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip admission auth-proxy-banner http** [*banner-text* \| *file-path*]<br>例： | ローカルバナーをイネーブルにします。<br>（任意）*C banner-text C*（*C* は区切り文字）、またはバナーに表示されるファイ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config)# **ip admission auth-proxy-banner http C My Switch C** | ル（たとえば、ロゴまたはテキストファイル）のファイル パスを入力して、カスタム バナーを作成します。 |
| ステップ 4 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 6 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# Web ベース認証キャッシュ エントリの削除

Web ベース認証キャッシュ エントリを削除するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **clear ip auth-proxy cache** {* \| *host ip address*}<br>例：<br>デバイス# **clear ip auth-proxy cache 192.168.4.5** | Delete 認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **clear ip admission cache** {* \| *host ip address*}<br>例：<br>デバイス# **clear ip admission cache 192.168.4.5** | Delete 認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。 |

# Web ベース認証ステータスの確認

すべてのインターフェイスまたは特定のポートに対する Web ベース認証設定を表示するには、このトピックのコマンドを使用します。

表 *38 :* 特権 *EXEC* 表示コマンド

| コマンド | 目的 |
|---|---|
| **show authentication sessions method webauth** | FastEthernet、ギガビット イーサネット、または 10 ギガビット イーサネットのすべてのインターフェイスに対する Web ベースの認証設定を表示します。 |
| **show wireless client mac-address** *a.a.a* **detail** | セッション固有のワイヤレス情報とワイヤレス状態を表示します。 |
| **show authentication sessions interface** *type slot/port*[**details**] | FastEthernet、ギガビット イーサネット、または 10 ギガビット イーサネットの特定のインターフェイスに対する Web ベースの認証設定を表示します。<br>セッション認識型ネットワーク モードでは、**show access-session interface** コマンドを使用します。 |

第 21 章

# ポート単位のトラフィック制御の設定


- ポートベースのトラフィック制御の概要 （483 ページ）


# ポートベースのトラフィック制御の概要

ポート ベースのトラフィック制御は、特定トラフィック状態に応じてポート レベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。次のポートベースのトラフィック制御機能がサポートされています。

- ストーム制御
- 保護ポート
- ポート ブロッキング
- ポート セキュリティ
- プロトコル ストーム プロテクション

## ストーム制御に関する情報

### ストーム制御

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム コントロール（またはトラフィック抑制）は、インターフェイスからスイッチングバスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

## トラフィック アクティビティの測定方法

ストーム コントロールは、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 秒単位で受信するビット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 小さいフレームのトラフィック レートの秒単位のパケット数。この機能は、グローバルにイネーブルです。小さいフレームのしきい値は、各インターフェイスで設定されます。

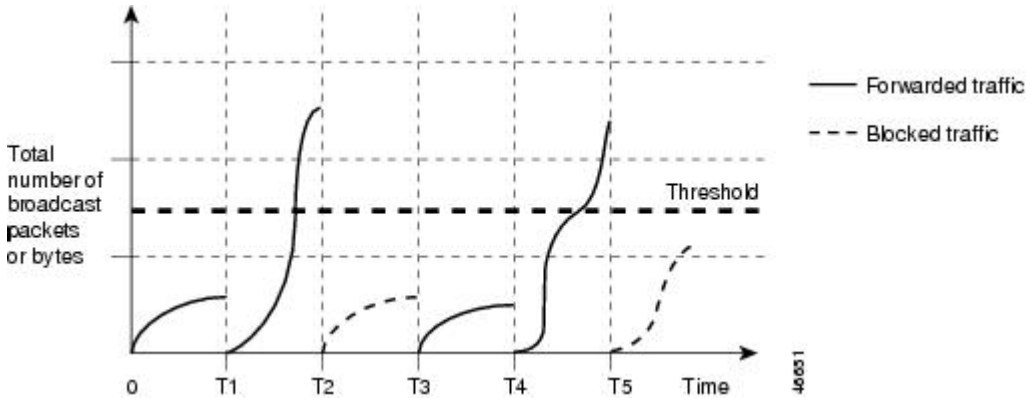
上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

（注） マルチキャストトラフィックのストーム制御しきい値に達した場合、ブリッジプロトコルデータ ユニット（BPDU）および Cisco Discovery Protocol フレームなどの制御トラフィック以外のマルチキャストトラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

## トラフィック パターン

**図 *31 :* ブロードキャスト ストーム制御の例**

次の例は、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。




T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。したがって、T2 と T5 の後のインターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過できるパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。

（注） パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィックタイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

# ストーム制御の設定方法

## ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数 % の差異が生じる可能性があります。

（注） ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、次の手順を実行します。

### 始める前に

ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet1/0/1** | 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **storm-control** {**broadcast** \| **multicast** \| **unicast**} **level** {*level* [*level-low*] \| **bps** *bps* [*bps-low*] \| **pps** *pps* [*pps-low*]}<br>例：<br>デバイス(config-if)# **storm-control unicast level 87 65** | ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。<br>キーワードの意味は次のとおりです。<br>• *level* には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。上限しきい値に到達すると、ポートはトラ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | フィックをブロックします。指定できる範囲は 0.00 ～ 100.00 です。<br>• （任意）*level-low* には、下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第 2 位まで）。この値は上限抑制値より小さいか、または等しくなければなりません。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ～ 100.00 です。<br>しきい値に最大値（100%）を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。<br>• **bps** *bps* には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをビット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。<br>• （任意）*bps-low* には、下限しきい値レベルをビット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ～ 10000000000.0 です。<br>• **pps** *pps* には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをパケット/秒で指定します（小 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。<br>• （任意）*pps-low* には、下限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は **0.0 ～** 10000000000.0 です。<br><br>BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号（k、m、g など）を使用できます。 |
| ステップ **5** | **storm-control action** {**shutdown** \| **trap**}<br>例：<br>デバイス(config-if)# **storm-control action trap** | ストーム検出時に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。<br>• ストーム中、ポートを errdisable の状態にするには、**shutdown** キーワードを選択します。<br>• ストームが検出された場合、SNMP トラップを生成するには、**trap** キーワードを選択します。 |
| ステップ **6** | **end**<br>例：<br>デバイス(config-if)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ **7** | **show storm-control** [*interface-id*] [**broadcast** \| **multicast** \| **unicast**]<br>例：<br>デバイス# **show storm-control gigabitethernet1/0/1 unicast** | 指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しない場合は、すべてのトラフィック タイプ（ブロードキャスト、マルチキャスト、ユニキャスト）の詳細が表示されます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 8 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# 保護ポートに関する情報

## 保護ポート

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ2トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャストトラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータ トラフィックは、レイヤ3デバイスを介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

スイッチ スタックは論理的には1つのスイッチを表しているため、レイヤ2トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチ スタックの保護ポート間では転送されません。

## 保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

## 保護ポートのガイドライン

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

# 保護ポートの設定方法

## 保護ポートの設定

### 始める前に

保護ポートは事前定義されていません。これは設定する必要があるタスクです。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/0/1** | 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **switchport protected**<br>例：<br>デバイス(config-if)# **switchport protected** | インターフェイスを保護ポートとして設定します。 |
| ステップ 5 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show interfaces** *interface-id* **switchport**<br>例：<br>デバイス# **show interfaces** | 入力を確認します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `gigabitethernet 1/0/1 switchport` | |
| ステップ 7 | **show running-config**<br>例：<br>デバイス# `show running-config` | 入力を確認します。 |
| ステップ 8 | **copy running-config startup-config**<br>例：<br>デバイス# `copy running-config startup-config` | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# 保護ポートの監視

表 *39 :* 保護ポートの設定を表示するコマンド

| コマンド | 目的 |
|---|---|
| **show interfaces** [*interface-id*] **switchport** | すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。 |

# ポート ブロッキングに関する情報

## ポート ブロッキング

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャスト トラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにします。

（注） マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

# ポート ブロッキングの設定方法

## インターフェイスでのフラッディング トラフィックのブロッキング

### 始める前に

インターフェイスは物理インターフェイスまたはEtherChannelグループのいずれも可能です。ポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/0/1** | 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **switchport block multicast**<br>例：<br>デバイス(config-if)# **switchport block multicast** | ポートからの未知のマルチキャストの転送をブロックします。 |
| ステップ 5 | **switchport block unicast**<br>例：<br>デバイス(config-if)# **switchport block unicast** | ポートからの未知のユニキャストの転送をブロックします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show interfaces** *interface-id* **switchport**<br>例：<br>デバイス# **show interfaces gigabitethernet 1/0/1 switchport** | 入力を確認します。 |
| ステップ 8 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 9 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# ポート ブロッキングの監視

表 *40*：ポート ブロッキングの設定を表示するコマンド

| コマンド | 目的 |
|---|---|
| **show interfaces** [*interface-id*] **switchport** | すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロッキングおよびポート保護の設定を含めて表示します。 |

# ポート セキュリティの前提条件

（注） 最大値をインターフェイス上ですでに設定されているセキュアアドレスの数より小さい値に設定しようとすると、コマンドが拒否されます。

# ポート セキュリティの制約事項

- スイッチまたはスイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management（SDM）テンプレートによって決められます。この値は、使用可能な MAC アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数を表します。
- ポートセキュリティは、EtherChannel インターフェイスではサポートされていません。

# ポート セキュリティの概要

## ポート セキュリティ

ポート セキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレス グループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュア ポートとしてポートを設定し、セキュア MAC アドレスが最大数に達した場合、ポートにアクセスを試みるステーションの MAC アドレスが識別されたセキュア MAC アドレスのいずれとも一致しないので、セキュリティ違反が発生します。また、あるセキュア ポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュア ポートにアクセスしようとしたときにも、違反のフラグが立てられます。

## セキュア MAC アドレスのタイプ

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- スタティックセキュア MAC アドレス：**switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレステーブルに保存された後、スイッチの実行コンフィギュレーションに追加されます。
- ダイナミック セキュア MAC アドレス：動的に設定されてアドレス テーブルにのみ保存され、スイッチの再起動時に削除されます。

- スティッキー セキュア MAC アドレス：動的に学習することも、手動で設定することもできます。アドレステーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

## スティッキ セキュア MAC アドレス

スティッキー ラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキー セキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。インターフェイスはスティッキ ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキー セキュア MAC アドレスに変換します。すべてのスティッキー セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキー セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション）に、自動的には反映されません。スティッキー セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキ セキュア アドレスを保存しない場合、アドレスは失われます。

スティッキ ラーニングがディセーブルの場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

## セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレス テーブルに追加されている状態で、アドレス テーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。
- ポートセキュリティが有効な状態で診断テストを実行しています。

違反が発生した場合の対処に基づいて、次の 3 種類の違反モードのいずれかにインターフェイスを設定できます。

- protect（保護）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。

（注） トランク ポートに protect 違反モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していなくてもVLANが保護モードの最大数に達すると、ラーニングがディセーブルになります。

- restrict（制限）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
- shutdown（シャットダウン）：ポート セキュリティ違反により、インターフェイスが error-disabled になり、ただちにシャットダウンされます。そのあと、ポートの LED が消灯します。セキュアポートが error-disabled 状態の場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこの状態を解消するか、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して手動で再度有効にできます。これは、デフォルトのモードです。
- shutdown vlan（VLAN シャットダウン）：VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。

次の表に、ポートセキュリティをインターフェイスに設定した場合の違反モードおよび対処について示します。

表 *41* : セキュリティ違反モードの処置

| 違反モード | トラフィックの転送 [16] | SNMP トラップの送信 | Syslog メッセージの送信 | エラー メッセージの表示 [17] | 違反カウンタの増加 | ポートのシャットダウン |
|---|---|---|---|---|---|---|
| protect | x | x | x | x | x | x |
| restrict | x | 対応 | 対応 | x | ○ | X |
| シャットダウン | x | x | x | x | 対応 | 対応 |
| shutdown vlan | x | x | ○ | x | ○ | X [18] |

[16] 十分な数のセキュアMACアドレスを削除するまで未知の送信元アドレスを持つパケットがドロップされます。

[17] セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラー メッセージを返します。

[18] 違反が発生した VLAN のみシャットダウンします。

## ポート セキュリティ エージング

ポート上のすべてのセキュア アドレスにエージング タイムを設定するには、ポート セキュリティ エージングを使用します。ポートごとに2つのタイプのエージングがサポートされています。

- absolute：指定されたエージング タイムの経過後に、ポート上のセキュア アドレスが削除されます。
- inactivity：指定されたエージングタイムの間、セキュアアドレスが非アクティブであった場合に限り、ポート上のセキュア アドレスが削除されます。

## ポート セキュリティとスイッチ スタック

スタックに新規に加入したスイッチは、設定済みのセキュア アドレスを取得します。他のスタック メンバーから新しいスタック メンバーに、ダイナミック セキュア アドレスがすべてダウンロードされます。

スイッチ（アクティブ スイッチまたはスタック メンバのいずれか）がスタックから離れると、その他のスタック メンバに通知が行き、そのスイッチが設定または学習したセキュア MAC アドレスがセキュア MAC アドレス テーブルから削除されます。

## デフォルトのポート セキュリティ設定

表 *42*：デフォルトのポート セキュリティ設定

| 機能 | デフォルト設定 |
|---|---|
| ポート セキュリティ | ポート上でディセーブル |
| スティッキー アドレス ラーニング | ディセーブル |
| ポートあたりのセキュア MAC アドレスの最大数 | 1。 |
| 違反モード | shutdown。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。 |
| ポート セキュリティ エージング | ディセーブルエージング タイムは 0<br>スタティック エージングはディセーブル<br>タイプは absolute |

## ポート セキュリティの設定時の注意事項

- ポート セキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートをダイナミック アクセス ポートにすることはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- 音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュア アドレスを設定する必要があります。
- トランクポートがポートセキュリティで設定され、データトラフィック用のアクセスVLANと音声トラフィック用の音声 VLAN に割り当てられている場合、**switchport voice** およびインターフェイス コンフィギュレーション コマンドを入力して **switchport priority extend** も効果はありません。

  接続装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレス、音声 VLAN の IP アドレスの順に要求すると、アクセス VLAN だけが IP アドレスに割り当てられます。
- インターフェイスの最大セキュア アドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングをサポートしていません。

次の表に、他のポートベース機能と互換性のあるポート セキュリティについてまとめます。

**表 *43*：ポート セキュリティと他のポートベース機能との互換性**

| ポート タイプまたはポートの機能 | ポート セキュリティとの互換性 |
|---|---|
| DTP [19] ポート [20] | なし |
| トランク ポート | あり |
| ダイナミックアクセスポート[21] | なし |
| ルーテッド ポート | なし |
| SPAN 送信元ポート | あり |

| ポート タイプまたはポートの機能 | ポート セキュリティとの互換性 |
|---|---|
| SPAN 宛先ポート | なし |
| EtherChannel | X |
| トンネリング ポート | あり |
| 保護ポート | あり |
| IEEE 802.1x ポート | あり |
| 音声 VLAN ポート[22] | あり |
| IP ソース ガード | あり |
| ダイナミック アドレス解決プロトコル（ARP）インスペクション | あり |
| Flex Link | 対応 |

[19] DTP = Dynamic Trunking Protocol

[20] **switchport mode dynamic** インターフェイス コンフィギュレーション コマンドで設定されたポート A。

[21] **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドで設定される VLAN Query Protocol（VQP）ポート。

[22] ポートに最大限可能なセキュアなアドレスを設定します（アクセス VLAN で可能なセキュアなアドレスの最大数に 2 を加えた数）。

## ポートベースのトラフィック制御の概要

ポート ベースのトラフィック制御は、特定トラフィック状態に応じてポート レベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。次のポートベースのトラフィック制御機能がサポートされています。

- ストーム制御
- 保護ポート
- ポート ブロッキング
- ポート セキュリティ
- プロトコル ストーム プロテクション

# ポート セキュリティの設定方法

## ポート セキュリティのイネーブル化および設定

### 始める前に

このタスクは、ポートにアクセスできるステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制約します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet1/0/1** | 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **switchport mode** {**access** \| **trunk**}<br>例：<br>デバイス(config-if)# **switchport mode access** | インターフェイス スイッチポート モードを access または trunk に設定します。デフォルト モード（dynamic auto）のインターフェイスは、セキュア ポートとして設定できません。 |
| ステップ 5 | **switchport voice vlan** *vlan-id*<br>例：<br>デバイス(config-if)# **switchport voice vlan 22** | ポート上で音声 VLAN をイネーブルにします。<br>vlan-id：音声トラフィックに使用する VLAN を指定します。 |
| ステップ 6 | **switchport port-security**<br>例： | インターフェイス上でポートセキュリティをイネーブルにします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if)# **switchport port-security** | （注） 特定の条件下では、スイッチスタックのメンバーポートでポートセキュリティが有効になっていると、DHCPおよびARPパケットがドロップされます。これを解決するには、インターフェイスで shut と no shut を設定します。 |
| ステップ **7** | **switchport port-security [maximum** *value* [**vlan** {*vlan-list* \| {**access** \| **voice**}}]]<br>例：<br>デバイス(config-if)# **switchport port-security maximum 20** | （任意）インターフェイスの最大セキュアMACアドレス数を設定します。スイッチまたはスイッチスタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されているMACアドレスの最大数によって決まります。この値は、アクティブな SDM テンプレートによって決まります。この値は、使用可能なMACアドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュアMACアドレスで使用される MAC アドレスを含む）の総数を表します。<br>（任意）**vlan**：VLAN 当たりの最大値を設定します。<br>**vlan** キーワードを入力後、次のいずれかのオプションを入力します。<br>• *vlan-list*：トランク ポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、VLAN 単位の最大値を設定できます。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。<br>• **access**：アクセス ポートで、VLAN をアクセス VLAN として指定します。<br>• **voice**：アクセス ポートで、VLAN を音声 VLAN として指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。 |
| ステップ **8** | **switchport port-security violation** {**protect** \| **restrict** \| **shutdown** \| **shutdown vlan**}<br>例：<br>デバイス(config-if)# **switchport port-security violation restrict** | （任意）違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。<br>• **protect**：ポート セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。<br>（注） トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。<br>• **restrict**：セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。セキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きま |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | す。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。<br>• **shutdown**：違反が発生すると、インターフェイスが error-disabled になり、ポートの LED が消灯します。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。<br>• **shutdown vlan**：VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。<br>（注） セキュア ポートが error-disabled ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーションコマンドを入力して、このステートから回復させることができます。手動で再びイネーブルにするには、**shutdown** および **no shutdown** インターフェイス コンフィギュレーションコマンドを入力するか、**clear errdisable interface vlan** 特権 EXEC コマンドを入力します。 |
| ステップ 9 | **switchport port-security [mac-address** *mac-address* [**vlan** {*vlan-id* \| {**access** \| **voice**}}]<br>例：<br>デバイス(config-if)# **switchport** | （任意）インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定したセキュア MAC アドレスが最大数よ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice` | り少ない場合、残りの MAC アドレスは動的に学習されます。<br>（注） このコマンドの入力後にスティッキー ラーニングをイネーブルにすると、動的に学習されたセキュアアドレスがスティッキー セキュア MAC アドレスに変換されて実行コンフィギュレーションに追加されます。<br>（任意）**vlan**：VLAN 当たりの最大値を設定します。<br>**vlan** キーワードを入力後、次のいずれかのオプションを入力します。<br>• *vlan-id*：トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。<br>• **access**：アクセス ポートで、VLAN をアクセス VLAN として指定します。<br>• **voice**：アクセス ポートで、VLAN を音声 VLAN として指定します。<br>（注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。 |
| ステップ 10 | **switchport port-security mac-address sticky**<br>例： | （任意）インターフェイス上でスティッキラーニングをイネーブルにします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス(config-if)# **switchport port-security mac-address sticky** | |
| ステップ 11 | **switchport port-security mac-address sticky** [*mac-address* \| **vlan** {*vlan-id* \| {**access** \| **voice**}}]<br>例：<br>デバイス(config-if)# **switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice** | （任意）スティッキー セキュア MAC アドレスを入力し、必要な回数だけコマンドを繰り返します。設定したセキュア MAC アドレスの数が最大数より少ない場合、残りの MAC アドレスは動的に学習されてスティッキー セキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。<br>（注） このコマンドの入力前にスティッキー ラーニングをイネーブルにしないと、エラーメッセージが表示されてスティッキー セキュア MAC アドレスを入力できません。<br>（任意）**vlan**：VLAN 当たりの最大値を設定します。<br>**vlan** キーワードを入力後、次のいずれかのオプションを入力します。<br>• *vlan-id*：トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。<br>• **access**：アクセス ポートで、VLAN をアクセス VLAN として指定します。<br>• **voice**：アクセス ポートで、VLAN を音声 VLAN として指定します。<br>（注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 12 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 13 | **show port-security**<br>例：<br>デバイス# **show port-security** | 入力を確認します。 |
| ステップ 14 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 15 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーションファイルに設定を保存します。 |

## ポート セキュリティ エージングのイネーブル化および設定

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュアポート上のデバイスを削除および追加し、なおかつポート上のセキュアアドレス数を制限できます。セキュアアドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **interface** *interface-id*<br>例：<br>デバイス(config)# **interface gigabitethernet 1/0/1** | 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **switchport port-security aging** {**static** \| **time** *time* \| **type** {**absolute** \| **inactivity**}}<br>例：<br>デバイス(config-if)# **switchport port-security aging time 120** | セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにします。またはエージング タイムやタイプを設定します。<br>（注） スイッチは、スティッキー セキュア アドレスのポート セキュリティ エージングをサポートしていません。<br>このポートに、スタティックに設定されたセキュアアドレスのエージングをイネーブルにする場合は、**static** を入力します。<br>*time* には、このポートのエージング タイムを指定します。指定できる範囲は、0 ～ 1440 分です。<br>**type** には、次のキーワードのいずれか 1 つを選択します。<br>• **absolute**：（任意）エージング タイプを絶対エージングとして設定します。このポートのセキュア アドレスはすべて、指定した時間（分単位）が経過すると期限切れになり、セキュア アドレス リストから削除されます。<br>• **inactivity**：（任意）エージング タイプを非アクティブ エージングとして設定します。指定された time 期間中にセキュア送信元アドレスからのデータ トラフィックがない場合に限り、このポートのセキュア アドレスが期限切れになります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show port-security** [ **interface** *interface-id*] [**address**]<br>例：<br>デバイス# **show port-security interface gigabitethernet 1/0/1** | 入力を確認します。 |
| ステップ 7 | **show running-config**<br>例：<br>デバイス# **show running-config** | 入力を確認します。 |
| ステップ 8 | **copy running-config startup-config**<br>例：<br>デバイス# **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# ポート セキュリティの設定例

次に、ポート上でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する例を示します。違反モードはデフォルトです。スタティック セキュア MAC アドレスは設定せず、スティッキー ラーニングはイネーブルです。

```
デバイス(config)# interface gigabitethernet 1/0/1
デバイス(config-if)# switchport mode access
デバイス(config-if)# switchport port-security
デバイス(config-if)# switchport port-security maximum 50
デバイス(config-if)# switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 上にスタティック セキュア MAC アドレスを設定する例を示します。

```
デバイス(config)# interface gigabitethernet 1/0/2
デバイス(config-if)# switchport mode trunk
デバイス(config-if)# switchport port-security
デバイス(config-if)# switchport port-security mac-address 0000.0200.0004 vlan 3
```

次に、ポートのスティッキー ポート セキュリティをイネーブルにする例を示します。データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュア アドレスの総数を 20 に設定します（データ VLAN に 10、音声 VLAN に 10 を割り当てます）。

```
デバイス(config)# interface tengigabitethernet 1/0/1
デバイス(config-if)# switchport access vlan 21
デバイス(config-if)# switchport mode access
デバイス(config-if)# switchport voice vlan 22
デバイス(config-if)# switchport port-security
デバイス(config-if)# switchport port-security maximum 20
デバイス(config-if)# switchport port-security violation restrict
デバイス(config-if)# switchport port-security mac-address sticky
デバイス(config-if)# switchport port-security mac-address sticky 0000.0000.0002
デバイス(config-if)# switchport port-security mac-address 0000.0000.0003
デバイス(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice

デバイス(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
デバイス(config-if)# switchport port-security maximum 10 vlan access
デバイス(config-if)# switchport port-security maximum 10 vlan voice
```

# プロトコル ストーム プロテクションに関する情報

## プロトコル ストーム プロテクション

スイッチがアドレス解決プロトコル（ARP）または制御パケットでフラッドされると、CPU の高い使用率により CPU のオーバーロードが発生する可能性があります。これらの問題は、次のように発生します。

- プロトコル制御パケットが受信されず、ネイバーの隣接がドロップされるため、ルーティング プロトコルがフラップする場合があります。
- スパニングツリー プロトコル（STP）ブリッジ プロトコル データ ユニット（BPDU）が送受信されないため、STP が再収束します。
- CLI が遅くなるか応答しなくなります。

プロトコル ストーム プロテクションを使用すると、パケットのフロー レートの上限しきい値を指定して、制御パケットが送信されるレートを制御できます。サポートされるプロトコルは、ARP、ARP スヌーピング、Dynamic Host Configuration Protocol（DHCP）v4、DHCP スヌーピング、インターネット グループ管理プロトコル（IGMP）、および IGMP スヌーピングです。

パケットのレートが定義されたしきい値を超えると、スイッチは指定されたポートに着信したすべてのトラフィックを 30 秒間ドロップします。パケット レートが再度計測され、必要な場合はプロトコル ストーム プロテクションが再度適用されます。

より強力な保護が必要な場合は、仮想ポートを手動で errdisable にし、その仮想ポートのすべての着信トラフィックをブロックできます。また、手動で仮想ポートをイネーブルにしたり、仮想ポートの自動再イネーブル化の時間間隔を設定することもできます。

（注） 超過したパケットは、2 つ以下の仮想ポートにおいてドロップされます。

仮想ポートのエラー ディセーブル化は、EtherChannel インターフェイスと Flexlink インターフェイスではサポートされません。

## デフォルトのプロトコル ストーム プロテクションの設定

プロトコル ストーム プロテクションはデフォルトでディセーブルです。これがイネーブルになると、仮想ポートの自動リカバリがデフォルトでディセーブルになります。

# プロトコル ストーム プロテクションの設定方法

## プロトコル ストーム プロテクションのイネーブル化

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **psp** {**arp** \| **dhcp** \| **igmp**} pps *value*<br>例：<br>デバイス(config)# **psp dhcp pps 35** | ARP、IGMP、または DHCP に対してプロトコル ストーム プロテクションを設定します。<br>*value* には、1 秒あたりのパケット数のしきい値を指定します。トラフィックがこの値を超えると、プロトコル ストーム プロテクションが適用されます。範囲は毎秒 5 ～ 50 パケットです。 |
| ステップ 4 | **errdisable detect cause psp**<br>例：<br>デバイス(config)# **errdisable detect** | （任意）プロトコル ストーム プロテクションの errdisable 検出をイネーブルにします。この機能がイネーブルになると、仮想ポートが errdisable になります。この機能がディセーブルになると、 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | **cause psp** | そのポートは、ポートを errdisable にせずに超過したパケットをドロップします。 |
| ステップ 5 | **errdisable recovery interval** *time*<br>例：<br>デバイス | （任意）errdisable の仮想ポートの自動リカバリ時間を秒単位で設定します。仮想ポートが errdisable の場合、この時間を過ぎるとスイッチは自動的にリカバリします。指定できる範囲は 30 ～ 86400 秒です。 |
| ステップ 6 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show psp config** {**arp** \| **dhcp** \| **igmp**}<br>例：<br>デバイス# **show psp config dhcp** | 入力を確認します。 |

# プロトコル ストーム プロテクションのモニタリング

| コマンド | 目的 |
|---|---|
| **show psp config** {**arp** \| **dhcp** \| **igmp**} | 入力内容を確認します。 |

# ポートベースのトラフィック制御に関するその他の関連資料

### MIB

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

### シスコのテクニカル サポート

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

第 22 章

# Cisco TrustSec の設定


- Cisco TrustSec の概要 （513 ページ）
- Cisco TrustSec の機能 （513 ページ）
- Cisco TrustSec の機能情報 （517 ページ）


## Cisco TrustSec の概要

Cisco TrustSec は、ネットワーク内のユーザ、ホスト、およびネットワーク デバイスを強力に識別する機能に基づいた、シスコ ネットワーク デバイスのセキュリティを改善します。TrustSec は、特定の役割についてデータ トラフィックを一意に分類することで、トポロジに依存しない、スケーラブルなアクセス コントロールを実現します。TrustSec は、認証されたピアおよびこれらのピアとの暗号化リンク間で信頼を確立することで、データの機密保持および整合性を保証します。

Cisco TrustSec の主要コンポーネントは、Cisco Identity Services Engine（ISE）です。スイッチ上で手動で設定することもできますが、Cisco ISE は TrustSec ID およびセキュリティ グループ ACL（SGACL）でスイッチをプロビジョニングできます。

## Cisco TrustSec の機能

次の表に、TrustSec がイネーブルになった Cisco スイッチで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability リリースによって、サポートされるスイッチの数および各スイッチでサポートされる TrustSec 機能の数は増加しています。

| Cisco TrustSec の機能 | 説明 |
|---|---|
| 802.1AE タギング（MACSec） | IEEE 802.1AE に基づくワイヤレート ホップ単位レイヤ 2 暗号化のプロトコル。<br><br>MACSec 対応デバイス間において、パケットは送信デバイスからの出力で暗号化され、受信デバイスへの入力で復号化されます。デバイス内では平文です。<br><br>この機能は、TrustSec ハードウェア対応デバイス間だけで利用できます。<br><br>（注） この機能は、Catalyst 3850 および Catalyst 3650 スイッチではサポートされていません。 Cisco IOS XE Denali 16.1.1<br><br>（注） この機能は 2960x ではサポートされていません。 |
| エンドポイント アドミッション コントロール（EAC） | EAC は、TrustSec ドメインに接続しているエンドポイント ユーザまたはデバイスの認証プロセスです。通常、EAC はアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可に成功すると、ユーザまたはデバイスに対してセキュリティ グループ タグが割り当てられます。現在、EAC は 802.1X、MAC 認証バイパス（MAB）、および Web 認証プロキシ（WebAuth）とすることができます。 |
| ネットワーク デバイス アドミッション コントロール（NDAC） | NDAC は、TrustSec ドメイン内の各ネットワーク デバイスがピア デバイスのクレデンシャルおよび信頼性を確認できる認証プロセスです。NDAC は、IEEE 802.1X ポート ベースの認証に基づく認証フレームワークを利用し、EAP 方式として EAP-FAST を使用します。NDAC プロセスの認証および許可に成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションとなります。<br><br>（注） この機能は 2960x ではサポートされていません。 |

| Cisco TrustSec の機能 | 説明 |
|---|---|
| セキュリティ グループ アクセス コントロール リスト（SGACL） | セキュリティ グループ アクセス コントロール リスト（SGACL）は、セキュリティ グループ タグをポリシーと関連付けます。ポリシーは、TrustSec ドメインから出力される SGT タグ付きトラフィックに対して適用されます。<br>（注） この機能は、リリース 15.2(4) E の Catalyst 3560cx ではサポートされていません。 |
| Cisco TrustSec SGACL のハイ アベイラビリティ | Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）は、Cisco StackWise 技術をサポートしているスイッチでのハイ アベイラビリティ機能をサポートしています。Cisco StackWise 技術によってステートフルな冗長性が提供され、スイッチ スタックはアクセス制御エントリを強制し、処理できます。<br>この機能を有効にする Cisco TrustSec 固有の設定はありません。<br>この機能は、Cisco IOS XE Release Denali 16.2.1 以降で、Catalyst 3850 および 3650 シリーズ スイッチでのみサポートされます。 |
| セキュリティ アソシエーション プロトコル（SAP） | NDAC 認証のあと、セキュリティ アソシエーション プロトコル（SAP）は、その後の TrustSec ピア間の MACSec リンク暗号化のキーおよび暗号スイートについて、自動的にネゴシエーションを行います。SAP は IEEE 802.11i で定義されます。<br>（注） この機能は、Catalyst 3850 および Catalyst 3650 スイッチではサポートされていません。 Cisco IOS XE Denali 16.1.1<br>（注） この機能は 2960x ではサポートされていません。 |

| Cisco TrustSec の機能 | 説明 |
|---|---|
| セキュリティ グループ タグ（SGT） | SGT は、TrustSec ドメイン内の送信元のセキュリティ分類を示す 16 ビットの単一ラベルです。イーサネット フレームまたは IP パケットに追加されます。<br>（注） この機能は、Catalyst 2960cx および Catalyst 3560cx ではサポートされていません。 |
| SGT Exchange Protocol（SXP） | Security Group Tag Exchange Protocol（SXP）。SXP を使用すると、TrustSec にハードウェアで対応していないデバイスが Cisco Identity Services Engine（ISE）または Cisco Secure アクセス コントロール システム（ACS）から認証されたユーザとデバイスの SGT 属性を受信できます。デバイスは、次にセキュリティ グループ アクセス コントロール リスト（SGACL）強制のために、送信元トラフィックをタグ付けする TrustSec にハードウェアで対応しているデバイスに、sourceIP-to-SGT バインディングを転送できます。 |

リンクの両端で 802.1AE MACsec をサポートしている場合、SAP ネゴシエーションが実行されます。サプリカントとオーセンティケータの間で EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティパラメータの交換、およびキーの管理が実行されます。これらの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョンとライセンスおよびリンク ハードウェア サポートに応じて、SAP ネゴシエーションは次の動作モードの 1 つを使用できます。

- Galois Counter Mode（GCM）：認証と暗号化
- GCM authentication（GMAC）：GCM 認証、暗号化なし
- No Encapsulation：カプセル化なし（クリア テキスト）
- null：カプセル化、認証または暗号化なし

# Cisco TrustSec の機能情報

表 *44 : Cisco TrustSec* の機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| • NDAC<br>• SXPv1、SXPv2<br>• SGT<br>• SGACL レイヤ 2 の適用<br>• SGT および VLAN から SGT へのマッピングのインターフェイス<br>• サブネットと SGT のマッピング<br>• レイヤ 3 ポート マッピング（PM）<br>• レイヤ 3 アイデンティティ ポート マッピング（IPM）<br>• セキュリティグループ名のダウンロード<br>• SXP ループ検出<br>• ポリシーベースの CoA | Cisco IOS XE 3.3SE | これらの機能が Catalyst 3850 および 3650 スイッチに追加されました。 |

第 23 章

# コントロール プレーン ポリシングの設定


- CoPP の制約事項 （519 ページ）
- CoPP の概要 （520 ページ）
- CoPP の設定方法 （525 ページ）
- CoPP の設定例 （530 ページ）
- CoPP のモニタリング （536 ページ）
- CoPP の機能履歴と情報 （536 ページ）


## CoPP の制約事項

コントロール プレーン ポリシング（CoPP）の制約事項は、次のとおりです。

- 入力 CoPP だけがサポートされます。**system-cpp-policy** ポリシーマップは、入力方向でのみ、コントロール プレーン インターフェイスで使用可能です。
- コントロール プレーン インターフェイスにインストールできるのは、**system-cpp-policy** ポリシーマップのみです。
- **system-cpp-policy** ポリシーマップおよび 17 個のシステム定義のクラスは、変更または削除することはできません。
- **system-cpp-policy** ポリシーマップの下で許可されるのは、**police** アクションのみです。システム定義クラスのポリシングレートは、秒単位のパケット/秒（pps）でのみ設定する必要があります。ユーザ定義のクラスマップの場合は、ビット/秒（bps）のみで設定する必要があります。
- システム定義のクラスマップのポリサーを無効にしないこと、つまり **no police rate** *rate* **pps** コマンドを設定しないことを推奨します。これを行うと、CPU へのトラフィックが多い場合に、システム全体の正常性に影響します。さらに、システム定義のクラスマップのポリサーレートを無効にした場合でも、システム起動プロセスを保護するために、システムはシステムのブートアップ後にデフォルトのポリサーレートに自動的に戻ります。
- 1 つ以上の CPU キューがそれぞれのクラス マップの一部となります。複数の CPU キューが 1 つのクラスマップに属している場合、クラスマップのポリサー レートを変更すると、そのクラス マップに属しているすべての CPU キューに影響します。同様に、クラスマッ

プでポリサーを無効にすると、そのクラスマップに属するすべてのキューが無効になります。各クラス マップに属する CPU キューの詳細については、表 45 : CoPP のシステム定義された値 （521 ページ） を参照してください。

- `system-cpp` ポリシーの下で設定されたクラスがデフォルト値のままの場合、それらのクラスに関する情報は **show run** コマンドで表示されません。代わりに **show policy-map system-cpp-policy** または **show policy-map control-plane** コマンドを使用します。

  引き続き **show run** コマンドを使用して、カスタムポリシーに関する情報を表示できます。

# CoPP の概要

この章では、コントロール プレーン ポリシング（CoPP）がdeviceで機能する仕組みと、その設定方法について説明します。

## CoPP の概要

CoPP 機能は、不要なトラフィックおよび DoS 攻撃から CPU を保護するdeviceのセキュリティを向上させます。また、他の優先順位の低い大量のトラフィックによって発生するトラフィックのドロップから、制御および管理トラフィックを保護することもできます。

deviceは通常、3 つの操作プレーンにセグメント化され、それぞれに独自の目的があります。

- データ パケットを転送するための、データ プレーン。
- データを適切にルーティングするための、コントロール プレーン。
- ネットワーク要素を管理するための、管理プレーン。

CoPP を使用することで、大半の CPU 行きトラフィックを保護し、ルーティングの安定性と信頼性を確保し、パケットを確実に配信することができます。特に重要なのは、DoS 攻撃から CPU を保護するために CoPP を使用できることです。

CoPP は、モジュラ QoS コマンドライン インターフェイス（MQC）および CPU キューを使用して、これらの目的を達成します。さまざまなタイプのコントロール プレーン トラフィックが特定の条件に基づいてグループ化され、CPU キューに割り当てられます。ハードウェアに専用のポリサーを設定することで、これらの CPU キューを管理できます。たとえば、特定の CPU キュー（トラフィック タイプ）のポリサー レートを変更したり、特定のタイプのトラフィックに対するポリサーを無効にしたりできます。

ポリサーはハードウェアに設定されていますが、CoPP は CPU のパフォーマンスやデータ プレーンのパフォーマンスには影響しません。しかし、CPU に着信するパケット数は制限されるため、CPU 負荷が制御されます。これは、ハードウェアからのパケットを待っているサービスが、より制御された着信パケットのレート（ユーザ設定可能なレート）を確認する可能性があることを意味します。

# システム定義の CoPP の特徴

deviceの初回の電源投入時は、システムによって次のタスクが自動的に実行されます。

- ポリシーマップ **system-cpp-policy** を検索します。見つからない場合、システムはそれを作成し、コントロールプレーンにインストールします。
- **system-cpp-policy** の下に 17 のクラスマップを作成します。

  次にdeviceの電源を入れたときに、すでに作成済みのポリシーとクラスマップがシステムによって検出されます
- デフォルトで、すべての CPU キューをそれぞれのデフォルトレートで有効にします。デフォルトのレートを「*CoPP* のシステム定義値」の表に示します。

次の表に、device をロードしたときにシステムが作成するクラスマップを示します。各クラスマップに対応するポリサーと、各クラスマップの下にグループ化された 1 つ以上の CPU キューを示します。ポリサーへのクラスマップの 1 対 1 のマッピングと、CPU キューへのクラスマップの 1 対多マッピングがあります。

**表 *45 : CoPP* のシステム定義された値**

| クラス マップ名 | ポリサー インデックス（ポリサー **No.**） | **CPU** キュー（キュー **No.**） | デフォルトのポリサーレート（**pps**） |
|---|---|---|---|
| system-cpp- police-data | WK_CPP_POLICE_DATA(0) | WK_CPU_Q_ICMP_GEN(3)<br>WK_CPU_Q_BROADCAST(12)<br>WK_CPU_Q_ICMP_REDIRECT (6) | 600<br>600<br>600 |
| system-cpp-police-l2-control | WK_CPP_POLICE_L2_CONTROL(1) | WK_CPU_Q_L2_CONTROL(1) | 2000 |
| system-cpp-police-routing-control | WK_CPP_POLICE_ROUTING_CONTROL(2) | WK_CPU_Q_ROUTING_CONTROL(4)<br>WK_CPU_Q_LOW_LATENCY (27) | 5400<br>5400 |
| system-cpp-police-control-low-priority | WK_CPP_POLICE_CONTROL_LOW_PRI(3) | WK_CPU_Q_GENERAL_PUNT(25) | 200 |
| system-cpp-police-punt-webauth | WK_CPP_POLICE_PUNT_WEBAUTH(7) | WK_CPU_Q_PUNT_WEBAUTH(22) | 1000 |
| system-cpp-police-topology-control | WK_CPP_POLICE_TOPOLOGY_CONTROL(8) | WK_CPU_Q_TOPOLOGY_CONTROL(15) | 13000 |
| system-cpp-police-multicast | WK_CPP_POLICE_MULTICAST(9) | WK_CPU_Q_TRANSIT_TRAFFIC(18)<br>WK_CPU_Q_MCAST_DATA(30) | 500<br>500 |

| クラス マップ名 | ポリサー インデックス（ポリサー No.） | CPU キュー（キュー No.） | デフォルトのポリサーレート（pps） |
|---|---|---|---|
| system-cpp-police-sys- data | WK_CPP_POLICE_SYS_DATA (10) | WK_CPU_Q_LEARNING_CACHE_OVFL(13)<br>WK_CPU_Q_CRYPTO_CONTROL(23)<br>WK_CPU_Q_EXCEPTION(24)<br>WK_CPU_Q_EGR_EXCEPTION(28)<br>WK_CPU_Q_NFL_SAMPLED_DATA(26)<br>WK_CPU_Q_GOLD_PKT(31)<br>WK_CPU_Q_RPF_FAILED(19) | 100<br>100<br>200<br>100<br>100<br>100<br>100 |
| system-cpp-police-dot1x-auth | WK_CPP_POLICE_DOT1X(11) | WK_CPU_Q_DOT1X_AUTH(0) | 1000 |
| system-cpp-police-protocol-snooping | WK_CPP_POLICE_PR | WK_CPU_Q_PROTO_SNOOPING(16) | 2000 |
| system-cpp-police-sw-forward | WK_CPP_POLICE_SW_FWD (13) | WK_CPU_Q_SW_FORWARDING_Q(14)<br>WK_CPU_Q_LOGGING(21)<br>WK_CPU_Q_L2_LVX_DATA_PACK (11) | 1000<br>1000<br>1000 |
| system-cpp-police-forus | WK_CPP_POLICE_FORUS(14) | WK_CPU_Q_FORUS_ADDR_RESOLUTION(5)<br>WK_CPU_Q_FORUS_TRAFFIC(2) | 1000<br>1000 |
| system-cpp-police-multicast-end-station | WK_CPP_POLICE_MULTICAST_STATION_SERVICE(6) | WK_CPU_Q_MCAST_END_STATION_SERVICE(20) | 2000 |
| **system-cpp-default** | WK_CPP_POLICE_DEFAULT_POLICER | WK_CPU_Q_DHCP_SNOOPING(17)<br>WK_CPU_Q_UNUSED (7)<br>WK_CPU_Q_EWLC_CONTROL(9)<br>WK_CPU_Q_EWLC_DATA(10) | 1000<br>1000<br>1000<br>1000 |
| system-cpp-police-stackwise-virt-control | WK_CPP_STACKWISE_VIRTUAL_CONTROL | WK_CPU_Q_STACKWISE_VIRTUAL_CONTROL (29) | 8000 |
| system-cpp-police-l2lvx-control | WK_CPP_ L2_LVX_CONT_PACK | WK_CPU_Q_L2_LVX_CONT_PACK(8) | 1000 |

# ユーザ設定可能な CoPP の特徴

次のタスクを実行して、コントロール プレーン トラフィックを管理できます。

（注） すべての ystem-cpp-policy コンフィギュレーションは、再起動後も保持されるように保存する必要があります。

### CPU キューのポリサーの有効化と無効化

CPU キューのポリサーを有効にするには、system-cpp-policy ポリシーマップ内で、対応するクラスマップの下にポリサーアクション（パケット/秒）を設定します。

CPU キューのポリサーを無効にするには、system-cpp-policy ポリシーマップ内で、対応するクラスマップの下のポリサーアクションを削除します。

（注） デフォルトのポリサーがすでに存在する場合は、その削除を慎重に考慮して制御します。そのようにしないと、システムが CPU ホグや制御パケットドロップなどのその他の異常を検出する場合があります。

### ポリサーレートの変更

これは、system-cpp-policy ポリシーマップ内で、対応するクラスマップの下にポリサーレートアクション（パケット/秒単位）を設定することで実行できます。

### ポリサーレートをデフォルトに設定

グローバル コンフィギュレーション モードで **cpp system-default** コマンドを入力することによって、CPU キューのポリサーをデフォルト値に設定します。

### ユーザ定義のクラスマップの作成

特定のトラフィッククラスに指定されたクラスマップがなく、このトラフィックを保護する場合は、そのようなトラフィックパケット用の特定のクラスマップ（フィルタ付き）を作成し、これらのユーザ定義のクラスマップを system-cpp-policy に追加できます。

system-cpp-policy が入力方向に適用されている間、転送エンジンドライバ（FED）はユーザ定義のクラスマップのポリサーを出力に変更します。したがって、すべてのユーザ定義クラスのフィルタとポリサーは、それぞれ出力分類とアクションとして適用する必要があります。ポリシーマップ自体は、この方向の変更による影響を受けません。

ユーザ定義のクラスマップを system-cpp-policy に追加すると、システムは自動的に（コントロールプレーンに加えて）32 個のすべての CPU キューにそれをインストールします。その結果、ポリシーのインスタンスは 33 個になります。これを確認するには、特権 EXEC モードで **show platform software fed switch** { *switch_number* } qos policy target status コマンドを入力します。

これらのクラスマップのポリシングレートは、アクティブキュー管理（AFD）ポリサーによって制御されます。AQM は、パケットをポートの送信キューに入れる前の、トラフィックフローのバッファ制御を提供し、特定のフローによるスイッチパケットメモリの占有が行われないよ

うにします。 AQM ポリサー機能が有効の場合、AQM ポリサーの制限を超えるユーザ定義のポリシングレートは無視されます。

ユーザ定義のクラスマップには、通常の QoS または ACL 分類フィルタがあります。

# ソフトウェアバージョンのアップグレードまたはダウングレード

## ソフトウェアバージョンのアップグレードと CoPP

デバイスのソフトウェアバージョンをアップグレードすると、システムは CoPP に必要な更新を確認して実行します（たとえば、`system-cpp-policy` ポリシーマップを確認し、欠落している場合は作成します）。また、アップグレードアクティビティの前後に特定のタスクを完了する必要があります。これにより、設定の更新が正しく反映され、CoPP が期待どおりに動作し続けることが保証されます。ソフトウェアのアップグレードに使用する方法に応じて、アップグレード関連のタスクはオプションのシナリオまたは推奨されるシナリオもあれば、必須のシナリオもあります。

ここでは、アップグレードのシステムアクションとユーザアクションについて説明します。また、リリース固有の警告も含まれます。

### アップグレードのシステムアクション

デバイスのソフトウェアバージョンをアップグレードすると、システムはこれらのアクションを実行します。これはすべてのアップグレード方法に適用されます。

- アップグレード前のデバイスに `system-cpp-policy` ポリシーマップがなかった場合、アップグレード時にシステムはデフォルトポリシーを作成します。
- アップグレード前のデバイスに `system-cpp-policy` ポリシーマップがあった場合、アップグレード時にシステムはポリシーを再生成しません。

### アップグレードのユーザアクション

アップグレードのユーザアクション（アップグレード方法に応じて）：

| アップグレード方法 | 条件 | アクション時間とアクション | 目的 |
|---|---|---|---|
| 標準[23] | なし（None） | **アップグレード後（必須）**<br>グローバルコンフィギュレーションモードで **cpp system-default** コマンドを入力します。 | 最新のデフォルトのポリサーレートを取得します。 |

[23] スイッチのリロードを伴うソフトウェアアップグレードの方法を指します。インストールモードまたはバンドルモードにすることができます。

## ソフトウェアバージョンのダウングレードと CoPP

ダウングレードのシステムアクションとユーザアクションについて、ここで説明します。

### ダウングレードのシステムアクション

デバイスのソフトウェアバージョンをダウングレードすると、これらのアクションが実行されます。これはすべてのダウングレード方法に適用されます。

- システムは `system-cpp-policy` ポリシーマップをデバイスに保持し、コントロールプレーンにインストールします。

### ダウングレードのユーザアクション

ダウングレードのユーザアクション：

| アップグレード方法 | 条件 | アクション時間とアクション | 目的 |
|---|---|---|---|
| 標準[24] | なし（None） | 操作は不要です。 | N/A |

[24] スイッチのリロードを伴うソフトウェアアップグレードの方法を指します。インストールモードまたはバンドルモードにすることができます。

ソフトウェアバージョンをダウングレードしてから再度アップグレードする場合、適用されるシステムアクションとユーザアクションは、アップグレードについて説明したものと同じです。

# CoPP の設定方法

## CPU キューの有効化またはポリサー レートの変更

CPU キューを有効にし、CPU キューのポリサー レートを変更する手順は、同じです。手順は次のとおりです。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例： | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | デバイス# **configure terminal** | |
| ステップ 3 | **policy-map** *policy-map-name*<br>例：<br>デバイス(config)# **policy-map system-cpp-policy**<br>デバイス(config-pmap)# | ポリシーマップ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **class** *class-name*<br>例：<br>デバイス(config-pmap)# **class system-cpp-police-protocol-snooping**<br>デバイス(config-pmap-c)# | クラス アクション コンフィギュレーションモードを開始します。有効にする CPU キューに対応するクラスの名前を入力します。「*CoPP* のシステム定義値」の表を参照してください。 |
| ステップ 5 | **police rate** *rate* **pps**<br>例：<br>デバイス(config-pmap-c)# **police rate 100 pps**<br>デバイス(config-pmap-c-police)# | 指定したトラフィック クラスに対し、1 秒間に処理される着信パケット数の上限を指定します。<br>（注） 指定するレートは、指定したクラスマップに属するすべての CPU キューに適用されます。 |
| ステップ 6 | exit<br>例：<br>デバイス(config-pmap-c-police)# **exit**<br>デバイス(config-pmap-c)# **exit**<br>デバイス(config-pmap)# **exit**<br>デバイス(config)# | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 7 | **control-plane**<br>例：<br>デバイス(config)# **control-plane**<br>デバイス(config-cp)# | 制御プレーン（config-cp）コンフィギュレーション モードを開始します。 |
| ステップ 8 | **service-policy input** *policy-name*<br>例：<br>デバイス(config)# **control-plane**<br>デバイス(config-cp)#**service-policy input system-cpp-policy**<br>デバイス(config-cp)# | system-cpp-policy を FED にインストールします。このコマンドは、FED ポリシーを表示するために必要です。このコマンドを設定しないと、エラーになります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 9 | **end**<br>例：<br>デバイス(config-cp)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 10 | **show policy-map control-plane**<br>例：<br>デバイス# **show policy-map control-plane** | system-cpp ポリシーの下で設定されたすべてのクラス、さまざまなトラフィックタイプに設定されたレート、および統計情報を表示します。 |

# CPU キューの無効化

CPU キューを無効にするには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **policy-map** *policy-map-name*<br>例：<br>デバイス(config)# **policy-map system-cpp-policy**<br>デバイス(config-pmap)# | ポリシー マップ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **class** *class-name*<br>例：<br>デバイス(config-pmap)# **class system-cpp-police-protocol-snooping**<br>デバイス(config-pmap-c)# | クラス アクション コンフィギュレーション モードを開始します。無効にする CPU キューに対応するクラスの名前を入力します。「*CoPP* のシステム定義値」の表を参照してください。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **no police rate** *rate* **pps**<br>例：<br>デバイス(config-pmap-c)# **no police rate 100 pps** | 指定したトラフィック クラスの着信パケットの処理を無効にします。<br>（注） これにより、指定したクラスマップに属するすべての CPU キューが無効になります。 |
| ステップ 6 | **end**<br>例：<br>デバイス(config-pmap-c)# **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show policy-map control-plane**<br>例：<br>デバイス# **show policy-map control-plane** | system-cpp ポリシーの下で設定されたすべてのクラス、およびさまざまなトラフィックタイプと統計情報に設定されたレートを表示します。 |

# すべての CPU キューに対するデフォルトのポリサー レートの設定

すべての CPU キューのポリサー レートをデフォルトのレートに設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **cpp system-default**<br>例：<br>デバイス(config)# **cpp system-default**<br>Defaulting CPP : Policer rate for all classes will be set to their defaults | すべてのクラスのポリサー レートをデフォルトのレートに設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | |
| ステップ 4 | **end**<br>例：<br>デバイス(config)# **end** | 特権 EXEC モードに戻ります。 |

# ユーザ定義のクラスマップの作成

system-cpp-policy でユーザ定義のクラスマップを作成し、ポリサーレートを bps で設定するには、次の手順に従ってください。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>デバイス> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>デバイス# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **class-map** *class-map-name*<br>例：<br>デバイス(config)# **class-map example_class**<br>デバイス(config-cmap)# | 作成するクラスマップを指定します。クラス マップ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **exit**<br>例：<br>Device(config-cmap)# **exit**<br>Device(config)# | クラス マップ コンフィギュレーション モードを終了します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **policy-map** *policy-map-name*<br>例：<br>`Device(config)# policy-map system-cpp-policy`<br>`Device(config-pmap)#` | ポリシー マップ名を入力します。ポリシー マップ コンフィギュレーション モードを開始します。 |
| ステップ 6 | **class-map** *class-map-name*<br>例：<br>`Device(config-pmap)# class example_class`<br>`Device(config-pmap-c)#` | クラス アクション コンフィギュレーション モードを開始します。クラスの名前を入力します。 |
| ステップ 7 | [**no**] **police rate** *target_bit_rate*<br>例：<br>`Device(config-pmap-c)# police 90000` | ビットレート/秒を指定し、8000 ～ 10000000000 の値を入力します。<br>（注） ユーザ定義のクラスマップのポリシングレートは、10000 pps 相当のトラフィックを超えることはできません。 |
| ステップ 8 | **end**<br>例：<br>`Device(config-pmap-c-police)# end`<br>`Device#` | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show policy-map control-plane**<br>例：<br>`Device# show policy-map control-plane` | `system-cpp` ポリシーの下で設定されたすべてのクラスを表示します。これには、ユーザ定義のクラスマップ、および設定されたレートが含まれます。 |

# CoPP の設定例

## 例：CPU キューの有効化または CPU キューのポリサー レートの変更

次の例に、CPU キューを有効にする方法、または CPU キューのポリサー レートを変更する方法を示します。ここでは、**class system-cpp-police-protocol-snooping** CPU キューが有効になり、ポリサー レートは **2000 pps** です。

```
デバイス> enable
デバイス# configure terminal
デバイス(config)# policy-map system-cpp-policy
```

```
デバイス(config-pmap)# class system-cpp-police-protocol-snooping
デバイス(config-pmap-c)# police rate 2000 pps
デバイス(config-pmap-c-police)# end


デバイス# show policy-map control-plane
Control Plane

  Service-policy input: system-cpp-policy

    <output truncated>


    Class-map: system-cpp-police-dot1x-auth (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: none
      police:
          rate 1000 pps, burst 244 packets
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop

    Class-map: system-cpp-police-protocol-snooping (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: none
      police:
          rate 2000 pps, burst 488 packets
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop

    <output truncated>

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

# 例：CPU キューの無効化

次に、CPU キューをディセーブルにする例を示します。ここでは、**class system-cpp-police-protocol-snooping** CPU キューが無効になります。

```
デバイス> enable
デバイス# configure terminal
デバイス(config)# policy-map system-cpp-policy
デバイス(config-pmap)# class system-cpp-police-protocol-snooping
デバイス(config-pmap-c)# no police rate 100 pps
デバイス(config-pmap-c)# end


デバイス# show running-config | begin system-cpp-policy

policy-map system-cpp-policy
```

```
 class system-cpp-police-data
  police rate 200 pps
 class system-cpp-police-sys-data
  police rate 100 pps
 class system-cpp-police-sw-forward
  police rate 1000 pps
 class system-cpp-police-multicast
  police rate 500 pps
 class system-cpp-police-multicast-end-station
  police rate 2000 pps
 class system-cpp-police-punt-webauth
 class system-cpp-police-l2-control
 class system-cpp-police-routing-control
  police rate 500 pps
 class system-cpp-police-control-low-priority
 class system-cpp-police-wireless-priority1
 class system-cpp-police-wireless-priority2
 class system-cpp-police-wireless-priority3-4-5
 class system-cpp-police-topology-control
 class system-cpp-police-dot1x-auth
 class system-cpp-police-protocol-snooping
 class system-cpp-police-forus
 class system-cpp-default

<output truncated>
```

# 例：すべてのCPUキューに対するデフォルトのポリサーレートの設定

次に、すべての CPU キューのポリサー レートをデフォルトに設定し、その後に設定を確認する例を示します。

```
デバイス> enable
デバイス# configure terminal
デバイス(config)# cpp system-default
Defaulting CPP : Policer rate for all classes will be set to their defaults
デバイス(config)# end

Device# show platform hardware fed switch 1 qos queue stats internal cpu policer
CPU Queue Statistics
==========================================================================================

                                                (default) (set)     Queue        Queue
QId PlcIdx  Queue Name                Enabled   Rate      Rate      Drop(Bytes)
Drop(Frames)
------------------------------------------------------------------------------------------
0    11     DOT1X Auth                 Yes      1000      1000      0            0

1    1      L2 Control                 Yes      2000      2000      0            0

2    14     Forus traffic              Yes      4000      4000      0            0

3    0      ICMP GEN                   Yes      600       600       0            0

4    2      Routing Control            Yes      5400      5400      0            0

5    14     Forus Address resolution   Yes      4000      4000      0            0

6    0      ICMP Redirect              Yes      600       600       0            0

7    16     Inter FED Traffic          Yes      2000      2000      0            0
```

```
8    4      L2 LVX Cont Pack            Yes     1000      1000     0            0

9    16     EWLC Control                Yes     2000      2000     0            0

10   16     EWLC Data                   Yes     2000      2000     0            0

11   13     L2 LVX Data Pack            Yes     1000      1000     0            0

12   0      BROADCAST                   Yes     600       600      0            0

13   10     Openflow                    Yes     100       100      0            0

14   13     Sw forwarding               Yes     1000      1000     0            0

15   8      Topology Control            Yes     13000     13000    0            0

16   12     Proto Snooping              Yes     2000      2000     0            0

17   6      DHCP Snooping               Yes     500       500      0            0

18   9      Transit Traffic             Yes     500       500      0            0

19   10     RPF Failed                  Yes     100       100      0            0

20   15     MCAST END STATION           Yes     2000      2000     0            0

21   13     LOGGING                     Yes     1000      1000     0            0

22   7      Punt Webauth                Yes     1000      1000     0            0

23   18     High Rate App               Yes     13000     13000    0            0

24   10     Exception                   Yes     100       100      0            0

25   3      System Critical             Yes     1000      1000     0            0

26   10     NFL SAMPLED DATA            Yes     100       200      0            0

27   2      Low Latency                 Yes     5400      5400     0            0

28   10     EGR Exception               Yes     100       100      0            0

29   5      Stackwise Virtual OOB       Yes     8000      8000     0            0

30   9      MCAST Data                  Yes     500       500      0            0

31   10     Gold Pkt                    Yes     100       100      0            0

* NOTE: CPU queue policer rates are configured to the closest hardware supported value

                      CPU Queue Policer Statistics
======================================================================
Policer    Policer Accept   Policer Accept  Policer Drop  Policer Drop
  Index         Bytes          Frames        Bytes          Frames
----------------------------------------------------------------------
0          0                0               0             0
1          0                0               0             0
2          0                0               0             0
3          0                0               0             0
4          0                0               0             0
5          0                0               0             0
6          0                0               0             0
```

```
7          0                0               0             0
8          0                0               0             0
9          0                0               0             0
10         0                0               0             0
11         0                0               0             0
12         0                0               0             0
13         0                0               0             0
14         0                0               0             0
15         0                0               0             0
16         0                0               0             0
17         0                0               0             0
18         0                0               0             0

                        CPP Classes to queue map
==========================================================================================
PlcIdx CPP Class                                :  Queues
------------------------------------------------------------------------------------------
0      system-cpp-police-data                   :  ICMP GEN/BROADCAST/ICMP Redirect/
10     system-cpp-police-sys-data               :  Openflow/Exception/EGR Exception/NFL
 SAMPLED DATA/Gold Pkt/RPF Failed/
13     system-cpp-police-sw-forward             :  Sw forwarding/LOGGING/L2 LVX Data
Pack/
9      system-cpp-police-multicast              :  Transit Traffic/MCAST Data/
15     system-cpp-police-multicast-end-station  :  MCAST END STATION /
7      system-cpp-police-punt-webauth           :  Punt Webauth/
1      system-cpp-police-l2-control             :  L2 Control/
2      system-cpp-police-routing-control        :  Routing Control/Low Latency/
3      system-cpp-police-system-critical        :  System Critical/
4      system-cpp-police-l2lvx-control          :  L2 LVX Cont Pack/
8      system-cpp-police-topology-control       :  Topology Control/
11     system-cpp-police-dot1x-auth             :  DOT1X Auth/
12     system-cpp-police-protocol-snooping      :  Proto Snooping/
6      system-cpp-police-dhcp-snooping          :  DHCP Snooping/
14    system-cpp-police-forus                :  Forus Address resolution/Forus traffic/
5      system-cpp-police-stackwise-virt-control :  Stackwise Virtual OOB/
16     system-cpp-default                       :  Inter FED Traffic/EWLC Control/EWLC
Data/
18     system-cpp-police-high-rate-app          :  High Rate App/
```

# 例：ユーザ定義のクラスマップの作成

デバイス

次に、ユーザ定義のクラスマップを作成し、それを `system-cpp-policy` に適用して、ポリシーの適用場所に関する情報を表示する例を示します。

ユーザ定義のクラスマップが `system-cpp-policy` に適用されます。つまり、ユーザ定義のクラスマップ `class-cpp-user` に一致する制御トラフィックは、ユーザ定義のクラスマップでの集約ポリサーによって異なります。ユーザ定義トラフィック クラスの統計情報はバイト単位で報告されます。

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map match-any class-cpp-user
Device(config-cmap)# match dscp cs1
Device(config-cmap)# exit
Device(config)# policy-map system-cpp-policy
Device(config-pmap)# class class-cpp-user
```

```
Device(config-pmap-c)# police rate 2m bps
Device(config-pmap-c-police)# end

Device# show policy-map control-plane
<output truncated>
Class-map: class-cpp-user (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match:  dscp cs1 (8)
      police:
          rate 2000000 bps, burst 62500 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps
<output truncated>
```

ユーザ定義のクラスマップを `system-cpp-policy` に追加すると、システムはコントロールプレーンに加えて、32 個すべての CPU キューに自動的にそれをインストールします（結果としてポリシーのインスタンスは 33 個になります）。

入力で system-cpp-policy が適用されていても、方向が出力（OUT）としてどのように表示されるかに注意してください。

```
Device# show platform software fed switch active qos policy target status

TCG status summary:

Loc Interface             IIF-ID           Dir State:(cfg,opr) Policy
--- --------------------- ---------------- --- --------------- --------------------
?:255 Control Plane       0x00000001000001 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-0          0x0000000100000d OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-1          0x0000000100000e OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-2          0x0000000100000f OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-3          0x00000001000010 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-4          0x00000001000011 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-5          0x00000001000012 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-6          0x00000001000013 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-7          0x00000001000014 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-8          0x00000001000015 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-9          0x00000001000016 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-10         0x00000001000017 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-11         0x00000001000018 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-12         0x00000001000019 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-13         0x0000000100001a OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-14         0x0000000100001b OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-15         0x0000000100001c OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-16         0x0000000100001d OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-17         0x0000000100001e OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-18         0x0000000100001f OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-19         0x00000001000020 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-20         0x00000001000021 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-21         0x00000001000022 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-22         0x00000001000023 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-23         0x00000001000024 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-24         0x00000001000025 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-25         0x00000001000026 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-26         0x00000001000027 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-27         0x00000001000028 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-28         0x00000001000029 OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-29         0x0000000100002a OUT VALID,SET_INHW  system-cpp-policy
```

```
?:0 CoPP-Queue-30         0x0000000100002b OUT VALID,SET_INHW  system-cpp-policy
?:0 CoPP-Queue-31         0x0000000100002c OUT VALID,SET_INHW  system-cpp-policy
```

# CoPP のモニタリング

CPU キューのトラフィックタイプやポリサーレート（ユーザが設定したレートやデフォルトのレート）などのポリサー設定を表示するには、次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| **show policy-map control-plane** | さまざまなトラフィックタイプに設定されたレートを表示します。 |
| **show policy-map system-cpp-policy** | system-cpp ポリシーの下で設定されたすべてのクラスとポリサーレートを表示します。 |
| **show platform hardware fed switch** {*switch-number* } **qos que stats internal cpu policer** | さまざまなトラフィックタイプに設定されたレートを表示します。 |
| **show platform software fed** {*switch-number* } **qos policy target status** | ポリシーステータスとターゲットポートタイプに関する情報を表示します。 |

# CoPP の機能履歴と情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

| 機能 | リリース | 機能情報 |
|---|---|---|
| コントロールプレーンポリシング（CoPP）または CPP | Cisco IOS XE 3.3SE | この機能が導入されました。 |
| CoPP の CLI コンフィギュレーション | Cisco IOS XE Denali 16.1.2 | この機能はユーザ設定可能です。CPU キューの有効化および無効化、ポリサー レートの変更、およびポリサー レートのデフォルトへの設定を行うための CLI 設定オプション。 |
| ユーザ定義のクラスマップ | Cisco IOS XE Everest 16.5.1a | このリリース以降、（フィルタ付きの）クラスマップを作成し、これらのユーザ定義のクラスマップを system-cpp-policy に追加できます。 |

| 機能 | リリース | 機能情報 |
| --- | --- | --- |
| CoPP のシステム定義値の変更 | Cisco IOS XE Everest 16.6.1 | 次の新しいシステム定義のクラスが導入されました。<br>• system-cpp-police-stackwise-virt-control<br>• system-cpp-police-l2lvx-control<br><br>次の新しい CPU キューが既存の system-cpp-default クラスに追加されました。<br>• WK_CPU_Q_UNUSED (7)<br>• WK_CPU_Q_EWLC_CONTROL(9)<br>• WK_CPU_Q_EWLC_DATA(10)<br><br>この新しい CPU キューが既存の system-cpp-police-sw-forward に追加されました。WK_CPU_Q_L2_LVX_DATA_PACK (11)<br>この CPU キューは使用できなくなりました。WK_CPU_Q_SGT_CACHE_FULL(27) |